HomePlug GREEN PHY Specification

Release Version 1.1

February 8, 2012

	Added new Power Management	

© 2010, 2012 HomePlug Power Alliance. ALL RIGHTS RESERVED
Notice: No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of HomePlug Power Alliance. HomePlug Power Alliance reserves the right to make changes to this specification at any time without notice and assumes no responsibility for its use. This specification contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire specification will be updated and distributed to all registered users.
Trademarks
"HomePlug" is a registered trademark of the HomePlug Powerline Alliance, Inc. in the United States and other countries. All product names and logos are trade and service marks of their respective companies.

Change History

GP1.1	**Corrected CRC-24 remainder equation per contribution:"STM_SE110429-00_r0_CRC-24 Correction.docx"**	**Jim Allen (ST)**
	Updated GP1.1 labels and Copyright dates	
	Added missing text for DC operation per contribution:" ATHR_AV110207-01_r1_DC Support.docx" in 5.1.1.1 and new 5.1.1.2	

	Added new Power Management features	
	Added informative information on how to calculate the PHY rate to clause 3.4.4	
	Added clarification about informative text to clause 1.4.1	
	Added Association text clarifications, r9	
	Updated references, ToC and index, fix clause indents	

HomePlug Limited Copyright License Agreement

By receiving, installing, copying, reviewing or otherwise using the HomePlug Green PHY Specification (the "***Specification***"), you (the "***Specification Recipient***") agree to the terms and conditions of this HomePlug Limited Copyright License Agreement (the "***Agreement***") by and between the HomePlug Powerline Alliance, Inc. ("***HomePlug***") and Specification Recipient.

NO HOMEPLUG SPONSOR MEMBER, CONTRIBUTOR ASSOCIATE, PARTICIPANT ASSOCIATE OR ADOPTER ASSOCIATE SHALL BE BOUND TO THE TERMS OR CONDITIONS OF THIS AGREEMENT WHILE IT IS A HOMEPLUG OR ASSOCIATE MEMBER. THIS AGREEMENT DOES BIND ALL HOMEPLUG SUPPORTER ASSOCIATES AND NON-MEMBERS.

- **The Specification.** "Specification" shall mean this HomePlug Logical Green PHY Specification document. HomePlug reserves the right to change the Specification at any time without notice to Specification Recipient.
- **Limited Copyright Grant.** Provided Specification Recipient complies with all terms and conditions of this Agreement, HomePlug grants Specification Recipient a non-exclusive, revocable, temporary, royalty-free, personal copyright to electronically store, display, and print the Specification.
- **Other Restrictions.** Specification Recipient shall not reproduce and/or distribute the Specification.
- **Ownership of the Specification.** All title and intellectual property in and to the Specification are owned by HomePlug and its licensor(s), if any.
- **Termination.** This Agreement and any and all rights hereunder may be terminated by HomePlug upon notice for any reason or no reason at all. Upon termination of this Agreement, Specification Recipient shall immediately cease any and all use of the Specification and destroy all copies of the Specification within its control.
- **No Warranties.** SPECIFICATION RECIPIENT ACKNOWLEDGES AND AGREES THAT THE SPECIFICATION IS PROVIDED "AS IS" AND WITH NO WARRANTIES WHATSOEVER, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, TITLE, FITNESS OF ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF THE SPECIFICATION AND/OR THIS AGREEMENT. THE SPECIFICATION RECIPIENT'S USE OF THE SPECIFICATION IS SOLELY AT THE SPECIFICATION RECIPIENT'S OWN RISK.
- **Limitation of Liability.** IN NO EVENT SHALL HOMEPLUG OR ANY HOMEPLUG MEMBER OR ASSOCIATE MEMBER BE LIABLE OR OBLIGATED TO THE SPECIFICATION RECIPIENT OR ANY THIRD PARTY IN ANY MANNER FOR ANY DIRECT, SPECIAL, NON-COMPENSATORY, CONSEQUENTIAL, INDIRECT, INCIDENTAL, STATUTORY OR PUNITIVE DAMAGES OF ANY KIND, INCLUDING, WITHOUT LIMITATION, LOST PROFITS AND LOST REVENUE, REGARDLESS OF THE FORM OF

ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT PRODUCT LIABILITY, OR OTHERWISE, EVEN IF HOMEPLUG OR ANY HOMEPLUG MEMBER HAS BEEN INFORMED OF OR IS AWARE OF THE POSSIBILITY OF ANY SUCH DAMAGES IN ADVANCE. THE LIMITATIONS SET FORTH ABOVE SHALL BE DEEMED TO APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDIES AVAILABLE TO THE SPECIFICATION RECIPIENT. THE SPECIFICATION RECIPIENT ACKNOWLEDGES AND AGREES THAT THE SPECIFICATION RECIPIENT HAS FULLY CONSIDERED THE FOREGOING ALLOCATION OF RISK AND FINDS IT REASONABLE, AND THAT THE FOREGOING LIMITATIONS ARE AN ESSENTIAL BASIS OF HOMEPLUG AND THE HOMEPLUG MEMBERS PERMITTING ACCESS TO THE SPECIFICATION. SPECIFICATION RECIPIENT FURTHER ACKNOWLEDGES AND AGREES THAT HOMEPLUG AND THE HOMEPLUG MEMBERS AND ASSOCIATE MEMBERS WOULD NOT HAVE PROVIDED THE SPECIFICATION RECIPIENT WITH ACCESS TO THE SPECIFICATION UNLESS THE SPECIFICATION RECIPIENT FULLY AGREED TO THE LIMITATIONS SET FORTH ABOVE. SPECIFICATION RECIPIENTS' SOLE AND EXCLUSIVE REMEDIES AND EXCLUSIVE LIABILITIES ARE SET FORTH IN THIS AGREEMENT.

- **Third Party Rights.** Certain elements of the Specification may be subject to third party intellectual property rights, including without limitation, patent, trademark and copyright rights. HomePlug is not responsible and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

- **Non-Applicability to Certain HomePlug Members and Associate Members.** Notwithstanding anything to the contrary in this Agreement, no HomePlug Sponsor Member, Contributor Associate, Participant Associate or Adopter Associate shall be bound to the terms or conditions of this Agreement while it is a member of HomePlug. This Agreement does bind all HomePlug Supporter Associates and non-members.

- **General**. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not invalidate or render unenforceable any other part of this Agreement, but this Agreement shall be construed as not containing the particular provision or provisions held to be invalid or unenforceable. No delay or omission by either party to exercise any right occurring upon any noncompliance or default by the other party with respect to any of the terms of this Agreement shall impair any such right or power or be construed to be a waiver thereof. A waiver by either of the parties hereto of any of the covenants, conditions or agreements to be performed by the other shall not be construed to be a waiver of any succeeding breach thereof or of any covenant, condition or agreement herein contained. Nothing set forth in this Agreement shall be deemed or construed to render the parties as joint venturers, partners or employer and employee. This Agreement, together with any documents referenced herein, sets forth the entire, final and exclusive agreement between the parties as to the subject matter hereof and supersedes all prior and contemporaneous agreements, understandings, negotiations and discussions, whether oral or written, between the parties; provided, however, that a HomePlug Sponsor Member, Contributor Associate, Participant Associate, Adopter Associate shall not be

bound to the terms of this Agreement while it is a HomePlug Member or Associate Member. This Agreement may be modified only pursuant to a writing executed by authorized representatives of HomePlug and Specification Recipient. This Agreement, and all the rights and duties of the parties arising from or relating in any way to the subject matter of this Agreement or the transaction(s) contemplated by it, shall be governed by, construed and enforced in accordance with the laws of the State of California (excluding any conflict of laws provisions of the State of California that would refer to and apply the substantive laws of another jurisdiction). **SPECIFICATION RECIPIENT CONSENTS TO THE EXCLUSIVE PERSONAL JURISDICTION OF THE FEDERAL AND STATE COURTS AND VENUE LOCATED IN SAN FRANCISCO, CALIFORNIA.**

- **Trademarks.** HomePlug is a registered trademark or service mark of the HomePlug Powerline Alliance, Inc. in the US and other countries. All other trademarks, registered trademarks, or service marks used in this document are the property of their respective owners and are hereby recognized. Specification Recipient shall not have any rights to reproduce HomePlug's trademarks or service marks except with HomePlug's prior written consent.

Table of Contents

List of Figures xxiv
List of Tables xxviii
List of Equations xxxvii
Chapter 1 Introduction 1
1.1 References 1
1.2 File Integrity Verification 2
1.3 Acronyms and Abbreviations 2
1.4 Conventions 11
1.4.1 Informative Text 11
1.4.2 Binary and Hexadecimal Numbers 11
1.4.3 Words and Phrases 12
1.4.4 Abbreviations 12
1.4.5 Message Nomenclature 13
1.4.6 Message Nomenclature 14
1.5 Overview of HomePlug Green PHY - A Low Power, Legacy Interoperable, Highly Reliable PLC from HomePlug 16
1.5.1 Comparisons between HomePlug GREEN PHY and HomePlug AV PHY [Informative] 17
1.5.2 Differences between HomePlug GREEN PHY and HomePlug AV PHY [Informative] 17
1.5.3 Differences between HomePlug GREEN PHY MAC (and above) and HomePlug AV MAC (and above) [Informative] 19
1.5.4 Identical Requirements for HomePlug GREEN PHY and HomePlug AV PHY 23
Chapter 2 System Overview 25
2.1 Network Reference Block Diagram 25
2.1.1 System Reference Model 25
2.1.2 Protocol Layer Diagram 26
2.2 Network Concepts 27
2.2.1 Physical Network 27
2.2.2 Logical Networks and SubAVLNs 27
2.2.3 Communication Inside an AVLN 28
2.3 Station Roles 30
2.4 Security Overview 31
2.4.1 Security Goals and Constraints 31
2.4.2 Threat Model 31
2.5 HomePlug GREEN PHY Operation Under Various Regulatory Jurisdictions 32
2.6 Parameter Specifications 32
Chapter 3 PHY Specification 35
3.1 Overview of HomePlug GREEN PHY 35
3.2 PPDU Structure and Generation 37

3.2.1 PPDU Formats 37
3.2.1.1 PPDU Formats for GREEN PHY 38
3.2.2 PPDU Structure 38
3.2.3 Symbol Timing 39
3.2.3.1 Guard Interval Timing for GREEN PHY 41
3.3 Frame Control Forward Error Correction 41
3.3.1 Frame Control Bits Flow 41
3.3.2 Turbo Convolutional Code Encoder 41
3.3.3 Frame Control Interleaver 42
3.3.4 Diversity Copier 42
3.4 Payload Forward Error Correction (FEC) Processing43
3.4.1 Scrambler 44
3.4.2 Turbo Convolutional Encoder 44
3.4.2.1 Turbo Convolutional Encoder for GREEN PHY 45
3.4.2.2 Constituent Encoders 45
3.4.2.3 Termination 46
3.4.2.4 Puncturing 47
3.4.2.5 Turbo Interleaving 48
3.4.3 Channel Interleaver 49
3.4.3.1 Channel Interleaver for GREEN PHY 52
3.4.4 ROBO Modes 52
3.4.4.1 ROBO Interleaver 54
3.5 Mapping 58
3.5.1 Empty Tone Filling 59
3.5.2 Last Symbol Padding 59
3.5.3 Mapping Reference 61
3.5.4 Mapping for Frame Control Coherent QPSK 66
3.5.5 Mapping for BPSK, QPSK, 8-QAM, 16-QAM, 64-QAM, 256-QAM, 1024-QAM 66
3.5.6 Mapping for ROBO-AV 70
3.6 Symbol Generation 70
3.6.1 Preamble 70
3.6.2 HomePlug 1.0.1 Frame Control 77
3.6.3 Frame Control 79
3.6.4 Payload Symbols 80
3.6.5 Priority Resolution Symbol 81
3.6.6 Relative Power Levels 83
3.6.7 Tone Mask 84
3.6.8 Amplitude Map 88
3.7 Transmitter Electrical Specification 88
3.7.1 Transmit Spectrum Mask 89
3.7.2 Spurious Transmission 90

3.7.3 Transmitter Accuracy 90
3.7.3.1 PHY Clock Frequency Tolerance 90
3.7.3.2 Transmit Constellation Error 91
3.7.3.3 Transmit Modulation Accuracy Test 91
3.8 Receiver Electrical Specification 97
3.8.1 Receiver Sensitivity 97
3.8.1.1 Receiver Minimum Input Voltage 98
3.8.1.2 Receiver Maximum Input Voltage 98
3.8.2 Receiver Input Impedance 98
3.8.3 Immunity to Narrowband Interference 98
3.8.4 Physical Carrier Sense 99
3.8.4.1 Detection of Priority Resolution Symbols 99
3.8.4.2 Detection of Preamble Symbols 100
Chapter 4 Frame Formats 101
4.1 Bit and Octet Order 101
4.1.1 Text Conventions 101
4.1.1.1 Binary Fields 101
4.1.1.2 Hexadecimal Fields 101
4.1.2 Bit and Octet Transmission Order at the MAC-PHY Interface 102
4.2 Cyclic Redundancy Check Calculation 105
4.2.1 CRC-32 105
4.2.2 CRC-24 106
4.3 MAC Frame Format 106
4.3.1 MAC Frame Header 107
4.3.1.1 MAC Frame Type (MFT) 107
4.3.1.2 MAC Frame Length (MFL) 109
4.3.2 Arrival Time Stamp 109
4.3.2.1 Arrival Time Stamp for GREEN PHY 109
4.3.3 Confounder 110
4.3.4 MSDU Payload 110
4.3.5 Management Message 110
4.3.6 Integrity Check Value 110
4.4 MAC Protocol Data Unit (MPDU) Format 111
4.4.1 MPDU Frame Control Fields 113
4.4.1.1 HomePlug 1.0.1 Frame Control 114
4.4.1.2 Delimiter Type (DT_AV) 114
4.4.1.3 Access Field (ACCESS) 114
4.4.1.4 Short Network ID (SNID) 115
4.4.1.5 Variant Fields (VF_AV) 115
4.4.1.6 Frame Control Check Sequence (FCCS_AV) 151
4.4.2 Format of Long MPDU Payload 151
4.4.2.1 Format of PHY Blocks 152

4.4.3 Format of Beacon MPDU Payload 156
4.4.3.1 Network Identifier (NID) 158
4.4.3.2 Hybrid Mode (HM) 160
4.4.3.3 Source Terminal Equipment Identifier (STEI) 160
4.4.3.4 Beacon Type (BT) 160
4.4.3.5 Non-Coordinating Networks Reported (NCNR) 161
4.4.3.6 Network Power Saving Mode (NPSM) 162
4.4.3.7 Number of Beacon Slots (NumSlots) 162
4.4.3.8 Beacon Slot Usage (SlotUsage) 162
4.4.3.9 Beacon Slot ID (SlotID) 163
4.4.3.10 AC Line Cycle Synchronization Status (ACLSS) 163
4.4.3.11 Handover-in-Progress (HOIP) 163
4.4.3.12 RTS Broadcast Flag (RTSBF) 164
4.4.3.13 Network Mode (NM) 164
4.4.3.14 CCo Capability (CCoCap) 165
4.4.3.15 Beacon Management Information (BMI) 165
4.4.3.16 Octet Pad (OPAD) 193
4.4.3.17 Beacon Payload Check Sequence (BPCS) 193
4.4.3.18 Proxy Level (Plevel) for GREEN PHY 193
4.4.3.19 Reusable SNID Flag (RSF) for GREEN PHY 193
4.4.4 Format of Sound MPDU Payload 194
Chapter 5 MAC Functional Description 195
5.1 Beacon Period Structure and Channel Access Mechanism 195
5.1.1 Beacon Period and AC Line Cycle Synchronization 195
5.1.1.1 Line Cycle Synchronization 195
5.1.2 Beacon Period Structure 198
5.1.2.1 Beacon Period Structure in CSMA-Only Mode 202
5.1.2.2 Beacon Period Structure in Uncoordinated Mode 204
5.1.2.3 Beacon Period Structure in Coordinated Mode 205
5.1.3 Channel Access 208
5.1.3.1 CSMA/CA Channel Access 208
5.1.3.2 TDMA Channel Access 210
5.2 Control Plane 211
5.2.1 Connections and Links 211
5.2.1.1 Global Links 213
5.2.1.2 Local Links 213
5.2.1.3 Connectionless “Links” 213
5.2.1.4 Link and Connection Identifiers 214
5.2.2 Transport Services 217
5.2.2.1 Connectionless Service (CLS) 217
5.2.2.2 Connection-Oriented Service (COS) 218
5.2.3 Connection Services 218

5.2.3.1 Connection Setup 218
5.2.3.2 Global Link Setup 221
5.2.3.3 Latency Effects on Global Link Setup 221
5.2.3.4 Connection Monitoring 222
5.2.3.5 Connection Teardown 222
5.2.3.6 Connections and Network Modes 226
5.2.3.7 Connection Reconfiguration 227
5.2.3.8 Global Link Reconfiguration Triggered by CCo 229
5.2.4 Connection Services for Broadcast/Multicast 232
5.2.4.1 Broadcast/Multicast Connection using Multiple Unicast Connections 233
5.2.5 Detect-and-Report Procedure 233
5.2.6 Channel Estimation 235
5.2.6.1 Channel Estimation Procedure 235
5.2.6.2 Dynamic Channel Adaptation 239
5.2.6.3 Maintenance of Tone Maps 243
5.2.6.4 Tone Map Intervals 243
5.2.6.5 Priority of Channel Estimation Response 244
5.2.6.6 Channel Estimation with Respect to the AC Line Cycle 245
5.2.6.7 HomePlug GREEN PHY Handling of Channel Estimation Requests from HomePlug AV 245
5.2.7 Link Status Function 246
5.2.8 Beacon Relocation Procedure 247
5.2.9 Signal Level Attenuation Characterization 248
5.3 Bridging 248
5.3.1 Acting as an AV Bridge 249
5.3.1.1 Behavior for Incoming Traffic from the Powerline Network 249
5.3.1.2 Behavior for Incoming Traffic from the Bridged Network 250
5.3.2 Communicating through an AV Bridge 250
5.3.2.1 Communication with a Known DA 251
5.3.2.2 Communicating with an Unknown DA 252
5.3.3 Bridging with Quality of Service 253
5.4 Data Plane 253
5.4.1 Communication between Associated and Authenticated STAs 254
5.4.1.1 MAC Frame Generation 254
5.4.1.2 MAC Frame Streams 255
5.4.1.3 Segmentation 257
5.4.1.4 Long MPDU Generation 258
5.4.1.5 Reassembly 259
5.4.1.6 Buffer Management, Flow Control, and Duplicate Detection 260
5.4.2 Communication between Associated but Unauthenticated STAs 268
5.4.3 Communication between STAs Not Associated with the Same AVLN 269
5.4.3.1 Multi-Network Broadcast 271

5.4.4 Summary of the MAC Frame Streams at STA 272
5.4.4.1 MAC Frame Streams for a STA That is Not Associated with Any AVLN 273
5.4.4.2 MAC Frame Streams for STA That is Associated but Not Authenticated with an AVLN 273
5.4.4.3 MAC Frame Streams for a STA That is Associated and Authenticated with an AVLN 273
5.4.5 Data Encryption 275
5.4.5.1 Encryption Method 275
5.4.5.2 PHY Block Body Encryption Bit Order 275
5.4.5.3 Initialization Vector Generation and Bit Order 275
5.4.5.4 PHY Block Body Encryption Key Bit Order 276
5.4.6 MPDU Bursting 276
5.4.6.1 MPDU Bursting for GREEN PHY 278
5.4.7 Bidirectional Bursting 278
5.4.7.1 Bidirectional Bursting during CSMA 280
5.4.7.2 Connections and Links during Bidirectional Bursts 282
5.4.7.3 Encryption of RSOF Payload 282
5.4.7.4 Bidirectional Bursting for GREEN PHY 283
5.4.8 Automatic Repeat reQuest (ARQ) 283
5.4.8.1 Selective ACK (SACK) 283
5.4.8.2 Retransmission 285
5.4.8.3 Broadcast/Multicast and Partial Acknowledgement 286
5.5 PHY Clock and Network Time Base Synchronization 286
5.5.1 BTS in Proxy Beacons 289
5.5.2 BTS in Discover Beacons 289
5.5.3 Arrival Time Stamp for MSDU Jitter and Delay Control 289
5.5.4 PHY Clock Correction 290
5.5.4.1 PHY Clock Correction When Participating in More Than One Network 290
5.5.5 Allocation Boundaries 290
5.6 Interframe Spacing 291
5.6.1 Measurement of Interframe Spacing 294
5.7 (deliberately blank - reserved for future use – avoiding section renumbering) (GREEN PHY) 294
5.8 Distributed Bandwidth Control for GREEN PHY 295
5.9 Power Save Mode for GREEN PHY 297
5.9.1 Basic Approach 297
5.9.2 Distribution of Power Save State information 300
5.9.3 CCo Power Save 301
5.9.4 Handling of Broadcast/Multicast transmissions 301
5.9.5 Network State changes and Power Save 302
5.9.6 Power Save and HomePlug AV 1.1 302
5.10 Routing and Repeating for GREEN PHY 303

5.10.1 GREEN PHY Station Acting as a Repeater for Unicast MSDUs 303
5.10.1.1 Local Routing Table for GREEN PHY 303
5.10.1.2 Communication between the CCo and a Hidden PCo for GREEN PHY 305
5.10.2 GREEN PHY Station Acting as a Repeater for Broadcast or Multicast MPDUs 305
5.10.2.1 Broadcast and Multicast Repeating Assignment for GREEN PHY 305
5.10.2.2 Broadcast and Multicast Repeating for GREEN PHY 306
5.11 Transmit Power Control for GREEN PHY 306
Chapter 6 Convergence Layer Functions 307
6.1 Overview 307
6.2 Classifier 307
6.2.1 Classifier Configuration 308
6.2.2 Classifier-Initiated (Automatic) Connection Setup 308
6.2.3 Ethernet SAP Classifier Rules 308
6.2.4 Packet Classification in HomePlug GREEN PHY 312
6.3 Ethernet SAP Classifier Rule Set Format 313
6.4 De-muxing 314
6.5 QoS Monitoring 314
6.6 Auto-Connect Service 314
6.6.1 Evaluation of Data Flow 315
6.6.2 ACS Processing 316
6.6.2.1 Data Flow Evaluation 316
6.6.2.2 After Data Flow Evaluation is Complete 316
6.6.2.3 Monitoring Automatic Connections 317
6.6.3 Auto Connect Service for GREEN PHY 317
6.7 Smoothing (Delay Compensation, Jitter Control) 317
6.7.1 Point-to-Point Smoothing 318
6.7.2 End-to-End Smoothing 318
6.7.3 Smoothing Control 318
6.7.3.1 Smoothing (Delay Compensation, Jitter Control) for GREEN PHY 319
Chapter 7 Central Coordinator 321
7.1 Power-On Network Discovery Procedure 321
7.2 STA Behavior After Power-on 323
7.2.1 Unassociated STA Behavior 324
7.2.2 Unassociated CCo Behavior 325
7.2.3 Behavior as a STA in an AVLN 326
7.2.3.1 Identifying HomePlug GREEN PHY Stations 327
7.2.4 Behavior as a CCo in an AVLN 327
7.2.5 Deciding AV-Only or Hybrid Mode 328
7.3 Forming or Joining an AVLN 329
7.3.1 AVLN Overview 329
7.3.1.1 Network Identification 329
7.3.1.2 Human-Friendly Station and AVLN Names 330

7.3.1.3 Get Full AVLN Information 330
7.3.1.4 Get Full STA Information 331
7.3.2 Association 331
7.3.2.1 TEI Assignment and Renewal 333
7.3.3 Method for Authentication 335
7.3.4 Forming a New AVLN 336
7.3.4.1 Two Unassociated STAs with Matching NIDs 337
7.3.4.2 Two Unassociated STAs Form an AVLN Using a DAK-encrypted NMK 340
7.3.4.3 Two Unassociated STAs: One in SC-Add and One in SC-Join 342
7.3.4.4 Two Unassociated STAs: Both in SC-Join 344
7.3.5 Joining an Existing AVLN 346
7.3.5.1 Matching NIDs 346
7.3.5.2 DAK-encrypted NMK 348
7.3.5.3 SC-Join and SC-Add 350
7.3.6 Leaving an AVLN 352
7.3.7 Removing a Station from an AVLN 353
7.4 Selection of CCo 353
7.4.1 CCo Selection for a New AVLN 353
7.4.1.1 Determination of SNID by a STA Acting as CCo in a Newly Formed AVLN (GREEN PHY) 354
7.4.2 User-Appointed CCo 354
7.4.3 Auto-Selection of CCo 356
7.4.3.1 CCo Capability 357
7.4.3.2 Order for Selection of CCo 357
7.5 Transfer/Handover of CCo Functions 358
7.6 Discover Process 361
7.6.1 Overview 361
7.6.1.1 Discover Beacons 361
7.6.1.2 Discovered STA List and Discovered Network List 362
7.6.1.3 Topology Table 362
7.6.1.4 Discover Period 363
7.6.2 Procedures 364
7.7 Proxy Networking with GREEN PHY Extensions to Support Routing and Repeating 364
7.7.1 Identification of Hidden Stations 366
7.7.2 Association of Hidden Station 366
7.7.3 Instantiation of Proxy Network 369
7.7.3.1 Selecting a PCo 369
7.7.3.2 PCo-Required Tasks 370
7.7.4 Proxy Beacons 370
7.7.5 Provisioning the NMK to Hidden Stations 370
7.7.6 Provisioning NEK for Hidden Stations (Authenticating the HSTA) 371

7.7.7 Exchange of MMEs Through a PCo 371
7.7.8 Transitioning from Being a STA to Being an HSTA 371
7.7.9 Transitioning from Being an HSTA to Being a STA 372
7.7.10 Recovering from the Loss of a PCo 372
7.7.11 Proxy Network Shutdown 372
7.7.12 Proxy Network Limitations 373
7.8 Bandwidth Manager 373
7.8.1 Connection Specification (CSPEC) 373
7.8.1.1 Connection Descriptor (CDESC) 381
7.8.1.2 Vendor-Specific QoS and MAC Parameters 382
7.8.1.3 Ordering of Fields within the CSPEC 383
7.8.1.4 Surplus Bandwidth 383
7.8.1.5 Minimum Set of QoS and MAC Parameters 383
7.8.1.6 CSPEC Reconfigurability 384
7.8.1.7 Connection Specification (CSPEC) for GREEN PHY 384
7.8.2 Scheduler and Bandwidth Allocation 384
7.8.2.1 Scheduler and Bandwidth Allocation for GREEN PHY 386
7.8.3 Connection Admission Control 386
7.8.3.1 Connection Admission Control for GREEN PHY 386
7.8.4 Beacon Period Configuration 387
7.8.5 Bandwidth Allocation for GREEN PHY 387
7.9 Backup CCo and CCo Failure Recovery 388
7.9.1 Backup CCo 388
7.9.2 CCo Failure Recovery 388
7.10 Security 389
7.10.1 Security Overview 389
7.10.2 Encryption Keys, Pass Phrases, Nonces, and Their Uses 390
7.10.2.1 Device Access Key (DAK) 390
7.10.2.2 Device Password (DPW) 391
7.10.2.3 Network Membership Key (NMK) 391
7.10.2.4 Network Password (NPW) 391
7.10.2.5 Network Encryption Key (NEK) 391
7.10.2.6 Temporary Encryption Key (TEK) 392
7.10.2.7 Nonces 392
7.10.3 Methods for Authorization (NMK Provisioning) 392
7.10.3.1 Security Level 394
7.10.3.2 Preloaded NMK 396
7.10.3.3 Direct Entry of the NMK 396
7.10.3.4 Distribution of NMK Using DAK 397
7.10.3.5 Distribution of NMK Using Unicast Key Exchange (UKE) 398
7.10.3.6 Distribution of NMK Using Other Key Management Protocols 400
7.10.3.7 Changing the NMK 401

7.10.4 NEK Provisioning 402
7.10.4.1 Provision NEK for new STA 402
7.10.4.2 Provision NEK for Part or All of the AVLN 402
7.10.5 Encryption Key Uses and Protocol Failures 403
7.10.6 AES Encryption Algorithm and Mode 405
7.10.6.1 PHY Block-Level Encryption 405
7.10.6.2 Payload-Level Encryption 405
7.10.7 Generation of AES Encryption Keys 406
7.10.7.1 Generation from Passwords 406
7.10.7.2 Automatic Generation of AES Keys 407
7.10.7.3 Generation of Nonces 408
7.10.8 Encrypted Payload Message 408
7.10.9 User Interface Station (UIS) 410
7.10.10 Resisting Common Security Attacks 411
7.10.10.1 Man-in-the-Middle (MITM) 411
7.10.10.2 Repetition (Replay) Attacks 411
7.10.11 Discussion of Security Mechanisms (Informative) 411
7.11 Network Power Management 413
Chapter 8 Multiple Networks 415
8.1 Overview of Network Operation Modes 415
8.1.1 CSMA-Only Mode 416
8.1.1.1 CSMA-Only Mode for GREEN PHY 416
8.1.2 Uncoordinated Mode 416
8.1.2.1 Uncoordinated Mode for GREEN PHY 416
8.1.3 Coordinated Mode 417
8.1.3.1 Coordinated Mode for GREEN PHY 417
8.2 Overview of Beacon Period Structure 417
8.2.1 Minimum CSMA Region Requirement 419
8.2.1.1 GREEN PHY Preferred Allocation and Minimum CSMA Region 419
8.3 Coordinated Mode 419
8.3.1 Interfering Network List 420
8.3.2 Group of Networks 420
8.3.3 Determining a Compatible Schedule 420
8.3.3.1 Computing the INL Allocation 421
8.3.4 Communication between Neighboring CCos 423
8.3.5 Neighbor Network Instantiation 424
8.3.5.1 Procedure to Establish a New Network in Coordinated Mode 424
8.3.5.2 Changing the Number of Beacon Slots 428
8.3.5.3 Setting the Value of SlotUsage Field 429
8.3.5.4 Examples 430
8.3.5.5 Scenario One 430
8.3.5.6 Scenario Two 431

8.3.5.7 Scenario Three 433
8.3.6 Procedure to Share Bandwidth in Coordinated Mode 434
8.3.7 Scheduling Policy 436
8.3.8 Procedure to Release Bandwidth 437
8.3.9 Procedure to Shut Down an AVLN 437
8.3.10 AC Line Cycle Synchronization in Coordinated Mode 438
8.4 Passive Coordination in CSMA-Only Mode 439
8.5 Transitions between Different Neighbor Network Operating Modes 439
8.5.1 Network Mode of a Newly Established AVLN 440
8.5.2 CSMA-Only Mode Transitions 440
8.5.3 Uncoordinated Mode Transitions 440
8.5.4 Coordinated Mode Transitions 441
8.6 Neighboring Networks with Matching NIDs 442
Chapter 9 HomePlug 1.0.1 Coexistence 443
9.1 Overview 443
9.2 HomePlug 1.0.1 Behavior 444
9.2.1 HomePlug 1.0.1-Prioritized CSMA/CA 444
9.2.2 HomePlug 1.0.1 Carrier-Sensing Mechanisms 444
9.2.3 HomePlug 1.0.1 Segment Bursting 446
9.2.4 Contention-Free Transmissions 446
9.2.5 Link Status 446
9.3 HomePlug AV Coexistence Modes 447
9.3.1 Detection and Reporting of Active HomePlug 1.0.1 and HomePlug 1.1 STAs 448
9.3.2 HomePlug 1.0.1/1.1 Coexistence Mode Changes 450
9.4 HomePlug 1.0.1-Compatible Frame Lengths 452
9.5 Medium Activity under Hybrid Mode 459
9.5.1 HomePlug AV Channel Access in Hybrid Mode 459
9.6 Contention-Free Access Coexistence 460
9.6.1 Contention-Free Period Initiation 461
9.6.1.1 Immediate Grant Using the RTS Delimiter 463
9.6.2 Medium Retention for Contention-Free Access 463
9.6.3 Medium Release After Contention-Free Access 463
9.7 CSMA/CA Coexistence 464
9.8 Coexistence with HomePlug 1.1 and Non-HomePlug Powerline Networks 464
9.8.1 HomePlug 1.0.1 Delimiters 465
9.8.2 HomePlug 1.1 Identification 465
9.8.3 Coexistence Allocation Information Delimiter (DT = 0b111 and CC = 0b0) 465
9.8.3.1 Allocation Identifier (AID) 466
9.8.3.2 Allocation Type (AT) 466
9.8.3.3 Allocation Variant Field (AVF) 467
9.8.3.4 Allocation Variant Field (AVF) for AT = 0b00 467
9.8.3.5 Frame Control Check Sequence (FCCS) 469

9.8.4 Coexistence Management Message Delimiter (DT = 0b111, CC = 0b1) 469
9.8.4.1 Message Type 470
9.8.4.2 Message Variant Field (MVF) 470
9.9 HomePlug 1.0.1 Link Status and AV Beacon 476
9.10 HomePlug 1.0.1/1.1 and Neighbor Networks 476
9.11 HomePlug 1.0.1/1.1 and Access Coexistence 478
Chapter 10 Access Coexistence 479
10.1 Flexible Time Division Access Coexistence 479
10.1.1 Terminologies 479
10.1.2 Assumptions 480
10.1.3 Access CCo Requirements 480
10.1.4 Access STA Requirements 480
10.1.5 Sharing of Resource between Access Network and In-Home Networks 481
10.2 Association, Authorization, and Authentication Procedures 481
10.2.1 Association Procedure 481
10.2.2 Authorization and Authentication Procedures 482
10.3 Bandwidth-Allocation Procedure 482
10.3.1 Using Access Network Resources 483
10.3.2 Using Resource from the In-Home Network 484
10.3.3 Using Neighbor Network Coordination 486
10.4 Bandwidth Release Procedure 488
10.5 Flexible Frequency Division Access Coexistence 490
10.5.1 FDMA Coexistence Management Messages (FCMMs) 491
10.5.2 Negotiation of the Channel 491
10.6 Flexible TDM Coexistence with Non-HomePlug Networks 492
Chapter 11 Management Messages 493
11.1 Management Message Format 493
11.1.1 Original Destination Address (ODA) 494
11.1.2 Original Source Address (OSA) 494
11.1.3 VLAN Tag 494
11.1.4 MTYPE 494
11.1.5 Management Message Version (MMV) 494
11.1.6 Management Message Type (MMTYPE) 495
11.1.7 Fragment Management Information 496
11.1.8 Management Message Entry Data (MME) 498
11.1.9 MME PAD 507
11.1.10 MME Support of HomePlug GREEN PHY 507
11.2 Station - Central Coordination (CCo) 520
11.2.1 CC_CCO_APPOINT.REQ 520
11.2.2 CC_CCO_APPOINT.CNF 520
11.2.3 CC_BACKUP_APPOINT.REQ 521
11.2.4 CC_BACKUP_APPOINT.CNF 522

11.2.5 CC_LINK_INFO.REQ 522
11.2.6 CC_LINK_INFO.CNF 522
11.2.7 CC_LINK_INFO.IND 523
11.2.8 CC_LINK_INFO.RSP 523
11.2.9 CC_HANDOVER.REQ 523
11.2.10 CC_HANDOVER.CNF 524
11.2.11 CC_HANDOVER_INFO.IND 524
11.2.12 CC_HANDOVER_INFO.RSP 525
11.2.13 CC_DISCOVER_LIST.REQ 526
11.2.14 CC_DISCOVER_LIST.CNF 526
11.2.15 CC_DISCOVER_LIST.IND 529
11.2.16 CC_LINK_NEW.REQ 529
11.2.16.1 Initiating MAC Address 530
11.2.16.2 Terminating MAC Address 530
11.2.16.3 Connection Identifier 531
11.2.16.4 Connection Specification 531
11.2.16.5 Forward Link and Reverse Link Bit Loading Estimates 531
11.2.17 CC_LINK_NEW.CNF 532
11.2.17.1 Result 533
11.2.17.2 Proposed CSPEC 533
11.2.18 CC_LINK_MOD.REQ 533
11.2.19 CC_LINK_MOD.CNF 534
11.2.20 CC_LINK_SQZ.REQ 535
11.2.21 CC_LINK_SQZ.CNF 535
11.2.22 CC_LINK_REL.REQ 535
11.2.23 CC_LINK_REL.IND 536
11.2.24 CC_DETECT_REPORT.REQ 537
11.2.25 CC_DETECT_REPORT.CNF 538
11.2.26 CC_WHO_RU.REQ 539
11.2.27 CC_WHO_RU.CNF 540
11.2.28 CC_ASSOC.REQ 540
11.2.28.1 Req Type 541
11.2.28.2 NID 541
11.2.28.3 CCo Capability 541
11.2.28.4 Proxy Networking Capability 542
11.2.29 CC_ASSOC.CNF 542
11.2.29.1 Result 542
11.2.29.2 NID 543
11.2.29.3 SNID 543
11.2.29.4 STA TEI 543
11.2.29.5 Lease Time 543
11.2.30 CC_LEAVE.REQ 544

11.2.31 CC_LEAVE.CNF 544
11.2.32 CC_LEAVE.IND 544
11.2.33 CC_LEAVE.RSP 545
11.2.34 CC_SET_TEI_MAP.REQ 545
11.2.35 CC_SET_TEI_MAP.IND 545
11.2.35.1 Mode 546
11.2.36 CC_RELAY.REQ 547
11.2.36.1 FDA 547
11.2.36.2 FTEI 547
11.2.36.3 Len 547
11.2.36.4 Payload 548
11.2.37 CC_RELAY.IND 548
11.2.37.1 OSA 548
11.2.37.2 OTEI 548
11.2.37.3 Len 548
11.2.37.4 Payload 549
11.2.38 CC_BEACON_RELIABILITY.REQ 549
11.2.39 CC_BEACON_RELIABILITY.CNF 549
11.2.39.1 Number of Beacon Periods (NBP) 550
11.2.39.2 Number of Missed Beacons (NMB) 550
11.2.40 CC_ALLOC_MOVE.REQ 550
11.2.41 CC_ALLOC_MOVE.CNF 551
11.2.42 CC_ACCESS_NEW.REQ 552
11.2.43 CC_ACCESS_NEW.CNF 552
11.2.44 CC_ACCESS_NEW.IND 554
11.2.45 CC_ACCESS_NEW.RSP 555
11.2.46 CC_ACCESS_REL.REQ 555
11.2.47 CC_ACCESS_REL.CNF 556
11.2.48 CC_ACCESS_REL.IND 556
11.2.49 CC_ACCESS_REL.RSP 557
11.2.50 CC_DCPPC.IND 557
11.2.51 CC_DCPPC.RSP 558
11.2.52 CC_HP1_DET.REQ 558
11.2.53 CC_HP1_DET.CNF 558
11.2.54 CC_BLE_UPDATE.IND 559
11.2.55 CC_BCAST_REPEAT.IND (GREEN PHY) 559
11.2.56 CC_BCAST_REPEAT.RSP (GREEN PHY) 560
11.2.57 CC_POWERSAVE.REQ (GREEN PHY) 560
11.2.58 CC_POWERSAVE.CNF (GREEN PHY) 560
11.2.59 CC_POWERSAVE_EXIT.REQ (GREEN PHY) 561
11.2.60 CC_POWERSAVE_EXIT.CNF (GREEN PHY) 561
11.2.61 CC_POWERSAVE_LIST.REQ (GREEN PHY) 562

11.2.62 CC_POWERSAVE_LIST.CNF (GREEN PHY) 562
11.3 Proxy Coordinator (PCo) Messages 563
11.3.1 CP_PROXY_APPOINT.REQ 563
11.3.1.1 ReqType 564
11.3.1.2 ReqID 564
11.3.1.3 GLID 564
11.3.1.4 Num HSTA 564
11.3.1.5 HSTA SA[1] to HSTA SA[N] 565
11.3.1.6 HSTA TEI[1] to HSTA TEI[N] 565
11.3.1.7 HSTA State[1] to HSTA STATE[N] 565
11.3.2 CP_PROXY_APPOINT.CNF 565
11.3.2.1 ReqID 566
11.3.2.2 Result 566
11.3.3 PH_PROXY_APPOINT.IND 566
11.3.3.1 PCo SA 566
11.3.3.2 PCo TEI 567
11.3.3.3 CCo SA 567
11.3.3.4 CCo TEI 567
11.3.3.5 GLID 567
11.3.4 CP_PROXY_WAKE.REQ 567
11.4 CCo - CCo 567
11.4.1 NN_INL.REQ and NN_INL.CNF 567
11.4.2 NN_NEW_NET.REQ 570
11.4.3 NN_NEW_NET.CNF 571
11.4.4 NN_NEW_NET.IND 573
11.4.5 NN_ADD_ALLOC.REQ 574
11.4.6 NN_ADD_ALLOC.CNF 575
11.4.7 NN_ADD_ALLOC.IND 575
11.4.8 NN_REL_ALLOC.REQ 576
11.4.9 NN_REL_ALLOC.CNF 577
11.4.10 NN_REL_NET.IND 578
11.5 Station – Station 580
11.5.1 CM_UNASSOCIATED_STA.IND 580
11.5.2 CM_ENCRYPTED_PAYLOAD.IND 580
11.5.2.1 Payload Encryption Key Select (PEKS) 581
11.5.2.2 AVLN Status 582
11.5.2.3 Protocol ID (PID) 582
11.5.2.4 Protocol Run Number (PRN) 583
11.5.2.5 Protocol Message Number (PMN) 583
11.5.2.6 Initialization Vector (IV) or Universally Unique Identifier (UUID) 583
11.5.2.7 Length (Len) 583
11.5.2.8 Random Filler (RF) 584

11.5.2.9 Management Message (MM) or HLE Payload 584
11.5.2.10 Cyclic Redundancy Check (CRC) 584
11.5.2.11 Protocol ID (PID - Encrypted) 584
11.5.2.12 Protocol Run Number (PRN - Encrypted) 584
11.5.2.13 Protocol Message Number (PMN - Encrypted) 584
11.5.2.14 Padding - Encrypted 584
11.5.2.15 RF Length (RFLen - Encrypted) 585
11.5.3 CM_ENCRYPTED_PAYLOAD.RSP 585
11.5.3.1 Result 585
11.5.4 CM_SET_KEY.REQ 585
11.5.4.1 Key Type 586
11.5.4.2 NID 587
11.5.4.3 New_EKS 587
11.5.5 CM_SET_KEY.CNF 588
11.5.6 CM_GET_KEY.REQ 588
11.5.6.1 Request Type 589
11.5.6.2 Requested Key Type 589
11.5.6.3 NID 590
11.5.7 CM_GET_KEY.CNF 590
11.5.7.1 Requested Key Type 591
11.5.8 CM_SC_JOIN.REQ 591
11.5.9 CM_SC_JOIN.CNF 592
11.5.10 CM_CHAN_EST.IND 592
11.5.10.1 MaxFL_AV 596
11.5.10.2 RIFS_AV_OneSym 596
11.5.10.3 RIFS_AV_TwoSym 596
11.5.10.4 RIFS_AV_G2Sym 597
11.5.10.5 FEC Type/Code Rate (FECTYPE) 597
11.5.10.6 Guard Interval Length (GIL) 597
11.5.10.7 Carrier Bit Loading Data Encoding (CBD_ENC) 598
11.5.10.8 Carrier Bit Loading Data (CBD) 598
11.5.11 CM_TM_UPDATE.IND 600
11.5.12 CM_AMP_MAP.REQ 603
11.5.13 CM_AMP_MAP.CNF 603
11.5.14 CM_BRG_INFO.REQ 604
11.5.15 CM_BRG_INFO.CNF 604
11.5.15.1 Bridge TEI (BTEI) 604
11.5.15.2 Number of Bridge Destination Addresses (NBDA) 605
11.5.15.3 Bridged Destination Address [i] (BDA[i]) 605
11.5.16 CM_CONN_NEW.REQ 605
11.5.17 CM_CONN_NEW.CNF 606
11.5.18 CM_CONN_REL.IND 607

11.5.19 CM_CONN_REL.RSP 607
11.5.20 CM_CONN_MOD.REQ 608
11.5.21 CM_CONN_MOD.CNF 608
11.5.22 CM_CONN_INFO.REQ 609
11.5.23 CM_CONN_INFO.CNF 609
11.5.24 CM_STA_CAP.REQ 610
11.5.25 CM_STA_CAP.CNF 610
11.5.26 CM_NW_INFO.REQ 612
11.5.27 CM_NW_INFO.CNF 612
11.5.28 CM_GET_BEACON.REQ 613
11.5.29 CM_GET_BEACON.CNF 614
11.5.30 CM_HFID.REQ 614
11.5.31 CM_HFID.CNF 615
11.5.32 CM_MME_ERROR.IND 615
11.5.33 CM_NW_STATS.REQ 616
11.5.34 CM_NW_STATS.CNF 616
11.5.35 CM_LINK_STATS.REQ 617
11.5.36 CM_LINK_STATS.CNF 618
11.5.37 CM_STA_IDENTIFY.REQ (GREEN PHY) 621
11.5.38 CM_STA_IDENTIFY.CNF (GREEN PHY) 621
11.5.39 CM_STA_IDENTIFY.IND (GREEN PHY) 622
11.5.40 CM_STA_IDENTIFY.RSP (GREEN PHY) 622
11.5.41 CM_ROUTE_INFO.REQ (GREEN PHY) 623
11.5.42 CM_ROUTE_INFO.CNF (GREEN PHY) 623
11.5.42.1 Route Data Rate (RDR[i]) 624
11.5.43 CM_ROUTE_INFO.IND (GREEN PHY) 624
11.5.44 CM_UNREACHABLE.IND (GREEN PHY) 624
11.5.44.1 Unreachable Time Stamp (UnrchTS) 625
11.5.45 CM_TRIGGER_ATTEN_CHAR.REQ 625
11.5.45.1 SOUND_TARGET 626
11.5.45.2 NUM_SOUNDS 626
11.5.45.3 Time_Out 626
11.5.45.4 RESP_TYPE 626
11.5.45.5 FORWARDING_STA 626
11.5.46 CM_TRIGGER_ATTEN_CHAR.CNF 627
11.5.47 CM_START_ATTEN_CHAR.IND 629
11.5.47.1 NUM_SOUNDS 651
11.5.47.2 Time_Out 651
11.5.47.3 RESP_TYPE 651
11.5.47.4 FORWARDING_STA 651
11.5.48 CM_ ATTEN_CHAR.IND 651
11.5.48.1 SOURCE_ADDRESS 651

11.5.48.2 ATTEN_PROFILE 651
11.6 Manufacturer-Specific Messages 651
11.7 Vendor-Specific Messages 651
Chapter 12 Service Access Point Primitives 653
12.1 Convergence Layer Information 653
12.1.1 H1 and M1 Interfaces 653
12.1.2 Protocol Adaptation Layers (PALs) 653
12.1.3 Service Access Points (SAPs) 654
12.1.4 Primitives 654
12.2 H1 SAPs 654
12.2.1 Protocol Adaptation Layer (Data Plane) 654
12.2.1.1 Ethernet II-Class (ETH) SAP 654
12.2.2 Control SAP Service 658
12.2.2.1 APCM_CONN_ADD.REQ 658
12.2.2.2 APCM_CONN_ADD.CNF 658
12.2.2.3 APCM_CONN_ADD.IND 659
12.2.2.4 APCM_CONN_ADD.RSP 660
12.2.2.5 APCM_CONN_MOD.REQ 660
12.2.2.6 APCM_CONN_MOD.CNF 661
12.2.2.7 APCM_CONN_MOD.IND 661
12.2.2.8 APCM_CONN_MOD.RSP 662
12.2.2.9 APCM_CONN_REL.REQ 662
12.2.2.10 APCM_CONN_REL.CNF 662
12.2.2.11 APCM_CONN_REL.IND 663
12.2.2.12 APCM_GET_NTB.REQ 663
12.2.2.13 APCM_GET_NTB.CNF 663
12.2.2.14 APCM_AUTHORIZE.REQ 664
12.2.2.15 APCM_AUTHORIZE.CNF 665
12.2.2.16 APCM_AUTHORIZE.IND 666
12.2.2.17 APCM_GET_SECURITY_MODE.REQ 666
12.2.2.18 APCM_GET_SECURITY_MODE.CNF 666
12.2.2.19 APCM_SET_SECURITY_MODE.REQ 667
12.2.2.20 APCM_SET_SECURITY_MODE.CNF 667
12.2.2.21 APCM_GET_NETWORKS.REQ 667
12.2.2.22 APCM_GET_NETWORKS.CNF 668
12.2.2.23 APCM_SET_NETWORKS.REQ 668
12.2.2.24 APCM_SET_NETWORKS.CNF 668
12.2.2.25 APCM_GET_NEWSTA.REQ 669
12.2.2.26 APCM_GET_NEWSTA.CNF 669
12.2.2.27 APCM_GET_NEWSTA.IND 670
12.2.2.28 APCM_SET_KEY.REQ 670
12.2.2.29 APCM_SET_KEY.CNF 671

12.2.2.30 APCM_GET_KEY.REQ 671
12.2.2.31 APCM_GET_KEY.CNF 671
12.2.2.32 APCM_STA_RESTART.REQ 671
12.2.2.33 APCM_STA_RESTART.CNF 672
12.2.2.34 APCM_NET_EXIT.REQ 672
12.2.2.35 APCM_NET_EXIT.CNF 672
12.2.2.36 APCP_SET_TONE_MASK.REQ 672
12.2.2.37 APCP_SET_TONE_MASK.CNF 673
12.2.2.38 APCM_STA_CAP. REQ 673
12.2.2.39 APCM_STA_CAP.CNF 673
12.2.2.40 APCM_NW_INFO.REQ 673
12.2.2.41 APCM_NW_INFO.CNF 673
12.2.2.42 APCM_LINK_STATS.REQ 673
12.2.2.43 APCM_LINK_STATS.CNF 674
12.2.2.44 APCM_GET_BEACON.REQ 674
12.2.2.45 APCM_GET_BEACON.CNF 674
12.2.2.46 APCM_GET_HFID.REQ 674
12.2.2.47 APCM_GET_HFID.CNF 674
12.2.2.48 APCM_SET_HFID.REQ 674
12.2.2.49 APCM_SET_HFID.CNF 675
12.2.2.50 APCM_SET_HD_DURATION.REQ (GREEN PHY) 675
12.2.2.51 APCM_SET_HD_DURATION.CNF (GREEN PHY) 675
12.2.2.52 APCM_ UNASSOCIATED_STA.IND (GREEN PHY) 675
12.2.2.53 APCM_SC_JOIN.REQ (GREEN PHY) 675
12.2.2.54 APCM_SC_JOIN.CNF (GREEN PHY) 675
12.2.2.55 APCM_SET_PPKEYS.REQ (GREEN PHY) 676
12.2.2.56 APCM_SET_PPKEYS.CNF (GREEN PHY) 676
12.3 M1 SAPs 677
12.3.1 MAC Service Definition 678
12.3.1.1 Overview 678
12.3.2 MAC Data Service 679
12.3.2.1 MD_DATA.REQ 679
12.3.2.2 MD_DATA.CNF 680
12.3.2.3 MD_DATA.IND 681
12.3.3 MAC Management Service 681
Chapter 13 Appendices 682
13.1 Priority Mapping (Informative) 682
13.2 User Experiences (UEs) (Informative) 683
13.2.1 UE1 – Preconfigured Set of Devices 684
13.2.2 UE2 – Network Password Entry 685
13.2.3 UE3 – Device Password Entry 685
13.2.4 UE4 – Simple Connect (Button Push) 686

13.2.4.1 UE4a – Two New Devices Form a New Network Using SC 686
13.2.4.2 UE4b – Adding a New Device to an Existing Network Using SC 687
13.2.4.3 UE4c – Adding Multiple New Devices Using SC Chaining 687
13.2.5 Changing Security Levels on a Device 687
13.2.5.1 Changing SL-HS to SL-SC 687
13.2.5.2 Changing SL-SC to SL-HS 688
13.3 Security State Transition Diagrams 688
13.3.1 State Definitions for Security Protocol State Machine688
13.4 Test Vectors 691
13.5 Example Hashed NMK, Hashed NID, and NMK Provisioning MME Using DAK 691
13.6 Example of NMK Provisioning Using UKE Mechanism 695
13.6.1 CM_GET_KEY.REQ 696
13.6.2 CM_GET_KEY.CNF 698
13.6.3 TEK Computation 699
13.6.4 CM_SET_KEY.REQ in CM_ENCRYPTED_PAYLOAD.IND 700
13.6.5 CM_SET_KEY.CNF in CM_ENCRYPTED_PAYLOAD.IND 703
13.7 Third Party Managed Security Deployment Scenarios 705
13.7.1 DAK Authorization 706
13.7.2 Push Button Authorization 706
13.7.3 Direct Entry Authorization 707
Chapter 14 ISP 720
14.1 ISP Overview 720
14.1.1 ISP BENTRY 720
14.1.1.1 ISP BENTRY: Beacon Entries in Various Beacons 720
14.1.1.2 ISP BENTRY: BEHDR Value 720
14.1.2 ISP BENTRY: ISP MME Types 720
14.1.3 Coexistence for ISP 721
Index 722

List of Figures

Figure 11: Message Nomenclature 13
Figure 12. Message Sequence Chart Conventions 15
Figure 21: System Block Diagram 25
Figure 22: Protocol Layer Architecture 26
Figure 23: Examples of PhyNets and AVLNs 29
Figure 31: HomePlug AV OFDM Transceiver for GREEN PHY 36
Figure 32: Hybrid Mode PPDU Structure – Single Symbol AV FC 39
Figure 33: Hybrid Mode PPDU Structure – Two Symbol AV FC 39
Figure 34: AV Mode PPDU Structure – Single Symbol AV FC 39
Figure 35: AV Mode PPDU Structure - Two Symbol AV FC 39
Figure 36: OFDM Symbol Timing 40
Figure 37: Frame Control FEC Encoder 41
Figure 38: Payload FEC Encoder Block Diagram 43
Figure 39: Data Scrambler 44
Figure 310: Turbo Encoder Block Diagram 44
Figure 311: 8-State Constituent Encoder 46
Figure 312: PN Generator 60
Figure 313: Extended Preamble Structure 70
Figure 314: Nominal Preamble Structure 72
Figure 315: Sections for Extended Preamble 74
Figure 316: AV Preamble Waveform 75
Figure 317: Hybrid Preamble Waveform 76
Figure 318: HomePlug 1.0.1 FC Macro Symbol 78
Figure 319: Single Bit Carrier-Symbol Waveform 78
Figure 320: HomePlug 1.0.1 FC Macro Symbol with Postfix and Shaping 79
Figure 321: AV PRS Waveform 83
Figure 322: Spectral Occupancy for Semi-Infinite Number of Carriers - Zoomed Out 85
Figure 323: Spectral Occupancy for Semi-Infinite Number of Carriers - Zoomed In 85
Figure 324: Spectral Occupancy of Set of HomePlug Carriers 87
Figure 325: HomePlug GREEN PHY Transmit Spectrum Mask for North America 89
Figure 41: Bit and Octet Transmission Order at the MAC-PHY Interface 102
Figure 42: Example of Field Spanning Across Octet Boundaries 103
Figure 43: Example of Figure-Based Representation of Fields That Do Not Obey Octet Boundaries 104
Figure 44: MAC Frame Format 107
Figure 45: MAC Frame when MFT=0b00 108
Figure 46: MAC Frame when MFT=0b01 108
Figure 47: MAC Frame when MFT=0b10 109

Figure 48: MAC Frame when MFT=0b11 109
Figure 49: MPDU Frame Formats in AV-Only Mode 112
Figure 410: MPDU Frame Formats in Hybrid Mode 112
Figure 411: Measurement of FL_AV 125
Figure 412: Duration Field in RTS/CTS When IGF is Set to 0b0 142
Figure 413: Duration Field in RTS/CTS When IGF is Set to 0b1 143
Figure 414: PHY Block Formats 153
Figure 415: Network Identifier 159
Figure 416: Example of Beacon Relocation 186
Figure 51: Line Cycle Time and Beacon Transmit Time 197
Figure 52: Example of Beacon Period Structure in Uncoordinated Mode 199
Figure 53: Example of Beacon Schedule Persistence 201
Figure 54: Beacon Period Structure in CSMA-Only Mode 203
Figure 55: Example of Beacon Period Structure in Uncoordinated Mode 205
Figure 56: Example of Beacon Period Structure in Coordinated Mode 207
Figure 57: Connection Setup 220
Figure 58: Global Link Setup 221
Figure 59: Connection Teardown for Connections with Only Local Links 224
Figure 510: Connection Teardown for Connections with Global Links 225
Figure 511: Connection Reconfiguration 228
Figure 512: Connection Squeeze/De-Squeeze 231
Figure 513: Detect-and-Report Procedure 234
Figure 514: Initial Channel Estimation 238
Figure 515: Dynamic Channel Adaptation 242
Figure 516: MAC Framing Process for Data Stream 257
Figure 517: MAC Segmentation and MPDU Generation 260
Figure 518: Transmit MAC Frame Stream FSM 262
Figure 519: Receive MAC Frame Stream FSM 265
Figure 520: Illustration of Multi-Network Broadcast Transmission 272
Figure 521: Example of MPDU Bursting 278
Figure 522: Bidirectional Burst Mechanism 279
Figure 523: Inter-frame Spacing during Bidirectional Burst 279
Figure 524: Bidirectional Bursts during CSMA 281
Figure 525: Beacon and CSMA Region Interframe Spacing 291
Figure 526: Contention-Free Interframe Spacing 292
Figure 527: Interframe Spacing for MPDU Bursting 293
Figure 528: Extended Interframe Spacing (EIFS_AV) 293
Figure 529: RCG Measurement 294
Figure 530: Examples of Power Save Schedules 299
Figure 71: Power-on Network Discovery Procedure 323
Figure 72: Unassociated STA Behavior 325
Figure 73: Unassociated CCo Behavior 326

Figure 74: Behavior as a STA in an AVLN 327
Figure 75: Behavior as a CCo in an AVLN 328
Figure 76. Getting Full AVLN Information 331
Figure 77. STA Association 332
Figure 78: Provision NEK for a new STA (Authentication) 336
Figure 79: AVLN Formation by Two Unassociated STAs with Matching NIDs 339
Figure 710: AVLN Formation Using a DAK-Encrypted NMK 341
Figure 711: AVLN Formation Using UKE by One STA in SC-Add and One STA in SC-Join 343
Figure 712: AVLN Formation Using UKE by Two STAs in SC-Join 345
Figure 713: New STA Joins Existing AVLN with Matching NID 347
Figure 714: New STA Joins AVLN by DAK-Encrypted NMK 349
Figure 715: New STA Joins Existing AVLN Using UKE 351
Figure 716: Disassociation - STA Leaves AVLN 352
Figure 717: User-Appointed CCo 356
Figure 718: Transfer of CCo Function 360
Figure 719: Proxy Network Created By Network 1 366
Figure 720: HSTA Association 368
Figure 721: Global Link Life Cycle 385
Figure 722: Green PHY Preferred CSMA allocation immediately following the Beacon Region. 387
Figure 723: Provision NEK for Part or All of the AVLN 403
Figure 724: Encrypted Payload Message when PID is between 0x00 and 0x03 409
Figure 725: Encrypted Payload Message when PID = 0x04 410
Figure 81: Flowchart for Computing INL Allocation 422
Figure 82: MSC to Set Up a New Network in Coordinated Mode 427
Figure 83: New CCo Detects Two Groups of Networks 428
Figure 84: Scenario One: Network A is in Uncoordinated Mode and CCo B Wants to Create a New Network 431
Figure 85: Scenario Two: Networks A and B are in Coordinated Mode and CCo C Wants to Create a New Network 432
Figure 86: Scenario Three: Networks A, B, and C are in Coordinated Mode and CCo D Wants to Create a New Network 434
Figure 87: MSC to Request Additional Bandwidth in Coordinated Mode 435
Figure 88: MSC to Release a Reserved Time Interval in Coordinated Mode 437
Figure 89: MSC to Shut Down an AVLN in Coordinated Mode 438
Figure 810. Neighbor Network Mode Transitions 442
Figure 91: AV Only Mode Processing for Detecting HomePlug 1.0.1 Transmission 449
Figure 92: Hybrid Mode Processing for Detecting HomePlug 1.0.1 Transmission 449
Figure 93: Central Coordinator HomePlug 1.0.1 Coexistence Mode Changes 452
Figure 94: Compatible Regular MPDU during Shared CSMA Using HomePlug 1.0.1 SOF with Response Expected 453

Figure 95: Compatible Regular MPDU during Shared CSMA Allocation Using HomePlug 1.0.1 SOF with no Response Expected 453
Figure 96: Compatible Regular MPDU during CFP Allocation Using HomePlug 1.0.1 SOF with No Response Expected 454
Figure 97: Compatible Burst MPDU Using HomePlug 1.0.1 SOF with no Response Expected 455
Figure 98: Compatible Hybrid RTS Delimiter when PRP Follows the CTS Delimiter 456
Figure 99: Compatible Hybrid RTS Delimiter when the Corresponding SOF Follows the CTS Delimiter 457
Figure 910: Compatible Hybrid RTS Delimiter during CFP Allocation when There is No Corresponding SOF Delimiter 457
Figure 911: HomePlug AV Channel Access in Hybrid Mode 460
Figure 912: CSMA LENGTH 468
Figure 101: CFP Setup in Access Network: Using a Resource from Access Network 483
Figure 102: Example of Beacon Schedules: Using Resource from an Access Network 484
Figure 103: CFP Setup in Access Network: Using Resource from the In-Home Network 485
Figure 104: Example of Beacon Schedules: Using Resource from In-Home Network 486
Figure 105: CFP Setup in Access Network: Using Neighbor Network Coordination 487
Figure 106: Example of Beacon Schedules: Using Neighbor Network Coordination 488
Figure 107: Bandwidth Release Initiated by Gateway STA 489
Figure 108: Bandwidth Release Initiated by the In-Home CCo 489
Figure 111: Illustration of Fragmentation of a MMENTRY 498
Figure 131: State Transition Diagram for HS Security Level 689
Figure 132: State Transition Diagram for Simple-Connect Security Level 690

List of Tables

Table 11: Acronyms and Abbreviations 3
Table 12: Words and Phrases 12
Table 13: Differences between HomePlug GREEN PHY and HomePlug AV PHY 18
Table 14: Differences between HomePlug GREEN PHY MAC and above) and HomePlug AV (MAC and above) 19
Table 21: PhyNets in Figure 23 27
Table 22: HomePlug AV Parameter Specifications 32
Table 23: HomePlug GREEN PHY parameters differing from HomePlug AV 1.1 34
Table 31: PPDU Formats 37
Table 32: OFDM Symbol Characteristics 40
Table 33: Diversity Copier Bit Ordering– Single Symbol Case 42
Table 34: Diversity Copier Bit Ordering - Two Symbol Case 43
Table 35: Rate ½ Puncture Pattern 47

Table 36: Rate 16/21 Puncture Pattern47
Table 37: Interleaver Parameters 48
Table 38: Interleaver Seed Table for FEC Block Size of 16 Octets 49
Table 39: Interleaver Seed Table for FEC Block Size of 136 Octets 49
Table 310: Interleaver Seed Table for FEC Block Size of 520 Octets 49
Table 311: Channel Interleaver Parameters 51
Table 312: Sub-bank Switching 52
Table 313: ROBO Mode Parameters 52
Table 314: Modulation Characteristics 58
Table 315: Tone Mask Amplitude Map and Tone Map 60
Table 316: Mapping Reference Phase Angle Numbers 61
Table 317: Bit Mapping 67
Table 318: Symbol Mapping (Except 8-QAM) 67
Table 319: Symbol Mapping for 8-QAM (not required for GREEN PHY) 69
Table 320: Modulation Normalization Scales 69
Table 321: SYNCP AV Phase Reference 71
Table 322: Relative Power Levels 83
Table 323: North American Carrier (Tone) and Spectral Masks 86
Table 324: Amplitude Map 88
Table 325: RMS Transmit Constellation Error (TCE_RMS) Limits 91
Table 41: Example of Tabulation of Fields That Do Not Obey Octet Boundaries 104
Table 42: MAC Frame Header Field 107
Table 43: MAC Frame Type Field Interpretation 108
Table 44: MPDU Frame Control Fields 113
Table 45: Delimiter Type Field Interpretation 114
Table 46: Access Field Interpretation 115
Table 47: Beacon Variant Fields 116
Table 48: HomePlug GREEN PHY Start-of-Frame Variant Fields (same as for HomePlug AV) 118
Table 49: Contention-Free Session Interpretation 119
Table 410: Beacon Detect Flag Interpretation 120
Table 411: HomePlug 1.0.1 Detect Flag Interpretation 120
Table 412: HomePlug 1.1 Detect Flag Interpretation 120
Table 413: Encryption Key Select Interpretation 121
Table 413b: Assignment of Previously Reserved Encryption Key Select Values for GREEN PHY 121
Table 414: PHY Block Size Interpretation 123
Table 415: Number of Symbols Interpretation 124
Table 416: Tone Map Index Interpretation 124
Table 417: Frame Length Interpretation 126
Table 418: MPDU Count Interpretation 126
Table 419: Bidirectional Burst Flag Interpretation 127

Table 420: Maximum Reverse Transmission Frame Length Interpretation 127
Table 421: Multicast Flag Interpretation 128
Table 422: Request SACK Retransmission Interpretation 129
Table 423: Convergence Layer SAP Type 129
Table 424: Data and Management MAC Frame Stream Command Interpretation 130
Table 425: Selective Acknowledgement Variant Field 131
Table 426: SACK Data Variant Field 132
Table 427: Contention-Free Session Interpretation 132
Table 428: Request Reverse Transmission Flag Interpretation 133
Table 429: Data and Management MAC Frame Stream Response Interpretation 133
Table 430: SACK Type Interpretation 134
Table 431: SACKI Field for Mixed Errors – Compressed (SACKT = 0b01) 135
Table 432: SACKI for Uniform (SACKT = 0b11) 136
Table 433: Receive Window Size Interpretation 137
Table 434: Request Reverse Transmission Length Interpretation 138
Table 435: Request to Send/Clear to Send Variant Field 139
Table 436: Contention-Free Session Interpretation 140
Table 437: RTS Flag Interpretation 141
Table 438: Sound MPDU Variant Field 144
Table 439: Sound MPDU PHY Block Size Interpretation 145
Table 440: Sound ACK Flag Interpretation 146
Table 441: Sound Complete Flag Interpretation 146
Table 442: Sound Reason Code Interpretation 147
Table 443: Reverse SOF Variant Field 148
Table 444: Contention-Free Session Interpretation 149
Table 445: Request Reverse Transmission Flag Interpretation 149
Table 446: Reverse SOF Frame Length Interpretation 150
Table 447: PB Header Format 153
Table 448: MAC Frame Boundary Offset Interpretation 154
Table 449: Management Message Queue Flag Interpretation 155
Table 450: MAC Frame Boundary Flag Interpretation 155
Table 451: Oldest Pending Segment Flag Interpretation 155
Table 452: Beacon Payload Fields 158
Table 452b: Assignment of Previously Reserved Beacon Payload Fields for GREEN PHY 158
Table 457: Number of Beacon Slots Interpretation 162
Table 465c: Assignment of Previously Reserved Beacon Entry Header Values for GREEN PHY 166
Table 465b: Assignment of Previously Reserved Beacon Entry Header Values for IEEE 1901 167
Table 465c: Assignment of Previously Reserved Beacon Entry Header Values for GREEN PHY 168
Table 466b: Additional Beacon Entries in Various Beacons for GREEN PHY 170

Table 467: BELEN Interpretation 170
Table 468: Non-Persistent Schedule BENTRY 171
Table 469: Persistent Schedule BENTRY 172
Table 470: PSCD Interpretation 172
Table 471: CSCD Interpretation 173
Table 472: Session Allocation Information Format without Start Time 174
Table 473: Session Allocation Information Format with Start Time 174
Table 474: Start Time Present Flag Interpretation 174
Table 475: Regions BENTRY 176
Table 476: Region Type (RT) Interpretation 177
Table 477: MAC Address BENTRY 178
Table 478: Discover BENTRY 178
Table 479: Discovered Info BENTRY 179
Table 480: Proxy Networking Capability Interpretation 180
Table 481: Backup CCo Capability Interpretation 180
Table 482: CCo Status 181
Table 483: PCo Status 181
Table 484: Backup CCo Status 181
Table 485:Beacon Period Start Time Offset BENTRY 182
Table 486: Encryption Key Change BENTRY 182
Table 487: KCCD Interpretation 183
Table 488: KBC Interpretation 183
Table 489: Central Coordinator Handover BENTRY 183
Table 490: Handover Countdown Interpretation 184
Table 491: Beacon Relocation BENTRY 184
Table 492: Relocation Countdown Interpretation 185
Table 493: Relocation Type Interpretation 185
Table 494: Leaving Group Flag Interpretation 185
Table 495: AC Line Sync Countdown BENTRY 187
Table 496: Change NumSlots BENTRY 187
Table 497: NSCCD Interpretation 188
Table 498: Change HM BENTRY 188
Table 499: HMCCD Interpretation 188
Table 4100: Change SNID BENTRY 189
Table 4101: SCCD Interpretation 189
Table 4102: Power Save BENTRY 190
Table 4103: Power Save Schedule (PSS) Format 191
Table 4104: Vendor Specific BENTRY 192
Table 4-105: Reusable SNID Flag Interpretation 193
Table 4106: Sound Payload Fields 194
Table 51: Setting the VCS Timer 209
Table 52: Summary of Link and Connection Identifiers 216

Table 52b: Assignment of Previously Reserved Values for Link and Connection Identifiers in GREEN PHY 217
Table 53: Initialization Vector Format 275
Table 5-4: Allowed PPDU combinations 295
Table 61: Convergence Layer Functions 307
Table 62: Classifier Rules for Ethernet II-Class Data SAP 310
Table 63: Format of Ethernet SAP Classifier Rule Set 313
Table 64: Smoothing/Jitter Control 318
Table 71: TEI Values 333
Table 72: Lease Values 334
Table 73: Order of Precedence in Selection of CCo 358
Table 74: Example of Topology Table 363
Table 75: Format of Connection Specification (CSPEC) 374
Table 76: Format of Connection Information (CINFO) 375
Table 77: Format of QoS and MAC Parameter Field in CSPEC 376
Table 78: QoS and MAC Parameter Fields Exchanged between HLE and CM, and between CMs 377
Table 79: Additional QoS and MAC Parameter Fields Exchanged between Two CMs 379
Table 710: QoS and MAC Parameter Fields between CM and CCo 380
Table 711: Format of the Body of Connection Descriptor 382
Table 712: Format of the Body of Vendor-Specific MAC and QoS Parameter 382
Table 713: Security Level Interpretation 394
Table 714: Security Level and NMK Provisioning. 394
Table 81: Interaction Between Different Regions 418
Table 82: Rules for Computing INL Allocation 423
Table 91: Receiver Actions on Receipt of HomePlug 1.0.1 Delimiters 445
Table 92: Parameters for CFPI Procedure 461
Table 93: HomePlug 1.0.1 Frame Control Fields 465
Table 94: Coexistence Allocation Information 466
Table 95: Allocation Types 467
Table 96: Allocation Variant Field for Allocation Type = 0b00 467
Table 97: Allocation Variant Field for AT = 0b000 and SLF = 0b0 468
Table 98: Allocation Variant Field for AT = 0b000 and SLF=0b1 468
Table 99: Allocation Variant Field (AT = 0b01 to 0b11) 469
Table 910: Management Message Delimiter 469
Table 911: Message Types 470
Table 912: Network Information Request Management Message 470
Table 913: Network Types 471
Table 914: Network Information Management Message 472
Table 915: Request TDMA Allocation Management Message 472
Table 916: Request Types 473
Table 917: TDMA Allocation Response Management Message 473

Table 918: Reset Allocation Information Management Message 474
Table 919: FDMA Band Request Management Message 474
Table 920: FDMA Band Response Management Message 475
Table 921: Response Status Values 475
Table 922: Current FDMA Band Usage Management Message 476
Table 111: Management Message Format 493
Table 112: Interpretation of Two LSBs of MMTYPE 495
Table 113: Interpretation of Three MSBs of MMTYPE 495
Table 114: Prefix Conventions when Naming Management Messages 498
Table 115: Management Message Type (Note there is a Table 11-5b) 501
Table 11-5b: Comparison of Management Message Types for HomePlug AV (STA and L0 CCo) vs. HomePlug GREEN PHY (STA and CCo) 508
Table 116: CC_CCO_APPOINT.REQ Message 520
Table 117: CC_CCO_APPOINT.CNF Message 521
Table 118: CC_BACKUP_APPOINT.REQ Message 521
Table 119: CC_BACKUP_APPOINT.CNF Message 522
Table 1110: CC_LINK_INFO.CNF Message 522
Table 1111: Format of LinkInfo[ ] Field 523
Table 1112: CC_HANDOVER.REQ Message 524
Table 1113: CC_HANDOVER.CNF Message 524
Table 1114: CC_HANDOVER_INFO.IND Message 525
Table 1115: Format of STA_Info[ ] Field 525
Table 1116: CC_DISCOVER_LIST.CNF Message 526
Table 1117: Format of StationInfo [ ] 527
Table 1118: Format of NetworkInfo[ ] 529
Table 1119: CC_LINK_NEW.REQ Message 530
Table 1120: CC_LINK_NEW.CNF Message 532
Table 1121: CC_LINK_MOD.REQ Message 534
Table 1122: CC_LINK_MOD.CNF Message 534
Table 1123: CC_LINK_SQZ.REQ Message 535
Table 1124: CC_LINK_SQZ.CNF Message 535
Table 1125: CC_LINK_REL.REQ Message 536
Table 1126: CC_LINK_REL.IND Message 537
Table 1127: CC_DETECT_REPORT.REQ Message 538
Table 1128: CC_DETECT_REPORT.CNF Message 538
Table 1129: Format of GLIDInfo( ) 539
Table 1130: CC_WHO_RU.REQ Message 540
Table 1131: CC_WHO_RU.CNF Message 540
Table 1132: CC_ASSOC.REQ Message 541
Table 1133: CC_ASSOC.CNF Message 542
Table 1134: Result Field Interpretation 542
Table 1135:Lease Time Field 543

Table 1136: CC_LEAVE.REQ Message 544
Table 1137: CC_LEAVE.IND Message 544
Table 1138. CC_SET_TEI_MAP.IND Message 545
Table 1139: Mode Field Interpretation 546
Table 1140: CC_RELAY.REQ Message 547
Table 1141: CC_RELAY.IND Message 548
Table 1142: CC_BEACON_RELIABILITY.CNF 549
Table 1143: CC_ALLOC_MOVE.REQ Message 551
Table 1144: CC_ALLOC_MOVE.CNF Message 552
Table 1145: CC_ACCESS_NEW.REQ Message 552
Table 1146: CC_ACCESS_NEW.CNF Message 553
Table 1147: CC_ACCESS_NEW.IND Message 554
Table 1148: CC_ACCESS_NEW.RSP Message 555
Table 1149: CC_ACCESS_REL.REQ Message 556
Table 1150: CC_ACCESS_REL.CNF Message 556
Table 1151: CC_ACCESS_REL.IND Message 557
Table 1152: CC_ACCESS_REL.RSP Message 557
Table 1153: CC_DCPPC.IND Message 558
Table 1154: CC_HP1_DET.CNF Message 559
Table 1155: CC_BLE_UPDATE.IND Message 559
Table 1156: CC_BCAST_REPEAT.IND Message 559
Table 1157: CC_POWERSAVE.REQ Message 560
Table 1158: CC_POWERSAVE.CNF Message 561
Table 1159: CC_POWERSAVE_EXIT.CNF Message 561
Table 1160: CC_POWERSAVE_LIST.CNF Message 562
Table 1161: CP_PROXY_APPOINT.REQ Message 563
Table 1163: HSTA State 565
Table 1164: CP_PROXY_APPOINT.CNF Message 565
Table 1165: Result 566
Table 1167: NN_INL.REQ and NN_INL.CNF Message 567
Table 1168: NN_NEW_NET.REQ Message 570
Table 1169: NN_NEW_NET.CNF Message 571
Table 1170: Format of Information Field when Result = 0x00 (Successful) 572
Table 1171: Format of Information Field when Result = 0x01 (Unsuccessful SNID) 572
Table 1172: Format of Information Field when Result = 0x02 (Unsuccessful SlotID) 573
Table 1173: NN_NEW_NET.IND Message 573
Table 1174: NN_ADD_ALLOC.REQ Message 574
Table 1175: NN_ADD_ALLOC.CNF Message 575
Table 1176: NN_ADD_ALLOC.IND Message 576
Table 1177: NN_REL_ALLOC.REQ Message 576
Table 1178: NN_REL_ALLOC.CNF Message 577
Table 1179:NN_REL_NET.IND Message 578

Table 1180: CM_UNASSOCIATED_STA.IND Message 580
Table 1181. CM_ENCRYPTED_PAYLOAD.IND Message 581
Table 1182: Payload Encryption Key Select Interpretation 582
Table 1183: AVLN Status Interpretation 582
Table 1184: Protocol ID Interpretation 583
Table 1185: CM_ENCRYPTED_PAYLOAD.RSP Message 585
Table 1186: Result Field Interpretation 585
Table 1187: CM_SET_KEY.REQ Message 586
Table 1188: Key Type Interpretation 587
Table 1189. CM_SET_KEY.CNF Message 588
Table 1190: CM_GET_KEY.REQ Message 589
Table 1191: CM_GET_KEY.CNF Message 590
Table 1192: CM_SC_JOIN.REQ Message 591
Table 1193: CM_SC_JOIN.CNF Message 592
Table 1194: CM_CHAN_EST.IND Message 593
Table 1195: RIFS_AV, RIFS_AV_OneSym, and RIFS_AV_TwoSym Interpretation 597
Table 1196: FEC Type/Code Rate Interpretation 597
Table 1197: Guard Interval Length Interpretation 598
Table 1198: CBD_ENC Interpretation 598
Table 1199: Interpretation of Modulation Type 599
Table 11101: Two Nibble Run Length Interpretation 600
Table 11102: Tone Map Update Information 601
Table 11103: Amplitude Update Indication 603
Table 11104: CM_AMP_MAP.CNF Message 603
Table 11105: Bridging Information Response 604
Table 11106: Bridging Information Variable Field (BIVF) 604
Table 11107: CM_CONN_NEW.REQ Message 605
Table 11108: CM_CONN_NEW.CNF Message 606
Table 11109: CM_CONN_REL.IND Message 607
Table 11110: CM_CONN_REL.RSP Message 607
Table 11111: CM_CONN_MOD.REQ Message 608
Table 11112: CM_CONN_MOD.CNF Message 608
Table 11113: CM_CONN_INFO.REQ Message 609
Table 11114: CM_CONN_INFO.CNF Message 610
Table 11115: Format of ConnInfo 610
Table 11116: CM_STA_CAP.CNF Message 610
Table 11117: CM_NW_INFO.CNF Message 612
Table 11118: NWINFO Field Format 613
Table 11119: CM_GET_BEACON.REQ Message 614
Table 11120: CM_HFID.REQ Message 614
Table 11121: CM_HFID.CNF Message 615
Table 11122: CM_MME_ERROR.IND Message 615

Table 11123: CM_NW_STATS.CNF Field Format 616
Table 11124: CM_LINK_STATS.REQ Message 617
Table 11125: CM_CONN_STATS.CNF Message 618
Table 11126: LinkStats Field Format for Transmit MFS 618
Table 11127: LinkStats Field Format for Receive MFS 620
Table 11128: CM_STA_IDENTIFY.CNF Field Format 621
Table 11129: CM_ROUTE_INFO.CNF Message 623
Table 11130: CM_ROUTE_INFO.CNF Message 624
Table 11132: CM_SLAC_PARM.CNF Message 627
Table 11133: CM_START_ATTEN_CHAR.IND Message 630
Table 11134: CM_START_ATTEN_CHAR.IND Message 631
Table 11135: CM_ ATTEN_CHAR.IND Message 633
Table 11-136: CM_ ATTEN_CHAR.IND ACVarField Contents 634
Table 11137: ATTEN_PROFILE field format 636
Table 11138: CM_ ATTEN_CHAR.RSP Message 636
Table 11139: CM_ ATTEN_CHAR.CNF ACVarField Contents 637
Table 11140: CM_ PKCS_CERT.REQ Message 638
Table 11142: CM_ PKCS_CERT.CNF Message 639
Table 11143: CM_ PKCS_CERT.IND Message 640
Table 11144: CM_ PKCS_CERT.RSP Message 641
Table 11145: CM_ MNBC_SOUND.IND Message 641
Table 11146: CM_ MNBC_SOUND.IND Message MSVarField Contents 642
Table 11147: CM_VALIDATE.REQ Message 643
Table 11148: VRVarField when SignalType is set to 0x00 644
Table 11149: CM_VALIDATE.CNF Message 644
Table 11150: VCVarField when SignalType is set to 0x00 645
Table 11151: CM_SLAC_MATCH.REQ Message 645
Table 11152: Content of CM_SLAC_MATCH.IND Var Field 646
Table 11153: CM_ SLAC_MATCH.CNF Message 647
Table 11154: Content of CM_SLAC_MATCH.CNF Var Field 648
Table 11159: Vendor-Specific MME Fields 651
Table 121: ETH_SEND.REQ Primitive 655
Table 122: ETH_SEND.CNF Primitive 655
Table 123: ETH_RECEIVE.IND Primitive 657
Table 124: APCM_CONN_ADD.REQ Primitive 658
Table 125: APCM_CONN_ADD.CNF Primitive 659
Table 126: APCM_CONN_ADD.IND Primitive 659
Table 127: APCM_CONN_ADD.RSP Primitive 660
Table 128: APCM_CONN_MOD.REQ Primitive 660
Table 129: APCM_CONN_MOD.CNF Primitive 661
Table 1210: APCM_CONN_MOD.IND Primitive 661
Table 1211: APCM_CONN_MOD.RSP Primitive 662

Table 1212: APCM_CONN_REL.REQ Primitive 662
Table 1213: APCM_CONN_REL.CNF Primitive 662
Table 1214: APCM_CONN_REL.IND Primitive 663
Table 1215: APCM_GET_NTB.REQ Primitive 663
Table 1216: APCM_GET_NTB.CNF Primitive 664
Table 1217: APCM_AUTHORIZE.REQ Primitive 665
Table 1218: APCM_AUTHORIZE.CNF Primitive 665
Table 1219: APCM_AUTHORIZE.IND Primitive 666
Table 1220: APCM_GET_SECURITY_MODE.REQ Primitive 666
Table 1221: APCM_GET_SECURITY_MODE.CNF Primitive 666
Table 1222: APCM_SET_SECURITY_MODE.REQ Primitive 667
Table 1223: APCM_SET_SECURITY_MODE.CNF Primitive 667
Table 1224: APCM_GET_NETWORKS.REQ Primitive 667
Table 1225: APCM_GET_NETWORKS.CNF Primitive 668
Table 1226: APCM_SET_NETWORKS.REQ Primitive 668
Table 1227. APCM_SET_NETWORKS.CNF Primitive 668
Table 1228. APCM_GET_NEWSTA.REQ Primitive 669
Table 1229: APCM_GET_NEWSTA.CNF Primitive 669
Table 1230: APCM_GET_NEWSTA.IND Primitive 670
Table 1231: APCM_SET_KEY.REQ Primitive 670
Table 1232: APCM_SET_KEY.CNF Primitive 671
Table 1233:. APCM_GET_KEY.REQ Primitive 671
Table 1234: APCM_GET_KEY.CNF Primitive 671
Table 1235. APCM_STA_RESTART.CNF Primitive 672
Table 1236. APCM_NET_EXIT.CNF Primitive 672
Table 1237: APCP_SET_TONE_MASK.REQ Primitive 672
Table 1238: APCP_SET_TONE_MASK.CNF Primitive 673
Table 1239: APCP_SET_TONE_MASK.REQ Primitive 675
Table 1240: APCM_SET_PPKEYS.REQ Primitive 676
Table 1241: APCM_SET_PPKEYS.CNF Primitive 676
Table 1242: APCM_SET_CCo.REQ Primitive 677
Table 1243: APCM_CONF_SLAC.REQ Primitive 677
Table 1244: MD_DATA.REQ Primitive 679
Table 1245: MD_DATA.CNF Primitive 680
Table 1246: MD_DATA.IND Primitive 681
Table 131: Recommended User Priority-to-Traffic Class Mappings 682
Table 132: Recommended Application Class-to-User Priority Mappings 683
Table 13-2b: Test Vectors 691
Table 133: Example AES Encryption Keys Hashed from Passwords 692
Table 134: Example NID Offset Hashed from NMK-HS with Appended Security Level 692
Table 135: Example CM_SET_KEY.REQ Message Provisioning NMK Using the DAK 693
Table 136: Example CM_ENCRYPTED_PAYLOAD.IND Message Provisioning NMK Using

the DAK 694
Table 137: CM_GET_KEY.REQ Provisioning NMK Using UKE – Message 1 696
Table 138: CM_GET_KEY.CNF Provisioning NMK Using UKE – Message 2 698
Table 139: CM_SET_KEY.REQ Provisioning NMK Using UKE – Payload of Message 3 700
Table 1310: CM_ENCRYPTED_PAYLOAD.IND Provisioning NMK Using UKE – Message 3 702
Table 1311: CM_SET_KEY.CNF Provisioning NMK Using UKE – Payload of Message 4 703
Table 1312: CM_ENCRYPTED_PAYLOAD.IND Provisioning NMK Using UKE – Message 4 704

List of Equations
Equation 41: PPB Formula 121
Equation 42: Formula for Reconstructing the PPB Exponent and Mantissa Values 122
Equation 43: Formula for Calculating the BLE 123
Equation 44: BLE Formula 123
Equation 45: Formula for Reconstructing the BLE Exponent and Mantissa Values 123
Equation 51: Formula for Calculating the RDR 304

Introduction

References

Documents referenced in this specification are listed below.

HomePlug Powerline Alliance, HomePlug 1.0.1 specification

Federal Information Processing Standards Publication 197: Specification for the Advanced Encryption Standard (AES) - November 26, 2001

National Institute of Standards and Technology Special Publication 800-38A, 2001 Edition: Recommendation for Block Cipher Modes of Operation, Methods and Techniques - December 2000

IEEE Std 802-2001: IEEE Standard for Local and Metropolitan Networks: Overview and Architecture – published 8 March 2002

RFC4086, Eastlake 3rd, D., J. Schiller, and S. Crocker, "Randomness Requirements for Security," RFC 4086, June 2005

Schneier, B., "Applied Cryptography: Protocols, Algorithms, and Source Code in C," 2nd Edition, John Wiley & Sons, 1996

FIPS 180-2, NIST, "Secure Hash Standard," August 26, 2002, (including the change notice dated February 25, 2004, concerning truncation)

PKCS #5 v2.0 standard, Password-based Cryptography Standard

ITU-T Rec. X.667 | ISO/IEC 9834-8 "Information Technology - Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: Generation and Registration of Universally Unique Identifiers (UUIDs) and their Use as ASN.1 Object Identifier Components," http://www.itu.int/ITU-T/studygroups/com17/oid/X.667-E.pdf, Sept. 2004.

Leach, P. and R. Salz, IETF RFC 4122, "A Universally Unique IDentifier (UUID) URN Namespace," http://www.ietf.org/rfc/rfc4122.txt, July 2005.

IEEE Std 802.1Q-1998: IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks

IEEE Std 802.3-2005: IEEE Standard for Information technology-Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications

RFC 768: User Datagram Protocol
RFC 791: Internet Protocol
RFC 793: Transmission Control Protocol
RFC 2205: Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification
RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
HomePlug Powerline Alliance, HomePlug AV 1.1 Specification (May 21, 2007)
IEEE P1901 Draft Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications (Apr 2010)
HomePlug Powerline Alliance, Policy 3: HomePlug AV AVLNs operating in Coordinated or Uncoordinate Mode in the presence of other HomePlug AV AVLNs operating in CSMA-Only mode
HomePlug Powerline Alliance, Policy 1.1: HomePlug AV v1.1 in the presence of HomePlug BPL devices based on HomePlug 1.0.1
RFC 5652: Cryptographic Message Syntax (CMS)
RFC 5258: Internet Message Access Protocol version 4 - LIST Command Extensions
RFC 3565: Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)
RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 5480: Elliptic Curve Cryptography Subject Public Key Information
RFC 5758: Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA

File Integrity Verification

All files distributed with the GREEN PHY specification are listed with a 64-digit hexadecimal hash calculated on the contents of the original file. The hash is calculated using the SHA-256 Message-Digest Algorithm as specified in reference [8]. All files distributed with the GREEN PHY specification can be verified against their originals by recalculating the SHA-256 hash and comparing it against the hash listed in this document.

Acronyms and Abbreviations

Table 11: defines the acronyms and abbreviations in this specification. For more information about an acronym or abbreviation, refer to the section shown in the **Section Ref.** column.

Table 11: Acronyms and Abbreviations

Acronym	Meaning	Section Ref.
ACK	ACKnowledge	4.4.1.3 4.4.1.4 4.4.1.5.3.7
ACLSS	AC Line Cycle Synchronized Status	4.4.3.10

ACS	Auto-Connect Service	6.6
AES	Advanced Encryption Standard	5.4.5.1
AFE	Analog Front End	3.1
AGC	Automatic Gain Control/ Automatic Gain Controller	3.1,3.6.1
AIFS	Allocation Interframe Spacing	5.6
API	Application Program Interface	12.1.4
ARP	Address Resolution Protocol	5.2.3.8.2
ARQ	Automatic Repeat Request	2.1.1
ATS	Arrival Time Stamp	6.7.3
AVF	Allocation Variant Field	9.8.3.3
AVLN	HomePlug AV In-Home Logical Network	2.2.3
BBT	BeaconBackoffTime	7.1
BCAST	Broadcast	5.2.3.8.2
BDA	Bridged Destination Address	11.5.15.3
BENTRY	Beacon Entry	4.4.3.15.4
BIFS	Burst Interframe Spacing	4.4.1.5.2.13.1
BLE	Bit Loading Estimate	4.4.1.5.2.10
BPCS	Beacon Payload Check Sequence	4.4.3.17
BPL	Broadband Access over Power Lines	Chapter 10
BPLN	Access/BPL Logical Network	Chapter 8
BPSK	Binary Phase Shift Keying	3.1, 3.5.5
BPST	Beacon Period Start Time	5.5.5
B2BIFS	Beacon-to-Beacon Interframe Spacing	5.6
BTO	Beacon Transmission Offset	4.4.1.5.1.2
BTS	Beacon Time Stamp	5.5
BTT	Beacon Transmit Time	5.5
BurstCnt	Burst Count	4.4.1.5.2.16
CBC	Cipher Block Chaining	5.4.5.1
CA	Contention Access	12.3.1.1.1
CC	Contention Control	9.4

CCo	Central Coordinator	Chapter 7
CEI	Channel Estimation Indication	5.2.6.1
CFP	Contention Free Period	5.1.1.2.1
CFPI	Contention-Free Period Initiation	9.6.1
CFS	Contention-Free Session	4.4.1.5.2.4 4.4.1.5.3.2 4.4.1.5.2.4
CI	Channel Interleaver	3.4.3
CID	Connection Identifier	5.2.1.4.2
CIFS	Contention Interframe Spacing	9.2.2
CIFS_AV	Contention Interframe Spacing	5.6.1
CINFO	Connection Information	7.8.1
CISPR	International Special Committee on Radio Interference	3.7.1
CL	Convergence Layer	Chapter 6 12.1
CLS	Connectionless Service	5.2.2.1
CLST	Convergence Layer SAP Type	4.4.1.5.2.23
CM	Connection Manager	2.1.2 7.8.1
CMS	Cryptographic Message Syntax	13.8.2.1
COS	Connection-Oriented Service	12.3.1.1.1
CP	Contention Period	5.1.1.2.1
CRC	Cyclic Redundancy Check	4.2
CSCD	Current Schedule Countdown	4.4.3.15.4.2.2
CSMA	Carrier Sense Multiple Access / Collision Detection	4.4.1.5.2.13.1 4.4.3.15.4.3.2
CSPEC	Connection Specification	5.2.1 7.8.1
CTS	Clear To Send	4.4.1.5.4
CW	Contention Window	9.2.2
DA	Destination Address	5.4.1

DAK	Device Access Key	7.10.2.1
DBC	Distributed Bandwidth Control	5.8
DCPPCF	Different CP PHY Clock Flag	4.4.1.5.2.19
DHCP	Dynamic Host Configuration Protocol	5.2.3.8.2
DPLL	Digital Phase Locked Loop	5.1.1.1
DPW	Device Password	7.10.2.2
DT	HomePlug 1.0.1 Delimiter Type	4.4.1.1
DT_AV	HomePlug AV Delimiter Type	4.4.1.2
DTEI	Destination Terminal Equipment Identifier	4.4.1.5.2.2
EIFS	`Extended InterFrame Space`	2.5
EKS	Encryption Key Select	4.4.1.5.2.8
EOF	End of Frame	9.3.1
ET	End Time	4.4.3.15.4.2.4.4
EVSE	Electric Vehicle Supply Equipment	13.8
FC	Frame Control	2.2.1
FC1.0.1	HomePlug 1.0.1 Frame Control	3.7.3.3.1
FCAV	Frame Control AV	3.7.3.3.2
FCCS	HomePlug 1.0.1 Frame Control Check Sequence	4.4.1.1
FCCS_AV	HomePlug AV Frame Control Check Sequence	4.4.1.5.6
FDCM	Frequency Division Coexistence Message	10.5.2
FEC	Forward Error Correction	11.5.10.5 3.3.1 3.4
FFDAC	Flexible frequency division access coexistence	10.5

FFT	Fast Fourier Transform	3.1
FL_AV	Frame Length	4.4.1.5.2.13.1
GLID	Global Link ID	5.2.1.4.1
GLID-F	GLID for the Forward Link	5.2.1.4.2
GLID-R	GLID for the Reverse Link	5.2.1.4.2 11.2.17 11.2.40
GreenPPEA	Green PHY-PEV-EVSE Association	13.8
HDTV	High Definition Television	5.4.6
HFID	Human Friendly Identifier	7.3.1.2
HLE	Higher Layer Entity	11.1 12.1.1
HM	Hybrid Mode	4.4.3.2
HOIP	Handover-in-Progress	4.4.3.11
HP10DF	HomePlug 1.0.1 Detect Flag	4.4.1.5.2.6 4.4.1.5.4.6
HP11DF	HomePlug 1.1 Detect Flag	4.4.1.5.2.7 4.4.1.5.4.7
HS-ROBO_AV	High-Speed ROBO Mode	3.4.4
HSTA	Hidden Station	7.7
HTTP	HyperText Transfer Protocol	10.1.3
ICV	Integrity Check Value	4.3.6
IEEE	Institute of Electrical and Electronics Engineers	4.1.2
IFFT	Inverse Fast Fourier Transform	3.1
IGF	Immediate Grant Flag	4.4.1.5.4.9
INL	Interfering Network List	8.1
IP	Internet Protocol	12.2.2.1
ISI	Inter-Symbol-interference	3.6.1
IV	Initialization Vector	5.4.5.3 11.5.2
KBC	Key Being Changed	4.4.3.15.4.8.2

KCCD	Key Change Countdown	4.4.3.15.4.8.1
LBDAT	Local Bridge Destination Address Table	5.3.1
LCT	Line Cycle Time	5.1.1.1
LID	Link Identifier	4.4.1.5.2.3 5.2.1.4.1
LLID	Local Link ID	5.2.1.4.1 5.4.1.2 12.3.1.1.1
LSB	Least-significant bit	4.1.1.1
MAC	Media Access Control	4.3 4.4 Chapter 5 7.8.1.1 12.3.1
MaxRxSSN	Maximum Receive Segment Sequence Number	5.4.1.6.2
MaxTxSSN	Maximum Transmit Segment Sequence Number	5.4.1.6.1
MCAST	Multicast	5.2.3.8.2
MCF	Multicast Flag	4.4.1.5.2.20 4.4.1.5.4.11
MFL	MAC Frame Length	4.3.1.2
MFSRspMgmt	Management MAC Frame Stream Response	4.4.1.5.3.7
MFSCmdData	Data MAC Frame Stream Command	4.4.1.5.2.25
MFSCmdMgmt	Management MAC Frame Stream Command	4.4.1.5.2.19
MFSRspData	Data MAC Frame Stream Response	4.4.1.5.3.6
MFT	MAC Frame Type	4.3.1.1
MINI-ROBO_AV	Mini-ROBO Mode	3.4.3.1
MinRxSSN	Minimum Receive Segment Sequence Number	5.4.1.6.2

MinTxSSN	Minimum Transmit Segment Sequence Number	5.4.1.6.1
MITM	Man-in-the-Middle	7.10.10.1
MM	Management Message	11.1
MME	Management Message Entry	11.1.8
MMQF	Management Message Queue Flag	4.4.2.1.1.4
MMTYPE	Management Message Type	11.1.6
MNBC	Multi-Network Broadcast	5.4.3.1
MNBF	Multi-Network Broadcast Flag	4.4.1.5.2.21
MPDU	MAC Protocol Data Unit	4.4
MPDUCnt	MPDU Count	4.4.1.5.2.15
MSB	Most-significant bit	4.1.1.1
MSC	Message Sequence Chart	7.3.1.3
MSDU	MAC Service Data Unit	4.3
NACK	Negative ACKnowledge	4.4.1 5.4.1.6.1
NBDA	Number of Bridged Destination Addresses	11.5.15.2
NBP	Number of Beacon Periods	11.2.39.10
NCNR	Non-Coordinating Networks Reported	4.4.3.5
NCo	Neighbor Coordinators	8.3.5.1
NEK	Network Encryption Key	7.10.2.5
NewEKS	New Key's EKS	4.4.3.15.4.8.3
NID	Network Identifier	0
NMB	Number of Missed Beacons	11.2.39.2
NMK	Network Membership Key	7.10.2.3
NMK-HS	NMK – Secure Security Level	7.10.3.1 7.10.3.1.1
NMK-SC	NMK – Simple Connect Security Level	7.3.4 7.10.3.1.2 7.10.3.5
NMK-SL	NMK – Security Level	7.3.1

NPSM	Network Power Saving Mode	4.4.3.6
NPW	Network Password	7.10.2.4
NTB	Network Time Base	5.5
NTB_STA	Network Time Base Estimate at Each Station	5.5
NumSlots	Number of Beacon Slots	4.4.3.7
ODA	Original Destination Address	11.1.1
OFDM	Orthogonal Frequency Division Multiplexing	3.1
OPAD	Octet Pad	4.4.3.15.4.14.1
OPSF	Oldest Pending Segment Flag	4.4.2.1.1.6
OSA	Original Source Address	11.1.2
OUI	Organizationally Unique Identifier	4.4.3.15.4.16, 7.8.1.2, 11.7
PAL	Protocol Adaptation Layer	12.1.2
PAPR	Peak-to-Average Power Ratio	3.5.3
PB	PHY Block	4.4.2.1
PBB	PHY Block Body	4.4.2.1.2
PBC	PHY Block Count	5.4.5.3.2
PBCS	PHY Block Check Sequence	4.4.2.1.3
PBH	PHY Block Header	4.4.2.1
PBSz	PHY Block Size	4.4.1.5.2.11 4.4.1.5.5.4
PCo	Proxy Coordinator	7.7
PCS	Physical Carrier Sense	3.8.4
PEKS	Payload Encryption Key Select	11.5.2.1
PEV	Plug-in Electric Vehicle	13.8
PHY	Physical Layer	Chapter 3
PhyClk	PHY (layer) Clock	3.7.3.1
PhyNet	Physical Network	2.2
PID	Protocol ID	11.5.2.3
PLID	Priority Link ID	5.2.1.3 5.2.1.4.1
PMN	Protocol Message Number	11.5.2.5

PN	Pseudo Noise	0 3.5.1
PPB	Pending PHY Block	4.4.1.5.2.8.1
PPDU	PHY Protocol Data Unit	3.2.1 3.2.1.1
PRN	Protocol Run Number	11.5.2.5 11.5.2.4
PRP	Priority Resolution Period	9.2.1
PRS	Priority Resolution Slots	3.6.5
PSCD	Preview Schedule Countdown	4.4.3.15.4.2.1
PSD	Power Spectral Density	3.6.6
PSTA	Proxy Station	7.7
PxN	Proxy Network	7.7
QAM	Quadrature Amplitude Modulation	3.1 3.5 3.6.1
QMP	QoS and MAC parameters	7.8.1
QPSK	Quadrature Phase Shift Keying	3.5.4 3.5.5
QoS	Quality of Service	5.3.3 6.5 7.8.1
RBAT	Remote Bridged Address Table	5.3.2
RCG	RTS-to-CTS Gap	5.6.1
REQ_TM	Max. Tone Maps Requested	4.4.1.5.5.8
RET	Region End Time	4.4.3.15.4.3
RFC	Request for Comments	1.1
RIFS_AV	Response Interframe Spacing	4.4.1.5.2.12
ROBO	ROBust OFDM	3.4.3.1
RRTF	Request Reverse Transmission Flag	4.4.1.5.3.5
RSC	Recursive Systematic Convolutional	0
RSOF	Reverse SOF	4.4.1.5.6

RSR	Request SACK Retransmission	3.6.2 4.4.1.5.2.22 3.8.4.1
SNR	Signal-to-Noise Power Ratio	3.8.4.1
RSVD	Reserved	4.4.1
RSVP	Resource Reservation Protocol	Chapter 13
RTS	Request To Send	4.4.1.5.4
RTSBF	RTS Broadcast Flag	4.4.3.12
RTSF	RTS Flag	4.4.1.5.4.8
RxWSz	Receive Window Size	4.4.1.5.3.10
SA	Source Address	5.4.1
SACK	Selective Acknowledgement	4.4.1.5.3 5.4.8.1
SACKD	SACK Data	4.4.1.5.3.8
SACKT	SACK Type	5.4.8.1
SAF	Sound ACK Flag	4.4.1.5.5.6
SAI	Session Allocation Information	4.4.3.15.4.1.2
SAP	Service Access Point	12.2
SBM	Subnet Bandwidth Manager	Chapter 13
SC-Add	Simple Connect Add State	7.3.5.3
SCF	Sound Complete Flag	4.4.1.5.5.7
SC-Join	Simple Connect Join State	7.3.5.3
SDTV	Standard Definition Television	5.4.6
SJR	Signal-to-Jammer Power Ratio	3.8.4.1 3.8.4.2
SL	Security Level	7.3.1 7.10.3.1
SLAC	Signal Level Attenuation Characterization	5.2.9
SlotID	Beacon Slot ID	4.4.3.9
SlotUsage	Beacon Slot Usage	4.4.3.8
SNID	Short Network Identifier	4.4.1.4 11.2.29.3

SNR	Signal-to-Noise Power Ratio	3.6.2 3.8.4.1 3.8.4.2 5.5.4
SOF	Start of Frame	4.4.1.5.2
SPCS	Sound Payload Check Sequence	4.4.4.1.2
SSN	Segment Sequence Number	4.4.2.1.1.1 5.4.1.3
STA	Station	2.3
STA_Clk	Station (free-running) Clock	3.7.3.1
STD-ROBO_AV	Standard ROBO Mode	3.4.3.1
STEI	Source Terminal Equipment Identifier	4.4.1.5.2.1
SYNCP, SYNCM	SYNChronization symbols	3.6.1
TCC	Turbo Convolutional Code	0
TCP	Transmission Control Protocol	6.2.2
TDMA	Time Division Multiple Access	5.1.3.1.3
TEI	Terminal Equipment Identifier	7.3.2.1 11.2.29.4
TEK	Temporary Encryption Key	7.10.2.6
TM	Tone Map	3.2.1
TMD	Tone Map Data	4.4.1.5.5.13 5.2.6.2 11.5.10
TMI_AV	Tone Map Index	4.4.1.5.2.13
TPD_RMS	Transmit Preamble Distortion	3.7.3.3.3
TPRSD_RMS	Transmit PRS Waveform Distortion	3.7.3.3.4
TXOP	Transmission Opportunity	7.8.1
UDP	User Datagram Protocol	6.3

UE	User Experience	13.2
UI	User Interface	7.3.1.2 7.4
UIS	User Interface Station	7.10.9
UKE	Unicast Key Exchange	7.10.3.5
USTT	Unassociated Station Transmissin Time	7.1
VCS	Virtual Carrier Sense	5.1.3.1.2
VF_AV	Variant Fields	4.4.1.5
VPBF	Valid PHY Block Flag	4.4.2.1.1.3
ZPAD	Zero Pad	4.4.4.1.1

Conventions

All sections in the body of this specification constitute normative text, except when explicitly identified as informative. Appendices are individually identified as being normative or informative.

Informative Text

When appropriate, informative text is placed throughout the specification to provide additional information (for example, to clarify a complex normative statement or to articulate an alternate solution). Informative text is either specified in the clause (for example see clauses 1.5.1 to 1.5.3), or set off in one or more separate paragraph, with a border surrounding the informative text. It is preceded by a header centered on the page, indicating that the text is informative. For example:

Informative: Example of Informative Text This is an example of how informative text shall be displayed herein. It may consist of more than one paragraph and it may wrap to additional pages.

Binary and Hexadecimal Numbers

Binary numbers are indicated by the prefix 0b followed by the binary digits. Hexadecimal numbers are indicated by the prefix 0x followed by the hexadecimal digits.

Words and Phrases

Table 12 describes the words and phrases used in this specification.

Table 12: Words and Phrases

Word or Phrase	Meaning
Shall	The definition is an absolute requirement of the specification. Either the term “required” or “must” may be used with this the same meaning.
Shall not	The definition is an absolute prohibition of the specification. The phrase “must not” may be used with this the same meaning.

Should	There may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. The phrase "this should not be done" may be used with this same meaning.
Reserved Should not	When the term "reserved" is used in this specification to define the meaning of a given value or set of values for a field or other
	An item is optional. One implementer may choose to include the item because a particular marketplace requires it or because the
May	implementer feels that it enhances the product, while another implementer may omit the same item. An implementation that does not include a particular option must be capable of interoperating with another implementation that does include the option without compromising the minimum set of functions required of all devices. This specification does clearly call out options. Similarly, an implementation that does include a particular option must be capable of interoperating with another implementation that does not include the option (except, of course, for the feature the option provides). The adjective "optional" may be used with this same meaning.

Reserved	The specified bits are not currently used and are only available for use via extensions to the specification. They are not available for use by a particular implementation of this specification. Reserved bits shall be set to zero by the sender. Reserved bits shall be ignored by the receiver. When the term “reserved” is used in this specification to define the meaning of a given value or set of values for a field or other element, it means the values are not currently used and are only available for use via extensions to the specification. They are not available for use by a particular implementation of this specification. Reserved values shall not be used by the sender. Reserved values shall be ignored by the receiver.

Abbreviations

Abbreviations are always expanded the first time they are used. The expansion is of the form “Term To Be Abbreviated (TTBA).” For example: “Central Coordinator (CCo).” The expansion is repeated where the term is actually defined, if different. Abbreviations are case sensitive.

Message Nomenclature

Message nomenclature (REQ, CNF, IND, RSP) shall follow the conventions shown in Figure 11. Request messages always end in .REQ. The response (if any) to a Request message is always a Confirmation message, which ends in .CNF.

Indication messages always end in .IND. The response (if any) to an Indication message is always a Response message, which ends in .RSP.

Figure 11: Message Nomenclature

Message Nomenclature

Message Sequence Charts (MSCs) shall follow the conventions shown in Figure 12. Time is shown vertically, with the earliest time at the top. Space is shown horizontally.

Stations of direct interest in the protocol being described are indicated by vertical lines, with a label at the top displaying the name of the station.

Bubbles are used to reveal processing that occurs at a station.

Messages are depicted as horizontal arrows originating at the sending station. The text describes the contents of the message and other characteristics as appropriate.

Messages sent to all stations (i.e., broadcast either within an AVLN or all stations) are shown as arrows that extend most, but not all, the way to one of the destination stations in the MSC. See the first message in Figure 12.

Messages that may be sent, depending on the circumstances, are shown with dashed lines. This convention is independent of the arrow termination conventions.

Messages sent to a specific station shown in the MSC (i.e., with a unicast MAC address) are depicted with the arrowhead terminating on the destination station. (Note that these messages might or might not use the broadcast TEI.) See the second and third messages in Figure 12.
Unicast or broadcast messages sent to other stations not shown in the MSC are depicted as short arrows that may repeat to indicate the sender repeating similar messages to multiple recipients. See the last three arrows in Figure 12.
Alternative protocol paths are separated by heavy dashed lines, and the alternative is labeled using rotated text on the left side.

Figure 12. Message Sequence Chart Conventions

Overview of HomePlug Green PHY - A Low Power, Legacy Interoperable, Highly Reliable PLC from HomePlug

The following criteria are considered to be essential for any technology targeting smart energy, home control, home automation, etc., applications:

- Maintain high reliability/robustness (which includes range/coverage) despite reduced complexity
- Coexistence and interoperability with existing, deployed, and standardized technologies
- Scale to support for many low rate devices on a shared medium (which translates to high, bursted, bit rates)
- Provide greatly reduced power consumption
- Be cost effective
- Address time to market concerns (which includes availability from multiple suppliers)

To address all of these criteria, the Home Plug Powerline Alliance has developed a new specification, "Green PHY", which is a greatly simplified derivative of the existing, widely deployed, HomePlug AV technology.

Basing the Green PHY upon HomePlug AV was a reasonable choice considering its field-proven characteristics, large and worldwide installed base, well established Compliance & Interoperability (C & I) program, and multi-vendor ecosystem. In effect, HomePlug AV jumpstarts the Green PHY.

HomePlug AV employs three robust modes of communication, called ROBO Modes, for several purposes, including beaconing, data broadcast/multicast communication, session setup, and exchange of Management Messages. All ROBO Modes use QPSK modulation, along with a ½ rate Turbo Convolutional Code. The Green PHY uses only these modes.

Besides the robust nature of these modes, the further advantages of using only the ROBO modes for the Green PHY are as follows:

- minimum impact on HPAV throughput
- interoperable with current HPAV and future IEEE P1901 solutions baselined on HPAV (the Green PHY will be certified by HomePlug as a profile of P1901)
- able to support multiple PHY Rates (3.8 Mbps, 4.9 Mbps, 9.8 Mbps)
- reuses the entire 2 – 30 MHz band
- reduces complexity of PHY (e.g., FEC, AFE, DFE)
- enables low power modes via reduced duty cycle (i.e., "awake" time)

Since a high speed bursted mode is used, an effective packet throughput (per device/ application) of approximately 250 kbps can met by utilizing <7% of the beacon period. However, since the Green device is only "on" or "awake" for this short interval, the estimated average power consumption is approximately 7% that of HPAV. To extrapolate further, by exploiting the duty cycle, 10 kbps could be provided using <1% duty cycle which provides opportunity for very low power modes. Alternately, higher throughput rates can be supported using more of the beacon period (but with a consequent increase in power consumption).

The advantages of reusing the entire 2 – 30 MHz band is that optimal performance can still be

3.4.2	Turbo Convolutional Encoder	rate 16/21 is not supported Fig 3-10b, puncturing is not

maintained (i.e., maximizing the number of potentially usable carriers) and tone masking and amplitude (TX power) maps for regulatory compliance and coexistence with HAM bands are still supported.

But it is not only in the PHY where advantages are obtained. Since the MAC is also reused, not only can the Green PHY device receive HPAV beacons, it can also transmit HPAV beacons. This means that a single, standalone Green PHY device can be a member of an AV network and can be the CCo in the AV network.

However, in order to reduce MAC complexity, a Green PHY device is only required to be a CCo in support of CSMA/CA only. In HPAV terms, the Green PHY device only needs to be a Level-0 CCo. This means that connection oriented communication cannot be controlled by a Green PHY devices, although it can participate in an AV network that permits connection oriented communications between HPAV devices.

A further simplification for the MAC occurs directly from the PHY simplification. Exclusive use of the ROBO modulation modes implies that there is no need to manage/maintain tone maps. Despite simplification of the MAC, reuse of the multiple priority level QoS mode and Priority Resolution mechanism allows for straightforward low latency support of Demand Response / Load Shedding.

Comparisons between HomePlug GREEN PHY and HomePlug AV PHY [Informative]

The material in this section informatively compares the HomePlug AV specification to the HomePlug GREEN PHY specification. However, it is essential to note that GREEN PHY is based upon HomePlug AV and is designed to be interoperable with HomePlug AV. Any items not specifically identified as being optional for GREEN PHY must be assumed to be requirements for both GREEN PHY and HomePlug AV.

Differences between HomePlug GREEN PHY and HomePlug AV PHY [Informative]

The material in this section points to the sections of this specification that modify (i.e., reduce or relax in functionality) HomePlug AV. Brief descriptions are included. However, this section must be considered as informational only and therefore used only as a quick reference for the reader.

Table 13: Differences between HomePlug GREEN PHY and HomePlug AV PHY

Chapter3	PHY	Description of change
3.1	Overview	GP overview; includes TX/ RX block diagram
3.2.1	PPDU Formats	GP PPDU payload formats are ROBO only
3.2.3	Symbol Timing	Table 3-2 (GIs for 417, 567, 3534 are not required)
3.4	Payload FEC Processing	Only rate ½ is supported by GP, 16/21 is not supported by GP; ROBO Interleaver is required

3.4.2	Turbo Convolutional Encoder	rate 16/21 is not supported Fig 3-10b, puncturing is not supported
3.4.2.2	Constituent Encoders	puncturing is not supported
3.4.2.3	Puncturing	puncturing Is not supported (Tables 3-5, 3-6)
3.4.3	Channel Interleaver	Table 3-11 (only rate ½ applies, rate 16/21 is not supported)
3.5	Mapping	Table 3-14 (only QPSK is required, only FC and ROBO are applicable) Only ROBO tone maps are supported by GP
3.5.2	Last Symbol Padding	Table 3-15 indicates that ROBO must obey/comply to the Tone Map/Tone Mask/ Amplitude MASK; other modulations are not applicable to GP
3.5.5	Mapping for BPSK, etc.	Only QPSK applies (all other modulation schemes do not apply) Only QPSK applies Table 3-17 only row for QPSK Table 3-18 only column for QPSK Table 3-19 not applicable Table 3-20 only row for QPSK
3.7.3.2	Transmit Constellation Error	Table 3-25, RMS Transmit Constellation Error Limit is -10 for GP PPDU
3.8.1.1	Receiver Minimum Input Voltage	Redefined, does not refer to rate 16/21, 1024-QAM
3.8.1.2	Receiver Maximum Input Voltage	Redefined, does not refer to rate 16/21, 1024-QAM

Differences between HomePlug GREEN PHY MAC (and above) and HomePlug AV MAC (and above) [Informative]

The material in this section points to the sections in this specification that either modify (e.g.,

reduce or relax functionality) or extend the HomePlug AV specfication. Brief descriptions are included. However, this section must be considered as informational only and therefore used only as a quick reference for the reader.

Table 14: Differences between HomePlug GREEN PHY MAC and above) and HomePlug AV (MAC and above)

Chapter 4	Frame Formats	description of change
4.3.2.1	Arrival Time Stamp	Not required as Connection services are not required for GREEN PHY
4.4.1.5.2.1.1	Source Terminal Equipment Identifier (STEI)	Behavior for routing/repeating in GREEN PHY
4.4.1.5.2.8.1	Encryption Key Select (EKS)	Describes additional feature
4.4.1.5.2.9 and 4.4.1.5.2.9.1	Pending PHY Blocks (PPB)	Behavior for routing/repeating in GREEN PHY
4.4.1.5.2.10 and 4.4.1.5.2.10.1	Bit Loading Estimate	Behavior for routing/repeating in GREEN PHY
4.4.1.5.2.13.1	Tone Map Index (TMI_AV)	Only ROBO modes are required for GREEN PHY
4.4.1.5.2.19.1	Different CP PHY Clock Flag (DCPPCF)	Optional feature for GREEN PHY
4.4.3	Format of Beacon MPDU Payload	New beacon payload fields for GREEN PHY
4.4.3.12.1	RTS Broadcast Flag (RTSBF)	Optional feature for GREEN PHY
4.4.3.15.2	Beacon Entry Header (BEHDR)	New beacon entry headers for GREEN PHY
4.4.3.15.4.6	Discovered Info BENTRY	New capability/versioning added for GREEN PHY
4.4.3.15.4.6.10	GREEN PHY Capability	New
4.4.3.15.4.6.11	HPAV Version	New
4.4.3.15.4.15 (and 4.4.3.15.4.15.1-6)	Power Save BENTRY	New Beacon Entry for GREEN PHY
4.4.3.18	Proxy Level (Plevel)	New feature
4.4.3.19	Reusable SNID Flag (RSF)	New feature
Chapter 5	MAC	description of change
5.1.1.1.1	Line Cycle Synchronization	Required for ISP
5.1.2.1.1	Beacon Period Structure in CSMA-Only Mode	CSMA-CA is required for GREEN PHY. Station must be Level 0 CCo
5.1.2.2.1	Beacon Period Structure in Uncoordinated Mode	Uncoordinated mode is not required for GREEN PHY. Station is not required to be Level 1 CCo
5.1.2.3.1	Beacon Period Structure in Coordinated Mode	Coordinated mode is not required for GREEN PHY. Station is not required to be Level 2 CCo

5.1.3.1.4	Channel Access Priority	Informative text added for Preferred Allocation
5.1.3.1.5	CSMA/CA Channel Access	References to Preferred Allocation and Distributed Bandwidth Control
5.2.1.3.1	Connectionless “Links”	Required for GREEN PHY
5.2.1.4.3	Link Identifiers	New feature added to identify GREEN PHY Preferred Allocations
5.2.1.4.4	Connection Identifiers	New feature added to identify GREEN PHY Preferred Allocations
5.2.3.1.1	Connection Setup	Not required for GREEN PHY
5.2.3.2.1	Global Link Setup	Not required for GREEN PHY
5.2.3.5.3	Connection Teardown	Not required for GREEN PHY
5.2.3.7.3	Connection Reconfiguration	Not required for GREEN PHY
5.2.3.8.2	Squeeze and De-squeeze	Not required for GREEN PHY
5.2.6.1.1.3	Channel Estimation	Not required for GREEN PHY as only ROBO modes are used.
5.2.6.7	Handling of Channel Estimation Requests	Although GREEN PHY does not initiate channel estimation, it is required to respond appropriately to channel estimation.
5.3.1.1.1	Behavior for Incoming Traffic	Behavior for routing/repeating in GREEN PHY
5.4.6.1	MPDU Bursting	Green PHY stations do not transmit MPDU bursts but are capable to receive MPDU bursts
5.4.7.4	Bidirectional Bursting	Not required for GREEN PHY
5.4.8.1.2	Request SACK Retransmission	Not required for GREEN PHY
5.8	Distributed Bandwidth Control	New feature
5.9	Power Save Mode	New feature
5.10	Routing and Repeating	New feature
5.11	Transmit Power Control	New feature
Chapter 6	Convergence Layer	description of change
6.2.4	Packet Classification	Clarification for GREEN PHY
6.6.3	Auto Connect Service	Not required for GREEN PHY
6.7.3.1	Smoothing	Not required for GREEN PHY
Chapter 7	CCo	description of change
7.2.3.1	Identifying HomePlug GREEN PHY Stations	New feature
7.3.5.3.1	SC-Join and SC-Add	Behavioral clarification
7.4.1	CCo Selection for a New AVLN	Behavioral clarification
7.7	Proxy Networking with GREEN PHY Extensions to Support Routing and Repeating	New features
7.7.1	Identification of Hidden Stations	Includes elaboration on new features

7.7.3.2	PCo-Required Task	Includes elaboration on new features
7.7.4	Proxy Beacons	Includes elaboration on new features
7.7.5	Provisioning the NMK to Hidden Stations	Includes elaboration on new features
7.7.6	Provisioning NEK for Hidden Stations (Authenticating the HSTA)	Includes elaboration on new features
7.7.7	Exchange of MMEs Through a PCo	Includes elaboration on new features
7.7.12	Proxy Network Limitations	Includes elaboration on new features
7.8.1.7	Connection Specification (CSPEC)	not required
7.8.2.1	Scheduler and Bandwidth Allocation	not required
7.8.3.1	Connection Admission Control	not required
7.8.5	Bandwidth Allocation	Informative text on Preferred Allocation
Chapter 8	Multiple Networks	description of change
8.1.1.1	CSMA-Only Mode	Required
8.1.2.1	Uncoordinated Mode	Not required
8.1.3.1	Coordinated Mode	Not required
8.2.1.1	GREEN PHY Preferred Allocation and Minimum CSMA Region	New feature
Chapter 11	MMEs	description of change
11	Management Messages	Many new MMEs for GREEN PHY, also many existing MMEs are not required
11.2.10	MME Support of HomePlug GREEN PHY	detailed description of required MMEs, optional MMEs, new MMEs
11.2.54	CC_BLE_UPDATE.IND	New
11.2.55	CC_BCAST_REPEAT.IND	New
11.2.56	CC_BCAST_REPEAT.RSP	New
11.2.57	CC_POWERSAVE.REQ	New
11.2.58	CC_POWERSAVE.CNF	New
11.2.59	CC_POWERSAVE_EXIT.REQ	New
11.2.60	CC_POWERSAVE_EXIT.CNF	New
11.2.61	CC_POWERSAVE_LIST.REQ	New
11.2.62	CC_POWERSAVE_LIST.CNF	New
11.5.10	CM_CHAN_EST.IND	additions to accommodate GP
11.5.29	CM_GET_BEACON.CNF	additions to accommodate GP
11.5.37	CM_STA_IDENTIFY.REQ	New
11.5.38	CM_STA_IDENTIFY.CNF	New
11.5.39	CM_STA_IDENTIFY.IND	New
11.5.40	CM_STA_IDENTIFY.RSP	New
11.5.41	CM_ROUTE_INFO.REQ	New
11.5.42	CM_ROUTE_INFO.CNF	New

11.5.42.1	Route Data Rate (RDR)	New
11.5.43	CM_ROUTE_INFO.IND	New
11.5.44	CM_UNREACHABLE.IND	New
11.5.44.1	Unreachable Time Stamp (UnrchTS)	New
Chapter 12	SAP Primitives	description of change
12.2.50	APCM_SET_HD_DURATION.REQ	new
12.2.51	APCM_SET_HD_DURATION.CNF	new
12.2.52	APCM_UNASSOCIATED_STA.IND	new
12.2.53	APCM_SC_JOIN.REQ	new
12.2.54	APCM_SC_JOIN.CNF	new
12.2.55	APCM_SET_PPKEYS.REQ	new
12.2.56	APCM_SET_PPKEYS.CNF	new
Chapter 14	ISP	description of change
14	ISP	new

Identical Requirements for HomePlug GREEN PHY and HomePlug AV PHY
Unless specifically identified as differing in functional requirement, (e.g.,, reduction or relaxation in functionality) all requirements for HomePlug AV are applicable to the HomePlug GREEN PHY.

System Overview
Network Reference Block Diagram
System Reference Model
At the highest level of abstraction, the HomePlug GREEN PHY system consists of the functional blocks shown in Figure 21. Note that the basic reference model is identical to HomePlug AV.

Figure 21: System Block Diagram
On the transmit side:
The PHY layer performs error-control correction, mapping into OFDM Symbols, and generation of time-domain waveforms.
The MAC determines the correct position of transmission, formats data frames into fixed-length entities for transmission on the channel and ensures timely and error-free delivery through Automatic Repeat Request (ARQ).
The Convergence layer performs bridging, classification of traffic into Connections, and data delivery smoothing functions.
The receive side performs the corresponding functions, in reverse.
Protocol Layer Diagram
Figure 22 shows the protocol entities defined in this specification interface as they relate to each other.
Protocol entities that get directly involved in the transfer of user payload make up the Data Plane of the protocol stack. Protocol entities that are involved in creating, managing and terminating the flow of data make up the Control Plane. Protocol entities communicate with each other through Service

Access Points (SAPs), i.e., well-defined interfaces described through primitives, which can be thought of as precursors of Application Programming Interfaces (APIs) between blocks that implement the protocol entities.
The specification has chosen to define the Control Plane as a single monolithic entity, called the "Connection Manager" (CM), rather than defining interfaces and primitives within the Control Plane. In each logical network (refer to Section 2.2.2) one station, called the Central Coordinator (CCo) (refer to Chapter 7), is responsible for setting up and maintaining the logical network, managing the communication resource on the wire, and coordinating with neighbor networks that use the same wire resource (refer to Chapter 8). The CCo may be viewed as a network-wide control plane entity. There is precisely one active CCo per network.

Figure 22: Protocol Layer Architecture

Network Concepts

Physical Network

The Physical Network (PhyNet) of a given STA (station) is the set of STAs that can physically communicate with the STA at least at the level of Frame Control (FC) and ROBO mode (i.e., it is the set of STAs seen by the PHY). All stations in a PhyNet have the potential to interfere with each other, but they also have the capability to minimize the mutual interference through coordination (refer to Chapter 8).
Note: A PhyNet is relative to a given STA, and it is possible that the PhyNets of physically close-by STAs are distinct. Figure 23 shows three examples of PhyNets, where the lines indicate ability to communicate on the PHY level. It is assumed that all STAs that can communicate with each of the depicted STAs in Figure 23 are shown in the figure. The PhyNets of all STAs in the three examples are summarized in Table 21. Note that:
In the first example (Figure 23a,) all stations can communicate with each other and the PhyNet of all stations is the same set {A,B,C,D,CCo}.
In the third example (Figure 23c), the PhyNet of D does not include the CCo. Furthermore, STA D is not in the PhyNet of the CCo, making D a "hidden station." A hidden STA is a station that does not belong to the PhyNet of the CCo, but belongs to the PhyNet of at least one STA that is in the PhyNet of the CCo.

Table 21: PhyNets in Figure 23

	Physical Networks (PhyNets) in …		
STA	Figure 23a	Figure 23b	Figure 23c
A	{A,B,C,D,CCo1}	{A,B,CCo1}	{A,B,CCo1}
B	{A,B,C,D,CCo1}	{A,B,CCo1}	{A,B,CCo1}
C	{A,B,C,D,CCo1}	{C,D,CCo2}	{C,D,CCo1}
D	{A,B,C,D,CCo1}	{C,D,CCo2}	{C,D}
CCo1	{A,B,C,D,CCo1}	{A,B,CCo1,CCo2}	{A,B,C,CCo1}
CCo2	N/A	{C,D,CCo1,CCo2}	N/A

Logical Networks and SubAVLNs

An AV In-Home Logical Network (AVLN) is the set of STAs, typically used in a home environment, that possess the same Network Identifier (NID) and NMK known by the CCo (refer

to Section 4.4.3.1). An AVLN typically will have a single Network Membership Key (NMK) (refer to Chapter 7), but may have more than one NMK for secure distribution of different Network Encryption Keys (NEKs – refer to Section 7.10). If the CCo elects to deploy multiple NEKs (possibly using multiple NMKs), several logical subnetworks of the AVLN are formed. These are called sub-AVLNs. Coordination, clock reference, and scheduling are performed on the basis of an AVLN. Cryptographic isolation is provided at the level of the sub-AVLN.

An AVLN is managed by a single STA called the Central Coordinator (CCo). Broadband Access over Power Lines (BPL) is beyond the scope of this specification, although Chapter 10 addresses the coexistence between AVLNs and BPL networks.

Note: An AVLN can coincide with the PhyNet of one or more STAs (as in Figure 23a) or be a subset of the PhyNet of a STA (as AVLN_1 in Figure 23b relative to the PhyNet of CCo1), or span the PhyNets of multiple STAs (as in Figure 23c). AVLN_1 and AVLN_2 in Figure 23b can form a pair of Neighbor Networks (refer to Chapter 8).

Communication Inside an AVLN

Two stations belonging to an AVLN will be able to communicate with each other if they belong to each other's PhyNet (see Figure 23). Note that it is possible, but not likely in typical deployments, that a broadcast transmission inside an AVLN is not received by all the stations of the AVLN. For example, in Figure 23c, broadcast transmissions from STA A will not be heard by stations C or D. Further, broadcast transmissions from CCo1 will not be heard by STA D, creating the need for STA C to act as a Proxy Coordinator (refer to Section 7.7) to manage STA D as part of the AVLN.

Figure 23: Examples of PhyNets and AVLNs

Station Roles

Each node in an AV Logical Network must have a minimum functionality, as described in the rest of this specification. Such a node is referred to as an AV Station, GREEN PHY Station, or simply "Station" (STA). In addition to the minimum functionality, STAs may also implement optional features.

Each STA in an AVLN shall be capable of managing the network, and *as a minimum* is responsible for:

Association and authentication of new STAs

Provisioning of Terminal Equipment Identifiers

CSMA-Only mode of operation and Passive Coordination of medium allocation with neighboring networks

Such a STA is called a Level-0 Central Coordinator (CCo) station (i.e., CCo without QoS support).

A STA that, in addition to the above functions, also provides:

Uncoordinated mode of operation

Provisioning of Global Link Identifiers, Admission control, and TDMA Scheduling for Global Links

is called a Level-1 CCo station. Level-1 CCos do not support Coordinated Mode.

A STA that, in addition to the above functions, also provides:

Coordinated Mode-based coordination with CCos of neighboring networks (NCCos) is called a Level-2 CCo station. The designation of Level-3 CCo is reserved for future CCos with advanced capabilities. At minimum, all stations are required to implement Level-0 CCo functionality. A station implementing HomePlug AV may support Level-1 or Level-2 CCo functionality. A station implementing only GREEN PHY is only required to implement Level-0 CCo functionality. More detailed description about CCo capabilities can be found in Section 7.4.3.1.

The abbreviation CCo may refer to any of these types of Central Coordinator, and in the absence of further qualification, its meaning should be clear from the context. CCos can either be preconfigured as such or be automatically selected using the procedures of Chapter 7. Only one STA in an AVLN can play the role of Central Coordinator at a time. An AVLN with a Level-x CCo is also referred to as Level-x AVLN throughout the specification.

One or more of the non-CCo stations of an AVLN may play a role in managing hidden STAs. Such STAs are called Proxy Coordinators (PCo) (refer to Chapter 7). The PCo functionality is optional.

One or more stations in the AVLN may act as bridges to other networks. The bridge is responsible for routing traffic between the AVLN and the other network based on a list of MAC addresses of devices it is bridging for. The bridge is also responsible for providing this list to other stations in the AVLN so other stations can efficiently deliver traffic within the AVLN using unicast transmissions.

Security Overview

This section provides an overview of security goals, controls, and issues as perceived during development of this specification. This section and all its subsections are informative.

Security Goals and Constraints

An AVLN (or sub-AVLN) should be equivalent to a Category 5 wired network as much as practical. Specifically:

Network stations (STAs) should not be allowed to join a user's AV Logical Network (AVLN) unless the user is confident that the station is the equipment he wants to add.

STAs within the same AVLN are assumed to be trustworthy (i.e., they do not perform hostile actions or divulge keys deliberately).

STAs within a sub-AVLN should be able to communicate confidentially (message contents should not be exposed to stations outside the sub-AVLN).

STAs within an AVLN should have confidence in the integrity of the messages they receive (i.e., they were neither damaged nor deliberately changed, nor are they replays or forgeries).

It should be hard for a different AVLN to "capture" a STA, but it should be easy for a user to reclaim a device he owns that was "captured" by another network.

A user should be able to reset a device and give or sell it to another user.

Threat Model

We assume that a neighbor may be able to eavesdrop on transmissions within a residence, and may also be able to send transmissions to stations within that residence, without the knowledge of the users in that residence. We try to protect the system against knowledgeable attackers with reasonable resources, but not against well-funded attackers. As a point of reference, one may

assume that the attacker has access to a handful (say 10) of the fastest commercially available PCs today.
We also assume that for most situations (particularly in regard to Simple Connect Security Level), the attacker will not have access to specialized hardware for signal processing or MPDU reception, other than commercially available HomePlug AV or HomePlug GREEN PHY chips.
All hosts that have access to the network as a member of the AVLN or through a bridge that has joined the AVLN are considered to be benign.
HomePlug GREEN PHY Operation Under Various Regulatory Jurisdictions
The frequency bands and the transmit power that can be used by power line communication systems can change based on the regulatory jurisdiction. As with HomePlug AV, the GREEN PHY system uses the Tone Mask (refer to Section 3.6.7) and Amplitude Map (refer to Section 3.6.8) to enable modification of the transmit power spectrum to comply with regulatory constraints. HomePlug GREEN PHY currently defines the Tone Mask and Amplitude Map for operation within North America. Tone Masks and Amplitude Maps for other regulatory jurisdictions will be set by HomePlug as regulations for those regions become clear.

Parameter Specifications
Table 22 lists the HomePlug AV parameter specifications.

Table 22: HomePlug AV Parameter Specifications

Parameter	Value	Section Reference
Allocation Interframe Spacing (AIFS)	30 sec min.	5.6
AllocationTimeUnit	10.24 sec	4.4.3.15.4.2.4.3 4.4.3.15.4.2.4.4 4.4.3.15.4.3.3 11.2.16.5.2
Beacon To Beacon Interframe Spacing (B2BIFS)	90 sec ±0.5 sec	5.6
Burst Interframe Spacing (BIFS)	20 ±0.5 sec	5.4.6
CCo_Failure_Time	≥ 10 Beacon Periods	7.9.2
CFPI_EIFS	250 sec	9.6.1
CIFS	35.84 ±0.5 sec (from start of extended Symbol(s) until start of PRS0)	1.1 (HomePlug 1.0.1 specification)
CIFS_AV	100 ±0.5 sec	5.6
Contention-Free Interframe Spacing (CFIFS_AV)	30 sec min. to 140 sec max.	5.6

CTS-MPDU Gap (CMG)	120 ±0.5 sec	4.4.1.5.4.12
Max-MPDU Time for		
Default Maximum MSDU Size	1522 octets	7.8.1
Discovered_List_Expire_Time	3 to 5 minutes	7.6.1.2
EIFS_AV	2920.64 ±5.0 sec	5.6
Extended Interframe Space (EIFS)	1695.0 ±5.0 sec	9.2.2
FAIL_WAIT	1 sec FAIL_WAIT 5 sec	5.4.1.6.2
FHM_TimeOut	1 sec	9.3.2
FragMMI_ReassemblyTimeOut	1 sec	11.1.7
GI (Guard Interval)	5.56 sec, 7.56 sec, 47.12 sec	3.2.3
HP1_FC_Thresh	2	0
HP1_FC_Thresh_Interval	1 second	0
HP1D_ReportDuration	1 sec	9.3.1
IDLE_BEACON_SLOT_TIMEOUT	10 * Beacon Period	8.3.9
LBDAT_EXPIRE_TIME	100 sec	5.3.1
LinkStatusTimeout	MaxDiscoverPeriod	5.2.7
MaxBeaconSlot	8	8.2
MAX_BIR_TIME	100 sec	5.3.1
Max_Missed_Beacon	2	7.9.2
MaxFL_AV	2501.12 sec ≤ MaxFL_AV ≤ 5241.6 sec	11.5.10.1
Maximum Beacon scan time (MaxScanTime)	4 sec	7.1
Maximum CCo Beacon Scan Time (MaxCCoScanTime)	2 sec	7.1
Maximum Discover Period (MaxDiscoverPeriod)	10 seconds	7.6.1.4
MaxNoBeacon	≥10	8.5.4
Max_Reassembly_Timer (for Connectionless traffic)	5 ms Max_TX_Timer 1 s	5.4.1.6.2
Max_TEK_Lifetime	120 seconds	7.10.2.6
MAX_TONE_MAPS	7	5.2.6.1.1
MMEResponse_WaitTime	2 seconds	5.3.1

Max_TX_Timer (for Connectionless traffic)	5 ms Max_TX_Timer 1 s	5.4.1.6.1
MIN_BIR_TIME	100 ms	5.3.1
MinCSMARegion	1500 sec	5.1
Minimum Beacon scan time (MinScanTime)	2 sec	7.1
Minimum CCo Beacon Scan time (MinCCoScanTime)	1 sec	7.1
Priority Resolution Slot (PRS)	35.84 ±0.5 sec	1.1 (HomePlug 1.0.1 specification)
RBAT_EXPIRE_TIME	≥ 100 sec	5.3.2
RIFS_AV	30 sec to 160 sec	5.6
RIFS_AV_default	140 ±0.5 sec	5.6
RIFS_hp1	26.0 ±0.5 sec	1.1 (HomePlug 1.0.1 specification)
RTS/CTS Gap (RCG)	120 ±0.5 sec	4.4.1.5.4.12
SHM_TimeOut	≥ 1 sec	9.3.2
Slot Time	35.84 ±0.5 sec	1.1 (HomePlug 1.0.1 specification)
Unassociated STA Advertisement Interval (USAI)	1 sec	7.1

Table 23: HomePlug GREEN PHY parameters differing from HomePlug AV 1.1

Parameter	Value	Section Reference
MAX_TONE_MAPS	0	5.2.6.1.1.3
Max_Route_Update_Time	30 minutes	5.10.1.1
Min_Route_Update_Time	5 minutes	5.10.1.1
RDR_Significant_Change	10 percent	5.10.1.1

PHY Specification

Overview of HomePlug GREEN PHY

The HomePlug GREEN PHY (GP) physical layer is the same as HomePlug AV physical layer with the exception that all required communications (including the AV Payload encoding) is limited

to the three ROBO-AV modes (i.e., MINI-ROBO_AV, STD-ROBO_AV and HS-ROBO_AV). Therefore, carriers are coherently modulated only with Quadrature Phase Shift Keying (QPSK). BPSK, 8-QAM, 16-QAM, 64-QAM, 256-QAM, and 1024-QAM are not required to be supported by GP. Furthermore, only rate ½ Turbo Convolutional Coding is required for GP (i.e., rate 16/21 is not required to be supported by GP).

Figure 3-1 shows a block diagram representation for the physical layer of the HomePlug GREEN PHY transmitter and receiver as based upon HomePlug AV. Note that references to HomePlug AV are retained in order to emphasize that GREEN PHY is a simplified derivative (or profile) of HomePlug AV . The transceiver block diagram is based on a 75 MHz clock frequency.

On the transmitter side, the PHY layer receives its inputs from the Media Access Control (MAC) layer. Three separate processing chains are shown because of the different encoding for HomePlug 1.0.1 Frame Control (FC) data, HomePlug AV Frame Control data, and HomePlug AV Payload data. AV Frame Control data is processed by the AV Frame Control Encoder, which has a Turbo Convolutional Encoder and Frame Control Diversity Copier while the HomePlug AV payload data stream passes through a Scrambler, a ½ rate Turbo Convolutional Encoder, channel interleaver and ROBO Interleaver. The HomePlug 1.0.1 Frame Control data passes through a separate HomePlug 1.0.1 Frame Control Encoder. The outputs of the three FEC Encoders lead into a common OFDM Modulation structure, consisting of a Mapper, Inverse Fast Fourier Transform (IFFT) processor, Preamble, and Cyclic prefix insertion, and symbol Window and Overlap block, which eventually feeds the Analog Front End (AFE) module that couples the signal to the power line medium.

Figure 31: HomePlug AV OFDM Transceiver for GREEN PHY

At the receiver, an AFE operates with an Automatic Gain Controller (AGC) and a time-synchronization module to feed separate Frame Control and Payload data recovery circuits. The Frame Control data is recovered by processing the received sample stream through a 384-point FFT (for HomePlug 1.0.1 delimiters) and a 3072-point FFT (for HomePlug AV), and through separate Frame Control Decoders for the HomePlug AV and HomePlug 1.0.1 Modes. The payload portion of the sampled time domain waveform, which contains only HomePlug AV formatted symbols, is processed through a 3072-point FFT, a Demodulator, ROBO de-interleaver and channel de-interleaver followed by a ½ rate Turbo Convolutional Decoder and a De-scrambler to recover the AV Payload data.

PPDU Structure and Generation

PPDU Formats

The term “PHY Protocol Data Unit” (PPDU) refers to the physical entity that is transmitted over the power line. PPDUs are generated by the PHY for transmission on the power line at the PHY interface.

As with HomePlug AV, the HomePlug GREEN PHY specification supports four PPDU formats as shown in Table 31 and specified in Section 3.2.1.1, that match the corresponding MAC Protocol Data Unit (MPDU) formats defined in Section 4.4. The HPAV FC and HP1.0.1 FC (when present) are used by the MAC for management purposes (see Chapter 4). The HPAV FC, the HP1.0.1 FC (when present) and the PPDU payload (when present) result from the mapping of the corresponding MPDU bits, as described in this chapter

Table 31: PPDU Formats

PPDU Format	Preamble Type	HP1.0.1 Frame Control (FC)	HPAV Frame Control (FC)	Payload
AV-only Long PPDU	HPAV	No	Yes	Yes
Hybrid Long PPDU	Hybrid	Yes	Yes	Yes
AV-only Short PPDU	HPAV	No	Yes	No
Hybrid Short PPDU	Hybrid	Yes	Yes	No

The AV Frame Control can be transmitted using either a single OFDM Symbol or two OFDM Symbols (refer to Section 3.2.3.1). When the Tone Mask defined in Section 3.6.7 is used, a single OFDM symbol shall be used to transmit the FC. The ability to transmit and receive the AV Frame Control using two OFDM Symbols is optional. The two symbol AV Frame Control is intended for use in networks where a large number of HomePlug carriers are masked. Such conditions may occur either due to regulatory constraints or due to the use of a Frequency Division Coexistence mechanism (refer to Section 10.5). However, each Tone Mask defined for AV operation must also specify the number of OFDM symbols used in transmitting the FC when the mask is employed. As with HomePlug AV, the mechanism to determine when two Frame Control symbols are to be used in the network is beyond the scope of this HomePlug GREEN PHY specification.

The PPDU payload shall be created using one of the following formats:

One or more 520-octet FEC blocks modulated using negotiated Tone Maps (TMs) (not required for GREEN PHY)

One 520-octet FEC block modulated using Standard ROBO Modulation

One, two, or three 520-octet FEC blocks using High-Speed ROBO Modulation

One 136-octet FEC Block modulated using negotiated TMs (not required for GREEN PHY)

One 136-octet FEC block modulated using Mini-ROBO Modulation

PPDU Formats for GREEN PHY

A station that only implements GREEN PHY shall follow the requirements described in section 3.2.1 with the following exceptions:

The PPDU payload shall be created using one of only the following formats:

One 520-octet FEC block modulated using Standard ROBO Modulation

One, two, or three 520-octet FEC blocks using High-Speed ROBO Modulation

One 136-octet FEC block modulated using Mini-ROBO Modulation

Negotiated Tone Maps (TMs) are not required for a station that implements only GREEN PHY.

PPDU Structure

There are two types of PPDU structures, depending on whether the PHY is operating in HomePlug 1.0.1-compatible Mode or AV-Only Mode. In the following paragraphs, these modes are referred to as Hybrid and AV Mode, respectively.

As with HomePlug AV, when the GREEN PHY operates in Hybrid Mode, the PPDU structure

consists of a HomePlug 1.0.1-compatible Preamble followed by a 1.0.1-compatible FC, AV FC (one or two OFDM Symbols), and optionally a PPDU payload, as shown in Figure 3-2 and Figure 3-3. When the PHY operates in AV Mode, the PPDU structure consists of an AV Preamble, an AV FC (one or two OFDM Symbols), and optionally a PPDU payload, as shown in Figure 3-4 and Figure 3-5. The combination of a Preamble, HomePlug 1.0.1 Frame Control (if any), and HomePlug AV Frame Control is referred to as a "Delimiter" throughout this specification.

For both Hybrid and AV Modes, the first and second payload symbols (D1 and D2) have a fixed guard interval of 567 samples. Starting with the third payload symbol (D3), one of the three generic GIs listed in Figure 36: OFDM Symbol Timing
Table 32 shall be used for the remainder of the PPDU. A receiver shall use the guard interval length associated with the Tone Map used for the PPDU (determined by decoding the AV_FC).

Figure 32: Hybrid Mode PPDU Structure – Single Symbol AV FC

Figure 33: Hybrid Mode PPDU Structure – Two Symbol AV FC

Figure 34: AV Mode PPDU Structure – Single Symbol AV FC

Figure 35: AV Mode PPDU Structure - Two Symbol AV FC

The payload symbols consist of a 3072-sample OFDM Symbol that is preceded by a cyclic prefix. The length of the guard interval for payload symbol(s) following the second one (D3 to the end of the PPDU) is fixed for the duration of the PPDU. Different values may be chosen, either on a per-Link basis or for different portions of the AC line cycle for a single Link, to optimize throughput as part of the channel estimation process (refer to Section 5.2.6). The different sizes supported for the guard interval are shown in Figure 36: OFDM Symbol Timing
Table 32.

Symbol Timing

The OFDM time domain signal, based on a 75 MHz sampling clock, is determined as follows. For Frame Control and Payload Symbols, a set of data points from the mapping block (refer to Section 3.5) is modulated onto the subcarrier waveforms using a 3072-point IFFT, resulting in 3072 time samples (IFFT interval). A fixed number of samples from the end of the IFFT are taken and inserted as a cyclic prefix at the front of the IFFT interval to create an extended OFDM Symbol. Figure 3-6 shows the OFDM Symbol timing, with specifics identified in Figure 36: OFDM Symbol Timing
.

Figure 36: OFDM Symbol Timing

Table 32: OFDM Symbol Characteristics

Symbol	Description	Time Samples	Time(Microseconds)
T	IFFT Interval	3072	40.96
t_{prefix}	Cyclic Prefix Interval	RI+GI	4.96+GI

T_E	Extended Symbol Interval ($T + t_{prefix}$)	$T+t_{prefix}$	45.92+GI
RI	Rolloff Interval	372	4.96
T_S	Symbol Period	3072+GI	40.96+GI
GI_{FC}	Frame Control Guard Interval	1374	18.32
GI	Payload Symbol Guard Interval, generically	417, 567, 3534	5.56, 7.56, 47.12
GI_{SR}	STD-ROBO_AV Payload Symbol(s) Guard Interval	417	5.56
GI_{HR}	HS-ROBO_AV Payload Symbol(s) Guard Interval	417	5.56
GI_{MR}	MINI-ROBO_AV Payload Symbol(s) Guard Interval	567	7.56
GI_{417}	Guard Interval, length = 417 samples Not required for GREEN PHY	417	5.56
GI_{567}	Guard Interval, length = 567 samples Not required for GREEN PHY	567	7.56
GI_{3534}	Guard Interval, length = 3534 samples Not required for GREEN PHY	3534	47.12

Guard Interval Timing for GREEN PHY

As noted in Table 3-2, a station that only implements GREEN PHY shall follow the requirements as described in section 3.2.3 with the following exceptions: Guard Intervals GI417, GI567, and GI3534 (see Table 3-2 “OFDM Symbol Characteristics”) are not required.

Frame Control Forward Error Correction

As with HomePlug AV, the Frame Control field in HomePlug GREEN PHY consists of 128 information bits. These bits are encoded and coherently QPSK modulated over one or two OFDM Symbols. To obtain a high reliability in the demodulation of the control bits, a frequency-diversity mode is implemented. The use of two symbols for Frame Control is optional, as it is intended to increase Frame Control robustness in cases where the available bandwidth is much smaller than that in the mask of Section 3.7.1 (refer to Section 3.2.1).

Figure 3-7 shows the FEC processing for the 128 Frame Control bits. The Frame Control FEC consists of a Turbo Convolutional Encoder that encodes 128 Frame Control bits into 256 coded bits, a Frame Control Interleaver, and a Diversity Copier that redundantly maps the 256 interleaved bits onto one or two OFDM Symbols.

Figure 37: Frame Control FEC Encoder

Turbo Convolutional Code Encoder

The Turbo Convolutional Code (TCC) Encoder is described in Section 0. The encoder is operated in rate ½ mode such that the 128 information bits produce 256 coded bits.

Frame Control Interleaver

The Frame Control Interleaver serves to randomize the TCC Encoder output bits before being copied multiple times and transmitted on the channel. The Interleaver is the 16-octet, rate 1/2 case described in Section 3.4.3.

Diversity Copier

The Diversity Copier replicates the 256 interleaved bits for QPSK mapping onto the used (non-masked) carriers. Because the bits have already been interleaved, the Diversity Copier needs only to maximally spread the bit copies. For the single FC symbol case, this is achieved by transmitting the copies of the interleaved bits consecutively (with wrapping), with an address offset of 128 between the in-phase (I) and quadrature (Q) channels. Table 33 defines this ordering, where the variable NumCarriers refers to the total number of non-masked carriers. For the standard 917 carriers and one FC OFDM Symbol, each bit is copied at least 7 times, and some bits are copied eight times.

Table 33: Diversity Copier Bit Ordering– Single Symbol Case

Used Carrier #	I-Channel Interleaved Bit Address	Q-Channel Interleaved Bit Address
0	0	128
1	1	129
2	2	130
…	…	…
c	c mod 256	(c+128) mod 256
…	…	…
NumCarriers-1	(NumCarriers-1) mod 256	((NumCarriers-1)+128) mod 256

When transmitting two FC OFDM Symbols, the I and Q bit addresses for the first symbol are the same as defined by Table 33. The addresses for the I and Q of the second symbol are equal to the first symbol's addresses plus an additional offset of 64, as in Table 34. In both tables, the variable **c** represents an index to the c^{th} non-masked carrier and the variable NumCarriers represents the total number of non-masked carriers.

Table 34: Diversity Copier Bit Ordering - Two Symbol Case

Used Carrier #	I-Channel Interleaved Bit Address Symbol 1	Q-Channel Interleaved Bit Address Symbol 1	I-Channel Interleaved Bit Address Symbol 2	Q-Channel Interleaved Bit Address Symbol 2
0	0	128	64	192
1	1	129	65	193
2	2	130	66	194
…	…	…	…	…
c	c mod 256	(c+128) mod 256	(c+64) mod 256	(c+192) mod 256
…	…	…	…	…
NumCarriers-1	(NumCarriers-1) mod 256	((NumCarriers-1) +128) mod 256	((NumCarriers-1) +64) mod 256	((NumCarriers-1) +192) mod 256

Payload Forward Error Correction (FEC) Processing

The Payload Forward Error Correction (Payload FEC) Encoder shall consist of a Scrambler, a Turbo Convolutional Encoder, and a Channel Interleaver (CI). When ROBO mode is used, the Channel Interleaver is followed by a ROBO Interleaver. The Payload FEC block operates on groups of octets called Physical Blocks (PBs) that are either 520-or 136-octets long (denoted as PB520 and PB136, respectively). Chapter 5 describes the generation of PBs. The Turbo Encoder shall operate in either rate 1/2 or rate 16/21 for PBs in Links that use TMs (refer to Chapter 5 for a definition of TMs). When transmitting a ROBO-AV PB, only ½ FEC rate shall be used. The following subsections describe each block of the Payload FEC Block diagram in Figure 3-8.

Figure 38: Payload FEC Encoder Block Diagram

Scrambler

The data scrambler block helps give the data a random distribution. The data stream shall be "XOR-ed" with a repeating Pseudo Noise (PN) sequence using the following generator polynomial (see Figure 3-9):

The bits in the scrambler shall be initialized to all ones at the start of processing each MPDU.

Figure 39: Data Scrambler

Turbo Convolutional Encoder

Data from the scrambler shall be encoded by a Turbo Convolutional Encoder (see Figure 3-10). Two rate 2/3 Recursive Systematic Convolutional (RSC) constituent codes and one Turbo Interleaver are used. Both Encoder 1 and Encoder 2 have 8-states. The Turbo code FEC block supports sizes of 520, 136, and 16 octets (referred to as PB520, PB136, and PB16, respectively). After puncturing, the code rate is either ½ or 16/21.

Figure 310: Turbo Encoder Block Diagram

Turbo Convolutional Encoder for GREEN PHY

A station implementing only GREEN PHY shall follow the requirements described in section 3.4.2 with the exceptions of:

- passing outputs **p** and **q** to the puncture circuit (since puncturing is not supported. This is illustrated in Figure 3-10b)
- code rate 16/21 (only code rate ½ is required for GREEN PHY)

Figure 310b: Turbo Encoder Block Diagram (GREEN PHY)

Constituent Encoders

Figure 3-11 shows the 8-state encoder used for Encoder 1 and Encoder 2.

The first bit of the PB is mapped to u1, the second to u2, and so on. Only output x0 is passed to the puncture circuit.

Figure 311: 8-State Constituent Encoder

Constituent Encoders for GREEN PHY

A station implementing only GREEN PHY shall follow the requirements described in section 3.4.2.2 with the exception of passing output x0 to the puncture circuit (since puncturing is not supported, as illustrated in Figure 3-10b).

Termination

Tail-bitten termination is used in each constituent encoder. Two passes of each encoder are required. First the encoder is initialized to the all-zeros state S_0 = [s1 s2 s3]= [0 0 0], and then the entire FEC block is passed through the encoder (the outputs are unused). The final state S_N is used to determine the starting state for the second pass (i.e., $S'_0 = f[S_N]$, where the prime (′) indicates states of the second pass). The function f[.] is chosen so the final state S'_N will equal the initial state S'_0 at the conclusion of the second pass. The entire FEC block is passed through the encoder a second time, this time outputting to the puncture circuit (note that the puncture circuit is not required for a station that only implements GREEN PHY).

Informative Text

The initial state of the second-pass S'_0, can be obtained from the final state of the first-pass S_N through the following equation:

where the state S is a 1x3 row vector with components as in the diagram of Figure 3.11, and the matrix M equals:

for the case of PB520 and PB16, and equals:

Informative Text
The initial state of the second-pass S'_0, can be obtained from the final state of the first-pass S_N through the following equation:

where the state S is a 1x3 row vector with components as in the diagram of Figure 3.11, and the matrix M equals:

for the case of PB520 and PB16, and equals:

for the case of PB136.

Puncturing

The u1, u2 systematic bits are never punctured. They are written to the data output buffer in natural order.

The p and q parity bits from Encoder 1 and Encoder 2, respectively, are punctured and written to the parity output buffer in natural order.

Table 35 shows the puncture pattern for rate ½ (i.e., no puncturing).

Table 35: Rate ½ Puncture Pattern

p	1111111111111111
q	1111111111111111

Table 36 shows the puncture pattern for rate 16/21.

Table 36: Rate 16/21 Puncture Pattern

p	1001001001001000
q	1001001001001000

Puncturing for GREEN PHY

A station that only implements GREEN PHY is not required to support puncturing.

Turbo Interleaving

A Turbo Interleaver is required to interleave the original sequence for the second constituent code, as shown in Figure 3-10. The Turbo Interleaver interleaves the PB in dibits, not bits, thus keeping the original bit pairs together. As a result, the Interleaver length (that is, the length of the Interleaver input and output sequences) equals the FEC dibit block size. The Turbo Interleaver output may be generated algorithmically, although a seed table is required for each FEC block size supported. Table 37 lists the parameters used for each FEC block size, with the corresponding seed tables provided in Table 38, Table 39, and Table 310. It is the seed table S, the corresponding seed table length N, and the interleaver length L that specify each interleaver mapping I( ).

Table 37: Interleaver Parameters

PB Size (Octets)	N Value	M Value	Interleaver Length L
16	8	8	64
136	34	16	544

520	40	52	2080

The Turbo Interleaver mapping is defined through the following interleaver equation:

$I(x) = [S(x \bmod N) - (x \mathit{div} N)*N + L] \mathit{mod} L$ for $x = 0, 1, \ldots, (L-1)$
where *div* is an integer division operation and *mod* is the modulo operation.
The interleaver mapping I(x) is then used to interleave the bits as shown below.
Note: When the output index x is even, the corresponding interleaved information bit pairs (bit 0 and bit 1 of the pair) are swapped.

where Data and IntData refer to the pre- and post-interleaver bit sequences respectively.

Table 38: Interleaver Seed Table for FEC Block Size of 16 Octets

x	0	1	2	3	4	5	6	7
S(x)	54	23	61	12	35	2	40	25

Table 39: Interleaver Seed Table for FEC Block Size of 136 Octets

x	0	1	2	3	4	5	6	7
S(x)	369	235	338	436	169	200	397	59
x	8	9	10	11	12	13	14	15
S(x)	298	20	265	429	294	466	16	48
x	16	17	18	19	20	21	22	23
S(x)	525	461	187	86	216	387	41	142
x	24	25	26	27	28	29	30	31
S(x)	247	314	79	486	512	103	476	345
x	32	33						
S(x)	4	105						

Table 310: Interleaver Seed Table for FEC Block Size of 520 Octets

x	0	1	2	3	4	5	6	7
S(x)	1558	1239	315	1114	437	956	871	790
x	8	9	10	11	12	13	14	15
S(x)	833	1152	147	506	589	388	1584	265
x	16	17	18	19	20	21	22	23
S(x)	981	220	1183	102	1258	1019	1296	737
x	24	25	26	27	28	29	30	31
S(x)	694	1495	612	453	1049	1450	531	47
x	32	33	34	35	36	37	38	39
S(x)	1368	645	166	322	1323	1404	0	881

Channel Interleaver

The natural bit order at the encoder output starts with all the data bits in the same order as at the input to the encoder, followed by all the parity bits in the same order as generated by the encoder. The two parity bits generated by the encoder (p and q from Figure 3-10) are interlaced, with the p

bit coming first. An entire turbo code PB is interleaved by the Channel Interleaver prior to mapping.

Informative Text
The interleaver and de-interleaver buffers are organized as Rx4 matrices (R varies depending on block size) to facilitate parallel turbo decoding by as many as four decoder engines. The following scheme allows simultaneous reads from the four sub-banks of the de-interleaver buffer to the input buffers of the turbo decoders.

In the following example, k represents the number of information bits and (n-k) represents the number of parity bits. The information bits are divided into four equal sub-blocks of k/4 bits, and the parity bits are divided into four equal sub-blocks of (n-k)/4 bits. For both PB520 and PB136, for both code rates (1/2 and 16/21), and for the FC case, the number of both information bits and parity bits is divisible by 4. In the encoder, the output buffer is split into four information sub-banks of k/4 bits and four parity sub-banks of (n-k)/4 bits. The encoder writes the first k/4 information bits (in natural order) to the first information sub-bank, the next k/4 bits to the second information sub-bank, and so on. Then it writes the first (n-k)/4 parity bits (in natural order) to the first parity sub-bank, the next (n-k)/4 bits to the second parity sub-bank, and so on.

Each of the information sub-blocks is interleaved in an identical manner by the nature in which the bits are read out of the sub-banks. The four information sub-banks of length k/4 may be thought of as one matrix consisting of k/4 rows and four columns, with column 0 representing the first sub-bank, column 1 representing the second sub-bank, and so on. Groups of four bits on the same row (one bit from each sub-block) are read out from the matrix at a time, starting with row 0. After a row has been read out, the row pointer is incremented by StepSize before performing the next row read (0, StepSize, 2* StepSize, …, [k/4]- StepSize). After (k/4)/ StepSize row reads, the end of the matrix has been reached. The row pointer is then initialized to 1 (rather than starting at 0 the previous time) and the process is repeated – reading rows, incrementing the row pointer by StepSize, and incrementing the starting row by 1 after (k/4)/StepSize row reads. For example the second pass will read rows (1, 1+StepSize, 1+2*StepSize , …, [k/4]-StepSize+1) and the third pass will read rows (2, 2+StepSize, 2+2*StepSize , …, [k/4]-StepSize+2). As a result, StepSize passes of (k/4)/StepSize row reads are required to read all bits from the matrix.

The parity bits for rate ½ are interleaved in a similar manner to the information sub-blocks. However instead of reading out of the ([n-k]/4)x4 parity matrix starting with row 0, the parity reads begin at a predetermined offset and wrap around when the end of the matrix is reached until arriving back at the starting row. Let t represent the sub-bank length for the parity subbanks, t = [n-k]/4. The first rows that are read are (offset, (offset+ StepSize) mod t, …, [(offset+t-StepSize) mod t]). Then the starting row pointer is incremented by 1 and the process is repeated StepSize-1 more times for a total of StepSize passes of ((n-k)/4)/StepSize row reads, thus reading rows (offset+1, (offset+1+StepSize) mod t, … , [(offset+1+t-StepSize) mod t]) during the second pass, for example.

The parity bits for rate 16/21 are interleaved in a similar manner to the rate ½ parity. The reading out of the parity matrix starts with an offset and wraps, as for rate ½ parity, except the row pointer is not re-initialized for each of the successive StepSize-1 passes. Again, let t represent the sub-bank

length for the parity subbanks, where t = [n-k]/4. After each row read, StepSize is added to the row pointer and a modulo-t is performed (offset, [offset+StepSize] mod t, [offset+2*StepSize] mod t, …). This process continues without row pointer re-initialization until all n-k parity bits have been read.

Table 311 lists the parity offsets used for each PB size and code rate combination.

Table 311: Channel Interleaver Parameters

PB Size	Code Rate	Offset (Parity)	StepSize
16 octets	1/2	16	4
520 octets	1/2	520	16
136 octets	1/2	136	16
520 octets Not required for GREEN PHY	16/21 Not required for GREEN PHY	170 Not required for GREEN PHY	16 Not required for GREEN PHY
136 octets Not required for GREEN PHY	16/21 Not required for GREEN PHY	40 Not required for GREEN PHY	8 Not required for GREEN PHY

Interleaved bits are read from each of the sub-banks in turn.

For rate 1/2, the first four bits to be transmitted on the channel are information bits, the next four bits are parity bits, and so on.

For rate 16/21, the first three 4-bit outputs are information bits, followed by four parity bits out. This is repeated for a total of 5 times (resulting in 20 x 4-bit outputs) before an extra information 4-bit read is output. This pattern repeats until all bits are transmitted.

In addition to the above process, sub-bank switching is performed to further interleave the bit-stream. The switching re-orders the 4-bit outputs, regardless of whether the nibble contains information or parity bits. Table 312 shows the switching, where b0, b1, b2, and b3 represent bit outputs from information or parity sub-bank 0, 1, 2, and 3 respectively. The leftmost bit in Table 312 is transmitted first (i.e., it has the smallest time index). The switched bit order changes after every two nibbles read, independent of whether the nibbles contained information, parity, or both.

Table 312: Sub-bank Switching

Output Nibble Number	Switched Bit Order
1 or 2	b0 b1 b2 b3
3 or 4	b1 b2 b3 b0
5 or 6	b2 b3 b0 b1
7 or 8	b3 b0 b1 b2
9 or 10	b0 b1 b2 b3

Channel Interleaver for GREEN PHY

A station that only implements GREEN PHY shall follow the requirements described in section 3.4.3 with the exception that code rate 16/21 (and associated Offset (Parity)) is not supported (as noted in Table 3-11 “Channel Interleaver Parameters”).

ROBO Modes

As with HomePlug AV, HomePlug Green PHY employs three robust modes of communication,

called ROBO Modes, for several purposes, including:
Beacon and data broadcast and multicast communication
Exchange of Management Messages
All ROBO Modes use QPSK modulation, along with a ½ rate Turbo Convolutional Code as described above. The ROBO Interleavers that follow the Channel Interleaver specified above introduce further redundancy by a factor that depends on the type of ROBO Mode (i.e., each FEC-coded bit is represented with multiple bits at the output of the ROBO Interleaver).
The ROBO Interleavers create redundancy by using the output of the CI of Section 3.4.3, and reading the output bits multiple times. Each readout may occur at a given cyclic shift. To ensure adequate frequency separation between the multiple copies of each bit, portions of the initial interleaved output are inserted between successive readouts of the Channel Interleaver output. The receiver may take advantage of the extra repetitions.

Table 313 shows the detailed interleaving scheme.

Table 313: ROBO Mode Parameters

ROBO Mode	Number of Copies (N_{copies})	PHY Rate (Default Tone Mask)	PB Block
STD-ROBO_AV	4	4.9226 Mbps	PB520
HS-ROBO_AV	2	9.8452 Mbps	PB520
MINI-ROBO_AV	5	3.7716 Mbps	PB136

The Standard ROBO Mode (STD-ROBO_AV) is the one normally used with PB520 PBs. The transmitter may use High-Speed ROBO Mode (HS-ROBO_AV) if it determines that reliable communication can be achieved with fewer number of copies and the higher rate achieved (twice as high as the one with STD-ROBO_AV) is desirable for efficient system operation. For example HS-ROBO_AV may be well suited for the multicast of media content to multiple stations in a network with very good channel characteristics between the transmitting station and the receiving stations. The Mini-ROBO Mode (MINI-ROBO_AV) is used with PB136. It has the highest number of copies, and it is used when a small payload needs high degree of reliability. The Beacon MPDU Payload is encoded using the MINI-ROBO_AV.

Note: The number of repetitions and PB size carried in each ROBO Mode is fixed. As a result the number of symbols needed to transmit a PPDU carrying a single PB as payload depends on the number of carriers in the active Tone Mask. If the number of carriers is below a certain number, the FL_AV parameter of a PPDU carrying a single PB520 in STD-ROBO_AV will exceed the MaxFL_AV that the transmitter and receiver are capable of supporting (refer to Section 4.4.1.5.2.13.1). The STD-ROBO_AV Mode shall not be used in such cases, and the other ROBO Modes shall be used instead.

Informative Text

The PHY Rates (Default Tone Mask) shown in Table 3-13 are approximations and are calculated as:

STD-ROBO_AV mode (916 carriers, QPSK modulation, TCC rate ½, 4 copies, GI 5.56 us):
916*2/2/4/(40.96e-6+5.56e-6) = 4.9226 Mbps

HS-ROBO_AV mode (916 carriers, QPK modulation, TCC rate ½, 2 copies, GI 5.56 us):
916*2/2/2/(40.96e-6+5.56e-6) = 9.8452 Mbps

MINI-ROBO_AV mode (915 carriers, QPSK modulation, TCC rate ½, 5 copies, GI 7.56 us):
915*2/2/5/(40.96e-6+7.56e-6) = 3.7716 Mbps

ROBO Interleaver
The definition of the ROBO Interleaver requires that the number of used carriers be a multiple of the number of ROBO copies. Thus, in step 5 of the following procedure, a special Tone Map is defined for ROBO that ensures a feasible number of carriers are modulated.

If denotes the sequence of bits at the output of the Channel Interleaver, the bit sequence at the output of the ROBO Interleaver is determined as follows. The notation means is the largest integer less than or equal to , and means is the smallest integer greater than or equal to .

- Define the following:

  number of bits per PHY Block (information and parity) at the output of the Channel Interleaver

  number of carriers turned on (in Tonemask)

  number of redundant copies of the data (see Table 313)

  number of bits per carrier (2 for QPSK)
- Determine the number of bits to pad:

-

Determine the cyclic shift:

-

Assign output of the ROBO Interleaver:

- Set ROBO Tonemap

  Set Tonemap to indicate that the first carriers are used with QPSK modulation, and that any remaining carriers () are encoded with BPSK using the Pseudo Noise generator defined in Section 3.5.

Mapping
The mapping function shall distinguish between Frame Control information, which is mapped into coherent QPSK only, and regular data, which generally is mapped into coherent Quadrature Amplitude Modulation (BPSK, QPSK, 8-QAM, 16-QAM, 64-QAM, 256-QAM, or 1024-QAM). Table 314 shows the modulation and bits per carrier for Frame Control and payload information. Except for ROBO-AV Mode, in which all unmasked carriers use QPSK modulation, a mixture of the modulations (also known as "bit-loading") may be used for different carriers in the mask when creating the OFDM payload symbol(s).
Table 314: Modulation Characteristics

Information Type	Bits per Carrier	Modulation Type	GREEN PHY requirement
Frame Control	2	Coherent QPSK	YES
ROBO_AV (STD-ROBO_AV, HS-ROBO_AV, MINI-ROBO_AV)	2	Coherent QPSK	YES
Data	1	Coherent BPSK	NO
	2	Coherent QPSK	NO
	3	Coherent 8-QAM	NO
	4	Coherent 16-QAM	NO
	6	Coherent 64-QAM	NO
	8	Coherent 256-QAM	NO
	10	Coherent 1024-QAM	NO

The mapping block shall also be responsible for assuring that the transmitted signal conforms to the given Tone Map and Tone Mask.
Tone Masks are defined system wide (for all transmitters) and specify which carriers are used by the system (refer to Section 3.6.7). Tone Masks are obeyed by the transmitter during the Priority Resolution Symbols, Preamble, Frame Control Symbols, and all types of data modulation. On the other hand, the Tone Map contains a list of Modulation Types for all unmasked carriers (or tones) that are to be used on a particular unicast communication Link between two stations. For example, carriers that are experiencing fades may be avoided, and no information may be transmitted on those carriers. The Tone Map is obeyed by the data modulation modes and ignored when

transmitting Frame Control, ROBO_AV, Preamble, and Priority Resolution Symbols. Figure 312: PN Generator
Table 315 shows the signaling types that obey or ignore the Tone Map/Tone Mask. Figure 312: PN Generator
Table 315 also shows the impact of the Amplitude Map (refer to Section 11.5.12) on the various signaling types.
Empty Tone Filling
When the Tone Map indicates that a particular carrier shall not be used for information transmission, the mapping function shall use coherent BPSK, modulated with a binary value from the PN sequence defined below. The PN sequence shall be generated using the following generator polynomial (see Figure 3-12):

The bits in the PN sequence generator shall all be initialized to all ones at the start of the first OFDM payload symbol of each PPDU. When a carrier is encountered that is non-masked and not used for information, the existing value in the X^1 register shall be used for coherent BPSK modulation and the sequence shall be advanced. The sequence shall be advanced only when used as described above.
Last Symbol Padding
In general, the bits out of the CI to be mapped on to OFDM Symbols will not exactly fill all carriers of the last symbol in the PPDU. The PN sequence above shall also be used (without re-initialization) to fill the last PPDU OFDM Symbol. For a bit-loaded PPDU, a variable number of bits will be used from the X^1 to X^{10} registers, beginning with X^1, depending on how many bits are required to produce a constellation symbol for each carrier's modulation type. Similar to the case of the empty tone filling, the sequence is only advanced after each time it is used (i.e., once per carrier, when that carrier did not have enough remaining CI bits to entirely fill one constellation symbol).

Informative Text
For example, if there are only two bits left at the output of the CI and the next carrier to be modulated is using QAM-256, the bits in registers X^1 through X^6 will be appended to the two remaining CI bits (with the X^1 bit first in time after the last CI bit) so the Mapper has the required 8 bits (X^6, X^5, X^4, X^3, X^2, X^1, CI^{end}, CI^{end-1}) to produce a QAM-256 constellation symbol. The sequence will then be advanced. As all CI bits have now been used, the bits for the remaining carriers in the last OFDM Symbol will be read from the X^1 to X^{10} registers to produce constellation symbols for their respective modulation types, advancing the sequence only once per carrier after reading the PN bits.

Figure 312: PN Generator
Table 315: Tone Mask Amplitude Map and Tone Map

Symbols	Tone Mask	Amplitude Map	Tone Map
PPDU payload: BPSK, QPSK, 8-QAM, 16-QAM, 64-QAM, 256-QAM, 1024-QAM	Comply	Comply	Comply
Frame Control, ROBO-AV, Preamble, Priority Resolution Symbol	Comply	Comply	Ignore (HPGP) Comply (HPAV)

Informative Text

Typical usage of the **Tone Mask** is to disable the use of certain carriers to avoid interference from or to other applications, such as amateur radio bands. The Tone Mask may be preconfigured in certain geographical regions based on regulatory constraints. Stations must use the same Tone Mask to coexist and interoperate.

The **Amplitude Map** may be used to decrease the transmit amplitude of each unmasked carrier, if desired, to meet constraints such as radiation limits for BPL access usage on external transmission wires. In this way, the same Tone Mask, but different Amplitude Maps, can be used on the external wiring (BPL Access) and in the internal building wiring (PLC LAN), while still supporting interoperability. The Amplitude Map may be preconfigured for a particular application or may be configured by an authorized STA. The Amplitude Map affects only the transmit amplitude, not the encoding type used on a particular carrier

The **Tone Map** contains a list of carriers (or tones) as well as the associated encoding to be used on a particular unicast communication Link between two stations.

Mapping Reference

The phase reference is used as the initial phase of the FC and payload symbol(s) (refer to Section 3.6). Table 316 defines the phase angle numbers for each of the 1155 carriers. The actual phase, , for each carrier is defined as the carrier's phase angle number multiplied by .

Table 316: Mapping Reference Phase Angle Numbers

3072-IFFT Carrier #	Phase Angle #	3072-IFFT Carrier #	Phase Angle #	3072-IFFT Carrier #	Phase Angle #	3072-IFFT Carrier #	Phase Angle #	3072-IFFT Carrier #	Phase Angle #	3072-IFFT Carrier #	Phase Angle #	3072-IFFT Carrier #	Phase Angle #
74	0	239	1	404	5	569	5	734	1	899	0	1064	2
75	7	240	7	405	3	570	2	735	4	900	2	1065	3
76	7	241	6	406	1	571	6	736	7	901	4	1066	4

77	7	242	5	407	6	572	3	737	3	902	6	1067	5
78	7	243	4	408	4	573	7	738	6	903	1	1068	6
79	7	244	3	409	2	574	4	739	2	904	3	1069	7
80	7	245	2	410	7	575	0	740	5	905	5	1070	0
81	7	246	0	411	5	576	5	741	0	906	7	1071	2
82	7	247	7	412	3	577	2	742	4	907	2	1072	3
83	7	248	6	413	0	578	6	743	7	908	4	1073	4
84	7	249	5	414	6	579	3	744	3	909	6	1074	5
85	7	250	4	415	4	580	7	745	6	910	0	1075	6
86	7	251	2	416	1	581	4	746	1	911	2	1076	7
87	7	252	1	417	7	582	0	747	5	912	5	1077	0
88	7	253	0	418	4	583	4	748	0	913	7	1078	1
89	7	254	7	419	2	584	1	749	3	914	1	1079	2
90	7	255	5	420	0	585	5	750	7	915	3	1080	3
91	6	256	4	421	5	586	2	751	2	916	5	1081	4
92	6	257	3	422	3	587	6	752	5	917	7	1082	5
93	6	258	2	423	0	588	3	753	0	918	2	1083	6
94	6	259	0	424	6	589	7	754	4	919	4	1084	7
95	6	260	7	425	4	590	4	755	7	920	6	1085	0
96	6	261	6	426	1	591	0	756	2	921	0	1086	1
97	6	262	4	427	7	592	4	757	6	922	2	1087	2
98	5	263	3	428	4	593	1	758	1	923	4	1088	3
99	5	264	2	429	2	594	5	759	4	924	6	1089	4
100	5	265	0	430	7	595	2	760	7	925	0	1090	5
101	5	266	7	431	5	596	6	761	3	926	3	1091	6
102	5	267	6	432	2	597	2	762	6	927	5	1092	7
103	4	268	4	433	0	598	7	763	1	928	7	1093	0
104	4	269	3	434	5	599	3	764	4	929	1	1094	1
105	4	270	2	435	3	600	7	765	7	930	3	1095	2
106	4	271	0	436	0	601	4	766	3	931	5	1096	3
107	4	272	7	437	6	602	0	767	6	932	7	1097	4
108	3	273	6	438	3	603	5	768	1	933	1	1098	5
109	3	274	4	439	1	604	1	769	4	934	3	1099	5
110	3	275	3	440	6	605	5	770	7	935	5	1100	6
111	3	276	1	441	4	606	1	771	3	936	7	1101	7
112	2	277	0	442	1	607	6	772	6	937	1	1102	0
113	2	278	7	443	7	608	2	773	1	938	3	1103	1
114	2	279	5	444	4	609	6	774	4	939	5	1104	2
115	2	280	4	445	2	610	3	775	7	940	7	1105	3
116	1	281	2	446	7	611	7	776	2	941	1	1106	4
117	1	282	1	447	4	612	3	777	6	942	3	1107	4
118	1	283	0	448	2	613	0	778	1	943	5	1108	5
119	0	284	6	449	7	614	4	779	4	944	7	1109	6
120	0	285	5	450	5	615	0	780	7	945	1	1110	7
121	0	286	3	451	2	616	4	781	2	946	3	1111	0
122	7	287	2	452	7	617	0	782	5	947	5	1112	0
123	7	288	0	453	5	618	5	783	0	948	7	1113	1
124	7	289	7	454	2	619	1	784	3	949	1	1114	2
125	6	290	5	455	7	620	5	785	6	950	3	1115	3
126	6	291	4	456	5	621	1	786	1	951	5	1116	4
127	6	292	2	457	2	622	6	787	4	952	7	1117	4
128	5	293	1	458	0	623	2	788	0	953	1	1118	5
129	5	294	7	459	5	624	6	789	3	954	3	1119	6
130	4	295	6	460	2	625	2	790	6	955	4	1120	7

131	4	296	4	461	7	626	6	791	1	956	6	1121	7
132	4	297	3	462	5	627	3	792	4	957	0	1122	0
133	3	298	1	463	2	628	7	793	7	958	2	1123	1
134	3	299	7	464	7	629	3	794	2	959	4	1124	2
135	2	300	6	465	5	630	7	795	5	960	6	1125	2
136	2	301	4	466	2	631	3	796	0	961	0	1126	3
137	2	302	3	467	7	632	7	797	3	962	2	1127	4
138	1	303	1	468	5	633	3	798	6	963	3	1128	5
139	1	304	0	469	2	634	0	799	1	964	5	1129	5
140	0	305	6	470	7	635	4	800	4	965	7	1130	6
141	0	306	4	471	4	636	0	801	7	966	1	1131	7
142	7	307	3	472	2	637	4	802	2	967	3	1132	7
143	7	308	1	473	7	638	0	803	4	968	4	1133	0
144	6	309	7	474	4	639	4	804	7	969	6	1134	1
145	6	310	6	475	1	640	0	805	2	970	0	1135	1
146	5	311	4	476	6	641	4	806	5	971	2	1136	2
147	5	312	3	477	4	642	0	807	0	972	4	1137	3
148	4	313	1	478	1	643	4	808	3	973	5	1138	3
149	4	314	7	479	6	644	0	809	6	974	7	1139	4
150	3	315	6	480	3	645	4	810	1	975	1	1140	4
151	3	316	4	481	0	646	0	811	4	976	3	1141	5
152	2	317	2	482	6	647	4	812	7	977	4	1142	6
153	2	318	0	483	3	648	0	813	2	978	6	1143	6
154	1	319	7	484	0	649	4	814	4	979	0	1144	7
155	0	320	5	485	5	650	0	815	7	980	2	1145	7
156	0	321	3	486	2	651	5	816	2	981	3	1146	0
157	7	322	2	487	7	652	0	817	5	982	5	1147	0
158	7	323	0	488	4	653	4	818	0	983	7	1148	1
159	6	324	6	489	2	654	0	819	3	984	0	1149	2
160	6	325	4	490	7	655	4	820	6	985	2	1150	2
161	5	326	3	491	4	656	0	821	0	986	4	1151	3
162	4	327	1	492	1	657	4	822	3	987	6	1152	3
163	4	328	7	493	6	658	0	823	6	988	7	1153	4
164	3	329	5	494	3	659	4	824	1	989	1	1154	4
165	3	330	4	495	0	660	0	825	4	990	3	1155	5
166	2	331	2	496	5	661	4	826	6	991	4	1156	5
167	1	332	0	497	2	662	0	827	1	992	6	1157	6
168	1	333	6	498	7	663	4	828	4	993	7	1158	6
169	0	334	4	499	4	664	0	829	7	994	1	1159	7
170	7	335	3	500	2	665	4	830	2	995	3	1160	7
171	7	336	1	501	7	666	0	831	4	996	4	1161	0
172	6	337	7	502	4	667	4	832	7	997	6	1162	0
173	5	338	5	503	1	668	0	833	2	998	0	1163	1
174	5	339	3	504	6	669	3	834	5	999	1	1164	1
175	4	340	2	505	3	670	7	835	7	1000	3	1165	2
176	3	341	0	506	0	671	3	836	2	1001	4	1166	2
177	2	342	6	507	5	672	7	837	5	1002	6	1167	2
178	2	343	4	508	2	673	3	838	7	1003	7	1168	3
179	1	344	2	509	7	674	7	839	2	1004	1	1169	3
180	0	345	0	510	4	675	3	840	5	1005	3	1170	4
181	7	346	6	511	1	676	6	841	7	1006	4	1171	4
182	7	347	4	512	6	677	2	842	2	1007	6	1172	4
183	6	348	3	513	3	678	6	843	5	1008	7	1173	5
184	5	349	1	514	0	679	2	844	0	1009	1	1174	5

185	4	350	7	515	4	680	6	845	2	1010	2	1175	6
186	4	351	5	516	1	681	1	846	5	1011	4	1176	6
187	3	352	3	517	6	682	5	847	7	1012	5	1177	6
188	2	353	1	518	3	683	1	848	2	1013	7	1178	7
189	1	354	7	519	0	684	5	849	5	1014	0	1179	7
190	0	355	5	520	5	685	0	850	7	1015	2	1180	7
191	0	356	3	521	2	686	4	851	2	1016	3	1181	0
192	7	357	1	522	7	687	0	852	5	1017	5	1182	0
193	6	358	7	523	4	688	4	853	7	1018	6	1183	0
194	5	359	5	524	1	689	0	854	2	1019	0	1184	1
195	4	360	3	525	6	690	3	855	4	1020	1	1185	1
196	4	361	1	526	2	691	7	856	7	1021	2	1186	1
197	3	362	7	527	7	692	3	857	2	1022	4	1187	2
198	2	363	5	528	4	693	6	858	4	1023	5	1188	2
199	1	364	3	529	1	694	2	859	7	1024	7	1189	2
200	0	365	1	530	6	695	6	860	1	1025	0	1190	2
201	7	366	7	531	3	696	1	861	4	1026	1	1191	3
202	6	367	5	532	7	697	5	862	6	1027	3	1192	3
203	5	368	3	533	4	698	1	863	1	1028	4	1193	3
204	5	369	1	534	1	699	5	864	3	1029	6	1194	3
205	4	370	7	535	6	700	0	865	6	1030	7	1195	4
206	3	371	5	536	3	701	4	866	0	1031	0	1196	4
207	2	372	3	537	7	702	7	867	3	1032	2	1197	4
208	1	373	1	538	4	703	3	868	5	1033	3	1198	4
209	0	374	7	539	1	704	7	869	0	1034	4	1199	4
210	7	375	5	540	6	705	2	870	2	1035	6	1200	5
211	6	376	3	541	3	706	6	871	5	1036	7	1201	5
212	5	377	0	542	7	707	2	872	7	1037	0	1202	5
213	4	378	6	543	4	708	5	873	2	1038	2	1203	5
214	3	379	4	544	1	709	1	874	4	1039	3	1204	5
215	2	380	2	545	6	710	4	875	7	1040	4	1205	6
216	1	381	0	546	2	711	0	876	1	1041	6	1206	6
217	0	382	6	547	7	712	4	877	4	1042	7	1207	6
218	7	383	4	548	4	713	7	878	6	1043	0	1208	6
219	6	384	2	549	0	714	3	879	0	1044	2	1209	6
220	5	385	7	550	5	715	6	880	3	1045	3	1210	6
221	4	386	5	551	2	716	2	881	5	1046	4	1211	6
222	3	387	3	552	7	717	5	882	0	1047	5	1212	7
223	2	388	1	553	3	718	1	883	2	1048	7	1213	7
224	1	389	7	554	0	719	4	884	4	1049	0	1214	7
225	0	390	5	555	5	720	0	885	7	1050	1	1215	7
226	7	391	2	556	1	721	4	886	1	1051	2	1216	7
227	6	392	0	557	6	722	7	887	4	1052	4	1217	7
228	5	393	6	558	3	723	3	888	6	1053	5	1218	7
229	4	394	4	559	7	724	6	889	0	1054	6	1219	7
230	3	395	2	560	4	725	2	890	3	1055	7	1220	7
231	2	396	7	561	0	726	5	891	5	1056	0	1221	7
232	0	397	5	562	5	727	0	892	7	1057	2	1222	7
233	7	398	3	563	2	728	4	893	2	1058	3	1223	7
234	6	399	1	564	6	729	7	894	4	1059	4	1224	7
235	5	400	6	565	3	730	3	895	6	1060	5	1225	7
236	4	401	4	566	7	731	6	896	1	1061	6	1226	7
237	3	402	2	567	4	732	2	897	3	1062	7	1227	7
238	2	403	0	568	1	733	5	898	5	1063	1	1228	7

Informative Text

The phase reference may also be described in equation form as shown below. This form is described here as informative text due to possible differences in round off and varying interpretations of the floor() and mod() functions.

First, create the floating-point phase reference, $_{FLT}$, as

where:

.

is then created by quantizing $_{FLT}$ as follows:

for 74 ≤ c ≤ 1227

for c = 1228

In the above equation, indices 74 and 1228 correspond to 1.8 MHz and 30 MHz, respectively. As with HomePlug AV, these values are the minimum and maximum frequencies that the HomePlug GREEN PHY system can use.

One characteristic of OFDM is that it is possible for the time domain waveforms to have large instantaneous excursions above the average symbol power when a number of carriers end up transmitting the same phase during a particular OFDM Symbol. The phase reference is therefore used to introduce a phase shift between carriers to minimize the probability that many end up transmitting the same phase, minimizing the Peak-to-Average Power Ratio (PAPR). While any phase reference that introduces such shifts will work, the above reference was chosen because it produces a low PAPR symbol (frequency sweep or "chirp") if passed through the IFFT un-modulated.

Because a specific reference symbol is never transmitted through the channel, the receiver must estimate the attenuation and phase shift caused by the channel for each carrier from the Preamble and the FC. A partial channel reference for the FC (for those carriers that are in the Preamble) can be derived by using one or more of the Preamble SYNCP AV symbols as channel-reference symbols. Interpolation can then be performed to estimate attenuation and phase shift for the missing carriers in between.

The channel reference for the payload symbol(s) can be determined from the Frame Control symbol as follows. After demodulation and decoding of the Frame Control, the information bits are put back through the Frame Control FEC Encoder to determine which QPSK phases were actually transmitted during the Frame Control symbol. These phases are then subtracted from the received Frame Control phases essentially yielding a channel reference for the subsequent payload symbol(s).

Mapping for Frame Control Coherent QPSK

Mapped Value	1024-QAM $(x_9x_8x_7x_6x_5x_4x_3x_2x_1x_0)$

The $2*N_{Carriers}*N_{Symbols}$ bits of data from the Diversity Copier shall be mapped into coherent QPSK, where $N_{Carriers}$ is the number of non-masked carriers and $N_{symbols}$ is the number of FC OFDM Symbols. The mapping function for Frame Control shall obey the Tone Mask.

Mapping for BPSK, QPSK, 8-QAM, 16-QAM, 64-QAM, 256-QAM, 1024-QAM

Data bits shall be mapped for coherent QAM modulation. Mapping is performed on both the I and Q channels in the following way.

- The Mapper takes 1, 2, 3, 4, 6, 8, or 10 bits, depending on the constellation of the current symbol and maps them into the I and Q values of a symbol. Table 317 shows how the bits are mapped to a symbol. In all cases, the LSB x_0 has the earliest time index.

Note: BPSK has nothing transmitted in the Q channel.

- These bits are then mapped to the values in Table 318 and Table 319, resulting in I and Q values for each symbol.
- The symbols are scaled to produce a unity average power symbol. The I and Q values are multiplied by the power scale value in Table 320.

The mapping function for QAM modulation shall obey the Tone Mask; that is:

Carriers that are masked (refer to Section 3.6.7) are not assigned I and Q constellation symbols and The amplitude is set to zero.

Additionally all non-ROBO-AV PPDU payload mapping shall obey the Tone Map of a given Link (refer to Section 5.2.1 and Section 5.2.5).

Table 317: Bit Mapping

Modulation Scheme	Bits from Channel Interleaver	I Channel	Q Channel	GREEN PHY requirement
BPSK	x0	x0	---	NO
QPSK	x1x0	x0	x1	YES
8-QAM	x2x1x0	x1x0	x2	NO
16-QAM	x3x2x1x0	x1x0	x3x2	NO
64-QAM	x5x4x3x2x1x0	x2x1x0	x5x4x3	NO
256-QAM	x7x6x5x4x3x2x1x0	x3x2x1x0	x7x6x5x4	NO
1024-QAM	x9x8x7x6x5x4x3x2x1x0	x4x3x2x1x0	x9x8x7x6x5	NO

Table 318: Symbol Mapping (Except 8-QAM)

GREEN PHY requirement	NO	NO	NO	NO	YES	NO

Mapped Value	1024-QAM ($x_4x_3x_2x_1x_0$) ($x_9x_8x_7x_6x_5$)	256-QAM ($x_3x_2x_1x_0$) ($x_7x_6x_5x_4$)	64-QAM ($x_2x_1x_0$) ($x_5x_4x_3$)	16-QAM (x_1x_0) (x_3x_2)	QPSK (x_0) (x_1)	BPSK (x_0) (---)
+31	11000					
+29	11001					
+27	11011					
+25	11010					
+23	11110					
+21	11111					
+19	11101					
+17	11100					
+15	10100	1100				
+13	10101	1101				
+11	10111	1111				
+9	10110	1110				
+7	10010	1010	110			
+5	10011	1011	111			
+3	10001	1001	101	11		
+1	10000	1000	100	10	1	1
-1	00000	0000	000	00	0	0
-3	00001	0001	001	01		
-5	00011	0011	011			
-7	00010	0010	010			
-9	00110	0110				
-11	00111	0111				
-13	00101	0101				
-15	00100	0100				
-17	01100					
-19	01101					
-21	01111					
-23	01110					
-25	01010					
-27	01011					
-29	01001					
-31	01000					

Table 319: Symbol Mapping for 8-QAM (not required for GREEN PHY)		
Mapped Value I	Mapped Value Q	8-QAM ($x_2x_1x_0$)
-1	-1.29	000
-3	-1.29	001
+1	-1.29	010
+3	-1.29	011
-1	+1.29	100
-3	+1.29	101
+1	+1.29	110
+3	+1.29	111

Table 320: Modulation Normalization Scales

Modulation	PowerScale	GREEN PHY requirement
BPSK		NO
QPSK		YES
8-QAM		NO
16-QAM		NO
64-QAM		NO
256-QAM		NO
1024-QAM		NO

Mapping for ROBO-AV

For ROBO-AV modulation, the majority of non-masked carriers are mapped with coherent QPSK modulation. A small number of carriers may become unusable in a particular ROBO Mode, since the ROBO Modes require the number of carriers to be an integer multiple of the number of redundant copies in the interleaver. Section 3.4.3.1 defines the creation of ROBO Tone Maps.

Symbol Generation

The following subsections specify in equation form the output of the IFFT, Preamble insertion, Windowing, and the Cyclic prefix insertion blocks in Figure 3-1.

Preamble

As with HomePlug AV, and as shown in Figure 3-2 and Figure 3-4, the Preamble sequence used by a HomePlug GREEN PHY station depends on whether the station is operating in AV-Only Mode or Hybrid Mode. Both of these Preambles are modified versions of HomePlug 1.0.1 Preamble that enable better performance and coexistence. The unshaped extended Preamble waveform is shown in Figure 3-13.

Figure 313: Extended Preamble Structure

The SYNCP AV and SYNCM AV symbols shown in this figure are similar to HomePlug 1.0.1's SYNCP and SYNCM symbols, except the AV symbols utilize carriers spanning 1.8-30 MHz, whereas the HomePlug 1.0.1 Preamble uses only 76 carriers spanning 4.5-20.7 MHz. The symbols labeled "Last Half" and "First Half" span 192 samples or 2.56 us whereas the other symbols span 384 samples or 5.12 us. Therefore, there is a total of 3840 samples in the extended time domain waveform.

The reference phase angle numbers for the SYNCP AV symbol for all carriers spanning roughly 1.8-30 MHz are included in Table 321. The actual phase, in radians, is the Phase Angle Number multiplied by /8. As the SYNCM AV time domain waveform is defined as the SYNCP AV waveform multiplied by -1, the SYNCM AV phases are the SYNCP AV phases shifted by [illegible]radians.

When the North American Spectral Mask in Table 323 is the active spectral mask, the grayed carriers in Table 321 are masked. The set of unmasked carriers with spacing as in Table 321 is denoted as $c_{HP1.0\text{-}ES}$. The index "HP1.0-ES" refers to "HomePlug 1.0.1 Carriers – Extended Set."

Table 321: SYNCP AV Phase Reference

384-IFFT Carrier Number	Frequency (MHz)	Phase Angle Number	384-IFFT Carrier Number	Frequency (MHz)	Phase Angle Number	384-IFFT Carrier Number	Frequency (MHz)	Phase Angle Number
10	1.953125	15	58	11.32813	8	106	20.70313	8
11	2.148438	1	59	11.52344	1	107	20.89844	3
12	2.343750	0	60	11.71875	10	108	21.09375	15
13	2.539063	11	61	11.91406	3	109	21.28906	4
14	2.734375	12	62	12.10938	11	110	21.48438	10
15	2.929688	8	63	12.30469	4	111	21.67969	13
16	3.125000	15	64	12.50000	12	112	21.87500	15
17	3.320313	14	65	12.69531	4	113	22.07031	6
18	3.515625	5	66	12.89063	12	114	22.26563	11
19	3.710938	14	67	13.08594	3	115	22.46094	3

20	3.906250	13	68	13.28125	11	116	22.65625	2
21	4.101563	10	69	13.47656	2	117	22.85156	12
22	4.296875	4	70	13.67188	9	118	23.04688	13
23	4.492188	0	71	13.86719	0	119	23.24219	9
24	4.687500	0	72	14.06250	7	120	23.43750	7
25	4.882813	15	73	14.25781	13	121	23.63281	7
26	5.078125	15	74	14.45313	3	122	23.82813	8
27	5.273438	14	75	14.64844	10	123	24.02344	11
28	5.468750	13	76	14.84375	15	124	24.21875	12
29	5.664063	12	77	15.03906	5	125	24.41406	8
30	5.859375	11	78	15.23438	11	126	24.60938	1
31	6.054688	9	79	15.42969	0	127	24.80469	7
32	6.250000	7	80	15.62500	5	128	25.00000	8
33	6.445313	6	81	15.82031	10	129	25.19531	1
34	6.640625	3	82	16.01563	15	130	25.39063	7
35	6.835938	1	83	16.21094	3	131	25.58594	0
36	7.031250	15	84	16.40625	8	132	25.78125	12
37	7.226563	12	85	16.60156	12	133	25.97656	13
38	7.421875	9	86	16.79688	0	134	26.17188	0
39	7.617188	6	87	16.99219	4	135	26.36719	1

40	7.812500	3	88	17.18750	7	136	26.56250	1
41	8.007813	15	89	17.38281	11	137	26.75781	15
42	8.203125	12	90	17.57813	14	138	26.95313	11
43	8.398438	8	91	17.77344	1	139	27.14844	12
44	8.593750	4	92	17.96875	4	140	27.34375	6
45	8.789063	0	93	18.16406	7	141	27.53906	5
46	8.984375	11	94	18.35938	9	142	27.73438	13
47	9.179688	7	95	18.55469	11	143	27.92969	2
48	9.375000	2	96	18.75000	14	144	28.12500	9
49	9.570313	13	97	18.94531	15	145	28.32031	11
50	9.765625	8	98	19.14063	1	146	28.51563	14
51	9.960938	3	99	19.33594	3	147	28.71094	04
52	10.156250	13	100	19.53125	4	148	28.90625	09
53	10.351563	7	101	19.72656	5	149	29.10156	05
54	10.546875	2	102	19.92188	6	150	29.29688	08
55	10.742119	11	103	20.11719	7	151	29.49219	08
56	10.937500	5	104	20.31250	7	152	29.68750	09
57	11.132811	15	105	20.50781	8	153	29.88281	09

The time domain waveform elements of the extended Preamble structure in Figure 3-13 are defined as:

where $C_{HP1.0-ES}$ is the set of all unmasked carriers in the HomePlug 1.0.1 Extended Set (defined above), c is an index with values in $C_{HP1.0-ES}$, $c=0$ corresponds to D.C., and (c) denotes the phase angle number defined in Table 321 multiplied by $/8$. The scaling factor of $10^{3/20}$ is due to the Preamble Symbol power boost defined in Table 322. Therefore, the entire extended Preamble waveform, $S_{PreambleExt}$ is given by:

Informative Text

The creation of the extended Preamble begins with the time domain waveform of the nominal Preamble shown in Figure 314.

Figure 314: Nominal Preamble Structure

The nominal Preamble waveform, $S_{NomPreamble}$ is given by:

Note: Due to the SYNCP/SYNCM transition, additional filtering is required in notched bands to make the extended Preamble waveform meet the spectral mask. The following informative text describes one way to create a spectrally correct extended Preamble waveform, without using digital filters.

where S_{SYNCP_AV} = S_{SYNCM_AV} and is defined above with the exception that here all carriers in Table 321 may be used (not just the subset of unmasked carriers).

A 3072-FFT is performed on $S_{NomPreamble}$, the amplitude mask , is applied, and a 3072-IFFT is performed to create the masked nominal Preamble, $S_{NomPreambleMasked}$.

The vector sets all masked carriers (positive and negative frequencies) to 0 amplitude as:

where is the subset of all positive unmasked carriers, is the subset of all negative unmasked carriers, and c is an index with values in and .

After performing the IFFT, windowing is applied to the resulting waveform to create the two Preamble sections shown in Figure 315.

The "rising" part of the tapered windowing, w_{rise}, and the "falling" part, w_{fall} are defined as:

where the equation parameter RI is defined in Figure 36: OFDM Symbol Timing Table 32.

The waveform for Preamble Section A is therefore defined as:

Informative Text
The creation of the extended Preamble begins with the time domain waveform of the nominal Preamble shown in Figure 314.

Figure 314: Nominal Preamble Structure

The nominal Preamble waveform, $s_{NomPreamble}$ is given by:

where s_{SYNCP_AV} and s_{SYNCM_AV} are the same as defined above with the exception that here all carriers in Table 321 may be used (not just the subset of unmasked carriers).
A 3072-FFT is performed on $s_{NomPreamble}$, the amplitude mask , is applied, and a 3072-IFFT is performed to create the masked nominal Preamble, $s_{NomPreambleMasked}$.

The vector sets all masked carriers (positive and negative frequencies) to 0 amplitude as:

where is the subset of all positive unmasked carriers, is the subset of all negative unmasked carriers, and c is an index with values in and .
After performing the IFFT, windowing is applied to the resulting waveform to create the two Preamble sections shown in Figure 315.
The "rising" part of the tapered windowing, w_{rise}, and the "falling" part, w_{fall} are defined as:

where the equation parameter RI is defined in Figure 36: OFDM Symbol Timing
Table 32.
The waveform for Preamble Section A is therefore defined as:

where:

The waveform for Preamble Section B is defined as:

where:

Figure 315: Sections for Extended Preamble

Shaping is then applied to the extended Preamble to create the AV Preamble as defined by:

where:

to obtain the AV Preamble, as shown in Figure 316.

Figure 316: AV Preamble Waveform

The AV Frame Control symbol that follows is overlapped with the AV Preamble waveform by RI samples, as shown in Figure 3-5 for the general case.

The Hybrid Preamble is generated in a similar way to the AV Preamble, except the tapering on the end of the Preamble begins 384 samples earlier to effectively remove one SYNCM AV symbol as shown in Figure 317. The Hybrid Preamble is defined as:

where:

Figure 317: Hybrid Preamble Waveform

The HomePlug 1.0.1 Frame Control that follows is overlapped with the Hybrid Preamble waveform by RI samples, as shown in Figure 3-6 .

Inappropriate Heap

The Hybrid and AV Preambles differ in length by 384 samples. An extra SYNCM symbol is required in the AV Preamble for synchronization reliability to not be compromised by Inter-Symbol Interference (ISI), since part of the Preamble is overlapped with the AV FC symbol. Due to the way the HomePlug 1.0.1 FC is created in the Hybrid Preamble case, the overlap adds constructively. Therefore ISI is not present and the extra SYNCM symbol is not required.

While HomePlug 1.0.1 had six SYNCP symbols in the Preamble, the Hybrid and AV Preambles have 7.5. However, the Hybrid and AV Preambles also have shaping that affects the amplitude profile of the first 1.5 symbols. Since AGC algorithms are amplitude dependent, adding the extra 1.5 symbols ensures that both 1.0.1 and AV Preambles have the same number of "unshaped" SYNCP symbols. Therefore, for the same AGC algorithm, AGC convergence time for AV and Hybrid Preambles will be the same, or better, than that of HomePlug 1.0.1 Preambles.

Both the AV and Hybrid Preambles were chosen to facilitate interoperability with existing HomePlug 1.0.1 nodes. The same Preamble symbol length is used as well as the same transmitted magnitudes and phases for each of the HomePlug 1.0.1 carriers. Therefore, HomePlug 1.0.1 nodes will synchronize with AV nodes with similar reliability to that of HomePlug 1.0.1 nodes. The HomePlug 1.0.1 carriers span approximately 4.5 MHz to 20.7 MHz. For both Hybrid and AV Modes, extra carriers are used below 4.5 MHz and above 20.7

Informative Text

The Hybrid and AV Preambles differ in length by 384 samples. An extra SYNCM symbol is required in the AV Preamble for synchronization reliability to not be compromised by Inter-Symbol Interference (ISI), since part of the Preamble is overlapped with the AV FC symbol. Due to the way the HomePlug 1.0.1 FC is created in the Hybrid Preamble case, the overlap adds constructively. Therefore ISI is not present and the extra SYNCM symbol is not required.

While HomePlug 1.0.1 had six SYNCP symbols in the Preamble, the Hybrid and AV Preambles have 7.5. However, the Hybrid and AV Preambles also have shaping that affects the amplitude profile of the first 1.5 symbols. Since AGC algorithms are amplitude dependent, adding the extra 1.5 symbols ensures that both 1.0.1 and AV Preambles have the same number of "unshaped" SYNCP symbols. Therefore, for the same AGC algorithm, AGC convergence time for AV and Hybrid Preambles will be the same, or better, than that of HomePlug 1.0.1 Preambles.

Both the AV and Hybrid Preambles were chosen to facilitate interoperability with existing HomePlug 1.0.1 nodes. The same Preamble symbol length is used as well as the same transmitted magnitudes and phases for each of the HomePlug 1.0.1 carriers. Therefore, HomePlug 1.0.1 nodes will synchronize with AV nodes with similar reliability to that of HomePlug 1.0.1 nodes. The HomePlug 1.0.1 carriers span approximately 4.5 MHz to 20.7 MHz. For both Hybrid and AV Modes, extra carriers are used below 4.5 MHz and above 20.7 MHz to expand the Preamble bandwidth to 2 MHz to 28 MHz for the Tone Mask defined in Table 323. The extra bandwidth provides increased synchronization reliability for AV nodes, without affecting HomePlug 1.0.1 synchronization reliability.

HomePlug 1.0.1 Frame Control

As with HomePlug AV, to operate in Hybrid Mode, the GREEN PHY system must be able to generate HomePlug 1.0.1 Frame Control symbols that not only can be properly decoded by 1.0.1 stations, but also conform to the spectral mask defined in Table 323. The HomePlug 1.0.1 Frame Control segment, $FC_{HP1.0}$, of the Hybrid delimiter is defined by the following equations:

where

where S_{SYNCM_AV}, w_{rise}, and w_{fall}, are defined in Section 3.6.1, and

for $m=1,2,3,4.$ is defined in Table 321 and results from the mapping of the HomePlug 1.0.1 FC channel bits as described in the HomePlug 1.0.1 specification, and the index d takes values from 0 to 75 for the first symbol, 76 to 151 for the second symbol, 152 to 227 for the third symbol, and 228 to 383 for the fourth symbol. The set $C_{HP1.0}$ is the set of all unmasked carriers defined in the HomePlug 1.0.1 specification.

The portion of the waveform labeled Residual is not explicitly defined and is inserted to support generation of the FC 1.0 using the 3072-IFFT method described in the informative text below. For implementations not using the 3072-IFFT method, any waveform may be transmitted in this portion, provided that it will not result in spectral mask violations.

The FC1.0.1 segment shall overlap with the Hybrid Preamble by RI samples, that is, sample zero of FC1.0.1 shall be added to sample 3084 of the preamble and sample 371 (RI-1) of the FC1.0.1 symbol added to sample 3455 of the hybrid preamble.

Informative Text

As with HomePlug AV, to assemble 1.0.1-compatible FC symbols using the 3072-IFFT, the GREEN PHY node creates the waveform shown in Figure 318. This is referred to as the HomePlug 1.0.1 FC Macro Symbol.

The space labeled "Residual" refers to the fact that when using the 3072-IFFT to create the HomePlug 1.0.1 FC Macro Symbol, the resulting time domain waveform is 3072 samples long. As with HomePlug AV, while the waveform in this Region does not carry information, its presence is required (cannot be zeroed or discarded) to preserve the GREEN PHY spectral mask.

Figure 318: HomePlug 1.0.1 FC Macro Symbol

In the HomePlug 1.0.1 FC Macro Symbol, each HomePlug 1.0.1 FC sub-symbol carries unique data on each of its carrier frequencies, per the HomePlug 1.0.1 specification. This data is modulated on each of the sub-symbol's 76 HomePlug 1.0.1 carriers using BPSK. A representative waveform for a single data bit carrier in the FC1 sub-symbol is shown in Figure 319.

Figure 319: Single Bit Carrier-Symbol Waveform

When examined in the frequency domain, this waveform has a sin(x)/x amplitude profile and a phase profile that is dependent on its frequency (carrier number) and position in time (FC sub-symbol number). Furthermore, due to its sin(x)/x frequency amplitude, the majority of the signal power resides in the frequencies that are closest to the fundamental frequency.

Based on this information, the carrier waveform for each data bit of each FC symbol can be recreated using the 3072-IFFT and a table containing the magnitude and phase of the fundamental carrier as well as some number of carriers to either side of the fundamental.
If each symbol's contribution to each carrier frequency is summed together (in the frequency domain) and then summed with the frequency contribution of the Preamble prefix fragment (first RI samples of the waveform in Figure 318), the resultant will be a frequency domain representation of the desired waveform. Performing a 3072-IFFT on this representation will generate the desired HomePlug 1.0.1 FC Macro Symbol time domain waveform.
It has been found empirically that the fundamental carrier with 7 AV carriers to either side yields robust system performance (preliminary modeling shows ~18 dB SNR, with 15 total AV carriers per HomePlug 1.0.1 carrier).

Informative Text

As with HomePlug AV, to assemble 1.0.1-compatible FC symbols using the 3072-IFFT, the GREEN PHY node creates the waveform shown in Figure 318. This is referred to as the HomePlug 1.0.1 FC Macro Symbol.

The space labeled “Residual” refers to the fact that when using the 3072-IFFT to create the HomePlug 1.0.1 FC Macro Symbol, the resulting time domain waveform is 3072 samples long. As with HomePlug AV, while the waveform in this Region does not carry information, its presence is required (cannot be zeroed or discarded) to preserve the GREEN PHY spectral mask.

Figure 318: HomePlug 1.0.1 FC Macro Symbol

In the HomePlug 1.0.1 FC Macro Symbol, each HomePlug 1.0.1 FC sub-symbol carries unique data on each of its carrier frequencies, per the HomePlug 1.0.1 specification. This data is modulated on each of the sub-symbol’s 76 HomePlug 1.0.1 carriers using BPSK. A representative waveform for a single data bit carrier in the FC1 sub-symbol is shown in Figure 319.

Figure 319: Single Bit Carrier-Symbol Waveform

When examined in the frequency domain, this waveform has a sin(x)/x amplitude profile and a phase profile that is dependent on its frequency (carrier number) and position in time (FC sub-symbol number). Furthermore, due to its sin(x)/x frequency amplitude, the majority of the signal power resides in the frequencies that are closest to the fundamental frequency.

Based on this information, the carrier waveform for each data bit of each FC symbol can be recreated using the 3072-IFFT and a table containing the magnitude and phase of the fundamental carrier as well as some number of carriers to either side of the fundamental.

If each symbol’s contribution to each carrier frequency is summed together (in the frequency domain) and then summed with the frequency contribution of the Preamble prefix fragment (first RI samples of the waveform in Figure 318), the resultant will be a frequency domain representation of the desired waveform. Performing a 3072-IFFT on this representation will generate the desired HomePlug 1.0.1 FC Macro Symbol time domain waveform.

It has been found empirically that the fundamental carrier with 7 AV carriers to either side yields robust system performance (preliminary modeling shows ~18 dB SNR, with 15 total AV carriers per HomePlug 1.0.1 carrier).

Since the HomePlug 1.0.1 carriers are spaced 8 AV carriers apart, FC symbol carrier spectra will overlap. The data modulates the FC carriers using BPSK, hence, the modulation must be applied to the carriers and their associated sidebands before they are overlapped.

After producing the HomePlug 1.0.1 FC Macro Symbol, a postfix (copied samples from the beginning of the HomePlug 1.0.1 FC Macro Symbol) is added, so that no part of the fourth 1.0.1 FC symbol is in the RI overlap Region.

Frame Control

As with HomePlug AV, the generation of Frame Control symbol(s) for the GREEN PHY shall comply with the following equations. The angles are defined as the set of QPSK phases computed from the Mapper output (refer to Section 3.5). For example, if the Mapper output for a particular carrier is:

then (d) is 45. The first value of d for each symbol (corresponding to the minimum value of c) is equal to the number of carriers in the set C_{HPAV} multiplied by the symbol number m, with m = 0 for the first Frame Control symbol in the PPDU. The index d is incremented by one for each successive value of c in the set C_{HPAV}.

The waveform for a particular Frame Control symbol, $S_{FCAV}[n]$ is defined as:

where:

The equation parameters T, GI_{FC}, and RI are defined in Figure 36: OFDM Symbol Timing Table 32. w_{rise} and w_{fall} are defined in Section 3.6.1.

C_{HPAV} is the set of all unmasked carriers, c is an index with values in C, c = 0 corresponds to D.C., and [illegible]*(c)* is defined in Section 3.5.3. The scaling factor of $10^{3/20}$ is due to the Frame Control Symbol power boost defined in Table 322.

Payload Symbols

The generation of the Payload Symbols shall comply with the following equations. The time domain discrete waveform for one payload symbol is defined below.

where:

The equation parameters RI, T, and GI are defined in Figure 36: OFDM Symbol Timing Table 32. w_{rise} and w_{fall} are defined in Section 3.6.1. The scaling factor of $10^{2.2/20}$ is due to the PPDU Payload Symbol power boost defined in Table 322.

The set M is the subset of all carriers in the Tone Map for non-ROBO symbols, and the modified Tone Mask used by ROBO symbols (refer to Section 3.4.3.1), c is the carrier index with values in M and c = 0 corresponds to D.C., *(c)* is defined in Section 3.5.3, and and are defined as the set of phases and amplitudes respectively of the rectangular symbols out of the Mapper (see Table 318, Table 319, and Table 320). For example, if the Mapper output for a particular 16-QAM carrier is:

then **(d) = 1** and **(d) = 71.57°**. The first value of d for each symbol (corresponding to the minimum

value of c) is equal to the number of carriers in the set M multiplied by the symbol number m, with m = 0 for the first payload symbol in the PPDU. The index d is incremented by one for each successive value of c.

Priority Resolution Symbol

The Priority Resolution Symbol shall be used during the Priority Resolution Slots (PRS). The Priority Resolution Symbol is derived from the PRS waveform defined in the HomePlug 1.0.1 specification by:

Including the additional carriers defined for the AV Preamble

Reversing the sign of the phases used in the Preamble

Affixing an extra half of a sub-symbol to the beginning and end of the standard six HomePlug 1.0.1 PRS sub-symbols

Pulse-shaping the first and last RI samples of the resulting waveform

Beginning transmission of the waveform a half of a sub-symbol (2.56 µs) before the start of the actual slot time

The nominal PRS waveform is defined as:

where $C_{HP1.0\text{-}ES}$ is the subset of all unmasked HomePlug 1.0.1 Extended Set carriers, c is an index with values in $C_{HP1.0\text{-}ES}$, c=0 corresponds to D.C., and **(c)** denotes the phase angle number defined in Table 321 multiplied by **/8**. The scaling factor of $10^{3/20}$ is due to the Priority Resolution Symbol scaling defined in Table 322.

Informative Text

The nominal masked PRS waveform can be created using the 3072-IFFT. First, the nominal unmasked PRS waveform is defined as:

where are the phases defined in Section 3.6.1. A 3072-FFT is performed on S_{NomPRS}, the amplitude mask (refer to Section 3.6) is applied, and the IFFT is performed to create the masked nominal PRS waveform.

The PRS waveform is then created by windowing the first and last symbols, effectively shrinking the length of the waveform by one sub-symbol (5.12 µs):

where:

The equation parameters T and RI are defined in Figure 36: OFDM Symbol Timing Table 32. w_{rise} and w_{fall} are defined in Section 3.6.1. To minimize the effect of the symbol shaping on priority detection reliability, the transmission of the resulting PRS waveform, S_{PRS_AV}, begins one-half a sub-symbol, or 2.56 µs, *before* the start of the actual Priority Resolution Slot, as shown in Figure 321.

Figure 321: AV PRS Waveform

Relative Power Levels

As with HomePlug AV, since radiation compliance is measured using quasi-peak (not mean) power, GREEN PHY traffic must have the same peak Power Spectral Density (PSD) profile as HomePlug 1.0.1 traffic. However, due to the closer carrier spacing (24.414 kHz) of Frame Control and PPDU payload symbols compared to those of HomePlug 1.0.1 (195.31 kHz), the resulting PSD has less ripple. This translates into a boost of approximately 2.2 dB in average subcarrier power for Frame Control and PPDU payload symbols for HomePlug 1.0.1 and GREEN PHY to have the same peak power levels.

Additionally, there are some waveforms with relatively low duty cycles. They can therefore be transmitted at higher average power than other types of higher duty cycle traffic, without affecting the measured peak PSD.

Table 322 summarizes the relative subcarrier average power levels for HomePlug 1.0.1 and HomePlug GREEN PHY with the HomePlug 1.0.1 PPDU payload symbols (called “packet body” symbols in HomePlug 1.0.1) as a reference. HomePlug GREEN PHY stations shall adjust their average power to comply with this table.

Table 322: Relative Power Levels

Waveform Type	Average Subcarrier Power Boost	
	HomePlug 1.0.1	HomePlug AV and GREEN PHY
Preamble Symbols	3 dB	3 dB
Frame Control Symbols	0 dB	3 dB
PPDU Payload Symbols	0 dB	2.2 dB
Priority Resolution Symbols	3 dB	3 dB

Note: The boost in average power applies to both the IFFT interval and cyclic prefix (if applicable).

Tone Mask

As with HomePlug AV, a Tone (or Carrier) Mask defines the set of tones that can be used in a given regulatory jurisdiction or a given application of the HomePlug GREEN PHY system. Certain tones need to be turned off to comply with the spectral mask requirements of the Region or application. Table 323 defines the maximal Tone Mask that will comply with current North American regulations. Tone Masks for other regulatory jurisdictions will be set by HomePlug as regulations for those regions become clear. The spectral mask for North America is also shown in Table 323 and depicted in Figure 325. As with HomePlug AV, to meet other regulations or applications, a HomePlug GREEN PHY station shall be capable of supporting Tone Masks of any combination of unmasked carriers, from a minimum of 275 to a maximum of 1155 unmasked carriers, in the frequency range of 1.8 to 30 MHz (carrier numbers 74-1228).

The 3072-point IFFT generates 1536 positive frequency carriers, with the carrier frequency of carrier k equal to:

Hz

A given carrier k is turned off if its presence will result in the transmitted spectrum violating the spectral mask. This condition can be determined from the spectral mask and the composite spectral occupancy of a semi-infinite set of HomePlug carriers ending with a carrier with center at f = 0 Hz, as shown in Figure 322 and Figure 323. While both figures show the occupancy profile for the three payload symbol GI lengths of Figure 36: OFDM Symbol Timing
Table 32, Figure 323 zooms in to detail the 30 dB down cutoff bandwidths for the standard mask defined by Table 323.

Figure 322: Spectral Occupancy for Semi-Infinite Number of Carriers - Zoomed Out

Figure 323: Spectral Occupancy for Semi-Infinite Number of Carriers - Zoomed In

Informative Text
The spectral occupancy of a single base-band carrier can be determined by the following method. Beginning with the time-domain waveform of the general OFDM payload symbol window shape w[n] defined in Section 3.6.4, append a large number of zeros onto this waveform to create an extended window $\mathbf{w_{extended}}$. For example, add zeros so that the resulting waveform length is 3072*100 total samples.
Determine the over-sampled spectral occupancy (power) of this single base-band carrier by performing .
To get the combined occupancy for a large (semi-infinite) number of carriers, a summation can now be performed using $\mathbf{P_{BaseBand}}$. Before summing for each additional carrier, $\mathbf{P_{BaseBand}}$ is shifted to reflect the frequency difference between the current carrier power being summed and the original 0 Hz base-band carrier.

Table 323: North American Carrier (Tone) and Spectral Masks

Frequency (MHz)	PSD Limit (dBm/Hz)	Carrier On/Off	Notes
F <= 1.71	-87	Carriers 0-70 are OFF	AM broadcast band and lower
1.71<F<1.8	-80	Carriers 71-73 are OFF	Between AM and 160-meter band
1.8 <= F <= 2.00	-80	Carriers 74-85 are OFF	160 meter amateur band
2.00 < F < 3.5	-50	Carriers 86-139 are ON	HomePlug carriers
3.5 <= F <= 4.00	-80	Carriers 140-167 are OFF	80 meter amateur band
4.000 < F < 5.33	-50	Carriers 168-214 are ON	HomePlug carriers
5.33 <= F <= 5.407	-80	Carriers 215-225 are OFF	5 MHz amateur band

5.407 < F < 7.0	-50	Carriers 226-282 are ON	HomePlug Carriers
7.0 <= F <= 7.3	-80	Carriers 283-302 are OFF	40 meter amateur band
7.3 < F < 10.10	-50	Carriers 303-409 are ON	HomePlug carriers
10.10 <= F <= 10.15	-80	Carriers 410-419 are OFF	30 meter amateur band
10.15 < F < 14.00	-50	Carriers 420-569 are ON	HomePlug carriers
14.00 <= F <= 14.35	-80	Carriers 570-591 are OFF	20 meter amateur band
14.35 < F < 18.068	-50	Carriers 592-736 are ON	HomePlug carriers
18.068 <= F <= 18.168	-80	Carriers 737-748 are OFF	17 meter amateur band
18.168 < F < 21.00	-50	Carriers 749-856 are ON	HomePlug carriers
21.000 <= F <= 21.45	-80	Carriers 857-882 are OFF	15 meter amateur band
21.45 < F < 24.89	-50	Carriers 883-1015 are ON	HomePlug Carriers
24.89 <= F <= 24.99	-80	Carriers 1016-1027 are OFF	12 meter amateur band
24.99 < F < 28.0	-50	Carriers 1028-1143 are ON	HomePlug Carriers
F >= 28.0	-80	Carriers 1144-1535 are OFF	10 meter amateur band

The optional BPL coexistence AV Mode can turn off further carriers if frequency domain multiplexing is used. For example, if the band up to 10 MHz is reserved for BPL access, all carriers up to carrier number 420 are turned off in HomePlug GREEN PHY.

Figure 324: Spectral Occupancy of Set of HomePlug Carriers

Amplitude Map

In addition to the Tone Mask, each carrier will obey its Amplitude Map. The Amplitude Map specifies a possible transmit power-reduction factor for each subcarrier. For example, if the Amplitude Map entry for a particular carrier is 0b0010, that carrier is transmitted at 4 dB less power than the normal PSD limit (-50 dBm / Hz for unmasked carriers for the North American spectral mask). Table 324 defines the power reduction for each value of the Amplitude Map entry. Also, refer to Section 11.5.12.

The Amplitude Map affects only the amplitudes of the corresponding unmasked carriers set by the Mapper and therefore does not in any way affect the encoding used for Frame Control, Payload, or ROBO symbols and/or the number of unmasked carriers. Carriers with an Amplitude Map entry of 0b1111, referring to "Off (No Signal)," are not considered or processed as masked by any element of the transmit chain, even though they have zero amplitude. The Amplitude Map is applied to all PHY waveforms, including the Preamble, PRS symbols, 1.0.1 Frame Control, AV Frame Control, and Payload Symbols. Power-reduction values shall be met with an accuracy of ±1 dB for AMDATA values from 0b0000 through 0b1010 and an accuracy of ±2 dB for AMDATA values from 0b1011 through 0b1110.

An Amplitude Map with no reduction in the transmit power on all used carriers (as defined in Tone Mask) shall be used as the default Amplitude Map in North America.

Table 324: Amplitude Map

AMDATA	TX Power Reduction (dB)	AMDATA	TX Power Reduction (dB)
0b0000	0 (no reduction - default)	0b1000	16
0b0001	2	0b1001	18
0b0010	4	0b1010	20
0b0011	6	0b1011	22
0b0100	8	0b1100	24
0b0101	10	0b1101	26
0b0110	12	0b1110	28
0b0111	14	0b1111	Off (no signal)

Transmitter Electrical Specification

The following specification establishes the minimum transmitter technical requirements for interoperability. All transmitter electrical specification requirements are based on the Tone Mask defined in Table 323. Unless otherwise stated, transmitter specifications assume a 50 Ohm load between line and neutral terminals. All transmitter output voltages and spurious transmissions are specified as the voltage measured at the line terminal with respect to the neutral terminal.

Transmit Spectrum Mask

The metallic power spectral density shall be less than the upper bound shown in Figure 325 and Table 323, measured according to the following procedure.

Figure 325: HomePlug GREEN PHY Transmit Spectrum Mask for North America

The transmitted power spectral density shall be below the limits specified. Measurements are made using equipment conforming to CISPR 16 specifications with a resolution bandwidth of 9 kHz and a quasi-peak detector. The transmitter shall be configured to transmit continuously.

Measurement steps:

- Set the input attenuation level to avoid overloading the spectrum analyzer front-end when subjected to the full bandwidth HomePlug signal.
- Set the instrument to measure peak power in a 9 kHz resolution bandwidth (dBm/9 kHz.) and ensure the instrument is in linear display mode. Record the highest HomePlug GREEN

PPDU Data (ROBO AV modulation for PHY carrier 1.8 MHz to 30 MHz.

- Set the instrument to measure quasi-peak power in a 9 kHz resolution bandwidth (dBm/9 kHz.) Set the center frequency to the carrier frequency recorded in step 2. Set the span to 200 kHz. Record the maximum quasi-peak power.
- Add 1.05 dB envelope detector correction factor to the maximum quasi-peak power.
- Determine the spectrum analyzer's equivalent noise power bandwidth for the 9 kHz filter by measuring the analyzer filter's peak, 3 dB, 6 dB, and 20 dB points and forming a piecewise linear model of the filter. The equivalent noise power bandwidth is the bandwidth of a rectangular filter (brickwall filter) whose area equals that of the piecewise linear model.
- Calculate the maximum power spectral density for the STA under test by taking the value obtained in step 4 and subtracting 10 log (equivalent noise power bandwidth/1 Hz).

Note: Actual equipment transmitter output levels may vary from the limits shown here to meet international, regional, or national regulatory requirements. The transmit spectrum mask defined here is an upper bound for compliance with the specification, and serves as guidance for designing the dynamic range of receivers.

Spurious Transmission

The transmitter shall conform with spurious emissions regulations in effect for the country in which this station is used.

Transmitter Accuracy

PHY Clock Frequency Tolerance

The electrical clock signal used by each STA for its signal processing is called the STA Clock (STA_Clk). The STA_Clk frequency is not specified, but its tolerance shall be ±25 ppm maximum. Under fixed ambient temperature conditions, the STA_Clk frequency must lie in a 6 ppm band in any 30-second interval.

The OFDM symbol period and the period of each OFDM carrier shall contain the precise number of samples specified in Section 3.6, under all conditions (i.e., the sampling rate, carrier frequency, and OFDM symbol rate shall be locked relative to each other). The sampling rate used to specify the transmit signal (at 75 MHz, nominally [refer to Section 3.6]) is referred to as the PHY Clock (PhyClk).

The PhyClk of the CCo shall be derived from the CCo's STA_Clk. All non-CCo STAs shall correct their PhyClk, as specified in Section 5.5.

Transmit Constellation Error

The relative constellation RMS error (defined below), averaged over subcarriers, OFDM Symbols, and blocks of OFDM Symbols shall not exceed the values indicated in Table 325. The relative constellation RMS error shall be measured with all entries in the Amplitude Map set to 0b0000 (no power reduction - default).

Table 325: RMS Transmit Constellation Error (TCE_RMS) Limits

Constellation Type	RMS Transmit Constellation Error Limit (dB)
Frame Control 1.0.1	-10
Frame Control AV	-10

PPDU Data (ROBO AV modulation for GREEN PHY)	-10
PPDU Data (all modulations for HomePlug AV)	-32

Transmit Constellation Error for GREEN PHY

The transmit constellation error for HomePlug GREEN PHY shall be as described in section 3.7.3.2 with the following exception (as noted in Table 3-25): for Constellation Type of PPDU Data (ROBO AV modulation) the RMS Transmit Constellation Error Limit shall be -10 dB.

Transmit Modulation Accuracy Test

The transmit modulation accuracy test shall be performed by instrumentation that can digitize a transmitted analog signal at a sample rate of 75 MS/s or more, with sufficient accuracy in terms of amplitude, DC offset, and phase noise. One possible setup is to use a high-resolution digital oscilloscope to capture the transmitted waveform. The sampled signal shall be processed in a way similar to an actual receiver, according to steps defined in the following subsections.

For all measurements in the following subsections, the measuring apparatus shall estimate the frequency difference between the transmitter and its local clock, and shall remove the effects of this difference before calculation of the modulation accuracy and distortion quantities described below.

Transmit Modulation Frame Control 1.0.1 Accuracy Test

For this test, the transmitter must be in Hybrid Mode, so that a HomePlug 1.0.1 Frame Control (FC1.0.1) is present in the PPDU. To minimize the possibility of ISI affecting the measurements, all FFTs are taken at an offset ($CP_OFFSET_{1.0.1}$) with respect to symbol boundaries. For this test, $CP_OFFSET_{1.0.1}$=15. The following steps describe how to determine the Frame Control 1.0.1 RMS Constellation error from the digitized (75 MS/s) transmitted waveform:

- Detect the start of PPDU i.
- To obtain a reference vector for the coherently modulated OFDM Symbols, take a 384-FFT of the following four length 384 vectors and average the resulting 4 rectangular components for each subcarrier:

Vector 1: (last $CP_OFFSET_{1.0.1}$ samples of 2nd full SYNCP symbol; first 384-$CP_OFFSET_{1.0.1}$ samples of the 3rd full SYNCP) (first sample in vector is 960-$CP_OFFSET_{1.0.1}$ samples from the start of the Preamble)

Vector 2: (last CP_OFFSET1.0.1 samples of 3rd full SYNCP symbol; first 384-CP_OFFSET1.0.1 samples of the 4th full SYNCP)

Vector 3: (last CP_OFFSET1.0.1 samples of 4th full SYNCP symbol; first 384-CP_OFFSET1.0.1 samples of the 5th full SYNCP)

Vector 4: (last CP_OFFSET1.0.1 samples of 5th full SYNCP symbol; first 384-CP_OFFSET1.0.1 samples of the 6th full SYNCP)

Denote the averaged vector as $R_{i,0,k}$, where **i** is the PPDU index, and **k** is the subcarrier index (**subcarrier frequency = k·75 / 3072 MHz**) to all information bearing carriers.

- To obtain the transmit constellation for the four coherently modulated OFDM Symbols, for

each length 246+384 extended symbol (for example FC1, defined in Figure 319), first perform an FFT on the length 384 vector starting $CP_OFFSET_{1.0.1}$ samples back from the symbol IFFT interval (first sample in vector is $246\text{-}CP_OFFSET_{1.0.1}$ samples from the start of each extended symbol). Denote each of these FFT outputs as $R_{i,1,k}$, $R_{i,2,k}$, $R_{i,3,k}$, and $R_{i,4,k}$.

Then de-rotate the subcarrier values according to the estimated reference vector obtained in 2 above by computing:

where $C_{HP1.0}$ is the set of 76 unmasked subcarriers defined in the HomePlug 1.0.1 specification and $C_{HP1.0\text{-}ES}$ is defined in Section 3.6.1. The scaling factor is introduced to account for the different average power of the HomePlug 1.0.1 Frame Control relative to the Preamble average power, as in Table 322.

- The error between the transmitted and ideal constellation symbol is determined as the squared Euclidean distance between the two symbols (assuming that the ideal constellation symbol is that symbol from the original constellation with the smallest distance to the transmitted symbol).

  If $P^{FC101,TX}_{i,j,c}$ is the ideal complex constellation symbol corresponding to $P^{FC101,RX}_{i,j,c}$, the transmit constellation error is defined as:

- Repeat steps 1 through 4 for all PPDUs.
- Compute the RMS average for the HomePlug 1.0.1 Frame Control symbols as:

Note: The summation over the subcarriers should only include such carriers that are not masked. The test shall be performed over at least N_PPDUs = 10.

Transmit Modulation Frame Control and PPDU Data Accuracy Tests

For this test, all 3072-FFTs are taken at an offset (CP_OFFSET_{AV}) with respect to symbol boundaries to minimize the possibility of ISI affecting the measurements. For this test, $CP_OFFSET_{AV=384}$. As with HomePlug AV, the following steps describe how to determine the Frame Control RMS Constellation error from the digitized (75 MS/s) transmitted waveform:

- Repeat steps 1 and 2 from Section 3.7.3.3.1 to create $R_{i,0,k}$.

Take the 384-FFT of an ideal SYNCP_AV as in Section 3.6.1 and apply a phase shift to compensate for the $CP_OFFSET_{1.0.1}$ time shift in $R_{i,0,k}$.

where $C_{HP1.0\text{-}ES}$ is defined in Section 3.6.1.

Note: In the equation above and all following equations, "$1j$" refers to the square root of –1, whereas "j" by itself is used to signify the symbol index.

- Compute the partial 384-FFT normalization factors for each subcarrier as:

- To create the full 384-FFT normalization factors, $H^{384}_{i,0,k}$, stuff each masked carrier entry with that of the closest non-masked carrier. For example, if carrier 50 is masked and the closest unmasked carrier is carrier 52, then $H^{384}_{i,0,50} = H^{384,Partial}_{i,0,52}$.
- As H^{384} only provides channel state information for every 8th carrier when using 3072-FFT spacing, use linear interpolation on the rectangular components of H^{384} to convert the 384-FFT normalization factors into 3072-FFT normalization factors (H^{3072}).
- To obtain the transmit constellation for the coherently modulated Frame Control symbol(s), for each symbol, first perform an FFT on the length 3072 vector starting $CP_OFFSET_{AV=384}$ samples back from the beginning of the IFFT interval as in Figure 3-6 and Figure 36: OFDM Symbol Timing
- Table 32. Denote these FFT outputs as $R^{FCAV}_{i,1,k}$ and optionally $R^{FCAV}_{i,2,k}$. Then de-rotate the subcarrier values by computing:

where is the vector of reference phases defined in Section 3.5.3.

- The error between the transmitted and ideal constellation symbol is determined as the squared Euclidean distance between the two symbols (assuming that the ideal constellation symbol is that symbol from the original constellation with the smallest distance to the transmitted symbol).

  If $P^{FCAV,TX}_{i,j,k}$ is the ideal complex constellation symbol corresponding to $P^{FCAV,RX}_{i,j,k}$, then the transmit constellation error is defined as:

- Construct a channel reference, $R^{Data}_{i,0,k}$ for the PPDU payload symbol(s) from the Preamble and/or Frame Control Symbol(s).

  Note: This reference needs to take into account the fact that the FFT for the PPDU payload symbol(s) in the following steps is taken CP_OFFSET_{AV} samples back from the beginning of the IFFT interval.
- To obtain the transmit constellation for the coherently modulated PPDU payload symbol(s), for each symbol, first perform an FFT on the length 3072 vector starting CP_OFFSET_{AV} samples back from the beginning of the IFFT interval as in Figure 3-6 and Figure 36: OFDM Symbol Timing
- Table 32. Denote these FFT outputs as $R^{Data}_{i,j,k}$. Then de-rotate the subcarrier values by computing the following (where is the vector of reference phases defined in

Section 3.5.3):

- The error between the transmitted and ideal constellation symbol is determined as the squared Euclidean distance between the two symbols (assuming that the ideal constellation symbol is that symbol from the original constellation with the smallest distance to the transmitted symbol).

  If $P^{Data,TX}_{i,j,k}$ is the ideal complex constellation symbol corresponding to $P^{Data,RX}_{i,j,k}$, then the transmit constellation error is defined as:

- Repeat steps 1 through 10 for all PPDUs.
- Compute the RMS average for the Frame Control symbol(s) as:

  where N_PPDUs is the number of Frame Control (FCAV) symbols per PPDU and C_{HPAV} is the set of all unmasked carriers using 3072-FFT subcarrier spacing. The test shall be performed over at least N_PPDUs = 10.
- Compute the RMS average for the PPDU payload symbols as:

  where Nsymbols is the number of PPDU Payload symbols per PPDU. The test shall be performed for each modulation (all unmasked carriers running a single modulation type per test) over at least N_PPDUs = 10 with each PPDU having at least Nsymbols=10.

Transmit Preamble Distortion Test

The RMS Transmit Preamble Distortion (TPD_RMS, defined in detail later in this subsection) averaged over subcarriers, Preamble SYNCP symbols, and PPDUs of OFDM Symbols, shall not exceed –10 dB. The RMS transmit Preamble distortion test shall be performed using the same instrumentation as used for the Transmit Modulation Accuracy Test (described in Section 3.7.3.3.2). The transmitted waveform shall be sampled and processed in a manner similar to an actual receiver, according to the following steps, or an equivalent procedure:

- Detect the start of PPDU i.

  Note: For this test, the start of PPDU may have to be detected to within 0.15 of a sample or better to meet the required distortion limit.

- Perform an FFT on the 7 full unshaped OFDM Symbols (6 SYNCPs and first SYNCM) of the Preamble to obtain subcarrier received values, resulting in the vectors $R_{i,1,k}$, $R_{i,2,k}$, $R_{i,3,k}$, $R_{i,4,k}$, $R_{i,5,k}$, $R_{i,6,k}$, and $R_{i,7,k}$, where i is the PPDU index, and k is the subcarrier index.
- Normalize the amplitude of each element of the vectors obtained in b) to 1, thus obtaining

- Ideally, the phases of the complex points in the vectors $P_{i,j,k}$ should correspond to the phases given in Table 321. Define the phase distortion in each $P_{i,j,k}$ as:

and

- Repeat steps 1 through 4 for all PPDUs i=1, …, N_PPDUs.
- Compute the RMS transmit phase distortion as:

Note: The summation over the subcarriers should only include such carriers that are not masked. The test shall be performed over at least 40 PPDUs (N_PPDUs40).

Transmit Priority Resolution Symbol Accuracy

The RMS Transmit PRS Waveform Distortion (TPRSD_RMS, defined in detail below) averaged over subcarriers and PRS symbols, shall not exceed –10 dB. The transmitter PRS waveform distortion test shall be performed using the same instrumentation as used for the Transmit Modulation Accuracy Test (described in Section 3.7.3.3.2). The transmitted waveform shall be sampled and processed in a manner similar to an actual receiver, according to the following steps or an equivalent procedure:

- Detect the start of PRS waveform i.

Note: For this test, the start of the Preamble may have to be detected to within 0.15 of a sample or better, in order to meet the required distortion limit).

- Perform an FFT on the 4 unshaped PRS symbols (middle 4 of the 6 full Priority Resolution Symbols) to obtain subcarrier received values, resulting in the vectors $\mathbf{R_{i,1,k}}$, $\mathbf{R_{i,2,k}}$, $\mathbf{R_{i,3,k}}$, $\mathbf{R_{i,4,k}}$, $\mathbf{R_{i,5,k}}$, and $\mathbf{R_{i,6,k}}$, where $\mathbf{i}$ is the PRS waveform index and $\mathbf{k}$ is the subcarrier index.
- Normalize the amplitude of each element of the vectors obtained in b) to 1, thus obtaining:

Ideally, the phases of the complex points in the vectors $\mathbf{P_{i,j,k}}$ should correspond to the phases given in Table 321, shifted by 180 degrees. Define the phase distortion in each $P_{i,j,k}$ as:

- Repeat steps 1 through 3 for all PRS waveforms, $\mathbf{i=1}$, …, $\mathbf{NPRS}$.
- Compute the RMS transmit phase distortion as:

Note: The summation over the subcarriers should only include such carriers that are not masked. The test shall be performed over at least 40 PRS waveforms (NPRS40).

Receiver Electrical Specification

All receiver electrical specification requirements are based on the Tone Mask defined in Table 323. Unless otherwise stated, all receive signals and interference are specified as the voltage measured at the line terminal with respect to the neutral terminal.

Receiver Sensitivity

All measurements in the following subsections shall be made at the M1 Interface using a minimum of 10000 PBs of data with a PPDU length such that a minimum of 20 OFDM Symbols are transmitted per PPDU.

Receiver Minimum Input Voltage

The received block error rate (one or more errors occurring within the PB) will not exceed 0.1% when an all 1024-QAM rate 16/21 waveform is received with a signal level of 35 mVrms, without any interfering signals or signal impairments. The received block error rate will not exceed 0.1% when a STD-ROBO mode waveform is received with a signal level of 0.7 mVrms, without any interfering signals or signal impairments. In the interest of efficient utilization of the channel common resource, implementers are encouraged to strive for lower minimum signal levels.

Receiver Minimum Input Voltage for GREEN PHY

For a station that only implements GREEN PHY, the received block error rate will not exceed 0.1% when a STD-ROBO mode waveform is received with a signal level of 0.7 mVrms, without any interfering signals or signal impairments. In the interest of efficient utilization of the channel common resource, implementers are encouraged to strive for lower minimum signal levels.

Receiver Maximum Input Voltage

The received block error rate (one or more errors occurring within the PB) will not exceed 0.1% when an all 1024-QAM rate 16/21 waveform is received with a signal level of 8 Volts peak-to-peak, without any interfering signals or signal impairments.

Receiver Maximum Input Voltage for GREEN PHY

For a station that only implements GREEN PHY, the received block error rate (one or more errors occurring within the PB) will not exceed 0.1% with a signal level of 8 Volts peak-to-peak, without any interfering signals or signal impairments.

Receiver Input Impedance

When not transmitting, the PHY shall present a minimum impedance of 40 Ohms in the band extending from 1.8 MHz to 30 MHz measured between line and neutral terminals. The PHY shall present a minimum impedance of 20 Ohms in the ranges from 100 kHz to 1.8 MHz and from 30 MHz to 50 MHz.

Immunity to Narrowband Interference

The received PB error rate shall not exceed 1% when the desired waveform present at the receiver is corrupted by a constant sinusoidal interfering signal occupying any single frequency from 100 kHz to 30 MHz, producing a total signal-to-jammer power ratio of -25.0 dB at the receiver terminals. The level of the interfering signal shall be between 1.0 and 0.5 Vrms. Immunity shall be measured at the M1 Interface using a minimum of 10000 PBs of each of the PB520 and PB136 types.

Physical Carrier Sense

A Physical Carrier Sense (PCS) mechanism shall be provided by the receiver through the detection of Priority Resolution Symbols and the detection of Preamble Symbols.

Detection of Priority Resolution Symbols

The receiver shall be able to detect the presence of Priority Resolution Symbols within a Priority Resolution Slot Time with a miss rate not exceeding 1% using the standard North American mask under the following conditions:

When the desired PRS waveform present at the receiver has a signal power of –35 dBm and is corrupted by Gaussian noise producing a total SNR of 2 dB at the receiver terminal. For this test, the average signal power and average noise power are measured from the time domain waveforms of each, adjusting for differences in occupied bandwidth between the two waveforms. Let the

variable x(t) refer to the PRS time domain waveform present at the receiver before noise has been added, computed from the non-windowed portion of the waveform. Likewise, let the variable n(t) refer to the time domain AWGN waveform that will be added to s(t). Let $\mathbf{BW_{Signal}}$ and $\mathbf{BW_{Noise}}$ refer to the occupied bandwidth of **x(t)** and **n(t)**, respectively. Then the SNR shall be computed as:

Informative Text
For example, using the standard North American tone mask and a sampling rate of 75 MS/s, the 5.12 μs PRS symbols use 112 non-masked carriers. AWGN noise, also sampled at 75 MS/s, will occupy the entire bandwidth from DC to Nyquist (or equivalently 192 non-masked carriers). So the calculation should be performed as:

When the desired PRS waveform present at the receiver has a signal power of –35 dBm and is corrupted by a constant sinusoidal interfering signal occupying any single frequency from 100 kHz to 30 MHz, producing a total Signal-to-Jammer (SJR) power ratio of -25 dB at the receiver terminal. Again, let the variable x(t) refer to the Preamble time domain waveform present at the receiver before noise has been added. Let j(t) refer to the time domain waveform of the jammer. The SJR shall be measured as:

Detection of Preamble Symbols
The receiver shall be able to detect the presence of Preamble Symbols within a Slot Time with a miss rate not exceeding 1% using the standard North American mask under the following conditions:
When the desired Preamble Symbol waveform present at the receiver has a signal power of -35 dBm and is corrupted by Gaussian noise producing a total SNR of 2 dB at the receiver terminal. For this test, the average signal power and average noise power are measured from the time domain waveforms of each, adjusting for differences in occupied bandwidth between the two waveforms. Let the variable **x**(t) refer to the Preamble time domain waveform present at the receiver before noise has been added, computed from the non-windowed portion of the waveform. Likewise let the variable n(t) refer to the time domain AWGN waveform that will be added to s(t). Let $\mathbf{BW_{Signal}}$ and $\mathbf{BW_{Noise}}$ refer to the occupied bandwidth of x(t) and n(t) respectively. Then the SNR shall be computed as:

When the desired Preamble Symbol waveform present at the receiver has a signal power of –35 dBm and is corrupted by a constant sinusoidal interfering signal occupying any single frequency from 100 kHz to 30 MHz, producing a total SJR power ratio of -25 dB at the receiver terminal. Again, let the variable x(t) refer to the Preamble time domain waveform present at the receiver before noise has been added. Let j(t) refer to the time domain waveform of the jammer. The SJR shall be measured as:

Frame Formats

Bit and Octet Order

This section presents the conventions for interpreting bit and octet ordering for HomePlug GREEN PHY (which follows the same convention as HomePlug AV). The bit ordering at the Media Access Control-Physical (MAC-PHY) interface is also presented.

Text Conventions

This specification uses binary and hexadecimal notation of fields in text and tables. The interpretation of the bit and nibble ordering in these fields shall adhere to the rules described in the following sections.

Binary Fields

Binary fields shall be shown with a prefix of "0b" to indicate the binary (or base-2) nature of the data. The field shall start with the most-significant bit (MSB).

A general binary representation of a field has a format of 0bB*n*…B1B0, with bit "B*n*" representing the MSB and bit "B0" representing the least-significant bit (LSB).

Examples

In the following example, "1" is the LSB. The value of this field is equivalent to "1" in decimal notation: 0b001

In the following example, "1" is the MSB. The value of this field is equivalent to "16" in decimal notation: 0b10000

Hexadecimal Fields

Hexadecimal fields shall be shown with a prefix of "0*x*" to indicate the hexadecimal (or base-16) nature of the data. The field shall start with the most-significant nibble of the fields.

A general hexadecimal representation of a field has a format of 0xH*n*…H1H0, with nibble "H*n*" representing the most-significant nibble and nibble "H0" representing the least-significant nibble.

A hexadecimal field can be converted into a binary field by replacing each nibble with the corresponding binary value (following the representation of binary fields).

Examples

In the following example, "E" is the least-significant nibble: 0x00E.

In the following example, "e" is the least-significant nibble: 0x00e.

In the following example, "E" is the most-significant nibble: 0xE00.

In the following example, "e" is the most-significant nibble: 0xe00.

Bit and Octet Transmission Order at the MAC-PHY Interface

At the MAC-PHY interface, octets shall be transmitted in order, from the smallest numbered octet (Octet 0) to the largest numbered octet. Bits shall be transmitted from the LSB to the MSB. Figure 41 shows the bit and octet transmission order at the MAC-PHY interface.

Figure 41: Bit and Octet Transmission Order at the MAC-PHY Interface

When a field can be completely transmitted within an octet, the LSB used by the field within that octet shall be treated as the LSB bit of the field. When a field spans multiple octets, the LSB used

by the field in the least-significant octet shall be treated as the LSB bit of the field. Consequently, the LSB of the field is the first bit to be transmitted across the MAC-PHY interface.
Figure 42 shows an example of a field that spans across multiple octet boundaries. In this example:
Octet 0, Bit 0 is the LSB of Field F1.
Octet 0, Bit 3 is the MSB of Field F1.
Octet 0, Bit 4 is the LSB of Field F2.
Octet 1, Bit 5 is the MSB of Field F2.
Octet 1, Bit 6 is the LSB of Field F3.
Octet 1, Bit 7 is the MSB of Field F3.

Figure 42: Example of Field Spanning Across Octet Boundaries
Both tables and figures are used throughout the specification to indicate the bit and octet transmission ordering of various fields. Table 41 and Figure 43 show the representation of the fields in the above example using table and figure examples.
Note: For fields that have length in multiples of octets and obeying octet boundaries, the table representation does not include the “Bit Number” column. Similarly, the length of fields within the figure is presented in octets.

Table 41: Example of Tabulation of Fields That Do Not Obey Octet Boundaries

Field	Octet Number	Bit Number	Field Size (Bits)
Field 1	0	0 – 3	4
Field 2	0 – 1	4 – 7	10
	1	0 – 5	
Field 3		6 - 7	2
…			

Figure 43: Example of Figure-Based Representation of Fields That Do Not Obey Octet Boundaries

Notes:

The bit ordering in this section is the opposite from the bit ordering in the HomePlug 1.0.1 specification. The change was made to make bit and octet ordering consistent with the Institute of Electrical and Electronics Engineers (IEEE) Std 802-2001 [4]. The octet ordering in the HomePlug 1.0.1 specification and in this specification are the same.

The MAC addresses in this standard are represented as described in the IEEE Standard 802-2001 [4]. Thus, the least-significant bit of the first octet of the 48-bit MAC Address is the Individual/Group (I/G) bit.

The VLAN Tag field in this standard is represented as described in IEEE 802.1Q [11] Clause 9 for an Ethernet-encoded Tag Protocol ID.

The format of the MTYPE field (refer to Section 11.1.4), which contains the IEEE Assigned Unique Ethertype for AV, is as described in the IEEE 802.3 standard [12].

Cyclic Redundancy Check Calculation

As with HomePlug AV, the HomePlug GREEN PHY MAC uses Cyclic Redundancy Checks (CRCs) of different lengths to check correct demodulation or decryption of data. In all cases, the LSB of the first octet is input first in time to the CRC encoder. For information about the HomePlug GREEN PHY bit and octet ordering convention at the MAC-PHY interface, refer to Section 4.1.

CRC-32

CRC-32 shall be computed using the following standard generator polynomial of degree 32:

CRC-32 is the one's complement of the (modulo-2) sum of the following:

The remainder of divided (modulo-2) by $G(x)$, where k is the number of bits in the calculation fields, and

The remainder after multiplication of the contents (treated as a polynomial) of the calculation fields by x^{32} and division by $G(x)$.

The CRC-32 field shall be transmitted starting with the coefficient of the highest order term.

Informative Text

At the transmitter, the initial remainder of the division is preset to all ones and then modified by division of the calculation fields by the generator polynomial $G(x)$. The one's complement of this

Informative Text
As a typical implementation:
At the transmitter, the initial remainder of the division is preset to all ones and then modified by division of the calculation fields by the generator polynomial $G(x)$. The one's complement of this remainder is transmitted, with the highest-order bits first, as the CRC-32 field.
At the receiver, the initial remainder is preset to all ones. The serial incoming bits of the calculation fields and CRC-32, when divided by $G(x)$ in the absence of transmission errors, results in a unique nonzero remainder value. The unique remainder value is the polynomial:

CRC-24
CRC-24 shall be computed using the following standard generator polynomial of degree 24:

$G(x) = x^{24} + x^{23} + x^6 + x^5 + x + 1$
CRC-24 is the one's complement of the (modulo-2) sum of the following:
The remainder of divided (modulo-2) by , where is the number of bits in the calculation fields,

and
The remainder after multiplication of the contents (treated as a polynomial) of the calculation fields by and then division by .
The CRC-24 field shall be transmitted starting with the coefficient of the highest order term.

Informative Text
As a typical implementation:
At the transmitter, the initial remainder of the division is preset to all ones and then modified by division of the calculation fields by the generator polynomial G(x). The one's complement of this remainder is transmitted, with the highest order bits first, as the CRC-24 field.
At the receiver, the initial remainder is preset to all ones and the serial incoming bits of the calculation fields and CRC-24, when divided by G(x) in the absence of transmission errors, results in a unique nonzero remainder value. The unique remainder value is the polynomial:

MAC Frame Format
As with HomePlug AV, HomePlug GREEN PHY processes each MAC Service Data Unit (MSDU) and generates a MAC Frame. A MAC Frame is composed of a MAC Frame Header, optional Arrival Time Stamp (ATS) or random Confounder, optional MSDU Payload, optional Management Message, and an Integrity Check Value (ICV).
A MAC Frame shall contain either an MSDU Payload or Management Entry, but not both. A MAC Frame with a Management Entry shall never contain an ATS, but shall always contain a random Confounder. Section 5.4.1 provides information about the MAC Frame generation from an MSDU.

Figure 44: MAC Frame Format

MAC Frame Header

MAC Frame Header is a 2-octet field that carries information about the:

Validity of the MAC Frame

Presence of ATS

Length of the MAC Frame

Table 42 shows the MAC Frame Header.

Table 42: MAC Frame Header Field

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
MFT	0	0 - 1	2	MAC Frame Type
MFL	0	2 - 7	14	MAC Frame Length
	1	0 - 7		

MAC Frame Type (MFT)

MAC Frame Type (MFT) is a 2-bit field that indicates the type of information contained in the MAC Frame. Table 43 shows the interpretation of the values in this field.

Table 43: MAC Frame Type Field Interpretation

MFT Value	Interpretation
0b00	Indicates the presence of a bit pad in the MAC Frame Stream (refer to Section 5.4.1.3).
0b01	Indicates the presence of the MSDU Payload without an associated ATS.
0b10	Indicates the presence of the MSDU Payload along with an associated ATS.
0b11	Indicates the presence of a MAC Management Entry with associated Confounder.

When the MFT is 0b00, there is no MFL and the remaining octets (if any) to the next segment boundary (128 octet or 512 octet) are filled with padding. The padding shall be ignored by the receiver. See Figure 45.

Figure 45: MAC Frame when MFT=0b00

Informative Text
When the MFT is 0b00, the padding to the next segment boundary (128 octet or 512 octet) may be pseudorandom, zero-padding, or other padding. See Figure 45.

When the MFT is 0b01, there is an MSDU Payload with no Confounder and no ATS. See Figure 46.

Figure 46: MAC Frame when MFT=0b01

When MFT=0b10, there is an MSDU Payload with a 4-octet ATS. See Figure 47.

Figure 47: MAC Frame when MFT=0b10

When MFT=0b11, there is a MAC Management Message and a 4-octet Confounder. The Confounder shall be filled with a pseudorandom value. See Figure 48.

Figure 48: MAC Frame when MFT=0b11

MAC Frame Length (MFL)

MAC Frame Length (MFL) is a 14-bit field that specifies the MAC Frame length in octets, excluding the 2-octet MAC Frame Header field and the 4-octet ICV, but including the ATS or confounder (if either is present). A value of 0x0000 indicates a length of 1 octet, and so on.

Arrival Time Stamp

Refer to the Arrival Time Stamp parameter in Section 12.3.2.1.

Arrival Time Stamp for GREEN PHY

A station that only implements GREEN PHY is not required to implement the Arrival Time Stamp since Connection Services are not required.

Confounder

The Confounder consists of a 4-octet pseudorandom value.

Informative Text

IVs are predictable and could wrap around. This may be an issue when the same IV is used with the same NEK and the MFBO = 0. Segment Sequence Number (SSN) provides 16 bits of IV that should cycle through before repeating. Many of the fields in the FC will only vary a little over time if at all. In multimedia streams, the MFBO will cycle to some extent, and the changing FC fields should make about 28-30 bits of effective IV space, which is enough for at least 10 hours before IV repetition. The 32-bit ATS also makes the initial 16 octets of MAC Frames of high-data rate multimedia streams unpredictable, in effect extending the IV, so multimedia streams should not have problems with IVs. MAC management streams will normally have MFBO=0, and MMEs have little variability at their start (see Figure 48). Since bursting is also unlikely, the effective number of IV bits for MAC Management streams may be low, especially if the SSN is reset. This can provide a fair amount of known or guessed plaintext for an attacker. To combat this potential problem with repeating IVs, the NEK is required to change fairly often (at least once an hour). To increase the variability at the start of MMEs, the MF is required to have a 32-bit random Confounder. This has the effect of rendering otherwise identical messages sent under the same NEK and IV as different ciphertexts, defeating recognized ciphertext attacks.

MSDU Payload

Refer to the MSDU Payload parameter in Section 12.3.2.1.

Management Message

Refer to the Management Message parameter in Section 12.3.2.1.

Integrity Check Value

Integrity Check Value (ICV) is a CRC-32 computed over a MAC Frame. The ICV does not cover

the MAC Frame Header, ATS (if present), or confounder (if present). The ICV is computed as described in Section 4.2.1.

MAC Protocol Data Unit (MPDU) Format

The term "MAC Protocol Data Unit" (MPDU) refers to information that the MAC has asked the PHY to transport. As with HomePlug AV, four MPDU formats are defined for use by HomePlug GREEN PHY stations:

Two MPDU formats are used in AV-Only Mode.

Two MPDU formats are used in HomePlug 1.0.1 Coexistence (or Hybrid) Mode.

The term "Long MPDU" indicates an MPDU that carries payload information in addition to Frame Control information.

In AV-Only Mode, the Long MPDU carries 128-bit (AV) Frame Control information, followed by the MPDU Payload.

In Hybrid Mode, the Long MPDU carries 25-bit HomePlug 1.0.1 Frame Control information, followed by 128-bit (AV) Frame Control information, followed by the MPDU Payload.

The term "Short MPDU" indicates an MPDU that carries only Frame Control information.

In AV-Only Mode, the Short MPDU carries a 128-bit Frame Control block containing (AV) Frame Control information.

In Hybrid Mode, the Short MPDU carries 25-bit HomePlug 1.0.1 Frame Control information, followed by a 128-bit Frame Control block containing (AV) Frame Control information.

In the remainder of this specification, the terms "Long MPDU" and "Short MPDU" indicate either AV-Only Mode or Hybrid Mode Long and Short MPDUs, respectively. When a distinction needs to be made between Hybrid Mode and AV-Only Mode, the term "Hybrid" and "AV-Only" shall be explicitly used. Unless otherwise stated, Frame Control refers to HomePlug AV Frame Control information. Figure 49 shows the MPDU frame formats in AV-Only Mode. Figure 410 shows the MPDU frame formats in Hybrid Mode.

Figure 49: MPDU Frame Formats in AV-Only Mode

Figure 410: MPDU Frame Formats in Hybrid Mode

MPDU Frame Control Fields

MPDU Frame Control blocks are 128-bit blocks that carry Frame Control information. In Hybrid Mode, an additional 25-bit HomePlug 1.0.1 Frame Control provides coexistence with HomePlug 1.0.1 stations.

Table 44 defines the general Frame Control format: the HomePlug 1.0.1 Frame Control field, followed by 128-bit Frame Control Block carrying Frame Control information.

Table 44: MPDU Frame Control Fields

	Field	Octet Number	Bit Number	Field Size (Bits)	Definition
HomePlug 1.0.1 Frame Control	CC	-	-	1	Contention Control

	DT	-	-	3	Delimiter Type
	VF	-	-	13	Variant Field
	FCCS	-	-	8	Frame Control Check Sequence
HomePlug AV Frame Control Block	DT_AV	0	0 - 2	3	Delimiter Type
	ACCESS		3	1	Access Field
	SNID		4 - 7	4	Short Network Identifier
	VF_AV	1 - 12	-	96	Variant field
	FCCS_AV	13 – 15	-	24	HomePlug AV Frame Control Block Check Sequence

Note: Refer to HomePlug 1.0.1 specification for the bit and octet ordering of the fields in HomePlug 1.0.1 Frame Control.

HomePlug 1.0.1 Frame Control

The HomePlug 1.0.1 Frame Control field includes:

Contention Control (CC)

Delimiter Type (DT)

A variant field based on the Delimiter Type (VF)

A Frame Control Check Sequence (FCCS)

The interpretation of these fields is the same as described in the HomePlug 1.0.1 specification. HomePlug 1.0.1 Frame Control is used in Hybrid Mode and for all Beacon transmissions. As with HomePlug AV, HomePlug GREEN PHY stations manipulate these fields to ensure proper coexistence with HomePlug 1.0.1 stations (see Chapter 9).

Delimiter Type (DT_AV)

Delimiter Type (DT_AV) is a 3-bit field in the Frame Control Block that identifies the delimiter. Table 45 shows the various types of delimiters. The format of HomePlug AV variant fields depends on DT_AV (note: GREEN PHY uses the same variant field as HomePlug AV)

Table 45: Delimiter Type Field Interpretation

DT Value	Interpretation
000	Beacon
001	Start of Frame (SOF)

010	Selective Acknowledgment (SACK)
011	Request to Send (RTS)/Clear to Send (CTS)
100	Sound
101	Reverse Start of Frame (RSOF)
110 - 111	Reserved

Access Field (ACCESS)

Access Field (ACCESS) is a single-bit field in the Frame Control Block that indicates the type of network on which the MPDU was transmitted. The ACCESS field in a SACK, Sound ACK, and CTS delimiters shall be the same as the ACCESS field in the corresponding Data MPDU, Sound MPDU, and RTS, respectively.

Table 46: Access Field Interpretation

ACCESS Value	Interpretation
0b0	MPDU transmitted on an In-Home Network
0b1	MPDU transmitted on an Access Network

Short Network ID (SNID)

Short Network Identifier (SNID) is a 4-bit field in the Frame Control Block that is used to distinguish between MPDUs transmitted by different networks on the same power-line media (refer to Section 7.3.2.1.1). It is a shorthand representation of the Network Identifier (refer to Section 4.4.3.1). It is also used to distinguish between two AVLNs whose NMKs are different, but whose NIDs are the same. The correspondence between a SNID and a Network Identifier is established when both are transmitted in a Beacon MPDU. The SNID field in a SACK, Sound ACK, and CTS delimiters shall be the same as the SNID field in the corresponding Data MPDU, Sound MPDU, and RTS, respectively.

The CCo of an AVLN shall try to ensure that its SNID is not used by any of the Neighboring CCos or by any interfering networks of its Neighboring CCos (refer to Section 8.3.5.1). When the CCo determines that its SNID is being used by a Neighboring CCo or by any interfering networks of its Neighboring CCos, it shall randomly choose a new SNID from the list of SNIDs that are not in use by any Neighboring CCo or by some interfering network of a Neighboring CCo.

The CCo shall indicate the new SNID in the subsequent Central Beacon transmissions using the Change SNID BENTRY (refer to Section 4.4.3.15.4.14.1). Further, the CCo shall include the MAC Address BENTRY when the Change SNID BENTRY is present. All STAs in the AVLN shall continuously monitor the Central/Proxy Beacons and update the SNID associated with the AVLN.

Variant Fields (VF_AV)

The contents of the Variant Fields (VF_AV) in the Frame Control Block depend on the Delimiter Type (DT_AV). The format of these fields for Beacon, Start-of-Frame (SOF), Selective Acknowledgement (SACK), Request to Send/Clear to Send (RTS/CTS), and Sound delimiters is described in the following sections.

Beacon Variant Fields

The Beacon carries 136 octets of the Beacon payload. Table 47 lists the contents of the variant field of a Beacon delimiter. These contents are described in the following subsections. The format of the Beacon MPDU Payload is described in Section 4.4.3.

Table 47: Beacon Variant Fields

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
DT_AV	0	0 - 2	3	0b000 (Delimiter Type)
ACCESS		3	1	Access Field
SNID		4 - 7	4	Short Network Identifier
BTS	1	0 - 7	32	Beacon Time Stamp
	2	0 - 7		
	3	0 - 7		
	4	0 - 7		
BTO(0)	5	0 - 7	16	Beacon Transmission Offset – 0
	6	0 - 7		
BTO(1)	7	0 - 7	16	Beacon Transmission Offset – 1
	8	0 - 7		
BTO(2)	9	0 - 7	16	Beacon Transmission Offset – 2
	10	0 - 7		
BTO(3)	11	0 - 7	16	Beacon Transmission Offset – 3
	12	0 - 7		
FCCS_AV	13	0 - 7	24	Frame Control Check Sequence
	14	0 - 7		
	15	0 - 7		

Beacon Time Stamp (BTS)

Beacon Time Stamp (BTS) is defined as follows:

For the Central Beacon, BTS is the 32-bit value of the CCo's Network Time Base (NTB) at the start of the corresponding Beacon PPDU (refer to Section 5.5).

For the Proxy Beacon, BTS is the value of the NTB at the start of the Proxy Beacon PPDU, as estimated by the PCo.

For a Discover Beacon, BTS is the value of the NTB at the start of the Discover Beacon PPDU, as estimated by the STA transmitting the Beacon.

Beacon Transmission Offset (0 to 3)

Beacon Transmission Offset (0-3) fields are used to announce the offset of future Beacons from their expected location based on the CCo's 25 MHz (refer to Section 5.1). Each Beacon Transmission Offset field is a signed two's complement 16-bit value measured in units of the CCo 25 MHz clock period (i.e., based on the CCo's 25 MHz clock). BTO [0] provides the offset of the first Beacon that follows the current Beacon, BTO [1] provides the offset of the second Beacon that follows the current Beacon, and so on. The number of valid BTOs present in the Beacon is variable. A BTO value of 0x8000 shall be used to indicate that the corresponding BTO is invalid. BTO fields, together with the persistent schedule, enable a station to transmit accurately in its persistent allocation when a Beacon is missed.

The number of valid BTOs presented in a Beacon should, if possible, be chosen such that it is greater than or equal to the maximum persistence of schedule(s) present in the Beacon Payload. This will ensure that the reliability of knowing the Beacon Period Start Time of a Period is at least as good as the reliability of knowing the Persistent Allocation. Refer to Section 5.1.1.2.1 for details about persistent schedules.

Discover and Proxy Beacon shall set the values of BTO[0] through BTO[3] to the same values as the Central Beacon.

Start-of-Frame (SOF) Variant Fields

Long MPDU Start-of-Frame (SOF) control uses one 128-bit Frame Control Block to carry Frame Control information. Table 48 shows the contents of VF_AV fields for the SOF in HomePlug GREEN PHY.

Table 48: HomePlug GREEN PHY Start-of-Frame Variant Fields (same as for HomePlug AV)				
Field	Octet Number	Bit Number	Field Size (Bits)	Definition
DT_AV	0	0 - 2	3	0b001 (Delimiter Type)
ACCESS		3	1	Access Field
SNID		4 - 7	4	Short Network Identifier
STEI	1	0 - 7	8	Source Terminal Equipment Identifier
DTEI	2	0 - 7	8	Destination Terminal Equipment Identifier
LID	3	0 – 7	8	Link Identifier
CFS	4	0	1	Contention-Free Session
BDF		1	1	Beacon Detect Flag
HP10DF		2	1	HomePlug 1.0.1 Detected Flag
HP11DF		3	1	HomePlug 1.1 Detect Flag
EKS		4 - 7	4	Encryption Key Select
PPB	5	0 - 7	8	Pending PHY Blocks
BLE	6	0 - 7	8	Bit Loading Estimate
PBSz	7	0	1	PHY Block Size
NumSym		1 - 2	2	Number of Symbols
TMI_AV		3 - 7	5	Tone Map Index
FL_AV	8	0 - 7	12	Frame Length
	9	0 - 3		
MPDUCnt		4 - 5	2	MPDU Count

BurstCnt		6 - 7	2	Burst Count
BM-SACKI	10	4 - 7	4	Bit Map SACK info for the PBs sent in the Bidirectional Burst Flag
MRTFL		1 - 4	4	Max Reverse Transmission Frame Length
DCPPCF		5	1	Different CP PHY Clock Flag
MCF		6	1	Multicast Flag
MNBF		7	1	Multi-Network Broadcast Flag
RSR	11	0	1	Request SACK Retransmission
CLST		1	1	Convergence Layer SAP Type
MFSCmdMgmt		2 – 4	3	Management MAC Frame Stream Command
MFSCmdData		5 - 7	3	Data MAC Frame Stream Command
MFSRspMgmt	12	0 - 1	2	Management MFS Response for the data sent in the preceding Reverse SOFReverse SOF
MFSRspData		2 - 3	2	Data MFS Response for the data sent in the preceding Reverse SOFReverse SOF

BM-SACKI		4 - 7	4	Bit Map SACK info for the PBs sent in the preceding Reverse SOF
FCCS_AV	13	0 - 7	24	Frame Control Check Sequence
	14	0 - 7		
	15	0 - 7		

Source Terminal Equipment Identifier (STEI)

Source Terminal Equipment Identifier (STEI) is an 8-bit field that is set to the Terminal Equipment Identifier (TEI) assigned to the station transmitting the SOF delimiter.

Source Terminal Equipment Identifier (STEI) for Routing and Repeating (GREEN PHY)

When repeating broadcast MPDUs, this field shall be set to the TEI of the original sender, not the repeater.

Destination Terminal Equipment Identifier (DTEI)

Destination Terminal Equipment Identifier (DTEI) is an 8-bit field. As with HomePlug AV, this field is set to the TEI assigned to the HomePlug GREEN PHY station that is the intended destination of the MPDU.

Link Identifier (LID)

Link Identifier (LID) is an 8-bit field that indicates the Connection to which the MPDU Payload is associated (refer to Section 5.2.1.4).

Contention-Free Session (CFS)

The Contention-Free Session flag is a 1-bit field that indicates whether the SOF MPDU is transmitted in a contention-free or Carrier Sense Multiple Access (CSMA) allocation.

Table 49: Contention-Free Session Interpretation

CFS Value	Interpretation
0b0	SOF MPDU is transmitted in a CSMA allocation.
0b1	SOF MPDU is transmitted in a contention-free allocation.

Beacon Detect Flag (BDF)

Beacon Detect Flag (BDF) is a 1-bit field that indicates whether the station heard the Central Beacon transmission from the CCo of the AVLN to which it is associated during the current period. In Uncoordinated mode and Coordinated mode, this field shall be reset at the start of each Beacon Period, and subsequently updated based on the detection of Central Beacon in the Beacon Region. In CSMA-Only mode (refer to Section 8.1), this field shall be reset to 0b0 if it has been more than 1 Beacon Period duration of time since the Central Beacon was last heard.

Table 410: Beacon Detect Flag Interpretation

BDF Value	Interpretation

0b0	Beacon was not heard.
0b1	Beacon was heard.

HomePlug 1.0.1 Detect Flag (HP10DF)

HomePlug 1.0.1 Detect Flag (HP10DF) is a 1-bit field that indicates whether the station has detected the HomePlug 1.0.1 transmission.

Table 411: HomePlug 1.0.1 Detect Flag Interpretation

HP10DF Value	Interpretation
0b0	No HomePlug 1.0.1 transmissions are detected.
0b1	HomePlug 1.0.1 transmission is detected.

HomePlug 1.1 Detect Flag (HP11DF)

HomePlug 1.1 Detect Flag (HP11DF) is a 1-bit field that indicates whether the station has detected the HomePlug 1.1 transmission.

Table 412: HomePlug 1.1 Detect Flag Interpretation

HP11DF Value	Interpretation
0b0	No HomePlug 1.1 transmissions are detected.
0b1	HomePlug 1.1 transmission is detected.

Encryption Key Select (EKS)

Encryption Key Select (EKS) is a 4-bit field that is the Index of the Encryption Key used for encrypting segments. It is not to be confused with the Payload Encryption Key Select (PEKS), which is used to identify the Encryption Key used for MME Payloads. This field is only unambiguous when it is associated with the SNID of the AVLN.

Table 413: Encryption Key Select Interpretation

EKS Value	Interpretation
0b0000 - 0b0111	CCo Managed NEKs (AES 128-bit keys)
0b1000 - 0b1110	Reserved
0b1111	Indicates that MPDU segments are unencrypted.

Encryption Key Select (EKS) for GREEN PHY

GREEN PHY uses formerly reserved EKS Values to indicate a PPEK. When a PPEK is indicated, the key is distinguished by the STEI and DTEI.

Table 413b: Assignment of Previously Reserved Encryption Key Select Values for GREEN PHY

EKS Value	Interpretation
0b1000 - 0b1001	PPEKs (AES 128-bit keys)
0b1010 - 0b1110	Reserved

Pending PHY Blocks (PPB)

For unicast MPDUs, and broadcast MPDUs transmitted by the original source, Pending PHY Blocks (PPB) is an 8-bit field that contains the total number of PHY blocks pending transmission at the completion of the current MPDU (i.e., it does not include any PHY Blocks (PBs) contained in the current MPDU). PHY blocks pending transmission include previously untransmitted blocks and blocks awaiting retransmission.

The PPB is coded using an 8-bit floating-point format, with a 4-bit mantissa and a 4-bit exponent. The mantissa is transmitted in the most-significant four bits of the field, with the exponent transmitted in the least-significant four bits of the field (see Equation 41).

Equation 41: PPB Formula
The PPB can be reconstructed from the exponent and mantissa values using the formula in Equation 42.

Equation 42: Formula for Reconstructing the PPB Exponent and Mantissa Values

Pending PHY Blocks (PPB) (GREEN PHY)

A GREEN PHY station shall set the Pending PHY Blocks (PPB) field in the SOF as follows:

- if the MCF indicates broadcast, and the MPDU is being repeated by a STA other than the original source, then the PPB field shall contain the value **0xFF**.
- if the channel access priority used for PRS signaling is CAP1, CAP2 or CAP3, then the PPB field shall be set to 0xEF
- if the channel access priority used for PRS signaling is CAP0, then the PPB field shall be set to 0xDF

Bit Loading Estimate (BLE)
For unicast MPDUs, and broadcast MPDUs transmitted by the original source, Bit Loading Estimate (BLE) is an 8-bit field that represents the number of user data bits (i.e., data bit prior to Forward Error Correction (FEC) encoding) that can be carried on the channel per microsecond. It takes into account the overhead due to the cyclic prefix and FEC, but does not include overhead associated with the PPDU format (e.g., delimiter) and IFS. It shall be calculated using the formula in Equation 43.
In Equation 43:
T_S represents the symbol length in μs (including GI).
R represents the FEC code rate.
$P_{pb,error}$ indicates the PB error rate. $P_{pb,\ error}$ shall be chosen based on expected PB error rate on the Link when a new Tone Map is generated and shall remain fixed until the Tone Map becomes invalidated by a newer Tone Map.

Equation 43: Formula for Calculating the BLE
The BLE is coded for transmission in the variant field of the SOF MPDU using an 8-bit floating-point format. This format comprises a 5-bit mantissa and a 3-bit exponent. The mantissa is transmitted in the most-significant five bits of the field, with the exponent transmitted in the least-significant three bits of the field (see Equation 44).
Note: The BLE is constant for a given TMI.

Equation 44: BLE Formula
The BLE can be reconstructed from the exponent and mantissa values using the formula in Equation 45.

Equation 45: Formula for Reconstructing the BLE Exponent and Mantissa Values

Bit Loading Estimate (BLE) for Routing and Repeating (GREEN PHY)

When MCF indicates broadcast, and the MPDU is being repeated by a STA other than the original source, then BLE shall contain the TEI of the STA repeating the MPDU.

PHY Block Size (PBSz)

PHY Block Size (PBSz) is a 1-bit field that indicates the MPDU Payload block size.

Table 414: PHY Block Size Interpretation

PBSz Value	Interpretation
0b0	MPDU Payload contains a PHY block size of 520 octets.
0b1	MPDU Payload contains a PHY block size of 136 octets.

Number of Symbols (NumSym)

Number of Symbols (NumSym) is a 2-bit field that indicates the number of OFDM Symbols used for transmitting the MPDU Payload. The Receiver uses the Number of Symbols field to determine the RIFS_AV used in this transmission. When there are no payload symbols transmitted along with a SOF (i.e., NumSym = 0b00), the Response Interframe Spacing of the RIFS_AV_default shall be used.

Table 415: Number of Symbols Interpretation

NumSym Value	Interpretation
0b00	No MPDU Payload carrying OFDM Symbols is present.
0b01	One OFDM Symbol is used for transmitting the MPDU Payload.
0b10	Two OFDM Symbols are used for transmitting the MPDU Payload.
0b11	More than two OFDM Symbols are used for transmitting the MPDU Payload.

Tone Map Index (TMI_AV)

Tone Map Index (TMI_AV) is a 5-bit field that indicates the Tone Map to be used by the receiver in demodulating the MPDU Payload.

Table 416: Tone Map Index Interpretation

TMI_AV Value	Interpretation
0b00000	ROBO_AV Modulation
0b00001	High-Speed ROBO_AV Modulation
0b00010	Payload is modulated using Mini-ROBO Modulation. Mini-ROBO Modulation is also used for Beacon payload transmission.
0b00011	Reserved

0b00100 - 0b11111	Used to index the negotiated TMs. Within the receiver, the TMI_AV must be combined with the received STEI to uniquely determine the Tone Map. This range of values is not required for GREEN PHY stations.

Tone Map Index (TMI_AV) for GREEN PHY

A station that only implements GREEN PHY is only required to support TM__AV = 0b00000, 0b00001, and 0b00010 (ROBO modulation).

Frame Length (FL_AV)

Frame Length (FL_AV) is a 12-bit field that indicates the duration of MPDU Payload and the interframe space (BIFS or RIFS_AV) that follows the MPDU Payload. Table 417 shows the interpretation of this field. FL_AV is measured as the largest multiple of 1.28 µsec that is smaller than the duration from the last non-zero sample of the SOF delimiter to the first non-zero sample at the beginning of the preamble of the subsequent transmission.

For an MPDU with MPDUCnt set to 0b01, 0b10, or 0b11, FL_AV indicates the duration of the MPDU Payload and the following Burst Interframe Spacing (BIFS).

For an MPDU with MPDUCnt set to 0b00, FL_AV indicates the duration of MPDU Payload and the following Response Interframe Spacing (RIFS_AV).

Figure 411 shows the measurement of the FL_AV parameter.

Figure 411: Measurement of FL_AV

Note: RIFS_AV is a variable duration of time, based on the Tone Map used for modulating the MPDU Payload and the number of Orthogonal Frequency Division Multiplexing (OFDM) symbols used for carrying the MPDU Payload (refer to Section 5.6). The station(s) that is the intended destination of the MPDU Payload can use its knowledge of RIFS_AV to determine the duration of MPDU Payload. All other stations use FL_AV to determine the location of the Response delimiter.

The maximum value of FL_AV that can be used by the transmitter depends on the:

MaxFL_AV that the receiver can support.

MaxFL_AV that the transmitter can support.

HomePlug 1.0.1 Coexistence operating mode.

Whether the Long MPDU transmission is part of CSMA allocation or contention-free allocation.

As with HomePlug AV, a HomePlug GREEN PHY station shall be capable of supporting transmission and reception of an MPDU with a MaxFL_AV of at least 2501.12 sec. Ability to support larger FL_AV values is optional. Channel Estimation Indication (refer to Section 11.5.10) is used by the receiver to indicate the maximum value of FL_AV, MaxFL_AV that it is capable of receiving. The transmitter shall not transmit MPDUs with FL_AV value larger than the MaxFL_AV that the receiver is capable of receiving. All broadcast/multicast transmission shall not use FL_AV values that exceed 2501.12 sec.

As with HomePlug AV, in Hybrid Mode, the maximum value of FL_AV is further restricted to ensure that the HomePlug GREEN PHY MPDU transmission duration (including the response, if

any, and subsequent Interframe Spaces) does not exceed the EIFS time duration. Refer to Chapter 9 for information about HomePlug 1.0.1 coexistence.
During CSMA allocations, the maximum value of FL_AV that can be used shall be less than or equal to 2501.12 sec. This restriction is intended to reduce the cost of collisions during CSMA channel access.
Table 417: Frame Length Interpretation

FL_AV Value	Interpretation
0x000 – 0x03D	Reserved
0x03E – 0xFFF	Payload Length in multiples of 1.28 µsec

MPDU Count (MPDUCnt)
MPDU Count (MPDUCnt) is a 2-bit field that indicates the number of MPDUs to expect in the current burst transmission. Up to four MPDUs can be supported in a Burst. While this number indicates the upper limit, the actual number of MPDUs supported by a station depends on channel conditions and station capabilities.
Table 418: MPDU Count Interpretation

MPDUCnt Value	Interpretation
0b00	The MPDU either is not part of a burst or is the last MPDU of a burst.
0b01	One more MPDU is to follow, and so on.

Burst Count (BurstCnt)
Burst Count (BurstCnt) is a 2-bit field that is incremented after each MPDU burst is transmitted on the media for a particular Global Link; that is, it is incremented after transmission of a SOF with a specific GLID, with MPDUCnt = 0 and RSR = 0b0. The Burst Count value for a Global Link is not affected by transmissions for other Global Links. For Local Links and Priority Links, the Burst Count field shall be set to 0b00. Refer to Section 5.2.1 for more information about Local Links, Global Links, and Priority Links.
The BurstCnt field is used by the station receiving the SOF MPDU to resolve ambiguities in the request SACK retransmission protocol, as described in Section 5.4.8.1.1.
Bidirectional Burst Flag (BBF)
The Bidirectional Burst Flag (BBF) indicates that a Bidirectional Burst may continue after this MPDU. When this flag is set to 0, the receiver shall terminate the bidirectional burst with a SACK.
Table 419: Bidirectional Burst Flag Interpretation

BBF Value	Interpretation
0b0	The bidirectional burst shall terminate with a SACK after this MPDU
0b1	The bidirectional burst may continue after this MPDU

Maximum Reverse Transmission Frame Length (MRTFL)
The Maximum Reverse Transmission Frame Length (MRTFL) indicates the maximum frame length a receiver may use in a Reverse SOF. Table 420 shows the interpretation of the MRTFL field. This field is only valid when the Bidirectional Burst Flag (BBF) is set to 0b1.

Table 420: Maximum Reverse Transmission Frame Length Interpretation

MRTFL Value	Interpretation
0x0	163.84 µsec frame length
0x1	204.80 µsec frame length
0x2	245.76 µsec frame length
0x3	286.72 µsec frame length
0x4	327.68 µsec frame length
0x5	409.60 µsec frame length
0x6	491.52 µsec frame length
0x7	573.44 µsec frame length
0x8	655.36 µsec frame length
0x9	819.20 µsec frame length
0xa	983.04 µsec frame length
0xb	1146.88 µsec frame length
0xc	1310.72 µsec frame length
0xd	1638.40 µsec frame length
0xe	1966.08 µsec frame length
0xf	2293.76 µsec frame length

Different CP PHY Clock Flag (DCPPCF)

Different CP PHY Clock Flag (DCPPCF) is a 1-bit field that shall be set to 0b1 when the station uses a different PHY Receive Clock Correction during the Contention Period (CP) than the Short Network Identifier (SNID) indicated in the SOF. Otherwise, it shall be set to 0b0. This can occur when a station is associated with more than one network and uses the PHY Receive Clock Correction of another network during the CP. Any unicast MPDU to this station during the CP must use RTS/CTS to notify the receiver to apply the correct PHY Receive Clock Correction for the network identified by the SNID in the RTS. Also, refer to Section 5.5.4.1.

Different CP PHY Clock Flag (DCPPCF) for GREEN PHY

It is optional for a station that only implements Green PHY to interpret the DCPPCF field.

If the Green PHY station supports the interpretation of DCPPCF, its behavior is identical to that described in Section 4.4.1.5.2.19.

If the Green PHY station does not support the interpretation of DCPPCF field, it will not send RTS/CTS to notify the receiver to apply the correct PHY Receive Clock Correction.

Multicast Flag (MCF)

Multicast Flag (MCF) is a 1-bit field that indicates whether the Long MPDU Payload contains multicast/broadcast or unicast information.

Table 421: Multicast Flag Interpretation

MCF Value	Interpretation
0b0	The Long MPDU Payload contains unicast information.
0b1	The Long MPDU Payload contains multicast/ broadcast information.

Multi-Network Broadcast Flag (MNBF)

Multi-Network Broadcast Flag (MNBF) is a 1-bit field that indicates the MPDU is a broadcast to all stations regardless of the SNID or network association. The payload of a multi-network broadcast MPDU shall be limited to one segment and shall only contain MAC Management Messages. MSDU data is not allowed in a multi-network broadcast MPDU. The PHY Block Body shall be unencrypted and the EKS shall be set to 0b1111. The Multicast Flag (MCF) shall be set to 0b1 when MNBF is set.

For multi-network broadcast MPDUs, RTS/CTS shall be used to notify receiving stations to apply the correct PHY Receive Clock Correction for the network identified by the SNID in the RTS. If a proxy station is not available, a CTS is not required to transmit the MPDU following the RTS, and the TEI shall be set to the broadcast TEI.

Request SACK Retransmission (RSR)

Request SACK Retransmission (RSR) is a 1-bit field that is used to recover from a missing SACK MPDU on Global Links. The Request SACK Retransmission procedure is described in Section 5.4.8.1.1.

Table 422: Request SACK Retransmission Interpretation

RSR Value	Interpretation
0b0	The transmitter is not requesting retransmission of the SACK information.
0b1	The transmitter is requesting retransmission of the SACK information. The LID field shall contain a Global Link ID (GLID) and the BurstCnt field shall contain the most recent value transmitted for this GLID. Upon receiving this MPDU, the receiver shall transmit (or retransmit) the SACK information for the most recently received burst, as described in Section 5.4.8.1.1.

Convergence Layer SAP Type (CLST)

Convergence Layer SAP Type (CLST) is a 1-bit field that indicates the Convergence Layer SAP for which the current MPDU Payload is designated. The MAC receiver uses this information to reassemble and route the MSDUs to the correct Convergence Layer SAPs.

Table 423: Convergence Layer SAP Type

CLST Value	Interpretation
0b0	Ethernet II-class SAP
0b1	Reserved

Management MAC Frame Stream Command (MFSCmdMgmt)

Management MAC Frame Stream Command (MFSCmdMgmt) is a 3-bit field that contains the command from the transmitter's Management MAC Frame Stream to the corresponding reassembly stream at the receiver(s). Table 424 shows the interpretation of this field. For more information, refer to Section 5.4.1.6.

Table 424: Data and Management MAC Frame Stream Command

Interpretation

MFSCmdData, MFSCmdMgmt Value	Interpretation
0b000	INIT
0b001	IN_SYNC
0b010	RE_SYNC
0b011	RELEASE
0b100	NOP (No Operation)
Others	Reserved

Data MAC Frame Stream Command (MFSCmdData)

Data MAC Frame Stream Command (MFSCmdData) is a 3-bit field that contains the command from the transmitter's Data MAC Frame Stream to the corresponding reassembly stream at the receiver(s). Table 424 shows the interpretation of this field. For more information, refer to Section 5.4.1.6.

Management MAC Frame Stream Response (MFSRspMgmt)

Management MAC Frame Stream Response (MFSRspMgmt) is a 2-bit field that contains the response from the receiver's Management MAC Frame stream to the corresponding command (MFSCmdMgmt) from the transmitter in the Reverse SOF. Table 429 shows the interpretation of this field.

Data MAC Frame Stream Response (MFSRspData)

Data MAC Frame Stream Response (MFSRspData) is a 2-bit field that contains the response from the receiver's Data MAC Frame stream to the corresponding command (MFSCmdData) from the transmitter in the Reverse SOF. Table 429 shows the interpretation of this field.

Bit Map SACK Information (BM-SACKI)

The BM-SACKI field in the SOF acknowledges the PBs transmitted in the previous Reverse SOF. LSB indicates the reception status of the first PB and so on. A value of 0b0 indicates successful reception. BM-SACK field set to 0b0000 or 0b1111 has special interpretation as described below.

BM-SACK field set to 0b0000 shall indicate that all PBs transmitted in the corresponding Reverse SOF have been successfully received. Thus, if four or more PBs are transmitted in the corresponding Reverse SOF, and all of them were successfully received, the receiver shall set the BM-SACK field to 0b0000.

BM-SACK field set to 0b1111 shall indicate that all PBs transmitted in the corresponding Reverse SOF have been corrupted. Thus, if four or more PBs are transmitted in the corresponding Reverse SOF, and all of them were corrupted, the receiver shall set the BM-SACK field to 0b1111.

When more than 4 PBs are transmitted in the corresponding Reverse SOF and the original transmitter receives them with mixture of good and bad PBs, it shall send a SACK instead of a SOF (refer to Section 5.4.7).

MFSRspData and MFSRspMgmt shall be set to ACK and the BM-SACKI field set to 0b1111 in all SOFs other than the SOFs transmitted following the successful reception of a Reverse SOF.

Selective Acknowledgement (SACK) Variant Field

As with HomePlug AV, HomePlug GREEN PHY uses Selective Acknowledgements (SACKs) to indicate the need for selective retransmission of PBs received incorrectly. The receiver sends a

SACK in response to a SOF MPDU, with MPDUCnt = 0b00. Reception of HomePlug AV SOF with Request SACK Retransmission shall cause the receiver to generate a SACK response. Table 425 shows the various fields in the SACK response.

Table 425: Selective Acknowledgement Variant Field

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
RxWSz	-	-	4	Receive Window Size Only present for Priority Link; otherwise, 0b010 (Delimiter Type)
DT_AV	0	0 - 2	3	SackD and/or Access Field
ACCESS		3	1	
SNID		4 - 7	4	Short Network Identifier
DTEI	1	0 - 7	8	Destination Terminal Equipment Identifier
CFS	2	0	1	Contention-Free Session
BDF		1	1	Beacon Detect Flag
SVN		2	1	SACK Version Number
RRTF		3	1	Request Reverse Transmission Flag
MFSRspData		4 - 5	2	Data MAC Frame Stream Response
MFSRspMgmt		6 - 7	2	Management MAC Frame Stream Response
SackD	-		Var	Sack Data
BitPad	-		Var	Bit Pad

SACKI[1]	-	-	Var	SACK Receive Window Information for Size
RxWSz	-	-	4	Only present for Priority Link; otherwise, available for SackD and/or BitPad
RRTL	12	4 – 7	4	Request Reverse Transmission Length Only present If RRTF is set to 0b1; otherwise, available for SackD and/or BitPad
FCCS_AV	13	0 - 7	24	Frame Control Check Sequence
	14	0 - 7		
	15	0 - 7		

Table 426: SACK Data Variant Field

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
SACKT[3]	0	0 - 1	2	SACK Type for MPDUCnt 0b11
SACKT[2]		2 - 3	2	SACK Type for MPDUCnt 0b10
SACKT[1]		4 - 5	2	SACK Type for MPDUCnt 0b01
SACKT[0]		6 - 7	2	SACK Type for MPDUCnt 0b00
SACKI[3]	-	-	Var	SACK Information for MPDUCnt 0b11
SACKI[2]	-	-	Var	SACK Information for MPDUCnt 0b10

SACKI[1]	-	-	Var	SACK Information for MPDUCnt 0b01
SACKI[0]	-	-	Var	SACK Information for MPDUCnt 0b00

Destination Terminal Equipment Identifier (DTEI)

Destination Terminal Equipment Identifier (DTEI) is an 8-bit field. As with HomePlug AV, the value in this field is set to the TEI assigned to the HomePlug GREEN PHY station that is the intended destination of the SACK.

Contention-Free Session (CFS)

Contention-Free Session is a 1-bit field that indicates whether the SACK MPDU is transmitted in a contention-free or CSMA allocation.

Table 427: Contention-Free Session Interpretation

CFS Value	Interpretation
0b0	SACK MPDU is transmitted in a CSMA allocation.
0b1	SACK MPDU is transmitted in a contention-free allocation.

Beacon Detect Flag (BDF)

Beacon Detect Flag (BDF) is a 1-bit field that indicates whether the station heard the Central Beacon transmission from the CCo of the AVLN to which it is associated during the current period. The setting and interpretation of this field is the same as the corresponding BDF field in Section 4.4.1.5.2.5 and Table 410.

SACK Version Number (SVN)

SACK Version Number (SVN) is a 1-bit field that indicates the version of the SACK Variant field. As with HomePlug AV, this version of HomePlug GREEN PHY Stations shall set this field to 0b0 on transmit and ignore it on receive.

Request Reverse Transmission Flag (RRTF)

The Request Reverse Transmission Flag (RRTF) indicates that the receiver is requesting the transmitter initiates and/or continues a bidirectional burst. Setting this flag to 0b1 indicates the presence of the Request Reverse Transmission Length (RRTL) field in the SACK.

Table 428: Request Reverse Transmission Flag Interpretation

RRTF Value	Interpretation
0b0	Reverse transmission not requested; RRTL field not present
0b1	Reverse transmission requested; RRTL field present

Data MAC Frame Stream Response (MFSRspData)

Data MAC Frame Stream Response (MFSRspData) is a 2-bit field that contains the response from the receiver's Data MAC Frame stream to the corresponding command (MFSCmdData) from the transmitter. Table 429 shows the interpretation of this field. For more information, refer to Section

5.4.1.6.

Management MAC Frame Stream Response (MFSRspMgmt)

Management MAC Frame Stream Response (MFSRspMgmt) is a 2-bit field that contains the response from the receiver's Management MAC Frame stream to the corresponding command (MFSCmdMgmt) from the transmitter. Table 429 shows the interpretation of this field. For more information, refer to Section 5.4.1.6.

Table 429: Data and Management MAC Frame Stream Response Interpretation

MFSRspData and MFSRspMgmt Value	Interpretation
0b00	ACK
0b01	NACK
0b10	FAIL
0b11	HOLD

SACK Data (SACKD)

SACK Type (SACKT[3] – SACKT[0])

SACK Type (SACKT[3] – SACKT[0]) indicates the interpretation of the SACKI field for the MPDUs for which the SACKT applies (refer to Table 426). There are four SACK Type fields present in each SACK. SACKT[i] indicates the reception status of the MPDU with MPDUCnt =i in the burst. Consequently, SACKT[0] indicates the reception status of the last MPDU in the burst. Table 430 shows the interpretation of the value in the SACK Type field.

Note: In instances where the MPDU corresponding to SACKT[i] is not received (and potentially not transmitted by the sender), the corresponding SACKT value will be set to 0b10.

Table 430: SACK Type Interpretation

SACKT Value	Interpretation
0b00	Mixed – Bit Map SACK Information
0b01	Mixed – Compressed Bit Map SACK Information
0b10	MPDU was not received (i.e., either no Preamble was detected or a corrupt Frame Control was detected).
0b11	Uniform – See SACKI

SACK Information (SACKI[3] – SACKI[0])

The interpretation of SACK Information (SACKI[3] – SACKI[0]) depends on the corresponding SACK Type (SACKT) field. In all mixed-error encodings:

If there are insufficient bits in the encoding to represent all PBs transmitted for an MPDU, the remaining PBs whose status could not be represented shall all be considered to be in error.

If there are insufficient bits to represent one or more entire MPDUs after encoding the first ones, all the PBs in the MPDUs that could not be represented shall be considered to be in error.

Note: This arrangement can cause the encoder to between the two encoding methods to determine which one causes the least harm.

Bit Map SACK Information (SACKT = 0b00)

When SACKT is set to 0b00 (Mixed - Bit Map Information with Group Size One), the SACK Information shall indicate the reception status of each PB using a separate bit.
A value of 0b0 indicates that the corresponding PB is received successfully.
A value of 0b1 indicates errors.
PBs shall be acknowledged in the order they are received. Consequently, the first PB in the MPDU shall be the first PB to be acknowledged in the SACKI.
Compressed Bitmap SACK Information (SACKT=0b01)
When SACKT is set to 0b01 (Mixed Errors – Compressed), the SACKI field shall compress the bit map that otherwise would be sent as Bit Mapped (i.e., SACKI for SACKT = 0b00). Table 431 lists the mapping from the uncompressed bit map pattern to the code sent, and from the code received to the uncompressed bit map pattern. If the SACKI field has too few bits to encode the entire bit map, all the PBs after the last pattern encoded shall be considered to be bad. If the SACKI bits remaining are insufficient to represent the complete compressed code word, the encoder shall send a proper prefix of a valid code. The decoder shall ascertain that the compressed code word received is incomplete and shall consider all remaining bits of the bitmap to be 0b1. For example, if only two bits of SACKI remain with which to encode, and there are three remaining bitmap bits with values 0b010, the encoder shall send 0b01. The decoder shall recognize that this is not a complete compressed code word and shall assume that all the remaining PBs in the MPDU were not properly received.
Note: The LSB in the Table 431 corresponds to the first bit encountered in the stream (refer to Section 4.1).

Table 431: SACKI Field for Mixed Errors – Compressed (SACKT = 0b01)

Compression		Decompression	
Bit Map Pattern In	Compression Code Sent	Compression Code Received	Bit Map Pattern Out
0b11	0b11111	0b0	0b0000
0b101	0b101111	0b001	0b010
0b001	0b011	0b101	0b100
0b110	0b001111	0b011	0b001
0b010	0b001	0b0111	0b1000
0b100	0b101	0b001111	0b110
0b1000	0b0111	0b101111	0b101
0b0000	0b0	0b11111	0b11

If there are sufficient bits to encode all the PB status bits in an MPDU, but the compressed encoding must represent more bits than are required, the bit map may be padded by the encoder. All of the bits “encoded” in excess of the number of PBs in the corresponding MPDU shall be ignored on decoding and may take any convenient value during encoding. For example, if the last two bits of a bitmap corresponding to an MPDU remain to be encoded using the Compressed method and have a value of 0b00, any one of the three codes 0b101, 0b0111, or 0b0 (which correspond to bitmap values 0b100, 0b1000, and 0b0000, respectively) may be used. The encoder would be most efficient if the last encoding were used, since it only requires a single bit.

Uniform SACK Information (SACKT=0b11)
If SACKT is 0b11 (Uniform), the corresponding SACKI field is a 4-bit field that indicates the reception status for all PBs in the MPDU, as shown in Table 432.
Table 432: SACKI for Uniform (SACKT = 0b11)

SACKI	Interpretation
0b0000	All PBs received with errors.
0b0001	All PBs received correctly
0b0010	SACK Information not available (for use in RSR response)
0b0011	The TMI_AV used for the MPDU is invalid. • If TMI_AV corresponds to an AC Line Cycle adapted Tone Map, the transmitter should treat the intervals in the Beacon Period where the corresponding TMI_AV is being used as intervals without AC line cycle adapted Tone Map and not as Unusable intervals (refer to Section 11.5.10). • If TMI_AV corresponds to a Default Tone Map, the transmitter should use ROBO_AV Tone Map in place of Default Tone Map.
0b0100	The TMI_AV used for the MPDU is invalid. • If TMI_AV corresponds to an AC Line Cycle adapted Tone Map, the transmitter should treat the intervals in the Beacon Period where the corresponding TMI_AV is being used as intervals without AC line cycle adapted Tone Map and not as Unusable intervals (refer to Section 11.5.10). • If TMI_AV corresponds to a Default Tone Map, the transmitter should invalidate all Tone Maps and restart the initial channel estimation procedure.
0b0101	The TMI_AV used for the MPDU is invalid. Invalidate all Tone Maps and reinitiate the initial channel estimation procedure.
0b0110	PHY Block Decryption Error This failure code indicates that the receiver did not have the proper NEK to decrypt the PHY Blocks.

0b0111 – 0b1111	Reserved

Bit Pad (BitPad)

BitPad is a variable-length field that ensures the SACK MPDU Frame Control is 16 octets long.

Receive Window Size (RxWSz)

Receive Window Size (RxWSz) is a 4-bit field that indicates the reassembly buffer available for the corresponding MAC Frame Stream at the receiver. The Receive Window Size field is only present in the SACK data variant field of Local Links and Priority Links. Coding of this field is shown in Table 433.

Table 433: Receive Window Size Interpretation

RxWSz Value	Interpretation
0x0	4 segments of reassembly buffer are available
0x1	8 segments of reassembly buffer are available
0x2	16 segments of reassembly buffer are available
0x3	24 segments of reassembly buffer are available
0x4	32 segments of reassembly buffer are available
0x5	48 segments of reassembly buffer are available
0x6	64 segments of reassembly buffer are available
0x7	80 segments of reassembly buffer are available
0x8	96 segments of reassembly buffer are available
0x9	112 segments of reassembly buffer are available
0xA	128 segments of reassembly buffer are available
0xB	144 segments of reassembly buffer are available
0xC	160 segments of reassembly buffer are available
0xD	192 segments of reassembly buffer are available
0xE	224 segments of reassembly buffer are available
0xF	256 segments of reassembly buffer are available

Request Reverse Transmission Length (RRTL)

The Request Reverse Transmission (RRTL) is a 4-bit field that specifies the minimum required duration for a Reverse Transmission. The RRTL shall include the payload duration as well as the subsequent RIFS_AV that is being requested for the reverse transmission. Table 434 shows the interpretation of the RRTL field.

The Request Reverse Transmission Length field is only present if the Request Reverse Transmission Flag field is set to 0b1.

Table 434: Request Reverse Transmission Length Interpretation

RRTL Value	Interpretation
0x0	163.84 µsec frame length
0x1	204.80 µsec frame length
0x2	245.76 µsec frame length
0x3	286.72 µsec frame length
0x4	327.68 µsec frame length
0x5	409.60 µsec frame length
0x6	491.52 µsec frame length
0x7	573.44 µsec frame length
0x8	655.36 µsec frame length
0x9	819.20 µsec frame length
0xa	983.04 µsec frame length
0xb	1146.88 µsec frame length
0xc	1310.72 µsec frame length
0xd	1638.40 µsec frame length
0xe	1966.08 µsec frame length
0xf	2293.76 µsec frame length

Request to Send/Clear to Send (RTS/CTS) Variant Field

Table 435 shows the Request to Send/Clear to Send (RTS/CTS) variant field.

Table 435: Request to Send/Clear to Send Variant Field

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
DT_AV	0	0 - 2	3	0b011 (Delimiter Type)
ACCESS		3	1	Access Field
SNID		4 - 7	4	Short Network Identifier
STEI	1	0 - 7	8	Source Terminal Equipment Identifier
DTEI	2	0 - 7	8	Destination Terminal Equipment Identifier
LID	3	0 - 7	8	Link Identifier
CFS	4	0	1	Contention-Free Session
BDF		1	1	Beacon Detect Flag

HP10DF		2	1	HomePlug 1.0.1 Detect Flag
HP11DF		3	1	HomePlug 1.1 Detect Flag
RTSF		4	1	RTS Flag
IGF		5	1	Immediate Grant Flag
MNBF		6	1	Multi Network Broadcast Flag
MCF		7	1	Multicast Flag
DUR	5	0 - 7	14	Duration
	6	0 - 5		
RSVD		6 - 7	50	Reserved
	7	0 - 7		
	8	0 - 7		
	9	0 - 7		
	10	0 - 7		
	11	0 - 7		
	12	0 - 7		
FCCS_AV	13	0 - 7	24	Frame Control Check Sequence
	14	0 - 7		
	15	0 - 7		

Source Terminal Equipment Identifier (STEI)
Source Terminal Equipment Identifier (STEI) is an 8-bit field that is set to the TEI assigned to the station transmitting the RTS/CTS.
Destination Terminal Equipment Identifier (DTEI)
As with HomePlug AV, Destination Terminal Equipment Identifier (DTEI) is an 8-bit field that is set to the TEI assigned to the HomePlug GREEN PHY station that is the intended destination of the RTS/CTS.
Link Identifier (LID)
The interpretation of the Link Identifier (LID) field is the same as the corresponding Link Identifier (LID) field in Section 4.4.1.5.2.3.
Contention-Free Session (CFS)
Contention-Free Session (CFS) is a 1-bit field that indicates whether the RTS/CTS MPDU is transmitted in a CSMA or contention-free allocation.
Table 436: Contention-Free Session Interpretation

CFS Value	Interpretation
0b0	RTS/CTS MPDU is transmitted in a CSMA allocation.
0b1	RTS/CTS MPDU is transmitted in a contention-free allocation.

Beacon Detect Flag (BDF)
The interpretation of the Beacon Detect Flag (BDF) field is the same as the corresponding Beacon Detect Flag (BDF) field in Section 4.4.1.5.2.5.
HomePlug 1.0.1 Detect Flag (HP10DF)
The interpretation of the HomePlug 1.0.1 Detect Flag (HP10DF) field is the same as the corresponding HomePlug 1.0.1 Detect Flag (HP10DF) field in Section 4.4.1.5.2.6.
HomePlug 1.1 Detect Flag (HP11DF)
The interpretation of the HomePlug 1.1 Detect Flag (HP11DF) field is the same as the corresponding HomePlug 1.1 Detect Flag (HP11DF) field in Section 4.4.1.5.2.7.
RTS Flag (RTSF)
RTS Flag (RTSF) is a 1-bit field that indicates whether the corresponding MPDU is a CTS or RTS MPDU.
Table 437: RTS Flag Interpretation

RTSF Value	Interpretation
0b0	Corresponding MPDU is a CTS MPDU.
0b1	Corresponding MPDU is a RTS MPDU.

Immediate Grant Flag (IGF)
Immediate Grant Flag (IGF) is a 1-bit field that is set to 0b1 in the RTS to indicate that the receiver is provided with a reverse transmission for the duration indicated in the DUR field. This mechanism is used by the CCo to provide transmission opportunities to stations during the Contention Free Period Initiation (CFPI) (refer to Section 9.6.1.1).
For regular RTS/CTS transmissions, IGF shall be set to 0b0. IGF in the CTS shall be the same as the IGF in the corresponding RTS.

Multi-Network Broadcast Flag (MNBF)
The interpretation of the Multi-Network Broadcast Flag (MNBF) field is the same as the corresponding Multi-Network Broadcast Flag (MNBF) field in Section 4.4.1.5.2.21.
Multicast Flag (MCF)
Multicast Flag (MCF) is a 1-bit field that indicates whether the Long MPDU Payload in the Long MPDU to follow contains multicast/broadcast or unicast information. Multicast Flag is used as part of Partial Acknowledgment mechanism (refer to Section 5.4.8.3). The interpretation of this field is shown in Table 421.
Duration (DUR)
Duration (DUR) is a 14-bit field that indicates the duration of medium reservation in multiples of 1.28 s. The interpretation of this field depends on the Immediate Grant Flag (IGF). Regardless of the IGF field value, the RTS and CTS shall be separated by RTS-to-CTS Gap (RCG). However the gap between CTS and the subsequent transmission will depend on the IGF field.
When the IGF is set to 0b0 and a Long MPDU or a Burst of Long MPDUs follows an RTS or CTS transmission, the Duration field is measured from the end of the corresponding RTS or CTS until the end of the SACK. In this case, the CTS and start of the first or only MPDU in Burst transmission shall be separated by CTS-to-MPDU Gap (CMG).
Figure 412 shows the meaning of the DUR field for RTS and CTS when IGF is set to 0b0 and a burst of two MPDUs follows the RTS/CTS.
When the IGF is set to 0b0 and a stand-alone RTS/CTS is used (i.e., RTS/CTS without a Long MPDU), the DUR field in RTS is set to indicate the end of CTS and the DUR field in CTS is set to zero. During CSMA allocations, the end of CTS and the start of subsequent Priority Resolution Period shall be separated by CMG. During contention free allocations, the end of CTS and the start of subsequent transmission shall be separated by a minimum of CMG.
When the IGF is set to 0b1, the DUR field indicates the maximum duration of time that is allocated for the receiver. All transmissions from the receiver, including the SACK should be completed within the allocated time. In this case, the end of CTS and the start of subsequent transmission shall be separated by a minimum of CMG.
Figure 413 shows the meaning of DUR field for RTS and CTS, when the IGF is set to 0b1 and the receiver transmits a single MPDU during the allocation time.

Figure 412: Duration Field in RTS/CTS When IGF is Set to 0b0

Figure 413: Duration Field in RTS/CTS When IGF is Set to 0b1
Sound Variant Field
The Sound MPDU is used during channel estimation to estimate the characteristics of the channel. Table 438 shows the contents of the Sound MPDU variant field. Many of these fields are the same as those in the SOF variant field.

Table 438: Sound MPDU Variant Field

Field	Octet Number	Bit Number	Field Size (Bits)	Definition

DT_AV	0	0 - 2	3	0b100 (Delimiter Type)
ACCESS		3	1	Access Field
SNID		4 - 7	4	Short Network Identifier
STEI	1	0 - 7	8	Source Terminal Equipment Identifier
DTEI	2	0 - 7	8	Destination Terminal Equipment Identifier
LID	3	0 - 7	8	Link Identifier
CFS	4	0	1	Contention-Free Session
PBSz		1	1	PHY Block Size
BDF		2	1	Beacon Detect Flag
SAF		3	1	Sound ACK Flag
SCF		4	1	Sound Complete Flag
REQ_TM		5 - 7	3	Max Tone Maps Requested
FL_AV	5	0 - 7	12	Frame Length
	6	0 - 3		
MPDUCnt		4 - 5	2	MPDU Count
RSVD		6 - 7	2	Reserved
PPB	7	0 - 7	8	Pending PHY Blocks
SRC	8	0 - 7	8	Sound Reason Code
RSVD	9	0 - 7		Reserved
	10	0 - 7		
	11	0 - 7		
	12	0 - 7		

FCCS_AV	13	0 - 7	24	Frame Control Check Sequence
	14	0 - 7		
	15	0 - 7		

Source Terminal Equipment Identifier (STEI)

The interpretation of the Source Terminal Equipment Identifier (STEI) field is the same as the corresponding Source Terminal Equipment Identifier (STEI) field in Section 4.4.1.5.2.1.

Destination Terminal Equipment Identifier (DTEI)

The interpretation of the Destination Terminal Equipment Identifier (DTEI) field is the same as the corresponding Destination Terminal Equipment Identifier (DTEI) field in Section 4.4.1.5.2.2.

Contention-Free Session (CFS)

The interpretation of the Contention-Free Session (CFS) field is the same as the corresponding Contention-Free Session (CFS) field in Section 4.4.1.5.2.4.

PHY Block Size (PBSz)

PHY Block Size (PBSz) is a 1-bit field that indicates the Sound MPDU Payload block size, with 136 octets corresponding to mini-ROBO and 520 octets corresponding to ROBO modulation. This field is valid only in Long Sound MPDUs and shall be set to 0b0 in all Sound ACKs.

Table 439: Sound MPDU PHY Block Size Interpretation

PBSz Value	Interpretation
0b0	Sound MPDU Payload contains a PHY block size of 520 octets (ROBO).
0b1	Sound MPDU Payload contains a PHY block size of 136 octets (mini-ROBO).

Beacon Detect Flag (BDF)

The interpretation of the Beacon Detect Flag (BDF) field is the same as the corresponding Beacon Detect Flag (BDF) field in Section 4.4.1.5.2.5.

Sound ACK Flag (SAF)

Sound ACK Flag (SAF) is a 1-bit field that indicates whether the MPDU is a Sound MPDU or a Sound ACK MPDU. The Sound MPDU contains a payload that is used by the receiving station to estimate the channel characteristics. Sound ACK MPDU indicates the reception status and completion of the Sounding process (refer to Section 5.2.6). The Interframe Spacing between the Sound MPDU with MPDUCnt of 0b00 and corresponding Sound ACK is the RIFS_AV_default.

Table 440: Sound ACK Flag Interpretation

SAF Value	Interpretation
0b0	The MPDU is a Sound MPDU.
0b1	The MPDU is a Sound ACK MPDU.

Sound Complete Flag (SCF)

This field is valid only when the Sound ACK Flag (SAF) field is 0b1 **(refer to** Section 4.4.1.5.5.6).

Table 441: Sound Complete Flag Interpretation

SCF Value	Interpretation

0b0	The receiving STA has not received the Tone Map corresponding to Sound MPDU which has been used for channel estimation.
0b1	The receiving STA has received sufficient number of Sound MPDU to complete channel estimation.
0x04 – 0x1F	The five LSBs of this field contain the TMI_AV (refer to Section 4.4.1.5.2.13).

Max. Tone Maps Requested (REQ_TM)

Max. Tone Maps Requested (REQ_TM) is a 3-bit field that indicates the maximum number of TMs that the transmitting STA can support for the receiving station. The receiving STA should not generate more than this number of distinct TMs during the channel estimation procedures. ROBO Mode Tone Maps shall not be counted towards this limit. This field is valid only when the Sound ACK Flag (SAF) is zero (refer to Section 4.4.1.5.5.6) and shall be set to 0b000 in all Sound ACKs.

A value of 0b000 indicates that no Tone Maps can be supported. A value of 0b001 indicates that one Tone Map can be supported, and so on.

Frame Length (FL_AV)

The Frame Length field indicates the duration of the payload. For information about the coding of this field, refer to Section 4.4.1.5.2.13.1.

Note: If the SAF field is 0b1, the Number of Symbols must be set to 0b00 (i.e., the Sound ACK has no payload, refer to Section 4.4.1.5.2.12).

MPDU Count (MPDUCnt)

The interpretation of the MPDU Count (MPDUCnt) field is the same as the corresponding MPDU Count (MPDUCnt) field in Section 4.4.1.5.2.15.

Pending PHY Blocks (PPB)

The interpretation of this field is the same as Section 4.4.1.5.2.8.1.

Link Identifier (LID)

The interpretation of the Link Identifier (LID) field is the same as the corresponding Link Identifier (LID) field in Section 4.4.1.5.2.3.

Sound Reason Code

Sound Reason Code is an 8-bit field that indicates the reason for transmitting the Sound MPDU. The interpretation of this field is shown in Table 442. This field is valid only in Long Sound MPDUs and shall be set to 0x00 in all Sound ACKs.

Table 442: Sound Reason Code Interpretation

SRC Value	Interpretation
0x00 – 0x03	Reserved

0x04 – 0x1F	Sound MPDU transmitted to obtain the Tone Map corresponding to a TMI_AV, which has been specified by the receiver in the intervals information but is not recognized by the transmitter. The five LSBs of this field contain the TMI_AV (refer to Section 4.4.1.5.2.13). The receiver may resend the Tone Map Data (TMD) corresponding to TMI_AV or it may resend all valid Tone Maps upon the reception of this Sound Reason Code.
0x20 – 0xFB	Reserved
0xFC	Sound MPDU transmitted to indicate a Tone Map error condition detected at the transmitter. Receiver shall resend all valid Tone Maps.
0xFD	Sound MPDU transmitted as part of Initial Channel Estimation.
0xFE	Sound MPDU transmitted in an interval where receiver has indicated that no AC Line Cycle adapted Tone Maps are available.
0xFF	Sound MPDU transmitted in an interval specified as Unusable by the receiver.

Reverse SOF Variant Fields

As with HomePlug AV, the Reverse SOF is a long MPDU used to carry both SACK information and payload. It uses one 128-bit Frame Control Block to carry Frame Control information. Table 443 shows the contents of VF_AV fields for the Reverse SOF in HomePlug GREEN PHY.

Table 443: Reverse SOF Variant Field

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
DT_AV	0	0 - 2	3	0b101 (Delimiter Type)
ACCESS		3	1	Access Field
SNID		4 - 7	4	Short Network Identifier
DTEI	1	0 - 7	8	Destination Terminal Equipment Identifier
CFS	2	0	1	Contention-Free Session

BDF		1	1	Beacon Detect Flag
SVN		2	1	SACK Version Number
RRTF		3	1	Request Reverse Transmission Flag
MFSRspData		4 - 5	2	Data MAC Frame Stream Response
MFSRspMgmt		6 - 7	2	Management MAC Frame Stream Response
SackD	-		Var	Sack Data
BitPad	-		Var	Bit Pad
RxWSz	-	-	4	Receive Window Size Only present for Priority Links, otherwise available for SackD and/or BitPad
RRTL	9	4 – 7	4	Request Reverse Transmission Length Only present if RRTF is set to 0b1; otherwise, available for SackD and/or BitPad
RSOF_FL_AV	10	0 – 7	10	Reverse SOF Frame Length
	11	0 – 1		
TMI_AV		2 – 6	5	Tone Map Index
PBSz		7	1	PHY Block Size

NumSym	12	0 – 1	2	Number of Symbols
MFSCmdMgmt		2 – 4	3	Management MAC Frame Stream Command
MFSCmdData		5 – 7	3	Data MAC Frame Stream Command
FCCS_AV	13	0 - 7	24	Frame Control Check Sequence
	14	0 - 7		
	15	0 - 7		

Destination Terminal Equipment Identifier (DTEI)

Destination Terminal Equipment Identifier (DTEI) is an 8-bit field. As with HomePlug AV, this field is set to the TEI assigned to the HomePlug GREEN PHY station that is the intended destination of the MPDU.

Contention-Free Session (CFS)

The Contention-Free Session flag is a 1-bit field that indicates whether the SOF MPDU is transmitted in a contention-free or Carrier Sense Multiple Access (CSMA) allocation.

Table 444: Contention-Free Session Interpretation

CFS Value	Interpretation
0b0	SOF MPDU is transmitted in a CSMA allocation.
0b1	SOF MPDU is transmitted in a contention-free allocation.

Beacon Detect Flag (BDF)

The interpretation of the Beacon Detect Flag (BDF) field is the same as the corresponding Beacon Detect Flag (BDF) field in Section 4.4.1.5.2.5.

SACK Version Number (SVN)

SACK Version Number (SVN) is a 1-bit field that indicates the version of the SACK Variant field. As with HomePlug AV, this version of HomePlug GREEN PHY Stations shall set this field to 0b0 on transmit and ignore it on receive.

Receive Window Size (RxWSz)

Receive Window Size (RxWSz) is a 4-bit field that indicates the reassembly buffer available for the corresponding MAC Frame Stream at the receiver. The Receive Window Size field is only present in the SACK data variant field of Local Links and Priority Links. Coding of this field is shown in Table 433.

Request Reverse Transmission Flag (RRTF)

The Request Reverse Transmission Flag (RRTF) indicates that the receiver is requesting the

transmitter initiates and/or continues a bidirectional burst.

Table 445: Request Reverse Transmission Flag Interpretation

RRTF Value	Interpretation
0b0	Reverse transmission not requested; RRTL field not present.
0b1	Reverse transmission requested; RRTL field present.

Data MAC Frame Stream Response (MFSRspData)

Data MAC Frame Stream Response (MFSRspData) is a 2-bit field that contains the response from the receiver's Data MAC Frame stream to the corresponding command (MFSCmdData) from the transmitter. Table 424 shows the interpretation of this field.

Management MAC Frame Stream Response (MFSRspMgmt)

Management MAC Frame Stream Response (MFSRspMgmt) is a 2-bit field that contains the response from the receiver's Management MAC Frame stream to the corresponding command (MFSCmdMgmt) from the transmitter. Table 424 shows the interpretation of this field.

SACK Data (SACKD)

The SACK Data field is, with the exception of the number of bits, identical to the SACK Data field as described in Section 4.4.1.5.3.8.

Request Reverse Transmission Length (RRTL)

The Request Reverse Transmission (RRTL) is a 4-bit field that specifies the minimum required duration for a Reverse Transmission. The RRTL shall include the payload duration as well as the subsequent RIFS_AV that is being requested for the reverse transmission. Table 434 shows the interpretation of the RRTL field.

Reverse SOF Frame Length (RSOF_FL_AV)

The Reverse SOF Frame Length (RSOF_FL_AV) is a 10-bit field that specifies the duration for a Reverse Transmission. The RSOF_FL_AV shall include the payload duration as well as the subsequent RIFS_AV that is being requested for the reverse transmission.

Table 446: Reverse SOF Frame Length Interpretation

RSOF_FL_AV Value	Interpretation
0x0 – 0x03D	Reserved
0x03E – 0x1FF	Payload length in multiples of 1.28 μsec
0x200 – 0x3FF	Payload length from 655.36 μsec to 1963.52 μsec in steps of 2.56 μsec

Tone Map Index (TMI_AV)

Tone Map Index (TMI_AV) is a 5-bit field that indicates the Tone Map to be used by the receiver in demodulating the MPDU Payload as described in Section 4.4.1.5.2.13.

PHY Block Size (PBSz)

PHY Block Size (PBSz) is a 1-bit field that indicates the MPDU Payload block size as described in Section 4.4.1.5.2.11.

Number of Symbols (NumSym)

Number of Symbols (NumSym) is a 2-bit field that indicates the number of OFDM Symbols used for transmitting the MPDU Payload as described in Section 4.4.1.5.2.12.

Management MAC Frame Stream Command (MFSCmdMgmt)

Management MAC Frame Stream Command (MFSCmdMgmt) is a 3-bit field that contains the command from the transmitter's Management MAC Frame Stream as described in Section 4.4.1.5.2.24.

Data MAC Frame Stream Command (MFSCmdData)

Data MAC Frame Stream Command (MFSCmdData) is a 3-bit field that contains the command from the transmitter's Data MAC Frame Stream as described in Section 4.4.1.5.2.25.

Frame Control Check Sequence (FCCS_AV)

Frame Control Check Sequence (FCCS_AV) is a 24-bit field in the Frame Control Block, and is CRC-24 computed over the fields of Frame Control block. FCCS_AV is used to check the integrity of the AV Frame Control information. Section 4.2.2 describes the computation of CRC-24.

Format of Long MPDU Payload

The MPDU Payload shall have one of four formats:

One or more 520-octet PBs

A single 136-octet PB

136 octets of Beacon payload

136 or 520 octets of Sound payload

The contents of the AV Frame Control are used to interpret which of the four formats is used within the MPDU Payload.

A SOF delimiter with one or more OFDM Symbols (i.e., NumSym ≠ 0b00, refer to Section 4.4.1.5.2.12) and PBSz set to 0b0 indicates that the MPDU Payload contains one or more 520-octet PBs.

A SOF delimiter with one or more OFDM Symbols and PBSz set to 0b1 indicates that the MPDU Payload contains a 136-octet PB.

A Reverse SOF delimiter with one or more OFDM Symbols (i.e., NumSym ≠ 0b00, refer to Section 4.4.1.5.6.14) and PBSz set to 0b0 indicates that the MPDU Payload contains one or more 520-octet PBs.

A Reverse SOF delimiter with one or more OFDM Symbols and PBSz set to 0b1 indicates that the MPDU Payload contains a 136-octet PB.

The Beacon delimiter indicates that the MPDU Payload contains a 136-octet Beacon payload.

A Sound delimiter with the Sound ACK field set to 0b0, indicating that the MPDU Payload contains a 136- or 520-octet Sound payload.

As with HomePlug AV, a HomePlug GREEN PHY station shall not transmit more than one 136-octet PB in an MPDU. HomePlug GREEN PHY stations shall not mix 520-octet PBs with 136-octet PBs within the same MPDU. At high data rates, multiple PBs can fit in a single OFDM Symbol. In such cases, HomePlug GREEN PHY transmissions shall be restricted to have only one PB ending in the last symbol of the MPDU. This restriction is intended to allow sufficient processing time for the last PHY block within an MPDU.

The format of the 520-octet PB and 136-octet PB are described in Section 4.4.2.1. The format of the Beacon MPDU Payload is described in Section 4.4.3. The format of the Sound payload is described in Section 4.4.4.

Format of PHY Blocks

As with HomePlug AV, HomePlug GREEN PHY supports PB sizes of 520 octets and 136 octets. Each PB is mapped onto a single FEC block at the physical layer. Each PB contains a PHY Block Header (PBH), PHY Block Body (PBB), and PHY Block Check Sequence (PBCS). PBH and PBCS are four octets each. When the PB size is 520 octets, the PB Body is 512 octets long. When the PB size is 136 octets, the PBB is 128 octets long. Figure 414 shows the PB formats.

Figure 414: PHY Block Formats

PHY Block Header

Table 447 shows the fields in the 4-octet PB Header field. The format of the PHY Block Header is independent of the PB size being used.

Table 447: PB Header Format

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
SSN	0	0 - 7	16	Segment Sequence Number
	1	0 - 7		
MFBO	2	0 – 7	9	MAC Frame Boundary Offset
	3	0		
VPBF		1	1	Valid PHY Block Flag
MMQF		2	1	Management Message Queue Flag
MFBF		3	1	MAC Frame Boundary Flag
OPSF		4	1	Oldest Pending Segment Flag
RSVD		5 - 7	3	Reserved

Segment Sequence Number (SSN)

Segment Sequence Number (SSN) is a 16-bit field that shall be initialized to 0 and is incremented by 1 for each new segment in a transmit tuple. The SSN shall wrap around as needed. Section 5.4.1.2 and 5.4.1.3 define the transmit and receive tuples and provides information about the segmentation and reassembly processes.

MAC Frame Boundary Offset (MFBO)

MAC Frame Boundary Offset (MFBO) is a 9-bit field that carries the offset in octets of the MAC Frame boundary (i.e., the first octet of the first new MAC Frame) within the PHY Block Body.

This field is valid only when the MAC Frame Boundary Flag is set to 0b1.
Table 448: MAC Frame Boundary Offset Interpretation

MFBO Value	Interpretation
0b000000000	Indicates the first octet, and so on.

Valid PHY Block Flag (VPBF)
When Valid PHY Block Flag (VPBF) is set to 0b1, it indicates that the current PHY block contains valid data. When VPBF is set to 0b0, it indicates that the PB is empty. Empty PBs do not carry valid data. The receiver shall discard empty PBs and ignore their contents. Empty PBs add overhead and their use should be minimized. To improve performance, implementations may use repetition of valid PBs in place of empty PBs.
The PBB of an empty PB can be transmitted without encryption. If the PBB of an empty PB is encrypted, the contents that are encrypted to generate the empty PBB must consist of a pseudo-random data pattern. This pattern must be changed at least each time the station powers-up.
An empty PB may be transmitted anywhere in an MPDU. The presence of an empty PB does not affect the sequence numbering used to determine grouping of its neighbor PHY blocks (refer to Section 5.4.1.4).

Informative Text
Empty PB(s) may be added to the end of an MPDU to ensure that only one PB is ending in the last OFDM Symbol of the long PPDU. This results in the addition of one OFDM Symbol to the PPDU length. If the length of the PPDU cannot be increased (e.g., when the PPDU is transmitted at the very end of a contention-free allocation), an additional OFDM Symbol cannot be added to the PPDU length. In these cases, the transmitter may insert more than one PB worth of last symbol padding, as described in Section 3.5.2.

Management Message Queue Flag (MMQF)
Management Message Queue Flag (MMQF) is a 1-bit field. This information is used to determine which tuple a PB belongs during the reassembly process (refer to Section 5.4.1.4).
Table 449: Management Message Queue Flag Interpretation

MMQF Value	Interpretation
0b0	The PHY block is based on a MAC Frame containing MSDU Payload.
0b1	The PB contains data from a MAC Frame carrying Management Message.

MAC Frame Boundary Flag (MFBF)
MAC Frame Boundary Flag (MFBF) is a 1-bit field.
Table 450: MAC Frame Boundary Flag Interpretation

MFBF Value	Interpretation
0b0	No MAC Frame boundary is present.
0b1	A MAC Frame boundary is present in the current PBB.

Oldest Pending Segment Flag (OPSF)

Oldest Pending Segment Flag (OPSF) is a 1-bit field that is used to synchronize the transmitter and receiver with respect to the Minimum Segment Sequence Number (refer to Section 5.4.1.6).

Table 451: Oldest Pending Segment Flag Interpretation

OPSF Value	Interpretation
0b0	Indicates that the Segment contained in the PBB is not the oldest pending Segment in the corresponding MAC Frame Stream at the transmitter
0b1	Indicates that the Segment contained in the PBB is the oldest pending Segment in the corresponding MAC Frame Stream at the transmitter.

PHY Block Body

PHY Block Body (PBB) carries the encrypted segment as the payload. The PBB field is either 512 or 128 octets, depending on the PB size.

Note: A segment may have to be padded before encryption to ensure that it fits exactly into the PBB.

PHY Body Check Sequence (PBCS)

PB Check Sequence (PBCS) contains a 32-bit CRC and is computed over the PB Header and the encrypted PB Body. Once the MPDU is delivered to the destination, the PBCS of each PB is checked and the good PBs are decrypted and delivered to the appropriate reassembly buffer. PB failures are reported to the transmitting station by a SACK.

Format of Beacon MPDU Payload

The Beacon MPDU Payload carries 136 octets of payload modulation using the Mini-ROBO Modulation. The duration of time required to transmit the Beacon payload depends on the number of OFDM carriers in the active Tone Mask (refer to Section 3.4.3.1). As with HomePlug AV, HomePlug GREEN PHY stations shall use the active Tone Mask information to implicitly determine the Beacon payload duration.

Table 452: Beacon Payload Fields

Field	Octet Number	Bit Number	Field Size	Definition
NID	0	0 - 7	54	Network Identifier
	1	0 - 7		
	2	0 - 7		
	3	0 - 7		
	4	0 - 7		
	5	0 - 7		
	6	0 - 5		
HM		6 - 7	2	Hybrid Mode

STEI	7	0 - 7	8	Source Terminal Equipment Identifier
BT	8	0 - 2	3	Beacon Type
NCNR		3	1	Non-Coordinating Networks Reported
NPSM		4	1	Network Power Saving Mode
NumSlots		5 - 7	3	Number of Beacon Slots
SlotUsage	9	0 - 7	8	Beacon Slot Usage
SlotID	10	0 - 2	3	Beacon Slot ID
ACLSS		3 - 5	3	AC Line Cycle Synchronization Status
HOIP		6	1	Handover-In-Progress
RTSBF		7	1	RTS Broadcast Flag
NM	11	0 - 1	2	Network Mode
CCoCap		2 - 3	2	CCo Capability
RSVD		4 - 7	1	reserved
BMI	-	-	Var	Beacon Management Information
OPAD	-	-	Var	Octet Pad
BPCS	132	0 - 7	32	Beacon Payload Check Sequence
	133	0 - 7		
	134	0 - 7		
	135	0 - 7		

Table 4 shows the structure of the information payload in the Beacon.

Table 452: Beacon Payload Fields

Field	Octet Number	Bit Number	Field Size	Definition

NID	0	0 - 7	54	Network Identifier
	1	0 - 7		
	2	0 - 7		
	3	0 - 7		
	4	0 - 7		
	5	0 - 7		
	6	0 - 5		
HM		6 - 7	2	Hybrid Mode
STEI	7	0 - 7	8	Source Terminal Equipment Identifier
BT	8	0 - 2	3	Beacon Type
NCNR		3	1	Non-Coordinating Networks Reported
NPSM		4	1	Network Power Saving Mode
NumSlots		5 - 7	3	Number of Beacon Slots
SlotUsage	9	0 - 7	8	Beacon Slot Usage
SlotID	10	0 - 2	3	Beacon Slot ID
ACLSS		3 - 5	3	AC Line Cycle Synchronization Status
HOIP		6	1	Handover-In-Progress
RTSBF		7	1	RTS Broadcast Flag
NM	11	0 - 1	2	Network Mode
CCoCap		2 - 3	2	CCo Capability
RSVD		4 - 7	1	reserved
BMI	-	-	Var	Beacon Management Information

OPAD	-	-	Var	Octet Pad
BPCS	132	0 - 7	32	Beacon Payload Check Sequence
	133	0 - 7		
	134	0 - 7		
	135	0 - 7		

Table 452b: Assignment of Previously Reserved Beacon Payload Fields for GREEN PHY

Field	Octet Number	Bit Number	Field Size	Definition
RSF	11	4	1	Reusable SNID Flag
Plevel		5 - 7	3	Proxy Level

Network Identifier (NID)

Each AVLN shall have a 54-bit Network ID (NID) that, together with the SNID, uniquely identifies the network. The NID changes only when the NMK changes. This does not add complexity since every authenticated STA must receive the new NMK and can compute or receive the new NID at the same time.

The NID shall be generated by combining the Security Level (two bits) with the NID Offset (52 bits). The default NID Offset is generated by hashing the NMK. The mechanism for generating the NID Offset from the NMK shall be the PBKDF1 function, as shown in the PKCS #5 v2.0 standard, Password-based Cryptography Standard, using SHA-256 as the underlying hash algorithm. The iteration count used to calculate the NID Offset shall be 5. No salt shall be used. The MSB of the least-significant octet of the NMK shall be the leftmost bit of the input, as described in the FIPS-180-2 change notice. The leftmost 52 bits of the hash output shall be used, where the leftmost bit of the 52-bit truncated hash output is bit 7 of the NID offset, and the rightmost bit of the truncated hash output is bit 48 of the NID Offset. The default NID offset along with the Security Level form the default NID for an NMK-SL.

If the CCo elects to use multiple NMKs to cryptographically isolate STAs in an AVLN into multiple sub-AVLNs (as may be the case for a BPL network), the CCo may use the NID derived from one of its NMKs as the NID for its other NMKs. The Security Level of all NMKs shall be the same for all sub-AVLNs of an AVLN. It is incumbent upon the CCo to disambiguate the NMK using the STA's MAC address. A STA shall store the NID provided with an NMK with that NMK if the NID offset is not the default NID offset.

Note: The LSB of the NID offset is bit 0 and the MSB is bit 51 (see Figure 415). The two MSBs of the NID shall be the Security Level of the NMK (0b00 = Simple Connect and 0b01 = Secure, refer to Section 7.10.3.1).

Figure 415: Network Identifier

The NID shall be broadcast in the Beacon. The current CCo's MAC address may be discovered using the CC_WHO_RU.REQ/CNF message exchange or, if the Network Encryption Key (NEK)

is known, by observing the CC_SET_TEI_MAP.IND **MME** or through the discovery process.

Informative Text
A STA has one NMK in use at all times. When the NMK is being changed, the new NMK is stored by the STA until the change is effective, at which point the old NMK is discarded. If the HLE has stored multiple NMKs, the HLE should first request all NIDs visible to the STA to search for a matching NID. If none is found, the HLE should rotate through the NMKs in its possession to advertise them using the CM_UNASSOCIATED_STA.IND MME.

Hybrid Mode (HM)

Hybrid Mode (HM) is a 2-bit field that indicates the HomePlug 1.0.1 Coexistence operating mode of the AVLN. Discover and Proxy Beacons shall set this field to the value of the same field in Central Beacon.

Table 453: Hybrid Mode Interpretation

HM Value	Interpretation
0b00	The network is operating in AV Only Mode.
0b01	The network is operating in Shared CSMA Hybrid Mode (i.e., Hybrid Mode only in Shared CSMA allocations).
0b10	The network is operating in Fully Hybrid Mode (i.e., Hybrid Mode in Shared CSMA, Local CSMA, CFPI and CFP allocations).
0b11	The network uses Hybrid Delimiters for all transmissions, but may use frame lengths not compatible with HomePlug 1.0 (only valid in CSMA-Only mode).

In CSMA-Only Mode, the HM field indicates whether HomePlug 1.0-compatible frame lengths must be used, as all transmissions are in Hybrid Mode. When HM=0b10, HomePlug 1.0-compatible frame lengths must be used; when HM=0b11, Hybrid delimiters must be used, but frame lengths not compatible with HomePlug 1.0 (for example, using invalid HomePlug 1.0.1 frame control fields) may be used.

Source Terminal Equipment Identifier (STEI)

Source Terminal Equipment Identifier (STEI) is an 8-bit field that is set to the TEI assigned to the station transmitting the Beacon.

Beacon Type (BT)

Beacon Type (BT) is a 3-bit field that indicates the Beacon type. Table 454: Beacon Type Field Interpretation lists the Beacon types and their corresponding BT value.

All Beacon types share the same Beacon structure, but differ in functionality and the Beacon Management information they carry.

The Central Beacon is generated by the CCo of each AVLN. One of the main functions of Central Beacon is to carry medium allocation (or scheduling) information. Section 5.1.1.2.1 and Chapter 8 provide information about the Beacon Period structure and how this information is

conveyed using the central Beacon.
The Discover Beacon is transmitted by all associated and authenticated STAs periodically to aid in network-topology discovery, where other STAs update their Discovered STA Lists and Discovered Network Lists. The Discover Beacon also allows hidden STAs (i.e., STAs that cannot decode the Central Beacons from the CCo) to ascertain the Beacon Period structure and to associate with the CCo. For more information, refer to Section 7.6.1.1.
Proxy Beacons are used to manage hidden terminals (i.e., Proxy Networking) within an AVLN. For more information, refer to Section 7.7.4.
Table 454: Beacon Type Field Interpretation

BT Value	Interpretation
000	Central Beacon
001	Discover Beacon
010	Proxy Beacon
011 - 111	RSVD

Non-Coordinating Networks Reported (NCNR)
Non-Coordinating Network Reported (NCNR) is a 1-bit field that indicates the absence or presence of networks that are not coordinating with the CCo. The CCo sets the value of this field based on the Discovered Network Lists from its STAs. Discover and Proxy Beacons shall set this field to the value of the same field in Central Beacon.
Table 455: Non-Coordinating Networks Reported Field Interpretation

NCNR Value	Interpretation
0b0	Non-coordinating networks are not reported.
0b1	Non-coordinating networks are reported.

Network Power Saving Mode (NPSM)
Network Power Saving Mode (NPSM) is a 1-bit field that indicates whether the CCo has placed the network into Network Power Saving Mode. For more information, refer to Section 7.11. Discover and Proxy Beacons shall set this field to the value of the same field in Central Beacon.
Table 456: Network Power Saving Mode Interpretation

NPSM Value	Interpretation
0b0	Network Power Saving Mode is not active.
0b1	Network Power Saving Mode is active.

Number of Beacon Slots (NumSlots)
Number of Beacon Slots (NumSlots) is a 3-bit field that indicates the number of Beacon Slots in the Beacon Region. The maximum number of Beacon Slots in the Beacon Region is limited to MaxBeaconSlot. Discover and Proxy Beacons shall set this field to the value of the same field in Central Beacon.
Table 457: Number of Beacon Slots Interpretation

NumSlots Value	Interpretation

0b000	Current Beacon Region has one Beacon Slot.
0b001	There are two Beacon Slots in the Beacon Region, and so on.

Beacon Slot Usage (SlotUsage)

Beacon Slot Usage (SlotUsage) is an 8-bit bit-mapped field. Each bit in the field can have one of the values in Table 458. Refer to Section 8.3.5.3.

Table 458: Beacon SlotUsage Interpretation

SlotUsage Value	Interpretation
0b0	The slot is free.
0b1	The slot is occupied.

Beacon Slot ID (SlotID)

Beacon Slot ID (SlotID) is a 3-bit field that indicates the Beacon Slot number used by the current Beacon MPDU. Discover and Proxy Beacons shall set this field to the value of the same field in Central Beacon.

Table 459: Beacon Slot ID Interpretation

SlotID Value	Interpretation
0b000	The current Beacon MPDU is transmitted in the first Beacon Slot.
0b001	The second Beacon Slot, and so on.

AC Line Cycle Synchronization Status (ACLSS)

AC Line Cycle Synchronization Status (ACLSS) is a 3-bit field. The ACLSS shall be set to the current Beacon Slot ID if the CCo is locally tracking the AC Line cycle. If the CCo is tracking the AC line cycle synchronization of a Central Beacon of another CCo in a Group of networks, ACLSS shall be set to the Beacon Slot ID of that Central Beacon. Discover and Proxy Beacons shall set this field to the value of the same field in Central Beacon.

Handover-in-Progress (HOIP)

Handover-In-Progress (HOIP) is a 1-bit field that indicates whether a handover is in progress. If a handover is in progress, STAs and neighbor CCos shall wait before sending association or bandwidth requests to the CCo. Discover and Proxy Beacons shall set this field to the value of the same field in Central Beacon.

Table 460: Handover-In-Progress (HOIP) Interpretation

HOIP Value	Interpretation
0b0	Handover is not in progress.
0b1	Handover is in progress.

RTS Broadcast Flag (RTSBF)

The RTS Broadcast Flag (RTSBF) is a 1-bit field that indicates to all stations in the network that broadcast MPDUs must use RTS/CTS when RTSBF is set to 0b1.

The CCo shall maintain a list of all stations in the network (defined by the SNID), where DCPPCF is set in a CC_DCPPC.IND message and shall remove from the list any previously listed stations where DCPPCF is clear in a CC_DCPPC.IND message. If the list contains one or more stations, the CCo shall set RTSBF to 0b1. Otherwise, it shall be set to 0b0.

Stations that use a different PHY Receive Clock Correction during the CP are required to send a CC_DCPPC.IND message to the CCo. The message shall also be sent when a station changes from using a different PHY Receive Clock Correction to using the correct PHY Receive Clock Correction for the network. Discover and Proxy Beacons shall set this field to the value of the same field in Central Beacon.

RTS Broadcast Flag (RTSBF) for GREEN PHY

It is optional for a Green PHY CCo to support the reception of the CC_DCPPC.IND message. If it supports CC_DCPPC.IND message, the behavior of the CCo with respect to the RTS Broadcast Flag is as explained in section 4.4.3.1.2. Else, it shall set the RTS Broadcast Flag to 0b0.

It is optional for a Green PHY STA to interpret RTSBF field. If the Green PHY station supports the interpretation of RTSBF field, its behavior is same as described in 4.4.3.1.2. If a Green PHY station does not interpret the RTSBF field, the station will not use RTS/CTS to broadcast any MPDU.

Network Mode (NM)

The Network Mode (NM) field indicates the network mode of operation of the AVLN. The interpretation of this field is shown in Table 461. Refer to Section 8.1 for details.

Table 461: Network Mode Field Interpretation

NM Value	Interpretation
0b00	Uncoordinated Mode
0b01	Coordinated Mode
0b10	CSMA-Only Mode
0b11	RSVD

CCo Capability (CCoCap)

The CCo Capability (CCoCap) field indicates the CCo capability of the CCo of the AVLN. The interpretation of this field is shown in Table 462. Refer to Section 7.4.3.1 for details.

Table 462: CCo Capability Field Interpretation

CCoCap Value	Interpretation
0b00	Level-0 CCo Capable – does not support QoS and TDMA
0b01	Level-1 CCo Capable – supports QoS and TDMA but only in Uncoordinated Mode
0b10	Level-2 CCo Capable – supports QoS and TDMA in Coordinated Mode
0b11	Level-3 CCo Capable – future CCo capabilities

Beacon Management Information (BMI)

Beacon Management Information is a variable-length field that contains Beacon Management Messages.

Table 463: Beacon Management Information Format

Field	Octet Number	Field Size (Octets)	Definition
NBE	0	1	Number of Beacon Entries

BEHDR[1]	1	1	First Beacon Entry Header
BELEN[1]	2	1	First Beacon Entry Length = N[1]
BENTRY[1]	-	N[1]	First Beacon Entry
…			
BEHDR[L]	-	1	L^{th} Beacon Entry Header
BELEN[L]	-	1	L^{th} Beacon Entry Length = N[L]
BENTRY[L]	-	N[L]	L^{th} Beacon Entry

Number of Beacon Entries (NBE)

Number of Beacon Entries (NBE) indicates the total number of Beacon entries present in this Beacon payload.

Table 464: Number of Beacon Entries Interpretation

NBE Value	Interpretation
0x00 - 0x01	Reserved
0x02	Two Beacon entries are present, and so on

Beacon Entry Header (BEHDR)

Beacon Entry Header (BEHDR) indicates the type of Beacon entry. BENTRYs within the BMI shall be arranged in increasing order of their BEHDR Values. Thus when Non-Persistent Schedule BENTRY is present, it shall be the first BENTRY in the BMI. When the BENTRY contains Persistent Schedule BENTRYs carrying both current and future schedule information (refer to Section 4.4.3.15.4.2.1), the Persistent Schedule BENTRY carrying the current schedule information shall be presented before the Persistent Schedule BENTRY carrying the future schedule.

Table 465b: Assignment of Previously Reserved Beacon Entry Header Values for IEEE 1901

BEHDR Value	Interpretation
0x0E	RSN Information Element BENTRY (used by IEEE 1901, not supported by GREEN PHY)
0X0F	ISP BENTRY (used by IEEE 1901, required by GREEN PHY, see section 14.1.1..2)
0x10	Extended Band Stay Out BENTRY (used by IEEE 1901, not supported by GREEN PHY)
0x11	AG Assignment BENTRY (used by IEEE 1901, not supported by GREEN PHY)
0x12	Extended Carriers Support BENTRY (used by IEEE 1901, not supported by GREEN PHY)

Table 465c: Assignment of Previously Reserved Beacon Entry Header Values for GREEN PHY

BEHDR Value	Interpretation
0x13	Power Save BENTRY

Table 466 provides details about when each of the Beacon Entries is present in various Beacons.

Table 465: Beacon Entry Header Interpretation

BEHDR Value	Interpretation
0x00	Non-Persistent Schedule BENTRY
0x01	Persistent Schedule BENTRY
0x02	Regions BENTRY
0x03	MAC Address BENTRY
0x04	Discover BENTRY
0x05	Discovered Info BENTRY
0x06	Beacon Period Start Time Offset BENTRY
0x07	Encryption Key Change BENTRY
0x08	CCo Handover BENTRY
0x09	Beacon Relocation BENTRY
0x0A	AC Line Sync Countdown BENTRY
0x0B	Change NumSlots BENTRY
0x0C	Change HM BENTRY
0x0D	Change SNID BENTRY
0x0E – 0xFE	Reserved for future use
0xFF	Vendor-Specific BENTRY

Table 465b: Assignment of Previously Reserved Beacon Entry Header Values for IEEE 1901

BEHDR Value	Interpretation
0x0E	RSN Information Element BENTRY (used by IEEE 1901, not supported by GREEN PHY)
0X0F	ISP BENTRY (used by IEEE 1901, required by GREEN PHY, see section 14.1.1..2)
0x10	Extended Band Stay Out BENTRY (used by IEEE 1901, not supported by GREEN PHY)
0x11	AG Assignment BENTRY (used by IEEE 1901, not supported by GREEN PHY)
0x12	Extended Carriers Support BENTRY (used by IEEE 1901, not supported by GREEN PHY)

Table 465c: Assignment of Previously Reserved Beacon Entry Header Values for GREEN PHY

BEHDR Value	Interpretation

0x13	Power Save BENTRY
CCo Handover	

Table 466: Beacon Entries in Various Beacons

BENTRY	Central Beacon	Proxy Beacon	Discover Beacon
Non-Persistent Schedule BENTRY	See Note #1 below	Shall be present whenever it is present in the Central Beacon	Optional, whenever it is present in the Central Beacon or Proxy Beacon. See Note # 2 below
Persistent Schedule BENTRY	See Note #1 below	Shall be present whenever it is present in the Central Beacon	Optional, whenever it is present in the Central Beacon or Proxy Beacon. See Note # 2 below
Regions BENTRY	Shall always be present See Note #3 below	Shall always be present. Copied from the Central Beacon	Shall always be present. Copied from the Central Beacon or Proxy Beacon
MAC Address BENTRY	Optional	Optional	Shall always be present
Discover BENTRY	Shall be present whenever a Discover Beacon allocation is specified in any Schedule BENTRY	Optional if present in the Central Beacon and the Discover Beacon allocation is for the current STA or for a STA for which the current STA is not the PCo	Optional, when present in the Central Beacon or Proxy Beacon
Discovered Info BENTRY	Optional	Optional	Shall always be present
Beacon Period Start Time Offset BENTRY	Shall be present only when the network is operating in CSMA-Only mode	Shall always be present See Note #4 below	Shall always be present
Encryption Key Change BENTRY	Shall be present whenever the NEK of the AVLN is being changed (refer to Section 7.10.4.2)	Shall be present whenever it is present in the Central Beacon	Optional, whenever it is present in the Central Beacon or Proxy Beacon

CCo Handover BENTRY	Shall be present whenever there is Handover of CCo functions (refer to Section 7.5)	Shall be present whenever it is present in the Central Beacon	Shall be present whenever it is present in the Central Beacon or the Proxy Beacon
Beacon Relocation BENTRY	Shall be present whenever the Central Beacon is being relocated (refer to Section 5.2.8)	Shall be present whenever it is present in the Central Beacon	Shall be present whenever it is present in the Central Beacon or the Proxy Beacon
AC Line Sync Countdown BENTRY	Shall be present whenever a CCo in Coordinated mode is handing over the AC Line cycle Synchronization (refer to Section 8.3.9 and Section 8.3.10)	Optional if present in the Central Beacon	Optional if present in the Central Beacon or the Proxy Beacon
Change NumSlots BENTRY	Shall be present whenever the number of Beacon Slots in the Beacon Region are being changed (refer to Section 8.3.5.2)	Shall be present whenever it is present in the Central Beacon	Shall be present whenever it is present in the Central Beacon or the Proxy
Change HM BENTRY	Shall be present whenever the value of Hybrid mode of an AVLN in Coordinated mode is being changed (refer to Section 9.10)	Optional if present in the Central Beacon	Optional if present in the Central Beacon or the Proxy
Change SNID BENTRY	Shall be present whenever the SNID of an AVLN is being changed (refer to Section 4.4.1.4)	Shall be present whenever it is present in the Central Beacon	Shall be present whenever it is present in the Central Beacon or the Proxy
Vendor-Specific BENTRY	Optional	Optional	Optional

Notes:

- It is mandatory for the Central Coordinator to provide the allocation information for each Beacon Period using one or more of the following Schedule BENTRIES:

Non-Persistent Schedule BENTRY,

Persistent Schedule BENTRY carrying a current schedule, Persistent Schedule BENTRY carrying a future schedule	Shall be present whenever one or more STAs (including the CCo) is in the Power Save

At a minimum, allocation information contained in the Schedule BENTRIES must include the Shared CSMA Regions. STAs in the AVLN are not required to interpret the Regions BENTRY to determine transmission opportunities.

- It is recommended that the Non-Persistent and Persistent Schedule BENTRIES be included in the Discover Beacon whenever there is sufficient space available in the Beacon Payload.
- Regions BENTRY shall be present in CSMA-Only mode, Coordinated mode, and Uncoordinated mode.
- Proxy Beacon shall include Beacon Period Start Time Offset BENTRY in addition to all the BENTRIES present in the Central Beacon. In Coordinated mode and Uncoordinated mode, the Central Beacon shall include at least 5 octets of Octet PAD (refer to Section 4.4.3.15.4.14.1) whenever Proxy Coordinator(s) are present to enable the Proxy Coordinator(s) to include this additional BENTRY.

Table 466b: Additional Beacon Entries in Various Beacons for GREEN PHY

BENTRY	Central Beacon	Proxy Beacon	Discover Beacon
RSN Information Element BENTRY (used by IEEE 1901, not supported by GREEN PHY)	n/a	n/a	n/a
ISP BENTRY	See section 14.1.1.1	See section 14.1.1.1	See section 14.1.1.1
Extended Band Stay Out BENTRY (used by IEEE 1901, not supported by GREEN PHY)	n/a	n/a	n/a
AG Assignment BENTRY (used by IEEE 1901, not supported by GREEN PHY)	n/a	n/a	n/a
Extended Carriers Support BENTRY (used by IEEE 1901, not supported by GREEN PHY)	n/a	n/a	n/a

Power Save	Shall be present whenever one or more STAs (including the CCo) is in the Power Save mode	Shall be present whenever it is present in the Central Beacon	Optional, whenever it is present in the Central Beacon or Proxy Beacon.

Beacon Entry Length (BELEN)

Beacon Entry Length (BELEN) indicates the length of the Beacon entry, in octets.

Table 467: BELEN Interpretation

BELEN Value	Interpretation
0x00	A length of zero, and so on.

Beacon Entry (BENTRY)

The contents of the Beacon Entry (BENTRY) field depend on the Beacon Entry Header. The format of various Beacon entries is described in the following sections.

Non-Persistent Schedule BENTRY

Non-Persistent Schedule BENTRY contains the schedule that is valid in the current Beacon Period only. There must be no more than one Non-Persistent Schedule BENTRY in each Beacon. Contiguous allocations for the same GLID must be presented using a single Session Allocation Information within a Non-Persistent Schedule BENTRY.

Table 468: Non-Persistent Schedule BENTRY

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
NS	0	0 - 5	6	Number of Sessions = L 0x00 = zero 0x01 = one, and so on
RSVD		6 - 7	2	Reserved
SAI [0]	-	-	Var	Session Allocation Information – First Session
…				
SAI [L-1]	-	-	Var	Session Allocation Information – Last Session

Number of Sessions (NS)

Number of Sessions (NS) is a 6-bit field that indicates the number of sessions (L) for which Non-Persistent session allocation information is contained in the Beacon payload.

Session Allocation Information (SAI)

The interpretation of the Session Allocation Information (SAI) field is the same as the

corresponding Session Allocation Information (SAI) field in Section 4.4.3.15.4.2.4.

Persistent Schedule BENTRY

Persistent Schedule BENTRY describes the schedules that are valid for multiple Beacon Periods. There must be no more than one Persistent Schedule BENTRY carrying current schedule (i.e., PSCD = 0b000) and one Persistent Schedule BENTRY carrying future schedule (i.e., PSCD ≠ 0b000) in a Beacon (refer to Section 5.1.1.2.1). Within each Persistent Schedule, contiguous allocations for the same GLID must be presented using a single Session Allocation Information field.

Table 469: Persistent Schedule BENTRY

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
PSCD	0	0 - 2	3	Preview Schedule Countdown
CSCD		3 - 5	3	Current Schedule Countdown
RSVD		6 - 7	2	Reserved
NS	1	0 - 5	6	Number of Sessions = L 0x00 = zero, 0x01 = One, and so on.
RSVD		6 - 7	2	Reserved
SAI [0]	-	-	Var	Session Allocation Information – First Session
…				
SAI [L-1]	-	-	Var	Session Allocation Information – Last Session

Preview Schedule Countdown (PSCD)

Preview Schedule Countdown (PSCD) is a 3-bit field that contains schedule information.

Table 470: PSCD Interpretation

PSCD Value	Interpretation
0b000	The schedule information contained in the schedule BENTRY pertains to the currently used schedule.
non-zero value	The schedule information contained in the schedule BENTRY pertains to a future schedule.

	0b001		The future schedule will become current in 1 Beacon Period (i.e., the next Beacon Period).	Global Link ID (only the lower 7 bits)
GLID	0b010	1 - 7	The future schedule will become current in two Beacon Periods (i.e., the Beacon Period after next, and so forth).	

Current Schedule Countdown (CSCD)

When Preview Schedule Countdown (PSCD) is set to 0b000, the 3-bit Current Schedule Countdown (CSCD) field defines the number of Beacon Periods for which the current schedule is valid.

Table 471: CSCD Interpretation

CSCD Value	Interpretation
0b000	The current schedule is valid for only the current period.
0b001 - 0b110	The current schedule is valid for the current and next periods, and so on.
0b111	The current schedule is valid indefinitely.

The special value of 0b111 (indefinite persistence) indicates that the current schedule should be considered valid until new information superseding it is received. Indefinite current schedules shall only be used in CSMA-Only mode. Refer to Section 5.1.

When PSCD is non-zero:

The CSCD field provides a preview of the value that the published schedule will have in the first Beacon Period in which it is the current schedule.

The CSCD shall not be changed from its value in the first announcement of the previewed schedule.

Number of Sessions (NS)

Number of Sessions (NS) is a 6-bit field that indicates the number of sessions (L) for which persistent session allocation information is contained in the Beacon payload. The maximum number of sessions supported in a network is limited by the size of Beacon payload.

Session Allocation Information (SAI)

Session Allocation Information (SAI) provides the basic unit of medium allocation. The length of the SAI field is 3 or 4 octets, depending on whether the Start Time field is present.

When Start Time is not present, the SAI is 3 octets long (refer to Table 472).

When Start Time is present, SAI is 4 octets long (refer to Table 473).

Table 472: Session Allocation Information Format without Start Time

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
STPF	0	0	1	Start Time Present Flag = 0b0

GLID		1 - 7	7	Global Link Identifier (only the lower 7 bits of the GLID are specified since the high-order bit is always 1)
ET	1	0 - 7	12	End Time
	2	0 - 3		
RSVD		4 - 7	4	Reserved

Table 473: Session Allocation Information Format with Start Time

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
STPF	0	0	1	Start Time Present Flag = 0b1
GLID		1 - 7	7	Global Link Identifier (only the lower 7 bits of the GLID are specified since the high-order bit is always 1)
ST	1	0 - 7	12	Start Time
	2	0 - 3		
ET		4 - 7	12	End Time
	3	0 - 7		

Start Time Present Flag (STPF)

Start Time Present Flag (STPF) is a 1-bit field.

Table 474: Start Time Present Flag Interpretation

STPF Value	Interpretation
0b1	Indicates that the start time of the session is explicitly specified.

Global Link Identifier (GLID)

For information about the GLID, refer to Section 5.2.1.4.

Start Time (ST)

Start Time (ST) is a 12-bit field that specifies the time at which the session associated with a particular GLID will start. This field is required:

If there is no immediately preceding allocation or

If the End Time of the immediately preceding allocation is not the Start Time of the current allocation.

This field indicates the time in multiples of AllocationTimeUnit. A value of 0x000 indicates 0 sec,

and so on.
Start Time is measured relative to the start time of the corresponding Beacon Period. Beacon Period Start Time is same as the start time of the first (or only) Beacon Slot within the Beacon Region.
End Time (ET)
End Time (ET) is a 12-bit field that specifies the time at which the session associated with a particular GLID will end and thus communicates when the immediately succeeding session can begin to access the channel. This field indicates the time in multiples of AllocationTimeUnit. A value of 0x000 indicates 0 sec, and so on.
End Time is measured relative to the start time of the corresponding Beacon Period. Beacon Period Start Time is same as the start time of the first (or only) Beacon Slot within the Beacon Region.
Regions BENTRY
Regions BENTRY describes the top-level structure of the Beacon Period. This information is used to coordinate the sharing of bandwidth among Neighbor Networks.
Regions BENTRY is only interpreted by the CCos. All STAs that are part of an AVLN or that are trying to join with an AVLN should use the Schedule BENTRIES to determine the transmission opportunities.
Each Beacon shall include a Regions BENTRY. Furthermore, Regions BENTRY must cover the entire Beacon Period, excluding the Beacon Regions. There is one Region Type (RT) and one Region End Time (RET) field in the Regions BENTRY for each contiguous Region in the Beacon Period. Regions are listed in the order they occur in the Beacon Period. The start time of first Beacon Region is implicitly determined by using the Number of Slots field in the Beacon Frame Control and the SlotID in the Beacon payload. The start time of each successive Region is the end time (RET) of the previous Region in the Beacon Period. Within each Regions BENTRY, contiguous regions of the same type must be presented using a single {RT, RET} field pair.
In Uncoordinated Mode, the Regions BENTRY shows the maximum duration of persistent CFP allocation and the duration of persistent CP allocation within the Beacon Period. Changes to the Regions BENTRY should be minimized in Uncoordinated mode.

Table 475: Regions BENTRY

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
NR	0	0-5	6	Number of Regions = L 0x00 = none 0x01 = one, and so on
RSVD		6-7	2	Reserved
RT[1]	1	0-3	4	Region Type for Region #1
RET[1]		4-7	12	Region End Time for Region #1
	2	0-7		
...				

RT[L]	-	-	4	Region Type for Region #L
RET[L]	-	-	12	Region End Time for Region #L

Number of Regions (NR)

Number of Regions (NR) is a 6-bit field that contains a count of the number of Regions in the Beacon Period.

Region Type (RT)

Region Type (RT) is a 4-bit field that identifies the type of Region for which allocation is made using the Regions BENTRY. HomePlug AV uses Region Types for providing contention-free and CSMA/CA allocations and for coordination of sharing of medium between Neighbor Networks. A brief description of various Region types is presented below.

Reserved Region indicates Regions where the CCo provides scheduled access to stations within the AVLN. The persistent and Non-Persistent Schedule BENTRYs provide granularity on how the Reserved Region is to be used in each Beacon Period (refer to Section 5.1.1.2.1).

CSMA Region indicates Regions where all stations can access the medium using the CSMA/CA channel access mechanism described in Section 5.1.2.3.1. A CSMA Region is further classified into a Shared CSMA Region or a Local CSMA Region.

A Shared CSMA Region is available to neighboring AVLNs in the Interfering Network List (INL).

A Local CSMA Region is only available to the AVLN in which it is specified.

Stayout Region indicates Regions with one or more neighboring AVLNs in the INL-specified Reserved or Protected Regions (refer to Chapter 8).

Protected Region indicates Regions where another group of AVLNs with a different Beacon Period start time specified a Beacon Region (refer to Chapter 8).

Beacon Region indicates Regions where one or more AVLNs transmit Beacons (refer to Chapter 8).

Table 476: Region Type (RT) Interpretation

RT Value	Interpretation
0b0000	Reserved Region
0b0001	Shared CSMA Region
0b0010	Local CSMA Region
0b0011	Stayout Region
0b0100	Protected Region
0b0101	Beacon Region
0b0110 – 0b111	Reserved

Region End Time

Region End Time is a 12-bit field that defines the end time of a Region within the Beacon Period in multiples of AllocationTimeUnit. A value of 0x000 indicates 0 sec, and so on.

Region End Time is measured relative to the start time of the corresponding Beacon Period. Beacon

Period Start Time is same as the start time of the first (or only) Beacon Slot within the Beacon Region.

MAC Address BENTRY

MAC Address BENTRY specifies the MAC address of the STA that transmits the Beacon MPDU. This BENTRY must be present in a Discover Beacon. It is optional in other types of Beacons.

Table 477: MAC Address BENTRY

Field	Octet Number	Bit Number	Bits	Definition
MACAddr	0	0 - 7	48	MAC address of the STA that transmits the Beacon MPDU.
	1	0 - 7		
	2	0 - 7		
	3	0 - 7		
	4	0 - 7		
	5	0 - 7		

Discover BENTRY

Discover BENTRY carries the TEI of the STA that is designated to transmit the Discover Beacon. A CCo shall not include more than one Discover BENTRY in each Central Beacon.

In Uncoordinated and Coordinated modes, the CCo shall provide Non-Persistent TDMA allocation for transmission of the Discover Beacons. In CSMA-Only mode, the STA should contend using CSMA/CA channel access at CAP2 for transmission of the Discover Beacon. Since CSMA/CA channel access latencies can be large, the STA can contend for transmitting Discover Beacons in CSMA-Only mode until it obtains channel access. Thus, its Discover Beacon may be transmitted in a Beacon Period that is different than the Beacon Period in which the CCo designed the STA to transmit its Discover Beacon.

Table 478: Discover BENTRY

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
TEI	0	0 - 7	8	Terminal Equipment Identifier

Discovered Info BENTRY

Discovered Info BENTRY specifies the:

CCo, PCo, and Backup CCo capability

Current CCo, PCo, and Backup CCo status

Number of entries in the Discovered STA List and Discovered Network List of the STA transmitting the Beacon MPDU

This BENTRY shall be present in a Discover Beacon. It is optional in other types of Beacons.

Table 479: Discovered Info BENTRY

Field	Octet Number	Bit Number	Field Size (Bits)	Definition

NumDisSTA	1		8	Number of information has not been changed.
Updated	0	0	1	0b1 = information has been changed since the last query by the CCo.
CCo Capability		1 - 2	2	CCo Capability level – refer to Table 462 in Section 4.4.3.14
Proxy Networking Capability		3	1	0b0 = does not support Proxy Networking 0b1 = fully supports Proxy Networking
Backup CCo Capability		4	1	0b0 = STA does not support Backup CCo function 0b1 = STA supports Backup CCo function
CCo Status		5	1	0b0 = STA is not the CCo 0b1 = STA is the CCo
PCo Status		6	1	0b0 = STA is not a PCo 0b1 = STA is a PCo
Backup CCo Status		7	1	0b0 = STA is not a Backup CCo 0b1 = STA is a Backup CCo

NumDisSTA	1		8	Number of entries in the Discovered STA List
NumDisNet	2	4-6	8	Number of entries in the Discovered Network List
Authentication Status	3	0	1	STA's Authentication Status 0b0 = Associated but not authenticated 0b1 = Associated and authenticated
User-Appointed CCo Status		1	1	STA's status as a user-appointed CCo 0b0 = STA is not configured as user-appointed CCo 0b1 = STA is configured as a user-appointed CCo
GREEN PHY Capability		2-3	2	GREEN PHY Capability of a station 0b00 = STA is not GREEN PHY Capable 0b01 = STA is HP GP1.0 Capable 0b10-0b11 = Reserved

HPAV version
Number of AV version supported

HPAV version		4-6	3	HomePlug AV version supported 0b000 = HomePlug AV 1.1 supported 0b001- 0b110 = Reserved for future use 0b111 = No version of HomePlug AV supported
RSVD		7	1	Reserved

Updated

Updated shall be set to 0b1 if the content of the Discovered STA List or the Discovered Network List has been changed since the CCo sent the most recent CC_DISCOVER_LIST.REQ message to the STA. Updated shall be set to 0b0 otherwise.

CCo Capability

CCo Capability is set to specify the ability of the STA to act as a CCo (refer to Section 7.4.3.1). Interpretation is the same as in Table 462 in Section 4.4.3.14.

Proxy Networking Capability

Proxy Networking Capability is set to specify the ability of the STA to act as a Proxy relay or Proxy endpoint.

Table 480: Proxy Networking Capability Interpretation

Proxy Networking Value	Interpretation
0b0	STA does not support Proxy Networking.
0b1	STA supports Proxy Networking.

Backup CCo Capability

Backup CCo Capability is set to specify the ability of a STA to act as a Backup CCo.

Table 481: Backup CCo Capability Interpretation

Backup CCo Capability Value	Interpretation
0b0	STA does not support the Backup CCo function.
0b1	STA does support the Backup CCo function.

CCo Status

CCo Status indicates whether the STA is currently the CCo and transmitting the Central Beacon.

Table 482: CCo Status

CCo Status Value	Interpretation
0b0	STA is not the CCo.
0b1	STA is the CCo.

PCo Status

PCo Status indicates whether the STA is currently designated by the CCo to be a PCo and is currently transmitting a Proxy Beacon.

Table 483: PCo Status

PCo Status Value	Interpretation
0b0	STA is not a PCo.
0b1	STA is a PCo.

Backup CCo Status

Backup CCo Status indicates whether the STA has been designated by the CCo as a Backup CCo and is currently acting as a Backup CCo.

Table 484: Backup CCo Status

Backup CCo Status Value	Interpretation
0b0	STA is not a Backup CCo.
0b1	STA is a Backup CCo.

NumDisSTA

NumDisSTA is set to specify the number of entries in the STA's Discovered STA List.

NumDisNet

NumDisNet is set to specify the number of entries in the STA's Discovered Network List.

- GREEN PHY Capability

The GREEN PHY Capability field indicates whether the STA is GREEN PHY Capable or not and if so, the version of HomePlug GREEN PHY it supports. The interpretation of this field is as described in Table 4-79.

- HPAV Version (GREEN PHY)

The HPAV Version field indicates whether the STA supports any version of HomePlug AV and if so, the version of HomePlug AV it supports. The interpretation of this field is as described in Table 4-79.

Beacon Period Start Time Offset BENTRY

Beacon Period Start Time Offset BENTRY shall always be present in Proxy Beacons and Discover Beacons. BPSTO BENTRY shall also be present in Central Beacons when the AVLN is operating in CSMA-Only mode. This BENTRY indicates the offset of the start of the Preamble of this Beacon PPDU from the start time of the most recent Central Beacon Period of the corresponding AVLN.

Table 485:Beacon Period Start Time Offset BENTRY

Field	Octet Number	Field Size (Octets)	Definition
BPSTO	0 - 3	4	Beacon Period Start Time Offset, in multiple of 40 nanoseconds

0x000000 = zero nanoseconds

0x000001 = 40 nanoseconds, and so

BPSTO	0 - 2	3	Beacon Period Start Time Offset, in multiple of 40 nanoseconds 0x000000 = zero nanoseconds 0x000001 = 40 nanoseconds, and so on

Encryption Key Change BENTRY

Encryption Key Change BENTRY indicates that one of the AVLN's fundamental encryption keys is going to change.

Table 486: Encryption Key Change BENTRY

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
KCCD	0	0 - 5	6	Key Change Countdown
KBC		6	1	Key Being Changed
RSVD		7	1	Reserved
NewEKS	1	0 - 3	4	New Key's EKS or PEKS
RSVD		4 - 7	4	Reserved

Key Change Countdown (KCCD)

Key Change Countdown (KCCD) is a 6-bit field that indicates the number of Beacon Periods after which the new Key will become effective. When this BENTRY is present, KCCD shall decrement by one in each Beacon Period until the countdown is complete.

Table 487: KCCD Interpretation

KCCD Value	Interpretation
0x00	Reserved
0x01	Key Change will occur in the next Beacon Period, and so on.

Key Being Changed (KBC)

Key Being Changed (KBC) is a 1-bit field that identifies which key type (EKS or PEKS) is being changed.

Table 488: KBC Interpretation

KBC Value	Interpretation
0b0	Key is a Frame-level Encryption Key (NEK).
0b1	Key is a Payload Encryption Key (NMK is only legal value)

New Key's EKS (NewEKS)

If KBC = 0b0, NewEKS is the EKS of the new NEK that has been recently distributed to the

active STAs.
If KBC = 0b1, NewEKS = 0b0011, the PEKS value for NMK Encryption Key, which is the only Payload Encryption Key that requires a countdown in the Beacon. A new NMK and NID pair has been recently distributed to the active STAs.

CCo Handover BENTRY

Central Coordinator Handover BENTRY indicates an ongoing transfer of CCo function from the current station to a new station in the network.

Table 489: Central Coordinator Handover BENTRY

Field	Octet Number	Bit Number	Field Size	Definition
HCD	0	0 - 5	6	Handover Countdown
RSVD		6 - 7	2	Reserved
NCTEI	1	0 - 7	8	New CCo TEI

Handover Countdown (HCD)

Handover Countdown (HCD) is a 6-bit field that indicates the number of Beacon Periods after which the CCo handover will occur. When this BENTRY is present, HCD shall decrement by one in each Beacon Period until the countdown is complete.

Table 490: Handover Countdown Interpretation

HCD Value	Interpretation
0x00	Reserved
0x01	Handover will occur in the next Beacon Period, and so on.

New CCo TEI (NCTEI)

New CCo TEI (NCTEI) is an 8-bit field that indicates the Terminal Equipment ID of the New CCo.

Beacon Relocation BENTRY

Beacon Relocation BENTRY indicates relocation of Beacon to a different part of the AC line cycle.

Table 491: Beacon Relocation BENTRY

Field	Octet	Bit Number	Bits	Definition
RCD	0	0 - 5	6	Relocation Countdown
RLT		6	1	Relocation Type
LGF		7	1	Leaving Group Flag
RLO	1	0 - 7	17	Relocation Offset 0x00000 = zero 0x00001 = 0.32 sec, and so on
	2	0 - 7		
	3	0		

RLSlotID		1 - 3	3	Relocation SlotID
RSVD		4 - 7	4	Reserved

Relocation Countdown (RCD)

Relocation Countdown (RCD) is a 6-bit field that indicates the number of Beacon Periods after which the Beacon relocation will occur. When this BENTRY is present, RCD shall decrement by one in each Beacon Period until the countdown is complete. The Beacon Relocation BENTRY shall become effective and the BENTRY removed from the Beacon MPDU Payload in the Beacon immediately following the Beacon Period when RCD equals 1.

Table 492: Relocation Countdown Interpretation

RCD Value	Interpretation
0x00	Reserved
0x01	Beacon relocation will occur in the next Beacon Period, and so on.

Relocation Type (RLT)

Relocation Type (RLT) is a 1-bit field used to indicate whether the relocation is based on an Offset or change in the Beacon Slot number. Relocation SlotID type shall only be used when operating in Coordinated Mode. The new value for Relocation SlotID may be smaller or larger than the current Beacon Slot ID.

Table 493: Relocation Type Interpretation

RLT Value	Interpretation
0b0	Relocation type is Relocation Offset
0b1	Relocation type is Relocation SlotID

Leaving Group Flag (LGF)

The Leaving Group Flag (LGF) indicates the CCo is relocating the Beacon to leave the Group. This flag shall only be set when Relocation Type is Relocation Offset.

Table 494: Leaving Group Flag Interpretation

LGF Value	Interpretation
0b0	Not leaving the Group of networks
0b1	Leaving the Group of networks

Relocation Offset (RLO)

Relocation Offset (RLO) is an unsigned 17-bit field that indicates the offset of the new Beacon location from the current Beacon location. Figure 416 shows an example of Beacon relocation. This field indicates the time in multiples of 0.32 sec. Relocation SlotID shall be set to indicate to the value of Beacon Slot ID when the Offset becomes effective.

Note: When Relocation Offset is used, the relocated Beacon is always delayed in time relative to the old Beacon location. As shown in Figure 416, when Relocation occurs, there is always a dead spot between the end of the current Beacon Period and the beginning of the next (relocated) Beacon Period.

Figure 416: Example of Beacon Relocation

Relocation SlotID (RLSlotID)

Relocation SlotID (RLSlotID) is a 3-bit field that indicates the new Beacon Slot ID in a Group of networks. Relocation Offset shall be set to zero when Relocation Type is Relocation SlotID.

AC Line Sync Countdown BENTRY

AC Line Sync Countdown BENTRY is used to indicate the number of Beacon Periods in which the AC Line Cycle Synchronization of the Current CCo is going to change. When this BENTRY is present, the Countdown field shall decrement by one in each Beacon Period until the countdown is complete.

Table 495: AC Line Sync Countdown BENTRY

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
Countdown	0	0 - 5	6	Countdown indicates 0x00 = reserved 0x01 = change will be effective in the next Beacon Period, and so on.
RSVD		6 - 7	2	Reserved
Reason Code	1	0 - 1	2	Reason Code for the AC Line Sync Countdown 0b00 = AVLN Shut Down or leaving Group 0b01 = AC Line Cycle Synchronization handover to a CCo in a smaller Beacon Slot 0b10 – 0b11 = reserved
RSVD		2 - 7	6	Reserved

Change NumSlots BENTRY

The Change NumSlots BENTRY is used to change or update NumSlots for a Group of networks. This BENTRY shall be present in Discover and Proxy Beacons when present in the Central Beacon. Refer to Section 4.4.1.4 for use of this BENTRY.

Table 496: Change NumSlots BENTRY

Field	Octet Number	Bit Number	Field Size (Bits)	Definition

NSCCD	0	0 - 5	6	NumSlot Change Countdown
RSVD		6 - 7	2	Reserved
NewNumSlot	1	0 - 2	3	New NumSlot value
RSVD		3 - 7	5	Reserved

NumSlot Change Countdown (NSCCD)

NumSlot Change Countdown (NSCCD) is a 6-bit field that indicates the number of Beacon Periods after which the new NumSlot will become effective. When this BENTRY is present, NSCCD shall decrement by one in each Beacon Period until the countdown is complete.

Table 497: NSCCD Interpretation

NSCCD Value	Interpretation
0x00	Reserved
0x01	NumSlot change will occur in the next Beacon Period, and so on.

New NumSlot Value (NewNumSlot)

New NumSlot Value (NewNumSlot) is a 3-bit field that is the value of the NumSlot field in the Beacon MPDU Payload that will become effective for all networks in a Group of networks when the countdown is complete.

Change HM BENTRY

The Change HM BENTRY is used to change or update the Hybrid Mode (HM) field for a Group of networks. This BENTRY shall be present in Discover and Proxy Beacons when present in the Central Beacon. Refer to Section 9.10 for use of this BENTRY.

Table 498: Change HM BENTRY

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
HMCCD	0	0 - 5	6	Hybrid Mode Change Countdown
NewHM	0	6 - 7	2	New Hybrid Mode value

Hybrid Mode Change Countdown (HMCCD)

Hybrid Mode Change Countdown (HMCCD) is a 6-bit field that indicates the number of Beacon Periods after which the new value for HM shall become effective. When this BENTRY is present, HMCCD shall decrement by one in each Beacon Period until the countdown is complete.

Table 499: HMCCD Interpretation

HMCCD Value	Interpretation
0x00	Reserved
0x01	HM change will occur in the next Beacon Period, and so on.

New Hybrid Mode Value (NewHM)

New Hybrid Mode value (NewHM) is used to update the HM field in the Beacon MPDU Payload

for all networks in a Group of networks when the countdown is complete. The new value for HM is determined by the rules defined in Section 9.10.

Change SNID BENTRY

The Change SNID BENTRY is used to change or update the SNID (Short Network Identifier) field for an AVLN. This BENTRY shall be present in Discover and Proxy Beacons when present in the Central Beacon. Refer to Section 4.4.1.4 for use of this BENTRY.

Table 4100: Change SNID BENTRY

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
SCCD	0	0 - 3	4	SNID Change Countdown
NewSNID	0	4 - 7	4	New SNID value

SNID Change Countdown (SCCD)

SNID Change Countdown (SCCD) is a 4-bit field that indicates the number of Beacon Periods after which the new SNID value will become effective. When this BENTRY is present, the SCCD shall decrement by one in each Beacon Period until the countdown is complete.

Table 4101: SCCD Interpretation

SCCD Value	Interpretation
0x00	Reserved
0x01	The new SNID value will become effective in the next Beacon Period, and so on.

New SNID Value

New SNID value (NewSNID) is used to update the SNID field in the Beacon MPDU, the SOF, and elsewhere for all STAs in an AVLN when the countdown is complete. The new value for SNID is determined by the rules defined in Section 4.4.1.4.

Power Save BENTRY for GREEN PHY

The Power Save BENTRY is used to communicate Power Save information. This BENTRY shall be present in Discover and Proxy Beacons when present in the Central Beacon. Refer to Section 5.9 for use of this BENTRY.

Table 4102: Power Save BENTRY

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
BPCnt	0	0 – 7	12	Beacon Period Count
	1	0 - 3		
SPSF		4	1	Stop Power Save Flag
AV11PF		5	1	HomePlug AV 1.1 Stations Present Flag
RSVD		6-7	2	Reserved
TPSS	2	0-7	8	Power Save Schedule of the STA transmitting this Beacon
PSSI	3	0-7	8	Power Save State Identifier
TEI[1]	-	0-7	8	TEI of most recent station whose Power Save state changed
PSS[1]	-	0-7	8	Power Save Schedule of TEI[1]
…				
TEI[N]	-	0-7	8	TEI of station Nth most recent station whose Power Save state changed
PSS[N]	-	0-7	8	Power Save Schedule of TEI[N]

Beacon Period Count

PSP AWD	0 0	0-3 4-8	4 4	Power Save Window Period 0x0 = 1.5msec, 0x1 = 2msec, 0x2 = 4msec, 0x3 = 8msec, 0x4 = 16msec, 0x5 = 32msec, 0x6 = 64msec, 0x7 = 128msec, 0x8 = 256msec, 0x9 = 512 Beacon Periods 0xA = 1024 Beacon Periods 0xB = 2048 Beacon Periods 0xC = 4096 Beacon Periods 0xD = 8192 Beacon Periods 0xE = 16384 Beacon Periods 0xF = Reserved
				Beacon Periods 0xD = 2^5 = 32 Beacon Periods 0xE = 2^6 = 64 Beacon Periods 0xF = Reserved

PSP	0	0-3	4	Power Save Period 0x0 = 2^0 = 1 Beacon Period, 0x1 = 2^1 = 2 Beacon Periods 0x2 = 2^2 = 4 Beacon Periods … 0x9 = 2^9 = 512 Beacon Periods 0xA = 2^10 = 1024 Beacon Periods 0xB – 0xE = Reserved 0xF = Station is not in Power Save

Vendor-Specific BENTRY

The Vendor-Specific BENTRY enables vendor specific extensions to the Beacon Management Information. The ability to transmit and receive vendor-specific BENTRIES is optional.

The first three octets of the Vendor-Specific BENTRY shall contain the IEEE-assigned OUI as described in reference [4]. The bit and octet order of the Organizationally Unique Identifier (OUI) here and elsewhere in this specification is identical to the bit and octet order of the MAC address as described in Section 4.1.2. The remaining fields in this BENTRY are defined by the vendor.

Table 4104: Vendor Specific BENTRY

Field	Octet	Bit Number	Bits	Definition
OUI	0 – 2	0 - 7	24	Organizationally Unique Identifier
Vendor Defined	-	-	var	Vendor defined

Octet Pad (OPAD)

Octet Pad (OPAD) is a variable-length field used to ensure that the Beacon MPDU Payload is 136 octets long.

Beacon Payload Check Sequence (BPCS)

Beacon Payload Check Sequence (BPCS) is a 32-bit field that is used to check the integrity of the Beacon payload. BPCS is as 32-bit CRC computed on the Beacon payload excluding the BPCS field.

Proxy Level (Plevel) for GREEN PHY

The Proxy Level (Plevel) field shall be set to **0b000** if the Central Beacon of the AVLN is reliably detected. Otherwise, Plevel shall be set by adding **0b001** to the lowest value of Plevel received in Proxy Beacons of the AVLN that are reliably detected, but shall not exceed **0b111** Plevel shall be

set to **0b000** in Central Beacons.

Reusable SNID Flag (RSF) for GREEN PHY

Reusable SNID Flag (RSF) is used to allow other AVLNs to reuse the same SNID without ambiguity. A CCo that needs to allocate more than 63 TEIs shall set the RSF to 0b0 to reserve the complete TEI range. A CCo that does not need to allocate more than 63 TEIs shall set its RSF to 0b1 to allow another CCo to reuse the same SNID. In this case, the CCo shall allocate the TEIs in the range of [0x01-0x3F], or [0x40-0x7F] or [0x80-0xBF] or [0xC0-0xFE] including its own TEI.

Table 4-105: Reusable SNID Flag Interpretation

RSF Value	Interpretation
0b0	The SNID cannot be reused. The whole TEI range is in use by a single AVLN
0b1	The SNID can be reused if any of the 4 TEI ranges are not being used..

Format of Sound MPDU Payload

The Sound MPDU Payload carries 136 or 520 octets of payload modulation using Mini-ROBO or ROBO Modulation, respectively. Sound MPDUs are used during the channel estimation process, with the transmitter specifying whether the Sound MPDU has 136 or 520 octets of payload (refer to Section 4.4.1.5.2.11). The format of the Sound MPDU Payload is shown in Table 4. The Sound MPDU Payload shall not be encrypted.

Table 4106: Sound Payload Fields

Field	Octet Number		Field Size (Octets)	Definition
ZPAD	0 - 131 or 0 - 515		132 or 516	Zero Pad
SPCS	132 - 135 or 516 - 519		4	Sound Payload Check Sequence

Zero Pad (ZPAD)

Zero Pad (ZPAD) field consists of 132 or 516 octets of zeros.

Sound Payload Check Sequence (SPCS)

Sound Payload Check Sequence (SPCS) is used to check the integrity of the Sound payload. SPCS is a 32-bit CRC computed on the Sound payload.

MAC Functional Description

Beacon Period Structure and Channel Access Mechanism

As with HomePlug AV, HomePlug GREEN PHY uses Beacon-based periodic channel access mechanism. This section provides details on the dependence of the Beacon Period on the underlying AC Line cycle frequency and channel access within the Beacon Period.

Beacon Period and AC Line Cycle Synchronization

Informative Text

To improve performance and QoS stability in the presence of common powerline noise, the Beacon Period is synchronized with the 50 or 60 Hz AC line cycle. The duration of each Beacon Period is twice that of the AC line cycle period. There are variations in the phase and frequency of the AC line cycle. The CCo is responsible for performing this function. This section recommends the synchronization approach to provide consistent behavior and performance among different manufacturers.

Operation in scenarios where there is no AC line cycle (e.g., a DC network powerline) or when the AC line cycle is different than 50 Hz or 60 Hz is described in Section 5.1.1.2.

Line Cycle Synchronization

The powerline frequency will vary about the nominal line frequency of 60 Hz (or 50 Hz) due to variability in the power generation and distribution system. Channel adaptation and Tone Map generation rely on AC line cycle synchronization to adapt optimally to synchronous powerline noise. CCos shall phase lock the Beacon transmission to the AC line cycle to provide synchronization for all stations in the network. This will ensure that the Tone Map remains valid, even when the underlying AC line cycle frequency and phase characteristics change.

Line-cycle synchronization is achieved by having the CCo track a particular point in the AC line cycle using a Digital Phase Locked Loop (DPLL) or equivalent. Using a filter or digital lock loop algorithm, the CCo is able to eliminate NTB jitter in the measurement (e.g., zero crossing). The CCo uses its local tracking history to also predict future locations of the Beacons that it announces to all stations in the Beacon schedule.

One approach to AC line cycle synchronization is to use a detector to indicate the occurrence of a particular point in the AC line cycle (e.g., the rising edge zero-cross). The CCo's Network Time Base (NTB) (refer to Section 5.5) is captured at the time the detector is triggered at each line cycle. Time (denoted $LCTe_n$). The output is the filtered or smoothed estimate of the current line Cycle Time, denoted $LCTe_n$. The following algorithm is recommended for tracking Line Cycle Time (LCT, refer to Figure 51).

Initialization

$LCTe_0 = LCT_0$

$LCTe_1 = LCT_1$

$PERa_0 = PERa_1 = LCT_1 - LCT_0$

Tracking

Line Cycle Timing estimation ($LCTe_n$) for $n \geq 2$:

$PERa_n = PERa_{n-1} + w_p (ACT_n - LCT_{n-1} - PERa_{n-1})$

$LCTe_n = LCTe_{n-1} + PERa_n + w_f (LCT_n - (LCTe_{n-1} + PERa_n))$

where LCT_n is the value of the NTB at the n^{th} Line Cycle Time measurement (e.g., zero crossing).

Informative Text

One approach to AC line cycle synchronization is to use a detector to indicate the occurrence of a particular point in the AC line cycle (e.g., the rising edge zero cross). The CCo's Network Time Base (NTB) (refer to Section 5.5) is captured at the time the detector is triggered at each Line Cycle Time (denoted LCT_n). The output is the filtered or smoothed estimate of the current Line Cycle Time, denoted $LCTe_n$. The following algorithm is recommended for tracking Line Cycle Time (LCT, refer to Figure 51).

Initialization

$LCTe_0 = LCT_0$

$LCTe_1 = LCT_1$

$PERa_0 = PERa_1 = LCT_1 - LCT_0$

Tracking

Line Cycle Timing estimation (LCTe) for n ≥ 2:

$PERa_n = PERa_{n-1} + w_p (LCT_n - LCT_{n-1} - PERa_{n-1})$

$LCTe_n = LCTe_{n-1} + PERa_n + w_t (LCT_n - (LCTe_{n-1} + PERa_n))$

Where LCT_i is the value of the NTB at the i^{th} Line Cycle Time measurement (e.g., zero crossing time). $LCTe_i$ is the smoothed or filtered estimate of the i^{th} Line Cycle Time, $PERa_i$ is the filtered or smoothed estimate of the Line Cycle Period, and w_p and w_t are weighting constants of the form $1/2^k$, where k is a positive integer.

Larger values of k provide better filtering of the jitter caused by local noise or phase disturbances, but can result in poorer tracking of the AC line-cycle phase. It is also necessary to limit or clip the value of LCT_n to an expected range at the input to these functions so that occasional large jitter does not result in unnecessary large variations to the Beacon Period.

To ensure that stations with persistent allocations can transmit even when a Beacon is not detected, the CCo provides information about the location of future Beacons within the Beacon Payload. Figure 51 shows the Line Cycle Time and Beacon Transmit Time (BTT, defined in Section 5.5). The location of a Beacon that is p Beacon Periods in the future (BTT_{m+p}) shall be computed at the CCo as follows:

$$BTS_{m+p} = LCTe_n + (2*p*PERan) + BeaconOffset$$

$$BTO_{m+p} = BTS_{m+p} - BTS_{m+p-1} - 1{,}000{,}000; \text{ for 50Hz AC Line cycle}$$

$$BTO_{m+p} = BTS_{m+p} - BTS_{m+p-1} - 833{,}333; \text{ for 60Hz AC Line cycle}$$

where:

BTS_m is the value of the NTB at the current BTT.

BeaconOffset is the offset of the location of the Beacon from the Line Cycle Time Estimate.

BTO_{m+p} is the value of the Beacon Transmission Offset p-1 (BTO[p-1] (refer to Section 4.4.1.5.1.2) indicated in the Beacon Frame Control.
In general, BeaconOffset is fixed and will only change when the Beacon is relocated.

Figure 51: Line Cycle Time and Beacon Transmit Time

Synchronization in the absence of 50Hz or 60Hz Line Cycle
In scenarios where AVLN operates over power lines using DC or non-50 Hz/60 Hz AC, the CCo shall be preconfigured to select a beacon period matching either 50Hz (i.e., beacon period is 40msec) or 60Hz (i.e., beacon period is 33.33msec) based on the NTB.
STAs in the AVLN may either be preconfigured with the beacon period or infer the beacon period based on the periodicity of the central beacons. STAs in the AVLN shall track the beacon period start time based on the information provided by the CCo in the central beacons.

Line Cycle Synchronization for GREEN PHY
A GREEN PHY device must be capable of synchronizing to the AC line cycle. This feature enables coexistence with HPAV 1.1 and ISP (see chapter 14).
Beacon Period Structure
As with HomePlug AV, the HomePlug GREEN PHY Beacon Period is twice the underlying AC line cycle period. Thus, when operating in power line environments with an AC line cycle frequency of 60 Hz, the Beacon Period will be 33.33 msec. Similarly, when operating in power line environments with an AC line cycle frequency of 50 Hz, the Beacon Period will be 40 msec.
There are three types of Beacons: Central Beacon, Proxy Beacon, and Discover Beacon (refer to Section 4.4.3.4).
Central Beacons are issued by the CCo of an AVLN, and contain coordination information for the STAs within its AVLN, and for CCos of neighboring AVLNs.
Discover Beacons are used to exchange information about network topology and, in particular, to discover neighbor networks.
Proxy Beacons are issued by Proxy CCos within an AVLN to relay the information contained in the Central Beacon to hidden stations.
When and how these various types of Beacon are sent (and expected by a STA) depends on the network mode of the AVLN, which is indicated in the Beacon Delimiter (refer to Section 4.4.3.13).
The channel access information is communicated between CCos of neighboring AVLNs using the Regions BENTRY, from which a CCo determines when STAs within its AVLN may use CSMA/CA access or be assigned exclusive access through TDMA. The CCo then conveys this information to the STAs within its AVLN using Persistent and Non-persistent Schedule BENTRYs. The term “schedule” will be used to refer generically to persistent or non-persistent schedule information in either of these types of BENTRY, and both of these BENTRY types will be referenced generically as “Schedule BENTRYs.” A STA uses this schedule information to determine when it is eligible to access the channel using CSMA/CA or TDMA.
The overall structure of a Beacon Period consists of periods for transmission of Beacons and periods for transmission of data by STAs in the AVLNs sharing the medium. Within the

specification, the terms Contention Period (CP) and Contention Free Period (CFP) are used to indicate intervals of time where CSMA/CA- and TDMA-based channel access mechanisms are respectively used for medium sharing. How this is done depends on the AVLN's network mode (refer to Chapter 8) and the QoS needs of the streams in the AVLN. Regions BENTRYs specify what activity is possible for an AVLN for every interval of the Beacon Period, and are only relevant to coordination between neighbor networks (refer to Chapter 8); STAs within an AVLN do not interpret Regions BENTRYs. Schedule BENTRYs specify for a particular AVLN its CPs, CFPs, and by omission, periods during which no access is allowed (again, depending on the AVLN's network mode). The "big picture" intervals described in the Regions BENTRYs are called regions, while the AVLN-specific access intervals carried in Schedule BENTRYs are called allocations.

Figure 52 shows the Beacon Period synchronized to AC line cycle with Beacon, CSMA, and Reserved Regions, along with Persistent and Non-Persistent Contention-Free and CSMA allocations, for the case of an AVLN that is operating in Uncoordinated mode and is supporting three TDMA Sessions.

Figure 52: Example of Beacon Period Structure in Uncoordinated Mode

A Beacon Region consists of one or more Central Beacons. A Beacon consists of a Preamble, a Frame Control, and a 132-octet Beacon payload. The CCo generates the Central Beacon and transmits it in the Beacon Region in Uncoordinated and Coordinated modes. The location of the Beacon Region is specified in the Regions BENTRY for neighbor networks, but STAs within an AVLN calculate its location and duration from other information carried in the Beacon. In CSMA-Only mode, there is no Beacon Region.

Information describing the allocations within the Beacon Period is broadcast in the Beacon payload by using one or more Schedule Beacon Entries. This information is used by STAs within the network to coordinate sharing of bandwidth. The Beacon carries two types of scheduling information:

Non-persistent scheduling Information

Persistent scheduling Information

Persistent CFP schedule information is carried in the Persistent Schedule BENTRY. Persistent Schedule information is valid for the multiple periods and can contain the following types of allocations:

Persistent CSMA/CA Allocations (shared or local)

Persistent TDMA Allocations

The Persistent Schedule BENTRY has two fields that are used to interpret the persistence of schedule information:

Current Schedule Countdown

Preview Schedule Countdown

If the schedule is not changing, the schedule information reflects the current schedule and the Preview Schedule Countdown shall be zero. In this case, the Current Schedule Countdown indicates the minimum number of Beacon Periods for which the current schedule may be assumed valid. The Current Schedule Countdown value must not be smaller than the previous Current

Schedule Countdown value minus one. In this way, stations that miss Beacons will know how long they may use the current schedule information they have. It is important to note that to transmit in a TDMA allocation, a STA must have knowledge of the Beacon Period Start Time as well as the schedule information for that Beacon Period.

Current Schedule Countdown value may indicate indefinite persistence (refer to Section 4.4.3.15.4.2.2). This is needed when Beacons are sent using CSMA/CA. Persistent schedules with indefinite persistence shall only be used in CSMA-Only mode. An indefinitely persistent allocation remains valid until it is superseded by newer schedule information in a Central Beacon sent at some later time. When the new schedule information is sent, it should have a suitably large Current Schedule Countdown value depending on the reliability of Beacon reception in the AVLN. Any STA that does not receive the new schedule information by the time it becomes effective may transmit according to the old, indefinitely persistent allocation information, so caution is advised in the use of indefinite persistence.

When the CCo determines to change the schedule, it may transmit a Persistent Schedule BENTRY announcing the Preview Schedule. In this BENTRY, the Preview Schedule Countdown is set to a non-zero value. This value indicates that the schedule information is a new schedule (not the current schedule) and when the new schedule will take effect. In this case, the Current Schedule Countdown previews the value that the new schedule will have for its Current Schedule Countdown during the first Beacon Period when it takes effect. The Current Schedule Countdown value in this case is a preview value and must not change from its initial value. In this way, stations that miss Beacons will know when they can use the new schedule information they have and for how long it will be valid. This approach allows a number of repetitions of the new schedule to ensure that all stations have the relevant information, even if some stations miss the Beacon during the Beacon Period when the new schedule takes effect.

Each Central Beacon should carry a Persistent Schedule BENTRY with the Preview Schedule when the schedule is changing. It may also carry a separate Persistent Schedule BENTRY with the Current Schedule within the same Beacon. If it does, the Current Schedule Countdown field in this BENTRY shall be decremented to indicate the start of the new schedule.

There shall not be more than one Preview Schedule in existence at any time. This is more than just not allowing multiple BENTRYs with Preview Schedules in the same Beacon. If the CCo has announced a Preview Schedule, that Preview Schedule must become the current schedule before the CCo can announce a new Preview Schedule.

Figure 53 shows examples of schedule changes. Initially, Schedule A is in effect. In Beacon Period 2, the CCo determines that the schedule should change to Schedule B. So, beginning in Beacon Period 3, the CCo includes a BENTRY containing Schedule B with the values of PSCD and CSCD shown for the schedule. (The previewed schedules are shaded in the figure.) Although the CCo has the option of transmitting both Schedule A and Schedule B in separate BENTRYs, transmitting Schedule A is no longer necessary.

Once the CCo has announced Schedule B in Beacon Period 3, the earliest that Schedule B can be replaced by a new Schedule C is Beacon Period 9. That is because while the PSCD for Schedule B is non-zero, the CSCD is a preview of what the CSCD will be in the first Beacon Period that B is current (Beacon Period 6). Since the CCo chose a current schedule persistence preview value of 2,

Schedule B must be the current schedule for 3 Beacon Periods.

Figure 53: Example of Beacon Schedule Persistence

Persistence of schedule information improves reliability, but decreases responsiveness to urgent needs. A STA that requires additional allocation might communicate its request to the CCo in the same Beacon Period (3) in which a new schedule (B) is announced. This requires the session to wait for the announced schedule (B) to take effect before a revised schedule (C) can be broadcast. The revised schedule (C) must then countdown before it becomes effective, so the session may be forced to wait several Beacon Periods before it can obtain the additional allocation it needs.

To allow rapid response to urgent allocation requests, some portion of the contention-free allocation schedule may be non-persistent. This Non-Persistent allocation (provided using Non-Persistent Schedule BENTRY) provided for established CFP connections is termed Extra Allocation. It is necessary for a Station to receive the Beacon to utilize any Extra Allocation it is given in a Beacon Period, which makes Extra Allocations less reliable than the persistent allocations.

Non-Persistent CFP Schedule information is carried in the Non-Persistent Schedule BENTRY. Non-Persistent Schedule is valid only for the current period and can contain the following types of allocations,

Extra Allocations

CSMA/CA Allocations

Discover Beacon Allocation

The Discover Beacon Allocation provides Discover Beacon transmission opportunities for various stations in the network.

Beacon Period Structure in CSMA-Only Mode

In CSMA-Only mode, the Beacon Period structure consists of CSMA Regions and Stay-out Regions. The locations of the CSMA Regions are inferred from the Schedule BENTRYs of the Beacon payload. Details on how Stay-out Regions are determined can be found in Chapter 8. CSMA/CA will be used exclusively by all traffic in CSMA-Only mode. There are no Global Links (refer to Section 5.2), and all Stations can send traffic using CSMA/CA without regard to the start of the Beacon Period (i.e., a transmission can extend across the Beacon Period boundary since that region is not reserved for Central Beacon transmission in CSMA-Only mode). Schedules specify the locations of CSMA/CA allocation. Persistent schedules may be made with indefinite persistence (refer to Section 4.4.3.15.4.2.2). This is needed due to the unreliability of Beacon reception when CSMA/CA is used. A STA that has not heard a Central Beacon or Proxy Beacon for several Beacon Periods shall use its local clock to estimate the locations of the CSMA/CA allocations, and transmit in them, as long as the schedule information remains valid. An indefinitely persistent allocation remains valid until it is superseded by newer schedule information in a Central Beacon sent at some later time.

In CSMA-Only mode, all Beacons are transmitted using CSMA/CA. The Central Beacon should be transmitted as near to the start of the Beacon Period as possible. Proxy Beacons (if any) should be transmitted as soon after the Central Beacon is received as possible, and both shall be sent at priority CAP3. Discover Beacons should be transmitted as soon as possible after being designated

by the CCo in the Central Beacon, and they should be sent at priority CAP2. Since CSMA/CA transmissions rely on carrier sensing, Beacon reliability can be expected to be significantly better than that of TDMA Beacons in environments where TDMA allocations cannot be guaranteed due to hidden nodes. Implementations may optionally use RTS/CTS to enhance Beacon reliability. A Beacon sent in CSMA-Only mode does not have an explicit acknowledgment (i.e., SACK). Beacon transmission is followed by a Beacon-to-Beacon Interframe Space (B2BIFS), followed by Priority Resolution Slots.

In CSMA-Only mode, all transmissions are sent using Hybrid Delimiters. This simplifies neighbor network detection and coordination. Optionally, STAs may use non-compatible HomePlug 1.0 frame lengths when there are no HomePlug 1.0 stations detected, as expressed in the value of the Hybrid Mode field of the Beacon (refer to Section 4.4.3.2). Since all transmissions use CSMA/CA, Contention Free Period Initiation (CFPI) allocations are never used in CSMA-Only mode (refer to Chapter 9).

Figure 54 shows an example of the Beacon Period Structure in CSMA-Only Mode. Note that the Central Beacon is sent near the start of the Beacon Period, but had to first wait until another transmission ended, then contend for the channel using CSMA/CA with priority CAP3.

The Central Coordinator will maintain a logical Beacon Period Start Time (BPST) by indicating one or more Beacon Transmission Offsets (BTOs) in the Frame Control of the Central Beacon. Maintenance of the logical BPST is essential for channel adaptation and neighbor network coordination in CSMA-Only mode. Since CSMA collisions can result in Beacon loss, all stations in the AVLN should use local AC line cycle tracking to estimate the BPST when CCo Beacons cannot be detected. Together with indefinitely persistent CSMA/CA allocations, this allows a STA to transmit even when Beacons are not received reliably.

Figure 54: Beacon Period Structure in CSMA-Only Mode

Beacon Period Structure in CSMA-Only Mode for GREEN PHY

A GREEN PHY station is required to implement CSMA-Only Mode. Therefore, a GREEN PHY station must be capable of operating as an Level-0 CCo. Refer to Table 11-5b for a comparison between HPAV Level 0 CCo and HP GREEN PHY Level 0 CCo.

Beacon Period Structure in Uncoordinated Mode

The Beacon Period structure in Uncoordinated Mode consists of a Beacon Region followed by a CSMA Region optionally followed by one or more Reserved Regions and CSMA Regions. The duration of the Reserved Regions and CSMA Regions are inferred from the Schedule BENTRYs of the Beacon payload.

A CSMA Region must immediately follow the Beacon Region, and it must have a minimum length of MinCSMARegion as defined in Section 2.4. Additional CSMA Regions may also be present in the Beacon Period; the minimum length parameter does not apply to these additional CSMA regions. CSMA Regions use the channel access mechanism described in Section 5.1.3.1.

If there are streams that require QoS, and the CCo is capable of QoS management, there may be allocations for specific streams in the Reserved Regions. These may be either persistent or non-persistent, as discussed in Section 5.1.1.2.1.

Figure 55 shows the Beacon Period Structure in Uncoordinated mode.

The Central Beacon is always transmitted in Hybrid Mode using TDMA in the one and only Beacon slot in the Beacon Region, which is aligned with the start of the Beacon Period. All STAs refrain from transmitting during this interval. Proxy Beacons and Discover Beacons are also transmitted in Hybrid Mode using TDMA in intervals allocated for them in the Reserved Regions. While all Beacons are always sent in Hybrid Mode, all other traffic is sent in a mode that depends on the Hybrid Mode (HM) field value in the Beacon and the region in which the transmission occurs (refer to Section 4.4.3.2).

AC Line Cycle synchronization is performed by the CCo, and all STAs within the AVLN synchronize to the CCo using the Central and Proxy Beacons. Depending on the schedule persistence and the number of Beacon Transmission Offset (BTO) values, a STA that misses one or more Beacons may still be able to transmit in the appropriate times (either TDMA assigned to one of its streams, or CSMA/CA), but once either the future Beacon location information from the BTOs or the persistence of the schedule information has been exhausted, a STA must not transmit as part of that AVLN until it receives another Beacon. Lacking knowledge of the Beacon Period Start Time, a STA cannot be guaranteed of remaining silent during the Beacon Region, nor can it correctly interpret the schedule information. Lacking schedule information, it cannot know when CSMA/CA regions occur, nor its TDMA allocations.

Figure 55: Example of Beacon Period Structure in Uncoordinated Mode

Beacon Period Structure in Uncoordinated Mode for GREEN PHY

A station that only implements GREEN PHY is not required to be a Level-1 CCo and hence will not instantiate a network in uncoordinated mode. However, a GREEN PHY station could be a member of an AVLN operating in Uncoordinated Mode. Therefore, a GREEN PHY station must be capable of operating under an HPAV Level-1 CCo even though a GREEN PHY station itself is not required to be a Level-1 CCo.

When a network is operating in Uncoordinated Mode and a GPP allocation is present, the GPP allocation shall immediately follow the Beacon region and the minimum CSMA region shall immediately follow the GPP allocation. Refer to section 7.8.5 for information on GPP Allocation.

Beacon Period Structure in Coordinated Mode

Coordinated Mode is only used when one or more neighboring AVLNs are present. The Beacon Period structure in Coordinated Mode consists of a Beacon Region with one or more Beacon slots, followed by a CSMA Region, optionally followed by one or more Reserved Regions, CSMA Regions, Stay-out Regions, and Protected Regions. The duration of the Reserved Regions and CSMA Regions are inferred by STAs in the AVLN from the Schedule BENTRYs of the Beacon payload. A CCo computes these regions according to the methods described in Chapter 8.

Note: An AVLN Operating in Coordinated mode might have only one Beacon slot in its Beacon Region.

A CSMA Region must immediately follow the Beacon Region, and it must have a minimum length of MinCSMARegion as defined in Section 2.4. Additional CSMA Regions may also be present in the Beacon Period; the minimum length parameter does not apply to these additional CSMA regions. CSMA Regions use the channel access mechanism described in Section 5.1.3.1.

If there are streams that require QoS, and the CCo is capable of QoS management, then there may

be allocations for specific streams in the Reserved Regions. These may be either persistent or non-persistent, as discussed in Section 5.1.1.2.1.
Figure 56 shows the Beacon Period Structure in Coordinated mode with a multi-slot Beacon Region, CSMA Regions, Reserved Regions, and Stay-out Regions.
The Central Beacon is always transmitted in Hybrid Mode using TDMA in one of the Beacon slots in the Beacon Region, which is aligned with the start of the Beacon Period. All STAs refrain from transmitting during this interval. Proxy Beacons and Discover Beacons are also transmitted in Hybrid Mode using TDMA in intervals allocated for them in the Reserved Regions.
While all Beacons are always sent in Hybrid Mode, all other traffic is sent in a mode that depends on the Hybrid Mode (HM) field value in the Beacon and the region in which the transmission occurs (refer to Section 4.4.3.2).

Figure 56: Example of Beacon Period Structure in Coordinated Mode
Beacon Period Structure in Coordinated Mode for GREEN PHY
A station that only implements GREEN PHY is not required to be a Level-2 CCo and hence will not instantiate a network in Coordinated Mode. However, a GREEN PHY station could be a member of an AVLN operating in Coordinated Mode. Therefore, a GREEN PHY station must be capable of operating under an HPAV Level-2 CCo even though a GREEN PHY station itself is not required to be a Level-2 CCo.
When a network is operating in Coordinated Mode and a GPP allocation is present, the GPP allocation shall immediately follow the beacon region and the minimum CSMA region shall immediately follow the GPP allocation. Refer to section 7.8.5 for information on GPP Allocation.
Channel Access
Although HomePlug AV stations use both CSMA/CA as in the HomePlug 1.0.1 specification and a Beacon-based TDMA mechanism for sessions requiring guaranteed QoS, HomePlug GREEN PHY stations are only required to use CSMA/CA.
CSMA/CA Channel Access
The CSMA/CA channel access mechanism used by HomePlug AV Stations is the same as that of HomePlug 1.0.1,reference [1], with the following two exceptions:
A collision is inferred by AV stations under conditions described in Section 5.1.3.1.1.
The setting of the Virtual Carrier Sense (VCS) is defined in Section 5.1.3.1.2.
In Coordinated or Uncoordinated mode, a STA must start and complete any CSMA/CA transmission entirely within a CSMA/CA allocation, and must not transmit during the Beacon Region (as determined by the Beacon Period Start Time). In CSMA-Only mode, a STA is only required to refrain from any transmissions during Stay-out Regions, as there is no Beacon Region and the Beacons are sent using CSMA/CA access.
Collisions
During CSMA allocations, collisions can result when multiple stations choose the same back-off value. AV stations infer a collision based on the reception status of responses transmitted by the receiver. There are three conditions under which an AV station expects a response,
When a SOF delimiter is transmitted with MPDUCnt set to 0b00, a valid SACK delimiter with DTEI set to the TEI of the transmitter is expected, except as noted in Section 5.4.8.3.

When a Long Sound MPDU is transmitted with MPDUCnt set to 0b00, a valid Sound ACK is expected. A valid Sound ACK shall have its STEI, DTEI, and LID fields equal to the STEI, DTEI, and LID fields of the transmitted Long Sound MPDU, respectively. Furthermore, the LID of the Sound ACK shall be the same as the LID of the corresponding Long Sound MPDU.
When an RTS delimiter is transmitted, a valid CTS delimiter is expected. A valid CTS shall have its STEI and DTEI fields equal to the DTEI and STEI fields of the transmitted RTS, respectively. The LID of the CTS should be the same as the LID of the corresponding RTS.
The following conditions shall cause an AV transmitter to infer a collision:
no valid delimiter, an invalid delimiter or a delimiter other than the expected response is received when a response expected, or
when a SOF delimiter is transmitted with MPDUCnt set to 0b00 and a valid response is received with the SACK Data fields indicating that all PHY Blocks were received with errors.
Setting of Virtual Carrier Sense (VCS) Timer
A VCS timer is maintained by all AV stations to improve reliability of channel access during CSMA. The setting of the VCS timer is shown in Table 51.

Table 51: Setting the VCS Timer

Event Type	New VCS Timer Value	Medium State when VCS Timer Expires
Collision	EIFS_X	Idle
Frame Control with bad FCCS is received	EIFS_X	Idle
Frame Control with at least one invalid field is received	EIFS_X	Idle
Reserved Frame Control is received	EIFS_X	Idle
Start of Frame delimiter with MPDUCnt set to 0b00 is received	(FL_AV*1.28 s) + DelimiterTime + CIFS_AV	PRS0
Sound delimiter with MPDUCnt set to 0b00 is received	(FL_AV*1.28 s) + DelimiterTime + CIFS_AV	PRS0
Start of Frame delimiter with MPDUCnt set to 0b01, 0b10 or 0b11 is received	(FL_AV*1.28 s)	Search for next MPDU in the Burst
Sound delimiter with MPDUCnt set to 0b01, 0b10 or 0b11 is received	(FL_AV*1.28 s)	Search for next MPDU in the Burst
SACK delimiter is received	CIFS_AV	PRS0
RTS delimiter is received	RCG + DelimiterTime + CMG + DelimiterTime	Idle
CTS delimiter is received	(DUR*1.28 s) + CIFS_AV	PRS0

The value of EIFS_X depends on whether the transmissions in the corresponding CSMA interval are in hybrid mode or AV-only mode.

When operating in AV-Only mode, EIFS_X shall be equal to EIFS_AV.

When operating in Hybrid mode, EIFS_X shall be equal to EIFS.

RTS/CTS

The Request to Send (RTS) and Clear to Send (CTS) delimiters can be used by AV stations during CSMA allocations to handle hidden nodes. RTS/CTS exchange is also used to enable reliable exchange of data and management messages across stations that are tracking different networks. Refer to Section 5.4.3.1 and Section 4.4.1.5.2.19 for details.

Channel Access Priority

Section 13.1 provides the recommended mapping from the eight different user_priority values indicated in the VLAN Tag to the four channel access priorities supported by HomePlug AV and HomePlug GREEN PHY. Traffic belonging to both Local Links and Global Links can be transmitted in CSMA allocations. When Global Link traffic is transmitted in CSMA allocations, the channel access priority should also be based on the User Priority in the CINFO of the Link (refer to Section 7.8.1).

CSMA/CA Channel Access for GREEN PHY

A GREEN PHY Station uses CSMA/CA channel access mechanism to contend during Green PHY Preferred (GPP) allocations and CSMA allocations. The CSMA/CA channel access mechanism used by GREEN PHY Stations is identical to that of HomePlug AV (refer to section 5.1.3.1 and subsections 5.1.3.1.1 through 5.1.3.1.4).

The channel access priority of Green PHY transmissions during CSMA allocation shall be selected based on the Distributed Bandwidth Control protocol described in Section 5.8.

When a Green PHY station is provided with a GPP allocation by a future version of a HomePlug AV CCo, the Green PHY station shall prefer the GPP allocation when sending its traffic. Preferred use of GPP allocation by Green PHY stations enables efficient prioritization of HomePlug AV traffic (i.e., limits the duration of time for which HomePlug AV traffic is sent using PRS signaling at CAP0).

TDMA Channel Access

HomePlug AV stations use Beacon-based TDMA (or Contention Free Access) in both Uncoordinated mode and Coordinated mode for traffic requiring guaranteed QoS. TDMA allocations can be provided either on a per-Beacon Period basis (i.e., once per Beacon Period) or multiple times within each Beacon Period. Contention Free sessions shall go through the admission-control procedure before periodic access to the medium is granted. The admission-control procedure is controlled by the CCo.

A session with a regular CFP allocation can always start its transmission at its start time, as defined by the schedule, and must end its transmission by its end time, as defined by the schedule. If a session does not receive the Beacon, but the session has the current effective schedule information (due to schedule persistence), it may start its transmission during its allocated time.

Admission Control and Scheduling

The admission-control procedure in HomePlug AV deals with long-term allocation of network resources. All Contention-Free Sessions go through the admission-control procedure during

session establishment. Scheduling procedure deals with the short-term (on a Beacon-period basis) allocation of network resources.
Stations may find that they require more time to transmit their data than they have been allocated in a Beacon Period. This may be due to a change in the source rate or changes in channel characteristics. To ensure that stations obtain the required allocation promptly, special fields in the Frame Control are used to convey allocation requirements to the CCo. The CCo may respond with changes to the persistent part of the schedule. The persistent part of the schedule is not very responsive and cannot change rapidly, since it is based on the maximum Schedule Countdown value used in the network. The CCo can also use the Non-persistent Allocation (refer to Section 5.1.1.2.1) fields in the Beacon to provide immediate allocation.
Note: Non-persistent Allocations can be changed for every period and hence provide reasonably reliable and very efficient access with small delay to sessions with acute needs.

Control Plane
Connections and Links
A Connection is a data flow (a set of related MSDUs) between the HLE of the STA that establishes the Connection and the HLE(s) of one or more destination STAs. A Connection can be either unidirectional or bidirectional. The concept of Connections is for the convenience of the HLEs; within the CL and MAC, the Connection is decomposed into one or more unidirectional data flows called Links.
A Link is a unidirectional data flow (a packet or set of related packets) from the CL of the source of the Link to the CL of one or more destinations of the Link.
Links can be categorized as unicast or broadcast/multicast, depending on the number of destinations of Link. Unicast Links have a unique destination, whereas broadcast/multicast Links have multiple destinations.
A unicast Link may be either a Forward Link or a Reverse Link. The Forward Link is identified as originating at the STA that initiates the Connection establishment procedure and terminating on the STA(s) responding to the connection establishment request. The Reverse Link is in the opposite direction to the Forward Link.
A Connection can be composed of one of the following combinations of Links:

- A single unicast Link from the station that initiated the Connection to the terminating station of the Connection (i.e., a single Forward Link).
- A single unicast Link from the terminating station of a Connection to the initiating station of the Connection (i.e., a single Reverse Link).
- Both (1) and (2) (i.e., a bi-directional Connection composed of both a Forward Link and a Reverse Link).
- A single multicast/broadcast Link from the station that initiated the Connection to the terminating stations of the Connection.

The distinction between Connections and Links is made because, at the physical layer, each direction between two stations is likely to have different characteristics and must be allocated separately. By comparison, it is much easier for the HLE to request a bi-directional Connection and have the CM CM -> CM (Connection Manager, refer to Sections 2.1.2 and 7.8.1) and CCo

either set up both directions of the Connection (if the Connection can be accommodated) or neither. The CM will never set up only one Link of a bi-directional Connection.
HomePlug AV supports two types of Links:
Global Links
Local Links
These Link types are closely tied to the access methods used in HomePlug AV. In each STA, the HLE or CM chooses the Link type it wants to use to transport its data and indicates it to the peer STA as part of the CINFO (Connection Information - refer to Section 7.8.1).
Every Connection has a CSPEC (Connection Specification) associated with it (refer to Section 7.8.1). This CSPEC contains information about the QoS the Connection requires.
A bi-directional Connection has a bi-directional CSPEC that contains information about both the forward and reverse direction QoS requirements; one half either the forward or reverse portion of the CSPEC applies to each of the Links associated with the Connection.
A unidirectional Connection will specify only forward or reverse direction QoS requirements, depending on the direction in which the Connection's data traffic flows.
A Connection is created when the HLE in a given station initiates a messaging sequence to set up the Connection. Based on the CSPEC provided by the HLE, the CM in this station determines how many Links are required and whether each Link should be a Global Link or Local Link. The CM then communicates with the CM in the destination station, and possibly with the CCo, to establish the one or more Links required to realize the Connection.
Once the Connection is established, the STA is responsible for monitoring the QoS performance of each of its Links. If a Link is not performing according to its CSPEC, the CM may initiate a Link reconfiguration with a new CSPEC or it may tear down the Connection.
It is possible to have several Connections between two STAs. Each of these Connections will have either Global or Local Links along with its own, possibly unique, CSPEC.
Global Links
Global Links are established and controlled by the CCo at the request of a CM. The CCo assigns the Global Link a TDMA allocation and a GLID. Until the CCo assigns the GLID, the Global Link will be identified by the STEI and LLID assigned by the station that is the source of the Link. Thus, a Global Forward Link is identified by the STEI of the STA initiating the connection and the LLID-F. Similarly, a Global Reverse Link is identified by the STEI of the STA that is at the terminating end of the connection and the LLID-R.
A Global Link is managed globally by the CCo and locally by the CMs on each of the STAs involved in the Connection.
Local Links
A Local Link uses the CP. The CCo is not involved in establishing or controlling Local Links. It is the responsibility of the CM on the transmitting side of the Link to assign a LLID to identify the Link.
Connectionless "Links"
Connectionless data is transported in the CP using CSMA.
Each connectionless data packet is assigned a Priority Link ID (PLID) from a set of LID values (PLID = 0, 1, 2, 3) that are reserved for connectionless traffic. These PLIDs identify the priority of

the packet being transported but do not uniquely identify a particular data flow.
Connectionless “Links” for GREEN PHY
A station implementing only GREEN PHY is only required to support priority “connectionless” links.
Link and Connection Identifiers
This section discusses the various identifiers used for Links and Connections. A summary of this information can be found in Table 52.
Link Identifiers
The Link Identifiers (LIDs) are used to identify various Links within an AVLN. There are three types of Link identifiers: PLID, LLID, and GLID.
Priority Link ID: The PLID is used for connectionless traffic. It has a range of 0x00 to 0x03. The PLID indicates the traffic class for priority resolution during CSMA. The CL maps the eight 802.1 user priorities onto the four HomePlug AV traffic classes (PLIDs), as described in Section 13.1.
Local Link ID: The LLID is used for connection-oriented traffic carried within the contention period. It has a range of 0x04 to 0x7F.
Global Link ID: The GLID is assigned by the CCo and is unique in a network. It is used to identify different types of allocation. For contention-free allocation, it further identifies the unique Link that can use the medium.
0xFF = identifies a Local CSMA allocation.
0xFE = identifies a Shared CSMA allocation, which can be used only when the network is operating in Coordinated Mode.
0xFD = identifies an allocation used by a designated STA to transmit a Discover Beacon.
0xFC = identifies an allocation for Contention Free Period Initiation (CFPI).
0xF8 - 0xFB = reserved.
0x80 - 0xF7 = identifies a unique contention-free Link in the network.
Note: The type of the LID can always be distinguished by its value.
Using Link Identifiers to uniquely identify a MAC Frame Stream is described in Section 5.4.1.2.
Each Connection may have two Links associated with it:
Forward Link
Reverse Link
Thus, each Connection may have two LIDs:
Forward LID (LID-F)
Reverse LID (LID-R)
A primary function of the LID is to identify the MAC Frame Stream associated with the PB contained in a received MPDU. It is carried in the FC of each MPDU that transports PBs (i.e., SOF).
Assignment of LIDs
All LIDs are assigned at connection setup. The originating STA assigns a unique LLID immediately. This LLID will be used as part of the CID (refer to Section 5.2.1.4.2) and, if the forward LID will be local, this is the same value used for LID-F. The terminating STA assigns the LLID-R field if there is either a Local or a Global Reverse Link. Each STA shall select an LLID value that is unique within its transmitter. This allows the PBs in the MPDU to be routed to the

Local Link ID (LLID)	8b	0b0XXXXXXX		Values of 0x00 to 0x03 are not permitted for Control.

correct MAC stream solely on the basis of the LLID and disambiguated STEI in the Frame Control.
The CCo assigns the GLIDs used on Links in the CFP. Upon receipt of the CM_LINK_NEW.REQ, the CCo assigns GLIDs to one or both Links associated with the Connection. The CCo assigns these GLIDs to be unique within its network (i.e., the GLIDs alone identify the Connection without reference to the STEI). This allows the PBs in the MPDU to be routed to the correct MAC stream solely on the basis of the GLID in the Frame Control.

Connection Identifiers

When a Connection is first requested by an HLE, the CM assigns a Connection Identifier (CID) to the Connection. This Connection Identifier shall be unique for each Connection. It is assigned in a manner to ensure that it is globally unique with the network. The CID is used in communications between the STA and CCo, as well as between the STAs. It can also be used in primitives between the HLE and the CM.

The CID is a 16-bit value constructed by placing the TEI of the originating STA in the upper 8 bits and placing the LLID-F initially generated for the Connection by the originating STA in the lower 8 bits. The STA always generates an LLID-F for a Connection to construct the CID, even if the Connection does not have a Forward Link or if the Forward Link is to be a GLID-F. The CID does not change when and if the CCo assigns a GLID-F to the Connection.

When the CL receives an inbound data packet at the H1 interface, the Classifier (refer to Section 6.2) shall attempt to associate the data packet with a Connection. If it is successful, it will output the CID and LID of the Link that originates in that STA.

When the CL receives an outbound data packet at the M1 interface, it may use either the CID or the LID and STEI of the MSDU to identify the Connection. This will allow it to successfully route the data packet to the appropriate HLE at the H1 interface.

Table 52: Summary of Link and Connection Identifiers

Name	Length (Bits)	Format	Assigned by	Description / Notes
Connection ID (CID)	16b	8b OrigTEI + 8b LLID-F	Originating STA	Used by the CCo and the STAs to identify a Connection. May also be used in primitives between HLE and CM.
Link ID (LID)	8b			Used by the MAC to identify the MAC Frame Stream.

Local Link ID (LLID)		0b0XXXXXXX		Values of 0x00 to 0x03 are not permitted for LLIDs.
Forward (LLID-F)			Originating STA	Unique within the originating STA
Reverse (LLID-R)			Terminating STA	Unique within the terminating STA
Global Link ID (GLID)	8b	0b1XXXXXXX		Unique within the network
Local CSMA allocation		0xFF	Fixed in Spec	Used by CCo to identify local CSMA allocation.
Shared CSMA allocation		0xFE	Fixed in Spec	Used by CCo to identify shared CSMA allocation.
Discover Beacon Allocation		0xFD	Fixed in Spec	Used by CCo to identify Discover Beacon allocation.
CFPI Allocation		0xFC	Fixed in Spec	Used by CCo to identity Contention Free Period Initiation Allocation (refer to Section 9.6.1).
Reserved for future use		0xF8 - 0xFB	Fixed in Spec	Reserved for future use.
Forward (GLID-F)		0x80 - 0xF7	CCo	Contention-free allocation used by a designated STA.
Reverse (GLID-R)		0x80 - 0xF7	CCo	Contention-free allocation used by a designated STA.

Priority Link ID (PLID)	8b	0x00 - 0x03	Fixed in Spec	Used for connectionless traffic.

Link Identifiers for GREEN PHY

Link Identifiers for HomePlug GREEN PHY shall be identical to that of HomePlug AV (see section 5.2.1.4.1) with the following exceptions and additions:

0xFB = identifies GREEN PHY Preferred (GPP) allocations for GP Stations (i.e., uses a previously reserved value). Refer to section 7.8.5.

0xF8 - 0xFA = reserved.

Connection Identifiers for GREEN PHY

Connection Identifiers for HomePlug GREEN PHY shall be identical to that of HomePlug AV (see section 5.2.1.4.2) with the following exceptions and additions:

Table 52b: Assignment of Previously Reserved Values for Link and Connection Identifiers in GREEN PHY

GPP Allocation		0xFB	Fixed in Spec	Used by CCo to identity Allocations in which GREEN PHY stations may transmit after Association and Authentication
Reserved for future use		0xF8 - 0xFA	Fixed in Spec	Reserved for future use.
GPP Allocation		0xFB	Fixed in Spec	Used by CCo to identity Allocations in which GREEN PHY stations may transmit after Association and Authentication

Transport Services

HomePlug AV offers two transport services to the HLEs:

Connectionless Service (CLS)

Connection-Oriented Service (COS)

Connectionless Service (CLS)

Connectionless Service (CLS) transports individual data packets between HLEs on different stations.
CLS is used by an HLE prior to the time it sets up a Connection and selectively thereafter. It is also used by legacy applications that are unaware of the availability of Connection services.
All data traffic is connectionless unless:
The HLE establishes a Connection for the data traffic.
The Auto-Connect Service establishes a Connection based on the characteristics of the data traffic.
Connectionless traffic always uses the CP. It does not offer guaranteed QoS, but does support prioritization of packets as they flow through the system.
Connection-Oriented Service (COS)
Connection-Oriented Service (COS) allows two or more HLEs to set up a logical Connection between themselves.
A Connection can be either unidirectional (data flows in only one direction) or bidirectional (data flows in both directions).
Connection-oriented traffic can use either the CFP or the CP, depending on the QoS requirements of the Connection. CFP Connections are used to provide guaranteed QoS.
Connection Services
At a minimum, a STA must accept a single forward link as a receiver or initiate a single forward link as a transmitter. A STA is not required to support more than one connection at a time. The ability to accept requests to modify and tear down an existing Connection is also mandatory. The ability to set up a bi-directional CFP Connection is optional.
A STA shall have the ability to initiate and/or accept both local (CP) and global (CFP) forward links. A STA that has the ability to transmit payload received from the HLE shall be able to initiate both local (CP) and global (CFP) forward links. A STA that has the ability to receive payload for the HLE shall be able to accept both local (CP) and global (CFP) forward links.
Connection Setup
When an HLE requests the CM to set up a Connection:

- The HLE tells the CM the CSPEC for the new Connection, the destination STA's MAC address (either unicast or broadcast/multicast), and the Classifier rules that will match the messages sent by the HLE.
- The CM on the STA that initiated the Connection sends a CM_CONN_NEW.REQ message to the CM(s) on the terminating STA(s).
- The CM at the terminating STA informs the HLE of the new Connection using the APCM_CONN_ADD.IND primitive. The HLE responds with APCM_CONN_ADD.RSP primitive, indicating whether the connection can be added. The use of APCM_CONN_ADD.IND/RSP primitive during connection setup is optional.
- The CM at the terminating STA sends a CM_CONN_NEW.CNF message to the CM of the initiating station indicating whether the connection request is accepted or rejected.
- If negotiation between CMs is successful and no Global Links are required, the connection setup is complete and the HLE is notified.
- If negotiating between CMs is unsuccessful, the connection setup is deemed as failed. In the case of broadcast/multicast Link, it is possible that some of the destination CMs may

have accepted the Connection while other have rejected. In this case, the initiating CM shall send a CM_CONN_REL.IND message indicating the failure of the connection setup to all CMs that accepted the Connection. Reception of a CM_CONN_REL.IND shall cause the CMs on the terminating side of the Connection to release the connection and respond with a CM_CONN_REL.RSP message.

- If the negotiation between CMs is successful, the STAs may immediately start exchanging MPDUs belonging to that Connection. In case of Global Links, the Connection Identifier (CID) will be used to identify the MPDUs belonging to the Link until CCo provides a Global Link identifier.
- If the negotiation between CMs is successful and if Global Links are required, the initiating CM sends a CC_LINK_NEW.REQ to the CCo. CCo sends the CC_LINK_NEW.CNF message to all stations belonging to the Connection to indicate the success or failure of the Connection setup procedure.

The Auto Connect may request the CM to set up a Connection (refer to Section 6.6). The CMs are also responsible for configuring the Classifiers to identify packets belonging to Links (refer to Section 6.2).

A Global Link can be uniquely identified at each STA by either the:

Global Link Identifier that is assigned by the CCo, or

By the LLID together with the STEI in a SOF MPDU.

The use of LLID and STEI for identifying global links is primarily intended to minimize the latencies involved in delivering template based Auto connect traffic (refer to Section 6.6). In such cases, the LLID and STEI may be used (in the MPDU Frame Control) to identify the MAC Frame stream once the negotiation between CMs is successful and until the CCo assigns a Global Link identifier. Once the Global link Identifiers are assigned, stations shall use the GLID (in the MPDU Frame Control) to identify the MAC Frame Stream.

Receiving STAs shall be capable of receiving Global Link-based traffic, regardless of whether the transmitter uses a LLID/STEI or a GLID to identify the Link in the SOF MPDU Frame Control.

When a Connection Setup request was rejected by the CM due to insufficient station resources or rejected by the CCo due to insufficient bandwidth, a proposed CSPEC containing the fields of the CSPEC that can currently be supported should be communicated to the stations belonging to the Connection. This enables the Application or the CM to set up a new Connection for the streams, within the limits of the proposed CSPEC. The following rules shall be used in generating the Proposed CSPEC:

The Proposed CSPEC shall include all the QoS and MAC parameters (QMPs) from the requested CSPEC that the STA is currently capable of supporting.

If the value of a QMP in the requested CSPEC cannot be currently supported, but a different value of the QMP can be supported, the Proposed CSPEC shall include the QMP with a value that the STA is currently capable of supporting. For example, if the Receive Window Size of 256 Segments is requested and the STA is only capable of supporting Receive Window Size of 64 Segments, the Proposed CSPEC will have the Receive Window Size QMP set to 64.

If a specific QMP in the requested CSPEC cannot be supported at all, the Proposed CSPEC shall not include that QMP. For example, if the Bidirectional Bursting QMP is present in a CSPEC and

the STA is not capable of supporting Bidirectional Bursting, the Proposed CSPEC will not include this QMP. Similarly, if the requested CSPEC includes Vendor Specific QMP and the STA belongs to a different Vendor or cannot interpret the QMP, the Proposed CSPEC will not include the Vendor Specific QMP.
If a specific parameter in the CINFO of the requested CSPEC cannot be supported, but a different value of that parameter can be supported, the Proposed CSPEC shall have the parameter set to the value that the STA is currently capable of supporting.

Figure 57: Connection Setup
Connection Setup for GREEN PHY
A station implementing only GREEN PHY is only required to support priority "connectionless" links. As a result, Connection Setup procedure is not required. A HomePlug GREEN PHY station does not initiate the Connection Setup procedure. When a HomePlug GREEN PHY Station receives a Connection Setup request from another HomePlug Station, it shall respond with a CM_MME_ERROR.IND with 'ReasonCode' set to 0x00 (indicating that MME not supported).
Global Link Setup
For Connections that require Global Links, the CM of the STA that initiated the Connection will interact with the CCo to establish the Global Links as shown in Figure 58.

Figure 58: Global Link Setup
Global Link Setup for GREEN PHY
A station implementing only GREEN PHY is only required to support priority "connectionless" links. As a result, Global Link Setup procedure is not required. A HomePlug GREEN PHY station does not initiate the Global Link Setup procedure. When a HomePlug GREEN PHY Station receives a Global Link Setup request from another HomePlug Station, it shall respond with a CM_MME_ERROR.IND with 'ReasonCode' set to 0x00 (indicating that MME not supported).
Latency Effects on Global Link Setup
Since the Global Link Setup (**CC_LINK_NEW.CNF**) message may be transmitted in the CP, it is subject to variable latencies in delivery to the stations that are part of the connection. Therefore, these stations might not be synchronized with respect to the state of the Connection (i.e., accepted and active or failed) during the Global Link Setup process.
The station that is the source of a Global Link shall not start transmission of Segments belonging to that Link until the CCo has started providing CFP allocations for the GLID.
Due to processing latencies, it is possible that the transmitter may have already initiated transmission of segments before the receiver has processed CC_LINK_NEW.CNF. In such cases, when the receiver receives Segments belonging to a new GLID, it shall discard all the Segments and send a SACK with MFSRspData set to HOLD.
Connection Monitoring
Each CM will gather statistics for each Link. The CM will monitor the QoS being delivered to each Link and will reconfigure or tear down any Link that fails to meet its CSPEC, depending on the action specified by the CSPEC's Violation Policy parameter. If a Link is torn down, the corresponding Connection will also be torn down.

An HLE may request the performance statistics for its Connections from the CM at any time.

CM Behavior under Inactivity Interval

CSPEC may include an inactivity interval that indicates the maximum duration of time for which the Connection may remain active without receiving application data.

The source station of the Link (Local Link or Global Link) shall monitor the duration of all inactivity intervals and shall terminate the Connection if the inactivity interval exceeded the negotiated inactivity interval. The destination station of the Link may also monitor the inactivity intervals and may initiate the termination of the Link if inactivity interval is violated.

The source station of a Global Link shall continue to transmit SOF delimiter with MFSCmdData set to NOP (No Operation) during the inactivity periods. CCo shall continue to provide sufficient allocation for the transmission of SOF/SACK delimiters during each Beacon Period even when no Pending PHY Blocks are reported in the Frame Control.

Connection Teardown

The CM of either STA will tear down a Connection at the request of the HLE (APCM_CONN_REL.REQ primitive) or, if exception policy dictates, because the Connection's performance (i.e., the performance of one of its Links) is not meeting its CSPEC.

When either station decides to tear down the Connection, the teardown process depends on whether the Connection includes a Global Link.

For a Connection that contains only Local Links, the station initiating the teardown notifies the other station using the CM_CONN_REL.IND message. Reception of a CM_CONN_REL.IND shall cause the CM to release the connection and respond with a CM_CONN_REL.RSP (see Figure 59).

For a Connection that contains Global Links, the station initiating the teardown notifies the CCo by send the CC_LINK_REL.REQ message. Upon reception of this message, the CCo indicates the release of this Connection to all stations that are part of this Connection by sending CC_LINK_REL.IND message (see Figure 510).

The CCo may also initiate the teardown of a Connection due to bandwidth limitations. In such cases, the CCo sends the CC_LINK_REL.IND message to notify the teardown of the Connection to all stations that are part of the Connection.

The CCo may also initiate the teardown of a Connection at the request of a station within the AVLN that is not part of the Connection (i.e., neither the initiating station nor the terminating station(s)). This capability is required to provide flexibility for higher layer protocols like UPnP in managing the AVLN. When the CCo tears down a Connection at the request of a station within the AVLN that is not part of the Connection, it sends the CC_LINK_REL.IND message to notify the teardown of the Connection to stations that are part of the Connection as well as to the station that initiated the Connection teardown.

When the CM or CCo initiates a connection teardown due to violation of the CSPEC, the CSPEC fields that are violated and their values at the time when teardown is initiated may be communicated to other stations as part of the Violated CSPEC in CM_CONN_REL.IND, CC_LINK_REL.IND, and CC_LINK_REL.REQ. For example, if the CM tears down a Connection due to violation of the Average Data Rate, the Average Data Rate observed for the Link at the time at which connection teardown was initiated should be communicated.

When the CCo initiates a connection teardown due to insufficient bandwidth, it may communicate a proposed CSPEC containing the values of the CSPEC fields that can be supported to all stations belonging to that Connection as part of the Proposed CSPEC in CC_LINK_REL.IND. Proposed CSPECs enable applications capable of supporting the stream at multiple data rates to setup a new Connection within the limits of the Proposed CSPEC. Proposed CSPEC with Average Number of PBs per Transmit Operation set to zero should be communicated when no new stream can be admitted into the network.

Figure 59: Connection Teardown for Connections with Only Local Links

Figure 510: Connection Teardown for Connections with Global Links

Latency Effect on Teardown Messages

Since the connection-teardown messages are transmitted in the CP, they are subject to variable latencies in delivery to the stations that are part of the connection. Therefore, these stations and the CCo might not be synchronized with respect to the state of the Connection (i.e., active or teardown) during the teardown process.

A station shall use the following behavior after the teardown of a Connection as follows:

If the station is the source of a Link, it shall discard all packets received from the HLE that belong to that Link. The station may optionally send an SOF delimiter with MFSCmd set to RELEASE to indicate that Connection is released.

If the station is the destination of a Link, and if the MPDU containing segments belonging to that Link are received, it shall discard all the segments and shall send a SACK with MFSRspData set to FAIL.

Reception of a SACK delimiter with MFSRspData set to FAIL is an indication to the transmitter that the receiver has already terminated the Connection. The transmitter may locally terminate the Connection (i.e., without sending the teardown messages to other stations or CCo). The station may wait for connection-teardown messages (for determining the cause of the Connection teardown, etc.) before notifying the HLE.

For Connections with one or more Global Links, the absence of CFP allocations in Beacon Periods can be used as an indication of Connection termination. It is recommended that the stations terminate the Connection locally if CCo did not provide allocation for 10 consecutive Beacon Periods. Stations may wait for connection-teardown messages (for determining the cause of the Connection teardown, etc.) before notifying the HLE.

Hostile Connection Teardown

Under some conditions one or more stations that are part of a Connection may get disconnected without properly terminating the Connection. To ensure that network operations does not get adversely effected by such events, the following behavior is recommended for the STAs and CCo, The source of a Link may initiate a Connection teardown if it failed to receive a response (i.e., a valid SACK, CTS, or Sound Response) to its transmissions for at least 10 consecutive transmission attempts. The source of the Local Link may use all its transmissions to the destination (i.e., MPDUs carrying Segments intended for the destination but part of other Links) for making such decisions.

Global Links for which the source of the Link can be heard by the CCo (i.e., the Global Link is not managed in coordination with a Proxy Coordinator), the CCo may initiate a Connection teardown if no transmission from the source or destination of the Link are heard in the last 10 Beacon Periods.

Connection Teardown for GREEN PHY

A station implementing only GREEN PHY is only required to support priority "connectionless" links. As a result, Connection Teardown procedure is not required. A HomePlug GREEN PHY station does not initiate the Connection Teardown procedure. When a HomePlug GREEN PHY Station receives a Connection Teardown request from another HomePlug Station, it shall respond with a CM_MME_ERROR.IND with 'ReasonCode' set to 0x00 (indicating that MME not supported)

Connections and Network Modes

The MAC Service Type field in the CINFO is used by HLE to indicate whether the traffic belonging to the Links has to be transmitted using contention-based service, contention-free service, or contention-free preferred service.

Connections with all Links requiring only contention-based service will always us CSMA/CA channel access. Since CSMA/CA channel access is supported in all network modes (refer to Chapter 8) of the AVLN, such connections shall continue to operate even when the network mode changes.

Connections with one or both Link(s) requiring contention-free service can only be supported in Uncoordinated mode or Coordinated mode. Such connection setup requests shall be rejected if the network is operating in CSMA-Only mode. Further, such connections shall be released when the network mode changes from either Uncoordinated or Coordinated mode to CSMA-Only mode. Release of such connections when the network mode changes to CSMA-Only is implicit (i.e., the CCo shall not send CC_LINK_REL.IND message). CMs shall use the knowledge of network mode change to terminate the connection.

Connection with one or both Link(s) requiring "contention-free preferred" service and the remaining Link (if any) requiring Contention-based Service shall be supported in all network modes. Links requiring "contention-free preferred" service shall be handled as follows,

If the AVLN is operating in Uncoordinated or Coordinated mode, and if the Global Links can be successfully established, streams with "contention-free preferred" service should use Global Links.

If the AVLN is operating in Uncoordinated or Coordinated mode, and if the Global Links cannot be established or if the CCo terminates the established Global Links (by sending CC_LINK_REL.IND), the STAs shall either continue to send traffic belonging to the connection using Local Link Identifiers or terminate the connection.

If an AVLN operating in either Uncoordinated or Coordinated mode changes to CSMA-Only mode, any Global Links belonging to "contention-free preferred" service will be implicitly terminated (i.e., the CCo need not send CC_LINK_REL.IND). STAs shall use the knowledge of network mode change to discard Global Links, and shall either continue to send traffic belonging to the connection using Local Link Identifiers or terminate the connection.

If an AVLN operating in CSMA-Only mode changes to either Uncoordinated or Coordinated mode, the CM at the originating side of the Connection may either request the CCo to set up Global Links or continue to use the Local Links. If the Global Links are set up successfully, traffic

belonging to the “contention-free preferred” service shall be transmitted using Global Links. Otherwise, the STAs shall either continue to send traffic belonging to the connection using Local Link Identifiers or terminate the connection.

Connections using “contention-free preferred” service are only released when the CM at either the origination side or the terminating side of the Connection sends a CM_CONN_REL.IND or when the connection times-out (in case of a hostile connection teardown).

Connection Reconfiguration

Connection reconfiguration occurs when the CSPEC parameters of the Connection change. Connection reconfiguration occurs for several reasons, including:

The HLE initiates a change in CSPEC for reasons specific to the application,

The Auto-Connect or CM initiates a change in CSPEC when they determines that the CSPEC parameters have changed,

Figure 511 shows a Connection reconfiguration. The Connection reconfiguration process is similar to the new Connection setup process. Failure to reconfigure a Connection shall not cause the existing Connection to be dropped.

Acceptance of a connection-reconfiguration request (CM_CONN_MOD.REQ) for Connection involving Global Links shall cause the CM to update the local resource allocations to support the modified Connections. This local resource reconfiguration before getting the CC_LINK_MOD.CNF, will enable the CMs to deal with latency effects in delivering the CC_LINK_MOD.CNF to CMs involved in the Connection (i.e., one of the CMs can get the CC_LINK_MOD.CNF earlier than other, if the modification is accepted, can start transmitting stream based on the new CSPEC). Rejection of the connection modification by CCo shall cause the CMs to restore the local resource allocations.

When a Connection reconfiguration request was rejected by the CM due to insufficient Station resources or by the CCo due to insufficient bandwidth, a proposed CSPEC containing the fields of the CSPEC that can currently be supported may be communicated to the stations belonging to the Connection. This enables the Application or the CM setup a new Connection for the streams within the limits of the proposed CSPEC.

Figure 511: Connection Reconfiguration

HLE- or Auto Connect-Initiated Reconfiguration

When the HLE or Auto Connect determines that the Connection needs to be reconfigured, it negotiates with the other station for the reconfiguration (which involves changes to the CSPEC parameters) and then requests the CM to modify the Connection. The CM requests the CCo for a reconfigured allocation (if the affected Link is using the CFP).

Certain CSPEC parameters shall not be changed during Connection Reconfiguration (refer to Section 7.8.1). Classifier Rule Set(s) used to identify packet belonging to the Connection cannot be changed during Connection Reconfiguration.

CM-Initiated Reconfiguration

The CM initiates reconfiguration when the Exception Policy in the CSPEC requires Connection Reconfiguration under CSPEC violation. If the CM in either station determines that the allocation

needs to be reconfigured due to changes to CSPEC (for example, due to changes in traffic characteristics), it negotiates directly with the CCo. Then the CCo notifies both stations about the revised allocation.
The CM that is initiating the reconfiguration indicates the initiation of the reconfiguration procedure to the HLE using the APCM_CONN_MOD.IND. In this case, the corresponding APCM_CONN_MOD.RSP is not present.
Note: Allocation modifications required to support the current CSPEC (due to changes in channel characteristics) are performed without explicit messaging via Frame Control and the Beacon (refer to Section 5.2.3.7.3).
Connection Reconfiguration for GREEN PHY
A station implementing only GREEN PHY is only required to support priority "connectionless" links. As a result, Connection Reconfiguration procedure is not required. A HomePlug GREEN PHY station does not initiate the Connection Reconfiguration procedure. When a HomePlug GREEN PHY Station receives a Connection Reconfiguration request from another HomePlug Station, it shall respond with a CM_MME_ERROR.IND with 'ReasonCode' set to 0x00 (indicating that MME not supported)
Global Link Reconfiguration Triggered by CCo
The CCo can trigger reconfiguration of the Global Link because of:
Consolidation of TDMA assignments
Changes to channel characteristics
Squeeze/De-Squeeze
Global Link reconfiguration required to support the current CSPEC (which includes consolidation of TDMA assignments and adapting to changes in channel characteristics) is performed without explicit messaging via Frame Control and the Beacon. The CM at the source of a Global Link provides continuous estimates of the channel characteristics to the CCo by providing Bit Load Estimates in the Frame Control. The CM may also send a CC_BLE_UPDATE.IND message to the CCo when it notices significant changes to the Bit Loading Estimates. These estimates, along with the PPB information (also provided in the Frame Control), are processed by the CCo. This results in CCo-initiated changes to Global Link allocations to support the negotiated CSPEC. The CCo notifies the two STAs about the new allocation by updating the schedule information in the Beacon.
Squeeze and De-squeeze
The CCo of an AVLN may also reconfigure existing Connections by requesting Connection(s) to reduce their bandwidth usage (i.e., request to Squeeze) when bandwidth is scarce or by allowing them to increase their bandwidth usage (i.e., request to De-Squeeze) when bandwidth becomes available.
The CCo may request a Connection to squeeze when there is insufficient bandwidth available to support all the ongoing Connections (due to degradation in channel characteristics) or to accommodate a new Connection. In Coordinated Mode, a CCo may request one or more ongoing Connections to squeeze to accommodate Connections in neighbor network(s).
The CCo may request a squeezed Connection to de-squeeze when more bandwidth becomes available. Additional bandwidth may become available if channel conditions improve or when

Connections are released. In Coordinated Mode, new bandwidth may become available as Connections in neighboring networks are released. The CM may also continuously monitor the available bandwidth and request connection reconfiguration (to de-squeeze) when it determines that more bandwidth is available. CM may also periodically attempt to reconfigure a Connection while operating at a squeezed rate.

The ability for a CCo to request a Connection to squeeze is optional. The ability of a CM to squeeze an existing connection is optional.

The following procedure shall be used by the CCo to squeeze or de-squeeze a Connection:

- When a CCo determines that a Connection needs to be squeezed or de-squeezed, it shall send a CC_LINK_SQZ.REQ request to one of the stations belonging to that Connection. The exception to this rule is for broadcast/multicast Connections, in which case the CC_LINK_SQZ.REQ shall be sent to the initiating station.
- Reception of the CC_LINK_SQZ.REQ causes the CM to indicate the connection-reconfiguration request to the HLE by using the APCM_CONN_MOD.IND.
- The HLE responds with APCM_CONN_MOD.RSP to indicate whether the connection reconfiguration is successful.
- If the HLE accepts the connection reconfiguration, the CM will negotiate with the peer CM for connection reconfiguration. The procedure for performing this step is the same as described in Section 5.2.3.6.
- If the peer CM accepted the connection reconfiguration (as indicated by CM_CONN_MOD.CNF), the CM will send a CC_LINK_SQZ.CNF indicating successful reconfiguration along with CC_LINK_MOD.REQ to the CCo.
- If the peer CM rejected the connection reconfiguration, the CM will send a CC_LINK_SQZ.CNF indicating that the reconfiguration has failed.

Connection Squeeze/De-Squeeze procedure when the reconfiguration was successful is shown in Figure 512.

Figure 512: Connection Squeeze/De-Squeeze

Squeeze and De-squeeze for GREEN PHY

A station implementing only GREEN PHY is only required to support priority “connectionless” links. As a result, Squeeze and De-squeeze procedure is not required. A HomePlug GREEN PHY station does not initiate the Squeeze and De-squeeze procedure. When a HomePlug GREEN PHY Station receives a Squeeze or De-squeeze request from another HomePlug Station, it shall respond with a CM_MME_ERROR.IND with ‘ReasonCode’ set to 0x00 (indicating that MME not supported).

Connection Services for Broadcast/Multicast

Broadcast (BCAST) and multicast (MCAST) applications involve data transfer from one source to multiple destinations. Examples include:

Applications such as Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) broadcast short packets. The HomePlug AVLN needs to provide broadcast

capability for these short packets. ARP packets are typically 28 octets long and occur at a frequency of once every 2-5 minutes from a STA in the HomePlug AVLN. DHCP packets are typically 300 to 400 octets long and are generally sent when a STA is starting up (boot time).
Audio and video applications, especially streaming AV applications over IP, may be broadcast to all stations in the HomePlug AVLN or a subset of stations in the network (called multicasting). Such applications are also bandwidth and QoS intensive. Since broadcast over AVLN can be unreliable (due to the lack of acknowledgements from all members of the multicast group), it is desirable to transmit multicast streams as multiple unicast streams.
Information to be broadcast/multicast may be transmitted using Local Links or Global Links. The procedure for adding, modifying and tear down of these Links is similar to that of point-to-point with the following differences:
Broadcast/multicast Links are always unidirectional with the initiating station being the source of the Forward Link and the broadcast/multicast destinations being the destinations of the Link (i.e., point-to-multipoint)
The CM_CONN_NEW.REQ and CM_CONN_MOD.REQ shall be sent to all CMs in the broadcast/multicast group. The connection setup or reconfiguration is considered to have failed if any one of the CMs rejects.
The CM_CONN_REL.IND message shall be sent to all CMs in the broadcast/multicast group. Reception of a CM_CONN_REL.IND shall cause the CMs to release the Connection and respond with a CM_CONN_REL.RSP message.
If a Global Link is needed for broadcast/multicast stream, the CCo shall send CC_LINK_NEW.CNF, CC_LINK_MOD.CNF, CC_LINK_REL.IND messages to ALL stations in the network (either using a broadcast transmission or through multiple unicast transmissions).
All segments belonging to a broadcast/multicast Link shall be transmitted in broadcast MPDUs. Note that broadcast MPDUs use Mini-ROBO, ROBO, or High Speed ROBO modulations. Broadcasting is very inefficient over the powerline and it is recommended that the use of broadcast within AV networks be minimized.
Broadcast/Multicast Connection using Multiple Unicast Connections
Reliability of the broadcast/multicast transmissions can be increased by sending MSDUs to each of the destinations independently by using unicast transmission. When the number broadcast/multicast destinations are small, this mechanism can also enable better utilization of network bandwidth.
To support broadcast/multicast stream using multiple unicast transmissions, the following functions needs to be supported:
The CM that initiates the Connection should be capable of converting the broadcast/multicast Connection add or modify request into multiple unicast request.
The CL should be capable of replicating each broadcast/multicast Ethernet frame and passing them to each of the associated unicast MAC Frame streams. Note that the Original Destination address of the Ethernet frame does not change even when it is inserted into a unicast MAC Frame stream.
The ability to support broadcast/multicast Connections into unicast Connections is optional.
Detect-and-Report Procedure
The detect-and-report procedure is a process that allows the CCo to determine whether a STA is within the reception range of any ongoing powerline transmissions. The CCo requests a STA to

detect for ongoing transmissions in some specified time intervals for a specified amount of time. The STA listens for and detects Frame Controls (refer to Section 4.4.1) in the specified time intervals as instructed and reports the results back to the CCo. The ability for a CCo to initiate the detect-and-report procedure is optional. The ability for a STA to detect and report on-going transmissions is optional.

Consequently, the CCo may be able to determine whether potential transmissions from the STA involved would cause interference to any ongoing transmissions.

The detect-and-report procedure consists of the following steps (see Figure 513):

- The CCo initiates the procedure by sending the CC_DETECT_REPORT.REQ message to a STA. The message contains a field that specifies the amount of time the STA shall listen and detect for ongoing transmissions. It also contains one or more GLID fields, which together with the schedules in the Beacon MPDU, specify the time interval(s) where the STA shall detect for ongoing transmissions.
- The STA shall detect for any ongoing transmissions in the specified time interval(s) for the specified amount of time. The STA shall then send the CC_DETECT_REPORT.CNF message to the CCo. The message contains the type of transmissions (e.g., no transmissions, contention-free transmissions, and/or contention-based transmissions) that it can detect in the time intervals specified by the GLIDs. Detecting and reporting the signal level is optional. Stations that do not have this capability shall set Signal Level to 0x0 (information not available) in the CC_DETECT_REPORT.CNF message. Detecting and reporting the average BLE is optional. Stations that do not have this capability shall set Average BLE to 0x0 (information not available) in the CC_DETECT_REPORT.CNF message.

Figure 513: Detect-and-Report Procedure

The detect-and-report procedure may be useful in bandwidth allocation or scheduling. Upon receiving a Global Link set-up request (CC_LINK_NEW.REQ) message from a STA, if the Topology Table of the CCo indicates that the STA(s) involved with the Global Link set-up request can detect stations in other networks that are not coordinating with the CCo, the CCo may instruct the STA(s) to perform the detect-and-report procedure over some specified time interval(s). If the STA(s) report back that Frame Controls of contention-free Links are not detected in that time interval, the CCo may allocate that time interval to the STAs and indicate to the STAs that RTS and CTS may be required. However, if the STA(s) report back that Frame Controls of contention-free Links are detected, it indicates that any potential transmissions from the STA(s) may interfere with the ongoing contention-free transmissions and, therefore, the CCo might not allocate that time interval to the STAs.

To ensure that a STA's CSMA transmissions do not interfere with CFP allocation of a non-coordinating CCo(s), it is recommended that STAs defer from transmitting during intervals in the CSMA allocation where CFP transmissions have been detected in previous Beacon Periods.

Channel Estimation

Channel estimation is the process of measuring the characteristics of the powerline channel to adapt the operation of the PHY to provide optimal performance.

Channel estimation comprises:
Selection of the modulation method(s) used on each carrier. Any given carrier may use different modulations at different times within the AC line cycle period.
Selection of the FEC rate.
Selection of the guard interval length.
Selection of the intervals within the AC line cycle where a particular Tone Map setting applies.
The FEC rate and guard interval length can vary over the AC line cycle period, but they are the same for all carriers at any given time.
Note: A Tone Map consists of a unique set of modulation methods for each carrier, the guard interval for the OFDM Symbol, and the FEC Rate. In short, channel estimation is the process by which Tone Maps are selected for different intervals within the Beacon Period.
The results of channel estimation are reported to the CCo for use in allocating time in the CFP.
Channel Estimation Procedure
The channel estimation procedure enables a transmitter to obtain Tone Maps that can be used at various intervals of the AC line cycle while communicating with a particular receiver. Power line channels are unique between each transmitter and receiver. Hence, the channel estimation procedure must be executed independently between each transmitter and receiver. Tone Maps are exchanged between stations by means of CM_CHAN_EST.IND and/or CM_TM_UPDATE.IND Management Messages. These messages are also referred to as Channel Estimate Indication (CEI) messages within the specification.
The channel estimation procedure can be divided into two phases depending on whether the transmitter has any valid Tone Maps:
Initial channel estimation
Dynamic channel adaptation
The transmitter invokes initial channel estimation when it needs to transmit data to a particular destination and does not have any valid Tone Maps. During initial channel estimation, the transmitter sends one or more Sound MPDUs to the receiver. The Sound Reason Code in these Sound MPDUs is used to indicate that the Sound MPDUs are transmitted as part of an initial channel estimation procedure. The receiver shall use these Sound MPDUs to estimate the channel characteristics and designate a Default Tone Map that may be used by the transmitting STA anywhere in the AC line cycle. In addition, the receiver may also provide one or more AC line cycle adapted Tone Maps during Initial channel estimation. This approach allows the STA to start communicating using Tone Map modulated data quickly, and avoids the complicated interactions between the channel access procedures and the channel estimation procedures. This approach is very similar to the approach used in the HomePlug 1.0.1 system and is well suited to the transport of best effort data.
Once the initial channel estimation is complete, the receiver continuously monitors the channel characteristics based on received MPDUs (either data or Sound) and provides dynamic updates to the Default Tone Map and/or to the Tone Maps that are valid at specific intervals of the AC line cycle. This process is referred to as dynamic channel adaptation. In contrast to initial channel estimation, the receiver is responsible for invoking dynamic channel adaptation. The transmitter provides passive support by behaving as indicated in the CEI messages and indicating error events

using Sound MPDUs.
The channel estimation procedures also include mechanisms for negotiating the number of Tone Maps that can be used, maintaining lists of valid Tone Maps, and maintaining the lists of the intervals within the AC line cycle where each Tone Map may be used. The procedures are described in the following subsections.

Initial Channel Estimation

The transmitter initiates the channel estimation procedure if it does not have any valid Tone Maps. Initial channel estimation may take place in either the CP or the CFP. If the initial channel estimation is performed in the CP, the transmitter must contend for the channel prior to sending Sound MPDUs to the receiving STA. Conducting the initial channel estimation in the CP may preclude the transmitter from transmitting Sound MPDUs during certain parts of the AC line cycle. Similarly, if the initial channel estimation is performed in the CFP, the transmitter may lack sufficient CF allocation to span a complete AC line cycle. In either case, the receiving STA is required to provide a Tone Map referred to as the Default Tone Map that is valid for all portions of the Beacon Period (or AC Line cycle). The receiver may also provide one or more AC line cycle adapted Tone Map during Initial channel estimation.

> During the initial channel estimation procedure, the transmitter uses the Max Tone Maps Requested (REQ_TM) field in the Sound Frame Control to indicate the maximum number of Tone Maps that it can support. REQ_TM shall be a value in the range 0 to MAX_TONE_MAPS. Once a REQ_TM value is advertised to the receiver, the transmitter shall not change the value until it has reinitiated a new initial channel estimation procedure. The receiver shall store the number of Tone Maps supported by the transmitter until all the Tone Maps for the transmitter have become invalid (i.e., have been explicitly invalidated by the receiver or have become stale). The receiver shall ensure that the number of Tone Maps it provides to the transmitter never exceeds this limit. ROBO Tone Maps shall not be included in this limit. The Default Tone Map shall be included in this limit if it is a non-ROBO Tone Map.

Initial Channel estimation comprises the following steps (see Figure 514):

- The transmitting station has data to send and determines that it has no valid Tone Maps for communication with the destination STA.
- The transmitting station initiates the channel estimation procedure by sending a Sound MPDU with Sound Reason Code set to indicate Sounding for Initial Channel Estimation. This MPDU specifies the maximum number of Tone Maps that the transmitting STA can allocate to this Link (REQ_TM, refer Section 4.4.1.5.5.8).
- The receiving STA responds with a Sound MPDU, with the SAF (Sound ACK Flag) bit in the FC set to 0b1 and no payload.
- The transmitting STA continues sending Sound MPDU (SAF = 0) until the receiving STA responds with SAF = 0b1 and SCF (Sound Complete Flag) = 0b1, indicating that it has received sufficient data to generate the Tone Maps.
- The receiving STA generates a new Tone Map and assigns a new TMI_AV to it, and sends them to the transmitting STA in the CM_CHAN_EST.IND message. The newly assigned TMI_AV is the only entry in the valid TMI_AV list, and it shall indicate that the new Tone

Map is the Default Tone Map. The Response Type field for this CEI message shall indicate that the message contains a Default Tone Map that is generated as a result of the initial channel estimation procedure. Refer to section 5.2.6.7.

- The receiving STA may also generate one or more AC line cycle adapted Tone Maps after generating the Default Tone Map.
- The transmitting STA should begin to use the newly assigned Tone Maps immediately after reception.
- The receiving STA must be capable of decoding a PPDU encoded using the newly defined Tone Map(s) as soon as the Channel Estimation MME containing the Tone Map is delivered to the destination.

  An implementation may use ROBO-AV modes for transmitting data or management messages before completing the initial channel estimation. It is recommended that the use of ROBO-AV modes be minimized as they are very inefficient.

Figure 514: Initial Channel Estimation

Restrictions on Using the Sound MPDU in the CP during Initial Channel Estimation

The receiving STA shall indicate that the sounding process is complete (i.e., set the SCF bit in the Sound MPDU to 0b1) after receiving no more than 20 msec worth of ROBO modulated MPDU payload (i.e., either Sound MPDU payload or ROBO modulated Data MPDU payload)from the transmitting STA.

Special Use of ROBO Mode in the CP

ROBO Mode must be used for all communication with STAs in other networks. Refer to Section 5.4.3 for details about communication between STAs that are not part of the same AVLN.

Channel Estimation for GREEN PHY

A HomePlug GREEN PHY Station shall communicate with other HomePlug Stations only by using one of the ROBO Tone Maps. As a result, a HomePlug GREEN PHY Station does not initiate a channel estimation procedure. The ROBO Tone Map used is determined by the transmitting station. A HomePlug GP Station shall allow any of the ROBO tone maps to be the Default Tone Map.

Although a HomePlug GREEN PHY Station does not initiate a channel estimation procedure, a HomePlug Green PHY Station shall respond to channel estimation requests from HomePlug Stations. Refer to 5.2.6.7 for more details.

Note: It is recommended for a HomePlug GREEN PHY station to transmit by using the High Speed ROBO Tone Map, in order to optimize the network throughput. A HomePlug GREEN PHY station may monitor the PB error rate to determine the ROBO Tone Map (Standard ROBO or High Speed ROBO) to be used.

Dynamic Channel Adaptation

Dynamic channel adaptation is performed by the receiver subsequent to the initial channel estimation. This process may result in dynamic updates to the Default Tone Map (i.e., replacing an existing Default Tone Map with a new Default Tone Map). This process may also result in the generation of AC line cycle adapted Tone Maps that are valid at various intervals of the AC line

cycle, some of which may replace existing Tone Maps.
Channel adaptation during CP gets complicated due to the possibility of collisions. For this reason, the receiver may require the transmitter to not use a subset of the AC line cycle adapted Tone Maps in the CP. This information is conveyed independently for each Tone Map using the CPF field in the CEI messages. In contrast to the Default Tone Map, AC line cycle adapted Tone Maps are fine-tuned for channel characteristics within that specific interval of the AC line cycle. Hence, the transmitter should use the AC line cycle adapted Tone Map whenever one is available and can be used (based on CPF field in CEI).
The receiver uses the Sound Control field in the CEI messages to control the behavior of the transmitter during CP (SCL_CP) and CFP (SCL_CFP) when it encounters a region in the AC line cycle where there is no AC line cycle adapted Tone Map. When the Sound Control Field requires transmission of Sound MPDUs during intervals of the AC line cycle and there is no corresponding AC line cycle adapted Tone Maps, the transmitter should send Sound MPDUs.
The transmitter may choose to use the Default Tone Map or ROBO Tone Maps even when an AC line cycle adapted Tone Map is available and can be used during a specific interval. The transmitter may also choose to use the Default Tone Map or the ROBO Tone Map during intervals of the AC line cycle where the receiver requested Sound MPDUs. In such cases, the receiver might not be able to provide a new AC line cycle adapted Tone Map for that interval. The transmitter should minimize such deviations from recommended behavior.
Sound Control information (SCL_CP and SCL_CFP) provided by the receiver shall remain static throughout the channel adaptation process. The transmitter shall store the Sound Control information until all the Tone Maps have become invalidated (i.e., have been explicitly invalidated by the receiver or have become stale).
The Sound Reason Code (SRC) in the Sound MPDU shall be used by the transmitter to indicate the reason for transmitting Sound MPDUs. The transmitter sends Sound MPDUs for five different reasons, corresponding to different SRC values:

- Sound MPDU transmitted to obtain the Tone Map corresponding to a TMI_AV, which has been specified by the receiver in the intervals information, but is not recognized by the transmitter. Such conditions can occur when the CEI message carrying the Tone Map did not get delivered.
- Sound MPDU transmitted to indicate a Tone Map error condition detected at the transmitter. Receiver shall resend all valid Tone Maps. The transmitter may use this Sound Reason Code when it determines that the TMD (Tone Map Data – refer to Section 11.5.10) for multiple Tone Map Indices identified in the Valid Tone Map list are not available. Such conditions can occur when the CEI message(s) carrying the Tone Map(s) did not get delivered.
- Sound MPDU transmitted to obtain initial channel estimation.
- Sound MPDU transmitted in an interval where receiver has indicated that no AC line cycle adapted Tone Maps are available.
- Sound MPDU transmitted in an interval specified as Unusable by the receiver.

The Sound Complete Flag (SCF) in Sound ACK is used by the receiver to indicate that the receiver has received sufficient Sound MPDUs for completing the channel estimation. The interpretation of

SCF should be based on the Sound Reason Code (SRC) contained in the corresponding Long Sound MPDU.
For SRC case (1) above, SCF indicates the completion of channel estimation in the interval where the corresponding TMI_AV is used.
For SRC case (2) above, SCF indicates the completion of channel estimation in all intervals of the AC line cycle.
For SRC case (3) above, SCF indicates the completion of initial channel estimation.
For SRC cases (4) and (5) above, SCF indicates the completion of channel estimation in the interval where the corresponding Long Sound MPDUs are transmitted.
If a station has CFP allocation in intervals where Sounding was completed (i.e., SCF = 0b1 is received), it should start transmitting data using a ROBO_AV Tone Map. This procedure enables the transmitter and receiver to exchange Tone Maps using the Bidirectional Bursting procedure (refer to Section 5.4.7). In CP, once the Sounding is complete, the transmitter may wait until a Tone Map is defined for the corresponding interval before transmitting data. It may alternatively use a ROBO_AV Tone Map, but it is recommended that the use of ROBO_AV be minimized as it is very inefficient.
The Dynamic Channel Adaptation procedure is described below:

- The transmitting STA receives a Default Tone Map and zero or more AC line cycle adapted Tone Maps following the initial channel estimation (refer to Section 5.2.6.1.1). The CEI message includes the Sounding Control information (SCL_CP and SCL_CFP) that indicate when Sound MPDUs need to be transmitted to obtain an AC line cycle adapted Tone Map(s).
- The receiver continuously monitors the channel characteristics based on Tone Map modulated MPDUs and provides updates to existing Tone Maps and/or invalidates an existing Tone Map.
- The transmitting STA detects a transmit opportunity (in either CP or CFP) in an interval that does not have a valid AC line cycle adapted Tone Map. It uses the Sound Control information received in prior CEI messages to determine whether it needs to send a Sound MPDU or data modulated MPDU using the Default Tone Map.
- If the transmitter sends a Sound MPDU, the receiving STA responds to the Sound MPDU with a Sound MPDU containing no payload and SAF set to 0b1.
- The transmitting STA operates normally in intervals where valid Tone Maps are defined; that is, it sends one or more SOF MPDUs carrying user data and the receiving STA responds with a SACK MPDU.
- When the receiving STA has detected a sufficient number of Sound MPDUs, it responds with SCF set to 0b1 (i.e., sounding for the corresponding interval is complete) and generates a new Tone Map for the interval.
- The receiving STA sends the CM_CHAN_EST.IND (or CM_TM_UPDATE.IND) message to the transmitting STA. It provides a new Tone Map and indicates that this new Tone Map should be used in the interval in question.
- The transmitting STA should begin to use the newly assigned Tone Maps immediately after reception.

- The receiving STA must be capable of decoding a PPDU encoded using the newly defined Tone Maps as soon as the Channel Estimate Indication MME containing the Tone Map is delivered to the destination.
- The receiving STA should be capable of decoding a PPDU encoded using the old Tone Map until the transmitting STA has begun using the new Tone Map.

Note: The receiving STA is not required to generate a new Tone Map. It may instead simply extend an existing Tone Map to cover the interval in question. In this case, it sends the CM_CHAN_EST.IND (or CM_TM_UPDATE.IND) message with an updated INTERVALS field, but without a new Tone Map.

The receiver shall ensure that a valid Default Tone Map is always available at the transmitter during the dynamic channel adaptation process. The receiver may choose the Default Tone Map to be the same as one of the AC line cycle adapted Tone Maps. The receiver may also choose either STD-ROBO_AV or HS-ROBO_AV as a Default Tone Map.

A HomePlug GP Station shall allow any of the ROBO_AV tone maps to be the Default Tone Map.

Figure 515: Dynamic Channel Adaptation

Maintenance of Tone Maps

The receiver is responsible for ensuring that one or more valid Tone Maps are available in intervals of the AC line cycle where a transmitter may potentially transmit. Subsequent to generating a Tone Map, the receiver continues to monitor the MPDUs modulated with that Tone Map to determine whether the Tone Map is still valid. If the Tone Map is deemed to be invalid (for example, due to high PB errors), the receiver can provide a new Tone Map to replace the existing Tone Map or it may force the transmitter to invalidate the existing Tone Map.

There are two mechanisms that a receiver can use to invalidate a Tone Map:

- The receiver can transmit a CEI message with a valid Tone Map list that does not include the invalidated Tone Map.
- The receiver can indicate that a Tone Map is invalid in the SACKI field (refer to Section 4.4.1.5.3.8.2.3). This shall cause the transmitter to invalidate the Tone Map without the need to send any CEI message.

It is recommended that the receiver use a combination of both mechanisms for invalidating Tone Maps (i.e., the receiver sends a CEI message as soon as the Tone Map is invalidated and subsequently use SACKI to indicate that the TMI_AV is invalidated if the transmitter continues to use the invalidated Tone Map).

The ttransmitter shall associate all valid Tone Maps with a stale timer set to 30 seconds. If 30 seconds elapse since the last CEI message was received from the receiving station, all valid Tone Maps are considered stale and shall be discarded. If a CEI message is received, the transmitter shall discard all Tone Maps that are not in the valid Tone Map list of the CEI message and shall restart the 30-second stale timer for valid Tone Maps.

The transmitter should not expire a Tone Map unless the Tone Map becomes stale or unless it is explicitly requested to do so by the receiver using a CEI message.

Tone Map Intervals

Tone Map Intervals are defined as time periods within the Beacon Period where a particular Tone Map may be used. Since the CCo locks the Beacon Period to the AC line cycle, intervals are synchronized to the AC line cycle.

Channel and noise characteristics over the powerline tend to be periodic with the underlying AC line cycle. In some cases, these impairments occur at twice the frequency of the AC line cycle (i.e., 100 or 120 Hz), while in other cases they may occur at the same frequency as the AC line cycle. The Tone Map intervals are defined over the entire Beacon Period and are therefore periodic with a frequency of half the line cycle. The receiver explicitly specifies the selected Tone Map on all intervals within the Beacon Period. It is anticipated that the receiver will typically define the Tone Maps to be used over the AC line cycle and then repeat this definition to fill out the entire Beacon Period.

The receiving STA specifies the intervals within which various Tone Maps may be used, subject to the following rules:

The Default Tone Map may be used anywhere in the Beacon Period (refer to Section 5.2.6.6).

> Note: The Default Tone Map may be used in an Unusable interval. It is recommended that the transmission of data in Unusable intervals be minimized, as it will very likely be corrupted.

With the exception of the Default Tone Map, intervals are disjoint (non-overlapping).

The transmitter shall not transmit PPDUs with the PPDU Payload crossing the boundary between intervals using different Tone Maps, except when the PPDU payload starts or ends within 150 microseconds of the boundary. The following exceptions to this rule shall apply:

PPDUs using Standard ROBO, Mini ROBO, High Speed ROBO and Default Tone Maps are not restricted to Tone Map intervals,

Reverse SOF MPDU transmissions (refer to Section 5.4.7) are not required to strictly obey the Tone Map interval boundaries.

PPDU transmissions that use Tone Maps having a PHY data rate of less than 15 Mbps at the input to the FEC encoder are not required to strictly obey the Tone Map interval boundaries.

Note: To ensure proper channel estimation at the receiver, it is recommended that Tone Map boundaries be obeyed as closely as possible.

The receiver shall specify intervals that are large enough to carry a complete PPDU, including at least one PB, based on the indicated Tone Map.

The current intervals definition is always carried in the CEI message.

Priority of Channel Estimation Response

The nominal channel access priority for a CEI message shall be CA2. Optionally, if the request for Channel Estimation was sent at CA3 (i.e., Sound MPDU that is transmitted as part of a Global Link or a Link with channel access priority equal to CA3), the CEI message should be sent at CA3. To minimize delays experienced by the CEI message, it is recommended that the message not be multiplexed with segments from other MAC frame streams having a lower priority.

Channel Estimation with Respect to the AC Line Cycle

Channel and noise characteristics over powerlines tend to be periodic with respect to the underlying AC line cycle. The HomePlug AV channel estimation mechanism should take this into

consideration while generating the Tone Maps.
HomePlug AV channel estimation is performed with respect to the receiver. The receiver determines the number of Tone Maps (within the limits specified by the transmitter) and the intervals within the Beacon Period where they are valid. The interval information is sent to the transmitter along with the individual Tone Maps.
The transmitter then selects the Tone Map for a given PPDU based on the interval within the Beacon Period where the PPDU is to be transmitted. Since the Beacon Period is synchronous to the AC line cycle, the selection of Tone Maps by the transmitter is also synchronous to the AC line cycle.
HomePlug AV stations shall support a minimum of two transmit and two receive Tone Maps per station it is actively communicating with, for up to two stations. Thus, a HomePlug AV station shall be able to support a minimum of four transmit and four receive Tone Maps. Apart from these, all HomePlug AV stations shall also be capable of supporting Unusable Intervals. Unusable Intervals identify regions within the AC line cycle period where the channel estimation algorithm indicates poor channel characteristics. The receiver designates a particular interval of the line cycle as an Unusable Interval by setting TMI_AV to 0xFF. A HomePlug AV station should transmit in the Unusable Tone Map interval using a Sound MPDU (ROBO or Mini ROBO) so that the receiver may continue to estimate the channel during this interval. A Default or STD/Mini-ROBO_AV Tone Map may be used in an Unusable interval. It is recommended that the transmission of data in Unusable intervals be minimized, as it will very likely be corrupted. A receiver may choose to define an interval for either ROBO or HS-ROBO. A receiver shall not define an interval for Mini-ROBO. If the receiver specifies ROB0 or HS-ROBO, the transmitter may use Mini ROBO in that interval. This allows transmission of heavily padded segments that can fit in a PB136.

- HomePlug GREEN PHY Handling of Channel Estimation Requests from HomePlug AV

When a HomePlug AV 1.1 station wants to transmit data to a HomePlug GP station and it determines that no valid channel adapted Tone Maps exist for the GP station, it initiates the Channel Estimation Procedure and sends SOUND MPDUs as explained in Section 5.2.6.1. A HomePlug GP station shall acknowledge the SOUND MPDUs using a SOUND ACK MPDU and it shall set the Sound Complete Flag (SCF = 0b1) in the first SOUND ACK MPDU transmitted. The HomePlug GP station shall send a CM_CHAN_EST.IND MME with few specific fields set as described below.

- The MAXTM field shall be set to 0x00. By setting this field to 0x00, the HomePlug GP station indicates to the HomePlug AV 1.1 station that it is not capable of generating any Tone Maps.
- The RESPT field shall be set to 0x01.
- The CP_TMI_AV field shall be set to 0x00, indicating that the default Tone Map is Standard ROBO. Note: Alternately, a HomePlug GP station may set the CP_TMI_AV field to 0x01, indicating that the default Tone Map is High Speed ROBO provided that the GP station is capable of estimating the quality of the channel and also determines that High Speed ROBO transmissions can be supported on this channel.

- The SCL_CP field shall be set to 0x01.
- The SCL_CFP field shall be set to 0x01.
- The NTMI_AV field shall be set to 0x00.
- The NINT field shall be set to 0x01, indicating that there is only one tone map interval - the entire Beacon Period.
- The ET[0] field shall be set to a value greater than or equal to the Beacon Period.
- The INT_TMI_AV[0] field shall be set to 0xFE, indicating that there are no AC line cycle adapted Tone Map for the entire Beacon Period.
- The NEWTMI_AV field shall be set to 0x00
- The MAX_FL_AV field shall be set to indicate 2501.12 μs
- The RIFS_AV_1SYM field shall be set to indicate RIFS_AV_default.
- The RIFS_AV_2SYM field shall be set to indicate RIFS_AV_default.
- The RIFS_AV_GT2SYM field shall be set to indicate RIFS_AV_default.

Link Status Function

As with HomePlug AV, the Link Status Function provides a continuous indication of the presence of other HomePlug GREEN PHY stations on the physical medium. This function has several uses, such as providing a user an indication during installation that a particular GREEN PHY station can hear other HomePlug stations. This indication can also help manufacturers troubleshoot during customer-service calls. This function is typically indicated to the user by a Light-Emitting Diode (LED), though this is an implementation choice. Providing this indication to the user is optional. Link Status shall be active as long as any error-free Frame Control delimiter has been received in the past LinkStatusTimeout. Otherwise, the Link Status shall be inactive.

During normal network operation, the Frame Control delimiter is heard on a regular basis, due to the Central Beacon, Proxy Beacon, Discover Beacon, and the transmission of CM_UNASSOCIATED_STA.IND messages by Unassociated STAs.

Beacon Relocation Procedure

A CCo may relocate the position of its Beacon by transmitting the Beacon Relocation BENTRY in the Beacon. As described in Section 4.4.3.15.4.6, this BENTRY includes a relocation countdown that indicates the Beacon Period where the relocation will take effect.

There are two Relocation Types:

Relocation Type Relocation Offset is used to relocate a Central Beacon, except this type shall not be used to move to a different Beacon Slot in a Group that the CCo belongs to. Relocation Offset may be used to move to a Beacon Slot of a Group the CCo is joining. In this case, the NewNumSlot shall be set to the Beacon Slot number the Central Beacon of the CCo will occupy when the relocation become effective.

Relocation Type Relocation SlotID shall only be used to move the Central Beacon to another Beacon Slot in the Group of networks the CCo belongs to.

If the CCo is not in Coordinated Mode, the CCo shall broadcast the Beacon Relocation BENTRY in at least the last five Beacon Periods prior to relocating the Beacon. If the CCo is in Coordinated Mode, then the CCO shall broadcast the Beacon Relocation BENTRY in at least the last ten Beacon Periods prior to relocating the Beacon. When Relocation Type is Relocation Offset, then no schedule shall be broadcast that has a persistence lasting beyond the Beacon Period where the

relocation countdown equals zero, but the CCo may announce a Preview Schedule to take effect with the relocated Beacon. The CCo is responsible for coordinating its new schedule with any neighbor networks.

A STA receiving the Beacon Relocation BENTRY may continue to operate normally using the broadcast schedules through the last Beacon Period prior to the relocation (i.e., the Beacon Period where the relocation count equals one).

Note: When Relocation Type is Relocation Offset, the new Beacon location is always advanced in time relative to the old Beacon location. When Relocation Type is Relocation SlotID, the NewSlotID may be increased or decreased.

When coordinating as part of a Group of networks, the Beacon Relocation BENTRY with type set to Relocation Offset and the Leaving Group Flag set may be used to indicate the CCo is leaving the Group of networks. The AC Line Cycle Countdown BENTRY shall be present if the CCo is providing AC line cycle synchronization.

The Beacon Relocation BENTRY shall not be used to move the Beacon Region of a Group. Beacon Transmission Offset (BTO) does not include the change in Beacon Location due to the Beacon Relocation BENTRY. Thus, the location of the Beacon following the Beacon where RCD=1 shall be:

The current Beacon location plus BTO[0] + (1,000,000 or 833,333) + Beacon Relocation Offset when Relocation Type is Relocation Offset, or

The current Beacon location plus BTO[0] + (1,000,000 or 833,333) + Beacon Slot Length * (Relocation Slot ID – Current Slot ID) when Relocation Type is Relocation SlotID.

- Signal Level Attenuation Characterization

The Signal Level Attenuation Characterization (SLAC) is a protocol to measure the attenuation profile of a signal between GP Stations. The ability to support SLAC protocol is optional for Green PHY stations. SLAC may be used in applications such as Plug-in Electric Vehicle (PEV) and Sub-meter (SM) association.

Details of the PEV-EVSE Association procedure are described in Section 13.8.

Bridging

As with HomePlug AV, a GREEN PHY station shall support the ability to communicate with at least 32 bridged destination addresses. Bridging is accomplished through source-aware bridging, as opposed to transparent bridging. Both forms use MAC-level addresses for bridging decisions. Source-aware bridging is necessitated by the need of the transmitting station to know the MAC address of the station bridging for the destination. This is required to maintain efficient, reliable, high-speed communications on the network. By communicating directly to the bridge, the transmitting and receiving stations can ensure they use a proper channel map along with MAC-level acknowledgements if required.

There are two components to bridging:

Acting as a bridge

Communicating through a bridge

Acting as a bridge to another network is optional. The ability to communicate through a bridge is mandatory.

Acting as an AV Bridge

A device is acting as an AV Bridge if it is bridging traffic to a network that cannot natively receive said traffic. This is often the case when working with two different physical networks, such as a power line network and an 802.3, wired Ethernet network.

With source-aware bridging, the AV Bridge must be aware of, and learn the source MAC address of, all devices connected on the bridged network. An AV Bridge shall maintain a Local Bridge Destination Address Table (LBDAT) that lists all source addresses of the devices that it is aware of on the network for which it is bridging. The LBDAT shall be communicated to all other AV stations via the CM_BRG_INFO.CNF message.

The CM_BRG_INFO.CNF message shall be regularly communicated to all of the AV devices for which it has an active Tone Map with a period of no less than MIN_BIR_TIME seconds and no greater than every MAX_BIR_TIME seconds.

STAs in the AVLN may send a **CM_BRG_INFO.REQ** message to obtain the LBDAT of any other STA in the AVLN. All STAs in the AVLN shall be capable of properly responding to a **CM_BRG_INFO.REQ** with a **CM_BRG_INFO.CNF**. STAs that are not capable of acting as a bridge shall respond to a **CM_BRG_INFO.REQ** with a **CM_BRG_INFO.CNF** that has the Bridging Station Flag (BSF) set to indicate that the STA does not perform bridging functions (refer to Section 11.5.15). It is recommended that a STA sending **CM_BRG_INFO.REQ** wait for a minimum of MMEResponse_WaitTime for receiving the corresponding **CM_BRG_INFO.CNF** before determining that the message exchange has failed.

The AV Bridge shall age the LBDAT such that devices on the bridged network that have not transmitted a packet for at least LBDAT_EXPIRE_TIME are removed from the LBDAT.

Behavior for Incoming Traffic from the Powerline Network

When an AV Bridge receives traffic from the powerline, it shall forward that traffic to the bridged network if:

It contains an ODA corresponding to the broadcast address.

It contains an ODA corresponding to a multicast address.

An AV Bridge can forward all received unicast traffic to the bridged network. Optionally, an AV Bridge may filter unicast traffic with ODA that is known to exist on the powerline network before delivering it to the bridged network.

,

GREEN PHY Behavior for Incoming Traffic from the Powerline Network

The behavior of a Green PHY STA is identical to that described in Section 5.3.1.1, with the following exception:

A Green PHY STA that receives unicast traffic with an ODA for which it is acting as a repeater, shall forward the packet as described in Section 5.8.1. Otherwise, it may forward the traffic to the bridged network.

Behavior for Incoming Traffic from the Bridged Network

When an AV bridge receives traffic from the bridged network, it shall forward that traffic onto the powerline network if it contains:

An ODA corresponding to the broadcast address. The AV Bridge shall forward this traffic using the broadcast TEI.

An ODA corresponding to a multicast address. The AV Bridge shall forward this traffic using the

broadcast TEI.
A unicast ODA corresponding to the MAC address of an AV device. The AV Bridge shall forward this traffic using the TEI of that AV device.
A unicast ODA not known to exist on the powerline or another bridged network. The AV Bridge shall forward this traffic using the broadcast TEI.
A unicast ODA known to exist on another bridged network. The AV Bridge shall set the DTEI to the TEI of the AV Bridge bridging for the ODA on the other bridged network.
When an AV bridge receives traffic from the bridged network, it shall not forward that traffic onto the powerline network if it contains a unicast ODA corresponding to an entry in its LBDAT.
In effect, the AV Bridge must forward all traffic to the powerline unless it contains a DA corresponding to an entry in its LBDAT.
Communicating through an AV Bridge
Communication through a bridge is more aptly defined as how to communicate with a device whose DA is not known to exist on the AV network or any other known network. When this occurs, the traffic must be transmitted in such a way as to ensure that the intended devices will receive it, as long as the device's network is reachable.
AV Bridges will communicate their LBDATs to at least all stations for which the bridge has a current Tone Map. The CM_BRG_INFO.CNF message from an AV Bridge will contain the MAC addresses listed in the LBDAT for that bridge. The AV Station shall create a Remote Bridged Address Table (RBAT) containing the MAC addresses in the CM_BRG_INFO.CNF and associate it with the TEI for the AV Bridge that sent it. The AV Station shall maintain a separate RBAT for each AV Bridge that the Station is communicating with.
AV Stations shall independently age each RBAT so that if the station has not received a CM_BRG_INFO.CNF from the associated AV Bridge within at most RBAT_EXPIRE_TIME, it shall delete the RBAT for that bridge.
When an AV Station intends to transmit a packet containing a unicast ODA, it must determine whether that ODA is Known or Unknown.
An ODA is Known if it:
Corresponds to the MAC address of an AV station which is associated with a TEI.
Is listed in the RBAT for an AV Bridge and, hence, is a bridged destination on a remote network.
Is the multicast address of a known multicast group.
An ODA is Unknown if it is:
Unicast and not a known AV Station or a known Bridged Destination.
The broadcast address.
An unknown multicast address.
Communication with a destination differs, depending on whether its ODA is Known or Unknown.
Communication with a Known DA
To determine whether a DA is Known, the AV station must scan through its list of AV stations and its RBAT. If the AV station maintains a separate RBAT for each bridge, it should ensure that the scan order for the RBATs is performed in chronological order, starting with the most recently received RBAT and continuing to the oldest. This recommendation is important to properly track mobile STAs.

Known AV Station

When the ODA corresponds to another AV station, the sending station will know the destination station's TEI. When sending to a known AV Station, a sending station shall set the DTEI to the TEI of the destination station. The STEI shall be set to the TEI of the sending station.

Known Bridged Destination

When the ODA is listed in the RBAT for a known AV Bridge the sending station will know that the destination is located on a bridged network and is a Bridged Destination. When sending to a known Bridged Destination, a sending station shall set the DTEI to the TEI of the AV Bridge. The STEI shall be set to the TEI of the sending station.

Known Multicast Address

When the ODA is multicast and the sending station is aware of the unicast destinations (Known destinations) participating in the multicast group, the sending station may send the traffic unicast to the known destinations.

When sending multicast traffic to the known multicast participants, the sending station shall follow the rules above for sending traffic to Known AV Stations and/or Known Bridged Destinations as is appropriate.

Communicating with an Unknown DA

Unknown Unicast Destination

When a destination address is unicast and not a known AV Station or a known Bridged Destination, the sending station does not know whether the destination is on an AV network or a bridged network. Because of this, the traffic must be sent broadcast to ensure that it reaches its intended destination and for it to become Known.

When sending to an unknown destination, the sending station shall set the DTEI either to the TEI of the multicast proxy (refer to Section 5.4.8.3) or to broadcast TEI. The STEI shall be set to the TEI of the sending station.

Broadcast Address

When a destination address is the broadcast address the sending AV station must broadcast the traffic. When sending to the broadcast MAC address, the sending station shall set the DTEI either to the TEI of the multicast proxy (refer to Section 5.4.8.3) or to broadcast TEI. The STEI shall be set to the TEI of the sending station.

Unknown Multicast Address

An unknown multicast address is one in which the sending station is unaware of the unicast destinations participating in the multicast group. In this case, the sending station must broadcast the traffic.

When sending to an unknown multicast address, the sending station shall set the DTEI either to the TEI of the multicast proxy (refer to Section 5.4.8.3) or to broadcast TEI. The STEI shall be set to the TEI of the sending station.

Bridging with Quality of Service

A PLC-AV bridge that supports QoS will set up Connections with the PLC network on behalf of the STAs for which it is bridging. The method used depends on whether the bridge is a (normal) bridge or a smart bridge. A smart bridge is one that handles QoS and connection establishment above the H1 interface.

A normal bridge can use the optional Auto-Connect service (if available) for setting up Connections (refer to Section 6.6). After checking the Bridging Information Table to determine that the received Ethernet frame can be delivered to the final destination through a transmission over the PLC network, the bridge simply passes the packet through the H1 interface without any further effort. If the Classifier fails to find any matching rules to associate the packet with a Connection, it will pass the packet to the Auto-Connect service if available to determine whether a Connection should be established.

A smart bridge differs from a normal bridge in that the former shall have its own mechanism (e.g., a classifier) to determine whether a new Connection should be established, an existing Connection should be used, or a CLS should be used for each packet it receives from a STA for which it is bridging. If a Connection is required, a smart bridge shall use the Connection setup primitives and procedures (refer to Section 11.5.16 and Section 5.2.3.1) to set up a Connection with the peer bridge or station.

Data Plane

As with HomePlug AV, Data plane handling of information exchanged between HomePlug GREEN PHY stations will depend on the association and authentication status of the STAs relative to each other. STAs that are associated and authenticated with the same AVLN can exchange both Management messages and Data securely. Details of the data plane for such communications are described in Section 5.4.1. As with HomePlug AV, GREEN PHY limits communications between STAs that are not associated and authenticated with the same AVLN to only a subset of the Management Messages and prohibits the exchange of any Data. Section 5.4.2 provides details on the data plane for communication between two STAs that are associated with the same AVLN, but either one or both of them are not authenticated. Details of the data plane for communication between STAs that are either not associated with any AVLN or are associated with different AVLNs are described in Section 5.4.3.

Communication between Associated and Authenticated STAs

As with HomePlug AV, the HomePlug GREEN PHY MAC sublayer transports data passed down through the Data SAP. The term “MSDU” refers to the information that the MAC has been tasked to transport. The MSDU is passed to the MAC by way of the MD_DATA.REQ primitive (refer to Section 12.3.2.1). The MAC processes the MSDU and generates a MAC Frame. The MAC Frame is the basic entity that is subjected to the MAC services of reliable transport to a destination. MAC Frames that belong to the same stream are concatenated together into a MAC Frame Stream. The process of generating a MAC Frame Stream from MSDUs is referred to as “MAC Framing.”

The OSA and ODA fields in the MSDU indicate the original source address and original destination address of the MSDU. The ODA and/or OSA might not be the MAC addresses of HomePlug GREEN PHY stations within the AVLN. Such cases will occur when the MSDU Payload is bridged across the AVLN. The HomePlug GREEN PHY MAC uses the bridging function (refer to Section 5.3) to map the {OSA, ODA} to the powerline source and destination MAC addresses (i.e., {SA, DA}). Within an AVLN, each station is provided with a unique TEI. Thus, each SA and DA of unicast transmissions uniquely map on to the corresponding STEI and DTEI, respectively.

MAC Frame Generation

MSDUs either belong to an established Connection or are independent (i.e., connectionless MSDUs). The packet classifier at the CL determines the Link Identifier associated with the MSDU and passes it to the MAC sublayer as part of the MD_DATA.REQ primitive. MSDUs belonging to an established Connection have their LID set to the LLID or GLID associated with the Link. MSDUs that do not belong to an established Connection have their LID set to their corresponding PLID.

Note: The range of LID values can be used to determine whether the LID is a PLID, LLID, or GLID (refer to Section 5.2.1.4.1).

Connectionless MSDUs shall contain either an MSDU Payload or a Management Message. For connectionless MSDUs carrying an MSDU Payload, a MAC Frame is generated from each MSDU by prepending the MSDU Payload with a MAC Frame Header and adding an Integrity Check Value (ICV) at the end. The MAC Frame Type field in the MAC Frame Header indicates the absence of an ATS (i.e., Arrival Time Stamps are not allowed with connectionless MSDUs). The MAC Frame Length in the MAC Frame Header shall be set to the length of MSDU Payload. ICV is used to verify the correct decryption and reassembly of the MSDU Payload at the receiver. The ICV shall be computed over the MSDU Payload, excluding the MAC Frame Header.

All MSDUs that carry Management Messages shall have their LID set to a PLID value, regardless of whether they carry information relevant to an established Connection. Consequently, and as with HomePlug AV, GREEN PHY transmits all Management Messages connectionless as part of Management Message Streams. This ensures timely delivery of important Management Messages. The various types of Management Messages and their formats are described in Chapter 11. A MAC Frame is generated from a Management Message by prepending it with a MAC Frame Header and confounder, then adding an ICV at the end. The MAC Frame Type field in the MAC Frame Header shall indicate the presence of a Management Message with confounder. The MAC Frame Length in the MAC Frame Header indicates the length of the encapsulated Management Message including the confounder, but not including the MAC Frame Header or ICV. The ICV is used to confirm correct decryption and reassembly of the Management Message at the receiver. The ICV shall be computed over the Management Message, not including the MAC Frame Header or confounder.

The MAC Frame Header explicitly indicates the presence of a Management Message or MSDU Payload. This information is used to associate the contents with the correct MAC Frame Stream (refer to Section 5.4.1.2).

Connection-based MSDUs shall only carry an MSDU Payload (i.e., Management Messages are not allowed as part of connection-based MAC Frame Streams). MAC framing of Connection-based MSDUs will depend on whether the ATS option is used. This option is negotiated during the connection establishment process (refer to Section 5.2.3). When this option is not used, the MAC Framing for connection-based MSDUs is the same as that of connectionless MSDUs carrying MSDU Payloads.

ATS is used as part of the jitter-control mechanism (refer to Section 6.7.3). The CL is responsible for time stamping the arrival time of the payload associated with the MSDU (i.e., ATS) at the H1 interface and providing it to the MAC sublayer as part of MD_DATA.REQ primitive. When ATS

option is used, the MAC Frame shall consist of a MAC Frame header, followed by the ATS, followed by MSDU Payload followed by an ICV. The MAC Frame Type in the MAC header shall indicate the presence of ATS. The MAC Frame Length shall be set to the sum of the length of the ATS and the MSDU Payload. ICV shall be calculated on MSDU Payload only, excluding the MAC Frame Header and ATS.

MAC Frame Streams

As with HomePlug AV, the HomePlug GREEN PHY MAC segregates MAC Frames carrying MSDU Payload based on the {DTEI, LID, CLST} tuple with which they are associated. MAC Frames carrying MSDU Payload and belonging to the same {DTEI, LID, CLST} are concatenated to form a MAC Frame Stream. Since the MAC Frame Streams carry regular data, as opposed to Management Messages, they are also referred to as "data streams."

The HomePlug GREEN PHY MAC segregates MAC Frames carrying Management Messages based on the DTEI with which they are associated. MAC Frames carrying Management Messages and belonging to the same DTEI are also concatenated to form a MAC Frame Stream. These streams are referred to as "Management Streams."

Each stream belongs to one of the following categories:

Data streams for established Connections

MAC Frames that belong to each established Connection are provided with a separate MAC Frame Stream at the transmitter. This enables provisioning of QoS guarantees. The LLID or GLID uniquely identifies a Link at the transmitter. The LLID is used along with the STEI to uniquely identify a stream within an AVLN.

Data stream for connectionless MSDUs

Connectionless MAC Frames that belong to the same {DTEI, PLID, CLST} tuple are concatenated to form a separate MAC Frame Stream at the transmitter.

As in HomePlug AV, for GREEN PHY a DTEI of 0xFF indicates a multicast/broadcast transmission. As a result, all connectionless multicast and broadcast frames that belong to the same PLID shall be concatenated into a single MAC Frame Stream at the transmitter. For multicast/broadcast transmissions, distinction should be made between the DTEI associated with the stream (which is 0xFF) and the DTEI actually present in the Frame Control. The latter may be a unicast TEI, when the partial acknowledgments are used (refer to Section 5.4.8.3.). In this case, the Multicast Flag in the Frame Control is used to infer the presence of a multicast/broadcast payload.

Management Streams

MAC Frames that carry Management Messages and belong to the same DTEI are concatenated to form a separate MAC Frame Stream at the transmitter.

The MAC Frame Stream is the basic entity that is subjected to MAC Segmentation and Reassembly process. Figure 516 shows an example of chaining multiple MSDUs into a MAC Frame Stream.

PLID of Management Streams

Management Messages intended for the same DTEI are concatenated regardless of the PLID associated with them. This choice is intended to reduce the number of MAC Frame Streams that must be managed by the stations. Priority promotion of Management Streams is used to ensure that

high-priority Management Messages are delivered in a timely manner. When transmitting Segments of a Management Stream over the medium, each Management Stream shall be treated as having a priority (or PLID) equal to the highest priority Management Message (or its associated segment) pending in the stream. In addition to determining CSMA priority, the PLID associated with a Management Stream is used for deciding whether the segments of the Management Stream can be combined with data streams that are intended for the same DTEI (refer to Section 5.4.1.4). For example, consider a Management Stream that contains the three MAC Frames {MF1, MF2, MF3}. In this example, MF1 is the oldest MAC Frame and MF3 is the most recent. Further, consider the PLIDs {MF1, MF2, MF3} to be {0, 3, 0} respectively. Since the highest priority of the Management Message in this stream is 3, the PLID of the stream at this instance is treated as 3. Once all the segments carrying MF2 are transmitted to the destination (and assuming that segments from MF3 are still pending), the priority of the MAC Frame Stream is reduced to a PLID of 0.

Figure 516: MAC Framing Process for Data Stream

Segmentation

Using the MAC Framing process, MAC Frames are generated from MSDUs and multiple MAC Frames that belong to the same stream are concatenated into MAC Frame Streams. Each MAC Frame Stream is then segmented into 512-octet segments for transportation as part of an MPDU Payload. Each segment maps onto a single FEC Block of a PPDU at the physical layer. Since PHY errors occur on an FEC Block basis, segmentation ensures that only corrupt data is retransmitted. The MAC framing and segmentation processes ensure that maximum-size MPDUs are exchanged over the medium, improving protocol efficiency.

A segment can be generated from a MAC Frame Stream whenever there are enough octets to form a new segment. A MAC Frame Stream is treated as an octet stream for segmentation purposes. Thus, a segment can contain a fraction of a MAC Frame and/or multiple MAC Frames, depending on their sizes. For each segment, the MAC shall track the offset of the first MAC Frame Boundary within the segment. This information is transmitted along with the segment and is used by the receiver to demarcate the MAC Frames from the received segments. Each segment is also associated with a SSN. The SSN is initialized to zero for the first segment in a MAC Frame Stream and incremented by one when a new segment is generated (refer to Section 4.4.2.1.1.1). SSNs enable reception of out-of-order segments and duplicate detection at the receiver.

The end of the MAC Frame Stream might not contain enough octets to fill a segment completely at a time when the last MAC Frame should be sent. In such cases, the MAC Frame Stream shall be padded, so a segment can be formed. Padding adds overhead and, therefore, should be avoided whenever possible. It is recommended that padding of MAC Frame Streams to generate a segment be done just before the segment can be transmitted on the medium. The first two bits of the first (or only) octet in the pad shall be set to 0b00 to indicate the presence of an octet pad in the remainder of the segment. The receiver can then identify the octet pads and start processing the next segment. Note: The first two bits of a valid MAC Frame are never 0b00 (refer to Section 4.3).

Once a segment is formed as described above, it is treated as a single entity targeted for reliable delivery services by the MAC. Each segment is encrypted and then inserted into a PBB. A PB comprises the data bits of a FEC Block at the PHY layer. All PBs have a PB Header, PBB, and

PBCS. The PB Header field carries the Sequence Number and MAC Frame Boundary offset associated with the segment. The PB Header also indicates whether the segment belongs to a data stream or a Management Stream. The PBCS field is used to check the integrity of the PHY Block at the receiver.

Long MPDU Generation

A Long MPDU consists of Frame Control information followed by one or more PBs. Each Long MPDU Payload can carry segments from a data stream and/or a Management Stream. The following rules shall be used when segments from Management Streams are combined with segments from a data stream within a single MPDU:

Connectionless data streams can only be combined with Management Streams that are associated with the same {DTEI} and have the same PLID (refer to Section 5.4.1.2.1).

Global connection-based data streams (i.e., LID indicates a Global Link Identifier) can only be combined with Management Streams that are associated with same DTEI and have a PLID of 3.

Local connection-based data streams (i.e., LID indicates a Local Link Identifier) can only be combined with Management Streams that are associated with the same DTEI and have the same channel access priority.

MAC traffic may often require delivery of short messages. This is particularly true of Management Messages. When a segment containing 128 octets or less of MAC Frame Stream data is the only pending segment in a MAC Frame Stream, it may be transmitted as a padded segment in a 136-octet PB. The first octet of the segment pad indicates that the remainder of the segment is padded to the next 512-octet boundary, eliminating the need to send the rest of the padding in PBs. All receivers shall be capable of receiving a 136-octet PB containing a shortened 512-octet segment.

Note: If the segment is exactly 128 octets, the presence of an octet pad to the next 512-octet boundary is implicit. For example, if a station needs to send a 20-octet Management Message to another station and has no other Management Message segments pending to that station, it should transmit it using an MPDU with a single 136-octet PB.

An MPDU shall only contain PBs of the same size. This means that short Management Messages that are combined with data streams using 520-octet PBs must also use 520-octet PBs for transmission.

Note: Only one 136-octet PB is allowed per MPDU.

In the above example, if the 20-octet Management Message must be transmitted with segments of another data stream in the same MPDU, it must be transmitted as a padded 512-octet segment.

Deciding whether to transmit a segment using a 136- or 520-octet PB must be made independently at each transmission opportunity. In the above example, if the first transmission of the 20-octet Management Message (using a 136-octet PB) is not successful, and if there are more management segments available when the second transmission opportunity arrives, the Management Message must be retransmitted as a padded 512-octet segment along with other segment(s).

SSNs in the PB Header are 16 bits long. Comparison of SSNs should consider the SSN “wrap around.” In the remainder of this specification, SSN X is considered to be greater than SSN Y if the following condition is met:

$0 < (X-Y) \bmod 65536 < 32768$

The ordering of segments in an MPDU should obey the following rules:

Data segments in an MPDU shall be transmitted in no more than two groups.
Management segments in an MPDU shall be transmitted in no more than two groups.
A set of segments in an MPDU should be considered to be a group if they satisfy the following conditions:
They are transmitted contiguously in the MPDU(not counting PBs for which the Valid PHY Block Flag is not set).
If {SSN1, SSN2, … , SSNK} are the SSNs of segments in a group in the order they are transmitted on the medium, with SSN1 being the first segment to be transmitted, then the following relationship shall hold: SSN1 ≤ SSN2 ≤ …. ≤ SSNK.
Note: An MPDU carrying both data and management segments can have up to two groups of data segments and up to two groups of management segments.
Once a Long MPDU is generated, it is handed over to the physical layer for delivery.
Reassembly
The information contained in the Frame Control (refer to Section 4.4.1) and PB Header (refer to Section 4.4.2.1.1) is used by the receiver to determine uniquely the stream to which a segment belongs. The relevant fields in the Frame Control are {STEI, DTEI, MCF, and LID}. The relevant field in the PB Header is MMQF. When the Multicast Flag (MCF) field indicates the presence of a broadcast/multicast payload, the DTEI is assumed to be 0xFF for reassembly purpose (and the actual value DTEI present in the Frame Control is ignored).

Figure 517: MAC Segmentation and MPDU Generation
Buffer Management, Flow Control, and Duplicate Detection
As with HomePlug AV, GREEN PHY stations communicate with each other by exchanging segments from MAC Frame Streams. Successful communication between stations requires the transmitter and receiver(s) to be properly synchronized with respect to SSNs that are currently being used in the MAC Frame Streams. A flow-control mechanism is used to ensure that segments do not get dropped due to buffer overflow at the receiver. In addition, the transmitter should handle stale segments while the receiver should gracefully overcome reassembly failures. The receiver should also handle duplicate segments. This section provides the various mechanisms used by HomePlug GREEN PHY stations for buffer management, flow control, and duplicate detection.
Transmit Buffer Management
The transmitter associates each received MSDU with an expiration time. The expiration time of an MSDU shall be set to the sum of its ATS and Max_TX_Timer. For MSDUs belonging to an established Connection, the Max_TX_Timer shall be equal to the latency negotiated during the connection establishment procedure. Using the MAC Frame-generation process (refer to Section 5.4.1), each MSDU is converted into a MAC Frame and inserted into the corresponding MAC Frame Stream. The expiration time for a MAC Frame shall be the same as the expiration time of the corresponding MSDU. If a MAC Frame expires before a segment can be formed, the Frame shall be discarded. Each segment shall have an associated expiration timer. This expiration timer is the maximum of the expiration timers of the MAC Frames that it intersects.
Note: Once a segment is formed, only the segment's expiration time needs to be tracked. The expiration time of the MAC Frames that intersect it will have no relevance.

The transmitting MAC should discard segments after they have been delivered successfully. A segment is considered to be successfully delivered if the SACK indicates successful reception. Segments of a broadcast/multicast transmission that do not have a corresponding SACK (i.e., DTEI in the Frame Control set to broadcast TEI) may be considered to be delivered successfully. The transmitter may also send broadcast/multicast packets using partial acknowledgements (refer to Section 5.4.8.3) in which any station receiving the multicast/broadcast transmission can be designated (using the DTEI) as a proxy to send SACK responses. In such cases, the SACK generated by the proxy may be used to determine the successful delivery of the segments. If a segment-expiration time is reached and the segment is not currently being transmitted, the segment shall be discarded. If the segment-expiration time is reached when a segment is being transmitted, the transmitter shall wait until the current transmission is complete before the segment can be discarded.

As with HomePlug AV, each HomePlug GREEN PHY station shall be capable of tracking multiple MAC Frame Streams and their associated segments. For each MAC Frame Stream, the station shall track the Minimum Transmit Segment Sequence Number (MinTxSSN) and Maximum Transmit Segment Sequence Number (MaxTxSSN). MinTxSSN and MaxTxSSN are used to perform flow control at the transmitter. MinTxSSN is the SSN of the oldest pending Segment in the MAC Frame Stream. If there are no pending segments, MinTxSSN shall indicate the SSN that will be assigned to the next newly generated segment. MaxTxSSN is the SSN of the most recent segment that can be transmitted in the MAC Frame Stream before the segment with SSN of MinTxSSN is acknowledged successfully. The MaxTxSSN shall be the sum of RxWSz and the MinTxSSN minus one (i.e., MaxTxSSN = RxWSz + MinTxSSN -1). RxWSz is the maximum number of segments that the receiver is capable of buffering.

The RxWSz for various MAC Frame Streams is obtained as follows:

- For MAC Frame Streams of established Connections, RxWSz is negotiated during connection setup and shall remain fixed until the connection is terminated.
- For connectionless MAC Frame Streams carrying unicast data, RxWSz is initialized to 16 and is dynamically updated based on the RxWSz advertised in the SACK delimiter (RxWSz refer to Section 4.4.1.5.3.10).
- For MAC Frame Streams (both unicast and multicast/broadcast) carrying management messages, RxWSz is set to 8.

  Note: Compared with connectionless data streams, no negotiation of RxWSz is necessary for Management Streams.
- Broadcast and multicast data transmissions that are connectionless shall use an RxWSz of 16.
- MinTxSSN shall be set to 0x0000 when the MAC Frame Stream is initially formed. MinTxSSN is subsequently updated when one of the following conditions occurs:

  Oldest pending segment in the MAC Frame Stream is successfully delivered.
  Receiver indicates a reassembly failure (using MFSRsp = FAIL).

Note: Separate instances of this Finite State Machine (see Figure 518) are maintained for each MAC Frame Stream. The transmitter sets the MFSCmd fields in the SOF MPDU as appropriate for the MAC Frame Streams transported in the MPDU (MFSCmdData for data stream and

MFSCmdMgmt for the management stream). If no data is present for one of the streams, the associated MFSCmd is set to “No Operation” (NOP).

Figure 518: Transmit MAC Frame Stream FSM

As in Figure 518 shows, the transmitter transitions from the IDLE state (i.e. where no MAC Frame Stream is present) to the TX_INIT_MFS state when data is available for transmission. The transmitter sets MFSCmd to INIT in this state. It remains in this state until it receives a SACK with MFSRsp set to ACK, indicating that the receiver has successfully processed the INIT command. The transmitter then updates MinTxSSN, MaxTxSSN, and RxWSz and transitions to the TX_IN_SYNC state.

In the TX_IN_SYNC state, the transmitter sets MFSCmd to IN_SYNC. For each SACK received with MFSRsp set to ACK, the transmitter updates MinTxSSN, MaxTxSSN, and RxWSz. Reception of MFSRsp set to NACK indicates that the receiver has reduced the RxWSz and causes the transmitter to transition to the TX_RE_SYNC state. In the TX_IN_SYNC state, expiration of any unacknowledged segments causes the transmitter to update the OPSF of the next unacknowledged pending segment. If the expiration results in no unacknowledged segments remaining in the window, the transmitter transitions to the TX_RE_SYNC state.

In the TX_RE_SYNC state, the transmitter sets MFSCmd to RE_SYNC and must only transmit the oldest segment (this segment may be repeated multiple times within the MPDU). The transmitter remains in this state until it receives a SACK with MFSRsp equal to ACK and indicating the oldest pending segment is successfully delivered.

If the transmitter decides to release an existing MFS, it transitions immediately to the TX_RELEASE state, starts the release timer, and begins sending MFSCmd set to RELEASE. Reception of MFSRsp set to ACK indicates that receiver has received the release and causes the transmitter to transition to the IDLE state. If the release timer expires before the MFSRsp of ACK is received, the transmitter may immediately transition to the idle state.

Reception of MFSRsp set to FAIL indicates that the receiver does not have sufficient resources to process the MFS and causes the transmitter to transition to the FAIL state. The transmitter shall set the Fail Wait Timer to FAIL_WAIT upon entry into this state and ceases transmission of segments from this MFS until the Fail Wait Timer expires.

Reception of MFSRsp set to HOLD for an active unicast MFS shall cause the transmitter to wait for duration of one Beacon Period before attempting to send the Segments belonging to this MFS. Furthermore, all segments sent in that transmission shall be considered to have failed. The transmitter may also refrain from sending segments from Priority Links intended to that destination and having a priority lower that the priority of MFS for which the HOLD was received. Reception of multiple MFS Responses indicating HOLD for connection-based stream may cause the transmitter to terminate the Connection.

Successful delivery of the oldest pending segment in the MAC Frame Stream shall cause the transmitter to update the MinTxSSN to the SSN of the next oldest pending SSN.

The transmitter may declare a MAC Frame Stream as stale and release it. Such conditions can occur under poor channel conditions, network congestion, and resource re-allocation within the transmitter. Under such conditions, transmitters should transition to the TX_RELEASE state.

For broadcast/multicast Streams, the transmitter shall set the MFSCmd to NOP. When partial ARQ is used, the transmitter should retransmit any PBs that were not properly received (as indicated in the SACK) by the multicast proxy. The transmitter shall wait for at least 1 second of inactivity (i.e., at least 1 second has passed since the transmitter sent an MPDU with Segments from the MAC Frame Stream) before releasing a broadcast/multicast Stream.

Receive Buffer Management

Receivers shall be capable of simultaneous reassembling segments from multiple MAC Frame Streams. For each reassembly stream, the receiver shall track the Minimum Receive Segment Sequence Number (MinRxSSN) and the Maximum Receive Segment Sequence Number (MaxRxSSN). MinRxSSN indicates the SSN of the oldest expected Segment. MaxRxSSN is the SSN of the most recent segment that can be received. The receive window size of the reassembly buffer is the difference between the MaxRxSSN and the MinRxSSN plus one.

A finite state machine describing the operation of the unicast MFS in the receiver is shown in Figure 519.

Note: The MFS in the receiver is complicated by the processing latencies within the PHY. In particular:

There might not be time to complete the entire reassembly and delivery processes for all received segments before the corresponding SACK must be transmitted. The receiver design must update the MFS state and the MFSRsp field prior to transmission of the SACK.

The transmitter might not be capable of processing the contents of the SACK (including the MFSRsp fields) and updating the MFSCmd field prior to transmission of a subsequent SOF. The receiver design must accommodate this latency (the FSM in Figure 519 accommodates this latency).

Figure 519: Receive MAC Frame Stream FSM

The receiver processes each received segment belonging to a valid MAC Frame Stream as follows:
Reception of a segment with an SSN equal to MinRxSSN shall cause the receiver to process that segment and any remaining contiguous set of segments. The MinRxSSN shall be updated to the oldest expected SSN.
Reception a segment with an SSN in the range (MinRxSSN+1, MaxRxSSN) inclusive shall cause the receiver to treat the segment as being out-of-order. A receiver may optionally associate each received out-of-order segment with an expiration time. The computation of expiration time of a segment depends on whether the segment belonging to a connection-based stream contains ATS.
The expiration time of a segment belonging to a stream that does not include an ATS in the MAC Frames shall be the sum of the segment arrival time plus the Max_Reassembly_Timer. The Max_Reassembly_Timer for connection-based streams shall be set to the latency negotiated during connection setup minus the processing delays that will be incurred at the receiver. Connectionless streams shall use a Reassembly Timer set within the Max_Reassembly_Timer range.
The expiration time of a segment belonging to a stream that includes an ATS in the MAC Frames shall depend on whether an ATS field can be obtained from the corresponding segment. The ATS can be obtained from a segment if the segment contains a MAC Frame boundary of at least six octets before the end of the segment and the MFT indicates a valid MAC Frame. If an ATS can be obtained, the expiration time of the segment shall be set to the ATS plus the Max_Reassembly_Timer. Implementations may also optionally process multiple out-of-order segments to obtain the ATS. If the ATS cannot be obtained, the expiration time shall be set to the arrival time of the segment plus the Max_Reassembly_Timer.
Note: If the receiver does not implement the expiration time on out-of-order segments, the MAC Frame Stream may experience decreased performance and significantly larger segment loss under severe channel conditions.
If a segment is received with an SSN less than MinRxSSN, the segment shall be discarded.
For unicast MFS, reception of a segment with an SSN greater than the MaxRxSSN and the OPSF set to 0b0 (i.e., not the oldest segment in the transmitter queue) shall cause the receiver to drop the segment.
For broadcast/multicast MFS, reception of a segment with an SSN greater than the MaxRxSSN and the OPSF set to 0b0 shall cause the MaxRxSSN updated to the SSN of the received segment. The received segment is stored for subsequent reassembly. The MinRxSSN is updated appropriately.
Reception of an MPDU with a single segment with an SSN greater than MaxRxSSN and an OPSF set to 0b1 shall cause the receiver to set the MinRxSSN to the SSN of the received segment plus one. All pending segments with sequence numbers less than the new MinRxSSN shall be dropped.
The transmitter is responsible for ensuring that it is synchronized to the receiver with respect to the SSNs that are expected. The transmitter uses the MFSCmd fields in the SOF and the OPSF field in the PB header to accomplish this synchronization. Processing of these fields is described in Figure 518.
If an SOF is received with an MFSCmd of NOP, the receiver returns ACK in the associated MFSRsp field of the SACK.

In some cases, the receiver might not have sufficient buffer resources to continue receiving more Segments from the transmitter. This can occur when the STAs has a slow H1 interface or when the station has limited processing capabilities. Under such conditions, upon the reception of MPDUs with one or more Segments, the receiver can send a SACK with MFSRsp set to HOLD. This will cause the transmitter to refrain from sending more Segments of the MFS for one Beacon Period. Broadcast/multicast transmissions shall have the MFSCmd and MFSRsp fields always set to NOP and ACK, respectively. Further, the receiver shall release the MAC Frame Stream if no Segments belonging to the MAC Frame Stream were received for a duration of 1 second.

The receiver should ensure that all received MSDUs in a MAC Frame Stream are delivered in the order they arrived at the corresponding transmitter. This will require the receiver to store out-of-order segments until all the expected previous segments are received. Under some conditions, it is possible that the transmitter might not be able to successfully deliver some segments. If the receiver implements an expiration time on out-of-order segments, the receiver maintains a reassembly timer for each MAC Frame Stream with pending segments.

If a reassembly timer is used for streams without an ATS, it is recommended that it be set to the minimum of expiration times of at least the first 10 pending out-of-order segments.

If a reassembly timer is used for streams with an ATS, it is recommended that it be set to the minimum of the following:

Expiration of the oldest out-of-order segment for which the expiration timer is determined by means of ATS.

The minimum of expiration times of at least the first 10 pending out-of-order segments.

Expiration of the reassembly timer will cause the receiver to process the contiguous set of out-of-order segments, starting with the oldest pending segment. MinRxSSN shall be updated to the next SSN expected and MaxRxSSN is updated based on the modified MinRxSSN and the RxWSz. If out-of-order segments are still present, a new reassembly timer is started.

The receiver stores segments as they are correctly received, combining the oldest contiguous run of segments to form the MAC Frame Stream. The oldest undelivered MAC Frame is determined by using the MAC Frame Header length information and the PB Header MAC Frame Boundary Offset information. When all of its constituent segments have been received, the MAC Frame is formed and its ICV checked. If the ICV is correct, the MAC Frame is scheduled for delivery, either immediately or at the time specified by the ATS and the CSPEC for the stream. When all of the MAC Frames associated with a segment have been delivered, the segment may be discarded.

Communication between Associated but Unauthenticated STAs

Communication between Associated but Unauthenticated STAs refers to communication between a pair of STAs that are associated with the same AVLN and at least one of these STAs is not authenticated. Association and authentication status are known to associated STAs from the TEI Map information provided by the CCo. Communications between Associated but Unauthenticated STAs is similar to that between associated and authenticated STAs (refer to Section 5.4.1), with the following differences.

Data MSDUs shall not be exchanged between STAs that are associated but not authenticated with the same AVLN. Further, the management messages that can be exchanged shall be limited to the following:

CC_ASSOC
CC_LEAVE
CC_WHO_RU
CC_SET_TEI_MAP
CC_RELAY
PH_PROXY_APPOINT
CC_HFID
CM_HFID
CM_ENCRYPTED_PAYLOAD
CM_CHAN_EST
CM_TM_UPDATE
CM_SET_KEY
CM_GET_KEY
CM_STA_CAP
CM_MME_ERROR.IND
Vendor-specific MMEs
CM_SLAC_PARM
CM_START_ATTEN_CHAR
CM_ATTN_CHAR
CM_PKCS_CERT
CM_MNBC_SOUND
CM_VALIDATE
CM_SLAC MATCH
CM_SLAC_USER_DATA
The PHY Block Body shall be unencrypted and EKS shall be set to 0b1111.
Only CSMA allocations shall be used for transmitting the MPDUs.
Broadcast/multicast transmissions (i.e., DTEI=0xFF or MCF=1) should not be sent.
When an Associated but Unauthenticated STA becomes Authenticated, the STA shall continue to use any existing MAC Frame Streams. However, all subsequent transmissions to associated and authenticated STAs shall have the PHY Block Body encrypted using the NEK.
For example, consider an associated but unauthenticated STA having three Segments {S1, S2, S3} in its MAC Frame Stream. At this point the STA received a transmit opportunity and was able to successfully transmit Segments S1 and S3. If the STA gets authenticated before the next transmission opportunity for the pending Segment (S2), the STA should send Segment S2 encrypted using the NEK. The STA can continue to use this MAC Frame Stream for transmitting any new Segments that needs to be transmitted. Receivers should infer the authentication of the STA based on the PHY Block encryption and continue to properly reassemble the received Segments.
Communication between STAs Not Associated with the Same AVLN
There are several instances where STA(s) that are not associated with the same AVLN or are not associated with any AVLN need to communicate with each other. A few instances where such communication is needed between Unassociated STAs are as follows:

Exchange of CC_ASSOC.REQ/CNF between a new STA and a CCo.
Exchange of CM_SC_JOIN.REQ/CNF between STAs as part of distributing the NMK using the Unicast Key Exchange mechanism.
Exchange of management messages between CCo's as part of Neighbor Network Coordination.
Data MSDUs shall not be exchanged between STAs that are not associated with the same AVLN. Further, the management messages that can be exchanged shall be limited to the following:
CM_UNASSOCIATED_STA
CC_ASSOC
CC_WHO_RU
CC_RELAY
CM_HFID
CM_SC_JOIN
CM_ENCRYPTED_PAYLOAD
CM_STA_CAP
CM_MME_ERROR
CCo-to-CCo MMEs (refer to Section 11.4)
Vendor-specific MMEs
CM_SLAC_PARM
CM_START_ATTEN_CHAR
CM_ATTN_CHAR
CM_PKCS_CERT
CM_MNBC_SOUND
CM_VALIDATE
CM_SLAC MATCH
CM_SLAC_USER_DATA
Transmitters shall treat each Management Message that needs to be transmitted to STAs that are not associated with its AVLN (if any) or to STAs that are not associated with any AVLN, as belonging to a new MAC Frame Stream. Further, the following additional restrictions are imposed for these MAC Frame Streams:
The maximum length of each Management Message transmitted shall be limited to 502 octets. The payload of the Long MPDU shall be limited to one Segment and each Segment shall contain only one MAC Management Message.
The PHY Block Body shall be unencrypted and EKS shall be set to 0b1111.
The Segment Sequence Number (SSN) in the PB Header shall be set to 0x0000.
The Long MPDU payload shall be modulated using STD-ROBO_AV, MINI-ROBO_AV, or HS-ROBO_AV modulation.
In the SOF and SACK, the MAC Frame Stream Command and Response fields shall be set to NOP.
Transmissions to a STA that is associated with a different AVLN may be unicast (i.e., unicast DTEI) in instances where the {SNID, DTEI} and NTB of the destination are known. In this case, PHY clock correction based on the Network Time Base (NTB) of the destination shall be used. Further, STEI shall be set to 0x00 in the SOF.

Transmissions to an Unassociated STA or a STA whose Association status (i.e., the AVLN to which it is associated) is not known shall use Multi-Network Broadcast (MNBC) transmission mechanism (refer to Section 5.4.3.1). Multicast/broadcast transmissions to STA(s) that might not be associated with the transmitter's AVLN (if any) shall use Multi-Network Broadcast (MNBC) transmission mechanism.

Receivers shall identify transmissions from Unassociated STAs based on either the STEI set to 0x00 or the MNBF set to 0b1. Each received Unassociated STA transmission is assembled using a new receive MAC Frame Stream. Duplicate rejection cannot be achieved for Management Messages received from Unassociated STAs. Processing of such Management Messages should be designed to gracefully handle duplicate Management Messages.

Multi-Network Broadcast

Certain Management Messages require reception by all stations including stations that are not associated with any AVLN and stations associated with other AVLNs. Such transmissions shall use the Multi-Network Broadcast (MNBC) transmission mechanism.

Each Multi-Network Broadcast (MNBC) transmission shall have an RTS/CTS exchange before the Long MPDU carrying Management message is transmitted. RTS/CTS shall notify the receiving stations to apply the correct PHY Receive Clock Correction for the Long MPDU that follows based on the network identified by the SNID in the RTS. If a broadcast/multicast proxy station is not available, a CTS is not required to transmit the MPDU following the RTS (refer to Section 5.4.8.3). The Multi-Network Broadcast Flag (MNBF) in the SOF, RTS, and CTS indicates the MPDU is a broadcast to all stations regardless of the SNID or network association. All stations shall attempt to decode any MPDU when MNBF is set to 0b1.

To communicate to STAs in or tracking a non-coordinating neighboring network, Management Messages transmitted using MNBC transmission may be sent in both AV-Only mode as well as in Hybrid mode. This will enable STAs in AV-only mode as well as in Hybrid mode to properly detect the MME. MNBC transmissions shall be transmitted only during the Shared CSMA region of the AVLNs being tracked. Further, transmissions shall use the CSMA/CA channel access mechanism (refer to Section 5.4.3.1). If there are multiple groups of non-coordinating AVLNs, the Management Message may be transmitted in the Shared CSMA region of each group.

It is important to note that proper execution of the CSMA/CA channel access mechanism requires the STA to perform virtual carrier sense in the mode of the Shared CSMA region (i.e., AV-only or Hybrid mode) of the AVLN(s) being tracked. Thus, the STA that is transmitting the MNBC shall execute the CSMA/CA channel access mechanism in the mode of the AVLN before sending the MNBC. The RTS, CTS, SOF and SACK of the MNBC transmission can all be sent in AV-Only mode or in Hybrid mode. Note that the STA must contend separately for the AV-only mode transmission and the Hybrid mode transmission of the MNBC Management Message.

Note that a STA might not be able to send a Multi-Network Broadcast transmission until it hears an AVLN or it becomes a CCo or an Unassociated CCo. A request to send a multi-network broadcast transmission under such conditions may cause the transmitter to drop the request.

Figure 520 shows an example of the Multi-Network Broadcast transmission mechanism. In this example, STA1 is tracking the PHY Clock of SNID1 and transmits an MNBC transmission. The MNBF is set to 0b1 and the SNID is set to SNID1 in RTS, CTS and SOF. The Long MPDU is

transmitted using the PHY Clock Correction based on SNID1. Consider a receiving STA, STA2, that is tracking the PHY Clock of SNID2. Subsequent to reception of the RTS, it will determine that this is an MNBC based on the MNBF. The receiver then configures itself to receive the following Long MPDU using the PHY Clock correction of SNID1. This will enhance the reliability of the reception of the Long MPDU Payload. Subsequent to the reception of the Long MPDU, STA2 will revert to using the PHY Clock correction of SNID2.

Figure 520: Illustration of Multi-Network Broadcast Transmission

Summary of the MAC Frame Streams at STA

This section summarizes the MAC Frame Streams that can be present at each STA depending on the association and authentication status with an AVLN. The exact number of MAC Frame Streams instantiated by a STA at any time will be a subset of the list provided in this section.

MAC Frame Streams for a STA That is Not Associated with Any AVLN

Transmit MAC Frame Streams

Each Management Message that needs to be transmitted (i.e., each Unassociated STA transmission) will have a separate MAC Frame Stream (refer to Section 5.4.3).

Receive MAC Frame Streams

Each Management Message that is received from any Unassociated STA and is currently being reassembled (i.e., the MME is being extracted from the Segment) will have a separate MAC Frame Stream (refer to Section 5.4.3).

MAC Frame Streams for STA That is Associated but Not Authenticated with an AVLN

Transmit MAC Frame Streams

For each STA that is associated with its AVLN (irrespective of whether it is authenticated or not), a single Management MAC Frame Stream will be present (refer to Section 5.4.2).

Each Management Message that needs to be transmitted to an Unassociated STA(s) will have its own MAC Frame Stream (refer to Section 5.4.3).

Receive MAC Frame Streams

For each STA that is associated with its AVLN, a single Management MAC Frame Stream will be present (refer to Section 5.4.2).

Each Management Message that is received from any Unassociated STA and is currently being reassembled (i.e., extracting the MME from the Segment) will have its own MAC Frame Stream (refer to Section 5.4.3).

MAC Frame Streams for a STA That is Associated and Authenticated with an AVLN

Transmit MAC Frame Streams

For Associated and Authenticated STAs (refer to Section 5.4.1):

For each STA that is associated and authenticated with its AVLN, the following MAC Frame Streams may be present:

A single Management MAC Frame Stream

Four Data MAC Frame Streams for each of the four Priority Links

One Data MAC Frame Stream for each Local Link or Global Link that is established with traffic originating at the STA

One broadcast MAC Frame Stream for all Management Messages that need to be transmitted to all

Associated and Authenticated STAs.
Four broadcast MAC Frame Streams for each of the four PLIDs for connectionless broadcast data that needs to be transmitted to all Associated and Authenticated STAs.
One broadcast Data MAC Frame Stream for each of the connection based multicast/broadcast links with traffic originating at the STA.
For Associated but unauthenticated STAs
For each STA that is associated but not authenticated with its AVLN, a single Management MAC Frame Stream will be present (refer to Section 5.4.2).
For Unassociated STAs
Each Management Message that needs to be transmitted to an Unassociated STA(s) will have its own MAC Frame Stream (refer to Section 5.4.3).
Receive MAC Frame Streams
For Associated and Authenticated STAs
For each STA that is associated and authenticated with its AVLN, the following MAC Frame Streams may be present:
A single Management MAC Frame Stream.
Four Data MAC Frame Streams for each of the four Priority Links.
One Data MAC Frame Stream for each Local Link or Global Link that is established with traffic terminating at the STA.
One broadcast MAC Frame Stream for all Management Messages that are broadcasted from each STA in the AVLN.
Four broadcast MAC Frame Streams for each of the four PLIDs for connection-less broadcast data that are transmitted from each STA in the AVLN.
One broadcast Data MAC Frame Stream for each of the connection based multicast/broadcast links with traffic terminating at the STA.
For Associated but Unauthenticated STAs
For each STA that is associated but not authenticated with its AVLN, a single Management MAC Frame Stream will be present (refer to Section 5.4.2).
For Unassociated STAs
Each Management Message that is received from any Unassociated STA and is currently being reassembled (i.e., the MME is being extracted from the Segment) will have its own MAC Frame Stream (refer to Section 5.4.3).
Data Encryption
As with HomePlug AV, encryption in HomePlug GREEN PHY STAs is performed independently on each PBB (padded segment). Once a segment has been formed for transmission, it will always occupy a single PBB by itself. It may require different padding and length fields on each retransmission, and it shall be re-encrypted on each retransmission.
Section 13.4 describes the test vectors that are provided with this specification. It should eliminate any confusion about bit ordering, initialization vectors, etc.
Encryption Method
As with HomePlug AV, GREEN PHY STAs shall use 128-bit AES-based encryption in Cipher Block Chaining (CBC) Mode as the default encryption. The encryption algorithm shall be

implemented in accordance with with reference [2] Federal Information Processing Standards Publication 197 and reference [3] in Section 1.1. Also, refer to Section 7.10.6.

PHY Block Body Encryption Bit Order

The first in time bit of the PHY Block Body (LSB of octet 0) shall correspond to bit number 0 of the AES encoder defined in Section 3.1 of reference [2] Federal Information Processing Standards Publication 197.

Initialization Vector Generation and Bit Order

The Initialization Vector is generated from the Start of Frame Delimiter, the MPDU PB count, and from the PHY Block Header. Table 53 shows the format of the Initialization Vector. The LSB of octet number 0 of the IV shall correspond to bit number 0 of the AES encoder defined in Section 3.1 of reference [2] Federal Information Processing Standards Publication 197.

Table 53: Initialization Vector Format

Field	Octet Number	Definition
IV_SOF	0 – 11	IV fields from Start-of-Frame delimiter
PBC	12	PB Count
IV_PBH	13-15	IV fields from PHY Block Header

IV Fields from Start-of-Frame Delimiter (IV_SOF)

IV_SOF is the same as the 12-octet of the Start-of-Frame variant field (Section 4.4.1.5.2) of the MPDU in which the segment is being transmitted. The least-significant octet of the SOF variant field shall be the least-significant octet of IV_SOF, and so on.

PB Count (PBC)

PB Count (PBC) is an 8-bit field that contains the relative location of the PB in an MPDU. The first PB transmitted in the MPDU shall have a PB count of 0x00, the second PB transmitted in the MPDU shall have a PB count of 0x01, and so on.

The PB count shall be incremented for each PB in the MPDU, including empty PBs. As described in Section 4.4.2.1.1.3, empty PBs might or might not be encrypted (but the PB count is always incremented).

IV Fields from PHY Block Header (IV_PBH)

IV_PBH is the same as the three least-significant octets of the corresponding PB Header. The least-significant octet of the PB Header shall be the least-significant octet of IV_PBH.

PHY Block Body Encryption Key Bit Order

For the encryption of the PHY Block Body, the LSB of the first octet of the encryption key shall correspond to bit number 0 of the AES encoder defined in Section 3.1 of reference [2] Federal Information Processing Standards Publication 197.

MPDU Bursting

MPDU bursting is the process in which a station transmits multiple Long MPDUs in a Burst (without relinquishing the medium) before soliciting a response. A Burst may include multiple Data MPDUs or multiple Sound MPDUs. A Burst shall not contain a mix of Sound MPDUs and Data MPDUs.

When a Burst of Data MPDUs is transmitted, the SACK transmitted at the end of the MPDU

Burst contains the reception status of all the PBs in the Burst. When a Burst of Sound MPDUs is transmitted, the Sound ACK that is transmitted at the end of the MPDU Burst will indicate the reception status of the Sound MPDUs. Long MPDUs in a Burst are separated by BIFS. Since MPDU Bursts only require one response (and the time spent waiting for response and the subsequent interframe spacing) for a group of MPDUs, they provide higher MAC efficiency. Significant improvement in the performance can be obtained for high data rate streams, such as High Definition Television (HDTV) and Standard Definition Television (SDTV) streams, by using MPDU bursting. MPDU bursting is optional for the transmitter and mandatory for the receiver.

Figure 521 shows an example of MPDU bursting with three Data MPDUs in a Burst. The MPDUCnt field in the SOF delimiter (refer to Section 4.4.1.5.2.15) indicates the number of MPDUs that follow the current MPDU in the Burst. The first, second, and third (or last) MPDUs are indicated by MPDUCnt values of 2, 1, and 0, respectively.

Long MPDUs are categorized as Regular MPDUs or Burst MPDUs, depending on whether a response is expected at the end of their transmission. Long MPDUs that are followed by a response are referred to as Regular MPDUs and are indicated by setting the MPDUCnt in their delimiter to 0b00. The last Long MPDU in an MPDU Burst and Long MPDUs in all non-burst transmissions belong to this category. Long MPDUs that are followed by one or more long MPDUs are referred to as Burst MPDUs. In this case, MPDUCnt indicates the number of Long MPDUs to follow.

When a Data MPDU with a non-zero MPDUCnt field is received by a destination, the receiver shall refrain from generating a response and shall store the corresponding SACK information locally. This process continues until the last MPDU in the burst (indicated by MPDUCnt = 0b00) is received. Upon the reception of the last MPDU, the receiver shall aggregate all the SACK information and transmit it in a single SACK MPDU. The SACK Type (SACKT) field, along with the SACK Information (SACKI) field, contains the reception status of PBs in each of the MPDU.

If the transmitter fails to receive a SACK at the end of an MPDU Burst, it may send a SOF delimiter with Request SACK Retransmission (RSR) set to 0b1. This will cause the receiver to transmit (or retransmit) the SACK information, as described in Section 5.4.8.1.1.

When a Sound MPDU with a non-zero MPDUCnt field is received by the destination, the receiver shall refrain from generating a Sound ACK and shall wait for the subsequent Sound MPDU. This process continues until the last MPDU in the Burst (indicated by MPDUCnt = 0b00) is received. Upon reception of the last MPDU, the receiver shall respond with a Sound ACK. In contrast to SACK, Sound ACK only indicates the proper reception of the last Sound MPDU in the Burst and does not carry an indication on the reception status of other Sound MPDUs in the Burst.

> During the CP, the maximum duration of a MPDU Burst, including the response time and the subsequent Contention Interframe Spacing (CIFS_AV), shall be less than or equal to 5000 μsec. Furthermore, the maximum FL_AV that can be used in CP shall be restricted to 2501.12 μsec. An MPDU Burst with up to 4 MPDUs can be transmitted in CP, as long as the maximum duration of the MPDU Burst is less than 5000 μsec.

All Burst MPDUs shall use at least two OFDM Symbols for transmitting the MPDU Payload.

This restriction is necessary to ensure that the receiver has sufficient time to interpret the Frame Control and start searching for the next MPDU in the Burst.

Figure 521: Example of MPDU Bursting

MPDU Bursting for GREEN PHY

A station implementing only Green PHY shall not initiate MPDU bursting. However, a station implementing Green PHY shall accept the reception of MPDU Bursts that are transmitted from other stations that implement this feature.

Bidirectional Bursting

HomePlug AV stations may optionally support bidirectional bursting. This procedure allows a transmitting station to allocate part of a burst to a receiving station, so the receiving station can send data to the transmitting station over their "reverse channel."

The receiving station initiates bidirectional bursting using the Request Reverse Transmission Flag (RRTF) and Request Reverse Transmission Length (RRTL) fields in the Frame Control of the SACK. The RRTL field specifies the minimum required frame length for a Reverse SOF MPDU in the reverse direction.

Upon receiving the request, the original transmitter decides whether the request will be honored and its duration; the original transmitter should not grant a Maximum Reverse Transmission Frame Length for less than the duration requested by the original receiver. The original transmitting station grants the reverse transmission request by setting the BBF and the MRTFL field in the SOF. The MRTFL field includes payload and subsequent RIFS_AV, but not the Reverse Start Of Frame (RSOF) delimiter.

Figure 522 shows the bidirectional burst mechanism. When Dev B determines that it requires reverse direction transmission, it sets the RRTF and RRTL fields in the SACK or RSOF. This is set until Dev A responds with a grant for reverse transmission (by setting the BBF flag set to 0b1 and indicating the maximum duration of reverse transmission in MRTFL) or until there is no longer a need to request a transmission in the reverse direction.

Figure 522: Bidirectional Burst Mechanism

Figure 523 shows the various inter-frame spaces during a bidirectional burst. Interframe spacing of RIFS_AV shall always follow a Reverse SOF. The FL_AV field in Reverse SOF will include the Reverse SOF payload and the subsequent RIFS_AV.

Figure 523: Inter-frame Spacing during Bidirectional Burst

The bidirectional burst procedure is subject to the following restrictions:

Bursting can only be done in the forward direction. Reverse transmissions cannot burst.

Reverse transmissions shall restrict its transmission to the time allocated by the forward stream.

A SOF delimiter has only 4 bits for BM_SACKI. In case a Reverse SOF is transmitted with more than 4 PBs and the original transmitter receives a mixture of good and bad PBs, it shall send a SACK delimiter. This enables the original transmitter to properly acknowledge all the PBs in the Reverse SOF, however, this will also end the bidirectional burst.

A bidirectional burst sequence shall always start with a transmission in the forward direction.

Additional restrictions on bidirectional bursts are dependent on whether the burst is occurring in a CP allocation, or a CFP allocation.
Bidirectional bursts in CP allocations must end with a SACK. The SACK can be sent in either direction.
Bidirectional bursts in CFP allocations may end with a SACK or a Reverse SOF. All STAs supporting bidirectional bursts must support ending of a CFP allocation with a SACK (in either direction). This is the default mode of operation. Optionally, STAs supporting bidirectional bursts may also support ending of a CFP allocation with a Reverse SOF. The use of this option shall be communicated during connection setup as described in Section 5.4.7.2. When a bidirectional burst in a CFP allocation ends with a Reverse SOF, a minimum interframe space of RIFS_AV shall be present between the end of Reverse SOF payload and the end of CFP allocation. The optional support for CFP bidirectional bursts ending with Reverse SOF enables STAs to improve the efficiency of VoIP and other low data rate applications.
Bidirectional Bursting during CSMA
Figure 524 shows the usage of bi-directional bursts during CSMA. When Dev A gains access to the channel, it can set the BBF field in the SOF to indicate that the channel will not be relinquished after the first transmission. Dev B, by sending a Reverse SOF indicates to the other devices that they cannot access the channel following this transmission. Dev A can immediately follow the receipt of Reverse SOF with the transmission of another MPDU. If Dev B continues to request a bidirectional burst (as indicated by the RRTF and RRTL fields) and Dev A has no data to send, it may continue the burst by sending a short SOF with the BBF field set to one. Similarly, if Dev A has granted time for a reverse transmission and Dev B does not have any data to transmit, Dev B should continue the burst by sending a short RSOF. The sequence of bidirectional bursts shall be terminated with either Dev A or Dev B transmitting a SACK. Dev A may also instruct Dev B to terminate the burst by setting the BBF field to zero in the SOF. If either device suspects a collision (all received PBs bad), it should terminate the sequence of bidirectional burst with a SACK. Likewise, if no frame control is received, the sending device should assume a collision has occurred.
During a bidirectional burst, listening stations (i.e. stations not participating in the bidirectional burst) shall defer to the two stations participating in the bidirectional burst until the end of the burst. Upon receiving a SOF with MPDUCnt set to 0b00 and BBF set to 0b0, the third-party stations would infer that the bi-directional burst is ending and they would start priority contention at the end of the expected SACK transmission. If they receive an SOF with MPDUCnt set to 0b00 and BBF set to 0b1, they would start looking for a reverse transmission. If they receive a RSOF, they would continue to look for a SOF. If they receive a SACK at any time, they will start priority contention immediately.

Figure 524: Bidirectional Bursts during CSMA
The bidirectional burst procedure during CSMA is subject to the following additional restriction: The total duration of the bidirectional burst, including the final SACK and subsequent Contention Interframe Spacing (CIFS_AV), shall not exceed 5000 μsec.
RTS/CTS and Bidirectional Bursts

Bidirectional bursts may be used with RTS/CTS during CSMA.
When using RTS/CTS, the following additional restrictions apply to bidirectional bursts:
The total duration of the bidirectional burst including the final SACK and subsequent Contention Interfame Spacing (CIFS_AV) shall not exceed the Duration (DUR) specified in the CTS Frame Control.
The bidirectional burst must end with SOF with the BBF field set to 0b0 or RSOF MPDU, followed by a SACK in opposite direction. (When RTS/CTS is not used, the SOF with the BBF field set to 0b0 is not strictly required.)
Connections and Links during Bidirectional Bursts
The Reverse SOF FC (the reverse direction) does not contain an LID field, instead the LID is implied/derived by the LID in the preceding Long SOF FC (the forward direction).
For connectionless priority links (i.e., LIDs 0 to 3), the PLID of the data stream in the payload of the Reverse SOF shall be the same as the PLID contained in the corresponding SOF. Optionally, management messages at any priority are also allowed in the Reverse SOF.
For connections with a single forward link or a single reverse link, only management message at any priority shall be transmitted in the payload of the Reverse SOF.
For bidirectional connections, the LID of the data stream in the reverse direction shall be the LID of the other link in the connection. Optionally, management messages at any priority are also allowed in the payload of the Reverse SOF.
For bidirectional connections with two local links, L-1 and L-2, if traffic from link L-2 is required to be transmitted as part of Reverse SOF of a bidirectional burst initiated by L-1, the CSPEC shall indicate it by including the "Bidirectional Burst" CM-to-CM QoS and MAC Parameter (QMP, refer to Table 79) in the QMPs of Link-2. If L-1 is a Global Link, this QMP can also be used to indicate whether the bidirectional burst in CFP may end with a Reverse SOF. If the receiver does not support any of these options, it rejects the connection setup request. If the receiver accepts the connection and L-1 is a Global Link, "Bidirectional Burst" QMP (refer to Table 710) shall be included in the CM-to-CCo QMP of L-1 to indicate to the CCo that Bidirectional Bursting is intended to be used for L-2 traffic during the CFP. In this case, the "Surplus Bandwidth" QMP should consider the additional bandwidth required. Further, both Forward Bit Loading Estimates and Reverse Bit Loading Estimates shall be included in the CC_LINK_NEW.REQ.
If the connection setup is successful, only data belonging to the negotiated local link and optionally management messages can be sent in the reverse direction during bidirectional bursts.
Encryption of RSOF Payload
Reverse SOF FC does not contain an Encryption Key Select (EKS) field. The EKS of the Encryption Key used in encrypting the Reverse SOF payload shall be the same as the EKS contained in the preceding SOF FC.
Bidirectional Bursting for GREEN PHY
A station implementing only GREEN PHY shall not support bidirectional bursting. Therefore, a HomePlug GREEN PHY Station shall do the following to facilitate this:

- A HomePlug GREEN PHY transmitting station shall set the Bidirectional Burst Flag (BBF) to 0b0 in the Frame Control of the SOF MPDUs.
- A HomePlug GREEN PHY transmitting station shall set the MFSRspMgmt and

MFSRspData fields in the Frame Control of the SOF MPDUs to 0b00.

- A HomePlug GREEN PHY transmitting station shall set the BM_SACKI field in the frame control of the SOF MPDUs to 0b1111.
- A HomePlug GREEN PHY receiving station shall set the Request Reverse Transmission Flag (RRTF) in the SACK frame control to 0b0 indicating that there is no request for reverse transmission.

A HomePlug GREEN PHY Station does not use RSOF Frame Control. However, a HomePlug GREEN PHY station is required to defer during bidirectional bursting between HomePlug AV stations during CSMA/CA allocations.

Automatic Repeat reQuest (ARQ)

As with HomePlug AV, HomePlug GREEN PHY uses Selective Repeat Automatic Repeat reQuest at the segment level. Segments are sent as PBBs, each encrypted independently. Each PB is contained in its own FEC Block. An MPDU contains a variable number of FEC blocks, depending on the data rate and payload duration, and up to four MPDUs may be sent as a burst with a single SACK in response.

Selective ACK (SACK)

The SACK format provides support for up to four SACK Type (SACKT) fields, one per MPDU in a burst within the SACK delimiter. The SACKT and SACKI fields indicate whether:

All the PBs in the corresponding MPDU were received correctly.

All the PBs in the corresponding MPDU were received with errors.

The corresponding MPDU was not detected (i.e., either no Preamble was detected or a corrupt Frame Control was detected),

A mixture of good and bad PBs were found in the corresponding MPDU. In this case, the reception status of the PBs can be indicated using one bit per PB, one bit for a pair of PBs, or as a compressed version (refer to Section 4.4.1.5.3.8.2).

The receiver shall also use the MPDUCnt field of the MPDU header to detect entire missing MPDUs in a burst. These shall be signaled in the SACK using Uniform SACKT, with SACKI indicating that MPDU was not received. If no response is received when one is expected, or if the Frame Check Sequence (FCCS) of the SACK is incorrect, the sender shall assume there was a collision and that no PBs were received correctly. The sender may request retransmission of a missing SACK.

Request SACK Retransmission

The Request SACK Retransmission function is optional for the transmitter and mandatory for the receiver. The Request SACK Retransmission function is restricted to Global Links. Local Links and Priority Links shall set the RSR field in the SOF to 0b0.

On a Global Link, when a SACK MPDU is transmitted in response to a SOF with RSR = 0b0 (i.e., when SACK retransmission is NOT requested), the receiver shall store the SACKT, SACKI fields of the SACK MPDU and the GLID, BurstCnt, and STEI fields of the SOF. This data shall be discarded by the receiver upon receipt of another SOF MPDU with the same GLID, STEI, and RSR = 0b0. This data may be discarded at other times as an implementation option (e.g., to reduce memory requirements). All receivers shall store at least one set of SACKT and SACKI fields, along with their associated GLID, BurstCnt, and STEI values for transmission in response to a

SOF with RSR=0b1. Receivers may store more than one such set.
The transmitter may request retransmission of a missing SACK by sending an SOF with RSR = 0b1 under the following conditions:
The original SOF and (missing) SACK are associated with a Global Link and carry a GLID.
It has received a valid SACK MPDU from the receiver with this GLID during a previous transmission.
It has sent three or fewer bursts with this GLID to the receiver since the last valid SACK MPDU was received from the receiver. The end of each burst is indicated by transmission of zero in the BurstCnt field of the SOF MPDU.
If the above conditions are not met, the transmitter shall not send an SOF MPDU with RSR = 0b1.
A transmitting STA that has sent three or fewer bursts to a receiver may continue to send SOF on this Global Link with RSR = 1 until a valid SACK response is received.
Note: SOF MPDUs with RSR set to 0b1 shall not carry any payload.
A transmitting STA that does not meet the conditions for sending SOF with RSR = 0b1 above may send new bursts containing payload data to the receiver (with updated BurstCnt values). It may also send SOF with RSR = 0b0.
Upon receipt of an SOF with RSR = 0b1, the receiver shall do the following:
If SACKT and SACKI data are available corresponding to the GLID, STEI, and BurstCnt fields of the SOF, the receiver shall respond with a SACK containing these SACKT and SACKI fields.
If such SACKT and SACKI data are not available, the receiver shall respond with all SACKT and SACKI fields set to indicate that SACK information is not available(i.e., SACKT = 0b11 and SACKI = 0b11).

Informative Text
The request SACK retransmission function is not affected by intervening region boundaries or intervening contention-free allocation boundaries. Therefore, if a STA fails to receive a SACK at the end of its contention-free allocation, it may send RSR=0b1 at the start of a subsequent contention-free allocation and receive the appropriate SACK response, provided it has not sent any other SOF with the same GLID and with RSR = 0b0 in the intervening intervals.
Although this function is limited to Global Links, it is not necessarily restricted to the CFP. For example, a STA that fails to receive a SACK at the end of its contention-free allocation may contend for the medium and send a SOF with RSR = 0b1 in a subsequent CSMA Region.

Request SACK Retransmission for GREEN PHY
A station implementing only GREEN PHY shall not implement Request SACK Retransmission.
As a transmitter, a HomePlug GREEN PHY Station shall not request for SACK retransmissions and therefore shall always set the Request SACK Retransmission (RSR) field in the SOF to 0b0.
Retransmission
Segments held in PBs that are believed to have been received incorrectly, by explicit designation in the SACKI field or by the absence of a correct SACK, shall be subject to retransmission. A retransmitted segment is packaged in a new PB and is retransmitted with that MPDU, which may also contain new segments and Management Message stream segments.
The number of retries for a segment is limited by the latency requirements and Packet Loss

Tolerance of its stream, and the system limit on retries.

MAC Retransmission Strategies

The MAC layer at the transmitter may implement several advanced retransmission strategies to improve performance under degraded channel conditions. These functions include:

Negotiation with the CCo for additional bandwidth allocations to support retransmission.

A modified form of Packet Bursting, where some or all of the PBs in the burst are repeated in different MPDU within the burst. In this case, the receiver must use the SSN in the PB to filter out repeated PBs. Refer to Section 5.4.6 for more information about Packet Bursting.

Repeated transmission of one or more PBs within an single MPDU. In this case, the receiver must use the SSN in the PB to filter out repeated PBs.

The transmitter may use any or all of the strategies listed above to ensure reliable data transmission. Support for these functions is mandatory in the receiver and optional in the transmitter.

Broadcast/Multicast and Partial Acknowledgement

Multicast/broadcast transmissions cannot make use of the standard ARQ mechanism because there can be more than one destination that would acknowledge the transmission. The MAC improves the information available to the transmitter through a "partial ARQ" scheme in which one station in the group serves as a proxy to provide the Response. Using this mechanism, the DTEI of the multicast or broadcast transmission is set to the TEI of the proxy station. The presence of multicast payload in the MPDU is indicated by setting the Multicast Flag (MCF) in the Frame Control. All stations that receive the transmissions with MCF set to 0b1, shall reassembly the corresponding MPDU irrespective of the DTEI. The transmitter shall use the SACK information sent by the proxy to determine whether the transmission is successful.

When no proxy station is selected, the DTEI of the multicast MPDU shall be set to 0xFF. In this case, the transmitter assumes that all transmissions are successful.

Note: Broadcast transmissions that do not include a proxy for sending the SACK will still leave the necessary gap for RIFS_AV and SACK. This choice is made to simplify the determination of subsequent transmission opportunities. It is recommended that partial acknowledgment mechanism be used whenever possible.

A proxy station need not be part of the multicast group. ROBO, High-Speed ROBO, and Mini ROBO modulation methods shall be used for multicast/broadcast transmission.

The broadcast MAC address used by a HomePlug-AV station is 0xFFFFFFFFFFFF. TEI of all 1s is used to indicate multicast/broadcast payload.

PHY Clock and Network Time Base Synchronization

The CCo shall maintain a 32-bit timer, called the Network Time Base (NTB), clocked by a 25MHz clock derived from the CCo's STA_Clk, as defined in Section 3.7.3.1. The NTB is transmitted by the CCo in the Beacon and each STA in the AVLN receiving the Beacon synchronizes to the NTB. The CCo's STA_Clk and the Network Time Base are used to:

Correct the PhyClk used for the processing of transmit and receive signals at all non-CCo STAs in the AVLN.

Announce the future Beacon position and the Schedule within the Beacon Period.

Derive the ATS and perform the jitter control function (refer to Section 6.7).

The CCo shall embed a 32-bit BTS into the Beacon Frame Control (refer to Section 4.4.1.5.1.1).

The Beacon Time Stamp (BTS) is the value of the NTB at the BTT, which is defined as the time instant at which the first non-zero sample of this Beacon PPDU appears on the transmitter's analog output. The jitter of the BTS (BTS_JITTER) shall be no greater than 0.25 μsec. BTS_JITTER is due to the variations in the 25 MHz clocks and timers).

Information Text

One approach for achieving synchronization is to compute the frequency error between the CCo's STA_Clk and the STA's STA_Clk, and the offset between the corresponding time bases (i.e. the values in the 32-bit timers). When a Beacon is detected, the receiver stores the 32-bit value of its local timer at the time of reception of the beginning of the AV Preamble signal of Beacon n, denoted as $LTmr_n$. The received Beacon contains the Beacon Time Stamp, denoted as BTS_n. Propagation delay between the transmitter and receiver can be ignored; however, if it is known, it could be compensated for in the computation of the offset.

The following formulas can be used to estimate the clock frequency and timer offset errors:

$$FreqError_1 = (BTS_1 - BTS_0) / (LTmr_1 - LTmr_0)$$

$$Offset_1 = BTS_1 - LTmr_1$$

$$FreqError_n = FreqError_{n-1} + (BTS_n - BTS_{n-1}) / (LTmr_n - LTmr_{n-1}) - 1 - FreqError_{n-1}), n \geq 2$$

All stations in the AVLN shall maintain a local 32-bit timer, called the NTB_STA, which must be synchronized in frequency and absolute value to the NTB of the Central Coordinator. Synchronization is normally achieved through the reception of the Central Beacon. If the Central Beacon cannot be heard reliably, the station may synchronize to a Proxy Beacon. If neither the Central Beacon nor a Proxy Beacon can be heard reliably, the Discover Beacon of another station may be used for this function until a Proxy Beacon is established. The accuracy of NTB_STA is not explicitly specified, and implementations are free to use any synchronization method as long as all other timing specifications are met.

where:

BTT_0, BTT_1 are the BTT of any two Beacon instances, measured in μsec using a clock traceable to the same source as the source of the CCo STA_Clk.

BTS_0, BTS_1 are the values of the BTS in the corresponding Beacon FCs.

The difference between the value of the NTB and the BTT of a Beacon instance and the corresponding BTS shall be no greater than ±1250, corresponding to ±50 μsec of real time, for all Beacon instances. CCo implementations are not required to facilitate measurement of the above quantities, by exposing the value of the NTB, for example. The jitter requirement is motivated by fast frequency recovery at the STAs (see below and Section 5.5.4), and the absolute offset requirement by the distribution of a precise common clock to all nodes of the network for smoothing, and differential and absolute delay control purposes (refer to Chapter 6).

Informative Text

One approach for achieving synchronization is to compute the frequency error between the CCo's STA_Clk and the STA's STA_Clk, and the offset between the corresponding time bases (i.e. the values in the 32-bit timers). When a Beacon is detected, the receiver stores the 32-bit value of its local timer at the time of reception of the beginning of the AV Preamble signal of Beacon n, denoted as $LTmr_n$. The received Beacon contains the Beacon Time Stamp, denoted as BTS_n. Propagation delay between the transmitter and receiver can be ignored; however, if it is known, it could be compensated for in the computation of the offset.

The following formulas can be used to estimate the clock frequency and timer offset errors:

$$FreqError_1 = (BTS_1 - BTS_0) / (LTmr_1 - LTmr_0) - 1$$

$$Offset_1 = BTS_1 - LTmr_1$$

$$FreqError_n = FreqError_{n-1} + w_f ((BTS_n - BTS_{n-1}) / (LTmr_n - LTmr_{n-1}) - 1 - FreqError_{n-1}), n \geq 2$$

$$Offset_n = Offset_{n-1} + FreqError_n (LTmr_n - LTmr_{n-1}) + w_o ((BTS_n - LTmr_n) - (Offset_{n-1} - FreqError_n (BTS_n - LTmr_{n-1}))), n \geq 2$$

Note: w_o ***and*** w_f ***are weighting constants of the form*** $½^k$***, where*** k ***is a positive integer. Larger values of*** k ***provide better filtering of the uncertainty between each*** BTS_n ***and*** $LTmr_n$ ***pair caused by factors such as preamble detection jitter. Larger values of*** k ***result in a longer period of time to achieve convergence to the correct estimate of frequency error. When tracking a Beacon, it is recommended that a small value of*** k ***be used for the first samples and increased to the ultimate value.***

Once $FreqError_n$***, and*** $Offset_n$ ***are known to be accurate, the relationship between the Network Time Base estimate (NTB_STA$_i$) and the local timer at instance*** i ***is:***

$$NTB_STA_i = LTmr_i + Offset_n + FreqError_n (LTmr_i - LTmr_n)$$

$$LTmr_i = (NTB_STA_i + FreqError_n LTmr_n - Offset_n) / (1 + FreqError_n)$$

where $Offset_n$***,*** $FreqError_n$***, and*** $LTmr_n$ ***are the values computed from the most recently received Beacon.***

BTS in Proxy Beacons

Proxy Stations shall insert a BTS in the Proxy Beacon they transmit (refer to Section 4.4.1.5.1.1). The BTS jitter of a Proxy Beacon, defined in a fashion analogous to that of the CCo, shall be no greater than 0.5 µsec.

The error in the BTS of the Proxy Beacon (BTS_PxErr) shall be less than 2.5 µsec. The

BTS_PxErr is defined as:

where:
BRT_CCo is the Beacon Receive Time of the Central Beacon, defined as the time instant at which the first non-zero sample of the Central Beacon PPDU appears on the line at the PCo receiver.
BTT_PCo is the BTT of the Proxy Beacon.
BTS_CCo and BTS_PCo are the BTSs of the CCo and PCo Beacons, respectively.
All times are measured in μsec from an arbitrary reference point.
The maximum is taken over all paired (i.e., within the same Beacon Period j) Central and Proxy Beacon instances.

BTS in Discover Beacons

When STAs transmit a Discover Beacon, they must insert a BTS in the Beacon (refer to Section 4.4.1.5.1.1). The BTS jitter of a Discover Beacon, defined in a fashion analogous to the one for the CCo, shall be no greater than 0.5 μsec. The error in the BTS of the Discover Beacon, defined in a fashion analogous to the Proxy Beacon BTS error, shall be less than 2.5 μsec.

Arrival Time Stamp for MSDU Jitter and Delay Control

Each STA shall use its NTB_STA in generating the ATS (Arrival Time Stamp). The ATS is the value of the NTB or NTB_STA when the first octet of the MSDU arrives at the CL SAP of a station, and is used to provide jitter-control and smoothing functions (refer to Section 6.7.3) across the HomePlug AVLN.

PHY Clock Correction

The NTB should be used to synchronize the PHY signaling between stations to eliminate Inter-Carrier Interference without the need for high accuracy clocks. All stations shall adjust their PhyClk based on the current estimate of the CCo's STA_Clk frequency for all communications within a network (refer to Section 3.7.3.1). Following correction, the PhyClk frequency of a non-CCo STA, measured from the STA's transmitted signal, must be within ±1 ppm of the frequency of the CCo's PHY clock. This requirement shall be met under a constant-gain channel with SNR of at least 15 dB at the receiver.

PHY Clock Correction When Participating in More Than One Network

When a station associates with an additional network, the station must select which network PHY Clock Correction to apply for reception during the CP. The station must set DCPPCF to 0b1 in the SOF for all transmissions to stations in other networks. Refer to Section 4.4.1.5.2.19. Stations that use a different PHY Receive Clock Correction during the CP are also required to send a CC_DCPPC.IND message to the CCo. Refer to Section 4.4.3.10 and Section 11.2.50.

Upon reception of an RTS, the correct PHY Receive Clock Correction for the network identified by the SNID in the RTS should be applied for the reception of the following PPDU if the CCo for the SNID can be heard. A station may apply the correct Receive Clock Correction if it cannot hear the CCo but can hear a PCo or a Discover Beacon for that network.

Allocation Boundaries

The Beacon Payload contains information on the Contention Free and CSMA allocations. The Start Time and/or End Time of these allocations are based on the CCo's STA_Clk and are with respect to the Beacon Period Start Time. Not considering propagation delays, stations shall be capable of

tracking the allocation boundaries, with an accuracy of ±2 sec.
For Beacon Periods in which the CCo's Beacon is properly detected, the Beacon Period Start Time (BPST) should be obtained from the observed location of the Beacon. Stations may also infer the location of the BPST based on the BTO received in earlier Beacons. In this case, stations should use their current estimate of the CCo's STA_Clk frequency to determine the BPST.
In some cases, the end time of the last allocation in a Beacon Period can run into the next Beacon Period. Such cases occur due to the asynchronous nature of the Beacon position's movement to track the AC line cycle and the persistence of the allocations. The CCo should ensure that such cases are minimized. Stations shall stop transmissions earlier than the point of time indicated by the end time if it exceeds the next BPST.

Interframe Spacing

The interframe spacing varies for each region type within the Beacon Period. Figure 525 shows the interframe spacing for the Beacon Region and for the CSMA Region.
An interval of at least the Beacon-to-Beacon Interframe Spacing (B2BIFS) shall exist between the end of the last PPDU (of the last region) in the previous Beacon Period and the start of the next Beacon Region.
The Beacon Region shall be an integer number of Beacon Slots long. Each Beacon Slot shall include the length of the Beacon PPDU and an associated B2BIFS. As shown in the figure, the B2BIFS occurs after each Beacon PPDU.
Within a Beacon Period, an interval of at least the Allocation Interframe Spacing (AIFS) shall exist between the end of the last PPDU in a region and the start of the next region. The only exception to this rule is when a CSMA Region is followed by Reserved Region that starts with CSMA/CA Allocation (either persistent or non-persistent). In this case, the CSMA Region and the CSMA/CA Allocation are treated as a single, contiguous allocation and no Interframe spacing exists between them.
Note: The length of the Beacon PPDU is a function of the number of carriers in the active Tone Mask (refer to Section 3.6.7) and the number of Symbols used to encode the Frame Control Information (refer to Section 3.2.1).

Figure 525: Beacon and CSMA Region Interframe Spacing

Interframe spacing in the Reserved Region is shown in Figure 526. The STA transmitting in a contention-free allocation may start its transmission on the media immediately at the start of its allocation. The time between the end of a SOF PPDU and the corresponding SACK PPDU is the RIFS_AV. The time between the end of the SACK PPDU and a subsequent SOF PPDU is also CFIFS.
A minimum interval of AIFS must remain from the last PPDU (typically a SACK) and the end of each allocation in the Reserved Region. The only exception to this rule is when a Persistent CSMA/CA Allocation is followed by a non-Persistent CSMA/CA allocation. In this case, the Persistent CSMA allocation and the non-Persistent CSMA/CA allocation are treated as a single, contiguous allocation and no Interframe spacing exists between them.
RIFS_AV depends on the Tone Map used for modulating the MPDU Payload, as well the number of OFDM Symbols contained in the MPDU Payload. The following rules shall be used for

determining RIFS_AV,
All MPDU transmissions using ROBO, Mini-ROBO, or High-Speed ROBO modulation shall use Response Interframe Spacing of RIFS_AV_default.
MPDU transmissions based on negotiated Tone Maps, excluding ROBO, Mini-ROBO, and High-Speed ROBO modulations have an RIFS_AV determined by the receiver and communicated to the transmitter using the CM_CHAN_EST.IND Management Message. Variable RIFS_AV is intended to provide flexibility for implementations while ensuring interoperability. The RIFS_AV_OneSym, RIFS_AV_TwoSym, and RIFS_AV_G2Sym fields in the CM_CHAN_EST.IND contains the RIFS_AV to be used when the MPDU Payload is transmitted using one, two, and greater than two OFDM Symbols, respectively (refer to Section 11.5.10). A station shall used fixed values of RIFS_AV_OneSym, RIFS_AV_TwoSym, and RIFS_AV_G2Sym for all the Tone Maps that it generates.
MPDU transmission containing a Request SACK Retransmission (refer to Section 4.4.1.5.2.15) shall use Response Interframe Spacing of RIFS_AV_default.
The interframe spacing when MPDU bursting is employed is described in Figure 527.

Figure 526: Contention-Free Interframe Spacing

Figure 527: Interframe Spacing for MPDU Bursting
Two Extended Interframe Spacings, EIFS and EIFS_AV, are defined for use during the CSMA allocations. Extended Interframe Spacings are used when the station does not have complete knowledge of the state of the medium and when priority based-preemption is in effect. The former case can occur when the errors in the received frames (due to noise, collisions, etc.) make them impossible to decode unambiguously. The latter case occurs when a competing node has signaled its intention to transmit higher priority traffic in the Priority Resolution Slots.
EIFS shall be used when the network is operating in Hybrid Mode. The duration of EIFS is the same as in the HomePlug 1.0.1 specification. EIFS_AV shall be used when network is operating in AV Only Mode. EIFS_AV is the transmission duration of maximum mandatory AV Only Long MPDU with two Frame Control symbols along with the corresponding Response and subsequent CIFS_AV (see Figure 528).

Figure 528: Extended Interframe Spacing (EIFS_AV)
Measurement of Interframe Spacing
Several Interframe spaces are defined in the specification to accommodate propagation times and processing latencies.
Interframe space between two PPDU is the interval measured on the wire between (a) the last non-zero sample at the end of the last OFDM Symbol of the transmission that initiates the interframe space and (b) the first non-zero sample at the beginning of the preamble of the transmission following the interframe space. This interval is measured at the transmitter of the preamble that begins at the end of the interframe space.
Figure 411 and Figure 529 illustrate the measurement of interface spacing for RTS-to-CTS Gap (RCG). Interframe Spacing RIFS_AV, RIFS_AV_default, BIFS, CMG, RGIFS, B2BIFS, and

AIFS are interpreted in a similar manner.
CIFS_AV is the interval measured on the wire between the last non-zero sample at the end of the SACK delimiter and start of the first Priority Resolution Slot. Note that the first sample of the Priority Resolution Symbol in a Priority Resolution Slot starts 2.56 µsec before the start of Priority Resolution Slot and ends 2.56 µsec before the end of the corresponding Priority Resolution Slot (refer to Section 3.6.5).

Figure 529: RCG Measurement

- (deliberately blank - reserved for future use – avoiding section renumbering) (GREEN PHY)
-
- Distributed Bandwidth Control for GREEN PHY

Distributed Bandwidth Control (DBC) protocol enables Green PHY stations to limit the time-on-wire consumed by their transmissions at Channel Access Priority 1, 2 and 3 (i.e., CAP1, CAP2 and CAP3).
To facilitate identification of Green PHY start-of-frame (SOF) from non-Green PHY SOF, and to distinguish between Green PHY SOFs transmitted at CAP0 from those transmitted at CAP1, CAP2 or CAPs, each SOF transmitted from a Green PHY station shall set the Pending PHY Block field in the SOF as described in Section 4.4.1.5.2.9.1),
Each Green PHY station shall execute the DBC protocol described below during GPP allocations (refer to Section 7.8.5) as well as CSMA allocations.,

- Green PHY station shall store the PPDU Type and the time (i.e., time stamp of local clock or NTB) associated with the last two Green PHY transmissions with PPB field in SOF set to 0xEF.
  - The Green PHY transmissions shall include transmissions from the current station as well as transmissions detected from other Green PHY stations. Further, transmissions from the current station shall be included irrespective of whether the transmission is successful or not. Retransmission shall also be treated as a regular transmission.
  - The PPDU types used by Green PHY stations are as follows,
    - Mini ROBO
    - ROBO with 1 PHY Block
    - High Speed ROBO with 1 PHY Blocks
    - High Speed ROBO with 2 PHY Blocks
    - High Speed ROBO with 3 PHY Blocks
- A Green PHY station with a pending MPDU shall only contend at CAP1, CAP2 or CAP3 if its Pending PPDU and the PPDUs transmitted within the last 33.33 msec does not exceed the combinations shown in Table 5-4.

Table 5-4: Allowed PPDU combinations

Count	PPDU Combination
1	One ROBO PPDU & one Mini ROBO PPDU

2	Two Mini ROBO PPDUs
3	One Mini ROBO & One High Speed ROBO with 1 PB
4	One Mini ROBO & One High Speed ROBO with 2 PB
5	Two High Speed ROBO with 1 PB
6	One High Speed ROBO with 3 PB

Informative Text
Example of decisions based on rule # 2 are as follows,

- If the Green PHY station has a ROBO MPDU with one PHY Block and if in the last 33.33msec, two Mini ROBO PPDUs with PPB = 0xEF were transmitted, then the Green PHY station cannot contend
- If the Green PHY station has a ROBO MPDU with one PHY Block and if in the last 33.33msec, only one Mini ROBO PPDU with PPB = 0xEF have been transmitted, then the Green PHY station contend
- If the Green PHY station has a High Speed ROBO with 3 PBs, and if in the last 33.33msec, one Mini ROBO PPDU with PPB = 0xEF has been transmitted, then the Green PHY station cannot contend. However, the Green PHY station may choose to send an High Speed ROBO PPDU with two PHY Blocks.

- After Power-on or upon wake-up from power save, station shall wait for 33.33msec and follow the rule # 1 and rule # 2 before transmitting a PPDU at CAP1, CAP2 or CAP3.
- Green PHY PPDUs transmitted at CAP0 are not subjected to the above rules and may transmit at anytime during the CSMA allocation. It is important to note that packet belonging to Priority Link Identifier (PLID) queues with PLID = 0x01, 0x02 and 0x03 may be transmitted by contending at CAP0.

In certain scenarios, Green PHY stations may not get their fair share of bandwidth due to the presence of higher priority HPAV traffic (e.g., when traffic from Green PHY station is at CAP1 and AV station(s) is CAP2). In such cases, it is recommended that Green PHY stations promote the priority at which PRS signaling is sent (e.g., send PRS signals at CAP3), to ensure that they get their fair share of the bandwidth.

Note 1: Green PHY stations execute the DBC protocol irrespective of whether they detected a HomePlug AV or HomePlug 1.0 station/network

Note 2: Distributed Bandwidth Control protocol only limits the total bandwidth consumed by monitoring only SOF MPDUs (i.e., MPDUs carrying data or management messages). Beacon transmissions from Green PHY stations are ignored by the DBC protocol.

Note 3: Whenever a broadcast transmission is repeated by another Green PHY station, it sets the PPB field to 0xFF. Such retransmissions will not be counted towards the 7% bandwidth limit, since only SOFs with PPB = 0xEF are considered by the Distributed Bandwidth Control protocol.

- Power Save Mode for GREEN PHY

Power Save mode enables stations to reduce their average power consumption. This section describes the mechanism used to coordinate and communicate Power Save mode information among various stations in the AVLN.

- Basic Approach

In Power Save mode stations reduce their average power consumption by periodically transitioning between Awake and Sleep states. STAs in the Awake state can transmit and receive PPDUs over the powerline. In contrast, STA in Sleep state temporarily suspend transmission and reception of PPDUs over the powerline, thus reducing the station's average power consumption.

The following terminology is used in this specification,

- Awake Window - The periodic interval of time during which a STA in Power Save mode is required to be in the Awake state. The duration of the Awake Window can range from a few milliseconds to several Beacon Periods.
- Sleep Window - The periodic interval of time during which a STA in Power Save mode may be in the Sleep state and therefore not able to transmit or receive.
- Power Save Period (PSP) - The sum of Awake Window duration and Sleep Window duration. Power Save Period is restricted to 2^k multiples of Beacon Periods (i.e.., 1 Beacon Period, 2 Beacon Periods, 4 Beacon Periods, and so on).
- Power Save Schedule (PSS) – The power save schedule for each STA in power save mode is indicated by the combination of the 4-bit Power Save Period and Awake Widow duration values. To communicate with a STA in Power Save mode, other STAs in the AVLN need to know its PSS.

CCos coordinate Power Save mode operation for all STAs in the AVLN by:

- Optionally disabling Power Save mode for the AVLN (see the description of the Stop Power Save Flag in section **4.4.3.15.4.15)**
- Responding to request from STAs to enter and exit the Power Save mode
- Collecting the PSSes for all the STAs currently in Power Save mode, and distributing this information by placing the Power Entry BENTRY information in the beacon and in management messages.

It is mandatory for CCos to support coordination of AVLN Power Save mode operation and to be capable of accepting requests from STAs to enter Power Save mode.

It is optional for a STA or CCo to support operation in the Power Save mode. It is mandatory for a STA to track the Power Save schedules of other STAs in the AVLN and to communicate with them during their Awake Windows.

Before entering Power Save mode, STA shall send CC_POWERSAVE.REQ MME to the CCo and wait for the response from CCo. CC_POWERSAVE.REQ contains the requested Power Save Schedule (PSS). In CC_POWERSAVE.REQ, the PSP in the PSS shall have a value ranging from 0x0 to 0xA.

CCo responds to CC_POWERSAVE.REQ with a CC_POWERSAVE.CNF. CC_POWERSAVE.CNF indicates whether the CCo accepted the STA's request to enter Power Save mode. Reception of a CC_POWERSAVE.CNF with Result Code set to Accept causes the STA to go into Power Save mode.

For a STA in Power Save mode, the start of the Awake Window is as follows:

- An Awake Window shall start in each Beacon Period during which the Beacon Period Count (BPCnt, contained in the Power Save BENTRY) is an integer multiple of the STA's PSP.
- If there is GREEN PHY Preferred (GPP) allocation, then the start time of the Awake Window shall be the same as the start time of the GPP allocation in the Beacon Period
- If there is no GPP allocation, then the start time of the Awake Window shall be the same as the start time of the first CSMA allocation in the Beacon Period

Note: The location of the first CSMA allocation within a Beacon Period can be obtained from the Persistent and Non-Persistent Schedule BENTRIES.

Since PSP is always a 2^k multiple of Beacon Period and Awake Window start time in a Beacon Period is aligned for all stations, there is a guaranteed overlap of Awake Windows for all stations in Power Save mode. This overlap interval can be used for transmission of information that needs to be received by all stations within the AVLN.

Figure 5-30 shows an example of Power Save Schedule of four stations {A, B, C, D}. In this example,

- Station A has PSP of 1 Beacon Period, and Awake Window duration of 2 msec. Station A is awake for 2 msec every Beacon Period, with Awake Window start time aligned with the start of the first CSMA allocation within each Beacon Period
- Station B has PSP of 2 Beacon Periods and Awake Window duration of 4 msec. Station B's 4msec Awake Window starts at the start of the first CSMA allocation in every Beacon Period where BPCnt is an integer multiple of 2 (e.g., BPCnt = 0x010, 0x012, 0x014,…)
- Station C has PSP of 4 Beacon Periods and Awake Window duration of 6 msec. Station C's 6msec Awake Window starts at the start of the first CSMA allocation in every Beacon Period where BPCnt an integer multiple of 4 (e.g., BPCnt = 0x010, 0x014,…)
- Station D has PSP of 4 Beacon Periods and Awake Window duration of 1 Beacon Period. Station D's Awake Window starts at the start of the first CSMA allocation in every Beacon Period where BPCnt an integer multiple of 4 (e.g., BPCnt = 0x010, 0x014,…)

Note that in this example, stations are always awake at the same time once every 4 Beacon Periods for a duration of 2msec.

Figure 530: Examples of Power Save Schedules

Stations in Power Save mode shall be capable of receiving frames for the entire duration of their Awake Windows. It should be noted that the precise start time of the Awake Window can vary as the Beacon Period varies (due to AC line cycle variations). STAs shall take such variations into account to ensure that STAs remain in the Awake state for the entire Awake Window.

A STA that receives during its Awake Window the start of a MPDU addressed to the STA shall remain in the Awake state beyond the duration of its Awake Window, if necessary, in order to receive the complete MPDU. STAs should periodically exit the Sleep state to receive beacons as required in order to maintain synchronization with the network.

When a STA in Power Save mode has a MPDU to transmit, it shall use the Scheduling information in the Beacon and the Power Save Schedule of the receiver(s) to determine when the

MPDU has to be transmitted. Further, if the STA starts contending within a CSMA allocation, it shall treat the medium as BUSY and shall set VCS to MaxFL_AV. If the VCS timer expires, the STA shall transition to Idle state.

A STA exiting Power Save mode shall notify the CCo by sending the CC_POWERSAVE_EXIT.REQ MME. The CCo shall acknowledge the reception of CC_POWERSAVE_EXIT.REQ with CC_POWERSAVE_EXIT.CNF. In addition, a STA that receives a beacon with the Stop Power Save Flag set to one shall immediately exit the Power Save mode. In this case the STAs is not required to send the CC_POWERSAVE_EXIT.REQ MME.

- Distribution of Power Save State information

CCo shall maintain a Power Save State Identifier (PSSI) and Power Save schedules of STAs in the AVLN. PSSI is used to identify the Power Save state of the AVLN. PSSI is incremented by one whenever a STA (including the CCo) in the AVLN enters or exits Power Save mode.

All stations in the AVLN shall maintain a local copy of the Power Save State Identifier and Power Save schedules of STAs in the AVLN. Stations shall update their local copy based on the information provided by the CCo.

CCo uses the Power Save BENTRY to announce recent changes in the Power Save Schedule of STAs (including the CCo) in the AVLN. Each tuple {TEI[n], PSS[n]} in the Power Save BENTRY indicates a single Power Save Schedule change. The tuples are in chronological order with the most recent schedule change indicated first. Note that because schedule changes are indicated (rather than simply the current schedule for STAs), multiple schedule changes for a single STA may be indicated. The CCo should repeat the changes in Power Save Schedules in multiple Beacons to increase the probability of reception by all STAs in the AVLN. The number of schedule changes indicated is implementation dependant. In some cases, CCo may not be able to indicate all changes to Power Save Schedules in the Power Save BENTRY due to the limited Beacon Size. In such case, CCo may broadcast the Power Save schedules using CC_POWERSAVE_LIST.CNF.

STAs shall update their Power Save schedules based on the Power Save BENTRY. STAs compare their local PSSI with the PSSI in the Beacon. If they are the same, then STA's already has the current set of PSSes. If the STAs PSSI is different than the PSSI in the Beacon, then STAs can use the difference between them to determine the number of changes in the Power Save schedules. If the Beacon contains all the changes, then STA can update its local PSSI and Power Save Schedules. If Beacon does not contain all the changes in the Power Save Schedule, STAs may request the CCo using CC_POWERSAVE_LIST.REQ MME.

For example, if the local PSSI is 0x22 and the PSSI in the Beacon is 0x26, then the Power Save state of four STAs in the AVLN has changed. If the Beacon contains four recent changes (i.e., TEI[1], PSS[1] … TEI[4], PSS[4]), then the STA can update its local PSSI to 0x26 and the local Power Save Schedule is updated based on the four recent changes. In this example, if the Beacon contains only two recent changes (i.e., TEI[1], PSS[1], TEI[2], PSS[2]), then the STA may request the CCo for the Power Save List using CC_POWERSAVE_LIST.REQ MME.

STAs may request CCo to provide the Power Save list any time using the CC_POWERSAVE_LIST.REQ MME. Reception of a CC_POWERSAVE_LIST.REQ MME shall cause the CCo to respond with a CC_POWERSAVE_LIST.CNF MME.

When a STA sends MPDUs to a receiver and fails to get any acknowledgment (e.g., SACK, CTS, RSOF) after multiple attempts, STAs should request the CCo to provide the Power Save List using CC_POWERSAVE_LIST.REQ to confirm that the receiver is not in Power Save mode.

- CCo Power Save

CCo of an AVLN may operate in Power Save mode. However, the following restrictions apply:

- A CCo supporting active Global Links (i.e., TDMA allocations for QoS streams) shall not operate in power save mode
- The Maximum Power Save Period of a CCo in Power Save mode shall not be greater than the shortest Power Save Period currently being used by the STAs in the AVLN. If one or more STAs in the AVLN are not in Power Save mode the CCo may operate in Power Save mode. However, in this case, the Power Save Period of the CCo shall be one beacon period (PSP = 0).

  For example, in an AVLN if there are two stations in Power Save mode with PSP of 4 Beacon Periods and 32 Beacon Periods, then the maximum allowed PSP of the CCo is 4 Beacon Periods.
- The CCo shall not operate in Power Save mode when there are HomePlug AV 1.1 station(s) in the AVLN that do not support Power Save.

The CCo shall indicate its Power Save schedule using the TPSS field in the Power Save BENTRY. PSSI shall be incremented whenever CCo enters or exits Power Save mode and the CCO's Power Save State shall be included in the list of recent changes in Power Save Schedule BENTRY (i.e., TEI[1], PSS[1] … TEI[N], PSS[N]).

The CCo shall exit Power Save mode when CCo functionality is handed over to a new station. Further, CCo shall force all STAs in the AVLN to exit the Power Save mode by setting the Stop Power Save Flag before handing over the CCo functionality.

- Handling of Broadcast/Multicast transmissions

Broadcast transmission need to be received by all STAs in the AVLN. STAs transmitting broadcast MPDUs should take into account the Power Save Schedules of the stations in the AVLN to insure reliable reception by all stations. The following approaches are recommended for transmission of broadcast MPDUs,

- Broadcast transmissions may be send as multiple Unicasts to all STAs in the AVLN
- Broadcast MPDUs may be send in the common Awake Window of all stations in the AVLN

- Network State changes and Power Save

The CCo of an AVLN may need to change the network state when one or more STAs in the AVLN are in Power Save. Examples of network state changes include changing the Hybrid Mode of the AVLN, changing the NEK of the AVLN, relocating the beacon, and changing the SNID. The CCo is required to indicate the Beacon Period in which the network state changes using BENTRIES (e.g., Change HM BENTRY). When one or more STAs are in Power Save, the CCo may indicate the network state change information for several Beacon Periods to enable STAs in Power Save mode to track the network state change (for example the Hybrid Mode Change Count Down duration may be 64 Beacon Periods).

CCo may force STAs to exit the Power Save mode using the Stop Power Save Flag in the Power Save BENTRY before changing the network state.

- Power Save and HomePlug AV 1.1

HomePlug AV 1.1 specification does not support Power Save functionality described in this specification. However, HomePlug AV 1.1 implementations may support Power Save functionality described in this section. HomePlug AV 1.1 stations that implement Power Save shall indicate to the CCo their Power Save capability by using CM_STA_IDENTIFY.IND MME. The CCo may also request the Power Save support of a STA using the CM_STA_IDENTIFY.REQ MME.

The CCo shall indicate the presence of HPAV 1.1 stations that do not have extensions to support Power Save in the AVLN using the HomePlug AV 1.1 Present Flag in the Power Save BENTRY. STA in the AVLN may enter Power Save mode when there are HomePlug AV 1.1 stations in the AVLN.

Informative Text

HomePlug AV 1.1 stations that have not indicated their support for Power Save using the CM_STA_IDENTIFY.IND are not capable of decoding the Power Save Schedule and hence may try to send MPDUs intended for a station in Power Save mode during its Sleep Window. Since Awake Window is generally much smaller than the Sleep Window, it is likely that HomePlug AV 1.1 transmits multiple MPDUs during the Sleep Window and determine that the destination is not reachable, thus resulting in loss of communication. Implementations should take this into account to determine if they operate in Power Save mode in the presence of such HomePlug AV 1.1 stations.

- Routing and Repeating for GREEN PHY

Communication between STAs in an AVLN that cannot communicate directly is provided using one or more intermediate STAs as repeaters to deliver unicast, multicast and broadcast MSDUs to the destination STA(s). MAC Frames are retransmitted for unicast MSDUs, and PBs are repeated for broadcast MSDUs.

A GREEN PHY station should support routing and repeating of unicast and broadcast MSDUs. The ability to support routing and repeating of unicast MSDUs is recommended for a GREEN PHY station. The ability to support routing and repeating of broadcast/multicast MSDUs is recommended for a GREEN PHY station.

NOTE: Routing and repeating for GREEN PHY is functionally identical to and interoperable with IEEE 1901.

- GREEN PHY Station Acting as a Repeater for Unicast MSDUs

A GREEN PHY STA that supports repeating of unicast MSDUs shall maintain routing information for identifying the next STA to deliver a MAC Frame based on the ODA for MAC addresses known to be on the AVLN or known to be bridged by other STAs in the AVLN. This information is determined from the TEI Map received from the CCo in the CC_SET_TEI_MAP.IND MME, the LBDAT received from other STAs in the CM_BRG_INFO.CNF MME and routing information received from other STAs in the CM_ROUTE_INFO.CNF/IND MME.

PBs routed to/from associated but unauthenticated STAs shall be unencrypted while sent between authenticated STAs, and unencrypted when sent to/from the unauthenticated STA itself.

- Local Routing Table for GREEN PHY

A GREEN PHY that supports repeating of unicast MSDUs shall maintain a Local Routing Table (LRT) that contains routing information for every associated STA in the AVLN. The LRT includes the TEI of the best next station through which to route (NTEI), the Route Data Rate (RDR) and Route Number of Hops (RNH) for every associated STA in the AVLN (Ultimate Destination TEI, or UDTEI) except for itself. The complete set of TEIs for all associated STAs in the AVLN is provided in the CC_SET_TEI_MAP.IND MME most recently received from the CCo.

A GREEN PHY STA that supports repeating shall broadcast a CM_ROUTE_INFO.IND MME containing routing information from its LRT at least once every Max_Route_Update_Time and no more than once every Min_Route_Update_Time unless RDR_Significant_Change percent is exceeded. It shall also broadcast a CM_ROUTE_INFO.IND MME containing selected routing information from its LRT when significant changes occur. A change is considered to be significant if the RDR to a STA changes by more than RDR_Significant_Change percent. If a previously reachable UDTEI becomes unreachable, this is reported using a **CM_UNREACHABLE**.IND MME. A STA may also request the routing information by sending a CM_ROUTE_INFO.REQ MME.

A STA receiving a CM_ROUTE_INFO.IND or CM_ROUTE_INFO.CNF MME shall compute a candidate RDR (RDR') and RNH (RNH') for each UDTEI entry in the LRT. The candidate RDR (RDR') is computed from the RDR provided in the CM_ROUTE_INFO.IND MME and the average BLE of the transmit channel to the STA that sent the CM_ROUTE_INFO.IND MME as shown in Equation 5-1. The candidate RNH (RNH') is computed by adding 1 to the value of RNH received in the CM_ROUTE_INFO.IND MME. The RDR for a STA that can be communicated with directly is the average BLE of the transmit channel to the STA and the RNH is **0**.

Equation 51: Formula for Calculating the RDR

A STA receiving a CM_ROUTE_INFO.IND MME shall update the RDR/RNH/NTEI entry for each UDTEI in its LRT by selecting the best RDR/RNH pair of the existing entry in the LRT, the candidate RDR'/RNH' pair computed from the received CM_ROUTE_INFO.IND MME and the RDR/RNH for direct communication with the STA, except when the NTEI for the existing entry is the same as the candidate RDR'/RNH' pair. In this case the existing RDR/RNH pair is not selected since it is older than the newly computed RDR'/RNH' pair, and the LRT entry for that UDTEI shall be updated using the fresh information from the NTEI.

If a STA has the NTEI = UDTEI for another STA (i.e., it sends MPDUs directly to that STA), and the link to that STA is lost, then the STA shall send to each of its immediate neighbors a **CM_UNREACHABLE**.IND MME listing that UDTEI with its Unreachable Time Stamp value indicating the current NTB value at that STA. The STA shall also report in the **CM_UNREACHABLE**.IND MME all UDTEIs for which the NTEI is the TEI of the STA whose link was lost.

If a STA receives a **CM_UNREACHABLE**.IND MME containing one or more UDTEI for which the sender is the NTEI (i.e., the STA routes through the sender for that UDTEI), then the STA shall

consider those UDTEIs to be unreachable. The STA shall immediately report this to its neighbors by sending a **CM_UNREACHABLE**.IND MME listing all the UDTEIs that have become unreachable as a result of the received **CM_UNREACHABLE**.IND MME, copying the Unreachable Time Stamp field from the received MME into the transmitted MME. When the hold down period for the STA ends, the STA shall update its LRT for a UDTEI. The hold down period for an unreachable UDTEI lasts from the time t_0 that the path failure message is sent (the **value of the Unreachable** Time Stamp in the **CM_UNREACHABLE**.IND MME), until time $t = t_0 + HD_Duration$. The value of HD_Duration is set over the H1 interface. Once time t has been reached, the STA shall use information in received CM_ROUTE_INFO.IND MMEs to update the route to that UDTEI.

The RDR is coded for the field in the CM_ROUTE_INFO.IND MME using the same 8-bit floating-point format defined for the BLE, with the reserved value noted below. See Section 4.4.1.5.2.10 for more information on computing BLE and the 8-bit floating point field format. An RDR value encoded as **0x00** shall be used to represent an unreachable UDTEI or a UDTEI that is routed through the neighbor to whom the CM_ROUTE_INFO.IND MME is sent (i.e., split horizon with poison reverse). The RDR for any reachable UDTEI whose RDR is less than the rate represented as **0x01** shall be reported as **0x01**.

- Communication between the CCo and a Hidden PCo for GREEN PHY

When a PCo and the CCo cannot communicate directly, then the CC_RELAY.REQ/IND messages shall be sent to the GREEN PHY STA identified by the NTEI in the PCo or CCo entry in the LRT. The ability for a CCo to support a hidden PCo is optional. Further, the ability for a GREEN PHY STA to act as a hidden PCo is also optional.

- GREEN PHY Station Acting as a Repeater for Broadcast or Multicast MPDUs

Broadcast and multicast MPDUs are repeated at the PB level. The CCo will assign STAs in the AVLN to repeat broadcast and multicast transmissions from certain source STAs. The CCo can determine optimum repeating assignment from the Topology Table.

The ability for a GREEN PHY STA or a CCo to support repeating of Broadcast or Multicast repeating is optional.

- Broadcast and Multicast Repeating Assignment for GREEN PHY

A GREEN PHY STA may be assigned to repeat PBs received in broadcast and multicast MPDUs with STEIs listed in the **CC_BCAST_REPEAT**.IND message received from the CCo. STAs shall maintain a Broadcast and Multicast Repeating Assignment Table (BMRAT) when a **CC_BCAST_REPEAT**.IND message is received from the CCo. The STA shall send a **CC_BCAST_REPEAT**.RSP message to the CCo to indicate reception of the **CC_BCAST_REPEAT**.IND message.

The BMRAT contains a list of all TEIs for which the STA shall retransmit PBs when broadcast or multicast MPDUs are received with an STEI matching a TEI in the BMRAT. STAs shall perform duplicate rejection in order to avoid duplicate retransmissions of PBs.

If an MPDU is sent to the broadcast address, then its PBs are repeated encrypted if the MPDU was encrypted, or unencrypted if they were not encrypted.

- Broadcast and Multicast Data SAPs for GREEN PHY

Data SAPs (Section 12.2.1 and Section 12.3.2)
consist of primitives that enable applications to
send and receive data via the HomePlug AV

Data SAPs and PLCs

A STA assigned to repeat PBs received in broadcast and multicast MPDUs shall consult its BMRAT whenever a broadcast or multicast MPDU is received. If the originating STA for the MPDU (the STEI in the Frame Control) is in the BMRAT, the STA shall insert the PBs into the reassembly buffer according to their PBSN as usual, and will schedule any PBs that are not duplicates of ones already received to be broadcast. These PBs shall be sent in an MPDU with the STEI copied from the incoming MPDU, the PPB set to **0xFF**, and the TEI of the repeating STA stored in the BLE field.

- Transmit Power Control for GREEN PHY

Transmit Power Control is an optional feature available to a HomePlug GREEN PHY Station, wherein a station may vary its transmit power up to a maximum value depending on the channel conditions and the network topology. Transmit Power Control provides the following benefits:

- The interference caused to neighboring networks is reduced, thereby increasing spatial reuse.
- Stations implementing Transmit Power Control obtain better power savings.

A GREEN PHY station can maintain statistics about transmissions to each of the stations in the network using the information from the SACK corresponding to these transmissions. The station can use these statistics to determine the power with which it needs to transmit. The transmit power used by a station for communicating directly to another station can be modified dynamically (i.e., automatically reduced) provided the following conditions are met.

- The transmit power of the station must not exceed the limitations specified in 3.7.
- A transmitting station can establish reliable connectivity with a receiving station (in the same network) when using the maximum allowed transmit power. When using reduced power, a transmission from a station must be received properly by the receiving stations as if no Transmit Power Control were used (i.e., use of Transmit Power Control should not inadvertently create Hidden Stations).

A HomePlug GREEN PHY Station that implements Transmit Power Control may discontinue use of this feature if it determines that the receiver can no longer reliably receive the transmissions.

It is recommended that CCos doing Transmit Power Control should periodically transmit beacons using full power to allow new stations to join the network.

Convergence Layer Functions

Overview

The CL comprises the data plane between the H1 and M1 interfaces. It receives data frames from the Data SAPs on one interface, processes the frames (reformatting them as needed), and directs them to the appropriate destination SAP on the other interface.

Table 61 shows the major functions of the CL.

Table 61: Convergence Layer Functions

Data SAPs and PALs	Data SAPs (Section 12.2.1 and Section 12.3.2) consist of primitives that enable applications to send and receive data via the HomePlug AV protocol stack. Each HLE SAP is supported by a PAL that adapts the HLEs data packets for transport to and from the AV system.
Classification	CL function in the transmitter that maps individual data packets from the various SAPs into Connections
De-muxing	Receiver determines to which Connection a packet should be delivered.
Automatic Connection Service (ACS)	Detect certain data flows and then establish, maintain, and tear down Connections with QoS for these flows
QoS Monitoring	Monitor data traffic to ensure that the QoS guarantees of a Connection are being met.
Smoothing	Provide point-to-point smoothing (jitter control) to the HLEs that request it.

Classifier

Classifiers take incoming frames from the application and determine the Connection with which they are associated. They do this by using rules that are generated when the Connection is created. There can also be default rules for packets that do not satisfy the rules for any existing Connection. These rules will prescribe whether to:

Send the packet without a Connection.

Invoke Auto-Connect Service to create a Connection for the packet.

Discard the packet.

The Classifiers for each SAP operate based on Classifier Rule Sets. A single Classifier Rule Set contains one or more Classifier Rules and identifies packets belonging to a single LID. A packet is considered to match a specific Classifier Rule Set if it satisfies all the Classifier Rules contained in that Classifier Rule Set. If a packet delivered to a Classifier matches a Classifier Rule Set, it is sent over the referenced LID of that rule.

Classifier Configuration

The Classifier operates on Classifier Rule Sets that attempt to match packets received from the HLE to an active Connection.

When a new Connection is established, the CM on the source STA of each Link associated with the Connection shall configure the Classifier with classification rule. When the Connection includes a Reverse Link, the CM that initiated the connection setup shall provide the Classifier rule to the destination STA as part of CM_CONN_NEW.REQ.

Classifier-Initiated (Automatic) Connection Setup

If the optional Auto-Connect Service (ACS) is present, any packet given to the Classifier that does not match any of the Classifier Rule Sets will cause the Classifier to pass the packet to the ACS.

Ethernet SAP Classifier Rules

Classifier Rules are used by the local Classifier to detect individual streams of packets from all the packets that flow across the CL Data SAPs.

The Classifier Rules for Ethernet SAP are shown in Table 62. The Classifier Rule and its corresponding Classifier Rule Identifiers (CRIs) are shown in the first and second columns of the table. CRIs are used to identify Classifier Rules when Classifier Rule Sets are communicated using CM_CONN_NEW.REQ. The sizes of the Classifier Rules and their interpretation are shown in the third and fourth columns.

The following Classifier Rules shall be supported by all HomePlug AV stations:

- Ethernet Destination Address
- Ethernet Source Address
- VLAN User Priority

HomePlug AV stations that support bidirectional connections shall support the following additional Classifier Rules:

- IPv4 Source Address
- IPv4 Destination Address
- TCP Source Port
- TCP Destination Port

All other Classifier Rules are optional. Vendor Specific extensions to the Classifier Rules can be achieved by using the Vendor-defined Classifier Rule Identifiers, as shown in Table 62.

Table 62: Classifier Rules for Ethernet II-Class Data SAP

Classifier Rule	Classifier Rule Identifier	Classifier Rule Size (Octets)	Interpretation
Ethernet Destination Address	0x00	6	This rule indicates the Destination Address of the Ethernet frame. The format of this rule is described in the IEEE Standard 802-2001 [4]. The least-significant bit of the least-significant octet of this rule is the Individual/Group (I/G) bit of the 48-bit Ethernet MAC address.
Ethernet Source Address	0x01	6	This rule indicates the Source Address of the Ethernet frame. The format of this rule is described in the IEEE Standard

Ethernet Source Address	0x01	6	This rule indicates the Source Address of the Ethernet frame. The format of this field is described in IEEE Std 802-2001 [1]. The least significant bit of the first octet of this rule is the Individual/Group (I/G) bit of the 48-bit Ethernet MAC address.
VLAN ID	0x03	2	The 12 least-significant bits of this rule indicates the VLAN ID. The format of this field is described in the IEEE Std 802.1Q-1998 [11]. The remaining 4 bits shall be set to 0b0000.
			The 3 least-significant bits of this rule indicates the user_priority contained in the Ethernet VLAN Tag as defined in the IEEE
VLAN User Priority	0x02	1	Std 802.1Q-1998 (Virtual Bridged Local Area Networks [11]). The remaining 5 bits shall be set to 0b00000. A value of 0x00 shall indicate a user priority of 0. A value of 0x01 shall indicate a user priority of 1 and so on.

IPv4 Protocol	0x05	1	This rule indicates the Protocol field in the IPv4 header. The format of this rule is described in the RFC 791 (Internet Protocol) [14]. The most-significant bit of this rule shall correspond to the most-significant bit in the IPv4 Protocol field.
VLAN ID	0x03	2	This rule indicates the VLAN Identifier (VID) contained in the VLAN Tag as defined in the IEEE Std 802.1Q-1998 [11]. The remaining 4 bits shall be set to 0x0. A value of 0x0000 shall indicate null VID. A value of 0x0001 shall indicate the default PVID value used for classifying frames on ingress through a Bridge Port, and so on.
IPv4 Type of Service	0x04	1	This rule indicates the Type of Service (TOS) field in the IPv4 header. The format of this rule is described in the RFC 791 (Internet Protocol) [14]. The most-significant bit of this rule shall correspond to the most-significant bit in the IPv4 TOS field.

IPv4 Protocol	0x05	1	This rule indicates the Protocol field in the IPv4 header. The format of this rule is described in the RFC 791 [14]. The most-significant bit of this rule shall correspond to the most-significant bit in the IPv4 Protocol field. Thus, a value of 0b00000110 in this rule indicates Transmission Control Protocol (TCP).
IPv4 Destination Address	0x07	4	This rule indicates the Destination Address of the IP Version 4 packet. The format of this rule is described in the RFC 791 [14]. The most-significant bit of this rule shall correspond to the most-significant bit in the IPv4 Destination Address. Thus, a value of 0b0 in the most-significant bit in the least significant octet of this rule indicates a Class A IP destination address.
IPv4 Source Address	0x06	4	This rule indicates the Source Address of the IP Version 4 packet. The format of this rule is described in the RFC 791 [14]. The most-significant bit in the least significant octet of this rule shall correspond to the most-significant bit in the IPv4 Source Address. Thus, a value of 0b0 in the most-significant bit in the least significant octet of this rule indicates a Class A IP source address.

IPv6 Flow Label	0x09	3	This 20 bit indicates the Flow label of the IPv6 packet. The format of this field is as described in RFC 791 [14]. The most significant bit in the least significant octet of this rule shall correspond to the most-significant bit in the IPv4 Destination Address. Thus, a value of 0b0 in the most-significant bit in
IPv4 Destination Address	0x07	4	
			the least significant octet of this rule indicates a Class A IP destination address.
IPv6 Traffic Class	0x08	1	This rule indicates the Traffic Class of the IPv6 packet. The format of this field is as described in RFC 2460 (Internet Protocol Version 6 [17]). The most-significant bit in the octet of this rule shall correspond to the most-significant bit in the IPv6 Traffic Class.

IPv6 Destination Address	0x0B	16	This rule indicates the Destination Address of the IP Version 6 packet. The format of this field is as described in RFC 2460 [17]. The most-significant bit in the least significant octet of this rule shall correspond to the most-significant bit in the IPv6 Destination Address.
IPv6 Flow Label	0x09	3	This rule indicates the Flow Label of the IPv6 packet. The format of this field is as described in RFC 2460 [17]. The most-significant bit in the least significant octet of this rule shall correspond to the most-significant bit in the IPv6 Flow Label.
IPv6 Source Address	0x0A	16	This rule indicates the Source Address of the IP Version 6 packet. The format of this field is as described in RFC 2460 [17]. The most-significant bit in the least significant octet of this rule shall correspond to the most-significant bit in the IPv6 Source Address.

IPv6 Destination Address	0x0B	16	This rule indicates the Destination Address of the IP Version 6 packet. The format of this field is as described in RFC 2460 [17]. The most-significant bit in the least significant octet of this rule shall correspond to the most-significant bit in the IPv6 Destination Address.
TCP Source Port	0x0C	2	This rule indicates the Source Port of the TCP packet. The format of this field is as described in RFC 793 (Transmission Control Protocol [15]). The most-significant bit in the least significant octet of this rule shall correspond to the most-significant bit of the TCP Source Port.
TCP Destination Port	0x0D	2	This rule indicates the Destination Port of the TCP packet. The format of this field is as described in RFC 793 [15]. The most-significant bit in the least significant octet of this rule shall correspond to the most-significant bit of the TCP Destination Port.

UDP Source Port Vendor defined Classifier Rule	0x0E 0xE0 – 0xFF	2 -	This rule indicates the Source Port of the UDP packet. The format of this field is as described in RFC 768 [13]. The most-significant bit in the least significant octet of this rule shall correspond to the most-significant bit of the UDP Source Port. The Vendor-defined Classifier Rule shall contain the IEEE-assigned Organizationally Unique Identifier (OUI) [44] in the first three octets of the Vendor-defined Classifier Rule. The OUI shall be followed by vendor-specific information.
UDP Destination Port	0x0F	2	This rule indicates the Destination Port of the UDP packet. The format of this field is as described in RFC 768 [13]. The most-significant bit in the least significant octet of this rule shall correspond to the most-significant bit of the UDP Destination Port.
-	0x10 – 0xDF	-	Reserved for future use

Vendor defined Classifier Rule	0xE0 – 0xFF	-	Vendor-defined Classifier Rule The first three octets of the Vendor-defined Classifier Rule shall contain the IEEE-assigned Organizationally Unique Identifier (OUI, [4]) of the Vendor. The bit and octet order of the OUI is identical to the bit and octet order of the MAC address, as described in Section 4.1.2. All remaining octets of the Vendor-defined Classifier Rule are defined by the Vendor.

Packet Classification in HomePlug GREEN PHY

The classifiers may be used by HomePlug GP stations to determine the priority with which frames from the HLE need to be transmitted. The Classifier Rule Sets may use rules such as Ethernet addresses, IPv4/IPv6 Addresses, IPv4 Type of Service, etc., as specified in Section 6.2.3 to determine the priority of the frame.

Ethernet SAP Classifier Rule Set Format

The Ethernet SAP Classifier Rule Set contains a subset of the Ethernet SAP Classifier Rules. The format of the Ethernet SAP Classifier Rule Set is shown in Table 63.

Within a Classifier Rule Set, Classifier Rules shall be arranged in ascending order of the Classifier Rule Identifier values. For example, if IPv4 Source Address and UDP Source Port are both present in a Classifier Rule Set, the IPv4 Source Address rule appears before the UDP Source Port rule.

Table 63: Format of Ethernet SAP Classifier Rule Set

Field	Octet Number	Field Size (Octets)	Description
Classifier Rule Set Version	0	1	Version number of the Classifier Rule Set 0x00 = Current Version 0x01-0xFF = Reserved for future use.
Number of Classifier Rules	1	1	Number of Classifier Rules specified as part of the Classifier Rule Set = N 0x00 = zero, 0x01 = one, and so on
Classifier Rule Identifier # 1	2	1	Classifier Rule Identifier # 1 (refer to Table 6-3)
Classifier Rule Length # 1	3	1	Length of Classifier Rule identified by Classifier Rule Identifier # 1 (refer to Table 6-3) 0x00 = zero octets, 0x01 = one octet and so on.
Classifier Rule # 1	-	-	Classifier Rule # 1 (refer to Table 6-3)
…			
Classifier Rule Identifier # N	-	1	Classifier Rule Identifier # N (refer to Table 6-3)
Classifier Rule Length # N	-	1	Length of Classifier Rule identified by Classifier Rule

Classifier Rule Length # N	-	1	Length of Classifier Rule identified by Classifier Rule Identifier # N (refer to Table 6-3)
			0x00 = zero octets,
			0x01 = one octet and so on.

Classifier Rule # N	-	-	Classifier Rule # N (refer to Table 6-3)

The following additional restrictions on grouping the Classifier Rules while forming a Classifier Rule Set shall apply:

- Addressing (i.e., SA, DA) should be in only one of the following formats: Ethernet, IPv4, or IPv6.
- When Ethernet addressing is used, only Ethernet Classifier Rules (i.e., VLAN User Priority and VLAN ID) can be present in the Classifier Rule Set.
- When IPv4 addressing is used, the Classifier Rule Set can include other IPv4 Classifier Rules (i.e., IPv4 Type of Service, IPv4 Protocol), UDP Classifier Rules (i.e., UDP Source Port, UDP Destination Port), and TCP Classifier Rules (i.e., TCP Source Port, TCP Destination Port).
- When IPv6 addressing is used, the Classifier Rule Set can include other IPv6 Classifier Rules (i.e., IPv6 Traffic Class, IPv6 Flow Label), UDP Classifier Rules, and TCP Classifier Rules.
- TCP Classifier Rules should always be accompanied with IPv4 or IPv6 Classifier Rules.
- UDP Classifier Rules should always be accompanied with IPv4 or IPv6 Classifier Rules.

Any Classifier Rule Set that includes only the mandatory Classifier Rules and obeying the above restrictions in forming a Classifier Rule Set shall be supported by the STA.

De-muxing

Since there is currently only one SAP/PAL pair, Ethernet II-class, all received packets are sent directly to this SAP (i.e., de-muxing is not strictly necessary). However, if additional SAPs are added, it will be necessary for the implementers to de-mux data packets received at the M1 interface to deliver to the appropriate SAP. The Convergence Layer SAP Type (CLST) field contained in the SOF delimiter can be used to determine the SAP to which the payload of the MPDU belongs.

QoS Monitoring

The CL in both the transmitting and receiving STAs shall gather statistics about Link performance and pass them to the CM, so the CM can verify whether the data transport service levels being delivered satisfy the guaranteed QoS service level.

Auto-Connect Service

The Auto-Connect Service (ACS) is an optional service that provides support for:

Packets from legacy applications that start transmission without specifying QoS parameters.

Packets bridged from another network.

ACS provides the following benefits:

Establishes Connections with QoS CSPEC, even when the HLE does not set up the Connection.
Allows system to use CP or CFP, based on recognition of the application type or data-stream characteristics.
Efficient bandwidth management.
When the Classifier (refer to Section 6.2) encounters a packet that does not associate with an existing Connection, it shall refer the packet to ACS, so ACS can try to establish a Connection.
If the ACS service is not present in the STA (ACS is an optional service), the Classifier shall provide connectionless transport for the packet.
If ACS is present in the STA, it will attempt to determine whether COS is appropriate for the packet sequence of which the current packet may be a part, or whether the packet should be transported via CLS.
ACS will be presented with every data packet delivered to the H1 interface that is not part of an established Connection. Therefore, it must be extremely efficient and be able to quickly identify packets that are part of an ongoing connectionless data flow.
Evaluation of Data Flow
ACS will be presented with various kinds of packets to evaluate. These include:
Streamed packets for which transport in the CFP is appropriate.
RTP packets for which either CFP or CP transport may be appropriate.
Prioritized packets for which either CFP or CP transport (either connection-oriented or connectionless) may be appropriate.
Common Packets for which connectionless CP transport is appropriate.
ACS' decision about how packet(s) should be transported may be based on one or more of the following:
Polices established for identifying automatic Connections.
Templates: providing certain default rules; e.g., associating traffic on a particular IP port with a particular usage (and implying a level of QoS from that usage).
Heuristics: attempting to identify a need for a particular level of QoS from the statistical behavior of traffic offered. For example, Auto-Connect could monitor successive packets and judge whether they are streaming data (i.e., whether the packets should be transferred with reserved bandwidth channel). If it judges streaming data, it decides on the appropriate QoS parameters and notifies the CM to establish a Connection.
ACS Processing
The actions ACS takes to establish a Connection include:
ACS receives a "no match" indication for an incoming packet from the classifier.
ACS decides whether to invoke the COS or CLS.
ACS initiates the Connection setup process and specifies the CSPEC if COS is invoked.
ACS updates the Classifier with the appropriate GLID or LLID, so future packets are handled correctly by the classifier.
Auto-Connect also manages the Connections it establishes, including reconfiguration and teardown, which the HLE would normally perform.
Implementers shall establish controls internal to the Control Plane to enable ACS to have access to the same capabilities as an HLE, plus awareness of the data flow of the Connections that it

establishes.

Data Flow Evaluation

The number of packets ACS must examine to determine whether the packets are part of a "connection worthy" data flow depends on the method used for determination. If templates and/or policies are used, ACS may be able to determine connection-worthiness from a single packet. If Heuristics are used, ACS may need to examine many packets to determine how fast packets are arriving and how much bandwidth would be required for a Connection.

The ACS should release packets for CLS transport in the CP as soon as it finishes examining the packet. It should not hold packets while it is determining whether a Connection is warranted or while a Connection is being established.

After Data Flow Evaluation is Complete

Once ACS determines that a Connection should be established for a particular data flow, it will have established an initial CSPEC. ACS shall follow the same process as an HLE for establishing the Connection.

While Connections requested by an HLE are Connections between HLEs, Connections established by ACS are not. The difference is whether the Connection is negotiated between HLEs or between CLs. To ensure that the HLE is not notified of the events triggered by the establishing or maintenance of automatic Connections, Connections established by ACS shall be made in Automatic Connection Mode (refer to Section 11.5.16) and the CL shall not communicate connection-related primitives to the HLE for Connections made in Automatic Connection Mode.

Monitoring Automatic Connections

The ACS is responsible for performing activities that would normally be undertaken by the HLE, including management, reconfiguration, and teardown of the Connections it establishes.

In particular, ACS is responsible for:

Monitoring the data flow

Ensuring that the initial CSPEC it assigned is appropriate for the data flow

Making the appropriate adjustments to that CSPEC

This monitoring differs from the monitoring performed by the CL. CL Monitoring is to ensure that service level matches that guaranteed by the CSPEC. ACS monitoring is to ensure that QoS levels established in the CSPEC generated by ACS are appropriate for the data traffic carried by the automatic Connection.

Auto Connect Service for GREEN PHY

A station implementing only GREEN PHY only supports "connectionless" priority links. Therefore, a Home Plug GREEN PHY Station is not required to support the Auto Connection Service feature.

Smoothing (Delay Compensation, Jitter Control)

The terms "Smoothing," "Delay Compensation," and "Jitter Control" all refer to the smooth delivery of packets to the destination (rendering) application. Smoothing is necessary for many AV applications to provide an acceptable user experience (UE).

If smoothing is performed, each packet will be delivered to the rendering application at a constant delay interval after the packet was generated at the source application.

Point-to-Point Smoothing

Point-to-point smoothing is performed between two arbitrary points along the data path between the source and the destination. It is performed without awareness of or access to any timing information internal to the data stream. It is useful if the jitter introduced into the data stream is wholly contained by the points between which smoothing is performed. Point-to-Point Smoothing is an optional feature.

End-to-End Smoothing

End-to-end smoothing is performed between the source application and the destination application. It relies on timing information internal to the data stream. By definition, all jitter is introduced between the two end points and can be removed by end-to-end smoothing. If the data path between source and destination spans more than one network, end-to-end smoothing is the only technique for full jitter control.

Smoothing Control

The HLE may perform the smoothing itself (probably end-to-end smoothing) or it may request the CL to perform point-to-point smoothing.

Two fields in the CINFO portion of the CSPEC, Arrival Time Stamp to HLE (ATS) and Smoothing, are used to support this service. Table 64 provides a summary of how these two fields interact.

If the HLE wants the CL to perform smoothing and it is supported by the station, it shall request smoothing in its CSPEC. If the HLE wants a timestamp delivered to it, it shall request an ATS in its CSPEC. To provide end-to-end smoothing, the HLE should use the APCM_GET_NTB.CNF primitive to get the current value of the Network Time Base (refer to Section 12.2.2.13).

Table 64: Smoothing/Jitter Control

		Arrival Time Stamp to HLE (ATS)	
		Yes	No
Smoothing	Yes	CL will provide Smoothing Service and will pass a timestamp to the HLE.	CL will provide Smoothing Service using the ATS, but will not pass a timestamp to the HLE.
	No	CL will deliver packets & timestamps to HLE upon arrival.	CL will deliver packets to HLE upon arrival, but will not pass a timestamp to the HLE.

If the transmitting station detects either an ATS request or a smoothing request, it shall prepend a 32-bit ATS field before each MSDU that carries user traffic. The ATS is the value of the Network Time Base (refer to Section 5.5) of the transmitting station when the MSDU is received by the CL. At the receiving station, the presence or absence of ATS field(s) in a MAC Frame is indicated by the MFT field in the MAC Frame Header.

If ATS fields are present and if smoothing has been requested, the receiving station shall deliver MSDUs to the application based on the ATS value of the received MSDU in a way that will enable the stream to meet its latency and jitter requirements negotiated during the connection setup.

If ATS fields are present and if an Arrival Time Stamp has been requested, the receiving station shall deliver the ATS to the HLE (refer to Section 12.2.1.1.3).
If smoothing is not requested, MSDUs are delivered to the HLE, with or without timestamps, as soon as they are in sequence (i.e., no prior MSDUs are expected to be received).
Smoothing (Delay Compensation, Jitter Control) for GREEN PHY
A station implementing only GREEN PHY is not required to implement this feature.

Central Coordinator
Power-On Network Discovery Procedure
As with HomePlug AV, a GREEN PHY STA performs the Power-on Network Discovery Procedure to determine whether another HomePlug network is active and if a new AVLN can be instantiated. All STAs shall be capable of performing the Power-On Network Discovery Procedure.
Prior to initiating the Power-On Network Discovery Procedure, the GREEN PHY STA will select a BeaconBackoffTime (BBT). If the STA was the CCo of an AVLN before it was powered down, BBT should be chosen as a random value in the interval (MinCCoScanTime, MaxCCoScanTime). Otherwise, BBT shall be a random value in the interval (MinScanTime, MaxScantime). BBT is the maximum duration of time for which a STA will execute the Power-on Network Procedure.
During the Power-on Network Discovery Procedure, if one or more AVLNs are detected, the STAs shall attempt to transmit the CM_UNASSOCIATED_STA.IND MME using multi-network broadcast approximately once per Unassociated STA Advertisement Interval (USAI) to provide information to other stations that may be performing the same procedure. The transmission time of each CM_UNASSOCIATED_STA.IND MME (i.e., Unassociated Station Tranmission Time (USTT)) shall be randomly chosen (refer to Section 5.4.3.1). Further, the STA shall synchronize its PhyClk to one of the detected AVLNs, and shall use the SNID of that AVLN in the Multi-Network Broadcast transmissions. This provides a way for other STAs that also hear the same AVLN to apply the appropriate PhyClk correction for reception.
During the Power-On Network Discovery Procedure, while no AVLNs are detected, the STA shall search for Beacons and other unassociated STAs using Hybrid mode. After an AVLN is detected, the STA may adopt the HomePlug 1.0/1.1 coexistence mode of that AVLN. Optionally, the STA may continue to search in Hybrid mode (irrespective of the mode of the AVLN that it detected). This optional behavior will enable the STA to continue to detect Beacons of non-coordinating AVLNs (if any). It is important to note that proper execution of the CSMA/CA channel access mechanism requires the STA to perform virtual carrier sense in the mode of the Shared CSMA region (i.e., AV-only or Hybrid mode) of the AVLN(s) being tracked. Thus, if the Shared CSMA region is in AV-Only mode and the STA is searching in Hybrid mode, it has to transition to AV-only mode during the AVLNs Shared CSMA region as soon as it has a pending transmission. The STA should also transition back to Hybrid mode after the transmission is completed.
During the Power-On Network Discovery Procedure, detection of an AVLN with matching NID causes the unassociated STA to follow the procedure described in Section 7.3.5 for joining the AVLN . If the STA successfully joins the AVLNs, it shall terminate the power-on network

procedure and become a STA in the AVLN (refer to Section 7.2.3). Failure to join successfully shall cause the STA to continue with the power-on network procedure.
Upon the expiration of the BBT, the STA shall process all the received Unassociated STA information (if any) as follows:
If the STA detects other Unassociated STAs with a matching NID, it shall use the procedure described in Section 7.4.1 to determine whether it has to become the CCo and instantiate a new AVLN.
If the STA detects no other AVLNs and there are no Unassociated STAs with matching NID, it shall become an Unassociated CCo (refer to Section 7.2.1),
In all other cases, the STA shall operate as an Unassociated STA (refer to Section 7.2.1).
A STA that failed to form or join an AVLN during the Power-on procedure shall operate in Unassociated STA Mode or Unassociated CCo Mode. Both these modes are generically called Unassociated STA Mode. Section 7.2.1 and Section 0 provide details on the Unassociated STA Mode and Unassociated CCo Mode respectively.
Figure 71 shows the basic functional flow for Power-on Network Discovery Procedure.

Figure 71: Power-on Network Discovery Procedure
STA Behavior After Power-on
Once the power-on procedure is completed, a STA can be an Unassociated STA, Unassociated CCo, STA of an AVLN or CCo of an AVLN. This section describes the behavior of STA in each of these modes.
Unassociated STA Behavior
An Unassociated STA that detects other AVLNs shall continue to send CM_UNASSOCIATED_STA.IND MME using multi-network broadcast approximately once per MaxDiscoverPeriod to provide information to other stations. The transmission time of each CM_UNASSOCIATED_STA.IND MME shall be randomly chosen. Further, the STA shall synchronize its PhyClk to one of the detected AVLNs, and shall use the SNID of that AVLN in the Multi-Network Broadcast transmissions. This provides a way for other STAs that also hear the same AVLN to apply the appropriate PhyClk correction for reception.
Detection of an AVLN with matching NID causes the unassociated STA to follow the procedure described in Section 7.3.5 for joining the AVLN. If the STA successfully joins the AVLN, it shall become a STA in the AVLN. Failure to join successfully shall cause the STA to continue operating as an Unassociated STA.
If an Unassociated STA determines that there are no AVLNs to track (i.e., AVLN(s) that it is tracking no longer exist), it shall become an Unassociated CCo.
Detection of a CM_UNASSOCIATED_STA.IND MME with matching NID causes the STA to follow the procedure described in Section 7.3.4.1.
Figure 7-2 shows the basic functional flow for Unassociated STA behavior.

Figure 72: Unassociated STA Behavior
Unassociated CCo Behavior
The mode of operation of an Uncoordinated CCo with respect to HomePlug 1.0/1.1 coexistence

shall be based on the detection status of HomePlug 1.0/1.1 delimiters (refer to Section 9.3). The neighbor network mode of operation of an Unassociated CCo shall be either CSMA-Only mode or Uncoordinated mode, as described in Section 8.5. Unassociated CCos shall periodically send Discover Beacons as required by the Discover Process (refer to Section 7.6). An Unassociated CCo shall not transmit the CM_UNASSOCIATED_STA.IND MME.
Detection of an AVLN shall cause the Unassociated CCo to start operating as an Unassociated STA.
Reception of valid CC_ASSOC.REQ shall cause the Unassociated CCo to become a CCo.
Figure 73 shows the basic functional flow for Unassociated CCo behavior.

Figure 73: Unassociated CCo Behavior

Behavior as a STA in an AVLN

Upon joining the AVLN, if the STA is a user-appointed CCo (refer to Section 7.4.2) and the existing CCo of the AVLN is not a user-appointed CCo, the STA sends a CC_CCO_APPOINT.REQ to the existing CCo to hand over the CCo functionality. Successful handover of the CCo functionality will cause the STA to become a CCo.
A CCo-capable STA may also become a CCo as a result of CCo selection procedure execution (refer to Section 7.4) or subsequent to CCo failure, if the STA is a backup CCo (refer to Section 7.9.2).
If a STA in the AVLN fails to detect the Central or Proxy Beacons of the AVLN that it is part of for MaxNoBeacon and it is not the backup CCo, it should restart the Power-on procedure.
If a STA in the AVLN is requested to leave the AVLN, it shall become an Unassociated STA.
Figure 74 shows the basic functional flow for the behavior as a STA in an AVLN.

Figure 74: Behavior as a STA in an AVLN

- Identifying HomePlug GREEN PHY Stations

A HomePlug GREEN PHY Station or a HomePlug AV station (with a version greater than 1.1) shall advertise its GREEN PHY Station type and capabilities (e.g., the station is HomePlug GREEN PHY ver 1.0 capable) to the CCo after the association and authentication process. This advertisement is done using CM_STA_IDENTIFY.IND MME. The format of the CM_STA_IDENTIFY.IND MME is described in Section 11.5.39. The CCo acknowledges the receipt of this MME using a CM_STA_IDENTIFY.RSP MME. A HomePlug GREEN PHY Station shall also advertise its HomePlug AV version number and/or GREEN PHY station type and capabilities to the other stations in the network using the discover beacons. A HomePlug GREEN PHY Station shall use the GREEN PHY Capability and HPAV version fields of Discovered Info BENTRY wherein it indicates its device type. Refer to Table 4-79 for more details. Alternately, any HomePlug GREEN PHY Station or a future version of HomePlug AV station may request the Station Identification information using a CM_STA_IDENTIFY.REQ MME. A HomePlug GREEN PHY Station or a future version of HomePlug AV station responds to this request using a CM_STA_IDENTIFY.CNF MME. The format of the CM_STA_IDENTIFY.CNF MME is as described in Section 11.5.38.

Behavior as a CCo in an AVLN

Once a STA becomes a CCo, if it determines that there are no STAs that have successfully joined the AVLN, it shall start a Join Wait Timer. Join Wait Timer is the duration of time for which the STA will act like a CCo if no other STA has successfully joined the AVLN. It is recommended that Join Wait Timer be set to at least MaxDiscoverPeriod to provide sufficient time for STAs to join the AVLN. If a STA joins the AVLN before the expiration of Join Wait Timer, the timer shall be cleared. Expiration of a Join Wait Timer shall cause the CCo to operate as an Unassociated CCo if there are no other AVLNs present; otherwise, it shall start operating as an Unassociated STA. Handing over of the CCo functionality to another STA in the AVLN shall cause the CCo to become a STA in the AVLN.
If all the STAs associated with the AVLN leave the AVLN and there are no other AVLNs detected, the CCo shall operate as an Unassociated CCo. If all the STAs associated with the AVLN leave the AVLN and there is at least one other AVLN detected, the CCo shall become an Unassociated STA.
Figure 75 shows the basic functional flow for the behavior as a CCo in an AVLN.

Figure 75: Behavior as a CCo in an AVLN
Deciding AV-Only or Hybrid Mode
If a STA joins an AVLN, it shall adopt the mode of that AVLN (although it shall inform the CCo of the traffic it has detected, which may change the mode later – refer to Section 9.3.1 and Section 9.3.2). When forming an AVLN (either as an Unassociated CCo or as the CCo of an AVLN with other STAs), the STA that becomes the CCo must determine the mode of the AVLN (refer to Section 9.3.2).
All STAs shall search for HomePlug 1.0.1 and HomePlug 1.1 transmissions during the power-on procedure. This information is used to determine the coexistence mode of the AVLN when the STA becomes a CCo and instantiates a new AVLN. During Power-on, detection of HP1_FC_Thresh valid HomePlug 1.0.1 or HomePlug 1.1 transmissions over an interval of HP1_FC_Thresh_Interval or less shall constitute detection of HomePlug 1.0.1 or HomePlug 1.1 activity, respectively.

Forming or Joining an AVLN
AVLN Overview
An AVLN is formed by STAs that possess a common NID and CCo. STAs in an AVLN will typically possess a common NMK and Security Level (SL), but a CCo may divide an AVLN into sub-AVLNs, each with its own NMK. All NMKs that are associated with the same NID shall have the same SL, which is provided in the **CM_SET_KEY.REQ** MME or in the **APCM_SET_KEY.REQ** primitive. When no AVLN exists and a STA discovers one or more other stations with the same NMK and SL, the STAs shall form an AVLN if at least one is CCo-capable. If a STA discovers an existing AVLN with the NMK and SL it possesses, it shall join the existing AVLN. An AVLN is formed or joined using Association and Authentication.
To join (participate in) an AVLN, a STA must have:
A valid NMK and Security Level (NMK-SL, obtained by Authorization — a.k.a. NMK

Provisioning, as described in Section 7.10.3).
A unique TEI (obtained by Association, as described in Section 7.3.2).
The current NEK (obtained by Authentication, as described in Section 7.3.3).
Usually, the NMK-SL and NID are stored in non-volatile memory.

Network Identification

Each AVLN has a Network Identifier (NID) that is provided with or generated from the NMK-SL and is used to help a STA identify another STA or AVLN with the same NMK-SL. Section 4.4.3.1 describes how the NID is generated.

It is possible, though highly unlikely, for different NMKs to hash to the same NID value. Consequently, the NID is not guaranteed to be unique and is not guaranteed to identify a STA or AVLN with the same NMK. Neighboring AVLNs could have different NMKs, but the same NID. STAs shall attempt to join each STA or AVLNs that possess the NID that is associated with or generated from the NMK the STA possess. Networks with the same NID are uniquely identified by the SNID and NID pair.

It is also permitted for the CCo to use the same NID for multiple NMKs, forming a sub-AVLN with each NMK. As the NIDs are the same, a STA with an (NID,NMK) pair whose NID matches the NID of an AVLN shall attempt to join that AVLN. The CCo must disambiguate the NMK depending upon its knowledge of the STA's MAC address.

Human-Friendly Station and AVLN Names

STA manufacturers shall provide default "Human Friendly" Identifiers (HFIDs) to the STAs. An HFID shall be a string of up to 64 ASCII characters chosen from the range ASCII[32] to ASCII[127]. The HFIDs shall be stored in non-volatile memory. The HFID shall be null-terminated (ASCII[00]). If the HFID is a full 64 characters in length, an implicit null character shall be interpreted in the "65^{th} character position."

User Interface (UI) software should provide functionality to enable the user to enter/modify user-entered "human friendly" names for each STA actively joined to the AVLN and for the AVLN itself. These user-entered HFIDs are distinct from the manufacturer-set HFID for the STA, which is permanent. The UI may provide a way for the user to cause the HFID to be sent or replaced with the null string when it is sent in the clear. Authenticated stations may refuse to provide the HFID to STAs outside the AVLN (i.e., always encrypt MMEs containing the HFID with the NEK).

The HFID of an AVLN is obtained by sending a CC_WHO_RU.REQ MME and receiving the associated CC_WHO_RU.CNF reply. These may be sent and received unencrypted. The HFID of a STA is obtained by sending a CM_ HFID.REQ MME and receiving the associated CM_ HFID.REQ reply. These are ordinarily sent and received encrypted with the NEK.

Get Full AVLN Information

The NID is contained in each Beacon transmitted by the CCo. Ordinarily, this will be sufficient, but there will be circumstances when the STA needs additional information about the AVLN (e.g., to identify the AVLN to the user it will need to get the HFID of the AVLN). The Message Sequence Chart (MSC) shown in Figure 76 allows the new STA to get full AVLN information prior to obtaining a TEI. If the STA already has a TEI, that value shall be used within the messages.

Figure 76. Getting Full AVLN Information

Get Full STA Information

The SNID and TEI are contained in each MPDU transmitted by a STA. Ordinarily, this will be sufficient, but there will be circumstances when a user needs additional information about the STA (e.g., the HFID of the STA is useful to identify the STA to the user).

The CM_GET_HFID.REQ MME may be used to get the HFIDs of the STA (manufacturer-set HFID or user-set HFID) or the HFID of the Network. A STA that belongs to an AVLN may elect not to provide the actual HFIDs if the request is not encrypted with the NEK, but to replace them with the null string. A STA whose NMK has never been used by it to join or to form an AVLN should respond with its actual HFID in the clear when requested to do so.

The CM_STA_CAP.REQ MME may be used to get detailed information about the STA including optional features the STA supports, the HomePlug AV version, the OUI and the product manufacturer's version number.

Association

Association is a process by which a STA obtains a valid TEI from the CCo of the AVLN with which it wants to associate. Disassociation is a process by which a STA should stop using a valid TEI for an AVLN with which it was once associated. Upon disassociation, the TEI becomes invalid until reassigned.

There is a single method of Association, but there are several methods of Disassociation.

When a STA initially wants to communicate with an AVLN, it shall perform Association as shown in Figure 77.

Figure 77. STA Association

When two Unassociated STAs try to form an AVLN, a STA that determines that another STA is better suited to become the AVLN's CCo and that the two STAs should form an AVLN (by matching NIDs or SC-Join states) shall wait for the other STA to establish the AVLN and start transmission of Central Beacons. A STA that decides it should become the CCo based on CCo capabilities, matching NIDs, or SC-Join/Add states shall start transmitting Central Beacons and wait for a CC_ASSOC.REQ MME from the other STA, as described in Section 7.1.

When a STA joins an AVLN, the CCo shall provide the complete TEI Map to that STA and update all other STAs in the AVLN with the new TEI Map information using the CC_SET_TEI_MAP.IND MME.

TEI Assignment and Renewal

The CCo assigns a Terminal Equipment Identifier (TEI) to each STA when it successfully associates with the AVLN. The TEI shall be 8 bits long and shall be unique within the AVLN. Table 71 shows the possible values of the 8-bit TEI. Note the TEI value of 0x00, which may be used by a new STA or by a CCo that wants to communicate with another CCo. The new STA shall recognize that the CC_ASSOC.CNF MME (sent with the broadcast TEI) is for it by verifying that the ODA in the MME is its MAC address.

Table 71: TEI Values

TEI Value	Interpretation

0x00	TEI not yet assigned. This value may be used by a CCo to communicate with another CCo or by a new STA that has not yet associated with the AVLN.
0x01 - 0xFE	Identifies a STA within the AVLN.
0xFF	Broadcast TEI (All STAs shall treat message as addressed to them). This value shall never be used as an STEI.

The CCo maintains the list of assigned TEIs and the corresponding mapping of MAC addresses. The CCo shall send the CC_SET_TEI_MAP.IND MME (unencrypted) to the new STA to provide it with the current (TEI, MAC address) mappings of all existing STAs in the AVLN.
The CCo shall send the CC_SET_TEI_MAP.IND MME (encrypted) to update all authenticated STAs with any changes in the mappings (e.g., a new STA has joined the AVLN).
After a STA is disassociated (or has been expelled), its TEI will be reclaimed by the CCo. The reclaimed TEI shall not be reused for a period of at least 5 minutes and the CCo shall send the CC_SET_TEI_MAP.IND MME to update all authenticated STAS with the disassociation(s).
An authenticated STA may use the CC_SET_TEI_MAP.REQ MME to query the CCo for a full copy of the TEI Map. The CCo shall respond to the STA with the CC_SET_TEI_MAP.IND to provide the TEI map.
Disambiguated TEIs
Although the CCo ensures that the TEIs it assigns are unique within the AVLN, the same TEI value may be assigned to a different STA in a neighbor AVLN, so it is important to disambiguate the TEI by associating it with the network where it is generated. The NID or the SNID can be used for this purpose.
TEI Leases and Renewals
When the CCo assigns or renews a TEI it shall specify a lease time. This is the length of time for which the STA may use the TEI. If the lease time expires before the TEI is renewed, the STA shall stop using the TEI and apply for another. Permitted lease values are shown in Table 72.
Table 72: Lease Values

Lease Value	Interpretation
0x0000	Reserved
0x0001 - 0xFFFF	Lease time in minutes (maximum value exceeds 45 days) 0x000F = 15 minutes is default lease time for STAs that are associated but not authenticated. 0x0B40 = 48 hours is default lease time for an authenticated STA.

Lease time is measured from the time the CCo generated the corresponding CC_ASSOC.CNF. Variable amount of delay can be incurred from the time the CCo generated the CC_ASSOC.CNF and the STA receives and processes the message. Implementations should consider this when determining the expiry time of the TEI lease and the time at which the STA starts renewing its TEI lease. Before the lease time has expired, a STA shall go through the association process again to

renew its TEI. It is recommended that the STA starts its TEI renewal process at least 5 seconds before the expiration of its lease time. The ReqType field in the CC_ASSOC.REQ message shall be set to indicate that it is a renewal request. If the CCo accepts the renewal request, the same TEI shall be assigned to the STA. If the STA fails to renew its TEI before it expires, the CCo shall s the STA from the AVLN.

A renewal CC_ASSOC.REQ message may also be sent by an existing STA to a PSTA to indicate that the existing STA can no longer decode the (Central) Beacons reliably. The PSTA shall forward the CC_ASSOC.REQ message to the CCo. The CCo shall accept the renewal request, create a Proxy Network, and assign the same TEI to the existing STA. Refer to Section 7.7.

When to Stop Using a TEI

A STA shall stop using a TEI if any one of the following events occurs:

The TEI's lease time expires before the STA has successfully renewed the lease.

The STA disassociates from the AVLN (refer to Section 7.3.5.1).

The AVLN's CCo asks the STA to leave the AVLN (refer to Section 7.3.6).

Updating STAs with the TEI MAP

When there is a change in the TEI Map, such as when a STA associates, authenticates, or leaves the AVLN, the CCo shall send a CC_SET_TEI_MAP.IND message to all STAs in the AVLN. A STA can request the current TEI Map from the CCo using the CC_SET_TEI_MAP.REQ message.

Method for Authentication

Once a STA has associated and has a valid NMK, it shall use this NMK to join the AVLN. If the CCo verifies the STA's NMK, it will give the STA an NEK. Once a STA is authenticated successfully, the CCo shall maintain the STA's authentication status as long as the STA's association status is maintained. Thus, a STA is not required to re-authenticate subsequent to TEI renewal.

There is one method for Authentication; it is used by all STAs. The joining STA shall send a CM_GET_KEY.REQ containing KeyType = NEK, the STA's TEI and MAC address. It shall also contain a freshly generated nonce. The message shall be placed in an Encrypted Payload of a CM_ENCRYPTED_PAYLOAD.IND MME encrypted by the NMK, with PID=0x00 and PMN=0x01.

If the CCo confirms that the correct NMK was used to encrypt the message, it shall send a CM_GET_KEY.CNF message (in a CM_ENCRYPTED_PAYLOAD.IND with the payload encrypted with the NMK) to the STA. This message shall contain the NEK and EKS along with the nonce sent in the request and shall be placed in an Encrypted Payload encrypted using the NMK. The procedure is shown in Figure 78.

If the CCo cannot decrypt the request encrypted by that NMK (indicated by CM_ENCRYPTED_PAYLOAD.RSP with Result = Failure), the new STA shall flag the NMK as invalid on this AVLN (NID and SNID) and either restart the process of obtaining a (valid) NMK on this AVLN or try to join a different AVLN (same NID but different SNID).

The new STA can begin using the NEK as soon as it successfully receives it from the CCo.

Figure 78: Provision NEK for a new STA (Authentication)

Forming a New AVLN

Two Unassociated STAs can form a new AVLN when one of four conditions is met:

They have the same (NID,NMK) pair, and one or both receives the other's CM_UNASSOCIATED_STA.IND MME (refer to Section 7.3.4.1).

One STA sends the other STA its NMK encrypted with the other STA's DAK (refer to Section 7.3.4.2).

They both have NMK-SCs, and one's HLE indicates that it should enter the SC-Join state and the other's HLE indicates that it should enter the SC-Add state (refer to Section 7.3.4.3).

They both have NMK-SCs and the HLE of each indicates they should enter the SC-Join state (refer to Section 7.3.4.4).

In each of these cases, two Unassociated STAs exchange MMEs that includes the CCo capability of each STA, and from these MMEs each STA recognizes that a new AVLN needs to be formed. One of the STAs will become the CCo (as described in Section 7.4.1) and the other will associate with the new CCo, and possibly perform the NMK key exchange and ultimately authenticate. CM_SET_KEY.REQ/CNF, CM_UNASSOCIATED_STA.IND**,** and CM_SC_JOIN.REQ/CNF MMEs contain CCo capability information; this information allows the recipient to determine which STA should become the CCo of the new AVLN. Whichever STA has the greater CCo capability (as defined in Section 7.4.1 shall become the new CCo. Once the AVLN is formed, the CCo may be changed due to other factors.

A STA that determines that another STA should become the CCo (refer to Section 7.4.1) shall wait to try to associate with it until it starts receiving the Central Beacon from that STA or possibly another STA. Such STAs may only repeat the MMEs that the other STA must receive to prompt it to form an AVLN. The other STA should reach the same conclusion and become a CCo and start issuing Central Beacons, perhaps in Coordinated Mode if a neighboring network is present. A STA that becomes a CCo shall begin transmitting the Central Beacon and shall continue to do so as long as at least one STA has successfully associated with it or while it hears MMEs from other STAs that should associate with it.

When the STA has or receives an NMK associated with an NID matching that of the new CCo (possibly as a result of one of the processes described above), it shall try to authenticate using the protocol described in Section 7.10.4. If authentication fails, the NMKs are not the same and the protocol aborts. In this case, if the CCo has no associated STAs, it shall cease AVLN operation and returns to being an Unassociated STA (unless it cannot detect any other AVLN). If authentication failed for reason other than different NMKs, the STAs should try again to form a new AVLN. If authentication succeeds, the initial AVLN formation is complete and the STAs may go on to add more STAs to the AVLN, select a new CCo, etc.

Two Unassociated STAs with Matching NIDs

Two STAs with identical NMKs and identical Security Levels will also have identical default NIDs. Identical NIDs do not guarantee that the NMKs are identical, but the probability against this is very small. The NID is advertised in the CM_UNASSOCIATED_STA.IND MME, so when one STA receives the other STA's CM_UNASSOCIATED_STA.IND MME, it will observe the matching NID.

At this point, one of the STAs (or a third STA) must become a CCo as defined in Section 7.4.1.

The CM_UNASSOCIATED_STA.IND MME contains the CCo capability and the MAC address of the sender (as part of the generic MME format). The receiver can then decide whether it or another STA should become the CCo.
If the STA determines that it should become the CCo, it shall form a new AVLN and start sending Central Beacons, then wait for the other STA(s) to associate.
If the STA determines that another STA should become the CCo, it shall wait until it detects a Central Beacon with matching NID. In the meanwhile, the STA shall continue to send CM_UNASSOCIATED_STA.IND MMEs periodically in case the other STA did not correctly receive its earlier advertisements and hence does not know to become the CCo of a new AVLN.
After the non-CCo STA has detected the new CCo's Beacon with matching NID, it shall send the CCo a CC_ASSOC.REQ MME asking it for a TEI.
If more than one AVLN with the same NMK is formed, the STA may attempt to join any AVLN with matching NID that it detects. These AVLNs may merge using the mechanism described in Section 8.6.
Once the STA has associated with the CCo, it shall try to authenticate as described in Section 7.10.4.
This entire process is shown in Figure 79.

Figure 79: AVLN Formation by Two Unassociated STAs with Matching NIDs

Two Unassociated STAs Form an AVLN Using a DAK-encrypted NMK

When the HLE provides a STA with the DAK of another station and tells it to send the other STA an NMK and NID, the STA shall broadcast a CM_SET_KEY.REQ MME containing a TEK and encrypted with the DAK as the payload of a CM_ENCRYPTED_PAYLOAD.IND MME, sent unencrypted using multi-network broadcast. All STAs that receive the MME shall try to decrypt it; if one succeeds, that successful STA shall respond with a CM_SET_KEY.CNF MME encrypted with the TEK as the payload of a CM_ENCRYPTED_PAYLOAD.IND MME sent unencrypted using unicast.
Note: A STA that fails to decrypt a CM_ENCRYPTED_PAYLOAD.IND MME that uses a DAK for payload encryption shall not respond to that MME with a CM_ ENCRYPTED_PAYLOAD.RSP MME, but shall silently drop the message.
Each STA compares the CCo capability fields (present in the first two messages) and determines which STA should become the CCo, as defined in Section 7.4.1. Once one STA becomes the CCo and the other STA has associated with it, the STAs complete the protocol as described in Section 7.10.3.4. When the protocol is completed successfully, the STA that is not the CCo shall authenticate with the CCo to obtain the NEK. The new CCo shall use in its Central Beacon the NID that was sent with the NMK; the other STA must also use the NID associated with the NMK and wait for a Central Beacon with the matching NID before it authenticates with the CCo.
The STA sending the DAK-encrypted payload shall continue to transmit these periodically until it either receives a response or until it times out.
If the STA that was given the DAK by its HLE later joins with some other STA to form an AVLN, it may restart this protocol by sending the DAK-encrypted payload as an AVLN STA.
An associated (and even authenticated) STA that receives a new NMK via DAK-encrypted

payload shall leave its current AVLN and form an AVLN with the STA that initiated the DAK-based protocol, even if that STA is not initially part of any AVLN.
The entire process (omitting failure paths) is shown in Figure 710. See also Section 7.10.3.4.

Figure 710: AVLN Formation Using a DAK-Encrypted NMK

Two Unassociated STAs: One in SC-Add and One in SC-Join

When the HLE places a STA into the SC-Join state, it transmits CM_SC_JOIN.REQ MMEs using multi-network broadcast periodically until it either joins an AVLN or times out. If the HLE places the STA into the SC-Add state, however, it does not advertise this, but waits to hear another STA transmitting CM_SC_JOIN.REQ MMEs until it either adds a new STA or times out. Optionally, a STA in the Simple Connect SL may cache recently received CM_SC_JOIN.REQ MMEs in anticipation of its HLE placing it into the SC-Add state.
When a STA in the SC-Add state detects a CM_SC_JOIN.REQ MME, it responds to it with a CM_SC_JOIN.CNF MME. The STA that was in the SC-Add state then becomes the CCo of a new AVLN and starts issuing Beacons. When the STA in the SC-Join state detects the Beacons, it associates with the CCo, regardless of relative CCo capabilities. This case is distinguished from the case below in which two Unassociated STAs are in SC-Join by the STA in SC-Add setting the CCo Status field to 0b1. If the joining STA has greater CCo Capability, it will later become the CCo through autoselection of the CCo and the CCo Handover process (refer to Section 7.4.3 and Section 7.5).
After the new STA has associated with the new CCo, the two STAs optionally perform Channel Adaptation (refer to Section 5.2.6) to have channel adapted tone maps. Finally, the CCo shall start the UKE protocol. This first establishes a shared TEK, which is used by the CCo to provide the new STA with its NMK (refer to Section 7.10.3.5). When the new STA has the NMK, it shall authenticate and join the AVLN.
Note: The STA in SC-Add state will pass the NMK-SC it posses to the STA in SC-Join state. A random NMK-SC is not generated. A user may place an Unassociated STA in the SC-Add state if that STA had been part of an AVLN (in the SC security level) that is not currently present to add a new STA to that AVLN (i.e., to pass the NMK-SC of that AVLN to the new STA in SC-Join state). See also Section 7.10.3.1.2.
This entire process is shown in Figure 711.

Figure 711: AVLN Formation Using UKE by One STA in SC-Add and One STA in SC-Join

Two Unassociated STAs: Both in SC-Join

It is possible that both STA's HLEs can be placed in the SC-Join state. In this case, both will begin to transmit CM_SC_JOIN.REQ MMEs with their CCo capability using multinetwork broadcast. When a STA in SC-Join mode receives another STA's CM_SC_JOIN.REQ MME, it shall determine which STA should become the CCo as defined in Section 7.4.1. If it is the one to become the CCo, it shall change its state to SC-Add, generate a new random NMK-SC, send a CM_SC_JOIN.CNF MME to the other STA with its NID, establish itself as a CCo, and start issuing Central Beacons, forming a Neighbor Network if necessary. When the other STA receives

the CM_SC_JOIN.CNF MME and detects the Beacon with the same NID, it shall associate with the new CCo. The two STAs shall optionally perform channel adaptation prior to commencing the UKE protocol as above (refer to Section 7.3.4.3).
The STA that determines it should not become the CCo must wait for the other STA to send the CM_SC_JOIN.CNF MME and for that STA to begin issuing Central Beacon. In the meanwhile, the STA shall continue to send CM_SC_JOIN.REQ MMEs periodically in case the other STA did not correctly receive its earlier transmissions and hence does not know to send the CM_SC_JOIN.CNF MME and become the CCo of a new AVLN.
This entire process is shown in Figure 712.

Figure 712: AVLN Formation Using UKE by Two STAs in SC-Join

Joining an Existing AVLN

An Unassociated STA may join an existing AVLN when one of the following three conditions is met:

- It has the same NMK and Security Level and detects the AVLN's Central Beacon or the Discover Beacon of one of the STAs in the AVLN (refer to Section 7.3.5.1).
- One of the AVLN STAs sends the Unassociated STA its NMK encrypted with the Unassociated STA's DAK (refer to Section 7.3.5.2).
- The AVLN has an NMK-SC, the Unassociated STA's HLE indicates that it should enter the SC-Join state, and the HLE of a STA in the AVLN indicates that it should enter the SC-Add state (refer to Section 7.3.5.3).

In each of these cases, based on the initial information that is received or exchanged, the Unassociated STA will recognize that it needs to associate with an existing AVLN. After association, the STA proceeds with the protocol to receive the NMK for the AVLN if it does not already posses it. Upon successful reception of the NMK for the AVLN, the STA then authenticates using the NEK distribution protocol described in Section 7.3.3.

Matching NIDs

Two STAs with identical NMKs and identical Security Levels will also have identical default NIDs. Identical NIDs do not guarantee that the NMKs are identical, but the probability against this is very small. The NMK held by a STA may be associated with a non-default NID; in this case, the non-default NID associated with the NMK shall be used for matching purposes. The NID is advertised in the Central Beacon, Proxy Beacon, and Discover Beacons, so when an Unassociated STA receives one of these, it shall observe the matching NID.
The Unassociated STA must take the first step; the AVLN STAs (including the CCo) must wait for it to initiate the process. The Unassociated STA shall send the CCo a CC_ASSOC.REQ MME asking for an initial TEI within the AVLN. The CCo shall reply with a CC_ASSOC.CNF MME with STATUS=Success and a TEI assignment, unless it is out of TEIs or is in the process of transferring CCo status to another STA. In the latter cases, the CCo shall reply with STATUS=Defer, and the new STA will have to retry later.
Once the STA has associated with the CCo, it shall try to authenticate as described in Section 7.10.4.
This entire process is shown in Figure 713.

Figure 713: New STA Joins Existing AVLN with Matching NID

DAK-encrypted NMK

When a STA with a suitable User Interface (the UIS) already on an AVLN is provided with the DAK of another STA and told by the HLE to send the other STA its current NMK, the UIS shall transmit a CM_SET_KEY.REQ MME containing a TEK and encrypted with the DAK as the payload of a CM_ENCRYPTED_PAYLOAD.IND MME, sent unencrypted using multi-network broadcast. The STA need not be the CCo to do this; it is sufficient that it is in an AVLN.

All STAs that receive the MME shall try to decrypt it; if one succeeds, that successful STA shall respond with a CM_SET_KEY.CNF MME encrypted with the TEK as the payload of a CM_ENCRYPTED_PAYLOAD.IND MME, sent unencrypted, then it shall associate with the AVLN's CCo and complete the protocol as described in Section 7.10.3.4 A STA that fails to successfully decrypt a payload encrypted with a DAK shall ignore the message

When the DAK-encrypted NMK provisioning protocol is completed successfully, the new STA shall accept the NMK and SL, then shall try to authenticate with the CCo as described in Section 7.10.4 and join the AVLN.

This entire process is shown in Figure 714.

Figure 714: New STA Joins AVLN by DAK-Encrypted NMK

SC-Join and SC-Add

When the HLE places a STA into the SC-Join state, the STA shall transmit CM_SC_JOIN.REQ MMEs using multi-network broadcast periodically until it either joins an AVLN or times out. If the HLE places the STA into the SC-Add state, however, the STA shall not advertise this, but shall wait to hear another STA transmitting CM_SC_JOIN.REQ MMEs until it either adds a new STA or times out. Optionally, a STA in the Simple Connect SL may cache recently received CM_SC_JOIN.REQ MMEs in anticipation of its HLE placing it into the SC-Add state.

When the AVLN STA in the SC-Add state detects a CM_SC_JOIN.REQ MME, it shall respond with a CM_SC_JOIN.CNF MME. The STA need not be the CCo to do this; it is sufficient that it is in an AVLN. The new STA in the SC-Join state associates with the AVLN. At this point, the two STAs optionally perform Channel Adaptation (refer to Section 5.2.6.2) to have channel adapted tone maps.

Once the new STA has associated with the AVLN (and optionally established channel adapted tone maps), the AVLN STA shall start the UKE protocol. The AVLN STA knows the new STA has associated due to the updated TEI Map received from the CCo. The UKE protocol first establishes a shared TEK, which is used by the AVLN STA to provide the new STA with its NMK-SC (refer to Section 7.10.3.5). When the new STA has the NMK-SC, it shall try to authenticate with the CCo as described in Section 7.10.2.5 and join the AVLN.

This entire process is shown in Figure 715.

Figure 715: New STA Joins Existing AVLN Using UKE

SC-Join and SC-Add for GREEN PHY

When a STA is in the SC-Add state detects a CM_SC_JOIN.REQ MME, it will inform the HLE

using an APCM_SC_JOIN.REQ (refer to Section 12.2.2.52) and wait for the HLE to reply with an APCM_SC_JOIN.CNF. The STA with then reply to the new STA using CM_SC_JOIN.CNF MME containing the information from the APCM_SC_JOIN.CNF.

Leaving an AVLN

If the STA is powered down or instructed to leave the AVLN by the user, it shall notify to CCo of its departure as shown in Figure 716.

The STA shall wait until it receives an acknowledge response from the CCo before actually leaving. If it does not receive an ACK within 3 Beacon Periods, it will try to send the message a second time, after which it shall not use the TEI it had been assigned for any further communications with the AVLN (the CCo or any member STA).

If the user has overtly requested disassociation (note that power down is an implicit request, not an overt request), the user may also want to tell the STA to not try to re-associate with the AVLN in future. In this case, the STA must also change the NMK.

Figure 716: Disassociation - STA Leaves AVLN

When a STA leaves an AVLN (including TEI lease expiration), the CCo shall update all other STAs in the AVLN with the new TEI Map using the CC_SET_TEI_MAP.IND MME.

Removing a Station from an AVLN

The only secure way to remove a STA from an AVLN is to change the NMK (refer to Section 7.10.3.7. The DAK of the removed STA should be discarded.

A CCo may send a CC_LEAVE.IND MME to a STA to remove the STA from the AVLN. The CCo may also change the NEK and not provide the new NEK to the STA it wants to remove.

Selection of CCo

The first STA to instantiate a network becomes the CCo. As the network evolves with more STAs joining or leaving the AVLN, another STA may be more suitable to fulfill the role of CCo. The current CCo shall apply the CCo selection procedure on an ongoing basis to identify the best STA within the AVLN to perform the function. If a more suitable STA is identified by the selection process, the current CCo process must hand over the function to the STA selected by the Auto-Select function.

The CCo can be automatically selected and does not require the user to have any knowledge of the CCo function or its operation. This function is called Auto-Selection of the CCo. All STAs must support the Auto-Selection function.

Alternately, the STA operating as the CCo may have been appointed by the user through a UIS provided on the AVLN. The ability to provide a user interface for enabling the user to appoint the STA or another STA as a CCo is optional for the STA. All CCo's shall be capable of handing over CCo functionality when requested by another authenticated STA in the AVLN.

CCo Selection for a New AVLN

When an Unassociated STA determines that a new AVLN needs to be formed based on the MMEs it received, the STA shall determine whether it should become the CCo for the new AVLN based on the CCo Capability field and the OSA contained in those MMEs. Refer to Section 7.3.4 for more information about how a STA determines when a new AVLN needs to be formed.

If the CCo Capability of the Unassociated STA is greater than that of the other STAs detected, or if

the STA's MAC address is greater than the other STAs' when the CCo Capability is equal to the greatest capability detected, the STA shall become the CCo, possibly in Coordinated Mode if neighboring networks are detected, and begin transmitting the Central Beacon. For comparing MAC Addresses, the Individual/Group (I/G) bit of the 48-bit MAC address shall be treated as the least-significant bit in the least-significant octet.
An exception is an Unassociated STA that is in SC-Add state will always become the CCo (refer to Section 7.3.4.3).
Determination of SNID by a STA Acting as CCo in a Newly Formed AVLN (GREEN PHY)
When a new AVLN is formed by an unassociated STA and the unassociated STA has become the CCo of the AVLN, the STA (as the new CCo) shall randomly choose a SNID value which is not being used by any other AVLN heard during Power-On Network Discovery, and set the RSF and TEI Range according to the number of TEIs required. If all the SNID values are being used, the STA (as the CCo of the new AVLN) shall randomly select a SNID among those with RSF equal to one and set its own RSF to one. The TEI values of the STAs associated to this network shall be in the range of [0x01-0x3F], or [0x40-0x7F] or [0x80-0xBF] or [0xC0-0xFE] in order not to collide with the other AVLN with matching SNID.

User-Appointed CCo

The following procedure describes the user-appointed CCo process. Figure 717 shows this function.

- The user enters the MAC address of the STA that should be assigned the role of CCo. The user enters this MAC address into a UI made available by a STA that is already associated and authenticated with the network.
- The UI STA shall communicate with the existing CCo via a CC_CCO_APPOINT.REQ message, with the Request Type indicating a request to appoint a STA with the MAC address contained in the CC_CCO_APPOINT.REQ message as a user-appointed CCo (i.e., ReqType = 0x00).
- If the current CCo is a user-appointed CCo or the STA that needs to be appointed as a CCo is not part of the AVLN, the current CCo shall send CC_CCO_APPOINT.CNF indicating a failure. Otherwise, the current CCo responds by querying the appointed STA with a CC_HANDOVER.REQ message, requesting the STA to assume the role of the CCo. The message shall indicate that the handover is due to user appointment.
- The STA responds with a CC_HANDOVER.CNF message, where the STA either accepts the transfer of the CCo function or declines to do so.
- The current CCo passes on this response to the UI STA through the CC_CCO_APPOINT.CNF message. If the user-appointed STA is the same as the UI STA that sent the CC_CCO_APPOINT.REQ message, the existing CCo shall send a CC_CCO_APPOINT.CNF message to the UI STA with a successful code and initiate the handover function.

If the response from the appointed STA is positive, the existing CCo must initiate a CCo handover using the Handover function described in Section 7.5.
If the response is negative, no further action is required from the existing CCo.

- The current CCo shall carry out the remaining steps of the handover function (refer to

Section 7.5).

A user-appointed CCo shall not perform the Auto-Selection of the CCo function. The CCo role is only transferred when the current user-appointed CCo disassociates (or is powered down) from the network. All CCo-capable STAs shall store in non-volatile memory information about whether they are a user-appointed CCo for an AVLN. If a STA that is a user-appointed CCo disassociates from the AVLN and re-associates with it at some later time, it shall first determine whether the existing CCo of the AVLN is user appointed. If the existing CCo is not a user-appointed CCo, it shall become the CCo by following the procedure described above.

A user-appointed CCo can be un-appointed as a user-appointed CCo by transmitting a CC_CCO_APPOINT.REQ message with a Request Type indicating un-appointment of the existing CCo as a user-appointed CCo (i.e., ReqType = 0x01). Upon un-appointment as a user-appointed CCo, the CCo shall continue to act as a CCo and start performing Auto-Selection of the CCo function. The CC_CCO_APPOINT.REQ message with ReqType = 0x01 can also be sent to any STA in the AVLN that is not acting as a CCo, but is configured to act like a user-appointed CCo. Such scenarios can occur when the user inadvertently appoints more than one STA in the AVLN as a user-appointed CCo. If a STA in the AVLN that is not acting as a CCo receives the CC_CCO_APPOINT.REQ message with ReqType = 0x01 , it shall cause the STA to un-appoint itself as a user-appointed CCo and respond with a CC_CCO_APPOINT.CNF message.

A user-appointed CCo can be un-appointed as a user-appointed CCo and a new STA in the AVLN can be appointed as a user-appointed CCo by transmitting a CC_CCO_APPOINT.REQ message with Request Type indicating a simultaneous un-appointment of the existing CCo as a user-appointed CCo and transfer the CCo functionality to a new user-appointed CCo (i.e., ReqType = 0x02).

Un-appointment of a user-appointed CCo shall only be performed by the user (or Host). Thus, CC_CCO_APPOINT.REQ MMEs with Request Type 0x01 and 0x02 shall only be generated by the Host.

The user-appointed CCo status field in the Discover Info BENTRY shall be used by STAs to notify their user-appointed CCo status to all other STAs in the AVLN. This information can be used by STAs to determine whether the existing CCo is a user-appointed CCo. This information can also be used to detect the presence of multiple user-appointed CCos in the AVLN.

Figure 717: User-Appointed CCo

Informative Text
The user-appointed CCo selection method may result in undesirable consequences, such as disruption of ongoing Connections, reduction in coverage within the home, no connects, and so on. Since this option requires the user to understand the CCo function, it is recommended that the option be provided only to advanced users.

Auto-Selection of CCo

The current CCo, unless user appointed, must analyze the Topology Table for the AVLN at least once every MaxDiscoverPeriod duration. The rules of precedence described below apply to all STAs in the AVLN to rank their suitability in assuming the CCo function. If the CCo identifies a

STA in the Topology Table that ranks higher, the CCo shall initiate the CCo handover procedure to that STA. Refer to Section 7.5.

If there is a tie in the rank of STAs in the network for choice of successor CCo, the CCo may select one of the tied STAs at random to become the new CCo. The current CCo shall not hand over the CCo role to any STA that is ranked below its own rank. The current CCo may hand over the CCo role to any STA that has a rank that is the same as its own rank. Under such conditions, implementations must ensure that CCo functionality does not continuously transfer between STAs that have the same rank as the CCo.

CCo Capability

Every STA shall perform the mandatory functions required of a STA. However, manufacturers may differentiate STAs based on implementation attributes or other criteria (e.g., differentiated CCo-capability as described below). The CCo capability of each STA shall be classified into four categories (refer to Section 4.4.3.15.4.6.2):

- **Level-0 CCo:** Level-0 CCo does not support QoS (i.e., cannot schedule any contention-free allocations). The mandatory functions of a Level-0 CCo are:

AC Line Cycle Synchronization (refer to Section 5.1.1).

All mandatory functions defined in Chapter 7, except Bandwidth Management (Section 7.8).

CSMA-Only mode of operation with Passive Coordination (Chapter 8).

All mandatory HomePlug 1.0.1 Coexistence functions defined in Chapter 9.

- **Level-1 CCo**: Level-1 CCo supports QoS when operating in Uncoordinated mode. The mandatory functions of a Level-1 CCo are:

All mandatory functions of Level-0 CCo.

All of the mandatory Bandwidth Management functions defined in Section 7.8

- **Level-2 CCo**: Level-2 CCo Capable STA supports Coordinated mode of operation. The mandatory functions of a Level-2 CCo are:

All mandatory functions of a Level-1 CCo.

Coordinated mode of operation in the presence of a Neighbor Network.

- **Level-3 CCo:** Level-3 CCo is a future-generation CCo.

An AVLN with a Level-x CCo is also referred to as Level-x AVLN throughout the specification. All STAs shall be capable of operating as a STA in a Level-0, Level-1, or Level-2 AVLN. The CCo capability of each STA shall be provided to the CCo in the CC_ASSOC.REQ message at the time of association. Every STA shall also declare its CCo capability in its Discover Beacon transmission. The CCo shall maintain the CCo capability of each associated STA in the network in its Topology Table. The CCo capability of the CCo of an AVLN is indicated in all Central, Proxy, and Discover Beacons.

Order for Selection of CCo

The order of precedence used by the Auto Selection function to identify the most suitable STA in the AVLN to assume the role of CCo is shown in Table 73.

- STA capability is the highest criterion for ranking STAs. This criterion is mandatory. A STA with Level-1 CCo capability is ranked higher than a STA with Level-0 capability and so on.
- The number of STAs in the Discovered STA List of a STA is the next-highest criterion in

ranking a STA's suitability. This criterion is optional. The STA in the network that supports bi-directional Links with the maximum number of STAs provides the best coverage and may be deemed suitable to be a CCo. The STA in the Topology Table with the largest number of STAs in its Discovered Station List should be ranked the highest in this criterion. Ties would be broken by giving preference to the STA that was in the Discovered Station List of the most other STAs.

- The number of networks discovered by a STA is the next most important ranking criterion. This criterion is optional. The STA in the network that discovers the largest number of neighbor networks may be deemed suitable to be a CCo to coordinate with the neighbor networks. The STA in the Topology Table with the largest number of entries in the Discovered Network List is preferred.

Table 73: Order of Precedence in Selection of CCo

Order	Criteria	Note
1	User-appointed CCo (Optional)	If the user-appointed STA accepts the CCo function, this STA remains the CCo.
2	CCo Capability (Mandatory)	Level-3 CCo ranks the highest, followed by Level-2 CCo, followed by Level-1 CCo, followed by Level-0 CCo.
3	Number of discovered STAs in the Discovered Station List (Optional)	Higher is preferred
4	Number of discovered networks in the Discovered Network List (Optional)	Higher is preferred

Transfer/Handover of CCo Functions

The transfer of the CCo function from the current CCo to another STA (or the new CCo) in the network is shown in Figure 718. The handover may be initiated when the user has appointed a new CCo or a new CCo is selected by the Auto-Selection process. The handover might not be initiated if any other change involving a Beacon countdown is in progress (e.g., Schedule change, NEK change, Beacon relocation, etc.)

Every CCo shall support "hard handover": every CCo-capable STA shall be able to take over the role of the current CCo when requested and start transmitting Beacons for the network when the handover countdown expires.

The current CCo and the new CCo may optionally exchange CSPEC and BLE information about active Connections in the network during the handover process so that the new CCo may be able to maintain uninterrupted service at the agreed upon QoS level for those Connections. This optional process is called "soft handover."

The following steps describe the handover process:

- The current CCo shall send a CC_HANDOVER.REQ message to the STA, requesting it to

Informative Text

It might not be possible to maintain uninterrupted service at the agreed-upon QoS level, even if

- active the role of the CCo. The message indicates whether a soft handover is requested.
- The STA responds with a CC_HANDOVER.CNF message where the STA either accepts the transfer of the CCo function or declines to do so.

If the STA rejects the request, the handover process is deemed to have failed. If the new CCo selection was based on the Auto-Selection process, the CCo may start a new CCo handover process with another station in the AVLN.

If the STA accepts the request, the current CCo shall continue with the following steps.

- The current CCo shall set the Handover-In-Progress (HOIP) bit in the Beacon to indicate that handover is in progress. When this bit is set, STAs and neighbor CCos shall wait before sending new association requests or bandwidth requests to the current CCo. Refer to Section 4.4.3.11.
- If it is a soft handover, the current CCo shall send a **CC_LINK_INFO.IND** message to the new CCo to transfer the CSPEC and BLE information about all Global Links in the AVLN. The new CCo acknowledges the proper reception of this message using **CC_LINK_INFO.RSP**. If it is a hard handover, **CC_LINK_INFO.IND/RSP** messages are not exchanged.
- The CCo shall initiate a transfer of relevant network information to the new CCo via the CC_HANDOVER_INFO.IND message. The message includes an indication that this message is transmitted as part of a CCo handover, the identity of the Backup CCo (if any) (refer to Section 7.9), and the list of associated and authenticated STAs in the network. The new CCo shall send a **CC_HANDOVER_INFO.RSP** message to indicate successful reception of **CC_HANDOVER_INFO.IND**.
- The current CCo shall begin a handover countdown using the CCo Handover BENTRY (refer to Section 4.4.3.15.4.9).
- When the countdown expires, the current CCo shall stop transmitting the Beacon and the new CCo shall take over the Beacon transmission.
- The new CCo transmits the Beacon Time Stamp in its Beacons based on either its own STA_Clk or NTB_STA from the old CCo (refer to Section 5.5). Since the Network Time Base used by the new CCo can be different than the Network Time Base of the old CCo, all STAs in the AVLN with active CIDs should apply a correction to their timing based on the observed difference between the two BTSs in the last transmission of the old Beacon and the first transmission of the new Beacon.
- If it is a soft handover, the new CCo shall also maintain the persistent schedule of the last Beacon transmitted by the “old” CCo.
- The new CCo shall also reset the HOIP bit in the Beacon.
- All STAs in the AVLN shall renew their TEIs (refer to Section 7.3.2.1.2) subsequent to a CCo handover.

Figure 718: Transfer of CCo Function

Informative Text
It might not be possible to maintain uninterrupted service at the agreed-upon QoS level, even if soft handover is used. Until the new CCo obtains detailed information about CSPECs, line cycle-dependent TMs, etc., it will not have sufficient information to make correct scheduling decisions. There may also be connectivity issues that will need to be resolved (e.g., appointment of new PCos) for proper communication of schedules and connection requirements.

Discover Process

Overview

The Discover Process is a periodic, low-overhead background process that is ongoing within the network where each associated and authenticated STA takes turn in transmitting a Discover Beacon as instructed by the CCo.

The purposes of the Discover Process are:

To allow the CCo and STAs to determine the identity and capability of other STAs in the network. Each STA creates and updates its Discovered STA List as an output of this function.

To allow the CCo to discover networks that it cannot detect directly. Each STA creates and updates a Discovered Network List as an output of this function.

The Discovered STA Lists and Discovered Network Lists of the CCo and of all STAs are used by the CCo to create the Topology Table which is used by the CCo in the CCo-selection process.

To allow HSTAs (i.e., STAs that cannot directly detect the Central Beacons transmitted by the CCo, but can detect Discover Beacons transmitted from certain STAs) to communicate with the CCo and to associate and authenticate with the network with the STA transmitting the Discover Beacon acting as a proxy to relay MMEs.

Discover Beacons

A Discover Beacon is a special type of Beacon that is transmitted by an associated and authenticated STA in the network during the Discover Process. It contains information including the NID of the network, the TEI, the MAC address (using the MAC Address BENTRY, Section 4.4.3.15.4.4), and the number of discovered STAs and networks and the CCo capability (using the Discovered Info BENTRY, Section 4.4.3.15.4.6) of the transmitting STA.

The Discover Beacon contains a copy of the Regions BENTRY and Schedule BENTRIES of the Central Beacon. Schedule BENTRIES provide the locations of the persistent and non-persistent CSMA allocations as well as all the CF allocations in the Beacon Period. HSTAs that can detect the Discover Beacon can use this information to exchange association and authentication messages with the CCo, using the STA transmitting the Discover Beacon as a relay. Refer to Section 7.7 for more details on association of HSTAs.

Each STA shall update its Discovered STA List and Discovered Network List when it detects a Discover Beacon from another STA.

The CCo shall interpret the Discovered Info BENTRY contained in the Discover Beacon. If the BENTRY indicates that the content of the Discovered STA List or Discovered Network List has been updated recently, the CCo may choose to query the STA transmitting the Discover Beacon for the latest Discovered STA List and Discovered Network List.

Discovered STA List and Discovered Network List

Each STA shall record the identity and attributes of every STA (from its own network and from

different networks) whose Discover Beacons it can decode correctly. This information is maintained in the Discovered STA List. The Discovered STA List contains the MAC address of the STA that was heard, a flag to indicate whether the discovered STA is associated with the same or a different network, and the Short Network Identifier (SNID) (refer to Section 4.4.1.4) of the network with which the discovered STA is associated. The CCo, PCo, and Backup CCo capability and corresponding status of the transmitting STA shall also be recorded. The Signal Level and Average BLE may optionally be recorded. This optional information may be used by the CCo to determine whether or not to coordinate with another CCo or Group. The Discovered STA list shall be updated every time the STA receives a Discover Beacon from another STA. An example of a Discovered STA List for STA A in Figure 719 is {MAC ADDRESS(CCo), MAC ADDRESS(B), MAC ADDRESS(C), MAC ADDRESS(E)}. STA D is not in this list, as STA A cannot detect transmissions accurately from STA D.

Each STA shall also maintain a Discovered Network List. This list shall be updated when the STA receives and decodes a Central, Proxy, or Discover Beacon with an NID (refer to Section 4.4.3.1) that is different from the NID of its own network. Each entry of the Discovered Network List contains the NID, SNID, network mode, hybrid mode flag, number of Beacons Slots (refer to Section 4.4.3.7), and start time of the Beacon Region of that network relative to the start of the Beacon Period.

An aging mechanism shall also be implemented to remove stale entries from the Discovered STA List and Discovered Network List. An entry from the Discovered STA List shall be removed if a Discover Beacon or other transmission from that STA has not been detected for at least Discovered_List_Expire_Time. An entry from the Discovered Network List shall be removed if a Central, Proxy, or Discover Beacon or other transmission from that network has not been detected for at least Discovered_List_Expire_Time.

Note: For each unique network discovered, the STA may have received Central, Proxy and Discover Beacons from more than one STA of that network. Even if this is the case, there shall be only one entry for that network in the Discovered Network List.

Topology Table

The CCo maintains a Topology Table, which is a composite of the Discovered STA Lists and the Discovered Network Lists of all the STAs and HSTAs associated and authenticated with the CCo, together with the CCo's own Discovered STA List and Discovered Network List. The Topology Table shall contain the MAC addresses of all STAs and the Network Identifiers of all networks discovered by every STA and HSTA associated and authenticated with the CCo.

The CCo shall use its Topology Table to make decisions such as identifying HSTAs, identifying suitable PCos and establishing PxNs, and determining which STA can best fulfill the role of the PCo. The CCo may also use the Topology Table to determine the scope of a broadcast (i.e., which STAs can receive the BCAST/MCAST from the broadcasting STA) and whether bi-directional Connections can be established between STAs requesting such a point-to-point or point-to-multipoint Connection.

The CCo may use the Topology Table to try to avoid interfering with a neighbor network with which it is not coordinating directly. If a STA in the network reports a non-coordinating network in its Discovered Network List, it is recommended that the CCo refrain from scheduling any

contention-free allocations that overlap with the Beacon Region or the minimum CSMA Region of any non-coordinating network. Refer to Section 5.2.5

Figure 719 and Table 74 show an example of a Topology Table for the AVLN “Network 1”.

Table 74: Example of Topology Table

List of Associated and Authenticated STAs	Discovered STA Lists	Discovered Network Lists
MAC ADDRESS(CCo)	{MAC ADDRESS(A), MAC ADDRESS(B), MAC ADDRESS(C)}	{NID(NCo)}
MAC ADDRESS(A)	{MAC ADDRESS(CCo), MAC ADDRESS(B), MAC ADDRESS(C), MAC ADDRESS(E)}	{empty}
MAC ADDRESS(B)	{MAC ADDRESS(CCo), MAC ADDRESS(A), MAC ADDRESS(C), MAC ADDRESS(D), MAC ADDRESS(E)}	{empty}
MAC ADDRESS(C)	{MAC ADDRESS(CCo), MAC ADDRESS(A), MAC ADDRESS(B), MAC ADDRESS(D)}	{empty}
MAC ADDRESS(D)	{MAC ADDRESS(B), MAC ADDRESS(C), MAC ADDRESS(E)}	{empty}
MAC ADDRESS(E)	{MAC ADDRESS(A), MAC ADDRESS(B), MAC ADDRESS(D)}	{empty}

Discover Period

The CCo shall schedule each and every associated and authenticated STA in the network and the CCo itself to transmit a Discover Beacon at least once in MaxDiscoverPeriod.

Procedures

The Discover Process consists of the following steps:

At least once in every Discover Period, the CCo shall schedule an opportunity to transmit a Discover Beacon for every associated and authenticated STA in the network (including HSTAs) and the CCo itself. In Uncoordinated and Coordinated modes, a special contention-free allocation (refer to Section 5.2.1.4.1) is provided using Non-Persistent Schedule BENTRY to specify the location where a Discover Beacon shall be transmitted. In CSMA-Only mode, the STA sends a Discover Beacon using CSMA/CA channel access at CAP2. The Discover BENTRY (refer to Section 4.4.3.15.4.2) is used to identify the STA that transmits the Discover Beacon. The CCo shall not include more than one Discover BENTRY in each Central Beacon.

The STA identified by the Discover BENTRY shall construct and broadcast a Discover Beacon

when scheduled by the CCo.
Every STA that receives a Discover Beacon and is able to correctly decode the Beacon shall update its own Discovered STA List with the MAC address of the STA transmitting the Discover Beacon. The receiving STA shall also record the CCo capability of the STA transmitting the Discover Beacon. Every STA may also update its Discovered STA List every time it decodes a transmission from another STA successfully, in addition to the updates based on receipt of Discover Beacons.
Periodically, the CCo shall query all STAs associated with the CCo, including HSTAs, to obtain their individual Discovered STA Lists and Discovered Network Lists. The CCo shall construct and update its Topology Table using this information. The CCo sends a CC_DISCOVER_LIST.REQ message to a STA to query for its Discovered STA List and Discovered Network List. The STA responds with the information in a CC_DISCOVER_LIST.CNF message. STAs in the AVLN shall also send the CC_DISCOVER_LIST.IND message to the CCo in an unsolicited manner when they detect a new neighboring AVLN.
Proxy Networking with GREEN PHY Extensions to Support Routing and Repeating
Proxy Networking in GREEN PHY is an extension from Proxy Networking in HomePlug AV 1.1. The extensions add support for multiple levels of Proxy Coordinators and also support routing and repeating functionality.
Every STA in the AVLN must be able to communicate directly or indirectly with the CCo. All STAs are free to communicate with other STAs in the same AVLN, provided the power line channel characteristics between the two communicating STAs permit communication, but such communication is not required.
A Hidden STA (HSTA) is a STA that cannot communicate directly with the AVLN's CCo and, as a result, must communicate indirectly, relaying messages via a proxy. By definition, an HSTA cannot hear the Beacons transmitted by the CCo; it can, however, infer the existence of the AVLN from Discover Beacons transmitted by other STAs or Proxy Beacons transmitted by Proxy Coordinators (PCos). The HSTA uses information from these Beacons to learn the identity of the AVLN and to identify a Proxy STA (PSTA), see below, or existing PCo to relay messages to/from the CCo. A PSTA or PCo that cannot communicate directly with the AVLN's CCo shall route messages to the CCo based on the LRT.
Once the CCo receives a message and becomes aware of the HSTA, it appoints a STA (possibly the PSTA) as a PCo. From that point on, all messages will be relayed between the HSTA and the CCo via the PCo, routing the relay messages based on the LRT when necessary.
A Proxy Network (PxN) is a network established by the CCo when it appoints a PCo to support one or more HSTAs. A Proxy Network (PxN) is always associated with an existing AVLN and is a wholly contained part of the AVLN. It consists of a PCo (appointed by the CCo) and one or more HSTAs. PxNs are strictly the concern of the AVLN to which they belong. Multiple networks that are neighbors may each independently support PxNs.
All operations of the HSTAs are controlled by the CCo with the PCo serving as a relay. Since the HSTA must obtain information contained in the CCo's Beacon, the PCo shall transmit a Proxy Beacon (refer to Section 7.7.4) once every Beacon Period. In Uncoordinated and Coordinated modes, the CCo shall specify TDMA allocations in which the Proxy Beacons need to be

transmitted. During CSMA-Only mode, the Proxy Coordinator should transmit the Proxy Beacon using CSMA/CA at CAP3 as soon as the Central Beacon from CCo is received.
Figure 719 shows an example of Network 1 containing a PxN. Within the PxN, STA B is the PCo, and STAs D and E are HSTAs.

Figure 719: Proxy Network Created By Network 1
Proxy networking is an optional feature. Proxy Networking includes STAs functioning as Hidden Stations, Proxy Stations, Proxy Coordinators, and Central Coordinators. All these features are optional. In the remainder of this section, the terms Hidden Station, Proxy Station, Proxy Coordinator, and Central Coordinator refer to STAs that support the optional Proxy networking feature. Each STA shall advertise in its Discover Beacon whether it supports Proxy Networking. When a STA announces in its Discover Beacon that it is unable to support Proxy Networking, HSTAs or the CCo shall not transmit CC_RELAY MMEs or the CP_PROXY_APPOINT MMEs to that station.
Identification of Hidden Stations
If the STA cannot hear a CCo's Beacon, but can determine the existence of the AVLN from Discover Beacons or Proxy Beacons, it knows it is an HSTA. If the HSTA hears a Proxy Beacon, it shall request that PCo to relay its messages to the CCo. If the HSTA does not hear a Proxy Beacon, it shall select a STA from among those from which it has heard Discover Beacons, and ask that STA to serve as a PSTA and relay its initial message to the CCo. The HSTA should select a PCo or STA with the lowest Plevel.
When the CCo receives the first relayed message from a NewHSTA, it recognizes that there is a new HSTA that wishes to associate with the AVLN. The method by which the CCo receives the association request message from the HSTA is described in Section 7.7.2. The accurate decryption and interpretation of the association request message from the HSTA informs the CCo of the presence of an HSTA in the network.
Before responding to the HSTA's association request message, the CCo shall appoint a PCo to support the HSTA as described in 7.7.3.
Association of Hidden Station
The association of a new STA which is in range with the CCo is described in Section 7.3.2. When the new STA (or more appropriately a New Hidden STA (NewHSTA)) is out of range of the CCo, it shall perform the association described below and shown in Figure 720.
Note: The fundamental association messaging is identical for both STAs and HSTAs. The only difference for a NewHSTA is the encapsulation of the messages within CC_RELAY.REQ/IND messages and the insertion of the CP_PROXY_APPOINT.xxx messaging between the CC_ASSOC.REQ and the CC_ASSOC.CNF messages.
The new STA shall encapsulate the CC_ASSOC.REQ MME within a CC_RELAY.REQ MME and send it to the PCo or the PSTA. If the HSTA does not know the CCo's TEI or MAC address, it shall set the FDA and FTEI field to the broadcast MAC address and TEI respectively. Otherwise, it shall set the FDA and FTEI field to the MAC address and TEI of the CCo.
The PCo or the PSTA shall decapsulate the CC_ASSOC.REQ MME, re-encapsulate it inside a CC_RELAY.IND MME. The values of the OSA and OTEI fields inside the CC_RELAY.IND

MME are set to the MAC address of the NewHSTA and the TEI used by the NewHSTA (which is 0x00). The PCo shall send the CC_RELAY.IND MME to the CCo. Normally the PCo would use the FDA and FTEI fields of the CC_RELAY.REQ MME to address the CC_RELAY.IND MME but in this case, the NewHSTA could not supply them. The PCo can identify the destination by virtue of the fact the OTEI field is 0x00 (new STA) and recognize that the only STA that can be addressed when the STEI = 0x00 is the CCo (refer to Section 7.3.2.1).
The CCo shall extract the Payload field of the CC_RELAY.IND MME and process the association request.
If it determines to accept the association request, the CCo shall appoint a PCo, as described in Section 7.7.3. The messaging for PCo appointment shall occur before the CCo replies to the association request.
After appointing a PCo, the CCo shall create a CC_ASSOC.CNF MME and encapsulate it inside a CC_RELAY.REQ MME. The FDA and FTEI fields inside the CC_RELAY.REQ MME are set based on the OSA and OTEI fields inside the CC_RELAY.IND MME. The CCo shall send the CC_RELAY.REQ MME to the newly appointed PCo.
If the association request is rejected, the CC_ASSOC.CNF MME shall be encapsulated as just described and sent to the PSTA that relayed the original CC_ASSOC.REQ MME.
If the association request is accepted, the CC_ASSOC.CNF MME contains the TEI assigned to the new STA and the lease time.
The PCo or the PSTA shall extract the CC_ASSOC.CNF MME from the CC_RELAY.REQ MME, encapsulates it inside a CC_RELAY.IND MME and sends it to the NewHSTA. The FDA and FTEI fields inside the CC_RELAY.REQ MME provide the required addressing information to send the CC_RELAY.IND MME.

Figure 720: HSTA Association

Instantiation of Proxy Network

A PxN is established when the CCo appoints a PCo to support one or more HSTAs. The PxN consists of the PCo and the HSTA(s) that it supports.
A PxN is established when:
The CCo learns of the presence of an HSTA through relay of a CC_ASSOC.REQ MME from a PSTA. There are two sub-cases:
A STA that cannot hear the CCo joins the AVLN for the first time.
A STA that is already authenticated becomes unable to hear the CCo because of changing channel conditions.
The CCo decides to change the PCo because:
The PCo STA is leaving (or has left) the AVLN, or
The CCo determines that another STA is better suited to being the PCo for this particular PxN.
The CCo may also choose to reassign HSTAs from one PxN to another PxN. The CCo should attempt to minimize the number of PxNs that it creates. This may require it to reconfigure PxNs (e.g., combine two or more PxNs into a single PxN) as the Discovery Process progresses.

Selecting a PCo

The determination of which STA to assign as a PCo is an implementation decision. The only

requirement is that the PCo must be able to communicate bi-directionally with both the CCo and the HSTA.

Initially, the PSTA may be the only choice for the PCo of a NewHSTA. Once the NewHSTA has been admitted to the network and begun partaking in the Discovery Process, the CCo may determine that another STA is better suited (e.g., because it can support more HSTAs than the current PCo).

The CCo assigns a STA to the role of PCo by sending it a CP_PROXY_APPOINT.REQ MME, giving it the particulars of the assignment. The designated STA has the option of accepting or refusing the PCo service role. It shall notify the CCo of its decision via the CP_PROXY_APPOINT.CNF MME.

It the STA accepts the PCo role and if the ReqType = Add, the PCo shall notify the HSTA(s) it has assumed responsibility for via the PH_PROXY_APPOINT.IND.

PCo-Required Tasks

The PCo shall relay management messages between its assigned HSTA(s) and the CCo. The PCo is only required to relay MMEs which are encapsulated in a CC_RELAY.REQ MME addressed to it. The PCo shall de-encapsulate the MMEs and re-encapsulate them in a CC_RELAY.IND MME and send them to their destination, routing them based on the Local Routing Table (LRT – see Section 5.8.1.1) when necessary.

The PCo shall also broadcast a Proxy Beacon (Section 7.7.4) once during each Beacon Period in an allocation specified by the CCo and identified by a GLID. When a PCo cannot reliably detect the CCo, it shall select a PCo with the lowest Plevel that it can reliably detect. In Uncoordinated and Coordinated modes, the selected PCo shall specify TDMA allocations in which the Proxy Beacons need to be transmitted. During CSMA-Only mode, the PCo should transmit the Proxy Beacon using CSMA/CA at CAP3 as soon as the Proxy Beacon from the selected PCo is received.

Proxy Beacons

A Proxy Beacon is a special type of Beacon that is transmitted by a PCo once every Beacon Period. It provides timing and schedule information for the HSTAs in the PxN. It contains the TEI of the transmitting STA (the PCo) and the Network ID of the network. It also contains any other BENTRYs found in the current Beacon, with the exception that the PCo may optionally omit an entire BENTRY (refer to Table 4-66).

Provisioning the NMK to Hidden Stations

If the HSTA and the UIS are within range of each other, the provisioning of NMK to a HSTA is the same as described in Section 7.10.3. The HSTA may receive the broadcast message a second time, relayed from its PCo; it shall ignore this duplicate message.

If the HSTA and the UIS are not in rage of each other, the PCo's Relay functions will support NMK provisioning automatically.

All Encryption Key management methods rely on Encrypted Payloads, so they may be relayed freely and securely without intermediate knowledge of any encryption keys. Furthermore, all of the NMK provisioning methods begin with a broadcast CSMA message, which the PCo will encapsulate and relay to its HSTAs, as described in Section 7.7.7.

If the HSTA elects to respond to the broadcast message, the HSTA shall encapsulate its response (the encrypted payload MME) in a CC_RELAY.REQ MME and send it to the PCo which shall

relay it to the UIS. The UIS shall process the MME encapsulated in the CC_RELAY.IND MME it receives as if it had been received directly except that it shall encapsulate its reply in a CC_RELAY.REQ MME that it sends to the PCo. The HSTA and the UIS shall continue encapsulating their messages in the CC_RELAY.REQ MMEs for the duration of the protocol run. The PCo shall act as a relay for these messages.

Provisioning NEK for Hidden Stations (Authenticating the HSTA)

There is no difference in the process for an HSTA joining the AVLN than for any other STA except that the messages in the protocol run (Section 7.10.4) shall be encapsulated in CC_RELAY.xxx MMEs and relayed via the PCo.

Once the HSTA has been authenticated, the CCo shall send a CP_PROXY_APPOINT.REQ (ReqType=Update) to tell the PCo that the HSTA is authenticated.

An HSTA may communicate with any other STA in the AVLN (subject to powerline channel characteristics) once the HSTA is associated and been authenticated by the CCo via the PCo.

Exchange of MMEs Through a PCo

Only MMEs destined to or originated from a CCo shall be relayed through a PCo. Data transmission is not permitted using the CC_RELAY.IND/RSP **MMEs**.

Other MMEs may be routed as defined in Section 5.8

All CC_RELAY.REQ MMEs shall be encrypted with the NEK unless the transmitting STA is not yet part of the Network. STAs that are not yet part of the network are permitted to send CC_RELAY.REQ MMEs unencrypted.

The PCo shall encrypt each CC_RELAY.IND MME using the NEK unless it is directed to a station that has not yet been authenticated into the AVLN. The PCo shall broadcast any unencrypted CC_RELAY.IND MME that contains a CM_ENCRYPTED_PAYLOAD.IND. This is necessary so that the UIS can monitor the Protocol Run for an MITM attack. The HSTA shall not accept a CC_RELAY.IND MME that contains an CM_ENCRYPTED_PAYLOAD.IND message unless it is broadcast.

Transitioning from Being a STA to Being an HSTA

It is possible that an existing STA may no longer be able to decode the CCo's Beacons reliably. This might occur because channel conditions have changed significantly. It might also occur after a CCo handover if the existing STA is no longer within range of the new CCo. When this happens, the existing STA shall re-associate with the CCo through a PSTA (or existing PCo). The procedure is the same as the association procedure for a HSTA (Section 7.7.2), except the ReqType field in the CC_ASSOC.REQ message (refer to Section 11.2.28) shall indicate that it is a renewal request. Since the message was delivered to the CCo in a CC_RELAY.IND MME, the CCo shall assign a PCo to support the new HSTA and then process the TEI renewal request normally.

Transitioning from Being an HSTA to Being a STA

It is possible that an existing HSTA can decode the CCo's Beacons reliably. This might occur because channel conditions have changed significantly. It might also occur after a CCo handover if the existing HSTA is within range of the new CCo. When this happens, the existing STA shall re-associate with the CCo directly. The procedure is the same as the association procedure for a STA (Section 7.3.2) except that the ReqType field in the CC_ASSOC.REQ message (refer to Section

11.2.28) shall indicate that it is a renewal request.
Since the message was received directly from a STA that the CCo knows as hidden, the CCo shall remove the STA from the PCo's list of supported HSTAs using the CP_PROXY_APPOINT.REQ message with a ReqType of "Delete." If the PCo now has no more HSTAs assigned to it, the CCo shall shut down the PxN, as described in Section 7.7.11.
Recovering from the Loss of a PCo
It is possible for the PCo to drop out of the network without warning, either due to equipment failure or because the user unknowingly unplugged the STA that was serving as PCo. In this case, the HSTA will observe that it is no longer receiving Proxy Beacons from its PCo. When its schedule expires, it shall select another PSTA (or PCo) and reassociate with the CCo using the procedure described in Section 7.7.8. The CCo shall notice that the TEI of the relay device is different than the TEI of the HSTA's assigned PCo and shall assign the HSTA to a new PCo.
Proxy Network Shutdown
Once established, the PxN shall continue until the PCo is instructed by the CCo to halt PCo functions. Instruction for this occurs via the CP_PROXY_APPOINT.REQ message with a ReqType = Shutdown.
The CCo shall shutdown the PxN when all of the HSTAs assigned to the PCo have:
Disassociated,
Had their TEI leases expire,
Been transferred to another PCo, or
Transitioned from being an HSTA to a STA
Proxy Network Limitations
Proxy Networking suffers from the following limitation:
Some bandwidth-management metrics (e.g., BLEs, queue depth) are in the Frame Control; the CCo will not hear them and will not be able to provide full bandwidth-management services. A STA may provide the CCo with BLE information using the **CC_BLE_UPDATE**.IND message sent via relay.
Bandwidth Manager
The main functions performed by the Bandwidth Manager in the CCo are:
Scheduling and Bandwidth Allocation to Connections: The CCo receives requests from STAs in the network, requesting bandwidth assignments for Connections. In response, the CCo must assign a Global Connection ID (GLID) and schedule allocations to the Connection. The traffic characteristics, QoS guarantees, MAC services, and MAC parameters specific to a Connection are defined in the Connection Specification (CSPEC). Sounding and Channel Estimation results are used by the Bandwidth Manager in making allocations to Connection requests.
Admission Control: When the CCo receives the connection establishment or connection-reconfiguration requests from a STA, the Bandwidth Manager must determine whether there is adequate bandwidth available to support the request, without compromising the QoS of existing Connections. The Bandwidth Manager is responsible for either accepting or rejecting the requests.
Beacon Period Configuration and Beacon Transmission: The Bandwidth Manager must determine the allocations within a Beacon Period. It assembles and broadcasts the Beacon once every Beacon Period.
Connection Specification (CSPEC)

Connection Specification contains the set of parameters that define the characteristics and QoS expectations of a Connection. Connections can be either unidirectional or bi-directional. For bi-directional Connections, the Connection Specification for both the Forward Link and Reverse Link is contained in the CSPEC.
The format of the CSPEC is shown in Table 75. The first two octets of the CSPEC indicate the length (in octets) of the CSPEC information to follow.
The CSPEC of each Link is composed of two parts:
The Connection Information (CINFO)
The QoS and MAC parameters (QMP)

Table 75: Format of Connection Specification (CSPEC)

Field	Octet Number	Field Size (Octets)	Definition
CSPEC_LEN	0 - 1	2	Length of CSPEC, including the 2-octet CSPEC_LEN field 0x0000 = 0 octets, and so on
CINFO (Forward)	-	1 or 5	Forward Connection Information
CINFO (Reverse)	-	1 or 5	Reverse Connection Information
QMP (Forward)	-	Var	Forward QoS and MAC Parameters Only present if Connection requires a Forward Link
QMP (Reverse)	-	Var	Reverse QoS and MAC Parameters Only present if Connection requires a Reverse Link

CINFO identifies the attributes of the Connection and the MAC and PAL operations required by the Connection at the source and destinations STAs. The format of the CINFO fields is shown in Table 76. A separate CINFO field is required for the forward and reverse directions of the Connection.
The CINFO, QoS, and MAC parameter fields specifically apply to the forward or Reverse Links, as indicated in the CSPEC.

Table 76: Format of Connection Information (CINFO)

Field	Octet	Field Size (Octets)	Description	Reconfigurable
Valid CINFO	0	1	0x00 = contention-free service. In this case, connection setup shall fail if the requested Global Link(s) are not established. 0x01 = Valid CINFO shall be set to 0x00 if the corresponding link is not present. If Valid CINFO is set to 0x00, the remaining field in the CINFO and the corresponding QMP fields are not present in the CSPEC. 0x02 – 0xFF = reserved 0x00 = CINFO is not valid. 0x01 = CINFO is valid 0x02 – 0xFF = reserved. Valid CINFO shall be set to 0x01 if the connection setup shall use local link(s). 0x02 – 0xFF = reserved.	No
MAC Service Type	1	1		

MAC Service Type	1	1	0x00 = contention-free service. In this case, connection setup shall fail if the requested Global Link(s) cannot be established. 0x01 = contention-based service. In this case, connection setup shall use local link(s). 0x02 = contention-free service preferred. In this case, connection will use Global Links if the network is operating in Uncoordinated mode or Coordinated mode and the Global Link(s) can be established. Otherwise, the connection will use contention based service. 0x03 - 0xFF = reserved Refer to Section 5.2.3.5.3 for details. This field is only present when Valid CINFO is set to

Arrival Time Stamp to HLE (ATS)	3	1	For contention-based service, this field indicates the channel access priority to be used by packets belonging to this Link when they are transmitted in CSMA allocations. This field is only present when Valid CINFO is set to 0x01. 0x00 = CAP0, 0x01 = CAP1, 0x02 = CAP2, 0x03 = CAP3, 0x04 - 0xFF = reserved	Yes
User Priority	2	1		

Arrival Time Stamp to HLE (ATS)	3	1	0x00 = ATS should not be passed to the HLE. 0x01 = ATS should be passed to the HLE (at the receiver) for each MSDU. 0x02 - 0xFF = reserved This field is only present when Valid CINFO is set to 0x01.	No
Smoothing	4	1	0x00 = smoothing is not requested. 0x01 = if supported, receiver shall activate smoothing function / delay compensation function. 0x02 - 0xFF = reserved This field is only present when Valid CINFO is set to 0x01.	No

The QoS and MAC parameters identify the QoS requirements (delay, jitter, data rates), as well as MAC parameters that are specific to the particular Connection. The QoS parameters are generated by the Connection Manager using the Auto-Connect function or through PAL-specific primitives exchanged between the higher layer applications and the CM.

Each QoS and MAC parameter field consists of a Forward/Reverse (F/R) field, a Length (LEN) field, and a 1-octet Field Identifier (FID) field, followed by the Body of the QoS and MAC Parameter field. Table 77 shows the format of a QoS and MAC parameter field.

The QMPs exchanged between the HLE and Connection Manager are shown in Table 78.

The QoS and MAC parameters exchanged between two CMs include the parameters shown in Table 78 and Table 79.

The QoS and MAC parameters exchanged between the CM and CC are shown in Table 710.

Table 77: Format of QoS and MAC Parameter Field in CSPEC

Function	Octet Number	Field Size (Octets)	Description
Forward/Reverse (F/R)	0	1	0x00 = forward (from source to receiver) 0x01 = reverse (from receiver to source) 0x02 - 0xFF = reserved
Length (LEN)	1	1	Length of the Body Field, in Octets 0b0000000 = 0 octets, and so on.
Field Identifier (FID)	2	1	Identifier of the QoS and MAC parameter field
Delay Bound	0x00	4	Maximum amount of time (Octets) to transport an MSDU, measured from the time the MSDU arrives at the Convergence Layer SAP of the transmit station until the time is transmitted or retransmitted successfully across the powerline network and
Body	-	Var.	Data of the QoS and MAC parameter field

Table 78: QoS and MAC Parameter Fields Exchanged between HLE and CM, and between CMs

CSPEC Field	FID	LEN (Octets)	Descriptions	Reconfigurable

Jitter Bound Delay Bound	0x01 0x00	4 4	Maximum difference in the delay experienced by any two MSDU. Delay is measured from the time the MSDU arrives at the Convergence Layer SAP of the transmit station until the time is transmitted or retransmitted successfully across the powerline network and delivered out of the Convergence Layer SAP of the receive station(s). Unit is microseconds. 0x00000000 = 0 microseconds, and so on. The maximum allowed value is 10 seconds.	Yes

Maximum MSDU Size	0x03	2	Maximum MSDU Payload Size in octets. If this parameter is not specified, a value of "Default Maximum MSDU Size" is assumed.	Yes
Jitter Bound	0x01	4	the transmit station until it is successfully delivered out of the Convergence Layer SAP of the receive station(s). Unit is microseconds. 0x00000000 = 0 microseconds and so on. The maximum allowed value is 10 seconds.	
Average MSDU Size	0x02	2	Average MSDU Payload Size in octets (refer to Section 12.3.2.1.1) 0x0000 = 0 octets and so on.	Yes

Maximum MSDU Size	0x03	2	The maximum application data Payload Size in octets. If this parameter is not specified, a value of "Default Maximum MSDU Size" is assumed. This does 0x0000 = 0 octets and so on.	Yes
Minimum Data Rate	0x05	2	The average application data rate specified at the CL SAP that is required for transport of MSDUs belonging to this Link. This does not include the MAC and PHY overhead incurred in transferring the MSDU. Units in multiples of 10 Kilobits per second (kbps). 0x0000 = 0 Kbps, 0x0001 = 10 Kbps and so on.	Yes
Average Data Rate	0x04	2		

Maximum Data Rate	0x06	2	The maximum application data rate specified at the CL SAP that is required for transport of MSDUs belonging to this Link. This does not include the MAC and PHY overhead incurred in transferring the MSDU. Units in multiples of 10 Kilobits per second (kbps). 0x0000 = 0 Kbps, 0x0001 = 10 Kbps and so on.	Yes

Maximum Data Rate	0x06	2	The maximum application data rate specified at the CL SAP that is required for transport of MSDUs belonging to this Link. This does not include the MAC and PHY overhead incurred in transferring the MSDU. Units in multiples of 10 Kilobits per second (kbps). 0x0000 = 0 Kbps, 0x0001 = 10 Kbps and so on.	Yes
Maximum Inter-TXOP time	0x07	2	Maximum time allowed between two transmission opportunities (TXOPs) on the medium for this Link. Unit is microseconds. 0x0000 = 0 microseconds.	Yes
Minimum Inter-TXOP time	0x08	2	Minimum time allowed between two transmission opportunities (TXOPs) on the medium for this Link. Unit is microseconds. 0x0000 = 0 microseconds	Yes

Maximum Burst Size	0x09	2	Maximum size of a single burst of contiguous L2CAP SDUs that can be delivered by the application at the sending side in one interval. Unit: octets. 0x0000 = 0 octets.	Yes
Inactivity Interval	0x0b	4	Time duration in milliseconds. 0x00000000 = indefinite (i.e. connection should be considered active until explicitly terminated). 0x00000001 = 1 millisecond and so on.	Yes
Exception Policy	0x0a	1	Configuration bit mask that allows the CM to control the behavior of the transmitting application data before the CM can release the data. 0x00 = terminate the connection. 0x01 = reconfigure the connection. 0x02 – 0xFF = reserved.	Yes

MSDU Error Rate	0x0c	2	Maximum MSDU error rate requested for the connection. The value of x is specified in the most-significant 8 bits in unsigned integer format. The value of y is specified in the least-significant 8 bits in unsigned integer format. The MSDU error rate is x•10^-y.	Yes
Inactivity Interval	0x0b	4	Maximum duration of time a connection is allowed to remain inactive without transporting any application data before the CM can release the allocation. The units are milliseconds. 0x00000000 = indefinite inactivity interval (i.e., Connection should be considered active until explicitly terminated). 0x00000001 = 1 millisecond and so on. The maximum allowed value is 60 seconds.	

CDESC	0x0e	13 or 37	MSDU error rate requested. It is expressed as $x \bullet 10^{-y}$. The value of x is specified in the most-significant 8 bits in unsigned integer format. The value of y is specified in the least-significant 8 bits in unsigned integer format.	Yes
MSDU Error Rate	0x0c	2		
CLST	0x0d	1	Convergence Layer SAP Type This field supports negotiation of Connections using Convergence Layer SAPs other than the 802.3 SAP. If this field is not present, the 802.3 SAP is assumed. **CLST Value** / **Interpretation** 0x00 — IEEE 802.3 SAP others — Reserved	No

CDESC	0x0e	13 or 37	Connection Descriptor (refer to Section 7.8.1)	
Vendor Specific	0x0f	Var	Vendor specific QoS and MAC information (refer to Section 7.8.1)	Yes
Smallest Tolerable Average Data Rates	0x11	2	Smallest Tolerable Average Data Rate indicates the smallest average data rate at which the application is capable of operating. Units in multiples of 10 Kilobits per second (kbps).	
ATS Tolerance	0x10	2	Measured variance in value of Arrival Time Stamp (ATS) from the synchronized Network Time Base at the time the ATS is applied to the MSDU arriving at the Convergence Layer SAP of the transmit station. Unit is microseconds. 0x0000 => 0 microseconds and so on.	Yes

Rx Window Size	0x13	2	Receive window	
Smallest Tolerable Average Data Rates	0x11	2	Tolerable Average Data Rate indicates the smallest average Data rate at which the application is capable of operating. Units in multiples of 10 Kilobits per second (kbps). 0x0000 = 0 Kbps, 0x0001 = 10 Kbps and so on.	No
Original Average Data Rate	0x12	2	Original Average Data Rate indicates the average data rate at which the application intends to operate when sufficient station and network resources are available. Units in multiples of 10 Kilobits per second (kbps). 0x0000 = 0 Kbps, 0x0001 = 10 Kbps and so on.	No

Table 79: Additional QoS and MAC Parameter Fields Exchanged between Two CMs

QoS and MAC Parameter Field (CM-CM)	FID	LEN (Octets)	Descriptions	Reconfigurable

Rx Window Size	0x13	2	This parameter shall indicate the number of 512-octet segments that the Receiver Window Size can accommodate. The minimum value shall be 1 and the maximum value shall be 65535.	No
Smoothing Buffer Size	0x14	3	The smoothing buffer size in octets that is required to support the Link at the transmitter and receiver. If this field is not present and smoothing is requested, the default buffer size is chosen to be the product of Delay (in seconds) and Average Data Rate (in bits per second) 0x000000 = 1 octet and so on.	No
Bidirectional Burst	0x15	1	These traffic is intended to be transmitted as part of Reverse SQF of the Bidirectional Bursts initiated	No

Bidirectional Burst	0x15	1	This parameter shall only be present in QMPs of Local Link that belong to a bidirectional Connection, and whose traffic is intended to be transmitted as part of Reverse SOF of the Bidirectional Bursts initiated by the other Link in the connection. The presence of this indicates that the payload of this Local Link has to be transmitted as part of Reverse SOF of Bidirectional Bursts. A value of 0x00 is used when both links are local links. A value of 0x01 indicates that the Bidirectional Bursts in CFP will always end with a SACK. A value of 0x02 indicates that the Bidirectional Burst in CFP may end with a Reverse SOF.

			The minimum number of 520-octet PHY Blocks per TXOP required	

Table 710: QoS and MAC Parameter Fields between CM and CCo

QoS and MAC Parameter Field (CM-CCo)	FID	LEN (Octets)	Description	Reconfigurable
Minimum Number of PBs per TXOP	0x82	2	The number of uniformly spaced TXOPs requested per Beacon Period. 0x00 = 1 TXOP per Beacon Period 0x01 = 2 TXOPs per Beacon Period 0x02 = 3 TXOPs per Beacon Period 0x03 = 4 TXOPs per Beacon Period 0x04 - 0xFF = reserved	No
TXOPs per Beacon Period	0x80	1		
Average Number of PBs per TXOP	0x81	2	The average number of 520-octet PHY Blocks per TXOP required for transporting MSDUs belonging to this Link. 0x0000 = 0 PBs per TXOP and so on.	Yes

Minimum Number of PBs per TXOP	0x82	2	The minimum number of 520-octet PHY Blocks (PBs) that must be transported during a TXOP in order to request extra bandwidth to clear the backlog. If there is sufficient bandwidth available, the CC should allocate extra PBs for transporting the MSDUs belonging to this Link.	Yes
PPB_Threshold	0x84	2	The maximum number of 520-octet PHY Blocks per TXOP required for transporting the MSDUs belonging to this Link. 0x0000 = 0, and so on	Yes
Maximum Number of PBs per TXOP	0x83	2	Pending PHY Block threshold that must be exceeded before the CC should allocate Extra TXOP Allocation when the MSDUs belonging to this Link.	Yes

PPB_Threshold	0x84	2	The Pending PHY Block (PPB) threshold indicates the threshold of Pending PBs at which the Link requires extra bandwidth to clear the backlog. If there is sufficient bandwidth available, the CCo should provide Extra Allocation when the PPB threshold is exceeded. 0x0000 = 0 PBs and so on	Yes
Surplus Bandwidth	0x85	2	Surplus Bandwidth (refer to Section 7.8.1.4)	No
Exception Policy	0x0a	1	0x00 = terminate the Connection. 0x01 = reconfigure the Connection. 0x02 to 0xFF = reserved	Yes
CDESC	0x0e	13 or 37	Connection Descriptor (refer to Section 7.8.1.1)	Yes
Vendor Specific	0x86	Var	Vendor-Specific QoS and MAC information (refer to Section 7.8.1.1)	Yes

Smallest Tolerable Average Number of PBs per TXOP Bidirectional Burst	0x87 0x89	2 1	This parameter indicates that this Average Number of PBs per TXOP indicates the smallest average number of PBs per TXOP (refer to Section 5.4.7) capable of operating. 0x0000 = 0 PBs per TXOP and so on.	No
			Original Average Number of PBs per TXOP indicates the average number of PBs per TXOP at which	
Original Average Number of PBs per TXOP	0x88	2	the application intends to operate when sufficient station and network resources are available. 0x0000 = 0 PBs per TXOP, and so on	No

Source IP Addr		-		4 or 16	This parameter indicates that this Global link will be used for Bidirectional	IP Address of Source HLE 4 Octets Long for IP
Bidirectional Burst	0x89		1		Bursting for a Local Link that is part of this connection (refer to Section 5.4.7). 0x00 = bidirectional burst will always end with a SACK. 0x01 = bidirectional burst may end with a Reverse SOF. All other values are reserved.	No

Connection Descriptor (CDESC)

The QoS and MAC Parameters of the CSPEC exchanged between the HLE and CM, between CMs, and between CM and CCo can optionally include a Connection Descriptor (CDESC). A Connection Descriptor is a set of fields that defines the Connection to the HLEs (refer to Table 711). It is used by UPnP QoS and possibly other HLEs. This field is for HLE use only; the AV system merely passes the information to all involved STAs (including the CCo) so the HLE can later construct a list of the active Connections without having to query every STA.

There shall be at most one CDESC per CSPEC (even if the Connection is bidirectional) and the Forward/Reverse field of the QMP field containing the CDESC shall have no meaning and shall be ignored by the receiving entities.

Table 711: Format of the Body of Connection Descriptor

CDESC Field	Octet Number	Field Size (Octets)	Descriptions
IP Version	0	1	IP protocol version 0x00 = IP Version 4 0x01 = IP Version 6 0x02 - 0xFF = reserved

Source IP Addr	-	4 or 16	IP Address of Source HLE 4 Octets Long for IP v4, 16 Octets Long for IP v6
Source IP Port	-	2	IP Port number (corresponding to the Protocol Type) of Source HLE
Destination IP Addr	-	4 or 16	IP Address of Destination HLE 4 octets long for IP v4, 16 octets long for IP v6
Destination IP Port	-	2	IP Port number (corresponding to the Protocol Type) of Destination HLE
Protocol Type	-	1	IP Protocol Type (e.g., TCP, UDP)

Vendor-Specific QoS and MAC Parameters

The QoS and MAC Parameters of the CSPEC exchanged between the HLE and CM, between CMs and between CM and CCo may optionally include vendor-specific parameters. A vendor-specific QoS and MAC parameter has a Field Identifier (FID) of 0xFF. The first 3 octets of the Data field of this parameter contain the IEEE-assigned Organizationally Unique Identifier (OUI) assigned to the vendor as shown in Table 712 and specified in Section 11.7.

Table 712: Format of the Body of Vendor-Specific MAC and QoS Parameter

Field	Octet Number	Bit Number	Field Size (Bits)	Definition
OUI	0	7 - 0	8	OUI first octet
	1	7 - 0	8	OUI second octet
	2	7 - 0	8	OUI third octet
Vendor Defined	--	--	--	Vendor defined

Ordering of Fields within the CSPEC

CSPECs exchanged between CMs and between CM and CCo shall obey the following rules:

If the CSPEC contains both Forward Link and Reverse Link CSPECs, the Forward Link QMP field shall be presented before the Reverse Link.

Within the CSPEC of each Link, the QMP fields shall be arranged in ascending order of the Field Identifier values. For example, if delay and jitter are both exchanged for the Forward Link between two CMs, the delay parameter appears before the jitter parameter in the Forward Link CSPEC.

Surplus Bandwidth

Surplus Bandwidth indicates the excess amount of bandwidth required to support the Link relative to the Average Number of PBs per Transmit operation. A value of 0x00 indicates that no surplus bandwidth is required. A value of 0x01 indicates that one PB per Transmit Operation amount of surplus bandwidth is required and so on.
The CCo shall use surplus Bandwidth during the initial admission control procedure. A Connection shall be rejected if the Average number of PBs per Transmit Operation along with the requested Surplus Bandwidth cannot be allocated. The CCo shall use the following parameters for converting PBs to allocation time requirements:
MaxFL_AV value of 2501.12 sec shall be used in AV-only Mode. In Hybrid mode, the HomePlug 1.0-compatible Frame Length (FL_AV) shall be used (refer to Section 9.4).
RIFS_AV value of RIFS_AV_default shall be used.
CFIFS_AV value of 140 sec shall be used.
Tone Map boundaries as in Section 5.2.6.4 shall be obeyed.
Bursting shall be assumed with a maximum of four MPDUs per Burst.
Minimum Set of QoS and MAC Parameters
If contention-free service is requested in the MAC Service Type parameter of CINFO, the following minimum set of QoS and MAC parameters between the HLE and the CM and between the two CMs shall be specified:
Average Data Rate
At least one of Delay Bound and Maximum Inter-TXOP Time
The minimum additional set of QoS and MAC parameters that shall be exchanged between the two CMs are:
RX Window Size
If contention-free service is requested in the MAC Service Type parameter of CINFO, the following minimum set of QoS and MAC parameters between the CM and the CCo shall be specified:
TXOPs Per Beacon Period
Average Number of PBs per TXOP
CSPEC Reconfigurability
Most, but not all, CSPEC fields may be modified (reconfigured) over the life of the Connection. There are a few that shall not be modified once the Connection is established. Whether a field can be modified is indicated in the “Reconfigurable” column of Table 78, Table 79, and Table 710. Connection modification request will be rejected if the reconfigured CSPEC cannot be supported.

Connection Specification (CSPEC) for GREEN PHY

A station implementing only GREEN PHY is not required to implement this feature (i.e., only priority “connectionless” links are required to be implemented by a GREEN PHY station).

Scheduler and Bandwidth Allocation

The CCo implements scheduling algorithms for the CFP. These algorithms make bandwidth assignments in the form of time grants. The assignments are carried in the Persistent and Non-Persistent Schedule BENTRYs that are broadcast in the Beacon.
The scheduling algorithms make updates to the schedules based on the following events:
Requests for new Links from STAs within the network.

Request for Link reconfigurations from existing Links within the network.
Changes to the capacity of existing Links as a result of changes to the physical channel.
Figure 721 contains a finite state machine diagram describing the life cycle of a Global Link. The lifecycle of the Link typically begins when the CCo receives a CC_LINK_NEW.REQ message from a station in the network.
The CC_LINK_NEW.REQ message contains the CSPEC and CINFO parameters for a Connection that requires use of the CFP. It also includes Bit Load Estimates (BLEs) for the physical channel between the STAs requesting the Link. These BLEs are based on communications between the STA that occurred during the CP.

Figure 721: Global Link Life Cycle

The CCo performs admission control on the Link based on the BLE. If there is sufficient bandwidth available to support the Link, the CCo sends the CC_LINK_NEW.CNF message indicating success and containing the GLID for the Link(s) to both STAs. At this point, the Link is active and carrying user data.
If the admission-control function returns failure to allocate, the CCo sends a CC_LINK_NEW.CNF message indicating failure along with a Proposed CSPEC to both STAs involved in the connection setup.
While the Link is active, the CCo "sniffs" on the FC fields transmitted in the delimiter by the STA. The SOF FC contains a BLE field and a PPB field. The CCo uses the contents of the BLE field to update its estimates of the channel capacity vs. line cycle. It uses the PPB field to determine whether to increase or decrease persistent allocation and/or to provide non-persistent allocation for the Link.
As Figure 721 shows, the CCo may update schedule (i.e., Persistent and Non-Persistent allocations) based on one of the following events:
The STA may request a change in the QoS parameters of a Link. In this case, if sufficient bandwidth is available, the CCo updates the Schedule; otherwise, the modification request is rejected.
The CCo decides that a change to the schedule is needed based on the PPB and BLE fields.
Schedule updates are indicated to all stations in the network using Persistent and Non-Persistent BENTRYs in the Beacon.

7.8.2.1 Scheduler and Bandwidth Allocation for GREEN PHY

A station implementing only GREEN PHY is only required to be Level-0 capable. Therefore, HomePlug GREEN PHY Stations are not required to support Scheduling and Bandwidth Allocation functionality.

Connection Admission Control

The Connection Admission Control procedure ensures that the station and network resources are not over allocated, thus ensuring the QoS guarantee on admitted Connections.
CMs shall execute the Connection Admission Control procedure whenever a new Connection is requested or an existing Connection is modified. CMs may also continuously monitor existing Connections for adherence to the negotiated traffic characteristics (traffic policing) and QoS

guarantees. Violation of the CSPEC parameters may cause the CM to reconfigure or tear down an existing Connection.
The CCo shall execute the admission control procedure when a new Global Link is requested or an existing Global Link is modified. The CCo shall also continuously monitor all existing Global Links and it may modify or terminate Connections if the available bandwidth is not sufficient to satisfy the CSPEC requirements.

7.8.3.1 Connection Admission Control for GREEN PHY

A station implementing only GREEN PHY is only required to be Level-0 capable. Therefore, HomePlug GREEN PHY Stations are not required to support Connection Admission Control functionality.

Beacon Period Configuration

The Bandwidth Manager must determine the allocations within a Beacon Period. If Neighbor Networks are present, it must ensure that allocations within its network are compatible with the Neighbor Networks in its INL.
The Bandwidth Manager assembles the portion of the Beacon payload dealing with bandwidth allocation.

Bandwidth Allocation for GREEN PHY

Green PHY Preferred (GPP) allocations are based on the presence of Green PHY stations in the AVLN. Green PHY stations may treat the GPP allocation to have forever persistence (i.e., always present). Thus, Green PHY stations may transmit in GPP allocations without processing Persistent and Non-Persistent Schedules in the Central Beacon.

Figure 722: Green PHY Preferred CSMA allocation immediately following the Beacon Region.

Informative Text

Future HomePlug AV CCo operating in Uncoordinated Mode provides Green PHY Preferred (GPP) allocations for Green PHY traffic. Future HomePlug AV CCo operating in Coordinated Mode provides GPP allocations for Green PHY Traffic provided it is not Coordinating with a HomePlug AV 1.1 CCo. The duration of the GPP allocation is 7% of the Beacon Period. GPP allocation immediately follows the Beacon Region. Future HomePlug AV CCo may use Persistent or non-Persistent schedule BENTRIES to indicate the GPP allocations. Future HomePlug AV CCo provides a CSMA allocation of at least MinCSMARegion duration immediately following the GPP allocation.

Backup CCo and CCo Failure Recovery

Each CCo-capable STA may optionally implement the “Backup CCo” function. When such a STA is appointed by the current CCo as the Backup CCo of a network, and when the current CCo suffers from a failure, the Backup CCo shall execute the CCo failure recovery procedure.

Backup CCo

The CCo may optionally designate a STA as the Backup CCo by sending a

CC_BACKUP_APPOINT.REQ message with the Appoint/Release flag set to 0x00 (Appoint). The STA that is identified shall respond with a CC_BACKUP_APPOINT.CNF message. Depending on whether the STA supports the Backup CCo function, it may accept or reject the request.

The function of the Backup CCo is to assume the role of the CCo in the event of a CCo failure. The Backup CCo may be selected by an analysis of the Topology Table using the criteria defined in Table 73. The Backup CCo is not selected on a periodic basis like the Auto-selection function for the CCo. The CCo may evaluate its Topology Table to find an alternate Backup CCo only when the current Backup CCo disassociates from the network.

When the CCo role is handed over to a new STA, the new CCo shall be informed of the identity of the Backup CCo (if any) in the CC_HANDOVER_INFO.IND message. The new CCo may choose to appoint a new STA as the Backup CCo. When the new CCo chooses a different STA to be the Backup CCo, it shall inform the current Backup CCo via the CC_BACKUP_APPOINT.REQ message with the Appoint/Release flag set to 0x01 (Release), prior to appointing a new Backup CCo.

The CCo should keep the Backup CCo up-to-date with the list of associated and authenticated stations in the AVLN by sending **CC_HANDOVER_INFO.IND** message with the Reason Code set to 0x01 (Update of network information to Backup CCo). The Backup CCo shall send a **CC_HANDOVER_INFO.RSP** message to indicate successful reception of **CC_HANDOVER_INFO.IND**.

The current CCo may also send **CC_LINK_INFO.IND** message(s) to the Backup CCo to transfer the CSPEC and BLE information about all Global Links in the AVLN. The Backup CCo shall acknowledge the proper reception of this message using **CC_LINK_INFO.RSP**.

CCo Failure Recovery

It is possible for the existing CCo to drop out of the network without warning either because of equipment failure or because the user unknowingly unplugged the STA that was serving as the CCo.

If a Backup CCo is appointed in the network and if the Backup CCo does not receive any Central Beacons from the CCo for (Max_Missed_Beacon) Beacon Periods, and during the same time period, the Beacon Detect Flag (refer to Section 4.4.1.5.2.5) in the Frame Controls of all transmissions indicate Beacons are not detected, the Backup CCo shall assume the role of the new CCo, and perform the following steps:

- The Backup CCo shall transmit a Central Beacon in the same Beacon Slot used by the old CCo once every Beacon Period.
- The Backup CCo may maintain the persistent schedule of the last received Beacon.
- The Backup CCo shall include the MAC Address BENTRY in at least the first 10 Central Beacons it transmits following a CCo failure. This will enable STAs in the AVLN to determine that a Backup CCo has taken control of the AVLN.
- The Backup CCo may request the CSPEC and BLE of all active contention-free Links in the schedule from each STA involved using the CC_LINK_INFO.REQ/ CNF message exchange.

- The Backup CCo may appoint a new Backup CCo.
- The Backup CCo shall perform normal CCo operations.
- All STAs in the network shall adjust their clocks based on the new Network Time Base being transmitted by the Backup CCo.
- All STAs in the AVLN shall renew their TEIs (refer to Section 7.3.2.1.2) once the Backup CCo starts sending the Central Beacons.

All STAs in the AVLN shall reinitiate the power-on network procedure (refer to Section 7.1) when a CCo failure occurs and the Backup CCo (if any) fails to takeover as the new CCo. A STA should wait for at least CCo_Failure_Time before reinitiating the power-on network procedure.

Security

Security Overview

As with HomePlug AV, HomePlug GREEN PHY security performs two functions:

Controlling access to the AVLN. This function is described in Section 7.10.3.

Securing the privacy of data transferred on the AVLN. This function is described in Section 7.10.6.1.

Security is provided by means of a single encryption algorithm and a single hash function:

128-bit AES encryption (refer to Section 7.10.6)

SHA-256 secure hash function

Security is also enhanced through the use of nonces (Section 7.10.7.3), which help to prevent unauthorized replays of MMEs.

Access to the AVLN and ability to participate in the AVLN is provided by encryption keys and passwords.

Informative Text
With the exception of the encryption of PBs in the MAC/PHY using the NEK, all security-related activities (e.g., payload encryption and key management) take place in an entity that may be thought of as the "Security Layer." This entity is implementation dependent and is assumed to lie in the Control Plane. The Security Layer is responsible for generating the CM_ENCRYPTED_PAYLOAD.IND messages.

Encryption Keys, Pass Phrases, Nonces, and Their Uses

As with HomePlug AV, all the encryption keys used in HomePlug GREEN PHY are 128-bit AES keys. These may be machine-generated or they may be based on pass phrases. Password" and "pass phrase" both describe the same object. The term "pass phrase" is preferred, but the term "password" is also preserved because of its use in acronyms such as "DPW" and "NPW." Keys based on pass phrases come in two varieties:

Device Passwords (DPWs)

Network Passwords (NPWs)

In addition, as with HomePlug AV, GREEN PHY uses Hash Keys (longer, machine-generated strings) for the UKE protocol, and nonces for freshness and association between messages in a protocol run.

Device Access Key (DAK)

The Device Access Key (DAK) is unique to a STA. Each STA is provided with a unique DAK

during manufacture. Another STA may—if it knows a particular STA's DAK use that DAK to encrypt a message intended only for the particular STA. Upon receipt, such a message is treated as equivalent to the direct entry of the NMK from HLE. The DAK shall never be reset and it shall never be sent over the medium, even in encrypted MMEs. Support for the DAK is mandatory.

Informative Text Implementers may choose to provide a means to change a compromised DAK using some type of firmware upgrade methodology.

Device Password (DPW)

As part of the packaging of the product (perhaps as a label on the back or bottom of the product), the user shall be provided with a Device Password (DPW) a password that will uniquely generate the new STA's unique DAK via the standard hashing algorithm defined in Section 7.10.7.1. The DPW is the value that is actually entered by the user during Authorization using the DAK (refer to Section 7.10.3.4).

Network Membership Key (NMK)

The Network Membership Key (NMK) is used by a STA to prove its membership in an AVLN (or a sub-AVLN); i.e., its right to join (participate in) a sub-AVLN. Thus the NMK defines the sub-AVLN. The user may designate the NMK(s) — by entering an NPW — or may elect machine generation (which is more secure). Hashing the NMK produces the default NID offset, but the NMK may be associated with a non-default NID in some cases. Support for two NMKs (one present and one future) and their associated NIDs is mandatory.

The NMK is associated with a Security Level (SL). The NMK's SL defines the SL of the sub-AVLN and must be the same for all sub-AVLNs in an AVLN; the SL determines what key distribution methods are allowed for that NMK. The SL associated with an NMK is passed to the STA as part of the NID in the **CM_SET_KEY.REQ** MME or in the **APCM_SET_KEY.REQ** primitive.

Network Password (NPW)

The Network Password (NPW) is the value that generates the NMK when it is run through the hashing function described in Section 7.10.7.1.

Network Encryption Key (NEK)

During normal operation, most messages are encrypted using the Network Encryption Key (NEK), which shall only be generated by the CCo and is never exposed to the user. Support for two NEKs (one present and one future) is mandatory.

The NEK shall only be set by a CCo internally generating it randomly (refer to Section 7.10.7.2), or by the NEK-provisioning processes, whereby the CCo provides a STA with the NEK in an MME encrypted with the NMK. The NEK is not known by a STA until the STA has completed the authentication process (refer to Section 7.10.4) and joined the AVLN.

Temporary Encryption Key (TEK)

The Temporary Encryption Key (TEK) is an AES key that is used to encrypt messages on a temporary private channel between two STAs. It may be distributed using the receiver's DAK, or generated by the Unicast Key Exchange (UKE) protocol (protected from standard equipment by unicast, and possibly at the signal level by tone map modulation). It can be used over unauthenticated channels (i.e., it may be distributed without proof of freshness using the DAK, or

it may be generated using UKE). It shall not be distributed to more than one STA, and both sender and receiver must discard it after no more than Max_TEK_Lifetime. If the TEK was exchanged using UKE, it may be used only until a protocol message with PMN=0xFF is sent or until the protocol aborts (by either STA). Once a message with PMN=0xFF has been sent, the TEK established at the beginning of that protocol run shall no longer be used. Support for at least one TEK is mandatory. Refer to Section 7.10.7.2 for generation of random AES keys.

Nonces

Nonces are pseudo-random numbers (i.e., the sequence of values that they take for a given station are unpredictable) that are used only once. Practically, as the number of bits in a nonce is finite, they may repeat, but the same nonce should never be used with the same encryption key; that is, changing the encryption key in essence clears the set of unusable nonces.

Nonces are used to prevent replay attacks (when a STA receives a nonce that it recently generated, it can be assured that the message it received was composed recently also). They may also be used to associate messages in a protocol run, though this is accomplished in through the use of Protocol IDs, Protocol Run Numbers, and Protocol Message Numbers. A station need only generate one nonce per run of a protocol (i.e., the value of My Nonce for that STA may remain constant for a run of a protocol), but a new nonce should be generated for each new protocol run. This reflects the purpose of nonces to provide a STA with a quantity it believes to be freshly generated (to defeat replay attacks) and to use for association of messages within the protocol run. Refer to Section 7.10.7.3 for generation of nonces.

Methods for Authorization (NMK Provisioning)

An AVLN is defined as a set of stations that share a common NID and CCo with which they share a common NMK and Security Level. Typically, all STAs in an AVLN can communicate with each other and share a common NMK and Security Level, but the CCo may form separate sub-AVLNs within an AVLN, each with its own NMK.

Before a new STA can participate in an AVLN, it must determine whether to join an existing AVLN or form a new one. The determination of whether to join a given AVLN consists of three decisions:

- At what level of security does the user wish the AVLN to operate?
- Does the STA want to authorize the AVLN? (More precisely: does the STA's owner want to have the STA join the AVLN?)
- Does the AVLN want to authorize the STA's membership request? (More precisely: does the AVLN's owner want to allow the STA to join the AVLN?)

These decisions must occur before a new STA can fully participate in the selected AVLN. The first decision determines the operating mode of the AVLN and the ways in which its NMK(s) may be distributed. All three decisions implicitly require user participation and approval. It is possible for all three decisions to be made simultaneously by a single action of the user. Several alternative methods of NMK Provisioning are provided to enable these UEs. These methods are specified in this section.

Regardless of whether the three processes occur separately or concurrently, the end result — if successful — is that the STA possesses a Network Membership Key (NMK) that it can use now and in the future to join the AVLN.

In general, NMK Provisioning will occur once and the authorization will be permanent. It is possible for the STA to be expelled from an AVLN by providing a different NMK to all stations except the STA being expelled, which would invalidate the STA's NMK. Subsequent distribution and use of a new NEK(s) then excludes the expelled STA from secure communication within the AVLN.

Informative Text
It is the implementer's responsibility to inform the user if a STA cannot connect to an AVLN because of a Security Level mismatch. If the user needs to change the Security Level for a STA to join an AVLN, the user should be so advised. This situation can arise when the user enters the NPW on multiple devices or uses a mix of mechanisms to distribute NMKs.

There are three methods for NMK Provisioning; each has its own merits and shortcomings, which are described with the UEs that these methods support (refer to Section 13.2). These methods are covered in the following sections:

NMK Obtained by Direct Entry (Section 7.10.3.3)

NMK Obtained From AVLN Using DAK Encryption (Section 7.10.3.4)

NMK Obtained From AVLN Using UKE (Section 7.10.3.5)

Support for all methods is mandatory. Note, however, that the user experience(s) supported by a method will not be available to the user in the absence of a suitable user interface on the STA. Depending upon the method used, the STA might or might not need to engage in AVLN communication prior to obtaining the NMK. The Security Level of the AVLN may also restrict the methods that may be used for NMK distribution.

The choice of the preferred method for obtaining an NMK from among those supported by an implementer is left to the user. NMK Provisioning is closely linked to Security and Privacy. It is expected that the user will determine which method to use based upon the method's ease of use and the user's perceived need for security and privacy.

Regardless of how the NMK is obtained, the STA shall store the NMK and its Security Level in its non-volatile memory. If the NID associated with the NMK is not based on the default NID offset, the NID shall also be stored in non-volatile memory. The NMK shall be replaced with a pseudo-random value and associated with its default NID upon reset.

Security Level

The Security Level of the NMK defines both the Security Level of the AVLN and the methods that can be used to distribute the NMK. The SL is encoded as part of the NID so that AVLNs at different SLs cannot be considered to be the same AVLN even if the rest of their NID is the same. Table 713 shows the interpretation of the 2-bit SL value.

Table 713: Security Level Interpretation

Security Level Value	Interpretation
0b00	Simple Connect. The NMK may have been exchanged using UKE.
0b01	Secure Security Level. The NMK must not have been exchanged using UKE.
0b10-0b11	Reserved.

Table 714: Security Level and NMK Provisioning.

Key Status	Description	NMK Provisioning Allowed
NMK-SC	Simple Connect, NMK randomly generated by MAC or set by HLE	Direct (from HLE), UKE or DAK
NMK-HS	Secure Security Level, NMK hashed from password – Password can be application generated for the first station, but the user would have to record the password or use DAK provisioning for all additional stations. The STA ignores local Add/Join button presses (i.e., Add, Join button presses and UKE distribution require an explicit UI Security Level change, or reset).	Direct (from HLE) or DAK

Informative Text
The Security Level applies primarily to Encryption Key Management protocols. It is assumed that all data plane traffic and — with a few exceptions specified herein — all MMEs will be encrypted with the NEK. STAs are not required to accept and should not process any unencrypted data plane traffic and should not be assumed to do so. STAs are not required to accept unencrypted control plane traffic outside of the exceptions specified herein, and should not be assumed to do so. STAs that do accept other unencrypted traffic do so at their own risk.

Secure Security Level
An NMK-HS shall be associated with Secure Security Level. A STA shall only accept a new NMK-HS that is either set by direct entry by the host or sent using the DAK-based distribution method (refer to Section 7.10.3.4). These are termed Secure key distribution methods. It shall not distribute an NMK-HS in its possession except by using the DAK of another STA.
A STA shall neither accept nor distribute an NMK-HS using Unicast Key Exchange (UKE). A STA with an NMK-HS shall ignore local Add/Join button presses.
Simple Connect Security Level
An NMK-SC shall be associated with Simple Connect Security Level. A STA shall only accept a new NMK-SC that it generates, or is sent using UKE or its DAK, or that it receives from the HLE using the APCM_SET_KEY.REQ primitive. The NMK-SC should be generated randomly by the first STA to become the CCo of a Simple Connect Security Level AVLN. A STA in Simple Connect may use UKE or the DAK of another STA to distribute NMK-SCs.
Just because a STA is in Simple Connect SL does not mean that it will provide its NMK-SC or accept a new NMK-SC from another STA using UKE. The HLE must place the STA in the SC-

Join state to accept an NMK-SC from another STA using UKE, and must place the STA in the SC-Add state to provide its NMK-SC to another STA using UKE.
Note: An Unassociated STA may be placed in the SC-Add state so that its NMK-SC will be used for the AVLN. This may be desirable if the STA has the NMK of an existing AVLN whose other STAs are not currently present.
If a STA in the SC-Join state observes another STA in the SC-Join state and it determines it should become the CCo, it shall generate a new NMK-SC, enter the SC-Add state, and provide its new NMK-SC to the other STA using UKE, as specified in Section 7.3.4.4.
Note: The HLE of a device may put the STA into the SC-Join state without user intervention under some circumstances. Conversely, the user may explicitly put any STA (including one already in an AVLN, even the CCo of an AVLN) into SC-Join state, causing it to discard its current NMK (even if it is an NMK-SC) and seek another STA in SC-Add or SC-Join. A STA that was previously in an AVLN must not use the NMK from that AVLN if it has been placed into SC-Join, even it if automatically enters the SC-Add state as described above.
Changing the Security Level
A STA that changes Security Level shall discard the previous NMK.
A Station in Secure Security Level may only be changed to Simple Connect SL by receipt of an NMK-SC in the DAK-based distribution method (refer to Section 7.10.3.4), or by the HLE. If it is changed to Simple Connect SL by the HLE (e.g., by resetting the STA), it shall generate a new NMK. In either case, it shall discard the previous NMK-HS.
A STA in Simple Connect SL may only be changed to Secure SL by receipt of an NMK-HS in the DAK-based distribution method (refer to Section 7.10.3.4) or by the HLE. If it is changed to Secure SL by the HLE, the HLE shall supply the new NMK-HS. In either case, the STA shall discard the previous NMK-SC.
Preloaded NMK
All devices are required to have an NMK at all times, so at a minimum, each device must have a random NMK. However, a vendor may replace the random NMK with an NMK derived from an NPW of the vendor's choice. This NMK must be set at the Secure Security Level. Alternatively, a vendor may cause several devices shipped as a set to have the same randomly generated NMK set at the Simple Connect Security Level. These options allow vendors to ship products that connect to each other out of the box for user convenience.
Direct Entry of the NMK
Direct entry only implies that the HLE somehow obtains an NMK that it intends for the STA to use, and passes it to the Convergence Layer along with the NID (including the Security Level) using the APCM_SET_KEY.REQ primitive or the CM_SET_KEY.REQ message over the H1 interface. The CL shall store it for current and future use in joining the specified AVLN. The HLE may obtain the NMK from a set of (NID,NMK) pairs that it has stored, from user entry of an NPW(and generation of the default NID), from key exchange using some higher layer authentication mechanism or by other means (refer to Section 7.10.3.6 and Section 13.2).
As with HomePlug AV, if a HomePlug GREEN PHY Device is provided with a suitable user-interface mechanism, it may permit the user to enter the Network Password directly into the STA, from which the NMK-HS and default NID are generated. The user-interface mechanism may also

allow the user to enter a non-default NID. The HLE will obtain the Network Password (NPW) and Secure Security Level from the user, generate the NMK-HS (as described in Section 7.10.7.1) and default NID offset, and pass the NMK-HS with Security Level of the NID set to Secure to the CL via the APCM_SET_KEY.REQ primitive or the CM_SET_KEY.REQ message. Whether the HLE retains the NPW and NID for future use is an implementation issue.

A STA that changes the NMK in this manner shall leave its current AVLN (if any) and become an Unassociated STA. It may join an existing AVLN or form a new one if it detects another STA with the same NMK-SL (refer to Section 7.3.4.1 and Section 7.3.4.2).

Distribution of NMK Using DAK

The user may enter the DPW of a STA into any UIS on the AVLN (or into an Unassociated STA). The HLE will derive the DAK and pass it to the STA, possibly with the NMK and NID to distribute, using the APCM_AUTHORIZE.REQ primitive. The STA shall use the DAK to perform Payload Encryption of a CM_SET_KEY.REQ MME containing a Temporary Encryption Key (TEK) and transmit the encrypted payload to the STA in a CM_ENCRYPTED_PAYLOAD.IND MME using multi-network broadcast (refer to Section 5.4.3.1). The protocol ID used shall be PID=0x02 (refer to Section 11.5.2.2) and the PMN shall be 0x01. The UIS shall periodically broadcast this message until it either receives a response or times out.

When the new STA receives and correctly decrypts the payload of this message using its DAK, as indicated in the PEKS, it cannot tell if the message is a replay or not. The new STA shall use the TEK supplied to respond with a CM_SET_KEY.CNF MME containing a new nonce in a CM_ENCRYPTED_PAYLOAD.IND MME unicast to the sender indicating that it has a matching DAK.

By receiving the TEK-encrypted payload in the response, the UIS knows that the new STA has a matching DAK and has the TEK. The UIS shall wait until both it and the New STA are associated with the same AVLN (known from the TEI Map information) before resuming the DAK-encrypted NMK key distribution protocol.

Note: A STA receiving a DAK-encrypted TEK does not need to disassociate from its current AVLN until it has correctly received the NMK later in the protocol. This is to facilitate its return to the current AVLN should the protocol fail.

Both STAs have obtained CCo capability and AVLN status information from the invitation messages exchanged. If the UIS is part of an AVLN, the new STA (i.e., the one whose DAK was used to encrypt the first MME) shall associate with the AVLN of the UIS. If the UIS determines it will become the CCo (as defined in Section 7.4.1), it shall begin transmitting Central Beacons and the new STA shall associate with the CCo (UIS). If the UIS is an Unassociated STA and the new STA is determined to become the CCo, the new STA shall become the CCo and the UIS shall associate with it.

Once the two STAs are associated with the same AVLN, the key distribution protocol resumes. The UIS shall send the new STA the NMK in a CM_SET_KEY.REQ MME as an encrypted payload encrypted with the DAK in a unicast CM_ENCRYPTED_PAYLOAD.IND MME, including the nonce received in the previous CM_SET_KEY.CNF MME. The new STA shall receive this and obtain the NID (including the Security Level) and NMK, which it now knows to

be fresh because of the nonce. The new STA shall confirm its correct receipt of the NMK by using it to encrypt the CM_SET_KEY.CNF MME sent as an encrypted payload in a unicast CM_ENCRYPTED_PAYLOAD.IND MME in response.
By virtue of receiving the third message in the protocol correctly (encrypted with its DAK and containing a new NMK and NID), the STA will know that the user wants it to join the AVLN from which the NMK was received and shall join it immediately, even if it is already participating in another AVLN. A STA shall set its security mode to the Security Level provided in the NID sent in the **CM_SET_KEY.REQ** MME when it receives the NMK via DAK-based encryption and should discard its current NMK.
Note: The STA should not discard its current NMK(s) upon receipt of a DAK-encrypted CM_SET_KEY.REQ MME, as this may be a replay. Should the protocol abort before reception of the UIS' NMK, the new STA shall disassociate from the UIS AVLN, reassociate (if necessary) with its previous AVLN, and resume use of its current NMK.
If the protocol completes successfully, the STA (i.e., the one that does not have the NEK) shall disassociate and associate (if not already associated with the correct AVLN) and authenticate using the NMK, as described in Section 7.3.3.
The entire process for an Unassociated STA forming a new AVLN is shown in Figure 710 (refer to Section 7.3.4.2) and for an AVLN STA adding a new STA, the process is shown in Figure 714 (refer to Section 7.3.5.2). Absent receipt of a response to its initial invitation, the UIS need not send an abort message. A STA that receives an abort message with matching PRN from the other STA shall terminate the protocol on its end unless it has already completed it. In particular, a New STA that correctly receives the NMK may attempt to authenticate with that NMK regardless of whether it receives an abort message later.
Distribution of NMK Using Unicast Key Exchange (UKE)
If both the new STA and an existing STA have suitable user interfaces — alphanumeric entry is not a requirement— the new STA may, upon invitation, establish a private channel with the UIS using Unicast Key Exchange (UKE) method, establish a shared TEK and then obtain the NMK via the TEK-secured communications channel. This also requires that the AVLN be in Simple Connect (SC) Security Level, one STA be in the SC-Join state and the other be in the SC-Add state.
Note: The user may explicitly place a STA already in an AVLN in SC-Join state, causing it to leave its current AVLN and seek another to join (even if it later becomes the CCo as provided below). If the UKE protocol aborts, the STA may resume using the existing NMK. Likewise, an Unassociated STA may be placed in the SC-Add state in order that it continue to use its current NMK (e.g., when this is one previously used in an AVLN, but the other STAs are not currently present).
When an Unassociated STA in the SC-Join state observes another STA in the SC-Join state and determines that it should become the CCo, it shall enter the SC-Add state, generate a new random NMK-SC, and become the CCo of a new AVLN, as specified in Section 7.3.4.4. Once the user has directed the STA to join an AVLN (possibly with a single button press at the STA) and has directed the AVLN to adopt a new STA (possibly with a single button press at a designated STA already on the AVLN), the AVLN can give the STA the NMK. Two stages are involved in this process.

- First, a private channel is established using Unicast Key Exchange (UKE) method.
- Second, the network STA (the one with the NMK to distribute) sends the new STA the NMK over the private channel.

Informative Text

There is some chance that a new STA joins the wrong AVLN, or that an AVLN adopts the wrong new STA. In the former case, the new STA may be directed to join a different AVLN. In the latter case, the AVLN may expel the incorrectly adopted new STA. In extreme cases, the user may have to abandon UKE and use one of the other, more secure methods to distribute the NMK to the desired stations.

Once a shared AES key is established, it shall be used until the protocol is aborted or the TEK is superseded by additional AES encryption keys, subject to limitations (e.g., TEK timeout – refer to Section 7.10.2.6).

Note: Two STAs can use this method to establish a private AES key likely to be known only to themselves and distribute a new NMK-SC, even if they already share a common AES key known to other STAs (e.g., an NMK or an NEK).

To use UKE, the two STAs should receive some positive indication from the user that they are to join the same AVLN at the Simple Connect SL. This requires both STAs to be at the Simple Connect SL, and implies that they both have NMK-SCs. The two STAs first detect each other (using CM_SC_JOIN.REQ/CNF MMEs) and either associate with an existing AVLN or form a new AVLN (if both are Unassociated STAs). Once the two STAs are associated with the same AVLN (known from the TEI Map updates from the CCo), they should establish channel adapted tone maps (refer to Section 5.2.6) and then start the UKE protocol.

UKE requires that the STAs use unicast communications to derive the common TEK. Each STA contributes a secret Hash Key during an exchange of unencrypted, unicast CM_GET_KEY.REQ/CNF MMEs with Requested Key Type=HashKey with the PID=0x03, PMN=0x01 and 0x02 respectively. The STA in SC-Add sends the CM_GET_KEY.REQ MME, and the STA in SC-Join responds with the CM_GET_KEY.CNF MME containing the PEKS chosen by the STA in SC-Join. The two Hash Keys are concatenated and hashed to produce the shared, unauthenticated TEK as defined in Section 7.10.7.2. The secrets (Hash Keys) exchanged by the STAs shall be pseudorandom strings of length 384 octets.

The first two messages in UKE are sent unencrypted. These messages shall be unicast and should be sent using channel-adapted tone maps. These messages should not be retransmitted (that is, if the PB containing a Hash Key is not properly received, a new Hash Key should be generated before retransmitting; alternatively, if either of the two initial messages fails to deliver on the first attempt, then the protocol may be aborted and resumed with a different PRN).

Once both STAs have the TEK derived from the Hash Keys, the STA in SC-Add shall send the STA in SC-Join the NMK and the NID (which shall indicate SC Security Level) in a CM_SET_KEY.REQ MME, containing the nonce received in the previous message, as an encrypted payload encrypted with the TEK with PID=0x03 and PMN=0x03 in a unicast CM_ENCRYPTED_PAYLOAD.IND MME. If the NID received with the NMK in the CM_SET_KEY.REQ MME does not indicate that the SL is SC, the receiver shall abort the

protocol by sending an unencrypted CM_ENCRYPTED_PAYLOAD.RSP with Result set to Abort. Otherwise, the STA in SC_Join shall respond with a CM_SET_KEY.CNF MME, containing the nonce just received, encrypted with the NMK with PID=0x03 and PMN=0xFF in a unicast CM_ENCRYPTED_PAYLOAD.IND MME. This verifies that the NMK was received and concludes the UKE portion of the process.

The new STA shall then go on to authenticate using the NMK to obtain the NEK from the CCo. The entire process for Unassociated STAs is described in Section 7.3.4.3 and Section 7.3.4.4. For one Unassociated STA and one STA in an AVLN, it is described in Section 7.3.5.3.

Distribution of NMK Using Other Key Management Protocols

As an alternative to the methods described in this specification for Authorization, and as with HomePlug AV, GREEN PHY fully supports the use of HLE standards such as 802.1x, EAP, and SNMP.

All messages sent by the HLE for key distribution shall be transmitted as CM_ENCRYPTED_PAYLOAD.IND MMEs with PID=0x04. The 16-octet field used for the IV in encrypted messages shall be used for the UUID (see references [9], [10]) of the protocol sending the messages. This field shall remain constant for the duration of the protocol run. The UUID field may be used by the HLE to distinguish between application protocols using this lower level transport mechanism.

The entire “encrypted” payload portion of the message shall not be interpreted by the sending or receiving STA, and is thus available to the HLE to carry its protocol messages. In particular, the STA shall not check the PID, PRN, or PMN fields across the “encrypted” and “unencrypted” parts of the MME. References to PID, PRN, and PMN in this section only concern the “unencrypted” fields of the MME.

The STA shall use the ODA and its knowledge of TEIs to determine whether or not to broadcast a message it receives from the HLE with PID=0x04. The OSA and/or ODA in these messages might not belong to a STA. All messages in the same protocol run shall use the same PRN (randomly selected by the HLE application at the start of the protocol run), and the first message shall have PMN=0x01. Subsequent messages in the protocol run shall increment the PMN until the last message, which shall have PMN=0xFF. A STA that receives a valid CM_ENCRYPTED_PAYLOAD.IND MME with PID=0x04 from the powerline medium shall pass the entire CM_ENCRYPTED_PAYLOAD.IND MME to its HLE for processing.

If a STA receives (from its HLE or from the powerline medium in response to a message it sent) a valid CM_ENCRYPTED_PAYLOAD.IND MME with PID=0x04 and PMN=0x02, it may choose to associate with the same AVLN of the other STA or form a new AVLN as described in Section 7.3.4 and Section 7.4.1. In particular, this is desirable when one or both of the STAs are unassociated. Sufficient information is present from the messages (the SNID and TEI) that the STAs can communicate using unicast without association, but communication may be more reliable if they are associated with the same AVLN.

The HLEs that generate and process these messages are responsible for properly setting the PRN and incrementing the PMN. A STA that transmits one of these messages using MNBC may repeat that message unchanged multiple times for reliability purposes. A STA that receives duplicate messages (i.e., with the same PID, PRN, and PMN) may discard the duplicate copies silently. The

HLE must be able to manage reception of duplicate messages. It is up to the HLE to generate the response to any message received.

When the HLE sends the last message in the protocol, it shall use PMN=0xFF, regardless of the success or failure of the protocol. If the protocol succeeds in providing an NMK to the new STA, the HLE for the STA receiving the NMK shall use the APCM_SET_KEY.REQ primitive to set the NMK and NID (including the SL) of its STA, as described in Section 7.10.3.3. When both STAs have the NMK, both should also have the same NID, and the STAs should form an AVLN as described in Section 7.3.4.1 or expand an existing AVLN as described in Section 7.3.5.1.

Changing the NMK

If for some reason (e.g., a rogue STA has managed to get into the AVLN) the user suspects a hostile environment, the user may force a change to the NMK. Essentially, this redefines the AVLN and the NID may change along with the NMK. The user shall change the NMK (and typically, the NID) for each STA that held the compromised NMK individually, using direct entry, the DAK if it is available (Section 7.10.3.4), or UKE (Section 7.10.3.5). In the latter case, only an NMK-SC may be distributed.

Changing the NMK may change the NID, which is expected to be a disruptive event. That is, while the STAs in the AVLN are receiving the new NMK, leaving the old AVLN with the compromised NMK and NEK, and joining the new AVLN, they might not be able to sustain QoS levels for ongoing connections. In fact, they may have to terminate existing connections and establish new connections in the new AVLN. The degree to which the STA and the HLE shield applications and the user from these interruptions of services is both implementation and vendor dependent.

NEK Provisioning

The NEK is always provided by the CCo, and always encrypted by the NMK. The NEK shall not be set using any other encryption key or by an unencrypted MME. The NEK is never passed over the H1 interface (neither to the host from the STA nor from the host to the STA). NEK provisioning can be initiated in one of two ways:

A new STA joins an AVLN and is given the NEK (with PID=0x00, Section 7.10.4.1)

The CCo determines to change the NEK for part or all of the AVLN ((with PID=0x01, Section 7.10.4.2)

Provision NEK for new STA

NEK provisioning for a new STA is called Authentication and is described in Section 7.3.3.

Provision NEK for Part or All of the AVLN

The CCo may update the NEK at any time, and is required to do so as specified in Section 7.10.2.5. It does so using the procedure shown in Figure 723. The PID shall be set to 0x01 for all messages in this protocol. The CCo will provision each STA individually to get a positive ACK from each STA. After all active STAs have been provisioned with the new NEK and EKS, the CCo shall cause the change to be effective by putting an Encryption Key Change BENTRY in the Beacon for the appropriate number of Beacon Periods. If a STA that belongs to an AVLN detects an Encryption Change BENTRY in that AVLN's Beacon and the STA does not have the new NEK, it shall request the new NEK from the CCo using the authentication procedure specified in Section 7.3.3. The STA shall not use the new NEK until indicated by the CCo in the Encryption Key Change BENTRY in the Central or Proxy Beacon.

Figure 723: Provision NEK for Part or All of the AVLN

Encryption Key Uses and Protocol Failures

Encryption keys are used for specific purposes, and improper use of these keys is one of several forms of protocol failure.

The NEK is used exclusively for encrypting PBBs (i.e., at the PHY level); that is, only PBBs are encrypted with the NEK, and nothing else may be encrypted with the NEK. All data plane traffic and most control traffic will be between authenticated STAs in an AVLN, and those PBBs will be encrypted using the current NEK for that AVLN. A few messages may be sent unencrypted at the PHY level. For more information, refer to Table 115 in Section 11.1.8.

A failure to decrypt a PBB using the NEK cannot be detected by the PHY; it can only use the PBCS to check that the encrypted PBB was demodulated properly, then decrypt whatever it receives. Proper decryption of the PBB can only be checked by the ICV at the MAC Frame level. Incorrect MAC Frames shall be discarded silently by the receiver, and it is up to the HLE to recover from this loss.

All other keys (DAK, NMK, TEK) are used to encrypt the payload of CM_ENCRYPTED_PAYLOAD.IND MMEs, which are usually sent unencrypted at the PHY level. (Figure 723 is an anticipated exception.) How a STA responds to a CM_ENCRYPTED_PAYLOAD.IND MME depends on how it was sent as well as the ability of the STA to decrypt it and to validate it.

When the PID is 0x04, only the unencrypted fields are checked, and the entire CM_ENCRYPTED_PAYLOAD.IND MME shall be passed from the HLE to the PHY or from the PHY to the HLE without interpreting the “encrypted” (or “uninterpreted”) portion (see Figure 724 and Figure 725).

A STA that receives a CM_ENCRYPTED_PAYLOAD.IND MME shall attempt to decrypt the payload using the key indicated in the PEKS, if it is valid and the PID is not 0x04. Proper decryption is determined by using the last octet to ascertain the length of the Random Filler, then decoding the encapsulated MME for the MME length, and then checking the CRC as well as the Protocol Identifier (PID), PRN, and PMN (refer to Section 7.10.8). These last three should match their unencrypted values exactly. Lastly, if a TEK is used, it must not have expired (refer to Section 7.10.2.6). Failure to decrypt a CM_ENCRYPTED_PAYLOAD.IND MME properly shall cause the recipient to respond with a CM_ENCRYPTED_PAYLOAD.RSP MME indicating failure, unless the CM_ENCRYPTED_PAYLOAD.IND MME was sent with a broadcast address ODA. Note that a broadcast DTEI may be necessary even when the transmission is unicast in the ODA, so the DTEI cannot be used to determine whether a response is needed.

If the CM_ENCRYPTED_PAYLOAD.IND MME is decrypted correctly, other checks must be performed at the level of the protocol. At a minimum:

The PID, PRN, and PMN must be appropriate.

The key indicated in the PEKS and the encapsulated MME type must be appropriate for the PID and PMN.

The nonces, if any, in the encapsulated MME must be valid.

The PID must be between 0x00 and 0x04. All protocol runs shall start with the first message

having PMN=0x01 and end with the last message having PMN=0xFF. If the PMN is greater than 0x01, the PRN must be already known and the Your Nonce field in the current message must match the My Nonce field in the previous message in that protocol run; otherwise, the protocol run is aborted. The PMN must be in the appropriate range for the PID, and must be the next PMN expected in that run of the protocol (the special PMN value of 0xFF is the sole exception and is used to indicate the last message). Once a STA sends or receives a message with PMN=0xFF, it shall ignore all further messages with that PID and PRN. It is recommended that at least 16 of the most recently used sets of {PID,PRN} pairs are stored. Except for PID=0x04, the key indicated by the PEKS must be of the correct type for that PID and PMN, and the MME must be of the correct type for that PID and PMN

A CM_ENCRYPTED_PAYLOAD.IND MME with an incorrect PID, an unknown PRN with PMN greater than 0x01, an out-of-sequence PMN, or an encapsulated MME of the wrong type for the PID and PMN shall be ignored. An exception for duplicate MMEs is noted below. A correct MME type that has other defects may be ignored or, if it is a request, may cause a corresponding confirm to be sent indicating failure. When a confirm MME indicating failure is sent, it shall be sent as the body of an encrypted payload MME that does not encrypt its payload (indicated by PEKS=0xF; refer to Section 11.5.2.1).

The higher protocol must be able to withstand the loss of a message in the protocol sequence. This is done by setting a timer for a time by which a response is expected, and retransmitting the last message if no response has been received by that time. Since these protocol messages are exchanged using CSMA, and may also have to traverse several layers of processing by the recipient, the timer should be set to account for these latencies. When a duplicate of the previous received message in a protocol run is received, then a duplicate of the message sent in response to it (if any) must be sent.

AES Encryption Algorithm and Mode

AES Encryption may be performed either at the PHY Block level, as described in Section 5.4.7.1, and/or within a CM_ENCRYPTED_PAYLOAD.IND MME. Both modes are mandatory.

PHY Block-Level Encryption

As with HomePlug AV, GREEN PHY uses the 128-bit Advanced Encryption Standard (AES) algorithm in CBC Mode. The encryption method is described in Section 5.4.7.1.

The 4-bit Encryption Key Select (EKS) in the Frame Control is an index of the encryption key used for encrypting the PBBs. EKS values are defined in Section 4.4.1.5.2.8. The values instruct the STA about how to encrypt/decrypt the message, including use of no encryption at all.

Payload-Level Encryption

Payload level encryption shall be identical to PHY Level encryption with the following exception:

Only a portion of the payload is encrypted.

The PEKS (called the PEKS to distinguish it from the EKS) identifying the Encryption Key and, if AES encryption is used, the Initialization Vector are carried in the unencrypted portion of the payload.

The bit ordering is different.

The payload shall be padded to a 128-bit boundary as needed. The padding shall be random bits.

CM_ENCRYPTED_PAYLOAD.IND Message Encryption

If encryption is specified in the CM_ENCRYPTED_PAYLOAD.IND message, the encrypted portion of the payload shall be encrypted using 128-bit AES-algorithm in CBC Mode. Refer to Section 5.4.7.1.

Section 13.5 provides an example that shows payload encryption. It should eliminate any confusion about bit ordering, initialization vectors, etc.

Note: The bit ordering for the Encrypted Payload and corresponding Initialization Vector and Encryption Key is different than the bit ordering defined in Section 5.4.7 for PHY Block Body.

Encrypted Payload Encryption Bit Order

The MSB of the first octet of the Encrypted Payload shall correspond to bit number 0 of the AES encoder defined in Section 3.1 of reference [2] Federal Information Processing Standards Publication 197.

Encrypted Payload Initialization Vector Bit Order

The MSB of the first octet of the IV shall correspond to bit number 0 of the AES encoder defined in Section 3.1 of reference [2] Federal Information Processing Standards Publication 197.

When PID=0x04, this field shall be used as a Unique Universal Identifier (UUID, see references [9], [10]). The MSB of the first octet of this field shall correspond to the MSB of octet 0 of the UUID.

Encrypted Payload Encryption Key Bit Order

The MSB of the first octet of the Encryption Key shall correspond to bit number 0 of the AES encoder defined in Section 3.1 of reference [2] Federal Information Processing Standards Publication 197.

Generation of AES Encryption Keys

Generation from Passwords

The HP-AV privacy function may at times require the generation of an encryption key from a password. In all such cases, the mechanism for creating a key from a password shall be the PBKDF1 function, as shown in the PKCS #5 v2.0 standard, Password-based Cryptography Standard, using SHA-256 as the underlying hash algorithm. The iteration count used to calculate the key shall be 1000. The salt value shall be 0x0885 6DAF 7CF5 8185 **for DAKs and** 0x0885 6DAF 7CF5 8186 **for NMK-HSs**. After the 1000^{th} iteration, the leftmost 16 octets of the SHA-256 output (as described in FIPS-180-2 change notice) shall be used as the AES encryption key. The first octet of the output corresponds to octet 0 of the AES encryption key. The bit ordering of the AES encryption key within an octet is dependent on where it is used. Refer to Section 7.10.6.2.1.3 and Section 5.4.5.4.

HP-AV passwords (DPW and NPW) shall be limited to strings of ASCII characters chosen from the range ASCII[32] to ASCII[127]. The length of a DPW shall be between 16 and 64 characters inclusive. The length of a NPW shall be between 8 and 64 characters inclusive. Users shall be provided a warning by the user interface that the entered NPW may not be secure when the user enters a NPW less than 24 characters in length. Passwords are not sent to the Convergence Layer and it is recommended that they not be retained. DPWs should be pseudo-randomly generated and recommended to be a minimum of 20 characters long. It is recommended that pseudo-random NPWs be a minimum of 16 characters long and user-selected NPWs a minimum of 24 characters long.

Automatic Generation of AES Keys

All STAs shall be able to generate Hash Keys (used in UKE) and AES encryption keys (e.g., NEK, NMK, and TEK) directly. The generation of these is implementation dependent. Implementers shall ensure that key and secret generation are based on a good random number generation algorithm. The method used shall be at least as good as the following baseline method. In the baseline method, a station shall use a keyed cryptographic hash algorithm (such as the one used to generate keys from passwords) with a key distinct to the station and not the same as its DAK. It shall maintain an internal counter that is never exposed. This counter value shall be hashed to obtain a pseudorandom number, and the counter shall be incremented each time a pseudorandom number is generated. RFC 4086 [5] and the book on Applied Cryptography by Schneier [6] may be used for guidance.

The TEK for the UKE method is generated from the Hash Keys using SHA-256 as the underlying hash algorithm and truncating the output. The AES key shall be the leftmost 128 bits of output (as described in FIPS-180-2 change notice), and the input shall be the first Hash Key (from the CM_GET_KEY.REQ MME) with the MSB of the least-significant octet of the first Hash Key as the leftmost bit of input to the SHA-256 function, concatenated with the second Hash Key (from the CM_GET_KEY.CNF MME) with LSB of the most-significant octet of the second Hash Key as the rightmost bit of input to the SHA-256 function. Also refer to Section 7.10.3.5.

The iteration count used to calculate the key shall be 0 (i.e., hash once). There shall be no salt. After one iteration, the leftmost 16 octets of the SHA-256 output (as described in FIPS-180-2 change notice) shall be used as the AES encryption key. The first octet of the output corresponds to octet 0 of the AES encryption key. The bit ordering of the AES encryption key within an octet is dependent on where it is used. Refer to Section 7.10.6.2.1.3 .

Generation of Nonces

Generation of nonces shall be done in a way so that the repetition of a nonce is very unlikely and that the nonces are not predictable. A method at least as good as the one described in Section 7.10.7.2 for automatic generation of AES keys shall be used. A possible way to generate a nonce is to use a counter that is passed through a keyed secure hash function. The counter is incremented each time a nonce is generated and the key for the hash is kept private to the station. The same key and counter may be used for generating nonces and random numbers for different purposes, by using additional information specific to the purpose that is also passed through the hash function.

Encrypted Payload Message

The CM_ENCRYPTED_PAYLOAD.IND management message may be exchanged over the medium unencrypted. As such, they are most useful for the processes that establish or distribute keys. They may also be used by higher layer protocols to perform discovery or key distribution (with PID=0x04 - refer to Section 7.10.3.6).

As with HomePlug AV, within HomePlug GREEN PHY, these are used for five distinct purposes:

Distribution of the NEK using the NMK based on a request from a STA seeking to authenticate (PID=0x00 - refer to Section 7.10.4).

Distribution of the NEK using the NMK initiated by the CCo when rotating the NEK (PID= 0x01 – refer to Section 7.10.4)

Distribution of the NMK using the DAK (PID=0x02 – refer to Section 7.10.3.4).
Distribution of the NMK using UKE (PID=0x03 – refer to Section 7.10.3.5).
Execution of higher layer protocols (PID=0x04 – refer to Section 7.10.3.6).
Each of these is given its own PID for use in the PID fields (one unencrypted, one encrypted, except when PID=**0x04**) of the CM_ENCRYPTED_PAYLOAD.IND message. The PID value of 0x04 is set aside for higher layer protocols, so that the MAC knows to pass these messages across the H1 interface uninterpreted. For interpretation of PID values, refer to Section 11.5.2.3 and Table 1184.
Figure 724 shows an entire Encrypted Payload Message when PID is between **0x00** and **0x03**, including all of its components contributed by MAC Framing and other processes.

Figure 724: Encrypted Payload Message when PID is between 0x00 and 0x03
The PEKS indicates the AES encryption key used to encrypt the payload (refer to Section 11.5.2.1 and Table 1182). When used with a higher layer protocol or when a confirm MME indicating failure is sent, a PEKS of No Key (0x0F), may be used to indicate that the payload is not encrypted.
When PID=**0x04**, the 16-octet IV field shall be used for a UUID (see references [9], [10]), and the portion of the CM_ENCRYPTED_PAYLOAD.IND MME from Random Filler to RF Length shall not be interpreted by the STA (see Figure 725). This entire portion shall instead be HLE protocol payload (i.e., the eight fields defined for the encrypted portion are instead defined by the higher layer protocol).

Figure 725: Encrypted Payload Message when PID = 0x04
The limitation of MNBC transmissions to a single PB constrains the length of the CM_ENCRYPTED_PAYLOAD.IND MME to be no more than 502 octets, and the HLE Payload to be no more than 460 octets, unless the CM_ENCRYPTED_PAYLOAD.IND MME is fragmented. Fragmentation at the MAC level is discouraged, however, due to the unreliability of MNBC, and if necessary, should be done by the HLE.
User Interface Station (UIS)
A UIS is any station that is capable of providing a suitable mechanism (preferably keyboard and display) to enable user interaction with the AVLN and capable of supporting network control and security functions for the AVLN. It might not be physically attached to the AVLN (i.e., it might connect through a bridging STA).
There is no limit to the number of UISs that may exist in the AVLN.

Resisting Common Security Attacks

Man-in-the-Middle (MITM)
A man in the middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. In the absence of countermeasures, Key Exchange protocols are vulnerable to this kind of attack.
As with HomePlug AV, GREEN PHY only admits this attack when UKE is in use. If threat

analysis shows this type of attack is likely, then Secure Security Level should be used.

Repetition (Replay) Attacks

Repetition attacks involve the attacker capturing a message or sequence of messages and playing it (them) back at a later time. This attack can be thwarted by the use of Nonces. A nonce is a parameter that varies with time. It can be a timestamp or some other special value that changes with time. The use of nonces reduces the likelihood of replay attacks.

When called for in the specification, a nonce shall be created and included (as My Nonce) in an MME from one STA to another. The receiving STA shall take this value and embed it (as Your Nonce) in the MME it sends in response to the original MME. When the STA that created the nonce receives the reply, it knows with a high degree of certainty that the reply is fresh. A STA sending a nonce in one message is required to verify that the same nonce is returned in the next message of the protocol, if any. A nonce mismatch shall cause the protocol to abort.

Once a particular value has been used as a nonce, it shall not be reused, except within the same protocol run (refer to Section 7.10.2.7). The next time that STA transmits a message that includes a nonce, it shall generate another one. The method used to generate nonces is an implementation decision. Although there is no explicit requirement that a value provided as a nonce not occur again within a specific time interval, implementers shall endeavor to generate nonces using a method that ensures nonce values do not repeat often and that it is not easy to predict the nonce's value. Refer to Section 7.10.7.3.

Discussion of Security Mechanisms (Informative)

The highly structured nature of the contents being encrypted makes these messages susceptible to recognizable plaintext attack. That is, an attacker can tell, with a good deal of certainty, when the right key has been guessed from the structure of the decrypted data. However, the key space is 128 bits and flat, and the keys used for data encryption are randomly selected by the CCo. Therefore, finding the right NEK by brute force is a risk we accept, given the threat model (refer to Section 2.4.2.

Keys based on pass phrases are another issue and come in two varieties:

Device Passwords (DPWs)

Network Passwords (NPWs)

The specification requires these to be at least 12 characters long, selected from a range of ASCII 32 – 127 (96 characters). The DPW must be randomly chosen by the OEM, so its entropy should be at least 6 bits per character ($\log_2(96) > 6.5$). With a 20-symbol DPW, this should translate to at least 120 bits of search space. Only if an OEM uses short or non-random DPWs could this be a problem. Even the shortest (12 symbols) random DPWs should be equivalent to 12x6.5 = 78 bits, which can be brute-forced, but not without great effort. The threat model is for typical individuals, not for well-heeled governments or corporations. If the data requires protection against greater threats than this, higher level security should be applied. The recommended minimum length of 15 characters for DPWs and machine generated NPWs is equivalent to 97.5 bits.

NMKs are used infrequently, and are also 128 bits long. Brute forcing these should be no easier than brute-forcing the NEKs, with the exception of NMKs based on user-chosen NPWs. These NPWs must be at least 12 characters long, and are recommended to be at least 24 characters long. With natural language entropy of 2-3 bits per character, these lengths translate to 48-72 bits of

entropy in the key. NPWs of length up to 64 characters are supported, providing 128 bits of entropy in the key for users concerned about weak NPWs.
The use of distinct salts for generation of DAK and NMK-HS means that an attacker cannot use a table generated for one of these types of keys to attack another type of key.
Initialization vectors are either random (in encrypted payload MMEs) or are derived from the frame control, the PB header, and the position of the PB within the MPDU. While it is possible for an IV to repeat in less than the hour maximum between NEK changes, the primary threat in CBC mode is recognized ciphertext. The contents are likely to be different in high-speed multimedia streams, and for MMEs, a random confounder is included to thwart this attack.
TEKs derived through the UKE process are based on secret Hash Keys provided by the initiator and the respondent. These are each 384 octets long, and while they are sent in the clear, they should be sent in unicast messages, which should use channel-adapted tone maps. To intercept one of these correctly, the eavesdropper would at the least have to use non-standard equipment capable of receiving unicast MPDUs not destined for it. If the MPDUs are sent using channel adapted tone maps, the eavesdropper would have to know the tone map used, and have a signal to noise ratio at least as good as the receiver on the majority of the carriers. Otherwise, there are likely to be too many bit errors for the FEC to correct. The systematic bits may be recovered with confidence level, however, leaving the attacker with reasonable certainty in some of the received bits. For the hash function to produce the right key, however, all of the input bits must be correct, so the attacker must guess values for all uncertain bits. The hash key length provides 6144 bits total for hashing, so if the attacker is uncertain about only 1% of these, he still has to search a 61-bit space. To intercept these unicast messages at all, non-standard equipment must be used, and due to attenuation and frequency-selective fading, the attacker would have to have access to the power lines comparable to the user himself.
Network Power Management
If the CCo of an AVLN does not detect a valid AV Frame Control (excluding Beacon Frame Controls) from STAs that are associated with its AVLN for at least 30 seconds, the CCo shall enter Network Power Saving Mode.
In Network Power Saving Mode, the CCo shall:
Set the NPSM bit in the Beacon.
Specify a schedule consisting of only the Beacon Region, a CSMA Region of length equal to minCSMARegion, and a Reserved Region of sufficient size to support any necessary Discover Beacons and Proxy Beacons. The remainder is specified as Stayout region.
Upon detection of a valid AV Frame Control (excluding Beacon Frame Controls) from a STA associated with its AVLN, the CCo shall exit NPSM and reset the NPSM bit in the Beacon. It may then update the schedule to make additional time available in the CSMA Region.
Since a HSTA cannot rely on the CCo detecting its transmissions to exit Network Power Saving Mode, the PCo shall monitor the CSMA Region while in Network Power Saving Mode, and shall send a CP_PROXY_WAKE.REQ to the CCo if it detects a valid AV Frame Control.

Multiple Networks
Overview of Network Operation Modes

In certain scenarios, an AVLN may detect other HomePlug-based neighboring networks. In general, six types of HomePlug neighbor networks can be present:

- HomePlug 1.0.1-based in-home networks: HomePlug 1.0.1 in-home networks are identified by the INVALID field in the HomePlug 1.0.1 EOF set to 0b0 and the RSVD field in the HomePlug 1.0.1 EOF set to 0b0000000000.
- HomePlug 1.1-based networks: HomePlug 1.1 in-home networks are identified by the INVALID field in the HomePlug 1.0.1 EOF set to 0b0 and bit number 8 in the HomePlug 1.0.1 EOF set to 0b1.
- HomePlug 1.0.1-based Access network: HomePlug 1.0.1 Access networks are identified by the INVALID field in the HomePlug 1.0.1 EOF set to 0b0 and bit number 9 in the HomePlug 1.0.1 EOF set to 0b1.
- HomePlug 1.0.1-based Access network with VoIP Provisioned: HomePlug 1.0.1 Access networks with VoIP provisioned are identified by the INVALID field in the HomePlug 1.0.1 EOF set to 0b0 and bit number 10 in the HomePlug 1.0.1 EOF set to 0b1.
- HomePlug AV-based or HomePlug GREEN PHY in-home networks: HomePlug AV and GREEN PHY in-home networks have the Access bit in the AV delimiter set to 0b0.
- HomePlug AV-based Access networks: HomePlug AV Access networks have the Access bit in the AV delimiter set to 0b1.

Note: A network can be simultaneously a HomePlug 1.1 based network and a HomePlug 1.0.1 based Access network. This indicates that the HomePlug 1.0.1 based Access network is HomePlug 1.1 capable (refer to Section 9.8). Similarly, a network can be simultaneously a HomePlug 1.1 based network and a HomePlug 1.0.1 based Access network with VoIP provisioned. A network can be both a HomePlug 1.0.1-based Access network and a HomePlug 1.0.1-based Access network with VoIP provisioned at the same time.

Detection of HomePlug 1.0.1-based in-home networks (1) will only affect the Hybrid mode of operation of the AVLN. However, for all other cases, the network mode of the AVLN can also change based on the CCo capability, the type of neighbor network detected, and the network policy for behavior in the presence of neighboring networks.

An AVLN operates in one of the following three modes based on the CCo Capability and Neighbor Network detection:

CSMA-Only Mode

Uncoordinated Mode

Coordinated Mode

CSMA-Only Mode

All STAs shall support CSMA-Only mode. Beacon Period structure and Channel Access Mechanism in CSMA-Only mode is described in Section 5.1.2.1. Transitions into and out of CSMA-Only mode are described in Section 8.5.

If a CCo operating in CSMA-Only mode can reliably detect Central or Proxy Beacons from one or more AVLN operating in Coordinated mode, it shall adjust its schedule and perform Passive Coordination with one and only one of those AVLNs. Passive Coordination provided by CCo operating in CSMA-Only mode enables Level-2 CCos to support TDMA even in the presence of neighboring AVLNs operating in CSMA-Only mode. Section 8.4 provides details on Passive

Coordination.

CSMA-Only Mode for GREEN PHY

Since CSMA is the only required mode for GREEN PHY, a GREEN PHY station is required to be capable of operating as a Level-0 CCo. Refer to Chapter 11, Table 11-5b for a comparison of Level-0 CCo functionality between HPAV L0 CCo and HP GP L0 CCo

Uncoordinated Mode

Uncoordinated mode is only supported by Level-1 and Level-2 CCos. Beacon Period structure and Channel Access Mechanism in Uncoordinated mode is described in Section 5.1.2.1. Transitions into and out of Uncoordinated mode are described in Section 8.5.

A CCo operating in Uncoordinated mode shall generate its own timing and transmit its periodic Beacon independently of other networks. In Uncoordinated mode, QoS can be guaranteed by allocating dedicated contention-free allocations to applications that require QoS.

Uncoordinated Mode for GREEN PHY

A GREEN PHY station must be capable of being a member of an AVLN operating in Uncoordinated Mode. However, a station that only implements GREEN PHY is not required to be a Level-1 or Level-2 CCo.

Coordinated Mode

Coordinated mode is only supported by a Level-2 CCo. Section 8.2.1.1 and Section 5.1.2.2.1 provide details about the Beacon Period Structure and neighbor network coordination in Coordinated mode. Transitions into and out of Coordinated mode are described in Section 8.5.

In Coordinated mode, a network shall share bandwidth with Level-2 neighboring networks in its INL, such that QoS can be guaranteed within each network by using Reserved Regions. Further, networks in Coordinated mode shall also provide a larger Minimum CSMA Region to neighboring networks operating in CSMA-Only mode (refer to Section 8.4).

In Coordinated Mode, the Regions BENTRY (refer to Section **4.4.3.15.3**) of the Beacon of a network shall be compatible with the Regions BENTRY of other networks in its INL. For example, if one network specifies a Reserved Region and a network in the INL specifies a Stayout Region in the same interval, the two schedules are said to be compatible. On the other hand, if a network specifies a Reserved Region and a network in the INL specifies a CSMA Region, they are said to be incompatible. The rules used to compute a compatible schedule are described in Section 8.3.3.

Coordinated Mode for GREEN PHY

A GREEN PHY station must be capable of being a member of an AVLN operating in Coordinated Mode. However, a station that only implements GREEN PHY is not required to be a Level-2 CCo.

Overview of Beacon Period Structure

A Beacon Period is made up of some or all of the following five Regions. Its structure is specified in the Regions BENTRY of the Beacons for use by neighboring CCos.

Beacon Region: Beacon Region is only present when the network is operating in Uncoordinated or Coordinated mode. Beacon Region indicates the TDMA allocation during which Central Beacons of the AVLNs are transmitted. The Beacon Region consists of one to a maximum of MaxBeaconSlot Beacon Slots. In Uncoordinated mode, exactly one Beacon Slot is present. In Coordinated mode, one or more Beacon slots are present. The duration of each Beacon Slot is

equal to the sum of the duration of a Beacon PPDU and the subsequent Beacon-to-Beacon Interframe Space (B2BIFS) Space (B2BIFS). Each CCo transmits a Beacon in one of the Beacon Slots every Beacon Period. The NumSlots, SlotID, and SlotUsage fields in the Beacon Frame Control and Beacon MPDU Payload (Section 4.4.1.5.1 and Section 4.4.3) are used to specify the Beacon Region structure of a network. STAs within an AVLN use this information to determine the duration of the Beacon Region.

CSMA Region: STAs in a network are allowed to contend for the channel with other STAs using CSMA/CA in this region. Communication between two or more interfering networks is possible if they have an overlapping CSMA Region. For each network in Coordinated or Uncoordinated mode, there shall be a CSMA Region (called "Minimum CSMA Region") immediately following the Beacon Region to support these two functions. Refer to Section 8.2.1 for more details.

Reserved Region: Reserved Regions are only present when the network is operating in Uncoordinated or Coordinated mode. A Reserved Region is a time interval that is reserved by a network. The network that owns the Reserved Region shall schedule the transmission of its contention-free Links here. In addition, the AVLN may also schedule CSMA allocations that can be used only by the STAs in that network. A network may have any number of Reserved Regions in a Beacon Period. Persistent and Non-Persistent Schedule BENTRYs (refer to Section 4.4.3.15.4.2 and Section 4.4.3.15.4.1) are used to provide the details of all the contention-free allocations and CSMA allocations in the Reserved Regions. When a network specifies a Reserved Region in a certain time interval, all its interfering networks shall specify a Stayout Region (to be defined next) in the same interval.

Note: It is possible to have two non-interfering networks specify a Reserved Region in the same interval. This results in channel reuse with a higher total capacity.

Stayout Region: A network operating in Coordinated mode shall specify a Stayout Region if one or more of the neighboring networks in its INL have specified a Reserved Region or a Protected Region in the same interval. A network operating in CSMA-Only mode and providing Passive Coordination to a CCo in Coordinated mode shall specify a Stayout Region in all regions other than the CSMA Regions. The CCo shall not allow stations in its network to transmit in a Stayout Region.

Protected Region: Protected Region is only present when the network is operating in Coordinated mode. When a CCo detects the existence of another group with a different timing and if it optionally decides to coordinate with networks in that Group, it shall specify a Protected Region in the same interval where the Beacon Region of the other group is located. The CCo shall not allow stations in its network to transmit in a Protected Region.

Table 81 shows the interaction between the different Regions.

Table 81: Interaction Between Different Regions

Owner CCo	Neighbor Coordinator That Hears the Owner and is in the Same Group	Neighbor Coordinator That Hears the Owner and is in a Different Group
BEACON	BEACON	PROTECTED
PROTECTED	PROTECTED or STAYOUT	BEACON
RESERVED	STAYOUT	STAYOUT

CSMA	CSMA or STAYOUT	CSMA or STAYOUT

Minimum CSMA Region Requirement

Each network operating in Uncoordinated mode or Coordinated mode shall specify a CSMA Region, called the Minimum CSMA Region, immediately following the Beacon Region. This Minimum CSMA Region, together with other CSMA Regions located elsewhere in the Beacon Period, may be used for the following:

Exchange of priority-based user data between STAs using CSMA/CA.

New STAs to associate with the network.

Existing STAs to exchange management messages with the CCo (e.g., to set up a new Link).

New CCos to exchange management messages to establish new Neighbor Networks.

Existing Neighbor Coordinators (NCos) to exchange management messages with the CCo (e.g., to share bandwidth, or to change the number of Beacon Slots).

The duration of this Minimum CSMA Region must be greater than or equal to a system parameter, MinCSMARegion.

The start time of the Minimum CSMA Region is equal to the end time of the Beacon Region and, therefore, it changes as the number of Beacon Slots in the Beacon Region changes. Furthermore, the minimum duration requirement of the Minimum CSMA Region imposes a lower limit on the end time of the Minimum CSMA Region. Any Reserved Regions or Stayout Regions that may have located within this lower limit must be converted to a CSMA Region.

GREEN PHY Preferred Allocation and Minimum CSMA Region

When GPP allocation is present, the GPP allocation shall immediately follow the Beacon Region and the Minimum CSMA region shall immediately follow the GPP allocation (refer to section 7.8.5).

Coordinated Mode

Coordinated mode is only supported by Level-2 CCos. A Level-2 CCo typically operates in Coordinated mode if it detects one or more Level-0, Level-1, or Level-2 CCos. Refer to Section 8.5 for details on when a Level-2 AVLN operates in Coordinated mode.

It is important to note that Level-2 CCo can operate in Coordinated mode even if it detects only Level-0 or Level-1 AVLNs. In this case, the Beacon Region in Coordinated mode will only have one Beacon Slot and the Level-2 CCo provides fair share of CSMA Region to the neighboring Level-0/Level-1 AVLNs that are passively coordinating (refer to Section 8.4).

The following section provides details about neighbor network coordination between various Level-2 CCos operating in Coordinated mode.

Interfering Network List

Each Level-2 CCo must maintain an Interfering Network List (INL). The INL of a CCo (or of a network) contains the list of all Level-2 networks that interfere with the network controlled by the CCo.

It is assumed that if two Level-2 CCos can detect each other's Beacon transmissions, the two networks interfere with each other. Furthermore, it is assumed that all STAs in the two networks also interfere with each other.

Note: Two interfering Level-2 networks might not coordinate with each other if they are in different Groups (refer to Section 8.3.2). In this case, the two interfering networks might not be in

each other's INL, even though the two networks interfere with each other.

Group of Networks

A Group of networks is defined as a collection of one or more Level-2 networks that have the same system timing (that is, the Beacon Periods of these networks align with each other). It is possible to have two or more Groups of networks in the vicinity of each other. Refer to Section 8.3.5.1.1 for an example.

Network coordination between interfering networks that are in the same Group is mandatory.

Network coordination between interfering networks that are in different Groups is optional.

Determining a Compatible Schedule

If the new CCo establishes a new network in Uncoordinated Mode, initially it shall specify a Beacon Region with one Beacon Slot, a random contention-free allocation for the transmission of Discover Beacons and CSMA allocations for the remainder of the Beacon Period.

Alternatively, if a new Level-2 CCo joins an existing group of networks in Coordinated Mode, the schedule of its Beacon must be compatible with the schedules of the existing networks in its INL. The rules to determine a compatible schedule are given in this section. First, the new CCo shall find out the combined effect of the schedules of all the networks in its INL, called the INL allocation, using the procedure described in Section 8.3.3.1.

Once the INL allocation is computed, the rules used by a new CCo to set the Region Types of the Regions BENTRY are as follows. Initially, the new CCo shall not specify any Reserved Regions.

If the INL allocation is a Beacon Region and the first entry, the new CCo shall specify a Beacon Region. However, if it is not the first entry, the new CCo shall specify a Protected Region

Otherwise, if the INL allocation is a Protected Region or a Reserved Region, the new CCo shall specify a Stayout Region.

Otherwise, the new CCo shall specify a CSMA Region in all other intervals.

Once a network is established in Coordinated Mode, the rules used by an existing CCo to set the subsequent Region Types of the Regions BENTRY are as follows:

If the INL allocation is a Beacon Region and if it is the first entry, the existing CCo shall specify a Beacon Region. However, if it is not the first entry, the existing CCo shall specify a Protected Region.

If the INL allocation is a Protected Region or a Reserved Region, the existing CCo shall specify a Stayout Region.

If the INL allocation is a CSMA Region, the existing CCo shall specify a CSMA Region. The existing CCo may propose to use this time interval in the future (refer to Section 8.3.5).

If the INL allocation is a Stayout Region, the existing CCo may specify a CSMA Region or a Reserved Region. The existing CCo may propose to use this time interval in the future (refer to Section 8.3.5).

Computing the INL Allocation

The CCo shall decode the Beacons of all the networks in its INL and compute the combined effect of their allocations. This is called the INL allocation. For example, if one neighbor network in the INL specifies a Reserved Region and another neighbor specifies a CSMA or Stayout Region, the resultant INL allocation is a Reserved Region, because a Reserved Region "outweighs" both CSMA and Stayout Regions.

Figure 81 shows the algorithm that a CCo uses to compute its INL allocation. In the algorithm, it is assumed that numeric values are assigned to BEACON, PROTECTED, RESERVED, CSMA, and STAYOUT and the values are such that BEACON > PROTECTED > RESERVED > CSMA > STAYOUT to make the flowchart simpler. It has nothing to do with the RT field defined in the Regions BENTRY.
The inputs of the algorithm TYPE[n][i] and ENDTIME[n][i] are obtained from the RT and RET fields of the Region's message of all neighbor Beacons, where "n" represents which neighbor network, and "i" represents which schedule for that neighbor network. The entries TYPE[n][] and ENDTIME[n][] for each network shall be shifted, if necessary, to account for any difference in system timing.

Figure 81: Flowchart for Computing INL Allocation
Table 82 summarizes the rules in determining the INL allocation. The CCo concerned has two interfering networks in its INL:
Network A
Network B
The Regions BENTRY of network A and network B are shown in the first and second columns of Table 82. The resultant INL allocation is shown in the third column.
Table 82: Rules for Computing INL Allocation

Region Type of Neighbor A	Region Type of Neighbor B	INL Allocation of Neighbors A and B
BEACON	BEACON, PROTECTED, RESERVED, CSMA, or STAYOUT	BEACON
PROTECTED	BEACON	BEACON
PROTECTED	PROTECTED, RESERVED, CSMA, or STAYOUT	PROTECTED
RESERVED	BEACON	BEACON
RESERVED	PROTECTED	PROTECTED
RESERVED	RESERVED, CSMA, or STAYOUT	RESERVED
CSMA	BEACON	BEACON
CSMA	PROTECTED	PROTECTED
CSMA	RESERVED	RESERVED
CSMA	CSMA, or STAYOUT	CSMA
STAYOUT	BEACON	BEACON
STAYOUT	PROTECTED	PROTECTED
STAYOUT	RESERVED	RESERVED
STAYOUT	CSMA	CSMA
STAYOUT	STAYOUT	STAYOUT

Communication between Neighboring CCos

Either Multi-Network Broadcast, as in Section 5.4.3.1, or unicast MPDUs shall be used for communication with a neighbor CCo. No association is required.
When unicast MPDUs are used for communication with a neighbor network, the SNID and DTEI of the neighbor CCo and an STEI of 0x00 shall be used. The PHY transmit clock for the unicast PPDU shall be based on the current estimate of the PHY Clock frequency of the neighbor CCo. These unicast MPDUs shall be limited to one segment and shall only contain MAC Management Messages. The PHY Block Body shall be unencrypted and EKS shall be set to 0b1111.

Neighbor Network Instantiation

If a CCo has determined that it will create a Neighbor Network, the CCo shall examine the Beacon Region of the Group it chooses to join. Based on the number of Beacon Slots and the occupancy of the Beacon Slots in the Beacon Region, the CCo performs the following:
If there are fewer than MaxBeaconSlot Beacon Slots in the Beacon Region, or if the CCo can find a vacant Beacon Slot to use, the CCo shall try to create a network in Coordinated Mode (refer to Section 8.3.5.1). The neighbor network instantiation is completed.
Otherwise, if the Beacon Region has MaxBeaconSlot Beacon Slots already and the CCo cannot find a vacant Beacon Slot to use, the behavior is to instantiate a network in Uncoordinated Mode.
Procedure to Establish a New Network in Coordinated Mode
To establish a new network in Coordinated Mode, the (new) CCo shall choose a SNID, find a vacant Beacon Slot in the Beacon Region to use, and specify a Beacon Period structure that is compatible (refer to Section 8.2 where the "compatible" rules are defined) with all the networks that are in its INL. Key steps include:

- Choosing a SNID. The new CCo first exchanges the NN_INL.REQ and NN_INL.CNF messages with the neighbor coordinators (NCos) in its INL. This step allows the new CCo to ascertain the SNID and NID of the interfering networks of an NCo. The new CCo shall then randomly choose a SNID value which is not being used by any of its NCo, or by any interfering networks of its NCos.
- Finding a Vacant Beacon Slot. The new CCo shall decode all Central, Discover, and Proxy Beacons that can be reliably detected to determine what Beacon Slots are available. The NumSlots field in the Beacon Variant Fields and the SlotID and SlotUsage fields in the Beacon payload field provide information about the Beacon Region structure of a network. The new CCo shall find a common Beacon Slot that is indicated as "free" in the SlotUsage field of all Beacons that are detected, including Central, Proxy, and Discover Beacons of any network.

If a vacant Beacon Slot cannot be found, the new CCo shall propose to use a new Beacon Slot (subject to the maximum limit of MaxBeaconSlot).

- Specifying a Compatible Beacon Period structure. After the new CCo sends a NN_NEW_NET.REQ message to request to establish a new neighbor network, the existing NCo shall return in the NN_NEW_NET.CNF message a Beacon Period structure (or schedule) that the NCo is going to use. The new CCo shall compute a compatible Beacon Period structure based on the schedules returned by all the NCos.

The procedures for establishing a new network in Coordinated Mode are shown in Figure 82 and described below. In Figure 82, it is assumed that the new CCo can decode Beacons from two

existing CCos (NCo 1 and NCo 2). In Case 1, both NCo #1 and NCo #2 accept the new CCo's request to set up a new AVLN. In Case 2, NCo #2 rejects the request.

After determining a SNID value, and a vacant Beacon Slot, the new CCo shall exchange the NN_NEW_NET.REQ and NN_NEW_NET.CNF messages with the NCos in its INL to establish a new network in Coordinated Mode. If the Result codes in all the NN_NEW_NET.CNF messages from the NCos are "Successful," the new CCo shall determine a compatible schedule to use based on the neighbor schedules returned by the NCos and establish a new neighbor network.

First, the new CCo shall send an NN_NEW_NET.REQ message to each of the NCos in its INL. The message shall be unencrypted and be sent in the CSMA Region specified by the Region BENTRY of each NCo's Beacon.

The NN_NEW_NET.REQ message contains the Beacon Slot number that the new CCo plans to use to transmit its new Beacons.

If the Beacon Slot specified in the NN_NEW_NET.REQ message does not exist, the message also implicitly requests NCos that are in the same Group to increase the size of the Beacon Region appropriately (subject to the maximum of MaxBeaconSlot Beacon Slots in a Beacon Region), and implicitly requests NCos that are in a different Group to increase the duration of its Protected Region appropriately (or to create a new Protected Region).

Consequently, NCos in the same Group that the new CCo chooses to join shall invoke the procedure in Section 8.3.5.2 to change the number of Beacon Slots in the Beacon Region. For NCos that are not in the Group that the new CCo chooses to join, if they decide to coordinate with the new CCo, they shall invoke the procedure in Section 8.3.6 to specify a Protected Region that overlaps with the Beacon Region proposed by the new CCo.

Next, the NCo shall reply the new CCo with an NN_NEW_NET.CNF message. If the new CCo's request is accepted by the NCo, a successful result code shall be returned in the NN_NEW_NET.CNF message. The NCo shall also specify its schedule in the NN_NEW_NET.CNF message, and shall not change its schedule until it has received the NN_NEW_NET.IND message from the new CCo. If the NCo rejects the new CCo's request, an unsuccessful result code shall be returned instead. Any NCo that is not in the same Group as the new CCo may choose not to coordinate with the new CCo and simply return a NN_NEW_NET.CNF message with the result code set to "unsuccessful, not in the same Group".

After the new CCo has received the NN_NEW_NET.CNF message with a successful result code from the NCo, it shall send the NN_NEW_NET.REQ message to the next NCo in its INL, and wait for the NN_NEW_NET.CNF message. This exchange of NN_NEW_NET.REQ/CNF messages shall continue with all the NCos in the INL as long as the NN_NEW_NET.CNF message has a successful result code.

Finally, when the new CCo has received NN_NEW_NET.CNF messages from all the NCos in its INL, it shall send the NN_NEW_NET.IND message back to the NCos. If all the NCos have replied with a successful result code in the NN_NEW_NET.CNF message, the status field of the NN_NEW_NET.IND message shall be set to "Go" to confirm that the new CCo is going to establish a new network. Furthermore, the new CCo shall compute a compatible schedule based on the neighbor schedules returned by the NCos in the NN_NEW_NET.CNF messages.

If an NCo has replied with an unsuccessful result code in the NN_NEW_NET.CNF message, the

new CCo shall stop the exchange of NN_NEW_NET.REQ/CNF messages with other NCos in its INL. The new CCo shall send an NN_NEW_NET.IND message with a status field of “Cancel” to inform the NCos that the request has been cancelled. The CCo shall send the NN_NEW_NET.IND message only to those NCos that have replied with a successful result code in the NN_NEW_NET.CNF message.

Figure 82: MSC to Set Up a New Network in Coordinated Mode

New Network Instantiation Amid Two Groups of Networks

A new CCo may detect two or more Groups of networks in the vicinity of each other (see Figure 83 for an example). In this example, two existing networks (NCo #1 and NCo #2) cannot detect each other’s Beacons, and there is a fixed time offset between their Beacon Period boundaries. When a new STA (CCo) wants to start a new network, the new CCo can detect and decode the Beacons from both NCo #1 and NCo #2. Since the timings of the two existing networks are different, the new CCo shall acquire only one of the two timings.

In the example, the new CCo chooses the same timing as NCo #1. The new CCo shall exchange the NN_NEW_NET.REQ/CNF/IND messages with NCo #1 to establish a new neighbor network in Coordinated Mode. The new network and the network of NCo #2 may cause interference to each other because they do not coordinate with each other.

The new CCo may optionally exchange the NN_NEW_NET.REQ/CNF/IND messages with NCo #2, in addition to NCo #1. The Offset field in the NN_NEW_NET.REQ message sent to NCo #2 is set to a non-zero value to indicate that the new CCo has a different system timing than NCo #2. If NCo #2 accepts the request of the new CCo, all three networks shall coordinate with each other. The new CCo shall specify a Protected Region in the same interval where NCo #2 has specified a Beacon Region.

Figure 83: New CCo Detects Two Groups of Networks

Changing the Number of Beacon Slots

When a CCo in a Group of networks determines that the number of Beacon Slots needs to be changed, the Change NumSlots BENTRY is added to the Central Beacon with NewNumSlots set to the new proposed value for NumSlots. The NumSlot Change Countdown (NSCCD) field should be set to a value large enough to ensure the BENTRY will propagate to and from the furthest CCo in the Group. A value of at least 16 is recommended.

All CCos in a Group of networks that detect a Change NumSlots BENTRY in the Central Beacon of another CCo in the Group shall add the BENTRY to their Central Beacon. The value for NewNumSlots shall be the larger of the highest SlotID of CCos it directly detected in the Group or the value of NewNumSlots detected in the BENTRY of the other Central Beacons. NSCCD must be set to assure the value is identical for all Central Beacon in a Beacon Period of the Group.

Any CCo in a Group of networks that detects a higher value for NewNumSlots or NSCCD in the BENTRY of another Central Beacon in the Group shall change the corresponding field in their BENTRY to match the larger value.

The change becomes effective in the Beacon Period following the Beacon Period where NSCCD reaches 1. When the change becomes effective, the NumSlots field in the Beacon MPDU Payload

Informative Text

In this scenario (refer to Figure 84), initially network A is operating in Uncoordinated Mode and a new STA (CCo B) applies to start a new network.

When CCo B receives this message, it shall increase the number of Beacon Slots by one, and then send an NN_NEW_NET CNF message with a successful result code to CCo B.

CCo B shall then send an NN_NEW_NET IND message to CCo A to confirm the establishment of the new network.

Setting the Value of SlotUsage Field

A CCo in Coordinated Mode shall set the SlotUsage field (refer to Section 4.4.3.8) according to the following rules:

The bit corresponding to the Beacon Slot where the CCo transmits its own Beacon shall be set to 0b1.

The bit corresponding to the Beacon Slot where Beacons of a network are regularly detected shall be set to 0b1.

Remaining bits shall be set to 0b0.

Discover and Proxy Beacons shall set the SlotUsage field according to the following rules:

The bit corresponding to the Beacon Slot where Beacons of a network are regularly detected shall be set to 0b1.

Remaining bits shall be set to 0b0.

Note: The SlotUsage Field of Beacon transmissions of STAs in an AVLN might not match the SlotUsage Field of the AVLN's CCo. A STA in the AVLN will set the SlotUsage field to 0b0 for the SlotID of the Central Beacon for its AVLN if it is a Hidden STA. A CCo shall consider a Beacon Slot available if the bit is set to 0b0 in all Beacon transmissions that can be reliably detected including Discover and Proxy Beacons.

Examples

Neighbor network instantiation in three scenarios are described below.

Scenario One

Informative Text
In this scenario (refer to Figure 84), initially network A is operating in Uncoordinated Mode and a new STA (CCo B) decides to start a new network.
The Beacon of network A specifies that there is only one Beacon Slot in the Beacon Region.
CCo B sends an NN_NEW_NET.REQ message to CCo A. The message requests to use a new Beacon Slot, with SlotID=1, which is the second slot in the Beacon Region of network A.
When CCo A receives this message, it shall increase the number of Beacon Slot by one, and then send an NN_NEW_NET.CNF message with a successful result code to CCo B.
CCo B shall then send an NN_NEW_NET.IND message to CCo A to confirm the establishment of the new network in Coordinated Mode. CCo B will start transmitting its Beacons in the new Beacon Slot.
Network A shall then transition to Coordinated Mode.

Figure 84: Scenario One: Network A is in Uncoordinated Mode and CCo B Wants to Create a New Network

Scenario Two

Informative Text
Scenario Two is a continuation of Scenario One. In this scenario (refer to Figure 85), networks A and B are in Coordinated Mode and a new STA (CCo C) decides to start a new neighbor network. CCo C can decode Beacons from network B, but cannot decode Beacons from network A.
The Beacons of network B specify that the two Beacon Slots are occupied. Therefore, CCo C sends an NN_NEW_NET.REQ message to CCo B requesting to use a new Beacon Slot, with SlotID=2, which is the third slot in the Beacon Region.
When CCo B receives the message, it must first coordinate with the networks in its INL (i.e., network A) to increase the Beacon Region to three Beacon Slots using the Change NumSlots BENTRY.
Note: If CCo A and CCo B were in different Groups, the Change NumSlots BENTRY implicitly requests CCo A to change the duration of its Protected Region.
When the NumSlot Change Countdown is complete, CCo B shall send an NN_NEW_NET.CNF message to CCo C to accept its request to start the new neighbor network.
CCo C shall then send an NN_NEW_NET.IND message to CCo B to confirm the establishment of a new network. The SlotUsage field of the Beacon MPDU Payload for each CCo shall indicate only the Beacon Slots that are directly detected as occupied by the CCo or STAs in the CCo's AVLN as defined in Section 8.3.5.3. In this example, it is assumed that STAs in network A cannot detect CCo C and STAs in network C cannot detect CCo A.

Figure 85: Scenario Two: Networks A and B are in Coordinated Mode and CCo C Wants to Create a New Network

Scenario Three

Informative Text
Scenario Three is a continuation of Scenario Two. In this scenario (refer to Figure 86), networks A, B, and C are in Coordinated Mode, and a new STA (CCo D) decides to start a new neighbor network. CCo D and STAs in network D can decode Beacons from network C only. Also, STAs in network A and network B cannot detect CCo D.
The SlotUsage field of Beacons of network C specifies that the first three Beacon Slots are occupied. Therefore, CCo D sends an NN_NEW_NET.REQ message to CCo C requesting to use SlotID=3, which is the fourth slot in the Beacon Region.
When CCo C receives the message, it must first coordinate with the networks in its INL (i.e., network B) to increase the Beacon Region to four Beacon Slots using the Change NumSlots BENTRY. When the NumSlot Change Countdown is complete. CCo C shall then reply with an NN_NEW_NET.CNF message, accepting the CCo D's request. CCo D shall then send an NN_NEW_NET.IND message to CCo C to confirm the establishment of the new network.
In another possible scenario, a new STA (CCo E) can detect CCo A and CCo B and cannot detect the other networks. CCo E would select Beacon SlotID=3 since CCo A, CCo B, and all of the Discover and Proxy Beacons in those networks indicate it is free in the SlotUsage field. In this case, CCo E and CCo D will share the same Beacon Slot. Additionally, the Change NumSlots BENTRY is not necessary, since the number of Beacon Slots does not change.

Figure 86: Scenario Three: Networks A, B, and C are in Coordinated Mode and CCo D Wants to Create a New Network

Procedure to Share Bandwidth in Coordinated Mode

This section describes the procedure for sharing bandwidth between neighboring AVLNs operating in Coordinated Mode.

- The (source) CCo that requests to share new bandwidth with the NCos in its INL shall first determine new time interval(s) that it desires to reserve. Section 8.2 describes the rules that an existing CCo uses to choose a compatible schedule.
- The CCo shall send the NN_ADD_ALLOC.REQ message to each of the NCos in its INL. The message contains the additional time interval(s) that the source CCo is requesting.
- If the bandwidth request is accepted, the NCo shall reply with the NN_ADD_ALLOC.CNF message with a successful result code. The NCo shall also change the Region's message of its Beacon to reflect the changes in the schedule. Otherwise, the NN_ADD_ALLOC.CNF message with an unsuccessful result code is returned.
- When the CCo receives responses from all the NCos in the INL, it shall send the NN_ADD_ALLOC.IND message to the NCos in the INL. If all the NCos have replied with a successful result code in the NN_ADD_ALLOC.CNF message, the status field of the NN_ADD_ALLOC.IND message shall be set to "Go" to confirm that the CCo is going to reserve the time interval.
- If one or more NCos have replied with an unsuccessful result code in the

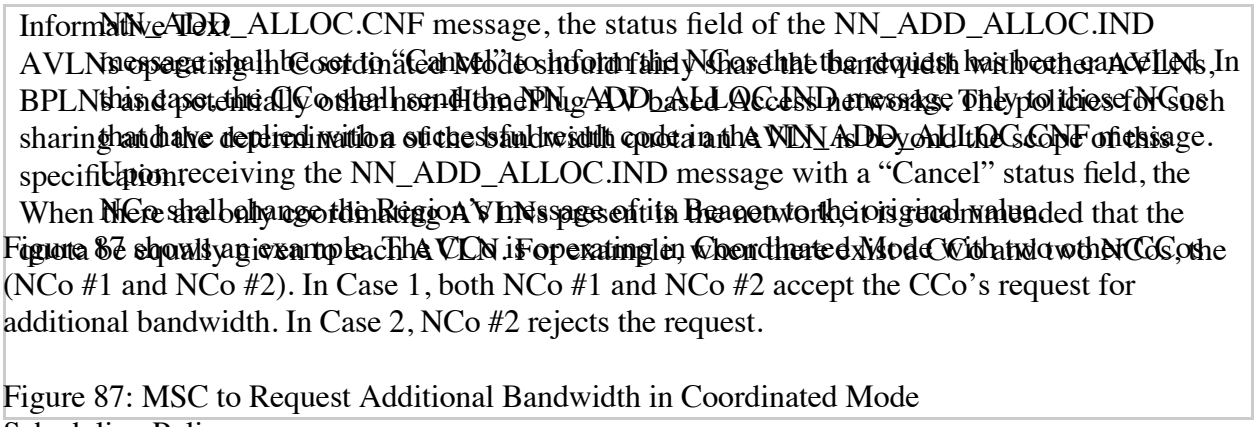

Figure 87 shows an example. The AVLN is operating in Coordinated Mode CCo with two other NCos (NCo #1 and NCo #2). In Case 1, both NCo #1 and NCo #2 accept the CCo's request for additional bandwidth. In Case 2, NCo #2 rejects the request.

Figure 87: MSC to Request Additional Bandwidth in Coordinated Mode

Scheduling Policy

AVLNs operating in Coordinated Mode use NN_ADD_ALLOC.REQ messages to request Bandwidth from Coordinating AVLNs in the INL. The following rules should be used for sharing the bandwidth between Coordinating AVLNs:

- The scheduling policy is on first-come, first-served basis when Shared CSMA Region is available. Thus, an AVLN (CCo) may obtain any amount of bandwidth from the Shared CSMA Region as far as the duration of MinCSMARegion is not violated.
- When a CCo requires more bandwidth for a new Connection or to support an existing Connection, then:
- If sufficient bandwidth is available in Shared CSMA Region (subjected to the MinCSMARegion restriction), the CCo can send NN_ADD_ALLOC.REQ asking for time allocation within the Shared CSMA Regions of the Neighbor CCos.
- If insufficient bandwidth is available in Shared CSMA Region, bandwidth occupancy of the AVLN is compared with the bandwidth quota.
- The CCo should not send NN_ADD_ALLOC.REQ to neighboring CCos if its AVLN is occupying more bandwidth than its bandwidth quota.
- If the CCo is not currently using its bandwidth quota, it can send NN_ADD_ALLOC.REQ asking for time allocation within the Reserved Regions of the Neighbor CCos.
- When a NN_ADD_ALLOC.REQ is received by a CCo that is currently using more than its share of the bandwidth quota, it should reconfigure and/or terminate existing Connection(s) to accommodate the request.
- AVLNs operating in Coordinated Mode should reserve only the minimum duration of time required to support the on-going Connections.

Informative Text

AVLNs operating in Coordinated Mode should fairly share the bandwidth with other AVLNs, BPLNs and potentially other non-HomePlug AV based Access networks. The policies for such sharing and the determination of the bandwidth quota an AVLN is beyond the scope of this specification.

When there are only coordinating AVLNs present in the network, it is recommended that the quota be equally given to each AVLN. For example, when there exist a CCo and two NCos, the quota is 33% of the maximum duration of Reserved Region (i.e., Beacon Period minus the duration of Beacon Region and MinCSMARegion). Note that unfair allocation of the quota may cause one or more AVLNs to stop coordinating with the other AVLNs in the group. This would result in interference between AVLNs, degrading performance for all the AVLNs.

Procedure to Release Bandwidth

Figure 88 shows the procedure for releasing a Reserved Region or a portion of it. The CCo that is releasing a reserved time interval shall send the NN_REL_ALLOC.REQ message to each NCo in its INL. The message specifies the time interval that is being released by the CCo. Each NCo shall reply with a NN_REL_ALLOC.CNF message.

Figure 88: MSC to Release a Reserved Time Interval in Coordinated Mode

Procedure to Shut Down an AVLN

Figure 89 shows the procedure for shutting down an AVLN. The CCo that is shutting down its AVLN shall send the NN_REL_NET.IND message to each NCo in its INL. The message specifies the Beacon Slot being used and the locations of the Reserved Regions that have been reserved by the CCo.

In addition, if the last Beacon Slot in the Beacon Region has been unoccupied for a period longer than IDLE_BEACON_SLOT_TIMEOUT, a CCo may request to reduce the number of Beacon Slots by using the process described in Section 8.3.5.2.

When an AVLN operating in Coordinated or Uncoordinated Mode shuts down, it shall use AC Line Sync Countdown BENTRY with the Reason Code = 0b00 (AVLN Shut Down or leaving Group) to indicate the number of Beacon Periods in which it is going to stop transmitting the Beacons (refer to Table 4-95 in Section 4.4.3.15.4.11). This information provided by the departing AVLN will enable other Coordinating CCos that are tracking the AC Line cycle to recover appropriately (refer to Section 8.3.9).

Figure 89: MSC to Shut Down an AVLN in Coordinated Mode

AC Line Cycle Synchronization in Coordinated Mode

In a group of Coordinating AVLNs, the CCo in the smallest occupied Beacon Slot number shall track the AC Line Cycle and should provide all four of the Beacon Transmit Offset values (BTO[0] through BTO[3]) to other coordinating CCos. This CCo shall also set the AC Line Cycle Synchronization Status (ACLSS) field to the Beacon Slot number it is currently occupying in the Central Beacon to indicate that it is tracking the AC line cycle. All other CCos in the group shall track a CCo that is reliably detected. The CCo that is tracked should have a smaller Beacon Slot

number.
To ensure that the Group of AVLN's operations does not get disrupted when a Coordinating CCo shuts down, the departing CCo shall use the AC Line Sync Countdown BENTRY to indicate the Beacon Period in which it will stop transmitting the Beacon. CCo's tracking the AC line cycle information provided by the departing CCo shall either choose a different CCo to track (if one or more is detected) or start tracking the AC Line cycle.
If a new AVLN joining a Group of Coordinating CCos determines that a Beacon Slot number smaller than the Beacon Slot of the CCo that is currently tracking the AC line cycle is not used, it may request that Beacon Slot only if the Beacon from the CCo that is currently tracking the AC line cycle is reliably detected. In such cases, when the new AVLN becomes part of the group and starts transmitting the Beacons, it shall initially track the AC line cycle information provided by the CCo transmitting Beacon in a larger Beacon Slot number and is currently tracking the AC line cycle. Once a CCo that is tracking the AC line cycle determines the presence of Beacon in a smaller Beacon Slot number, it shall handover AC line cycle synchronization by using the AC Line Sync Countdown BENTRY.
If a CCo in a Group determines that a Beacon Slot number smaller than the current Beacon Slot of the CCo is not used, it may use the Beacon Relocation BENTRY with Relocation Type set to SlotID to move to the smaller Beacon Slot number. A CCo in a Group may also use the Beacon Relocation BENTRY with Relocation Type set to SlotID to move to a different available Beacon Slot number as may be necessary to assure reliable Beacon reception for its AVLN.
Passive Coordination in CSMA-Only Mode
Level-0 and Level-1 CCos do not support TDMA in the presence of neighbor networks. Level-2 CCos support Coordinated mode, which enables neighboring Level-2 CCos to support TDMA. To further enhance the ability of Level-2 CCos in supporting TDMA in the presence of Level-0 and Level-1 CCos in CSMA-Only mode, a mandatory Passive Coordination procedure is defined for Level-0 and Level-1 CCos operating in CSMA-Only mode.
When a Level-1 or Level-0 CCo reliably detects Central or Proxy Beacons from one or more Level-2 CCos operating in Coordinated mode, it shall track the Beacon Period Start Time of one and only one such Level-2 CCo. Further, it shall process the Regions BENTRY of the Level-2 AVLN it is tracking and provide a Local Regions Schedule with CSMA Region during the interval where the neighboring AVLN has a CSMA Region and Stayout Region in the remainder of the Beacon Period. All STAs in the CSMA-Only mode AVLN shall refrain from transmitting (using Persistent and Non-Persistent Schedule BENTRIES) during the Stayout Region. This procedure is referred to as Passive Coordination.
When a Level-2 CCo operating in Coordinated mode detects Central Beacons from one or more Level-0 or Level-1 CCos, it should provide a larger minimum CSMA Region during the Beacon Period to share the medium fairly with Level-0/Level-1 AVLNs. The duration of the minimum CSMA Region shall be based on the sharing policy, which is defined in reference [21].
Transitions between Different Neighbor Network Operating Modes
The following sections describe the conditions that cause AVLNs to transition between various neighbor network modes. An AVLN detects the presence or absence of Neighbor Networks by means of the Discovery Process as described in Section 7.6.

Transitions between different Neighbor Network operation modes also depends on the network policy in the presence of the following types of neighboring networks:

- HomePlug 1.1-based networks,
- HomePlug 1.0.1-based Access network,
- HomePlug 1.0.1-based Access network with VoIP Provisioned, and
- HomePlug AV-based Access networks.

Policy-based transitions under such conditions are defined in reference [20].

Network Mode of a Newly Established AVLN

A new CCo may always establish an AVLN in CSMA-Only mode irrespective of the presence of any neighboring networks. This option simplifies the power-on procedure.

Optionally, a new CCo may use the knowledge of the detected neighboring networks to determine the Network Mode in which the AVLN needs to be established. If this option is used, the CCo can immediately transition from CSMA-Only mode before transmitting any Beacons, based on the transitions described in Section 8.5.2.

CSMA-Only Mode Transitions

Transitions from CSMA-Only mode are as follows:

CSMA-Only mode to Uncoordinated mode transitions

A Level-1 or Level-2 AVLN operating in CSMA-Only mode shall transition to Uncoordinated mode if it cannot detect any neighboring HomePlug AV in-home.

CSMA-Only mode to Coordinated mode transitions

A Level-2 AVLN operating in CSMA-Only mode shall transition to Coordinated mode if it can successfully coordinate with neighboring Level-2 or higher AVLNs.

A Level-2 AVLN operating in CSMA-Only mode shall transition to Coordinated mode if only neighbor networks in CSMA-Only mode are detected.

Uncoordinated Mode Transitions

Transitions from Uncoordinated mode are as follows:

Uncoordinated mode to Coordinated mode transition

A Level-2 AVLN operating in Uncoordinated mode shall transition to Coordinated mode if it detects Beacons from neighboring Level-0 or Level-1 AVLN.

A Level-2 AVLN operating in Uncoordinated mode shall transition to Coordinated mode if it can successfully coordinate with neighboring Level-2 AVLN(s).

Uncoordinated mode to CSMA-Only mode transition

A Level-1 AVLN operating in Uncoordinated mode shall transition to CSMA-Only mode if it detects any HomePlug AV in-home network.

A Level-2 AVLN operating in Uncoordinated mode shall transition to CSMA-Only mode if it cannot successfully coordinate with neighboring Level-2 AVLN(s).

Coordinated Mode Transitions

Transitions from Coordinated mode are as follows,

Coordinated mode to Uncoordinated mode transition

If all the networks in the Level-2 CCo's INL have shut down through the procedure described in Section 8.3.9 and no neighboring Level-0 or Level-1 AVLNs are detected, the CCo shall transition to Uncoordinated Mode.

If the Level-2 CCo can no longer decode any other Beacons from Coordinating Level-2 AVLNs for several Beacon Periods in a row, denoted by the parameter MaxNoBeacon, the CCo shall assume that all Coordinating Level-2 AVLNs have been powered off. In this case, the CCo shall transition to Uncoordinated Mode if no neighboring Level-0 or Level-1 AVLNs are detected.
If there are no Level-2 AVLNs present, and if Beacons from neighboring Level-0/Level-1 neighboring AVLNs cannot be detected for at least MaxDiscoverPeriod, the CCo shall assume that all neighboring Level-0/Level-1 AVLNs have been powered off and shall transition to Uncoordinated mode.

Coordinated mode to CSMA-Only mode transition

If a Level-2 CCo cannot successfully coordinate with neighboring Level-2 AVLNs, it shall transition to CSMA-Only mode.
Figure 810 shows the Neighbor Network mode transitions based on the rules described in Section 8.5.1 through Section 8.5.4. Several concise representations were used in this figure to simplify the conditions for various transitions. The interpretation of these is as follows:
HPAV_InHomeNNW = HomePlug AV in-home Neighbor Network
HPAV_InHomeNNW_L0 = Level-0 HomePlug AV in-home Neighbor Network
HPAV_InHomeNNW_L1 = Level-1 HomePlug AV in-home Neighbor Network
HPAV_InHomeNNW_L2 = Level-2 HomePlug AV in-home Neighbor Network
L1 = Level-1 CCo
L2 = Level-2 CCo
CoordSuc = Coordination with Neighboring Level-2 AVLN is successful

Figure 810. Neighbor Network Mode Transitions

Neighboring Networks with Matching NIDs

If a CCo identifies a neighboring CCo (NCo) where the NID is the identical to its own NID, it shall send a NN_INL.REQ message to the NCo with the identical NID.
A CCo that receives a NN_INL.REQ or NN_INL.CNF message from a NCo with an NID identical to its own shall compare the MyNumAuthSTAs field of that message with the total number of authenticated STAs in its AVLN including the CCo. If MyNumAuthSTAs in the received message is greater, or if it is the same but the MAC address of the NCo is greater than its own MAC address, it shall first send a CC_LEAVE.IND message with Reason field set to 0x02 (CCo shutting down due to a neighboring network with the same NID) to each STA in its AVLN, followed by performing the procedure to shut down an AVLN described in Section 8.3.9. After completing the shut down procedure, it shall begin the power-on network discovery procedure described in Section 7.1.
STAs receiving a CC_LEAVE.IND message with the Reason field set to 0x02 shall begin the power-on network discovery procedure described in Section 7.1.

Note: There is a very remote possibility (2^{-52}) that a neighboring network has the same NID, but different NMKs. Addressing this condition is outside the scope of this specification.

HomePlug 1.0.1 Coexistence

Overview

HomePlug AV STAs are likely to operate in environments containing legacy HomePlug 1.0.1

STAs. HomePlug 1.0.1 STAs transmit in the same frequency band as HomePlug AV STAs, resulting in interference. Hence, while true interoperability is not required, a means for coexistence is essential for both HomePlug AV and HomePlug 1.0.1 STAs to properly operate under such heterogeneous network conditions. HomePlug 1.0.1 STAs do not understand Beacon-based medium access and the interpretation of contention-free and CSMA Regions. To prevent HomePlug 1.0.1 stations from interfering with HomePlug AV transmissions, and to provide predictable behavior for HomePlug AV in the presence of HomePlug 1.0.1 STAs, all HomePlug AV stations shall implement the HomePlug AV Hybrid mode, as defined in Sections 9.3 through 9.7.

HomePlug AV Hybrid Mode not only defers HomePlug 1.0.1 stations from accessing the medium during the periodic contention-free intervals, it also enables fair sharing of the medium between HomePlug AV and HomePlug 1.0.1 CSMA/CA traffic. This section provides details on the HomePlug AV and HomePlug 1.0.1 coexistence. Section 9.2 provides a brief description of HomePlug 1.0.1 behavior relevant to HomePlug AV coexistence.

HomePlug 1.0.1 Behavior

This section describes HomePlug 1.0.1 behavior relevant to HomePlug AV and HomePlug 1.0.1 coexistence.

Note: This section is for informative purpose only and the reader should refer to the HomePlug 1.0.1 specification for detailed information.

HomePlug 1.0.1-Prioritized CSMA/CA

HomePlug 1.0.1 uses CSMA/CA access along with priorities. When the medium is perceived to be idle, a station may transmit an MPDU immediately. If the medium is not idle, a station must wait for the current transmission to end, then assert its priority in the Priority Resolution Period (PRP) that follows the transmission.

The PRP consists of two PRSs. Stations normally compete for access to the medium first by asserting their Channel Access Priority (CAP) in the PRP. CA3 is the highest priority and CA0 is the lowest. Each station with CA3 or CA2 traffic asserts a priority signal in the first PRS (PRS0), causing stations with CA1 or CA0 traffic to defer. Stations with CA3 traffic, and those with CA1 traffic that have not deferred, assert a priority signal in the second PRS (PRS1). This signal causes stations with CA2 and CA0 traffic to defer. A station that hears a higher CAP during the PRP ceases transmission and listens to the medium to receive delimiters that will inform it when the next PRP should occur.

A station that does not detect any stations with higher priority traffic in the PRP can contend for the medium in the contention period that starts immediately following the PRP. In this case, it randomly selects a number of contention slots to wait before transmitting. If it detects another transmission before its turn to transmit, it defers. This is inherently a randomized access to the medium, with no guarantee of success.

HomePlug 1.0.1 Carrier-Sensing Mechanisms

HomePlug 1.0.1 uses two carrier-sensing mechanisms to determine activity on the medium:

PCS

VCS

The PCS in HomePlug 1.0.1 is limited to Preamble-sequence detection and provided by the PHY.

Due to attenuation and noise, PCS based on received signal strength is unreliable. PCS is used in HomePlug 1.0.1 for early detection of the start of a delimiter, so that stations will attempt to receive the delimiter instead of transmitting. Determination of the medium status during the PHY Body of an MPDU is beyond the capability of PCS, and must be performed logically in the MAC using VCS.

VCS uses the information available in the Frame Control fields of the delimiters to predict future states of the medium. The Frame Length field of the SOF delimiter is used to predict when the corresponding End-of-Frame (EOF) delimiter is expected. If the SOF indicates that a response is expected, Frame Length also yields the time when the response delimiter (ACK, NAK, or FAIL) should occur, as this is a fixed time after the EOF. From the SOF until the EOF is expected, the STA attempts to receive a frame from the medium and does not search for another delimiter. When an EOF or a response delimiter is expected, the STA searches for the appropriate delimiter.

Table 91: Receiver Actions on Receipt of HomePlug 1.0.1 Delimiters

Delimiter Type Received	Actions at Receiver*
SOF without Response Expected	Attempt to receive PHY body for time given by frame length Attempt to receive EOF at time computed from frame length If EOF received, extract CAP Else ignore Start PRP at time computed from frame length
SOF with Response Expected	Attempt to receive PHY body for time given by frame length Attempt to receive EOF at time computed from frame length If EOF received, extract CAP Else ignore Attempt to receive response at time computed from frame length If response received, extract CAP Else ignore Start PRP at time computed from frame length
EOF without Response Expected	Start PRP after CIFS
EOF with Response Expected	Attempt to receive response after RIFS If response received, extract CAP Else ignore Start PRP at CIFS after response should have appeared
Response (ACK/NAK/FAIL)	Start PRP after CIFS

* The transmitter behaves differently; if an expected response is not received, it enters EIFS.

After a transmission (the end of the EOF if no response is expected, or the end of the response if one is expected), there is a delay of CIFS. Following the CIFS is the PRP as mentioned above,

which is followed by the Contention Window (CW). The CW consists of a sequence of Contention Slots (CSs), in which a station that won the PRP can start transmission. The CW extends for the maximum MPDU transmission time or until the first transmission starts, whichever comes first.
If a station becomes confused about the state of the medium (e.g., after a collision or when it receives an errorful SOF), it enters Extended Interframe Space (EIFS). EIFS is a waiting period equivalent to the maximum MPDU duration to allow a station to resynchronize with other stations on the medium. During EIFS, the station searches for a delimiter that will allow it to reestablish VCS and to begin to participate again.

HomePlug 1.0.1 Segment Bursting

The HomePlug 1.0.1 station that has broken a longer transmission into multiple MPDUs may employ segment bursting using the CC mechanism. Here, the transmitting station sets the CC bit in the SOF and the EOF, and the responding station sets it in the response delimiter. Stations with traffic at the same or a lower priority level are not allowed to assert priority in the PRP or to transmit on the medium until CC is reset. Segment bursting allows efficient delivery of long transmissions by eliminating waiting time and collisions.

Contention-Free Transmissions

Stations with higher priority traffic may interrupt a burst transmission by asserting their priority in the PRP. A station can only do this if it knows the CAP of the transmission, which is available in the EOF and in the response, but not in the SOF. Consequently, stations must assume that the CAP is CA3 (highest priority) until they learn otherwise from an EOF or a response. If a station does not hear either the EOF or a response, it enters EIFS at the time the next contention period should have begun. Since CAP is only known from the EOF or response, the HomePlug 1.0.1 node will assume that CAP is CA3 and will not assert priority in the PRP. This allows the PRP to be used by HomePlug AV transmissions during contention-free access.

Link Status

HomePlug 1.0.1 STAs are required to monitor the medium to ascertain whether they are still connected to the network. If the HomePlug 1.0.1 STA does not receive a valid delimiter for five seconds, it starts a polling process, transmitting Channel Estimation Requests until it either obtains a response or gives up. If it decides that it has been disconnected, it may continue to poll the medium to test for reconnection. To keep inactive HomePlug 1.0.1 STAs quiet, valid HomePlug 1.0.1 delimiters must be sent frequently enough to satisfy the link-status function.

HomePlug AV Coexistence Modes

HomePlug 1.0.1 coexistence is an operating mode for HomePlug AV STAs. The CCo of each AVLN determines the mode of operation of STAs associated with it. There are three modes in which an AVLN can operate:

- Fully Hybrid Mode: The AVLN operates in Fully Hybrid Mode if interfering HomePlug 1.0.1 stations are detected. In this mode, all CP and CFP transmissions use Hybrid Mode delimiters (refer to Section 3.2.1.1) to coordinate medium access with HomePlug 1.0.1 stations. In a Fully Hybrid mode AVLN that is operating in Uncoordinated mode, the CCo shall also specify Contention Free Period Initiation (CFPI) allocation(s) to defer HomePlug 1.0.1 stations from accessing the medium during Beacon Region and CFP allocations (refer to Section 9.6.1). In a Fully Hybrid mode AVLN that is operating in Coordinated mode,

the CCo should also specify Contention Free Period Initiation (CFPI) allocation(s) to defer HomePlug 1.0.1 stations from accessing the medium during Beacon Region and CFP allocations.

Note: A CCo in Coordinated mode might not be able to provide CFPI allocation before the Beacon Region if it is Reserved by its neighboring CCo (refer to Section 9.10).

- Shared CSMA Hybrid Mode: The AVLN operates in Shared CSMA Hybrid Mode if interfering HomePlug 1.1 stations are detected, and no interfering HomePlug 1.0.1 stations are detected. In Coordinated Mode, the CCo may also specify a Shared CSMA Hybrid Mode if a Coordinating CCo in the INL specified a Shared CSMA or Fully Hybrid Mode (refer to Section 9.10). In this mode, only the Shared CSMA allocations use hybrid delimiters to coordinate medium sharing.
- AV-Only Mode: The AVLN operates in AV-Only Mode if no interfering HomePlug 1.0.1 and HomePlug 1.1 stations are detected. In Coordinated Mode, this further requires that none of the Coordinating CCos detects HomePlug 1.0.1 or HomePlug 1.1 stations. In this mode, all CP and CFP transmissions use AV-Only delimiters.

Regardless of the AVLN's operating mode, all Beacon MPDUs always use a Hybrid delimiter structure. This choice simplifies the Neighbor Network operations in Coordinated Mode and also enables coexistence with HomePlug 1.1 and Non-HomePlug-based Access Networks (refer to Chapter 10).

In Hybrid Mode, HomePlug AV stations manipulate the fields of HomePlug 1.0.1 Frame Control to keep them synchronized and to control their access to the medium. Since HomePlug 1.0.1 stations use only eight different frame lengths, HomePlug AV MPDU transmissions must be modified to match these lengths. Apart from these, special mechanisms must be used to defer HomePlug 1.0.1 stations from accessing the medium during the Beacon Region and during the CFP allocations.

Coexistence requires HomePlug AV STAs to detect active HomePlug 1.0.1 STAs on the medium, and to change the coexistence modes in response to their presence or absence. HomePlug AV STAs use the presence of delimiters that are only used by HomePlug 1.0.1/1.1 STAs (and never used by HomePlug AV stations in Hybrid Mode) to determine the presence of HomePlug 1.0.1/1.1 STAs. All HomePlug AV STAs shall be capable of detecting HomePlug 1.0.1/1.1 STAs based on HomePlug 1.0.1 delimiters. HomePlug AV STAs that can interoperate with HomePlug 1.0.1/1.1 STAs may also use explicit message exchange to determine the presence of HomePlug 1.0.1/1.1 STAs. All HomePlug AV stations shall be capable of changing their operating mode dynamically based on information provided by the CCo in the Beacon.

Detection and Reporting of Active HomePlug 1.0.1 and HomePlug 1.1 STAs

AV STAs shall continuously monitor the medium during the AVLN's CSMA allocations as well as during their CFP allocations (i.e., CFP allocations for which the STA is either the source or destination of the Global Link) for HomePlug 1.0.1 and HomePlug 1.1 transmissions. The reception of an End of Frame (EOF) delimiter with the 10-bit Reserved Field set to 0x000 shall be considered a valid HomePlug 1.0.1 transmission. HomePlug 1.1 transmissions are identified as described in Section 9.8.2.

In HomePlug 1.0.1, the EOF delimiter is transmitted at the end of a HomePlug 1.0.1 Long MPDU.

Therefore, when a valid HomePlug 1.0.1 SOF Frame Control is detected along with an invalid AV Frame Control, AV stations shall try to search for an EOF delimiter based on the HomePlug 1.0.1 Frame Length (FL). It is also possible for the EOF delimiter to be detected without a corresponding HomePlug 1.0.1 SOF. Regardless of whether EOF delimiter is detected following a HomePlug 1.0.1 SOF delimiter, it confirms the presence of HomePlug 1.0.1/1.1 station(s).

Note: The Frame Length (FL) field in HomePlug 1.0.1 indicates the duration of the HomePlug 1.0.1 payload. This field is used by AV stations to determine the expected location of the EOF delimiter.

Figure 91 and Figure 92 show the processing for detecting HomePlug 1.0.1/1.1 transmission in AV Only Mode and Hybrid Mode, respectively. For AV Only Mode, Figure 91 assumes that the STA can simultaneously process the received signal for HomePlug 1.0.1 and HomePlug AV Frame Control. Implementations may also use preamble processing to determine whether the preamble is a HomePlug 1.0.1 or an AV preamble and use that information to decide whether a HomePlug 1.0.1 or a HomePlug AV Frame Control needs to be decoded subsequent to the preamble detection.

All AV stations that detected a HomePlug 1.0.1 or HomePlug 1.1 transmission shall report it to the CCo by setting the HomePlug 1.0.1 Detect Flag (HPI0DF) or HomePlug 1.1 Detect Flag (HP11DF), respectively, in the SOF and/or RTS delimiter of all subsequent transmissions they make for a duration of HP1D_ReportDuration. If there are no pending Segments to deliver, the Station may send a stand-alone RTS/CTS delimiter (i.e., RTS/CTS without a Long MPDU to follow).

AV stations shall also maintain statistics on the number of HomePlug 1.0.1/1.1 transmissions that were detected and report them to the CCo using the CC_HP1_DET.CNF message when explicitly requested by the CCo (using CC_HP1_DET.REQ). Stations may also send an unsolicited CC_HP1_DET.CNF message if they detect several HomePlug 1.0.1 transmissions and the network mode is either not changed to Fully Hybrid Mode or if none of the ongoing transmissions reports the detection of HomePlug 1.0.1 stations by setting the HP10DF. Similarly, Stations may send an unsolicited CC_HP1_DET.CNF message if they detect several HomePlug 1.1 transmissions and the network mode is in AV-Only Mode or if none of the ongoing transmissions reports the detection of HomePlug 1.1 stations by setting the HP11DF. HomePlug 1.0.1/1.1 detection statistics shall be reset when CC_HP1_DET.CNF is transmitted in response to a CC_HP1_DET.REQ.

Figure 91: AV Only Mode Processing for Detecting HomePlug 1.0.1 Transmission

Figure 92: Hybrid Mode Processing for Detecting HomePlug 1.0.1 Transmission

HomePlug 1.0.1/1.1 Coexistence Mode Changes

The CCo of each AVLN determines the HomePlug 1.0.1 coexistence mode of the AVLN. The Hybrid Mode (HM) Field in the Beacon is used by the CCo to indicate the operation mode of the AVLN.

On start-up, HomePlug AV STAs shall enter Fully Hybrid Mode and listen to the medium for

existing activity (in particular, they shall seek the CCo if one is present). If a Beacon from an existing AVLN is detected and the station intends to become part of that AVLN, it shall change its coexistence mode to that of the AVLN. If the STA successfully becomes part of that AVLN, its HomePlug 1.0.1 coexistence operating mode will depend on that AVLN's operating mode. The STA continues to report HomePlug 1.0.1 and HomePlug 1.1 detection status as described in Section 9.3.1.

If the HomePlug AV station starts a new AVLN in Un-Coordinated Mode, its operating mode shall be based on whether it detected HomePlug 1.0.1 and/or HomePlug 1.1 activity during the startup.

If HomePlug 1.0.1 activity is detected, the AVLN shall start operating in Fully Hybrid Mode.

If HomePlug 1.1 activity is detected and no HomePlug 1.0.1 activity is detected, the AVLN shall start operating in Shared CSMA Hybrid Mode.

If neither HomePlug 1.0.1 activity nor HomePlug 1.1 activity is detected, the AVLN shall start operating in AV-Only Mode.

If the HomePlug AV station intends to start a new AVLN in Coordinated Mode, it initially operates in the same operating mode as that of the coordinating AVLNs. If the AVLN becomes part of the group of Coordinating AVLN, its operating mode is determined by the operating mode of the Coordinating AVLNs, as well as the detection of HomePlug 1.0.1 and/or HomePlug 1.1 activity during startup.

If HomePlug 1.0.1 activity is detected, the AVLN shall start operating in Fully Hybrid Mode.

If HomePlug 1.1 activity is detected and no HomePlug 1.0.1 activity is detected, the AVLN shall start operating in Shared CSMA Hybrid Mode.

If neither HomePlug 1.0.1 nor HomePlug 1.1 activity is detected, and if the Coordinating AVLNs are operating in either Fully Hybrid Mode or Shared CSMA Mode, the AVLN shall start operating in Shared CSMA Hybrid Mode.

If neither HomePlug 1.0.1 activity nor HomePlug 1.1 activity is detected, and Coordinating AVLNs are operating in AV-Only Mode, the new AVLN shall start operating in AV-Only Mode.

The CCo and other stations in the AVLN exchange information to determine the operating mode of the AVLN. When a CCo in AV-Only Mode determines the presence of HomePlug 1.0.1 activity, it shall change the network mode to Fully Hybrid Mode. To allow the AVLN to revert to AV-Only Mode when all HomePlug 1.0.1 nodes become inactive, the CCo maintains a Fully Hybrid Mode Timer that shall be set to FHM_Timeout when it changes to Fully Hybrid Mode. This timer will be continuously reset when new HomePlug 1.0.1 activity is detected/reported while in Fully Hybrid Mode. If the Fully Hybrid Mode Timer expires and no HomePlug 1.1 activity is detected/reported, the CCo shall change to AV-Only Mode.

Similarly, when a CCo in AV-Only mode determines the presence of HomePlug 1.1 activity, it shall change to Shared CSMA Hybrid Mode. To allow the AVLN to revert to AV-Only Mode when all HomePlug 1.1 nodes become inactive, the CCo maintains a Shared CSMA Hybrid Mode Timer that shall be set to SHM_Timeout when it changes to Shared CSMA Hybrid Mode. This timer will be continuously reset when new HomePlug 1.1 activity is detected/reported while in Shared CSMA Hybrid Mode. If the Shared CSMA Hybrid Mode Timer expires and no HomePlug 1.1 activity is detected/reported, the CCo shall change to AV-Only Mode.

If the CCo in Shared CSMA Mode determines the presence of HomePlug 1.0.1 activity, it shall change the operating mode to Fully Hybrid and set the Fully Hybrid Mode timer to FHM_Timeout.
To ensure that no HomePlug 1.0.1 or HomePlug 1.1 activity is detected, the CCo may request stations to provide HomePlug 1.0.1 and HomePlug 1.1 detection status before changing from Fully Hybrid Mode or Shared CSMA Hybrid Mode to AV Only Mode. This procedure may also be used while transitioning from Fully Hybrid to Shared CSMA Hybrid Mode.
Figure 93 shows the CCo Coexistence Mode changes.
When operating in Coordinated Mode, HomePlug 1.0.1 and HomePlug 1.1 Coexistence Mode changes shall be made with the other AVLNs in the same group of Coordinating AVLNs. Refer to Section 9.10 for details.

Figure 93: Central Coordinator HomePlug 1.0.1 Coexistence Mode Changes

HomePlug 1.0.1-Compatible Frame Lengths

HomePlug AV stations use hybrid MPDUs when coexisting with HomePlug 1.0.1 and HomePlug 1.1 stations during the Fully Hybrid and Shared CSMA Hybrid operating modes. Hybrid MPDUs use hybrid delimiters consisting of a Hybrid Preamble, the HomePlug 1.0.1 Frame Control, and HomePlug AV Frame Control(s). This section describes how the HomePlug AV stations should manipulate the HomePlug 1.0.1 Frame Control fields and their Long MPDU lengths to keep HomePlug 1.0.1 stations synchronized properly.
Manipulation of HomePlug 1.0.1 Frame Controls in Long SOF MPDUs depends on,
Whether the transmission is made in a Shared CSMA allocation or a CFP Allocation, and
Whether the SOF Long MPDU is a Regular MPDU or a Burst MPDU.
Regular Long SOF MPDUs transmitted during Shared CSMA allocations shall ensure that the HomePlug AV and HomePlug 1.0.1/1.1 stations are synchronized with respect to the Priority Resolution Period. This shall be achieved by choosing FL_AV to be the largest multiple of 1.28 µsec that is smaller than the duration from the last non-zero sample of the SOF delimiter to the first non-zero sample at the start of the SACK preamble, so the start of the PRP can be indicated to HomePlug 1.0.1/1.1 stations using a compatible HomePlug 1.0.1 SOF FC in the hybrid delimiter.
HomePlug 1.0.1 SOF Frame Control allows for 16 compatible lengths:
Eight lengths use “SOF with response expected.”
The other eight lengths use “SOF with no response expected.”
Figure 94 and Figure 95 show the choice of compatible Regular Shared CSMA MPDUs with “SOF with response expected” and “SOF with no response expected,” respectively. The top half of each figure shows the HomePlug AV transmission, while the bottom half shows how HomePlug 1.0.1/1.1 stations interpret the activity on the medium.

Figure 94: Compatible Regular MPDU during Shared CSMA Using HomePlug 1.0.1 SOF with Response Expected

Figure 95: Compatible Regular MPDU during Shared CSMA Allocation Using HomePlug 1.0.1

SOF with no Response Expected

Regular Long SOF MPDUs and Long RSOF MPDUs that are transmitted during CFP allocations shall ensure that the HomePlug 1.0.1/1.1 stations start searching for delimiters at the next transmission opportunity. This shall be achieved by choosing FL_AV to be the largest multiple of 1.28 μsec that is smaller than the duration from the last non-zero sample of the SOF delimiter to th first non-zero sample at the start of the SACK preamble, so that the end of the PRP can be indicated to HomePlug 1.0.1/1.1 stations using a compatible HomePlug 1.0.1 SOF FC in the hybrid delimiter that is the same as the earliest time the next HomePlug AV transmission can begin.

Figure 96 shows the choice of compatible Regular CFP MPDUs with "SOF with no response expected." Furthermore, HomePlug 1.0.1 SOF Frame Control with Response Expected and Frame Length indicating 160 Symbols (i.e., the maximum allowed FL value) shall not be used during CFP allocations. This restriction provides two synchronization opportunities within EIFS duration of time (i.e., the time for which a HomePlug 1.0.1 searches for delimiter before accessing the medium). As a result, this restriction enhances the reliability with which the HomePlug 1.0.1 stations can be prevented from accessing the medium during CFP allocations.

HomePlug AV stations use a Short SOF delimiter for mechanisms such as Request SACK retransmissions. The rules for choosing HomePlug 1.0.1-compatible FL_AV are same as that of the corresponding Long SOF delimiters (described above).

Figure 96: Compatible Regular MPDU during CFP Allocation Using HomePlug 1.0.1 SOF with No Response Expected

Burst Long SOF MPDUs and Long RSOF MPDUs transmitted during Shared CSMA as well as CFP allocations shall ensure that HomePlug 1.0.1/1.1 stations start searching for delimiters when the next MPDU in the Burst is transmitted. This shall be achieved by choosing FL_AV to be the largest multiple of 1.28 μsec that is smaller than the duration from the last non-zero sample of the SOF delimiter to the first non-zero sample at the start of the preamble of the next MPDU in the Burst, such that the end of the PRP that can be indicated to HomePlug 1.0.1/1.1 stations using a compatible HomePlug 1.0.1 SOF FC in the hybrid delimiter is the same as the time at which the transmission of the next MPDU in the Burst begins.

Figure 97 shows the choice of compatible Burst MPDUs with "SOF with no response expected." During CFP allocations, the HomePlug 1.0.1 SOF Frame Control with Response Expected and Frame Length indicating 160 symbols (i.e., the maximum allowed FL value) shall not be used during CFP allocations.

Figure 97: Compatible Burst MPDU Using HomePlug 1.0.1 SOF with no Response Expected

HomePlug AV stations use Sound MPDUs for channel adaptation. Long Sound MPDUs shall follow the same rule as defined for Long SOF MPDUs for choosing HomePlug 1.0.1-compatible FL_AV.

HomePlug AV Hybrid SACK, CTS, and Short Sound delimiters shall have their HomePlug 1.0.1 Frame Control field set to indicate a Start of Frame with Response Expected with Tone Map Index (TMI) set to 0b00000 (i.e., ROBO Tone Map) and Frame Length set to 0x00 (i.e., 20 symbols). This combination of fields is treated as an invalid delimiter by HomePlug 1.0.1 station, thus

causing them to search for another delimiter for duration of EIFS.
The choice of HomePlug 1.0.1 Frame Control fields for a HomePlug AV Hybrid RTS delimiter depends on:
Whether RTS is transmitted during Shared CSMA or during CFP allocation, and
Whether RTS/CTS is followed by a corresponding SOF MPDU.
The Hybrid RTS delimiter during Shared CSMA when a PRP follows the corresponding CTS delimiter and Hybrid RTS delimiter that has a corresponding Hybrid SOF delimiter (i.e., RTS/CTS is followed by a Long SOF) shall have their HomePlug 1.0.1 Frame Control fields set to indicate a Start of Frame with Response Expected with a non-ROBO Tone Map Index (TMI) and Frame Length Set to 0x00 (i.e., 20 symbols).
Note: This choice causes HomePlug 1.0.1 stations to start searching for the delimiter after the following CTS delimiter. Figure 98 shows this choice of a compatible Hybrid RTS delimiter when PRP follows the CTS delimiter. Figure 99 shows the choice of a compatible Hybrid RTS delimiter when a corresponding SOF delimiter follows the CTS delimiter.
The Hybrid RTS delimiter transmitted during the CFP without a corresponding Hybrid SOF delimiter shall have its HomePlug 1.0.1 Frame Control fields set to indicate a Start of Frame with no Response Expected, with a non-ROBO Tone Map Index (TMI) and Frame Length Set to 0x00 (i.e., 20 symbols). Figure 910 shows the choice of a compatible Hybrid RTS delimiter during CFP allocation when there is no corresponding SOF delimiter.

Figure 98: Compatible Hybrid RTS Delimiter when PRP Follows the CTS Delimiter

Figure 99: Compatible Hybrid RTS Delimiter when the Corresponding SOF Follows the CTS Delimiter

Figure 910: Compatible Hybrid RTS Delimiter during CFP Allocation when There is No Corresponding SOF Delimiter
Beacon Delimiters are always transmitted in Hybrid Mode. HomePlug 1.0.1 Frame Control in the CCo Beacon is used to negotiate and allocate the medium with HomePlug 1.1 and Non-HomePlug-based stations (refer to Section 9.8 and Chapter 10). Since these use Reserved HomePlug 1.0.1 delimiter types, they cause HomePlug 1.0.1 stations to search for the duration of the EIFS.
When a CCo's Beacons do not carry negotiation and allocation delimiters, the setting of the HomePlug 1.0.1 Frame Control fields depends on whether the Beacon is the last Beacon in the Beacon Region.
If the Beacon is the last Beacon in the Beacon Region, the HomePlug 1.0.1 Frame Control fields shall be set to indicate a Start of Frame with no Response Expected, with a non-ROBO Tone Map Index (TMI), Frame Length Set to 0x01 (i.e., 40 symbols) and Contention Control bit set to 0b0.
If the Beacon is not the last Beacon in the Beacon Region, the HomePlug 1.0.1 Frame Control fields shall be set to indicate a Start of Frame with no Response Expected, with a non-ROBO Tone Map Index (TMI), Frame Length Set to 0x00 (i.e., 20 symbols) and Contention Control bit set to 0b1.

This will ensure that HomePlug 1.0.1 stations track each of the Beacons in the Beacon Region and start priority contention at the end of Beacon Region.
Proxy and discover Beacons shall have their HomePlug 1.0.1 Frame Control fields set to indicate a Start of Frame with no Response Expected, with a non-ROBO Tone Map Index (TMI) and Frame Length Set to 0x00 (i.e., 20 symbols).
When operating with a Tone Mask other than the one specified in Section 3.6.7, it might not be possible to provide a HomePlug 1.0.1-compatible MPDU length in the last Beacon with the current choice of B2BIFS. Under such conditions, a new B2BIFS that is larger than the currently specified B2BIFS will be used to ensure proper HomePlug 1.0.1 coexistence.
HomePlug 1.0.1 stations use the Contention Control (CC) bit to indicate that any station with a priority less than or equal to the priority of the current transmission shall not transmit. The HomePlug 1.0.1 SOF does not contain channel access priority information. Reception of a SOF delimiter with CC set to 0b1 causes HomePlug 1.0.1 stations to assume that the traffic has a priority of CAP3 (i.e., highest priority) until the corresponding EOF or Response is detected. Thus, a stand-alone HomePlug 1.0.1 SOF delimiter causes HomePlug 1.0.1 to defer for the duration of EIFS following the subsequent PRP. HomePlug AV stations can take advantage of this mechanism by setting the CC bit to 0b1 in valid HomePlug 1.0.1 delimiters, when HomePlug 1.0.1 transmissions needs to be deferred following the current transmission.
The following rules shall be used by HomePlug AV station for manipulating the CC bit in valid HomePlug 1.0.1 SOF FCs:
The CC bit shall be set to 0b1 in all CFP transmission, with the exception of last transmission in the CFP allocation when the CFP allocation is followed by a Shared CSMA allocation.
All Shared CSMA transmissions shall have the CC bit set to 0b0 with the following exceptions:
The Hybrid RTS delimiter shall always have the CC bit set to 0b1.
Burst MPDUs shall have always have the CC bit set to 0b1.
When a valid HomePlug 1.0.1 Frame Control is transmitted in a CCo Beacon, the CC bit shall be set to 0b1 in all Beacons, except the last Beacon in the Beacon region.
Medium Activity under Hybrid Mode
HomePlug AV uses repeating Beacon Periods to manage access to the medium. When there are active HomePlug 1.0.1 STAs, these are kept synchronized with the HomePlug AV nodes by transmitting HomePlug 1.0.1 delimiters. These are formed so that the VCS of HomePlug 1.0.1 nodes causes them to refrain from transmitting when the HomePlug AV STAs require predictable access to the medium, and fairly sharing the medium during CSMA/CA periods.
HomePlug AV Channel Access in Hybrid Mode
The channel access mechanism used by HomePlug AV stations in Fully Hybrid Mode is similar to the one used in AV-Only Mode, except for the following two differences:
All Shared CSMA allocations are shared in a fair manner with HomePlug 1.0.1 and/or HomePlug 1.1 stations.
The CCo may specify Contention Free Period Initiation (CFPI) allocations to defer HomePlug 1.0.1 stations from accessing the medium during CFP allocations and during the Beacon Region. CFPI allocations are only used when an AVLN operates in Fully Hybrid Mode (i.e., when interfering HomePlug 1.0.1 stations are present).

Figure 911 shows an example of medium allocation during Fully Hybrid Mode. There are five distinct allocation types:
Beacon Region
Shared CSMA allocation
CFPI allocation
Persistent Contention-Free Period (P-CFP)
Non-Persistent Contention-Free Period (N-CFP)

Figure 911: HomePlug AV Channel Access in Hybrid Mode

It is critical that the Beacon be issued precisely when it is expected. HomePlug AV stations require the Beacon to learn the allocations and other information needed to operate correctly. While the system has been designed to survive the loss of a Beacon from time to time, it cannot tolerate repeated Beacon loss. A station that does not receive the Beacon will not know what the non-persistent allocations are for that period, and hence cannot use any non-persistent allocation given to it in that Beacon Period. Therefore, it is critical to ensure that HomePlug 1.0.1 stations do not transmit during the Beacon Region. Similarly, to maintain guarantees on QoS, AV stations should be provided exclusive access during CFP Allocations. For this reason, the HomePlug 1.0.1 stations should also be deferred and excluded from medium access during P-CFP and N-CFP. During the Shared CSMA/CA portion of the Beacon Period, the HomePlug 1.0.1 stations compete for access to the medium along with the HomePlug AV stations, using priority-based CSMA/CA as in the HomePlug 1.0.1 specification. However, as the time for CFP allocations approaches, it is critical to secure the medium, so that the CFP allocations and Beacons can be issued precisely on time. For this reason, there is a period during which the HomePlug AV stations, and the CCo in particular, attempt to seize the medium from the HomePlug 1.0.1 stations. This is the CFPI period. If the medium is acquired early, the CCo can grant the remaining time in the CFPI allocation to specific station(s) by transmitting an RTS with Immediate Grant Flag (IGF) set (refer to Section 9.6.1.1).

Contention-Free Access Coexistence

To provide reliable contention-free access, all HomePlug 1.0.1 stations should be deferred from accessing the medium during the CFP. To provide fairness, all HomePlug 1.0.1 stations should be allowed access in Shared CP that starts soon after Beacon Region.

Contention-free coexistence is achieved in three stages:

- Initiate the CFP.
- Maintain the CFP.
- Terminate the CFP.

CFPI implies that the HomePlug 1.0.1 stations are brought into synchronization with the AV stations. CFPI starts before the start of CFP allocations and must end by the time CFP allocation starts. The HomePlug 1.0.1 stations are then deferred until the end of the CFP and during the subsequent Beacon Region. This is referred to as CFP maintenance. Initiation and maintenance require the CC bit to be set in the delimiters that are transmitted by the AV stations to cause the HomePlug 1.0.1 stations to defer. For the CSMA/CA access period to begin as soon as possible

after the Beacons, the last Beacon MPDU in the Beacon Region should have CC = 0b0 (when a valid HomePlug 1.0.1 Frame Control is used in the hybrid Beacon delimiter). This setting allows normal priority-based contention to resume and is referred to as CFP termination.
The Central Controller is responsible for CFPI. CFP maintenance is accomplished by the contention-free sessions to which the CCo has made allocations. CFP termination is performed by the last station transmitting in the CFP (when CFP is followed by Shared CSMA allocation) and/or the CCo.
Contention-Free Period Initiation
The CCo starts the CFPI process during the CFPI allocation. It is critical that CFPI allocation be long enough to defer HomePlug 1.0.1 stations reliably before issuing the Beacon. It is recommended that a 4 msec duration be allocated for CFPI. The CCo may specify multiple CFPI allocations during a single Beacon Period.
Table 92 shows the parameters used by the CFPI initiation procedure.

Table 92: Parameters for CFPI Procedure

Parameters	Interpretation
CFPIMode	When set to true, this indicates that the CCo is in CFP Initiation Mode
CFM	When set to true, indicates that the station has contention-free access to the medium
CFPIColCnt	Counter to track the number of collisions incurred while transmitting in Contention-Free Mode
MaxCFPICols	Maximum number of collisions that can be incurred by the CCo in CFP-Establishment Mode before losing contention-free access to the medium.
CFPI_EIFS	Modified EIFS duration used by CCo during CFPI.

The CFPI procedure used by the CCo is as follows:

- Set CFPI_Mode to true and reset CFPIColCnt to 0.
- If the medium state is {IDLE, IN_CW}, go to Step 5. Otherwise, go to Step 3.
- Wait for the next contention opportunity. If a Frame Control is detected during this time, go to Step 4. Otherwise, go to Step 5.
- If a Frame Control from the HomePlug 1.0.1 station is detected, go to Step 3.
- If there is sufficient time to transmit a test MPDU before that start of Beacon Period, transmit test MPDU with CC = 0b1 in the first contention slot and go to Step 6. Otherwise, the CFPI has failed and the CCo and other AV stations simply assert CA3 in any PRP encountered; go to Step 9.
- If the test MPDU is successfully delivered, the transmission is assumed successful and CFPI Mode ends; set CFPI_Mode to false, set CFM to true, and go to Step 8. Otherwise, go to Step 7.
- Increase CFMColCnt counter. If CFPI_Mode is true and CFMColCnt is less than

MaxCFPICols, wait for the start of next contention period and go to Step 5. Otherwise, perform all of the following,

Reset MaxCFPICols to 0.

Go to IN_EIFS State and set the waiting time to CFPI _EIFS.

Go to Step 3

- If the CFPI ends before the target start time of the Beacon Period, the CCo may issue an RTS with an immediate grant if time permits. The last allocation shall end such that the CFP allocations or the Beacon Region can start at the target start time. If there is not sufficient time to allocate access, the CCo shall transmit a hybrid SOF of a duration that ends as late before the target start as possible.
- If the CFPI failed, the CCo may issue a Beacon. The CCo may also change the duration of CFPI allocation used in the network.

The CCo uses the Test MPDU to reliably determine the acquisition of medium from HomePlug 1.0.1 stations. Test MPDU shall be the smallest possible Tone Map Modulated MPDU. Test MPDU is considered to be successfully delivered if its payload is successfully received by the destination.

Note: The test MPDU can carry segments from a MAC Frame Stream. The CCo can use the MPDU carrying invalid PHY Blocks if there are no segments available in the MAC Frame Stream.

In general, there are four possible times for the CCo to acquire the medium.

Tb-T > 900 microseconds. In this most common case, the CCo may grant the remaining time in the CFPI allocation to specific station(s) using by transmitting an RTS with Immediate Grant Flag (IGF) set (refer to Section 9.6.1.1).

900 > Tb-T > 421 microseconds. In this case, the CCo shall transmit a hybrid Long MPDU to occupy the time until the end of CFPI. The CCo may also transmit hybrid Long MPDUs in case 1.

421 > Tb-T > 179.52 microseconds. There is not sufficient time to transmit a hybrid MPDU, so the CCo shall transmit one or more FAIL delimiters with CC = 0b1 and CAP = 3.

179.52 > Tb-T. The CCo remains idle until the end of CFPI allocation.

All HomePlug AV stations shall assert in all PRP slots encountered while the CFPI procedure is in progress. CFPI protocol's aggressiveness can be varied by increasing the MaxCFPICols. For example:

By setting the MaxCFPICols to 8, the CFL can be made to continuously burst a maximum of 8 MPDUs before listening for activity on the medium.

By setting the MaxCFPICols to 1 and CFPI _EIFS to 1000 sec, the CFL can be made to listen for 1000 sec after every unsuccessful CFP initiation attempt.

Immediate Grant Using the RTS Delimiter

The CCo may provide an immediate grant to station(s) when the CFPI procedure is successfully completed before the end of CFPI allocation. This is achieved by transmitting an RTS delimiter with the Immediate Grant Flag (IGF) set to 0b1. Successful reception of the RTS shall cause the receiver to acknowledge using CTS. Furthermore, the station shall have exclusive access to the medium until the end of the duration indicated in the RTS.

If the LID in the RTS is set to a GLID, the receiver shall use the immediate grant to transmit Segments belonging to that Global Link prior to transmitting segments belonging to other MAC

Frame Streams. If the LID is not set to a GLID, the receiver may choose to transmit Segments from any of the MAC Frame Streams.

The station shall ensure that HomePlug 1.0.1 stations remain deferred during the immediate grant allocation. Thus, if a station getting the immediate grant has no pending Segments, it shall continue to transmit hybrid delimiter with CC set to 0b1 to prevent HomePlug 1.0.1 stations from accessing the medium. The station may use the immediate grant to transmit segments from one or more MAC Frame Streams.

Medium Retention for Contention-Free Access

During CFP allocations, each station that is the source of the CFP allocation shall be responsible for continuously deferring HomePlug 1.0.1 stations. This is achieved by transmitting Long MPDU with the CC bit set to 0b1 and MPDU lengths set as described in Section 9.4. Even when a CFP session has no data to send during its allocated interval, it shall continue to transmit delimiters so that HomePlug 1.0.1 stations remain deferred.

Medium Release After Contention-Free Access

When CFP allocation is followed by Hybrid CSMA allocation, the last transmission in the CFP allocation should set the CC bit in the HomePlug 1.0.1 delimiter to 0b0. Furthermore, the HomePlug 1.0.1 Frame Control fields should be chosen such that the PRP starts precisely at the end of CFP allocation. This will ensure that HomePlug 1.0.1 and AV stations are synchronized (with respect to the start of PRS Slots) at the start of the Shared CSMA allocation.

CSMA/CA Coexistence

As with HomePlug AV, fair and efficient sharing of the medium between HomePlug 1.0.1 and GREEN PHY CSMA/CA traffic requires GREEN PHY stations to behave in a manner similar to the HomePlug 1.0.1 stations. HomePlug GREEN PHY uses the same back-off mechanism as used by HomePlug 1.0.1 stations to ensure fair sharing on the medium between GREEN PHY and HomePlug 1.0.1 stations at the same priority level. Furthermore, as GREEN PHY stations must respect the priority levels, competing stations shall correctly indicate their priority in the PRS slots, and should listen for high priority HomePlug 1.0.1 traffic in that time.

For MPDU formats, it is important to recognize that the SOF simply reserves the medium for a period defined by the Frame Length (FL) field and delimiter type (response expected or no response expected). HomePlug 1.0.1 stations use VCS based on this information to know when to expect the EOF delimiter, and when to expect a response (if the delimiter so indicates). From the SOF until the first Priority Resolution Slot (PRS0), the medium is reserved and shall not be accessed by a station (except to send a response if required).

Coexistence with HomePlug 1.1 and Non-HomePlug Powerline Networks

HomePlug 1.1 is an enhancement to the HomePlug 1.0.1 specification, so that HomePlug 1.1 devices can better coexist with HomePlug AV networks. Using the HomePlug 1.0.1 delimiter to communicate allocation information, HomePlug AV can provide information to HomePlug 1.1 stations about the start and end of the HomePlug Shared CSMA Hybrid period. HomePlug 1.1 stations use this information to contend fairly with AV stations during this period, and refrain from transmissions during the remaining Beacon Period.

HomePlug 1.1 stations distinguish themselves from HomePlug 1.0.1 stations through the RSVD field in the HomePlug 1.0.1 End of Frame (EOF) Frame Control delimiter. When AV stations

determine that HomePlug 1.1 stations are present and HomePlug 1.0.1 stations are not present, they operate in Shared CSMA Hybrid Mode. In this mode, Contention-Free Period Initiation, Medium Retention and Release are not necessary (refer to Section 9.6).
Note: In Shared CSMA Mode, Hybrid operating mode is only used during Shared CSMA allocations and AV-only Mode of operation can be used in other allocations.
HomePlug 1.1 stations can also send and receive management messages to and from AV stations using the HomePlug 1.0.1 Frame Control delimiter.
The HomePlug 1.0.1 Frame Control may also be used to communicate allocation information and management messages between HomePlug AV and non-HomePlug powerline networks.
The features described in this section and the subsections are optional.
HomePlug 1.0.1 Delimiters
The HomePlug 1.0.1 Delimiter contains a 25-bit Frame Control Field and is used for long MPDU frames as Start of Frame (SOF) and End of Frame (EOF) delimiters and in short MPDU frames for the Response (RESP) delimiter (refer to Table 93). In HomePlug 1.0.1, Delimiter Type (DT) value 0b111 is reserved. For HomePlug 1.1, this reserved delimiter type along with the Contention Control (CC) bit are used identify the Coexistence Allocation Information Delimiter (DT = 0b111 and CC = 0b0) and identify the Coexistence Management Message Delimiter (DT = 0b111 and CC = 0b1).
Table 93: HomePlug 1.0.1 Frame Control Fields

Field	Bit Number	Bits	Definition
CC	24	1	Contention Control
DT	23 - 21	3	Delimiter Type
VF	20 - 8	13	Variant Field
FCCS	7 - 0	8	Frame Control Check Sequence

HomePlug 1.1 Identification
HomePlug 1.1 devices transmit the EOF delimiter in all long HomePlug 1.0.1 MPDU frames INVALID field set to 0b0 and bit number 8 in the HomePlug 1.0.1 EOF set to 0b1.
Coexistence Allocation Information Delimiter (DT = 0b111 and CC = 0b0)
The Coexistence Allocation Information Delimiter is used to communicate powerline medium allocation information to HomePlug 1.1 stations, between a HomePlug AV network and a non-HomePlug network, or between non-HomePlug networks. Since the CRC-8 is not reliable in detecting reception errors, the receiver must confirm that the delimiter is being received on a period basis, generally 33.3 or 40 milliseconds, before transmitting in the allocation communicated by the delimiter.
This delimiter communicates the start and end time of the periodic allocation for a network identified by the Allocation Type (AT) field. The Allocation Identifier (AID) is the address of the station transmitting the delimiter and is used in management messages to address the station.
In the case of an AV CCo transmitting Allocation Information for HomePlug 1.1 stations, the delimiter is communicated in the HomePlug 1.0.1 delimiter that is in the Hybrid Beacon transmission. The Allocation Identifier also indicates the number of HomePlug AV Beacon Slots following the Beacon Slot in which the delimiter was transmitted.

When HomePlug 1.1 stations are detected and no HomePlug 1.0.1 stations are detected, the CCo will change the mode of the HomePlug AV network to Shared CSMA Hybrid Mode. The CCo will transmit the HomePlug 1.0.1 Frame Control of the Hybrid Mode Beacon MPDU with Delimiter Type of 0b111 and CC set to 0b0 to communicate the CP allocation schedule to the HomePlug 1.1 stations in terms of the CSMA START TIME or the CSMA TIME (LENGTH). The format of the CSMA Allocation Information is shown in Table 94.

Table 94: Coexistence Allocation Information

HP1.0.1 Field	HPAV Interpretation	Bit Number	Bits	Definition
CC	CC	24	1	CC set to 0b0
DT	DT	23 - 21	3	Delimiter Type set to 0b111
VF	AID	20 - 18	3	Allocation Identifier
VF	AT	17 - 16	2	Allocation Type
VF	AVF	15 - 8	8	Allocation Variant Field
FCCS	FCCS	7 - 0	8	Frame Control Check Sequence

Allocation Identifier (AID)

The Allocation Identifier (AID) is a 3-bit field that is used to uniquely identify the station that is managing allocations. All allocation start and length information is specified relative to the corresponding Allocation Identifier.

When the Allocation Type is set to 0b00, the Allocation Identifier is set to the number of HomePlug AV Beacon Slots that follow the current Beacon Slot.

When the Allocation Type is not 0b00, stations should carefully select the Allocation Identifier to maximize the likelihood it is unique and avoid values that are already in used.

Allocation Type (AT)

The 2-bit Allocation Type (AT) is used to indicate the network for which the allocation is for (refer to Table 95). The HP1.1 Shared CSMA Allocation (AT = 0b00) is used by AV CCos to communicate the shared hybrid CSMA start and length to HomePlug 1.1 stations where the shared CSMA allocation starts immediately following the Beacon Slots. The other allocation types are more general purpose and specify an allocation including the start and length for either a HP Network (i.e., HomePlug AV and/or 1.1 stations) or for a non-HP Network. When a non-HP Network is communicating an allocation for an HP Network, the delimiter shall be transmitted synchronized to the AC line cycle, with a period equal to two line-cycle periods (33.3 or 40 milliseconds). HomePlug stations may ignore the Allocation Information Delimiter if it is not transmitted according to this requirement.

Table 95: Allocation Types

AT	Interpretation
0b00	HP1.1 Shared CSMA Allocation

0b01	HP Network Allocation
0b10	Non-HP Network Allocation
0b11	Reserved

Allocation Variant Field (AVF)

The Allocation Variant Field (AVF) is an 8-bit field whose format and function depend on the Allocation Type (AT).

Allocation Variant Field (AVF) for AT = 0b00

When the AT field is set to 0b00, the start time and duration of the shared hybrid CSMA interval are communicated to HomePlug 1.1 stations in the HomePlug 1.0.1 delimiter of the HomePlug AV Beacon.

Table 96 shows the structure of the AVF field for Allocation Type 0b00.

Table 96: Allocation Variant Field for Allocation Type = 0b00

Field	Bits	Definition
SLF	1	Start or Length Flag
AVF VF	7	ATF Variant Field Dependent on SLF

Start Time or Length Flag (SLF)

The Start Time or Length Flag (SLF) is used to indicate whether the ATF field specifies the CSMA START TIME or the CSMA TIME (LENGTH).

SLF = 0b0 designates the CSMA Start Time.

SLF = 0b1 indicates that the ATF field specifies the CSMA Length (duration).

Table 97 shows the overall structure of the ATF field and these fields are used to compute the CSMA Start Time when SLF = 0b0.

Table 97: Allocation Variant Field for AT = 0b000 and SLF = 0b0

Field	Bits	Definition
SLF	1	0b0
NFC	1	Number of Frame Control Symbols (0b0 =>1; 0b1 => 2)
NPL	6	Number of Payload Symbols Present

CSMA START TIME = (AID+1)(84.64 + NFC*59.28 + NPL*48.52 + B2BIFS) – 79.68

The CSMA START TIME is in units of microseconds measured from the end of the corresponding Coexistence Allocation Delimiter (last non-zero sample of the HomePlug 1.0.1 Frame Control) to the start time of the PRS signaling slot of the CSMA allocation.

When SLF = 0b1, the CSMA LENGTH (duration) is specified by the 7-bit ATF VF field, in multiples of 250 microseconds (see Table 98).

CSMA LENGTH = AVF_VF * 250

Table 98: Allocation Variant Field for AT = 0b000 and SLF=0b1

Field	Bits	Definition
SLF	1	0b1
AVF_VF	7	CSMA LENGTH (Duration)

The CSMA LENGTH is measured from the beginning of the first CSMA Priority Resolution Slot (PRS) to the end of the CSMA interval (see Figure 912).

Figure 912: CSMA LENGTH

Allocation Variant Field (AVF) for AT = (0b01 and 0b10)

This delimiter is used to communicate the allocation between HomePlug and non-HomePlug networks, or between non-HomePlug networks. The allocation may be negotiated using the management messages defined in Section 9.8.4. Table 99 shows the structure of the AVF field for AT= (0b01 and 0b10).

Table 99: Allocation Variant Field (AT = 0b01 to 0b11)

Field	Bits	Definition
SLF	1	Start or Length Flag
ALLOC_T	7	ALLOC START TIME or LENGTH

The ALLOC_T field is a 7-bit field used to specify ALLOC START TIME, in increments of 250 microseconds, when SLF = 0b0 and the ALLOC LENGTH, in increments of 500 microseconds, when SLF = 0b1. The ALLOC START TIME is measured from end of the corresponding Coexistence Allocation Delimiter (last non-zero sample of the HomePlug 1.0.1 Frame Control), to the start time of the allocation.

Frame Control Check Sequence (FCCS)

The Frame Control Check Sequence (FCCS) field is the same as in HomePlug 1.0.1.

Coexistence Management Message Delimiter (DT = 0b111, CC = 0b1)

The HomePlug 1.0.1 Frame Control reserved delimiter with DT = 0b111 and CC = 0b1 shall be used to define a Coexistence Management Message Delimiter, with field assignment, as shown in Table 910. This delimiter is used for exchanging management messages between stations in HomePlug AV networks, HomePlug 1.1 networks, and non-HomePlug networks. Since the CRC-8 is not reliable in detecting reception errors, each management message must be received exactly the same twice within 500 milliseconds to be accepted.

Table 910: Management Message Delimiter

HP1.0.1 Field	HP 1.1 Field	Bit Number	Bits	Definition
CC	CC	24	1	CC = 0b1
DT	DT	23 - 21	3	Delimiter Type 0b111
VF	MT	20 - 17	4	Message Type
VF	MVF	16 - 8	9	Message Variant Field
FCCS	FCCS	7 - 0	8	Frame Control Check Sequence

Message Type

The 4-bit Message Type field indicates the type of message being communicated. Table 911 shows

the interpretation of this field.

Table 911: Message Types

MT	Definition
0b0000	Network Information Request
0b0001	Network Information Response
0b0010	TDMA Allocation Request
0b0011	TDMA Allocation Response
0b0100	Reset Allocation Information
0b0101	FDMA Band Request
0b0110	FDMA Band Response
0b0111	Current Band Usage
0b01000 - 0b1111	RSVD

Message Variant Field (MVF)

The Message Variant Field (MVF) of the Coexistence Management Message Delimiter is a 9-bit message field that is used to convey management messages dependent on the Message Type (MT) field (see Table 911).

Network Information Request Message (MT=0b0000)

The Network Information Request management message is used to request the network information of a Network identified by the AID. The Network Information Request management message fields are shown in Table 912.

Table 912: Network Information Request Management Message

Field	Bits	Definition
AID	3	Allocation ID
NT	4	Network Type
TCF	1	TDMA Capability Flag
FCF	1	FDMA Capability Flag

Allocation Identifier (AID)

The Allocation Identifier (AID) is a 3-bit field used for uniquely identifying the station whose network information is being requested.

Network Type (NT)

The 2-bit Network Type (NT) field provides information on the type of network for the station making the request, as shown in Table 913.

Table 913: Network Types

NT	Definition
0b0000	HP 1.1
0b0001	HP AVLN
0b0010	HomePlug BPLN
0b0011 - 0b1111	Reserved – intended for future assignment

TDMA Capability Flag (TCF)

The TDMA Capability Flag (TCF) is set to 0b0 to indicate no TDMA support and to 0b1 to communicate TDMA capability.

FDMA Capability Flag (FCF)
The FDMA Capability Flag (FCF) is set to 0b0 to indicate no FDMA support and to 0b1 to communicate FDMA capability.
Network Information Response Message (MT=0b0001)
The Network Information Response management message is used to provide the network information of a Network identified by the AID. The Network Information Response management message fields are shown in Table 914.
Table 914: Network Information Management Message

Field	Bits	Definition
AID	3	Allocation ID
NT	4	Network Type
TCF	1	TDMA Capability Flag
FCF	1	FDMA Capability Flag

Allocation Identifier (AID)
The Allocation Identifier (AID) is a 3-bit field used for uniquely identifying the station responsible for allocation management. Stations should select the Allocation Identifier carefully to maximize the likelihood it is unique and avoid values that are already in used.
Network Type (NT)
Network Type (NT) is a 2-bit field that provides information on the type of network, as shown in Table 913.
TDMA Capability Flag (TCF)
The TDMA Capability Flag (TCF) is set to 0b0 to indicate no TDMA support and to 0b1 to communicate TDMA capability.
FDMA Capability Flag (FCF)
The FDMA Capability Flag (FCF) is set to 0b0 to indicate no FDMA support and to 0b1 to communicate FDMA capability.
TDMA Allocation Request Message (MT=0b0010)
The TDMA Allocation Request coexistence management message is shown in Table 915.
Table 915: Request TDMA Allocation Management Message

Field	Bits	Definition
AID	3	Allocation ID
ReqT	2	Request Type
PAR	4	Percent Allocation Requested

Allocation Identifier (AID)
The Allocation Identifier (AID) is a 3-bit field used to uniquely identify the allocation management station to which this request for TDMA allocation request is being sent. (For HPAV, the AID is the Beacon Slot Number.)
Request Type (RT)
The 2-bit Request Type (RT) field provides information on the nature of the request and the stations involved. A list of Request Types (RT) is shown in Table 916.
Table 916: Request Types

RT	Definition
0b00	HP In-Home
0b01	HP Access
0b10	Non-HP In-Home
0b11	Non-HP Access

Percent Allocation Request (PAR)

The 4-bit Percent Allocation Request (PAR) field specifies, in multiples of 6.25%, the percentage of the TDMA interval being requested for this TDMA allocation request.

TDMA Allocation Response Message (MT=0b0011)

The TDMA Allocation Response management message has the structure shown in Table 917.

Table 917: TDMA Allocation Response Management Message

Field	Bits	Definition
AID	3	Allocation ID
ResT	2	Response Type
PAG	4	Percent Allocation Granted

Allocation Identifier (AID)

The Allocation Identifier (AID) is a 3-bit field used for uniquely identifying the station responsible for allocation management.

Response Type (ResT)

The 2-bit Response Type (ResT) field provides information on the nature of the response and the stations involved. A list of Response Types (ResT) is shown in Table 916.

Percent Allocation Granted (PAG)

The 4-bit Percent Allocation Granted (PAG) field specifies, in multiples of 6.25%, the percentage of the TDMA interval being granted.

Reset Allocation Information Message (MT=0b0100)

The Reset Allocation Information management message has the structure shown in Table 918. This message is used to communicate that the allocation information must be reset due to a change such as a change in the number of HomePlug AV Beacon Slots that follow, which would cause a change in the AID and the CSMA START TIME.

Table 918: Reset Allocation Information Management Message

Field	Bits	Definition
AID	3	Allocation ID
RSVD	6	Reserved

Allocation Identifier (AID)

The Allocation Identifier (AID) is a 3-bit field used for uniquely identifying the station responsible for allocation management. The Reset Allocation Information management message used to advise stations to ignore (reset) allocation information associated with this Allocation Identifier. This may be necessary in HPAV when the Beacon Slot Number changes.

FDMA Band Request Message (MT=0b0101)

The FDMA Band Request management message is used to request the allocation of a particular frequency Band, and has the structure shown in Table 919.

Table 919: FDMA Band Request Management Message

Field	Bits	Definition
RSVD	1	Reserved
FreqS	4	Frequency Band Start
FreqE	4	Frequency Band End

Frequency Band Start (FreqS)

The 4-bit Frequency Band Start (FreqS) field specifies, in multiples of 2 MHz, the start of the frequency band allocation being requested.

Frequency Band End (FreqE)

The 4-bit Frequency Band End (FreqE) field specifies, in multiples of 2 MHz, the end of the frequency band allocation being requested.

FDMA Band Response Message (MT=0b0110)

The FDMA Band Response management message is used to indicate the status of an FDMA Frequency Band Request, and has the structure shown in Table 920.

Table 920: FDMA Band Response Management Message

Field	Bits	Definition
Status	1	Response Status Value
FreqS	4	Frequency Band Start
FreqE	4	Frequency Band End

Response Status Value (STATUS)

The 1-bit STATUS field in the FDMA Band Response management message in used to indicate the result of a corresponding FDMA Band Request. The response status values and the corresponding interpretation of the FreqS and FreqE fields are shown in Table 921.

Table 921: Response Status Values

Status	Definition
0b0	0 = rejected, not able, no proposal
0b1	1 = accepted/suggested if (FreqS, FreqE) same as in request => accepted. Otherwise, (FreqS, FreqE) indicates suggested values.

Frequency Band Start (FreqS)

The 4-bit Frequency Band Start (FreqS) field specifies, in multiples of 2 MHz, the start of the frequency band allocation.

Frequency Band End (FreqE)

The 4-bit Frequency Band End (FreqE) field specifies, in multiples of 2 MHz, the end of the frequency band allocation.

Current FDMA Band Usage Message (MT=0b0111)

The Current FDMA Band Usage management message is used to indicate the upper and lower boundaries of the current frequency band in use for a particular network, and has the structure shown in Table 922.

Table 922: Current FDMA Band Usage Management Message

Field	Bits	Definition

RSVD	1	Reserved
FreqS	4	Frequency Band Start
FreqE	4	Frequency Band End

Frequency Band Start (FreqS)

The 4-bit Frequency Band Start (FreqS) field specifies, in multiples of 2 MHz, the start of the current frequency band in use.

Frequency Band End (FreqE)

The 4-bit Frequency Band End (FreqE) field specifies, in multiples of 2 MHz, the end of the current frequency band in use.

HomePlug 1.0.1 Link Status and AV Beacon

Inactive HomePlug 1.0.1 nodes will remain silent, and not disrupt HomePlug AV communications, as long as they receive at least one valid HomePlug 1.0.1 delimiter every 5 seconds. Since all Beacons are transmitted using Hybrid Mode (and thus carry valid FC 1.0.1 information), the HomePlug 1.0.1 Link Status function will be satisfied.

HomePlug 1.0.1/1.1 and Neighbor Networks

When AVLNs operate in Coordinated Mode, it is possible for one or more AVLNs to detect the presence of HomePlug 1.0.1 or HomePlug 1.1 stations (refer to Section 9.3.1). To ensure proper operation under such conditions, the Hybrid operating mode of an AVLN in Coordinated Mode shall consider the Hybrid operating mode of other AVLNs in the group.

The CCo shall set the Hybrid Mode (HM) field based on its Hybrid operating mode, as defined in Table 453: Hybrid Mode Interpretation. The following rules shall be used to determine the Hybrid operating mode of an AVLN in Coordinated Mode when no Change HM BENTRY is present in any Central Beacon of any network in a Group of networks:

An AVLN that detects the presence of HomePlug 1.0.1 stations shall change its operating mode to Fully Hybrid, regardless of the hybrid operating mode of other Coordinating AVLNs.

An AVLN that detects the presence of HomePlug 1.1 stations and no HomePlug 1.0.1 station shall change its operating mode to Shared CSMA Hybrid Mode, regardless of the hybrid operating mode of other Coordinating AVLNs.

An AVLN operating in AV-Only Mode shall change the operating mode to Shared CSMA Hybrid Mode when one or more Coordinating AVLNs change their operating mode to either Shared CSMA Hybrid Mode or Fully Hybrid Mode.

AVLNs operating in Fully Hybrid Mode will need to defer HomePlug 1.0.1 stations from accessing the medium before the start of Beacon region. To enable Contention Free Period Initiation (CFPI), Shared CSMA Hybrid Mode AVLNs shall relinquish Reserved Regions that are within 4 milliseconds prior to the start of the Beacon Regions when requested by Coordinating AVLNs operating in Fully Hybrid Mode. AVLNs operating in Fully Hybrid mode shall request Reserved Regions from Coordinating AVLNs operating in Shared CSMA Hybrid mode, to provide CFPI before Beacon Regions.

Coordinating CCo’s operating in fully hybrid mode should provide CFPI allocations before CFP allocations and/or Beacon Regions that follow a local CSMA allocation or shared CSMA allocation. A CCo in fully hybrid mode should also provide CFPI allocations before CFP allocation that follows time intervals during which no STAs in the AVLN are transmitted. For

example, a CFP allocation that follows a Stayout Region should include a CFPI allocation.
To enable the Coordinating AVLNs to return to AV-Only Mode when HomePlug 1.0.1 and/or HomePlug 1.1 stations become inactive, CCo's of the AVLN can periodically add the Change HM BENTRY to the Central Beacon with NewHM set to AV Only Mode. The HM Change Countdown (HMCCD) field should be set to a value large enough to assure the BENTRY will propagate to and from the farthest CCo in the Group. A value of at least 16 is recommended.
All CCos in a Group of networks that detect a Change HM BENTRY in the Central Beacon of another CCo in the Group shall add the BENTRY to their Central Beacon. NewHM shall be set based on the following rules:
An AVLN that detects the presence of HomePlug 1.0.1 stations shall set NewHM to Fully Hybrid Mode.
An AVLN that detects the presence of HomePlug 1.1 stations and no HomePlug 1.0.1 stations shall set NewHM to Shared CSMA Hybrid Mode.
An AVLN that does not detect the presence of HomePlug 1.1 stations or HomePlug 1.0.1 stations shall set NewHM to the largest value of NewHM detected in other Central Beacon in the Group.
HMCCD must be set to assure the value is identical for all Central Beacons in a Beacon Period of the Group.
Any CCo in a Group of networks that detects a higher value for NewHM or HMCCD in the BENTRY of another Central Beacon in the Group shall change the corresponding field in their BENTRY to match the larger value.
The change becomes effective in the Beacon Period following the Beacon Period where HMCCD reaches 1. When the change becomes effective, the operating mode and the HM field in the Beacon MPDU Payload shall be set based on the most recent value of NewHM and the following rules; the BENTRY shall also be removed:
An AVLN that detects the presence of HomePlug 1.0.1 stations shall set the operating mode to Fully Hybrid Mode.
An AVLN that detects the presence of HomePlug 1.1 stations and no HomePlug 1.0.1 stations shall set the operating mode to Shared CSMA Hybrid Mode.
An AVLN that does not detect the presence of HomePlug 1.1 stations or HomePlug 1.0.1 stations shall set the operating mode and HM to AV-Only if current value of NewHM is AV-Only, otherwise the station shall set the operating mode to Shared CSMA Hybrid Mode.
The Change HM BENTRY shall only be used to change the operating mode from Fully Hybrid Mode or Shared CSMA Hybrid Mode to AV-Only Mode.
HomePlug 1.0.1/1.1 and Access Coexistence
The coexistence mechanism described in this section shall be used for coexistence of HomePlug AV Access networks with HomePlug 1.0.1 and/or HomePlug 1.1.

Access Coexistence
Note: This chapter is informative until the HomePlug Access (BPL) specification is complete, at which point this section may be revised.
HomePlug AV provides both time- and frequency-based coexistence of In-Home and Access

systems. Access systems are sometimes referred to as Broadband over Power Lines (BPL) in other parts of this specification. This chapter describes how In-Home Networks and an Access Network can coexist. It describes the Time Division Access Coexistence mechanisms that extend the Neighbor Network coordination described in Chapter 8 for access coexistence. It also describes the Frequency Division Access Coexistence mechanism. The features in this chapter are optional. However, coexistence with a HomePlug BPLN is mandatory using the Neighbor Network Coordination features described in Chapter 8.

Flexible Time Division Access Coexistence

The In-Home and Access Networks coexistence problem is slightly different than the (neighbor) In-Home Networks coexistence problem in that a STA (called Gateway STA) may belong to both an In-Home Network and the Access Network. As a result, additional requirements are placed on the Gateway STAs. Moreover, a Gateway STA may be able to obtain a CFP for its communication with the Access Network from either the Access Network or the In-Home Network it belongs to.

Terminologies

The following terms shall be used when discussing Access Network coexistence.

Access CCo: An Access CCo is a CCo that is controlled and owned by the Access Provider to provide services to Access Users (i.e., customers). An Access CCo maintains the Access Network and transmits a Beacon once every Beacon Period.

Gateway STA: A Gateway STA is a STA located inside the house of an Access User. The Gateway STA may belong only to the Access Network. However, if the Access User has its own In-Home Network, the Gateway STA may belong to both the Access Network and the In-Home Network.

Access Network: An Access Network consists of an Access CCo and Access STAs from all Access Users. A separate NEK is assigned by the Access CCo to each Access User.

Note: An Access User may have one or more Access STAs. Therefore, privacy can be protected between different Access Users.

In-Home CCo (or simply CCo): An In-Home CCo is a CCo that is owned by a user to set up an In-Home Network for delivery of audio, video, and data within the house. An In-Home CCo transmits a Beacon once every Beacon Period.

Note: An In-Home CCo may also be a Gateway STA.

In-Home Network: An In-Home Network consists of an In-Home CCo, In-Home STAs (or simply STAs), and optionally one or more Access STAs, all owned by the same user.

Assumptions

It is assumed that the Access CCo and the In-Home CCo(s):

Are within range of each other (that is, one is able to detect and decode the Beacon of the other).

Are operating in Coordinated Mode of the Neighbor Network coordination.

Access CCo Requirements

The Access CCo shall support the use of multiple network membership keys (NMKs) and multiple network encryption keys (NEKs). Each Access User should be assigned a different NMK and NEK during the association and authentication process. Therefore, the minimum number of NMKs and NEKs that the Access CCo must be able to handle is equal to the number of active Access Users in the Access Network. The Access CCo shall assign a single NID for all of its active

Access Users in the Access Network, so at most one NMK will be the default NID derived from the NMK.
The Access CCo shall support unencrypted association from Gateway STAs. It shall also support the use of a high-level application (e.g., secured HyperText Transfer Protocol (HTTP)) to validate the identity of an Access User/Gateway STA.
The Access CCo shall interpret the BENTRYs (refer to Section 4.4.3.15.4.1 and Section 4.4.3.15.4.2) in addition to the Region's BENTRY (refer to Section 4.4.3.15.4.3) of the Beacons of the In-Home CCo. This is required when the Access CCo is using bandwidth owned by the In-Home CCo (refer to Section 10.3.2).
Access STA Requirements
A Gateway STA shall support the following additional functionalities to communicate with an Access CCo:
It shall support unencrypted association with the Access CCo.
It shall support non-default NIDs (i.e., an NID associated with an NMK that is not derived from that NMK).
It shall support the use of a high-level application (e.g., secured HTTP) to prove the identity of the Access User to the Access CCo.
If an Access STA belongs to both the Access Network and an In-Home Network, it shall support the following additional functionalities:
It shall support the use of at least two NEKs, one for point-to-point communication with the Access CCo and the other for communication within the In-Home Network.
It shall support the use of two TEIs, one assigned by the Access CCo for use in the Access Network and the other assigned by the In-Home CCo for use in the In-Home Network.
Sharing of Resource between Access Network and In-Home Networks
A Gateway STA may be able to communicate with the Access CCo using a time interval that is owned by the In-Home CCo. In this case, the In-Home CCo shall continue to specify a CFP and the Access CCo shall continue to specify a Stayout Region during that time interval in their Beacons. However, the Access CCo may be allowed to transmit in that time interval. For more information, refer to Section 10.3.2.
Association, Authorization, and Authentication Procedures
Association Procedure
The association process of a Gateway STA is similar the procedure described in Section 7.3, with some minor modifications.
The Gateway STA shall scan for Beacons from the Access Network. The Access field in the Frame Control indicates whether the Beacons are from the Access Network or the In-Home network (refer to Section 4.4.1.3). The Gateway STA decodes the Beacon and locates the CSMA Region.
The Gateway STA then sends an unencrypted association message to the Access CCo in the CSMA Region. It shall support the use of a high-level application to prove the identity of the Access User to the Access CCo.
If Beacons from the Access Network cannot be detected, the Gateway STA shall never attempt to establish an Access Network. Instead, it shall continue to scan for Beacons from Access

Networks.
Furthermore, if the Gateway STA is configured to join both the Access Network and In-Home Network, it shall scan for Beacons from In-Home Networks as well. The Gateway STA shall proceed using the procedure described in Section 7.3 for joining an In-Home Network. The Gateway STA may become the CCo of the In-Home Network if it is the first STA to start up in the In-Home Network.

Authorization and Authentication Procedures

A Gateway STA and an Access Network CCo shall use procedures similar to those described in Section 7.3 for joining an Access Network. Differences are noted below.
First, since the NID used by an Access Network might not be derived from the NMK given to the Gateway STA for that Access Network, a Gateway STA shall use the NID (including the SL) provided to it with the NMK rather than the default NID when scanning for an NID match. The Gateway STA may attempt to associate and authenticate with an Access Network using the Access Network NMK it possesses, even if there is no NID match.
The NID to associate with an Access Network NMK is provided in one of two ways. It is either passed across the H1 interface along with the NMK using the **APCM_SET_KEY.REQ** primitive, or it is included in the **CM_SET_KEY.REQ** MME with the NMK in the payload of a **CM_ENCRYPTED_PAYLOAD.IND** MME that uses the DAK of the Gateway STA for payload encryption. In both cases, the Gateway STA shall associate the NID provided with the NMK with that NMK, rather than using the NMK to generate the NID offset to derive the default NID.
Once the Gateway STA has the NID and NMK, it shall obtain an NEK and EKS from the Access Network CCo in the manner described in Section 7.3.3 and Section 7.10.4.
The Access Network CCo will use a different NEK and may use a different NMK for each user. The EKS shall be the same for all users, however, so when a new EKS and NEK is distributed to any user, the EKS must be updated for all users. It is not required that the NEK change for all users, however. When the Access CCo has distributed the new EKS (and possibly, new NEKs) to all users in the Access Network, it shall use the countdown mechanism in Section 4.4.3.15.4.8 to make the new EKS and NEK(s) effective.
Since the NEK is different for every user, but the EKS is the same, the Access Network CCo shall use the MAC address (directly or indirectly through the TEI) of the Gateway STA to disambiguate the EKS when decrypting PBs from it. Likewise, it shall determine which NEK to use when encrypting PBs based on the destination STA's identity.
Since a different NMK may be given to each user, the Access Network CCo shall use the MAC address of the Gateway STA to determine which NMK to use when exchanging messages encrypted with an NMK. It is not necessary to coordinate NMK changes across all sub-AVLNs, so the Beacon-based countdown mechanism is not required.

Bandwidth-Allocation Procedure

This section describes the procedure used by a Gateway STA to set up a new CFP Connection to communicate with the Access CCo.
The Gateway STA and the Access CCo first exchange the CM_CONN_NEW.REQ and CM_CONN_NEW.CNF messages to set up the Connection. Next, the Gateway STA shall request

for bandwidth allocation (i.e., CFP) for the Connection.
Depending on whether the existing resource owned by the Access Network and/or In-Home Network is sufficient to support the new Connection, the procedure will involve one of the three scenarios described in Section 10.3.1 through Section 10.3.3.
Note: The procedure used by a Gateway STA to set up a new CFP Connection to communicate with another STA that also belongs to the same In-Home Network is the same as the one in Section 5.2.3.1. If the Gateway STA belongs only to the Access Network, the procedure to set up a new CFP Connection is the same as the one in Section 5.2.3.1, with the Gateway STA treated as the source STA and the Access CCo treated as both the destination STA and the CCo.
Using Access Network Resources
In this scenario, the Access Network is able to support the new CFP Connection with its existing resource (see Figure 101).
After receiving the CM_CONN_NEW.CNF message, the Gateway STA sends the CC_LINK_NEW.REQ message to the Access CCo. The message contains the STEI, DTEI, CSPEC, LLID, and channel estimate to the Access CCo.
If the Access CCo can support the new request with its existing share of resource, it shall send the CC_LINK_NEW.CNF message with a successful result code to the Gateway STA. The message contains the GLID assigned to the Link, which will appear in the schedule of the Beacons of the Access CCo.

Figure 101: CFP Setup in Access Network: Using a Resource from Access Network
Figure 102 shows an example of the schedules of the Beacons before and after the request is accepted in this scenario.

Figure 102: Example of Beacon Schedules: Using Resource from an Access Network
Using Resource from the In-Home Network
In this scenario, the Access Network is unable to support the new CFP Connection with its existing resource. However, the In-Home Network is able to support the new CFP Connection with its existing resource (see Figure 103).
If the Access CCo cannot support the new CFP Connection with its existing resource, the Access CCo shall send the CC_LINK_NEW.CNF message with an unsuccessful result code to the Gateway STA. The result code shall indicate that the Gateway STA should attempt to obtain resource from its own In-Home Network.
The Gateway STA shall then send the CC_ACCESS_NEW.REQ message to its In-Home CCo to request for resource.
If the In-Home CCo can support the request using its existing share of resource, it shall reply with the CC_ACCESS_NEW.CNF message with a successful result code to the gateway STA. The message contains the GLID that the In-Home CCo has assigned for the request. (The case where the In-Home CCo cannot support the request is considered in Section 10.3.3.)
The Gateway STA shall then send the CC_ACCESS_NEW.IND message with a successful result code to the Access CCo. This message contains the GCID that is assigned by the In-Home CCo for the CFP Link. The GCID will appear in the schedule of the Beacons of the In-Home CCo.

The Access CCo shall then reply with the CC_ACCESS_NEW.RSP message to confirm. The Gateway STA shall then send the CC_ACCESS_NEW.RSP message to its own In-Home CCo. For the time interval secured by the Gateway STA from its In-Home CCo, the Access CCo shall continue to specify a Stayout Region in the schedule of its Beacons. (The In-Home CCo shall continue to specify a CFP.) However, the Access CCo shall interpret the Schedule message of the In-Home CCo and is allowed to transmit in the time interval corresponding to the GLID assigned.

Figure 103: CFP Setup in Access Network: Using Resource from the In-Home Network

Figure 104 shows an example of the schedules of the Beacons before and after the request is accepted in this scenario.

Figure 104: Example of Beacon Schedules: Using Resource from In-Home Network

Using Neighbor Network Coordination

In this scenario, the Access Network and the In-Home Network are unable to support the new CFP Connection with their existing resource. Neighbor Network coordination is used to attempt to increase the share of resource used by the Access Network to support the Connection (see Figure 105).

Continuing from Section 10.3.2, if the In-Home Network cannot support the new CFP Connection with its existing resources, it shall send the CC_ACCESS_NEW.CNF message with an unsuccessful result code to the Gateway STA.

The Gateway STA shall then notify the Access CCo of the result using the CC_ACCESS_NEW.IND message with an appropriate result code. If the Access CCo decides to initiate Neighbor Network coordination to try to increase its share of resource for supporting the new Connection, it shall respond with CC_ACCESS_NEW.CNF, requesting the Gateway station to resend CC_LINK_NEW.REQ after one second.

Note: It is possible that the Neighbor Network coordination might not be complete in one second. In such cases, the CCo may hold the CC_LINK_NEW.CNF until a decision can be made.

If the Access CCo is able to obtain extra resource to support the new CFP Connection, it shall accept the subsequent CC_LINK_NEW.REQ by sending a CC_LINK_NEW.CNF, indicating a success. Otherwise, it shall respond with a CC_LINK_NEW.CNF to indicate failure.

Figure 105: CFP Setup in Access Network: Using Neighbor Network Coordination

Figure 106 shows an example of the schedules of the Beacons before and after the request is accepted in this scenario.

Figure 106: Example of Beacon Schedules: Using Neighbor Network Coordination

Bandwidth Release Procedure

The procedure for releasing an allocated bandwidth is similar to the case in Section 8.3.8, except when the scenario in Section 10.3.2 is used to request the bandwidth in the first place (that is, except when the resource is owned by the In-Home Network). This case is described in this section.

Either the In-Home CCo or the Gateway STA may initiate the bandwidth release. The Access CCo

shall never initiate the bandwidth release if the bandwidth used is owned by the In-Home CCo. Instead, after the connection teardown is performed, the Gateway STA shall initiate the Link release.

Figure 107 shows the MSG when the procedure is initiated by the Gateway STA after it and the Access CCo have performed the connection teardown.

Figure 107 – Bandwidth Release Initiated by Gateway STA

Figure 108 shows the MSG when the procedure is initiated by the In-Home CCo.

Figure 108 – Bandwidth Release Initiated by the In-Home CCo

Flexible Frequency Division Access Coexistence

HomePlug AV provides support for an optional second mode of coexistence with Access Networks through the use of frequency division. Two different mechanisms provide this capability. One that leverages an inherent feature of the HomePlug AV PHY.

One that uses FDMA Coexistence Management Messages (FCMMs) to negotiate the sharing of the channel.

A flexible frequency division option is provided to enable either the HomePlug AV network or an Access Network to use the full channel bandwidth when the other is not present or active. Either network can use FCMMs to request/reserve bandwidth from the other.

HomePlug AV stations can optionally use two symbol HomePlug AV Frame Control during Frequency Division Coexistence (refer to Section 3.2.1).

PHY Considerations

Flexible Frequency Division Access Coexistence (FFDAC) allows coexistence of home and Access PLC systems using disparate technologies, as long as these systems can exchange basic messages to negotiate dynamic, flexible sharing of frequency sub-bands. Efficient sharing in frequency domain, however, requires more stringent spectral containment at the transmitter and higher dynamic range and filtering at the receiver compared to time-domain sharing.

The HomePlug AV PHY uses windowed OFDM that provides good spectral containment by simply skipping the use of tones within and close to the border of a sub-band that needs to be relinquished to neighboring access networks. Although in this sense FFDAC is straightforward, in order to achieve good performance and efficient use of the bandwidth resource designers need to pay special attention to the following:

The signal level of the two networks may be very different at a given point in the medium. For example, the signal from the access station will be typically attenuated by many tens of dBs by the time it reaches a residence, and may be much smaller than a signal from the in-home network. This is known as a near-far scenario. In a near-far scenario, transmitters need to provide much better linearity to avoid jamming the signal of the other system with their out-of-band emissions. They are also likely to need some amount of flexible filtering determined by the transmitter linearity and the required rejection of out-of-band emissions.

Even in the presence of perfect spectral containment at the transmitter, the receivers in a near-far

Informative Text

PHY Considerations

Flexible Frequency Division Access Coexistence (FFDAC) allows coexistence of home and access PLC systems using disparate technologies, as long as these systems can exchange basic messages to negotiate dynamic, flexible sharing of frequency sub-bands. Efficient sharing in frequency domain, however, requires more stringent spectral containment at the transmitter and higher dynamic range and filtering at the receiver compared to time-domain sharing.

The HomePlug AV PHY uses windowed OFDM that provides good spectral containment by simply skipping the use of tones within and close to the border of a sub-band that needs to be relinquished to neighboring access networks. Although in this sense FFDAC is straightforward, in order to achieve good performance and efficient use of the bandwidth resource designers need to pay special attention to the following:

The signal level of the two networks may be very different at a given point in the medium. For example, the signal from the access station will be typically attenuated by many tens of dBs by the time it reaches a residence, and may be much smaller than a signal from the in-home network. This is known as a near-far scenario. In a near-far scenario, transmitters need to provide much better linearity to avoid jamming the signal of the other system with their out-of-band emissions. They are also likely to need some amount of flexible filtering determined by the transmitter linearity and the required rejection of out-of-band emissions.

Even in the presence of perfect spectral containment at the transmitter, the receivers in a near-far scenario need to accommodate signals from the neighboring system that enter the receiver at a much larger level than the desired signal. This set of conditions requires additional linearity and analog filtering in the receiver, possibly in combination with larger resolution requirements in the A/D converter. Additionally, the filtering needs to have programmable pass-bands, stop-bands, and sharp transition bands to maintain flexible sharing and efficient use of the spectrum.

FDMA Coexistence Management Messages (FCMMs)

Negotiation of the frequency bands between In-Home and Access Networks is accomplished using Coexistence Management Messages transmitted in HomePlug 1.0.1 delimiters as described in Section 9.8.4.

The FDMA Band Request Message is used to request the start and end frequency of a desired frequency band. This message is specified in Section 9.8.4.2.7).

The FDMA Band Response Message is used to indicate the result (rejected, granted or alternate recommendation) of an FDMA Band Request Message. This FDMA BAND Response Message is specified in Section 9.8.4.2.8).

The Current FDMA Band Usage Message is used to indicate the start and end frequency of the frequency band in current usage. This message is specified in Section 9.8.4.2.9).

Negotiation of the Channel

Under normal operation, either an In-Home or access station should operate without transmitting FCMMs, but shall always listen for the HomePlug 1.0.1 Preamble and FCMMs.

If an Access Network detects HomePlug 1.0.1 Preambles without detecting valid In-Home FCMMs, it shall begin transmitting Current Band Usage FCMMs.

If an Access Network detects In-Home Current Band Usage FCMMs, it shall transmit a Current

Band Usage Frequency Division Coexistence Message (FDCM).
If an In-Home Network detects an Access FCMM for the first time, it shall transmit an In-Home Current Band Usage FCMM. The In-Home Network shall also begin transmitting FCMMs.
If a Frequency Band Request FCMM is received, the other network shall reply with a Frequency Band Response FCMM.
Flexible TDM Coexistence with Non-HomePlug Networks
HomePlug AV networks optionally support flexible TDM Coexistence with non-HomePlug AV networks by exchanging information using the HomePlug 1.0.1 delimiters.
TDMA Coexistence Message defined in Section 9.8.4 are used to negotiate the percentage of bandwidth required. Subsequently, Coexistence allocation information described in Section 9.8.3 is used to indicate the start and end times of the TDMA allocations.

Management Messages
Management Message Format
The format of Management Messages is based on the standard Ethernet frame format, with a unique Ethertype assigned to HomePlug. HomePlug AV has a different Ethertype assignment than the Ethertype assigned to HomePlug 1.0.1. Management Messages are used for station-to-station control communication, but also may be used for control messages to and from a Higher Layer Entity (HLE). The Ethernet format enables messages to HLEs across an Ethernet network.
Table 111 shows the structure of the Management Message (MM).
Table 111: Management Message Format

Field	Octet Number	Field Size (bits)	Definition
ODA	0 - 5	48	Original Destination Address
OSA	6 - 11	48	Original Source Address
VLAN Tag	12 - 15	32	IEEE 802.1Q VLAN Tag (optional)
MTYPE	16 - 17	16	0x88e1 (IEEE-assigned Ethertype) Note: 0x88 is transmitted in the least-significant octet and 0xe1 is transmitted in the most-significant octet in conformance with IEEE 802.3.
MMV	18	8	Management Message Version

MMTYPE	19 - 20	16	Management Message Type
FMI	21	4	Fragmentation Management Information – 4 MSBs are Number of Fragments (NF_MI) of the MMENTRY 0x00 = MMENTRY is not Fragmented 0x01 = MMENTRY is Fragmented into two parts 0x02 = MMENTRY is Fragmented into three parts, and so on
		4	4 LSBs are Fragment Number (FN_MI) of the MMENTRY 0x00 = First or Only Fragment 0x01 = Second Fragment, and so on
	22	8	Fragmentation Message Sequence Number (FMSN)
MMENTRY	-	Var	Management Message Entry Data
MME PAD	-	0 - 46	MME PAD

Original Destination Address (ODA)

As with HomePlug AV, the Original Destination Address (ODA) is a 48-bit address of the HomePlug GREEN PHY station that is the ultimate destination of this Management Message. The address format follows the corresponding fields described in the IEEE 802-2001 [4] standard. Messages with an ODA other than the station's MAC address are delivered to the appropriate P1 or H1 interface.

Original Source Address (OSA)

As with HomePlug AV, the Original Source Address (OSA) is a 48-bit address of the HomePlug GREEN PHY station that is the original source of this Management Message. The address format follows the corresponding fields described in the IEEE 802-2001 [4] standard.

VLAN Tag

The VLAN Tag field, if present, contains four octets, as in IEEE 802.1Q [11], Clause 9 for

Ethernet-encoded Tag Protocol ID.

MTYPE

MTYPE shall be set to the IEEE-assigned Ethertype value of 0x88e1. The format of the MTYPE field follows the format of the Type/Length field described in the IEEE 802.3 standard [12]. This IEEE-assigned Ethertype may be used by future revisions of this specification and/or other specifications defined by the HomePlug Powerline Alliance. The Management Message Version (MMV) may be used to distinguish related messages defined in different specifications.

Management Message Version (MMV)

Management Message Version (MMV) is a 1-octet field that indicates the specification version used to interpret the Management Message.

All messages defined in HomePlug AV specification Version 1.0 shall have the MMV field set to 0x00.

All messages defined in HomePlug AV specification Version 1.1 shall have the MMV field set to 0x01.

All messages defined in HomePlug GREEN PHY specification Version 1.0 shall have the MMV field set to 0x01.

All other values of the MMV field are reserved. Implementation based on HomePlug AV specification Version 1.0 shall discard all Management Messages with MMV not equal to 0x00. It is optional for implementations based on HomePlug AV specification Version 1.1 to interoperate with implementations based on HomePlug AV specification Version 1.0. It is mandatory for implementations based on HomePlug GREEN PHY specification Version 1.0 to interoperate with implementations based on HomePlug AV specification Version 1.1. Implementations based on HomePlug AV specification Version 1.1 shall discard all Management Messages with MMV greater than 0x01.

Future revisions of this specification or specifications based on this one addressing other applications may use this field to interpret messages defined in more than one specification.

Management Message Type (MMTYPE)

Management Message Type (MMTYPE) is a 2-octet field that defines the Management Message that follows. Table 115 lists the various Management Message Types.

The two LSBs of MMTYPE indicate that the message is a Request, Confirm, Indication, or Response (see Table 112).

The three MSBs of the MMTYPE indicate the category to which the Management Message belongs, as shown in Table 113.

Table 112: Interpretation of Two LSBs of MMTYPE

MMTYPE Two LSB Value	Type	Description
0b00	REQ	Management Message Request
0b01	CNF	Management Message Confirm
0b10	IND	Management Message Indication

0b11	RSP	Management Message Response

Table 113: Interpretation of Three MSBs of MMTYPE

MMTYPE Three MSB Value	Type	Description
0b000	STA – Central Coordinator	Management Messages exchanged between STA and CCo
0b001	Proxy Coordinator	Management Messages exchanged with the Proxy Coordinator
0b010	Central Coordinator – Central Coordinator	Management Messages exchanged between neighboring CCos
0b011	STA – STA	Management Messages exchanged between two Stations
0b100	Manufacturer Specific	Management Message defined by the AV/GP chip manufacturers for exchanging manufacturer dependent control information across the H1 interface.
0b101	Vendor Specific	Management Message defined by either the AV/GP chip manufacturer or AV/GP product vendor for exchanging chip or product implementation dependent control information across the H1 interface and/or over the powerline (i.e., between stations).
0b110 - 0b111	Reserved	Reserved for future use

Fragment Management Information

The Number of Fragments (NF_MI), Fragment Number (FN_MI), and Fragmentation Message Sequence number (FMSN) fields enable transmission of management information (i.e., MMENTRY) using multiple management messages in instances where all the management information cannot fit in a single management message. The maximum size of management messages transmitted using multi-network broadcasting (refer to Section 5.4.3.1) is limited to 502 octets. For transmissions to STAs associated with the same AVLN, the maximum size of the

management message is limited to 1518 octets (including VLAN Tag). Management information that can be fit in a single management message shall not be fragmented.
Below is a complete list of MMTYPEs that may be fragmented:
CC_LINK_INFO.CNF
CC_LINK_INFO.IND
CC_HANDOVER_INFO.IND
CC_DISCOVER_LIST.CNF
CC_DISCOVER_LIST.IND
CC_SET_TEI_MAP.IND
CP_PROXY_APPOINT.REQ
CM_CONN_INFO.CNF
CM_NW_STATS.CNF
The NF_MI field indicates the number of management messages into which the management information is fragmented. A value of 0x0 indicates no fragmentation. A value of 0x1 indicates that the management information is fragmented across two management messages, and so on. The NF_MI field shall remain constant across all management messages that carry fragments of the same management information.
The FN_MI field indicates the fragment number of the management information contained within the management message. A value of 0x0 indicates the first or only fragment. A value of 0x1 indicates the second fragment and so on.
The FMSN field is initialized to zero and incremented by one when Management information has to be fragmented at the transmitter, regardless of the destination address or the type/version of the management message. The FMSN field shall be set to 0x00 in management messages that do not have to be fragmented. FMSN shall remain constant across all management messages that carry fragments of the same management information.
For Fragmentation purposes, the MMENTRY is treated as an octet stream. Each management message carrying fragmented MMENTRY shall contain the ODA, OSA, MTYPE, MMV, MMTYPE, and FMI fields followed by a fragment of the MMENTRY. The first fragment of the MMENTRY shall contain octets of the MMENTRY starting with the least-significant octet, and so on. When MMENTRY is fragmented, all fragments except the last one shall be of the maximum possible length.
Figure 111 shows fragmentation of a MMENTRY into three management messages. The receiver shall use the {ODA, OSA, MMV, MMTYPE, FMSN} tuple to uniquely identify fragments belonging to the same management information.
Due to the non-reliable nature of the powerline medium, it is possible to have scenarios where the receiver will not receive all fragments of a Management Information successfully. Reception of an out-of-order fragment indicates a lost fragment and shall cause the receiver to discard all fragments of the Management Information. If all received fragments of a Management Information are in order and one or more fragments are pending to be received, the receiver should wait for a minimum of FragMMI_ReassemblyTimeOut duration before declaring a reassembly failure.

Figure 111: Illustration of Fragmentation of a MMENTRY

Management Message Entry Data (MME)

The format of Management Message Entry Data (message) depends on the MMTYPE with which it is associated. Table 114 shows prefix conventions used when naming the Management Messages.

Table 114: Prefix Conventions when Naming Management Messages

Prefix	Description
CC	The message is between the Connection Manager (CM) and CCo.
CM	The message is between the CM and CM.
CP	The message is between the CCo and PCo.
PH	The message is between the PCo and Hidden station (HSTA).
NN	The message is between Neighbor Coordinators (NCos).

Some Management Messages are intended for use only by the HomePlug AV or HomePlug GREEN PHY Control Plane, and are not allowed over the H1 interface. The “From H1 Interface” and “To H1 Interface” columns in Table 115 indicate whether the MME can be received from or transmitted to the HLE (or bridged from another network) via the H1 interface, respectively. The interpretation of the values in this column is as follows:

Yes Indicates the message can be received or transmitted across the H1 Interface. The message can also be exchanged between stations over the Powerline.

No Indicates the message shall not be received from and shall not be transmitted to the H1 Interface. The message can be exchanged between stations over the Powerline.

Only Indicates the message can only be received from or transmitted to the H1 interface. The message shall never be transmitted over the powerline.

Some MMEs that are transmitted over the powerline can be generated by both the HLE (and transmitted to STA through the H1 interface) and by the Control Plane of the STA. When responses to such MMEs are received by the STA, there is ambiguity about whether the MME has to be sent to the HLE or to the Control Plane. Details about how such ambiguities are resolved is beyond the scope of this specification.

The optional/mandatory nature of the Management Messages depends on the STA Capabilities. Table 115 shows the optional/mandatory requirements for MMEs based on the CCo Capability (refer to Section 7.4.3.1) of the station. This table is intended to provide guidelines to implementers on the Mandatory MMEs that need to be implemented based on the CCo Capabilities of the station. The interpretation of each of the columns in this table is as follows:

Req. L-2 CCo TX Transmit requirement for a Level-2 CCo capable station acting as a CCo and as STA in an AVLN.

Req. L-2 CCo RX Receive requirement for a Level-2 CCo capable station acting as a CCo and as STA in an AVLN.

Req. L-1 CCo TX Transmit requirement for a Level-1 CCo capable station without QoS support acting as a CCo and as STA in an AVLN.

Req. L-1 CCo RX Receive requirement for a Level-1 CCo capable station without QoS support

acting as a CCo and as STA in an AVLN.
Req. L-0 CCo TX Transmit requirement for a Level-0 CCo capable station acting as a CCo and as STA in an AVLN.
Req. L-0 CCo RX Receive requirement for a Level-0 CCo capable station acting as a CCo and as STA in an AVLN.
A value of “M” in these columns indicates that the requirement is Mandatory. A value of “O” indicates that the requirement is Optional. A value of “X” indicates that a station should never transmit/receive the corresponding MME. Reception of an MME that is not supported by the station shall cause the station to respond with a CM_MME_ERROR.IND message (refer to Section 11.5.32).
The “NEK Encrypted” column indicates whether the corresponding MME is encrypted using NEK (i.e., PHY Block Body Encryption) by the transmitter (refer to Section 5.4.2) when sent over the powerline medium. A value of “Always” in this column indicates that the transmitter shall encrypt the MME. Furthermore, receivers shall discard such MMEs if they are transmitted in clear text. A value of “Never” in this column indicates that the MME shall never be NEK encrypted. A value of “Both” indicates that there are some instances where the MME is transmitted without NEK Encryption and other instances where the MME is transmitted with NEK Encryption. The NEK Encrypted column applies only to instances where MMEs are not transmitted as part of CM_ENCRYPTED_PAYLOAD.IND MME.
The nominal priority settings for the Management Messages is PLID = 0x02. Further recommendations for priority settings for CM_CHAN_EST.IND and CM_TM_UPDATE.IND are presented in Section 5.2.6.5.
As with HomePlug AV, HomePlug GREEN PHY allows two groups of MMTYPE values for Manufacturer-Specific and Vendor-Specific extensions to the MMEs defined within this specification. Manufacturer-Specific MMEs are only allowed across the H1 Interface and can be used as a way to implement H1 primitives. Manufacturer-Specific MMEs do not contain a way to identify the HLE that sent the MME and, hence, may limit their usability.
Vendor-Specific MMEs always include the Organizationally Unique Identifier (OUI) for the Vendor, enabling them to be uniquely identified. These can be exchanged across the H1 interface as well as over the powerline. STAs can use the CM_STA_CAP MMEs to determine the OUI of other STAs in the network.

Table 115: Management Message Type (Note there is a Table 11-5b)

MMTYPE Base Value	CC_HANDOVER_INFO.IND Interpretation (See Station – Central Coordination	From H1 Interface	To H1 Interface	Req. L-2 CCo TX	Req. L-2 CCo RX	Req. L-1 CCo TX	Req. L-1 CCo RX	Req. L-0 CCo TX	Req. L-0 CCo RX	NEK Encrypted By PHY
0x0000	CC_CCO_APPOINT.REQ (See Note #1)	Yes	No	M	M	M	M	M	M	Always
	CC_CCO_APPOINT.CNF (See Note #1)	No	Yes	M	M	M	M	M	M	Always
0x0004	CC_BACKUP_APPOINT.REQ	No	No	O	O	O	O	O	O	Always
	CC_BACKUP_APPOINT.CNF	No	No	O	O	O	O	O	O	Always
0x0008	CC_LINK_INFO.REQ	Yes	No	M	M	M	M	M	X	Always
	CC_LINK_INFO.CNF	No	Yes	M	M	M	M	X	M	Always
	CC_LINK_INFO.IND (See Note #3)	No	No	O	O	O	O	X	X	Always
	CC_LINK_INFO.RSP (See Note #3)	No	No	O	O	O	O	X	X	Always
0x000C	CC_HANDOVER.REQ (See Note #4)	No	No	M	M	M	M	M	M	Always
	CC_HANDOVER.CNF (See Note #4)	No	No	M	M	M	M	M	M	Always

0x0024 0x0010	CC_HANDOVER_INFO.IND (See Note #4)	No	No	M	M	M	M	M	M	Always
	CC_HANDOVER_INFO.REQ (See Note #4)									
	CC_HANDOVER_INFO.RSP (See Note #4)	No	No	M	M	M	M	M	M	Always
0x0014	CC_DISCOVER_LIST.REQ	Yes	No	M	M	M	M	M	M	Always
	CC_DISCOVER_LIST.CNF	No	Yes	M	M	M	M	M	M	Always
	CC_DISCOVER_LIST.IND	No	No	M	M	M	M	M	M	Always
0x0018	CC_LINK_NEW.REQ (See Note #2)	No	No	M	M	M	M	M	X	Always
	CC_LINK_NEW.CNF (See Note #2)	No	No	M	M	M	M	X	M	Always
0x001C	CC_LINK_MOD.REQ (See Note #2)	No	No	M	M	M	M	M	X	Always
	CC_LINK_MOD.CNF (See Note #2)	No	No	M	M	M	M	X	M	Always
0x0020	CC_LINK_SQZ.REQ (See Note #5)	No	No	O	O	O	O	X	O	Always
	CC_LINK_SQZ.CNF (See Note #5)	No	No	O	O	O	O	O	X	Always

0x0024	CC_LINK_REL.REQ (See Note #2)	No	No	M	M	M	M	M	X	Always
	CC_LINK_REL.IND (See Note #2)	No	No	M	M	M	M	X	M	Always
0x0028	CC_DETECT_REPORT.REQ (See Note #6)	No	No	O	O	O	O	X	O	Always
	CC_DETECT_REPORT.CNF (See Note #6)	No	No	O	O	O	O	O	X	Always
0x002C	CC_WHO_RU.REQ	Yes	No	M	M	M	M	M	M	Both
	CC_WHO_RU.CNF	No	Yes	M	M	M	M	M	M	Both
0x0030	CC_ASSOC.REQ	No	No	M	M	M	M	M	M	Both
	CC_ASSOC.CNF	No	No	M	M	M	M	M	M	Both
0x0034	CC_LEAVE.REQ	No	No	M	M	M	M	M	M	Both
	CC_LEAVE.CNF	No	No	M	M	M	M	M	M	Both
	CC_LEAVE.IND	No	No	M	M	M	M	M	M	Both
	CC_LEAVE.RSP	No	No	M	M	M	M	M	M	Both
0x0038	CC_SET_TEI_MAP.REQ	No	No	O	M	O	M	O	M	Both
	CC_SET_TEI_MAP.IND	No	No	M	M	M	M	M	M	Both
0x003C	CC_RELAY.REQ (See Note #7)	No	No	O	O	O	O	O	O	Both
	CC_RELAY.IND (See Note #7)	No	No	O	O	O	O	O	O	Both
0x0040	CC_BEACON_RELIABILITY.REQ	No	No	M	M	M	M	M	M	Always

	CC_BEACON_RELIABILITY.CNF	No	No	M	M	M	M	M	M	Always
0x0044	CC_ALLOC_MOVE.REQ	No	No	O	M	O	M	O	X	Always
	CC_ALLOC_MOVE.CNF	No	No	M	O	M	O	X	O	Always
0x0048	CC_ACCESS_NEW.REQ	No	No	O	O	O	O	O	X	Always
	CC_ACCESS_NEW.CNF	No	No	O	O	O	O	X	O	Always
	CC_ACCESS_NEW.IND	No	No	O	O	O	O	O	X	Always
	CC_ACCESS_NEW.RSP	No	No	O	O	O	O	X	O	Always
0x004C	CC_ACCESS_REL.REQ	No	No	O	O	O	O	O	X	Always
	CC_ACCESS_REL.CNF	No	No	O	O	O	O	X	O	Always
	CC_ACCESS_REL.IND	No	No	O	O	O	O	O	O	Always
	CC_ACCESS_REL.RSP	No	No	O	O	O	O	O	O	Always
0x0050	CC_DCPPC.IND (See Note #8)	No	No	O	M	O	M	O	M	Always
	CC_DCPPC.RSP (See Note #8)	No	No	M	O	M	O	M	O	Always
0x0054	CC_HP1_DET.REQ	No	No	M	M	M	M	M	M	Always
	CC_HP1_DET.CNF	No	No	M	M	M	M	M	M	Always
0x0058	CC_BLE_UPDATE.IND	No	No	O	M	O	M	O	X	Always
0x005C – 0x1FFC	Reserved for future use									

	Proxy Coordinator									
0x2000	CP_PROXY_APPOINT.REQ (See Note #9)	No	No	O	O	O	O	O	O	Always
	CP_PROXY_APPOINT.CNF (See Note #9)	No	No	O	O	O	O	O	O	Always
0x2004	PH_PROXY_APPOINT.IND (See Note #9)	No	No	O	O	O	O	O	O	Both
0x2008	CP_PROXY_WAKE.REQ (See Note #9)	No	No	O	O	O	O	O	O	Always
0x200C – 0x3FFC	Reserved for future use									
	CCo – CCo									
0x4000	NN_INL.REQ	No	No	M	M	X	X	X	X	Never
	NN_INL.CNF	No	No	M	M	X	X	X	X	Never
0x4004	NN_NEW_NET.REQ	No	No	M	M	X	X	X	X	Never
	NN_NEW_NET.CNF	No	No	M	M	X	X	X	X	Never
	NN_NEW_NET.IND	No	No	M	M	X	X	X	X	Never
0x4008	NN_ADD_ALLOC.REQ	No	No	M	M	X	X	X	X	Never
	NN_ADD_ALLOC.CNF	No	No	M	M	X	X	X	X	Never
	NN_ADD_ALLOC.IND	No	No	M	M	X	X	X	X	Never
0x400C	NN_REL_ALLOC.REQ	No	No	M	M	X	X	X	X	Never

0x6020	CM_RRL_ALLOC.CNF	No	No	M	M	X	X	X	X	Never
0x4010	NN_REL_NET.IND	No	No	M	M	X	X	X	X	Never
0x4014 – 0x5FFC	Reserved for future use	-								
	Station – Station									
0x6000	CM_UNASSOCIATED_STA.IND	No	Yes	M	M	M	M	M	M	Never
0x6004	CM_ENCRYPTED_PAYLOAD.IND	Yes	Yes	M	M	M	M	M	M	Both
	CM_ENCRYPTED_PAYLOAD.RSP	Yes	Yes	M	M	M	M	M	M	Both
0x6008	CM_SET_KEY.REQ	Yes	Yes	M	M	M	M	M	M	Always
	CM_SET_KEY.CNF	Yes	Yes	M	M	M	M	M	M	Always
0x600C	CM_GET_KEY.REQ	Yes	Yes	M	M	M	M	M	M	Never
	CM_GET_KEY.CNF	Yes	Yes	M	M	M	M	M	M	Never
0x6010	CM_SC_JOIN.REQ	No	No	M	M	M	M	M	M	Never
	CM_SC_JOIN.CNF	No	No	M	M	M	M	M	M	Never
0x6014	CM_CHAN_EST.IND	No	No	M	M	M	M	M	M	Both
0x6018	CM_TM_UPDATE.IND	No	No	O	M	O	M	O	M	Both
0x601C	CM_AMP_MAP.REQ	Yes	No	O	M	O	M	O	M	Always
	CM_AMP_MAP.CNF	No	Yes	M	O	M	O	M	O	Always

0x6020	CM_BRG_INFO.REQ (See Note #10)	Yes	No	O	M	O	M	O	M	Always
	CM_BRG_INFO.CNF (See Note #10)	No	Yes	M	M	M	M	M	M	Always
0x6024	CM_CONN_NEW.REQ (See Note #2)	No	No	M	M	M	M	M	M	Always
	CM_CONN_NEW.CNF (See Note #2)	No	No	M	M	M	M	M	M	Always
0x6028	CM_CONN_REL.IND (See Note #2)	No	No	M	M	M	M	M	M	Always
	CM_CONN_REL.RSP (See Note #2)	No	No	M	M	M	M	M	M	Always
0x602C	CM_CONN_MOD.REQ (See Note #2)	No	No	M	M	M	M	M	M	Always
	CM_CONN_MOD.CNF (See Note #2)	No	No	M	M	M	M	M	M	Always
0x6030	CM_CONN_INFO.REQ	Yes	No	M	M	M	M	M	M	Always
	CM_CONN_INFO.CNF	No	Yes	M	M	M	M	M	M	Always
0x6034	CM_STA_CAP.REQ	Yes	No	M	M	M	M	M	M	Both
	CM_STA_CAP.CNF	No	Yes	M	M	M	M	M	M	Both
0x6038	CM_NW_INFO.REQ	Yes	No	M	M	M	M	M	M	Always

	CM_NW_INFO.CNF	No	Yes	M	M	M	M	M	M	Always
0x603C	CM_GET_BEACON.REQ	Yes	No	M	M	M	M	M	M	Always
	CM_GET_BEACON.CNF	No	Yes	M	M	M	M	M	M	Always
0x6040	CM_HFID.REQ	Yes	No	M	M	M	M	M	M	Both
	CM_HFID.CNF	No	Yes	M	M	M	M	M	M	Both
0x6044	CM_MME_ERROR.IND	No	Yes	M	M	M	M	M	M	Both
0x6048	CM_NW_STATS.REQ	Yes	No	M	M	M	M	M	M	Always
	CM_NW_STATS.CNF	No	Yes	M	M	M	M	M	M	Always
0x604C	CM_LINK_STATS.REQ	Yes	No	M	M	M	M	M	M	Always
	CM_LINK_STATS.CNF	No	Yes	M	M	M	M	M	M	Always
0x6050 – 7FFC	Reserved for future use	-								
	Manufacturer Specific									
0x8000 – 0x9FFC	Manufacturer Specific Messages	Only	Only							-
	Vendor Specific									
0xA000 – 0xBFFC	Vendor-Specific Messages	Yes	Yes							Both

Notes:

- CC_CCO_APPOINT.REQ is generated by HLE. It is mandatory for stations to be able to receive this message from H1 interface and pass it to the CCo. Similarly, it is mandatory for all stations to be able to receive CC_CCO_APPOINT.CNF from any station in the AVLN and pass it to the HLE.
- Refer to Section 5.2.3 for details.
- Optional when the station does not support Soft Handover (refer to Section 7.5). Mandatory if it does.

- Support for Hard Handover is Mandatory (refer to Section 7.5).
- Optional if the station does not support Squeeze/De-Squeeze procedure (refer to Section 5.2.3.8.1). Mandatory if it does.
- Optional if the station does not support Detect-and-Report procedure (refer to Section 5.2.5). Mandatory if it does.
- Optional if the station does not support the Proxy Networking procedure (refer to Section 7.7). Mandatory if it does.
- Optional if the station does not support simultaneous participation in more than one network (refer to Section 5.5.4.1).
- Optional if the station does not support Proxy Networking (refer to Section 7.7). Mandatory if it does.
- Any STA can request bridging information by using CM_BRG_INFO.REQ. It is mandatory for all stations to respond with CM_BRG_INFO.CNF. It is mandatory that all bridges periodically generate CM_BRG_INFO.CNF (refer to Section 5.3).

MME PAD

Management Messages shall be at least 60 octets long. MME PAD is a variable-length field that shall be present in Management Messages whose length, excluding the MME-PAD (i.e., from ODA to MMENTRY), is less than 60 octets. When MME PAD is present, its length shall be chosen to be the smallest possible value to ensure that the Management Message length, including the MME PAD (i.e., from ODA to MME PAD), is equal to 60 octets.

MME Support of HomePlug GREEN PHY

HomePlug GP stations support only a subset of MMEs supported by HomePlug AV 1.1 Level-0 CCOs. Table 11-5b shows the MMEs supported by GP and AV 1.1 Level-0 CCo capable device. The interpretation of “From H1”, “To H1” and “NEK Encrypted by PHY” columns is the same as described in Section 11.1.8. The interpretation of the remaining columns is as follows:

- Req L-0 CCo TX - Transmit requirement for a HomePlug AV 1.1 Level-0 CCo capable device acting as a CCo in an AVLN
- Req L-0 CCo RX – Receive requirement for a HomePlug AV 1.1 Level-0 CCo capable device acting as a CCo in an AVLN
- Req L-0 STA TX - Transmit requirement for a HomePlug AV 1.1 Level-0 CCo capable device acting as a STA in an AVLN
- Req L-0 STA RX – Receive requirement for a HomePlug AV 1.1 Level-0 CCo capable device acting as a STA in an AVLN
- Req HPGP CCo TX - Transmit requirement for a GP device acting as a CCo in an AVLN
- Req HPGP CCo RX – Receive requirement for a GP device acting as a CCo in an AVLN
- Req HPGP STA TX - Transmit requirement for a GP device acting as a STA in an AVLN
- Req HPGP STA RX – Receive requirement for a GP device acting as a STA in an AVLN

	CC_LINK_INFO.IND (See

All Green PHY devices are CCo capable. In networks comprising both HomePlug AV 1.1 stations and HomePlug GP stations, HomePlug GP stations may receive MMEs that they do not support. In such instances, HomePlug GP stations shall send a CM_MME_ERROR.IND MME with the ReasonCode Field of that MME set to 0x00 – indicating that the MME is not supported.

Table 11-5b: Comparison of Management Message Types for HomePlug AV (STA and L0 CCo) vs. HomePlug GREEN PHY (STA and CCo)

MMTYPE Base Value	Interpretation	From H1	To H1	Req. L-0 CCo TX	Req. L-0 CCo RX	Req. L-0 STA TX	Req. L-0 STA RX	Req. HPGP CCo TX	Reg. HPGP CCo RX	Req. HPGP STA TX	Reg. HPGP STA RX	NEK Encrypted By PHY
	Station – Central Coordination											
0x0000	CC_CCO_APPOINT.REQ (See Note #1)	Yes	No	X	M	M	X	X	M	M	X	Shall
	CC_CCO_APPOINT.CNF (See Note #1)	No	Yes	M	X	X	M	M	X	X	M	Shall
0x0004	CC_BACKUP_APPOINT.REQ	No	No	O	X	X	O	O	X	X	O	Shall
	CC_BACKUP_APPOINT.CNF	No	No	X	O	O	X	X	O	O	X	Shall
0x0008	CC_LINK_INFO.REQ	Yes	No	X	X	M	X	X	X	X	X	Shall
	CC_LINK_INFO.CNF	No	Yes	X	X	X	M	X	X	X	X	Shall

	CC_LINK_INFO.IND (See Note #3)	No	No	X	X	X	X	X	X	X	X	Shall
	CC_LINK_INFO.RSP (See Note #3)	No	No	X	X	X	X	X	X	X	X	Shall
0x000C	CC_HANDOVER.REQ (See Note #4)	No	No	M	X	X	M	M	X	X	M	Shall
	CC_HANDOVER.CNF (See Note #4)	No	No	X	M	M	X	X	M	M	X	Shall
0x0010	CC_HANDOVER_INFO.IND (See Note #4)	No	No	M	X	X	M	M	X	X	M	Shall
	CC_HANDOVER_INFO.RSP (See Note #4)	No	No	X	M	M	X	X	M	M	X	Shall
0x0014	CC_DISCOVER_LIST.REQ	Yes	No	M	M	M	M	M	M	M	M	Shall
	CC_DISCOVER_LIST.CNF	No	Yes	M	M	M	M	M	M	M	M	Shall
	CC_DISCOVER_LIST.IND	No	No	X	M	M	X	X	M	M	X	Shall

0x0028	CC_DELINK_NEW.REQ (See Note #2)	No	No	X	X	M	X	X	X	X	X	Shall
	CC_LINK_NEW.CNF (See Note #2)	No	No	X	X	X	M	X	X	X	X	Shall
0x001C	CC_LINK_MOD.REQ (See Note #2)	No	No	X	X	M	X	X	X	X	X	Shall
	CC_LINK_MOD.CNF (See Note #2)	No	No	X	X	X	M	X	X	X	X	Shall
0x0020	CC_LINK_SQZ.REQ (See Note #5)	No	No	X	X	X	O	X	X	X	X	Shall
	CC_LINK_SQZ.CNF (See Note #5)	No	No	X	X	O	X	X	X	X	X	Shall
0x0024	CC_LINK_REL.REQ (See Note #2)	No	No	X	X	M	X	X	X	X	X	Shall
	CC_LINK_REL.IND (See Note #2)	No	No	X	X	X	M	X	X	X	X	Shall

0x0028	CC_DETECT_REPORT.REQ (See Note #6)	No	No	X	X	X	O	X	X	X	O	Shall
	CC_DETECT_REPORT.CNF (See Note #6)	No	No	X	X	O	X	X	X	O	X	Shall
0x002C	CC_WHO_RU.REQ	Yes	No	X	M	M	X	X	M	M	X	Both
	CC_WHO_RU.CNF	No	Yes	M	X	X	M	M	X	X	M	Both
0x0030	CC_ASSOC.REQ	No	No	X	M	M	X	X	M	M	X	Both
	CC_ASSOC.CNF	No	No	M	X	X	M	M	X	X	M	Both
0x0034	CC_LEAVE.REQ	No	No	X	M	M	X	X	M	M	X	Both
	CC_LEAVE.CNF	No	No	M	X	X	M	M	X	X	M	Both
	CC_LEAVE.IND	No	No	M	X	X	M	M	X	X	M	Both
	CC_LEAVE.RSP	No	No	X	M	M	X	X	M	M	X	Both
0x0038	CC_SET_TEI_MAP.REQ	No	No	X	M	O	X	X	M	O	X	Both
	CC_SET_TEI_MAP.IND	No	No	M	X	X	M	M	X	X	M	Both
0x003C	CC_RELAY.REQ (See Note #7)	No	No	O	X	O	O	O	X	O	O	Both
	CC_RELAY.IND (See Note #7)	No	No	X	O	O	O	X	O	O	O	Both

0x0040	CC_BEACON_RELIABILITY.REQ	No	No	M	X	X	M	O	X	X	O	Shall
	CC_BEACON_RELIABILITY.CNF	No	No	X	M	M	X	X	O	O	X	Shall
0x0044	CC_ALLOC_MOVE.REQ	No	No	X	X	O	X	X	X	X	X	Shall
	CC_ALLOC_MOVE.CNF	No	No	X	X	X	O	X	X	X	X	Shall
0x0048	CC_ACCESS_NEW.REQ	No	No	X	X	O	X	X	X	X	X	Shall
	CC_ACCESS_NEW.CNF	No	No	X	X	X	O	X	X	X	X	Shall
	CC_ACCESS_NEW.IND	No	No	X	X	O	X	X	X	X	X	Shall
	CC_ACCESS_NEW.RSP	No	No	X	X	X	O	X	X	X	X	Shall
0x004C	CC_ACCESS_REL.REQ	No	No	X	X	O	X	X	X	X	X	Shall
	CC_ACCESS_REL.CNF	No	No	X	X	X	O	X	X	X	X	Shall
	CC_ACCESS_REL.IND	No	No	X	X	X	O	X	X	X	X	Shall
	CC_ACCESS_REL.RSP	No	No	X	X	O	X	X	X	X	X	Shall
0x0050	CC_DCPPC.IND (See Note #8)	No	No	X	M	O	X	X	O	O	X	Shall

0x006C	CC_ISP_PortsReSync.REQ (see Note #8)	No	No	M	X	X	O	O	X	X	O	Shall
0x0054	CC_HP1_DET.REQ	No	No	M	X	X	M	M	X	X	M	Shall
	CC_HP1_DET.CNF	No	No	X	M	M	X	X	M	M	X	Shall
0x0058	CC_BLE_UPDATE.IND	No	No	X	X	O	X	X	X	X	X	Shall
0x005C	CC_BCAST_REPEAT.IND	Yes	No					O	X	X	O	Shall
	CC_BCAST_REPEAT.RSP	No	Yes					X	O	O	X	Shall
0x0060	CC_MH_LINK_NEW.REQ (see Note# 11)	No	No					X	X	X	X	Shall
	CC_MH_LINK_NEW.CNF (see Note# 11)	No	No					X	X	X	X	Shall
0x0064	CC_ISP_DetectionReport.IND (see Note# 12)	No	No					X	M	M	X	Shall
0x0068	CC_ISP_StartReSync.REQ (see Note# 12)	No	No					M	X	X	M	Shall

0x006C 0x0084	CC_ISP_Finish ReSync REQ (see Note# 12)	No	No					X	M	M	X	Shall
0x0070	CC_ISP_ReSyncDetected.IND (see Note# 12)	No	No					X	M	M	X	Shall
0x0074	CC_ISP_ReSyncTransmit.REQ (see Note# 12)	No	No					M	X	X	M	Shall
0x0078	CC_POWERSAVE.REQ	No	No					X	M	O	X	Shall
	CC_POWERSAVE.CNF	No	No					M	X	X	O	Shall
0x007C	CC_POWERSAVE_EXIT.REQ	No	No					X	M	O	X	Shall
	CC_POWERSAVE_EXIT.CNF	No	No					M	X	X	O	Shall
0x0080	CC_POWERSAVE_LIST.REQ	No	No					X	M	O	X	Shall
	CC_POWERSAVE_LIST.CNF	No	No					M	X	X	M	Shall

0x2008 0x0084	CP_PROXY_WAKEUP_POWERSAVE.REQ (See Note #9)	No	No					O	O	O	O	Shall
	CC_STOP_POWERSAVE.CNF	No	No					O	O	O	O	Shall
0x0088 – 0x1FFC	Reserved for future use	-	-									
	Proxy Coordinator											
0x2000	CP_PROXY_APPOINT.REQ (See Note #9)	No	No	O	X	X	O	O	X	X	O	Shall
	CP_PROXY_APPOINT.CNF (See Note #9)	No	No	X	O	O	X	X	O	O	X	Shall
0x2004	PH_PROXY_APPOINT.IND (See Note #9)	No	No	X	X	O	O	X	X	O	O	Both

0x2008	CP_PROXY_WAKE.REQ (See Note #9)	No	No	X	X	O	O	X	X	O	O	Shall
0x200C – 0x3FFC	Reserved for future use	-	-									
	CCo – CCo											
0x4000	NN_INL.REQ	No	No	X	X	X	X	X	X	X	X	Never
	NN_INL.CNF	No	No	X	X	X	X	X	X	X	X	Never
0x4004	NN_NEW_NET.REQ	No	No	X	X	X	X	X	X	X	X	Never
	NN_NEW_NET.CNF	No	No	X	X	X	X	X	X	X	X	Never
	NN_NEW_NET.IND	No	No	X	X	X	X	X	X	X	X	Never
0x4008	NN_ADD_ALLOC.REQ	No	No	X	X	X	X	X	X	X	X	Never
	NN_ADD_ALLOC.CNF	No	No	X	X	X	X	X	X	X	X	Never
	NN_ADD_ALLOC.IND	No	No	X	X	X	X	X	X	X	X	Never
0x400C	NN_REL_ALLOC.REQ	No	No	X	X	X	X	X	X	X	X	Never
	NN_REL_ALLOC.CNF	No	No	X	X	X	X	X	X	X	X	Never
0x4010	NN_REL_NET.IND	No	No	X	X	X	X	X	X	X	X	Never
0x4014 – 0x5FFC	Reserved for future use	-	-									

	CM_BRG_INFORM.IND											
0x6020 0x6000	CM_UNASSOCIATED_STA.IND	No	Yes	X	X	M	M	M	M	M	M	Never
0x6004	CM_ENCRYPTED_PAYLOAD.IND	Yes	Yes	M	M	M	M	M	M	M	M	Both
	CM_ENCRYPTED_PAYLOAD.RSP	Yes	Yes	M	M	M	M	M	M	M	M	Both
0x6008	CM_SET_KEY.REQ	Yes	Yes	M	M	M	M	M	M	M	M	Shall
	CM_SET_KEY.CNF	Yes	Yes	M	M	M	M	M	M	M	M	Shall
0x600C	CM_GET_KEY.REQ	Yes	Yes	M	M	M	M	M	M	M	M	Never
	CM_GET_KEY.CNF	Yes	Yes	M	M	M	M	M	M	M	M	Never
0x6010	CM_SC_JOIN.REQ	No	No	M	M	M	M	M	M	M	M	Never
	CM_SC_JOIN.CNF	No	No	M	M	M	M	M	M	M	M	Never
0x6014	CM_CHAN_EST.IND	No	No	M	M	M	M	M	X	M	X	Both
0x6018	CM_TM_UPDATE.IND	No	No	O	M	O	M	X	X	X	X	Both
0x601C	CM_AMP_MAP.REQ	Yes	No	O	X	X	M	O	X	X	O	Shall
	CM_AMP_MAP.CNF	No	Yes	X	O	M	X	X	O	O	X	Shall

0x6030 0x6020	CM_BRG_INFO.REQ (See Note #10)	Yes	No	O	M	O	M	O	M	O	M	Shall
	CM_BRG_INFO.CNF (See Note #10)	No	Yes	M	M	M	M	M	M	M	M	Shall
0x6024	CM_CONN_NEW.REQ (See Note #2)	No	No	M	M	M	M	X	X	X	X	Shall
	CM_CONN_NEW.CNF (See Note #2)	No	No	M	M	M	M	X	X	X	X	Shall
0x6028	CM_CONN_REL.IND (See Note #2)	No	No	M	M	M	M	X	X	X	X	Shall
	CM_CONN_REL.RSP (See Note #2)	No	No	M	M	M	M	X	X	X	X	Shall
0x602C	CM_CONN_MOD.REQ (See Note #2)	No	No	M	M	M	M	X	X	X	X	Shall
	CM_CONN_MOD.CNF (See Note #2)	No	No	M	M	M	M	X	X	X	X	Shall

0x6030	CM_CONN_INFO.REQ	Yes	No	M	M	M	M	X	X	X	X	Shall
	CM_CONN_INFO.CNF	No	Yes	M	M	M	M	X	X	X	X	Shall
0x6034	CM_STA_CAP.REQ	Yes	No	M	M	M	M	M	M	M	M	Both
	CM_STA_CAP.CNF	No	Yes	M	M	M	M	M	M	M	M	Both
0x6038	CM_NW_INFO.REQ	Yes	No	M	M	M	M	M	M	M	M	Shall
	CM_NW_INFO.CNF	No	Yes	M	M	M	M	M	M	M	M	Shall
0x603C	CM_GET_BEACON.REQ	Yes	No	M	M	M	M	O	O	O	O	Shall
	CM_GET_BEACON.CNF	No	Yes	M	M	M	M	O	O	O	O	Shall
0x6040	CM_HFID.REQ	Yes	No	M	M	M	M	M	M	M	M	Both
	CM_HFID.CNF	No	Yes	M	M	M	M	M	M	M	M	Both
0x6044	CM_MME_ERROR.IND	No	Yes	M	M	M	M	M	M	M	M	Both
0x6048	CM_NW_STATS.REQ	Yes	No	M	M	M	M	M	M	M	M	Shall
	CM_NW_STATS.CNF	No	Yes	M	M	M	M	M	M	M	M	Shall
0x604C	CM_LINK_STATS.REQ	Yes	No	M	M	M	M	M	M	M	M	Shall
	CM_LINK_STATS.CNF	No	Yes	M	M	M	M	M	M	M	M	Shall
0x6050	CM_ROUTE_INFO.REQ	Yes	No					O	O	O	O	Shall

	CM_ROUTE_INFO.CNF	No	Yes					O	O	O	O	Shall
	CM_ROUTE_INFO.IND	No	Yes					O	O	O	O	Shall
0x6054	CM_UNREACHABLE.IND	No	Yes					O	O	O	O	Shall
0x6058	CM_MH_CONN_NEW.REQ (See Note# 11)	No	No	-	-			X	X			Shall
	CM_MH_CONN_NEW.CNF (See Note# 11)	No	No	-	-			X	X			Shall
0x605C	CM_EXTENDED_TONEMASK.REQ (See Note# 11)	No	No	-	-			X	X			Shall
	CM_EXTENDED_TONEMASK.CNF (See Note# 11)	No	No	-	-			X	X			Shall
0x6060	CM_STA_IDENTIFY.REQ	Yes	No	-	-			M	M	M	M	Shall
	CM_STA_IDENTIFY.CNF	No	Yes	-	-			M	M	M	M	Shall

	CM_STA_IDENTIFY.ND	No	Yes	-	-			M	M	M	M	Shall
	CM_STA_IDENTIFY.RSP	Yes	No	-	-			M	M	M	M	Shall
0x6064	CM_SLAC_PARM_REQ	Yes	Yes					O	O	O	O	Never
0x6068	CM_SLAC_PARM.CNF	Yes	Yes					O	O	O	O	Never
0x606C	CM_START_ATTEN_CHAR.IND	Yes	Yes					O	O	O	O	Never
0x6070	CM_ATTN_CHAR.IND	Yes	Yes					O	O	O	O	Never
	CM_ATTN_CHAR.RSP	Yes	Yes					O	O	O	O	Never
0x6074	CM_PKCS_CERT.REQ	Yes	Yes					O	O	O	O	Never
	CM_PKCS_CERT.CNF	Yes	Yes					O	O	O	O	Never
	CM_PKCS_CERT.IND	Yes	Yes					O	O	O	O	Never
	CM_PKCS_CERT.RSP	Yes	Yes					O	O	O	O	Never
0x6078	CM_MNBC_SOUND.IND	Yes	Yes					O	O	O	O	Never
0x607C	CM_VALIDATE.REQ	Yes	Yes					O	O	O	O	Never
	CM_VALIDATE.CNF	Yes	Yes					O	O	O	O	Never

0x6080	CM_SLAC_MATCH.REQ	Yes	Yes					O	O	O	O	Never
	CM_SLAC_MATCH.CNF	Yes	Yes					O	O	O	O	Never
0x6084	CM_SLAC_USER_DATA.REQ	Yes	Yes					O	O	O	O	Both
	CM_SLAC_USER_DATA.CNF	Yes	Yes					O	O	O	O	Both
0x6088 – 7FFC	Reserved for future use	-	-									
	Manufacturer Specific											
0x8000 – 0x9FFC	Manufacturer Specific Messages	Only	Only									-
	Vendor Specific											
0xA000 – 0xBFFC	Vendor-Specific Messages	Yes	Yes									Both

Notes:

- CC_CCO_APPOINT.REQ is generated by HLE. It is mandatory for stations to be able to receive this message from H1 interface and pass it to the CCo. Similarly, it is mandatory for all stations to be able to receive CC_CCO_APPOINT.CNF from any station in the AVLN and pass it to the HLE.
- Refer to Section 5.2.3 for details.
- Optional when the station does not support Soft Handover (refer to Section 7.5). Mandatory if it does.
- Support for Hard Handover is Mandatory (refer to Section 7.5).
- Optional if the station does not support Squeeze/De-Squeeze procedure (refer to Section 5.2.3.8.1). Mandatory if it does.
- Optional if the station does not support Detect-and-Report procedure (refer to Section

MACAddr	7	0 or 6	5.2.5). Mandatory if it does. • Optional if the station does not support the Proxy Networking procedure (refer to Section 7.7). Mandatory if it does. • Optional if the station does not support simultaneous participation in more than one network (refer to Section 5.5.4.1). • Optional if the station does not support Proxy Networking (refer to Section 7.7). Mandatory if it does. • Any STA can request bridging information by using CM_BRG_INFO.REQ. It is mandatory for all stations to respond with CM_BRG_INFO.CNF. It is mandatory that all bridges periodically generate CM_BRG_INFO.CNF (refer to Section 5.3). • These MMEs are defined for IEEE 1901. However, they are not required to be supported by HomePlug GREEN PHY devices. • These MMEs are defined for IEEE 1901. These are required to be supported by HomePlug GREEN PHY devices. See section 14.1.2.	MAC address of the

Station - Central Coordination (CCo)

CC_CCO_APPOINT.REQ

The CC_CCO_APPOINT.REQ message is used to appoint a STA in the AVLN as a CCo and also to un-appoint an existing CCo from being a user-appointed CCo.

Table 116: CC_CCO_APPOINT.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
ReqType	0	1	Request Type 0x00 = request to appoint a STA with the indicated MAC Address as a user-appointed CCo 0x01 = request to un-appoint the existing CCo from being a user-appointed CCo. 0x02 = request to un-appoint the existing CCo from being a user-appointed CCo and to transfer CCo functionality to a new user-appointed CCo. 0x03 – 0xFF = reserved

Result	0	1	Result codes for ReqType = 0x00 (refer to Table 116) 0x00 = success, the user-appointed STA has accepted the handover request. 0x01 = failure, the user-appointed STA has rejected the handover request. 0x02 = failure, unknown user-appointed STA 0x03 = failure, the current CCo is already a user-appointed CCo. CCo functionality cannot be handed over until the current CCo is un-appointed as a user-appointed CCo. Results codes for ReqType = 0x01 (refer to Table 116) 0x04 = success, the existing CCo is un-appointed as a user
MACAddr	–-	0 or 6	MAC address of the STA that is appointed as a user-appointed CCo. This field is only present when ReqType is set to 0x00 or 0x02.

CC_CCO_APPOINT.CNF

The CC_CCO_APPOINT.CNF message is sent in response to a received CC_CCO_APPOINT.REQ message.

Table 117: CC_CCO_APPOINT.CNF Message

Field	Octet Number	Field Size (Octets)	Definition

Result	0	1	Results codes for ReqType = 0x00 (refer to Table 116) 0x00 = success, the user-appointed STA has accepted the handover request. 0x01 = failure, the user-appointed STA has rejected the handover request. 0x02 = failure, unknown user-appointed STA 0x03 = failure, the current CCo is already a user-appointed CCo. CCo functionality cannot be handed over until the current CCo is un-appointed as a user-appointed CCo. Results codes for ReqType = 0x01 (refer to Table 116) 0x04 = success, the existing CCo is un-appointed as a user appointed CCo 0X05 = success, the existing CCo is not a user-appointed CCo 0x06 = failure, other reasons Results codes for ReqType = 0x02 (refer to Table 116) 0x07 = success, the existing CCo is un-appointed. The new STA is appointed as a user appointed CCo

CC_BACKUP_APPOINT.REQ

The CC_BACKUP_APPOINT.REQ message is sent by the CCo to a STA to direct the STA to become a Backup CCo, or sent to an existing Backup CCo to release its duty as a Backup CCo.

Table 118: CC_BACKUP_APPOINT.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
Num	0	1	Number of GlobalLinkInfo fields to follow (=N).
Appoint/Release	0	1	0x00 = appoint 0x01 = release 0x02 - 0xFF = reserved
GlobalLinkInfo present	0	1	0x00 = no GlobalLinkInfo field follows 0x01 = one GlobalLinkInfo field follows 0x02 - 0xFF = reserved

CC_BACKUP_APPOINT.CNF

The CC_BACKUP_APPOINT.CNF message is sent by a STA to the CCo in response to a received CC_BACKUP_APPOINT.REQ message.

Table 119: CC_BACKUP_APPOINT.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
Result	0	1	0x00 = accepted 0x01 = failed, feature not supported 0x02 = failed, other reason 0x03 - 0xFF = reserved

CC_LINK_INFO.REQ

The CC_LINK_INFO.REQ message is sent by a STA to the CCo to request the CSPEC and BLE information of all active Global Links in the AVLN. The message field for this MME is NULL.

CC_LINK_INFO.CNF

The CC_LINK_INFO.CNF message is sent by the CCo in response to a received CC_LINK_INFO.REQ message. The message contains the CSPEC with CM-to-CCo QoS and MAC parameters and BLE information of all active Global Link(s) in the AVLN.

Table 1110: CC_LINK_INFO.CNF Message

Field	Octet Number	Field Size (Octets)	Definition

Forward Link BLE Num	- 0	Var 1	Number of Forward GlobalLinkInfo fields to follow (=N). 0x00 = no GlobalLinkInfo present
			0x01 = one GlobalLinkInfo field 0x02 = two GlobalLinkInfo fields, and so on
GlobalLinkInfo[1]	-	Var	Link information of the first Global Link
…	…	…	…
GlobalLinkInfo[N]	-	Var	Link information of the last Global Link

Table 1111: Format of LinkInfo[ ] Field

Field	Octet Number	Field Size (Octets)	Definition
CID	0 - 1	2	Connection Identifier of the Link (refer to Section 5.2.1.4.2)
STEI	2	1	TEI of the source STA.
DTEI	3	1	TEI of the sink STA.
LID-F	4	1	Link ID of the Forward Link. A value of 0x00 is used to indicate that this field is invalid.
LID-R	5	1	Link ID of the Reverse Link. A value of 0x00 is used to indicate that this field is invalid.
CSPEC	-	Var	CM-to-CCo Connection Specification in both forward (if any) and reverse (if any) links.

Forward Link BLE	-	Var	BLE of the Forward (refer to Section 11.2.16.5) This field is only present when the LID-F exists.
Reverse Link BLE	-	Var	BLE of the Reverse Link (refer to Section 11.2.16.5) This field is only present when the LID-R exists.

CC_LINK_INFO.IND

The CC_LINK_INFO.IND message is sent by a CCo to either a new CCo (during soft handover, refer to Section 7.5) or a Backup CCo (as part of CCo failure recovery, refer to Section 7.5) to provide the CSPEC with CM-to-CCo QOS and MAC parameters, and BLE information of the Global Link(s) that are active within the AVLN.

The format of this message is the same as the CC_LINK_INFO.CNF message in Section 11.2.6.

CC_LINK_INFO.RSP

The **CC_LINK_INFO.RSP** message is sent by the new CCo or Backup CCo to the current CCo to confirm the reception of the **CC_LINK_INFO.IND** message.

The message field for this message is NULL.

CC_HANDOVER.REQ

The CC_HANDOVER.REQ message is sent by the current CCo to another STA in the network to request the STA to become the new CCo.

Table 1112: CC_HANDOVER.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
Soft/Hard	0	1	0x00 = soft handover 0x01 = hard handover 0x02 – 0xFF = reserved
Reason	1	1	0x00 = user-appointed 0x01 = CCo-selection process 0x02 = current CCo is leaving the network. 0x03 – 0xFF = reserved

CC_HANDOVER.CNF

The CC_HANDOVER.CNF message is sent in response to a received CC_HANDOVER.REQ message.

Table 1113: CC_HANDOVER.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
Result	0	1	0x00 = STA accepts the request to become the new CCo. 0x01 = STA rejects the Soft handover request to become the new CCo. 0x02 = STA rejects any handover request to become the new CCo. 0x03 - 0xFF = reserved.

CC_HANDOVER_INFO.IND

The CC_HANDOVER_INFO.IND message is sent by the current CCo to the new CCo during the handover process. This message is also sent by the current CCo to the Backup CCo to enable recovery from CCo failure.

Table 1114: CC_HANDOVER_INFO.IND Message			Status of STA
Field	Octet Number	Field Size (Octets)	Definition
Status	7	1	Reason Code indicating the reason for sending
RSC	0	1	CC_HANDOVER_INFO.IND Message 0x00 = handover in progress. 0x01 = update of network information to Backup CCo to enable CCo failure recovery. 0x02-0xFF = reserved
BackupCCo	1	1	TEI of the Backup CCo (no Backup CCo if set to 0x00)
Num	2	1	Number of STAInfo[ ] fields to follow (=N). 0x00 = no STAInfo present 0x01 = one STAInfo field 0x02 = two STAInfo fields, and so on
STA_Info[1]	3 - 11	9	Information of the first STA.
…			
STA_Info[N]	-	9	Information of the last STA.

Table 1115: Format of STA_Info[ ] Field

Field	Octet Number	Field Size (Octets)	Definition
TEI	0	1	TEI of the STA.
MACAddr	1 - 6	6	MAC address of the STA.

Status	7	1	Status of STA 0x00 = associated, but not authenticated 0x01 = authenticated 0x02 = 0xFF = reserved
PTEI	8	1	TEI of the PCo responsible for the STA (set to 0x00 to indicate there is no PCo for the STA)

CC_HANDOVER_INFO.RSP

The CC_HANDOVER_INFO.RSP message is sent by the new CCo or Backup CCo to the current CCo to confirm the reception of the CC_HANDOVER_INFO.IND messages. The message field for this MME is Null.

CC_DISCOVER_LIST.REQ
The CC_DISCOVER_LIST.REQ message is sent by a STA to request the Discovered STA List and Discovered Network List of another STA.
The message field for this message is Null.
Although this message is typically sent by the CCo to a STA in the AVLN, any STA in the AVLN should be able to send this message to another STA in the AVLN and obtain the corresponding CC_DISCOVER_LIST.CNF.
CC_DISCOVER_LIST.CNF
The CC_DISCOVER_LIST.CNF message is sent by a STA in response to a received CC_DISCOVER_LIST.REQ message to report its Discovered STA List and Discovered Network List.
Table 1116: CC_DISCOVER_LIST.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
NumStation	0	1	Number of STAs discovered (=M). 0x00 = none 0x01 = one 0x02 = two, and so on
StationInfo[1]	-	12	Information about the first STA discovered (see Table 1117).
…			
StationInfo[M]	-	12	Information about the last STA discovered (see Table 1117).
NumNetwork	-	1	Number of networks discovered (=N).
NetworkInfo[1]	-	13	Information about the first network discovered (see Table 1118)
	…	…	
NetworkInfo[N]	-	13	Information about the last network discovered (see Table 1118).

Table 1117: Format of StationInfo [ ]				
Field	Octet Number	Bit Number	Field Size (Octets)	Definition
MACAddr	0 - 5		6	MAC address of the discovered STA
TEI	6		1	TEI of the discovered STA
SNID/Access SameNetwork	8 7		1 1	Short Network Identifier of the network of the discovered STA. The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to 0x00 = the discovered STA is associated with a different network. 0x01 = the discovered STA is associated with the same network. 0x02 – 0xFF = reserved

Proxy Networking Capability		3	1 bit	This field contains the proxy networking capability of the STA. The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.
SNID/Access	8		1	
Reserved	9	0	1 bit	Reserved
CCo Capability		1-2	2 bits	This field contains the CCo capability. The interpretation of these bits is the same as in Section 4.4.3.15.4.6.2.

Proxy Networking Capability		3	1 bit	This field contains the PCo capability. The interpretation of this bit is the same as in Section 4.4.3.15.4.6.3.
Backup CCo Capability		4	1 bit	This field contains the Backup CCo capability. The interpretation of this bit is the same as in Section 4.4.3.15.4.6.4.
CCo Status		5	1 bit	This field contains the CCo Status. The interpretation of this bit is the same as in Section 4.4.3.15.4.6.5.
PCo Status		6	1 bit	This field contains the PCo Status. The interpretation of this bit is the same as in Section 4.4.3.15.4.6.6
Backup CCo Status		7	1 bit	This field contains the Backup CCo Status. The interpretation of this bit is the same as in Section 4.4.3.15.4.6.7

Signal Level	10		1	0x00 = information not available 0x01 = signal level is > -10 dB, but ≤ 0 dB (relative to full transmit power, -50 dBm/Hz) 0x02 = signal level is > -15 dB, but ≤ -10 dB 0x03 = signal level is > -20 dB, but ≤ -15 dB … 0x0E = signal level is > -75 dB, but ≤ -70 dB 0x0F = signal level is ≤ -75 dB 0x10 – 0xFF = reserved
Average BLE	11		1	Average BLE. The Format is defined in Section 4.4.1.5.2.10. Average BLE may be estimated based on Discover Beacon reception. This field shall be set to zero if not provided. Providing a non-zero value is optional.

Table 1118: Format of NetworkInfo[ ]			Number of Beacon Slots
Field	Octet Number	Field Size (Octets)	Definition
NumSlots	9	1	0x00 – 0x1F – Network Identifier. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.
NID	0 - 6	7	
SNID/Access	7	1	Short Network Identifier of the network of the discovered STA. The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.
HM	8	1	The two LSBs of this field contain the Hybrid Mode of the AVLN. The interpretation of these bits is the same as in Section 4.4.3.2.

NumSlots	9	1	Number of Beacon Slots 0x00 = one Beacon Slot, and so on 0x08 - 0xFF = reserved
CoordinatingStatus	10	1	Coordinating Status of the CCo. 0x00 = unknown 0x01 = Non-Coordinating Network 0x02 = Coordinating, Group status unknown 0x03 = Coordinating Network in the same Group as this CCo 0x04 = Coordinating Network not in the same Group as this CCo 0x05 – 0xFF = reserved
Offset	11 - 12	2	Offset between the Beacon Region of the discovered network and the Beacon Region of the STA's own network. Units are AllocationTimeUnit. 0x0000 = zero or in the same Group 0x0001 = one AllocationTimeUnit, and so on

CC_DISCOVER_LIST.IND

The CC_DISCOVER_LIST.IND message shall be sent by a STA to the CCo in an unsolicited manner whenever the STA discovers a new network. The format of the MMENTRY for this field is the same as the MMENTRY for CC_DISCOVER_LIST.CNF.

CC_LINK_NEW.REQ

The CC_LINK_NEW.REQ message is sent by the initiating STA to the CCo to request connection setup in the CFP.

Table 1119: CC_LINK_NEW.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
Init.MAC Addr	0 - 5	6	MAC address of the STA initiating the Connection
Term. MAC Addr	6 - 11	6	MAC address of the terminating STA(s)
CID	12 - 13	2	Connection Identifier
CSPEC	-	Var	Connection Specification
Forward Link Bit Loading Estimates	-	1	Number of Intervals (N)
	-	2	Interval #1 End Time
	-	1	Interval #1 BLE
	…		
	-	2	Interval #N End Time
	-	1	Interval #N BLE
Reverse Link Bit Loading Estimates	-	1	Number of Intervals (K)
	-	2	Interval #1 End Time
	-	1	Interval #1 BLE
	…		
	-	2	Interval #K End Time
	-	1	Interval #K BLE

Note: The Connection Identifier (CID) serves as a unique identifier for the request.

Initiating MAC Address

Initiating MAC Address indicate the 48-bit Ethernet address of the power line station that is initiating the Connection.

Terminating MAC Address

Terminating MAC Address indicate the 48-bit Ethernet address of the power line station(s) that are at the terminating side of the Connection.

Connection Identifier

The CID serves as a unique identifier for the request. Interpretation of this field is the same as in Section 5.2.1.4.2.

Connection Specification

The interpretation of this field is the same as in Section 7.8.1.

Forward Link and Reverse Link Bit Loading Estimates

These fields indicate the Bit loading estimates of the corresponding Links based on channel adaptation.

Forward Link Bit Loading Estimates shall only be present when any of the following conditions is satisfied:
The Connection has a Global Forward Link , or
The Connection has a Local Forward Link and a Global Reverse Link. Further, the traffic in the Local Forward Link is intended to be transmitted as part of Reverse SOF (i.e., Bidirectional Bursts) during CFP of the Global Reverse Link.
Similarly, Reverse Link Bit Loading Estimates shall only be present when any of the following conditions is satisfied:
The Connection has a Global Reverse Link, or
The Connection has a Local Reverse Link and a Global Forward Link. Further, the traffic in the Local Reverse Link is intended to be transmitted as part of Reverse SOF (i.e., Bidirectional Bursts) during CFP of the Global Forward Link.
Number of Intervals
Number of Intervals indicates the number of intervals in which Bit Loading Estimates are presented. A value of 0x00 indicates that no Bit Loading Estimates are available.
Interval End Time # 1–N
Interval End Time indicates the end time of the corresponding Bit Loading Estimate interval in multiples of AllocationTimeUnit. End Times are measured with respect to the Beacon Period Start Time. Thus, a value of 0x0000 indicates that the end time is the same as Beacon Period start time. When BLE for multiple intervals is present, intervals shall be present in ascending order of time. Thus, the first interval shall be the closest to the Beacon Period Start Time and so on. Furthermore, intervals shall be non-overlapping and shall cover the entire Beacon Period. Therefore, the end time of the last interval shall be greater than or equal to the length of the Beacon Period.
Bit Loading Estimate # 1–N
Bit Loading Estimate indicates the PHY data rate that can be supported in the corresponding Interval. The interpretation of this field is the same as in Section 4.4.1.5.2.10.

CC_LINK_NEW.CNF

The CCo sends the CC_LINK_NEW.CNF message to the initiating STA and terminating STA(s) of a Connection to confirm the completion of establishment of the Global Links associated with the Connection.
Table 1120: CC_LINK_NEW.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
CID	0 - 1	2	Connection ID (refer to Section 5.2.1.4.2)
GLID-F	2	1	Newly assigned GLID for the Forward Link (refer to Section 5.2.1) A value of 0x00 is used to indicate that this field is invalid.

GLID-R	3	1	Proposed GSPEC GLID for the Reverse link A value of 0x00 is used to indicate that this field is not present.
Proposed CSPEC	-	Var	Proposed CSPEC including the CSPEC version number that the CCo is capable of supporting. This field is only present when Result is set to 0x01. When this field is present 0x00 = valid Proposed CSPEC – included this CSPEC or insufficient bandwidth 0x02 = failure – maximum number of links allocated per station already established 0x03 = failure – lack of CCo resources, try again later 0x04 = failure – link already established using the connection ID 0x05 = failure due to other reason 0x06 - 0xFF = reserved
Result	4	1	Indicates the Result of the Connection Setup Request 0x00 = success 0x01 = failure – unsupported CSPEC

Proposed CSPEC	-	Var	Proposed CSPEC indicating the CSPEC that the CCo is currently capable of supporting. This field is only present when Result is set to 0x01. When this field is present and a valid Proposed CSPEC is not included, this field shall be 2 octets long, with a value of 0x0000 (i.e., CSPEC_LEN = 0x0000). When a valid Proposed CSPEC is included, the interpretation of this field is the same as in Section 7.8.1.

Result

Result indicates the outcome of the request, according to the codes in Table 1120. If the CCo does not support some of the optional QoS parameters sent in the request's CSPEC, or if there is insufficient bandwidth available to admit the connection, then result 0x01 is used. In this case, the CCo has the option of returning a proposed CSPEC that indicates supported options and available bandwidth.

Proposed CSPEC

The CCo has the option of sending a proposed CSPEC when Result = 0x01. The Proposed CSPEC should indicate a CSPEC that, if included in a new request, the CCo can currently grant. If no Proposed CSPEC is included when Result = 0x01, then this field shall be 2 octets long, with the value 0x0000.

CC_LINK_MOD.REQ

The CC_LINK_MOD.REQ message is sent by either the initiating STA or the terminating station of a Connection to the CCo to request modification of Global Link(s).

Table 1121: CC_LINK_MOD.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
CID	0 - 1	2	Connection ID (refer to Section 5.2.1.4.2)

Modified CSPEC	2	Var	Modifies the result of containing the (complete) new CSPEC that is requested for the Connection. The interpretation of this field is the same as in Section 7.8.1.
Forward Link Bit Loading Estimates	-	Var	Bit Loading Estimates for the Forward Link The format of this field is the same as that of the corresponding field in Section 11.2.15. This field is only present when the Forward for the Connection (if any) is a Global Link.
Reverse Link Bit Loading Estimates	-	Var	Bit Loading Estimates for the Reverse Link The format of this field is the same as that of the corresponding field in Section 11.2.15. This field is only present when the Reverse Link for the Connection (if any) is a Global Link.

CC_LINK_MOD.CNF

The CC_LINK_MOD.CNF message is sent by the CCo to the STAs involved in a Connection to notify them that the reconfiguration of the CFP Link(s) has been completed successfully or failed.

Table 1122: CC_LINK_MOD.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
CID	0 - 1	2	Connection ID (refer to Section 5.2.1.4.2)

Modified CSPEC	2	Var	Modifies the CSPEC contained in the (modify) request. 0x00 = the CSPEC that is requested for the Proposed CSPEC field is present 0x02 - 0xFF = reserved
Proposed CSPEC	-	Var	Proposed CSPEC indicating the CSPEC that the CCo is currently capable of supporting. This field is only present when Result is set to 0x01. When this field is present and a valid Proposed CSPEC is not included, this field shall be 2 octets long, with a value of 0x0000 (i.e., CSPEC_LEN = 0x0000). When a valid Proposed CSPEC is included, the interpretation of this field is the same as in Section 7.8.1.

CC_LINK_SQZ.REQ

Table 1123: CC_LINK_SQZ.REQ Message

Field	Octet Number	Bit Number	Definition
CID	0 - 1	2	Connection ID (refer to Section 5.2.1.4.2)

Modified CSPEC	-	Var	Modified CSPEC indicating the current CSPEC supported for the connection. The interpretation of this field is the same as in Section 7.8.1.
Proposed CSPEC	-	Var	Proposed CSPEC (complete CSPEC) that is requested by the originator. This field is present and a valid Proposed CSPEC is not included, this field shall be 2 octets long, with a value of 0x0000 (i.e. CSPEC_LEN = 0x0000). When a valid Proposed CSPEC is included, Proposed CSPEC field is present

CC_LINK_SQZ.CNF

Table 1124: CC_LINK_SQZ.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
CID	0-1	2	Connection ID (refer to Section 5.2.1.4.2)
Result	2	1	Indicates the result of the Connection modify request. 0x00 = success 0x01 = failed, 0x02 - 0xFF = reserved

Proposed CSPEC	-	Var	Proposed CSPEC indicating the CSPEC that the CM is currently capable of supporting. This field is only present when Result is set to 0x01. When this field is present and a valid Proposed CSPEC is not included, this field shall be 2 octets long, with a value of 0x0000 (i.e., CSPEC_LEN = 0x0000). When a valid Proposed CSPEC is included, the interpretation of this field is the same as in Section 7.8.1.

CC_LINK_REL.REQ

The CC_LINK_REL.REQ message is sent by a STA to the CCo to request release of the Global Links associated with a Connection.

Table 1125: CC_LINK_REL.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
CID	0 - 1	2	Connection Identifier (refer to Section 5.2.1.4.2)
TEI	2	1	TEI of STA requesting release of Link. This may be the Station that has initiated the Connection, Station(s) that are at the terminating end of a Connection or another station within the AVLN (refer to Section 5.2.3.4.1).

Reason Code	3	1	Reason for Connection Termination 0x00 = normal release 0x01 = CSPEC violation, Violated CSPEC field is present 0x02 – 0xFF = reserved
Violated CSPEC	-	Var	Violated CSPEC indicating the CSPEC that are violated. This field is only present when Reason Code is set to 0x01. When this field is present and a valid Violated CSPEC is not included, this field shall be 2 octets long, with a value of 0x0000 (i.e., CSPEC_LEN = 0x0000). When a valid Violated CSPEC is included, the interpretation of this field is the same as in Section 7.8.1.

CC_LINK_REL.IND

The CC_LINK_REL.IND message is sent by the CCo to the initiating STA and terminal station(s) of a Connection to indicate release of the Global Links associated with a Connection. The message is generated in response to the corresponding CC_LINK_REL.REQ. The CCo may also generate this message in an unsolicited manner when an existing Connection is terminated due to insufficient bandwidth, violation of the CSPEC, or at the request of another station within the AVLN.

Note: The ability to initiate a connection teardown by a station that is not part of the Connection (i.e., neither the initiating station nor the terminating station(s)) is intended to provide flexibility for higher layer protocols like UPnP in managing the AVLN.

Table 1126: CC_LINK_REL.IND Message			Proposed CSPEC
Field	Octet Number	Field Size (Octets)	Indicating the CSPEC that the CC is currently capable of supporting.
CID	0 - 1	2	Connection Identifier (refer to Section 5.2.1.4.2).
Releasing Station MAC Address	2 - 7	6	This field contains the MAC Addresses of the station that initiated the release of the Connection. This field is only present when Reason Code is set to 0x01. When this field is present and a valid Proposed CSPEC is not included, this field shall be 2 octets long, with a value of
Proposed CSPEC	-	Var	Reason for Connection Termination
Reason Code	8	1	0x00 = normal release 0x01 = CSPEC violation, Violated CSPEC field is present 0x02 = insufficient bandwidth, Proposed CSPEC field is present
			0x03 = requested by another station within the AVLN that is not part of the Connection 0x04 – 0xFF = reserved

Violated CSPEC Proposed CSPEC	- -	Var Var	Violated CSPEC Proposed CSPEC indicating the CSPEC of the CSPEC that is violated This field is only present when Reason Code is set to 0x03 When this field is present and valid Violated CSPEC is not included, this field shall be 2 octets long, with a value of 0x0000 (i.e., CSPEC_LEN = 0x0000). When a valid Proposed CSPEC is included, the interpretation of this field is the same as in Section 7.8.1.

Violated CSPEC	-	Var	Violated CSPEC indicating the fields of the CSPEC that are violated. This field is only present when Reason Code is set to 0x02. When this field is present and a valid Violated CSPEC is not included, this field shall be 2 octets long, with a value of 0x0000 (i.e., CSPEC_LEN = 0x0000). When a valid Violated CSPEC is included, the interpretation of this field is the same as in Section 7.8.1.

CC_DETECT_REPORT.REQ

The CC_DETECT_REPORT.REQ message is sent by the CCo to request a STA to perform the detect-and-report procedure (refer to Section 5.2.5). The time interval(s) during which the STA shall listen for and detect ongoing transmissions are identified by one or more GLID fields in the message, together with the schedules in the Beacon. The amount of time in which the STA shall detect for ongoing transmissions is specified by the Duration field, in units of Beacon Periods.

Table 1127: CC_DETECT_REPORT.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
Duration	0	1	Amount of time to detect for ongoing transmissions, in units of number of Beacon Periods. 0x00 = zero Beacon Periods, 0x01 = one Beacon Period, and so on
NumGLID	1	1	The number of GLID fields in this message (=N). The maximum value for this field is 8. 0x00 = none 0x01 = one, and so on
GLID[1]	2	1	The first GLID to perform the detect-and-report procedure.
...	…	…	...
GLID[N]	N+1	1	The last GLID to perform the detect-and-report procedure.

CC_DETECT_REPORT.CNF

The CC_DETECT_REPORT.CNF message is sent by a STA to report to the CCo the results of the detect-and-report procedure. This message shall be sent by the STA that has received a CC_DETECT_REPORT.REQ message after the STA has finished detecting for ongoing transmissions for the specified amount of time. The message contains the number of GLIDs where detection was performed and the type(s) of Frame Controls detected in the time intervals specified by the GLIDs.

If, for a particular GLID, the detection results are different in different Beacon Periods, the types of all Frame Controls that are detected over the entire detection duration should be reported.

Table 1128: CC_DETECT_REPORT.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
NumGLID	0	1	Number of GLIDInfo() in this message (=N). 0x00 = none 0x01 = one, and so on

GLIDInfo[1]	1 - 6	6	Information about the first GLID (see Table 1129)
...	…	…	
GLIDInfo[N]	-	6	Information about the last GLID (see Table 1129)

Table 1129: Format of GLIDInfo( )

Field	Octet Number	Field Size (Octets)	Definition
GLID	0	1	GLID corresponding to this GLIDInfo[ ].
CFDetected	1	1	0x00 = (HomePlug AV or Hybrid) Contention-free Frame Controls are not detected. 0x01 = (HomePlug AV or Hybrid) Contention-free Frame Controls are detected. 0x02 – 0xFF = reserved
CSMADetected	2	1	0x00 = (HomePlug AV or Hybrid) Contention-based Frame Controls are not detected. 0x01 = (HomePlug AV or Hybrid) Contention-based Frame Controls are detected. 0x02 – 0xFF = reserved
HP1Detected	3	1	0x00 = HomePlug 1.0.1 (not including HomePlug Hybrid) Frame Controls are not detected. 0x01 = HomePlug 1.0.1 (not including HomePlug Hybrid) Frame Controls are detected. 0x02 – 0xFF = reserved

HP1Detected	3	1	0x00 = HomePlug 1.0.1 Frame Controls are not detected. 0x01 = HomePlug 1.0.1 (not including HomePlug Hybrid) Frame Controls are detected. 0x02 – 0xFF = reserved
OthersDetected	4	1	0x00 = other unknown types of transmissions are not detected. 0x01 = other unknown types of transmissions are detected. 0x02 – 0xFF = reserved
Signal Level	5	1	0x00 = information not available 0x01 = signal level is > -10 dB, but ≤ 0 dB (relative to full transmit power, -50 dBm/Hz) 0x02 = signal level is > -15 dB, but ≤ -10 dB 0x03 = signal level is > -20 dB, but ≤ -15 dB … 0x0E = signal level is > -75 dB, but ≤ -70 dB 0x0F = signal level is ≤ -75 dB 0x10 – 0xFF = reserved

HFID	13 - 76	64	A variable field that contains the Human Friendly ID (refer to Section 4.4.3.12.1).
Average BLE	6	1	Average BLE of The Network identified by HFID. Average BLE may be estimated based on Discover Beacon reception. This field shall be set to zero if not provided. Providing a non-zero value is optional.

CC_WHO_RU.REQ

This MME is used to request the identity of the AVLN from the CCo.

Table 1130: CC_WHO_RU.REQ Message

Field	Octet Number	Field Size	Definition
NID	0 - 6	7	NID of network being queried. This is necessary to avoid confusion if the STA can hear two CCos with the same TEI. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.

CC_WHO_RU.CNF

This MME provides the identity of the AVLN and the MAC address of the CCo.

Table 1131: CC_WHO_RU.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
NID	0 - 6	7	NID of network being queried. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The 2 MSBs shall be set to 0b00.
CMAC	7 - 12	6	CCo's MAC Address

HFID	13 - 76	64	ASCII value of Human Friendly ID (HFID) of AVLN (64 chars, max)

CC_ASSOC.REQ

Association requests are used to obtain TEI leases, so that a STA may be allocated time in a Beacon Period by the CCo that grants the TEI lease, and so that unicast communications may be used (otherwise, any MPDU sent to the STA must be broadcast and receivers must use the ODA to determine the intended recipient). A CC_ASSOC.REQ message may only be sent to a CCo, either directly or by relaying through a proxy.

Table 1132: CC_ASSOC.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
ReqType	0	1	0x00 = indicates whether this is a new request. 0x01 = indicates that this is a renewal request. 0x02 – 0xFF = reserved
NID	1 - 7	7	Network ID of the network with which the sender wants to associate. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.
CCo Capability	8	1	The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in Section 4.4.3.15.4.6.2. The six MSBs of this field shall be set to 0b000000.

Proxy Networking Capability	9	1	0x00 = STA does not support Proxy Networking. 0x01 = STA fully supports Proxy Networking. 0x02 – 0xFF = reserved
SNID	8	1	Short Network Identifier The 4 LSBs of this field contain the SNID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.

Req Type

Req Type is the type of the association request. It is used with an established AVLN for an Unassociated STA to join (0x00) or for an associated STA to renew its TEI lease (0x01). The rest of the values are reserved.

NID

Network ID (NID) of the network with which the sender wants to associate (refer to Section 4.4.3.1). The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00. Since all STAs always have an NID (even if it is based on a newly generated, random NMK), the requester will always have an NID to use.

CCo Capability

The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in Section 4.4.3.15.4.6.2. The six MSBs of this field are set to 0b000000. One of its uses is to determine which of two Unassociated STAs should become the CCo when they first form an AVLN. Refer to Section 7.4.1.

Proxy Networking Capability

This field indicates whether proxy networking is supported (0x01) or not supported (0x00). Refer to Section 7.7.

CC_ASSOC.CNF

Table 1133: CC_ASSOC.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
Result	0	1	Indicates success or failure (see Table 1134).
NID	1 - 7	7	Network ID The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.

SNID	8	1	Short Network Identifier The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs shall be set to 0x0.
STA TEI	9	1	TEI assigned to the STA (Valid if Result = “Success”)
Lease Time	10 - 11	2	Length of time for which TEI is valid, in minutes

Result

Table 1134: Result Field Interpretation

Result Value	Interpretation
0x00	Success – The STA is successfully associated and remaining field in the MME are valid
0x01	Failure due to temporary resource exhaustion, try again later.
0x02	Failure due to permanent resource exhaustion
0x03	Failure due to other reason
0x04 - 0xFF	Reserved

A TEI is supplied only when the value of Result is 0x00. 0x01, and 0x02 are used when the CCo has run out of TEIs. 0x03 is used for all other failure conditions and the rest of the values are reserved.

NID

NID of the network of the sender (refer to Section 4.4.3.1). The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.

SNID

The four LSBs are set to the Short Network ID (SNID) of the sender’s network. Refer to Section 4.4.3.1. The four MSBs are set to 0x0.

STA TEI

The STA TEI field is set to the TEI value assigned to the new STA or HSTA. This field is valid only if the Result field is “Success STA”. TEI values are shown in Table 71.

Lease Time

Lease Time is the length of time, in minutes, for which the TEI is valid. Permitted values of Lease Time are between 0x0001 and 0xFFFF. The value 0x0000 is reserved.

Table 1135:Lease Time Field

Lease Time Value	Interpretation

NID	1 - 7	7	Network ID. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two

0x0000		Reserved	
0x000F		= 15 Minutes: The default lease time for a STA that is associated but not authenticated.	
0x0B40		= 48 hours: The default lease time for a STA that has successfully authenticated.	
0xFFFF		= ~45.51 Days: The maximum value of the lease time parameter.	

CC_LEAVE.REQ

This message is sent by a station when it determines to leave the network. This may be because the STA is being powered down or because the user has instructed the STA to leave.

Table 1136: CC_LEAVE.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
Reason	0	1	Reason for the Disassociation 0x00 = user request 0x01 = power down 0x02 – 0xFF = reserved

CC_LEAVE.CNF

The CCo shall send this message in response to a CC_LEAVE.REQ message (refer to Section 11.2.30). The message field for the MME is NULL.

CC_LEAVE.IND

The CCo will send this message to a STA that is being asked to leave the AVLN.

Table 1137: CC_LEAVE.IND Message

Field	Octet Number	Field Size (Octets)	Definition
Reason	0	1	Reason for the Disassociation 0x00 = user request 0x01 = TEI Lease Expired 0x02 = CCo shutting down due to a neighboring network with the same NID 0x03 – 0xFF = reserved

NID	1 - 7	7	Network ID. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.

CC_LEAVE.RSP

The STA receiving the CC_LEAVE.IND shall send this message to acknowledge receipt of the CC_LEAVE.IND message. This is the last message for which the STA may use the TEI that it had been assigned. After sending this message, the STA shall cease all communication with the AVLN except for possibly restarting the association and authentication process. The message field for this MME is NULL.

CC_SET_TEI_MAP.REQ

The CC_SET_TEI_MAP.REQ MME is sent to the CCo by an authenticated STA to request that the CCo send it a complete TEI_MAP of the AVLN. The message must be encrypted with the NEK. The message field for this MME is NULL.

CC_SET_TEI_MAP.IND

The CC_SET_TEI_MAP.IND MME is sent by the CCo to notify one or more STAs of any changes to the (TEI, MAC address) mapping. The message must be encrypted with the NEK when sent to authenticated STAs in the AVLN. When it is sent to a newly associated STA that is not authenticated, it shall be sent unencrypted.

Table 1138. CC_SET_TEI_MAP.IND Message

Field	Octet Number	Field Size (Octets)	Definition
Mode	0	1	Mode (refer to Section 11.2.35.1)
Num	1	1	Number of STAs Mapped by This Message 0x00 = invalid, 0x01 = one Station, and so on
TEI_1	2	1	TEI of STA_1
Addr_1	3 -8	6	MAC address of STA_1
Status_1	9	1	Status of STA_1 0x00 = associated, but not authenticated 0x01 = authenticated 0x02 – 0xFF = reserved
…	…	…	…

TEI_n	-	1	TEI of STA_n
Addr_n	1 - 6	6	MAC address of STA_n
Len	7 - 8	2	Length of Payload in octets
Status_n	-	1	Status of STA_n 0x00 = associated, but not authenticated 0x01 = authenticated 0x02 = disassociated 0x03 – 0xFF = reserved

Mode

Mode identifies the purpose of this particular message, which is either to provide the current TEI-MAC Address Map in its entirety or to update particular entries.

Table 1139: Mode Field Interpretation

Result Value	Interpretation
0x00	Update Entire STA (TEI-MAC address) Mapping Typically unicast to a new STA when it joins the AVLN.
0x01	Add new STA entries. Typically sent to all STAs in the AVLN to notify them of the arrival of new STAs.
0x02	Delete existing STA entries. Typically sent to all STAs in the AVLN to notify them of the departure of STAs from the AVLN.
0x03 – 0xFF	Reserved

CC_RELAY.REQ

The CC_RELAY.REQ message is used to request a PSTA or PCo to forward an unencrypted MME to a final STA. The TEI and MAC address of the final STA are given as fields in the CC_RELAY.REQ message.

Upon receiving this message, the PSTA shall extract the Payload field, encapsulate it in a CC_RELAY.IND message and send it to the final destination STA.

If the PSTA has advertised in its Discover Beacon that it does not support Proxy Networking, it shall discard the CC_RELAY.REQ MME without acting upon it.

Table 1140: CC_RELAY.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
FDA	0 - 5	6	MAC address of the final destination STA
FTEI	6	1	TEI of the final destination STA

Len	7 - 8	2	Length of Payload in octets 0x00 = zero octets 0x01 = one octet, and so on
Payload	-	Var	Unencrypted MME that is destined for the final destination STA.

FDA

The FDA field is the MAC address of the final destination STA that shall receive the MME in the Payload field.

FTEI

The FTEI field is the TEI of the final destination STA that shall receive the MME in the Payload field. If this field is equal to the broadcast TEI, the PSTA shall use broadcast when relaying the MME in the Payload field.

Len

The Len field indicates the length of the MME in the Payload field, in octets.

Payload

The Payload field contains an unencrypted MME that is destined for the final destination STA.

CC_RELAY.IND

The CC_RELAY.IND message is used to forward an MME that was originally transmitted by an original source STA to a final destination STA.

If the STA has advertised in its Discover Beacon that it does not support Proxy Networking, it shall discard the CC_RELAY.IND MME without acting upon it.

Table 1141: CC_RELAY.IND Message

Field	Octet Number	Field Size (Octets)	Definition
OSA	0 - 5	6	MAC address of the original source STA that transmitted the Payload.
OTEI	6	1	TEI of the original source STA
Len	7 - 8	2	Length of Payload in octets. 0x00 = zero octets 0x01 = one octet, and so on

Payload	0 - 1	Var	MME that was transmitted by the original source STA and is being forwarded to the destination STA.

OSA

The OSA field is the MAC address of the original source STA that transmitted the MME in the Payload field. This field is obtained from the MSDU that was transmitted by the original source STA.

OTEI

The OTEI field is the TEI of the original source STA that transmitted the MME in the Payload field. This field is obtained from the MPDU that was transmitted by the original source STA.

Len

The Len field indicates the length of the MME in the Payload field, in octets.

Payload

The Payload field contains the MME that was transmitted by the original source STA and is destined for the final destination STA. The MME in the Payload field must be unencrypted.

CC_BEACON_RELIABILITY.REQ

CC_BEACON_RELIABILITY.REQ is used by the CCo to obtain the detection reliability of Central Beacon from other station(s) within the AVLN. The message field for this message is NULL. Beacon detection reliabilities can be used by the CCo for functions such as:

Determining the persistence of the Persistent Schedule.

Determining whether the Beacon has to be relocated to a different part of the AC line cycle.

Determining whether the CCo function has to be handed over to a different station in the Network.

CC_BEACON_RELIABILITY.CNF

CC_BEACON_RELIABILITY.CNF is generated by a station in response to the corresponding CC_BEACON_RELIABILITY.REQ (refer to Section 11.2.38). This message may also be generated in an unsolicited manner when a station observes poor Beacon detection.

Each station shall continuously monitor its CCo's Beacon reliability and report the reliability statistics using CC_BEACON_RELIABILITY.CNF. Beacon Reliability statistics shall be reset when a CC_BEACON_RELIABILITY.CNF is transmitted in response to a CC_BEACON_RELIABILITY.REQ.

Table 1142: CC_BEACON_RELIABILITY.CNF

Field	Octet Number	Field Size (Octets)	Definition

NBP	0 - 1	2	Number of Beacon Periods 0x0000 – zero Beacon Periods 0x0001 – one Beacon Period, and so on
GLID-F	2	1	Number of Missed Beacons 0x00 – zero missed Beacons 0x01 – one missed Beacon, and so on
NMB	2 - 3	2	GLID for the Global Link requested for this operation 0x00 – Global Link 0x01 – one of the Global Links present in this Connection 0x02 – two, and so on Bit 16: sense, LSBs of

Number of Beacon Periods (NBP)

Number of Beacon Periods (NBP) indicates the duration in multiples of Beacon Periods over which the Beacon detection reliability statistics were collected.

Number of Missed Beacons (NMB)

Number of Missed Beacons (NMB) indicates the number of Beacons missed in the duration indicated by the NBP field.

CC_ALLOC_MOVE.REQ

The CC_ALLOC_MOVE.REQ message is sent from a STA to the CCo to request that the allocation of an existing Link be moved to a different position within the AC line cycle. Either the originating or terminating STA of a unicast Connection may request either the Forward or Reverse Link (or both) to be moved.

A station shall not send a CC_ALLOC_MOVE.REQ more than once every five seconds for a particular Connection.

This message should be sent in response to channel conditions. It should not be sent as a result of changing QoS requirements (i.e. changes in the CSPEC).

Table 1143: CC_ALLOC_MOVE.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
CID	0 - 1	2	Connection ID

Reverse Link Bit Loading Estimates	-	Var	Bit Loading Estimates for the Reverse Link The format of this field is the same as that of the corresponding field in Section 11.2.15 This field is only present when GLID-F field contains a valid Global Link Identifier.
GLID-F	2	1	GLID for the Forward Link b7: 0 = no Global Link present in this direction or no change is requested on this Global Link. 1 = Global Link present in this direction b0-b6: seven LSBs of assigned GLID if b7 = 1
GLID-R	3	1	GLID for the Reverse Link b7: 0 = no Global Link present in this direction or no change is requested on this Global Link. 1 = Global Link present in this direction b0-b6: seven LSBs of assigned GLID if b7 = 1
Forward Link Bit Loading Estimates	-	Var	Bit Loading Estimates for the Forward Link The format of this field is the same as that of the corresponding field in Section 11.2.15 This field is only present when GLID-F field contains a valid Global Link Identifier.

Reverse Link Bit Loading Estimates	-	Var	Bit Loading Estimates for the Reverse Link The format of this field is the same as that of the corresponding field in Section 11.2.15 This field is only present when GLID-R field contains a valid Global Link Identifier.

CC_ALLOC_MOVE.CNF

The CC_ALLOC_MOVE.CNF is sent from the CCo to a STA in response to a CC_ALLOC_MOVE.REQ. This message indicates the CCo's response to the request. Should the request be accepted, the allocation is moved by changing the schedule announced in the Beacon. Note: Schedule changes occur asynchronously to the transmission of this message. Therefore, the schedule may be updated before this message is received by the requesting station.

Table 1144: CC_ALLOC_MOVE.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
CID	0 - 1	2	Connection ID
Result	2	1	Result 0x00 = request accepted. 0x01 = request rejected. Feature not supported 0x02 = request rejected. No suitable allocation available. 0x03 – 0xFF = reserved

CC_ACCESS_NEW.REQ

The CC_ACCESS_NEW.REQ message is sent by a Gateway STA to its In-Home CCo to request for resource to set up a CFP Connection with the Access CCo.

Table 1145: CC_ACCESS_NEW.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
STEI	0	1	Specifies the TEI of the Gateway STA that initiates the CFP Connection

DTEI	1	1	Specifies the DTEI of the Access CCo that terminates the CFP Connection
DAddr	2 - 7	6	Specifies the MAC address of the Access CCo that terminates the CFP Connection
Result LLID	0 8	1 1	Specifies the Local Link ID (LLID) of the CFP Connection. It is assigned locally by the initiating STA
CSPEC	-	Var	Specifies the QoS requirements of the CFP Connection
			Specifies the Bit Loading Estimates between the source and destination STAs (i.e., between the Gateway STA and the Access CCo) with respect to the AC line cycle. The format of this field is the same as the "Forward Link Bit Loading Estimates" field in Table 1119.
BLE	-	Var	

CC_ACCESS_NEW.CNF

The CC_ACCESS_NEW.CNF message is sent by an In-Home CCo to a Gateway STA in its In-Home Network in response to a CC_ACCESS_NEW.REQ message. The CC_ACCESS_NEW.REQ message contains a result code indicating the outcome of the request.

Table 1146: CC_ACCESS_NEW.CNF Message

Field	Octet Number	Field Size (Octets)	Definition

GCID-F Result	2 0	1 1	Specifies the Result of the request. 0x00 = Success 0x01 = Error. The GCID is not assigned for the requested Start Time, End Time, and Grant Interval. 0x02 – 0xFF = reserved
			0x02 – 0xFF = reserved
LLID	1	1	The LLID field in the CC_ACCESS_NEW.CNF message is copied from the same field in the CC_ACCESS_NEW.REQ message.

GCID-F GCID-R	2 4	1 1	Present if the Result field is **0x00**. When present, it is the GLID assigned (if any) to the forward CHP Link by the In-Home CCo. The MSB is set to 1 to indicate a GLID is assigned, and is set to 0 to indicate a GLID is not assigned for this direction. The least-significant seven bits represent the least-significant 7 bits of the GLID if one is assigned.
			Present if the Result
ChanEstF	3	1	field is **0x00**. When present, this field is valid if a GLID is assigned for this direction. 0x00 = channel estimation need not be performed in this direction. **0x01** = channel estimation must be performed in this direction. 0x02 – 0xFF = reserved

GCID-R	4	1	Specifies the reason for sending the message. When present, it is the GLID assigned (if any) to the reverse CFP Link by the In-Home CCo. The most-significant bit is set to 1 to indicate a GLID is assigned, and is set to 0 to indicate a GLID is not assigned for this direction. The least-significant 7 bits represent the least-significant 7 bits of the GLID if one is assigned.
Result	0	1	Present if the Result field is **0x00**. When present, this field is valid if a GLID is assigned for this direction. 0x00 = channel estimation need not be performed in this direction. **0x01** = channel estimation must be performed in this direction. 0x02 – 0xFF = reserved

CC_ACCESS_NEW.IND

The CC_ACCESS_NEW.IND message is sent by a Gateway STA to the Access CCo to notify the Access CCo that a CFP has been secured from its In-Home Network.

Table 1147: CC_ACCESS_NEW.IND Message

Field	Octet Number	Field Size (Octets)	Definition

GCID-F	2	1	Specifies the GCID for the CFP Connection. When assigned by the In-Home CCo, this field is set to 0x00. When assigned by the Gateway STA, this field is set to the GCID assigned by the Gateway STA and the In-Home CCo. In this case, the forward and reverse GCID, StartTime, EndTime, and ChanEst fields are present in the message.
Result	0	1	Specifies the Result for sending the message, it is the GLID (if any) to be used for the CFP Connection (specified by the Gateway STA and the In-Home CCo. In this case, the forward and reverse GCID, StartTime, EndTime, and ChanEst fields are present in the message. 0x01 = the Gateway STA is unable to obtain an allocation from its In-Home CCo. 0x02 – 0xFF = reserved
LLID	1	1	Specifies the LLID of the CFP Connection. It is assigned locally by the initiating STA

NID GCID-F	6-11 2	6 1	Present if the Result field is 0x00. When present, it is the GLID assigned (if any) to the forward CFP Link by the In-Home CCo. The MSB is set to 1 to indicate a GLID is assigned, and is set to 0 to indicate a GLID is not assigned for this direction. The least-significant seven
			bits represent the least-significant 7 bits of the GLID if one is assigned.
ChanEstF	3	1	Present if the Result field is 0x00. When present, this field is valid if a GLID is assigned for this direction. **0x00 = channel estimation need not be performed in this direction.** **0x01** = channel estimation must be performed in this direction. 0x02 – 0xFF = reserved
GCID-R	4	1	Corresponding fields for the Reverse Link. This field is similar to the GLID-F field.
ChanEstR	5	1	Corresponding fields for the Reverse Link. This field is similar to the ChanEstF field.

NID	6-11	6	Present if the Result field is 0x00. When present, it specifies the network ID of the In-Home Network who owns the CFP allocation. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.

CC_ACCESS_NEW.RSP

The CC_ACCESS_NEW.RSP message is sent by the Access CCo to the Gateway STA to confirm whether the CFP secured by the Gateway STA is acceptable. The CC_ACCESS_NEW.RSP MMENTY is also sent by the Gateway STA to its In-Home CCo to confirm whether the CFP secured is acceptable.

Table 1148: CC_ACCESS_NEW.RSP Message

Field	Octet Number	Field Size (Octets)	Definition
Result	0	1	Specifies whether the CFP is acceptable to the Access CCo: 0x00 = the Access CCo accepts the proposed CFP. 0x01 = the Access CCo rejects the proposed CFP because it conflicts with its other schedule. 0x02 = the Access CCo-initiated Neighbor Network Coordination, Resend CC_LINK_NEW.REQ after one second. 0x03 – 0xFF = reserved

LLID	1	1	The LLID field in the CC_ACCESS_NEW.CNF message is copied from the same field in the CC_ACCESS_NEW.IND message.
GCID-F	2	1	The Forward Global Link ID (GLID-F) field is copied from the same field in the CC_ACCESS_NEW.IND message.
GCID-R	3	1	The Reverse Global Link ID (GLID-R) field is copied from the same field in the CC_ACCESS_NEW.IND message.
BLE-F	-	Var	Specifies the bit loading estimation of the Forward Link The format of this field is the same as the “Forward Link Bit Loading Estimates” field in Table 1119
BLE-R	-	Var	Specifies the bit loading estimation of the Reverse Link The format of this field is the same as the “Reverse Link Bit Loading Estimates” field in Table 1119.

CC_ACCESS_REL.REQ

The CC_ACCESS_REL.REQ message is sent by the Gateway STA to its In-Home CCo to release the CFP it secured earlier for its communication with the Access CCo. Before sending this message, the Gateway STA must have already sent the CC_ACCESS_REL.IND message to the Access CCo and received the CC_ACCESS_REL.RSP message as a response.

Table 1149: CC_ACCESS_REL.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
Cause	0	1	Indicates the reason for the release of the CFP: 0x00 = normal release 0x01 – 0xFF = reserved
GCID-F	1	1	Has the same meaning as GLID-F in Section 11.2.44.
GCID-R	2	1	Has the same meaning as GLID-R in Section 11.2.44.

CC_ACCESS_REL.CNF

The CC_ACCESS_REL.CNF message is sent by an In-Home CCo to its Gateway STA in response to a received CC_ACCESS_REL.REQ message.

Table 1150: CC_ACCESS_REL.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
Result	0	1	Specifies the outcome of the release request. 0x00 = the request is accepted. 0x01 – 0xFF = reserved
GCID-F	1	1	The GLID-F field is copied from the same field in the CC_ACCESS_NEW.REQ message.
GCID-R	2	1	The GLID-R field is copied from the same field in the CC_ACCESS_NEW.REQ message.

CC_ACCESS_REL.IND

The CC_ACCESS_REL.IND message is sent from the In-Home CCo to the Gateway STA, or from the Gateway STA to the Access CCo, to indicate that the CFP allocated to the Gateway STA is to be released.

Table 1151: CC_ACCESS_REL.IND Message

Field	Octet Number	Field Size (Octets)	Definition
Cause	0	1	Has the same meaning as the corresponding fields in the CC_ACCESS_REL. REQ message.
GCID-F	1	1	Has the same meaning as the corresponding fields in the CC_ACCESS_REL. REQ message.
GCID-R	2	1	Has the same meaning as the corresponding fields in the CC_ACCESS_REL. REQ message.

CC_ACCESS_REL.RSP

The CC_ACCESS_REL.RSP message is sent from the Gateway STA to the In-Home CCo, or from the Access CCo to the Gateway STA, in response to a received CC_ACCESS_REL.IND message.

Table 1152: CC_ACCESS_REL.RSP Message

Field	Octet Number	Field Size (Octets)	Definition
Result	0	1	Has the same meaning as the corresponding fields in the CC_ACCESS_REL. RSP message.
GCID-F	1	1	Has the same meaning as the corresponding fields in the CC_ACCESS_REL. RSP message.
GCID-R	2	1	Has the same meaning as the corresponding fields in the CC_ACCESS_REL. RSP message.

CC_DCPPC.IND

The CC_DCPPC.IND message is sent by a station to the CCo to indicate that the station uses a different receive PHY clock correction during the CP than this network, identified by the SNID. The CC_DCPPC.IND message is also used to indicate when a station changes from using a

NHP1.0	2 - 3	2	Number of HomePlug 1.0.1 transmissions detected 0x0000 = zero

different PHY Receive Clock Correction to using the correct PHY Receive Clock Correction in the network. The interpretation of the Different CP PHY Clock Flag (DCPPCF) field is the same as the corresponding Different CP PHY Clock Flag (DCPPCF) field in Section 4.4.1.5.2.19 Also, refer to Sections 4.4.3.10 and 5.5.4.1.
Reception of a CC_DCPPC.IND message shall cause the CCo to respond with a corresponding CC_DCPPC.RSP message.

Table 1153: CC_DCPPC.IND Message

Field	Octet Number	Field Size (Octets)	Definition
DCPPCF	0	1	0x00 = same CP PHY Clock 0x01 = different CP PHY Clock 0x02 = 0xFF = reserved

CC_DCPPC.RSP

The CC_DCPPC.RSP message is sent by the CCo in response to the corresponding CC_DCPPC.IND message. The message field for this MME is NULL.

CC_HP1_DET.REQ

The CC_HP1_DET.REQ message is a request for the CCo to the station(s) to provide statistics on the detected HomePlug 1.0.1 and HomePlug 1.1 transmissions. The message field for this message is NULL.

CC_HP1_DET.CNF

The CC_HP1_DET.CNF message contains the HomePlug 1.0.1 and HomePlug 1.1 detection statistics. This message is generated in response to a corresponding CC_HP1_DET.REQ. This message may also be generated by AV or GREEN PHY stations in an unsolicited manner when HomePlug 1.0.1 and/or HomePlug 1.1 transmissions are detected. The message field for this message is shown in Table 1154. HomePlug 1.0.1/1.1 detection statistics shall be reset when a CC_HPI_DET.CNF is transmitted in response to a CC_HPI_DET.REQ.

Table 1154: CC_HP1_DET.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
NBP	0 - 1	2	Number of Beacon Periods over which statistics were collected 0x0000 = zero Beacon Periods 0x0001 = one Beacon Period, and so on

NumEntries NHP1.0	0 2 - 3	1 2	Number of HomePlug 1.0 transmissions detected 0x0000 = zero 0x0001 = one, and so on
NHP1.1	4 - 5	2	Number of HomePlug 1.1 transmission detected 0x0000 = zero 0x0001 = one, and so on

CC_BLE_UPDATE.IND

The CC_BLE_UPDATE.IND message is sent from the STA that is the source of a Global Link to the CCo to provide the latest Bit Loading Estimates. CC_BLE_UPDATE.IND may be transmitted by the Source of the Global Link any time it observes significant changes to the BLEs. Reception of CC_BLE_UPDATE.IND shall cause the CCo to update the Bit Loading Estimates for the Global Link and the duration of CF allocation accordingly.

Table 1155: CC_BLE_UPDATE.IND Message

Field	Octet Number	Field Size (Octets)	Definition
GLID	0	1	Global Link Identifier of the Global Link whose Bit Loading Estimates are updated.
Bit Loading Estimates	-	Var	Bit Loading Estimates for the Global Link The format of this field is the same as that of the Forward Link Bit Loading Estimate field defined in Section 11.2.15.

CC_BCAST_REPEAT.IND (GREEN PHY)

CC_BCAST_REPEAT.IND is sent by the CCo to provide a STA with the BMRAT, which is a list of STEIs for which the STA is responsible for retransmitting PBs for broadcast MPDUs received with a STEI in the BMRAT.

Table 1156: CC_BCAST_REPEAT.IND Message

Field	Octet Number	Field Size (Octets)	Definition

NumEntries	0	1	Number of entries = L
Result	0	1	0x00 = Accept 0x01 = One, and so on.
			STEI[0] of broadcast
STEI[0]	1	1	or multicast MPDUs where the PBs are to be retransmitted
STEI[1]	2	1	STEI[1] of broadcast or multicast MPDUs where the PBs are to be retransmitted
...			
STEI[L-1]	L	1	STEI[L-1] of broadcast or multicast MPDUs where the PBs are to be retransmitted

CC_BCAST_REPEAT.RSP (GREEN PHY)

CM_BR_REPEAT.RSP message is sent by the STA to confirm the reception of the CM_BR_REPEAT.IND message.

CC_POWERSAVE.REQ (GREEN PHY)

The CC_POWERSAVE.REQ message is sent by a STA to the CCo to request to go into Power Save.

Table 1157: CC_POWERSAVE.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
PSS	0	1	Power Save Schedule requested The format of the Power Save Schedule is shown in Table 4-103

CC_POWERSAVE.CNF (GREEN PHY)

The CC_POWERSAVE.CNF message is sent by the CCo in response to the corresponding **CC_POWERSAVE.REQ**. This message indicates whether the CCo accepted or rejected the request to enter Power Save mode. This message also includes the Power Save State Identifier and the list of all STAs (including CCo) in Power Save mode and their Power Save Schedules.

Table 1158: CC_POWERSAVE.CNF Message

Field	Octet Number	Field Size (Octet)	Definition

Result	0	1	Result 0x00 = Accept 0x01 = Reject 0x02-0xFF = Reserved
PSSI	1	1	Power Save State Identifier Refer to Section 4.4.3.15.4.15.5
NumTEI	1	1	Number of STAs in Power Save mode (=N) 0x00 = 0 0x01 = 1, and so on.
TEI[1]	-	1	TEI of station in Power Save mode
PSS[1]	-	1	Power Save Schedule of TEI[1] The format of the Power Save Schedule is shown in Table 4-103.
…			
TEI[N]	-	1	TEI of station in Power Save mode
PSS[N]	-	1	Power Save Schedule of TEI[N] The format of the Power Save Schedule is shown in Table 4-103.

CC_POWERSAVE_EXIT.REQ (GREEN PHY)

The CC_POWERSAVE_EXIT.REQ message is sent by a STA to the CCo to indicate that it has exited the Power Save mode. The message field for this MME is NULL.

CC_POWERSAVE_EXIT.CNF (GREEN PHY)

The CC_POWERSAVE_EXIT.CNF message is sent by the CCo to confirm that it has received the corresponding CC_POWERSAVE_EXIT.REQ message. This message also includes the Power Save State Identifier and the list of all STAs (including the CCo) in Power Save mode and their Power Save Schedules.

Table 1159: CC_POWERSAVE_EXIT.CNF Message

Field	Octet Number	Field Size (Octet)	Definition

PSSI	1	1	Power Save State Identifier Refer to Section 4.4.3.15.4.15.5
NumTEI	1	1	Number of STAs in
			Number of STAs in
NumTEI	1	1	Power Save mode (=N) 0x00 = 0 0x01 = 1, and so on.
TEI[1]	-	1	TEI of station in Power Save mode
PSS[1]	-	1	Power Save Schedule of TEI[1] The format of the Power Save Schedule is shown in Table 4-103.
…			
TEI[N]	-	1	TEI of station in Power Save mode
PSS[N]	-	1	Power Save Schedule of TEI[N] The format of the Power Save Schedule is shown in Table 4-103.

CC_POWERSAVE_LIST.REQ (GREEN PHY)

The CC_POWERSAVE_LIST.REQ message is sent by a STA to the CCo to request the list of STAs in Power Save mode. The message field for this MME is NULL.

CC_POWERSAVE_LIST.CNF (GREEN PHY)

The CC_POWERSAVE_LIST.CNF message is sent by the CCo in response to the corresponding CC_POWERSAVE_LIST.REQ message. This message contains the Power Save State Identifier and the list of all STAs (including CCo) in Power Save mode and their Power Save Schedules.

Table 1160: CC_POWERSAVE_LIST.CNF Message

Field	Octet Number	Field Size (Octet)	Definition
PSSI	1	1	Power Save State Identifier Refer to Section 4.4.3.15.4.15.5

NumTEI Num HSTA	1 3	1 1	Number of STAs in Power Save Fields (=N) 0x00 = no hidden STAs information provided.
TEI[1]	-	1	TEI of station in Power Save mode
			Power Save Schedule of TEI[1]
PSS[1]	-	1	The format of the Power Save Schedule is shown in Table 4-103.
…			
TEI[N]	-	1	TEI of station in Power Save mode
PSS[N]	-	1	Power Save Schedule of TEI[N] The format of the Power Save Schedule is shown in Table 4-103.

Proxy Coordinator (PCo) Messages

CP_PROXY_APPOINT.REQ

The CP_PROXY_APPOINT.REQ message is sent by the CCo to a PSTA to promote it to PCo or to a PCo to update the PCo's information. In both cases, the message contains information about HSTAs for which the PCo shall be responsible.

If the STA has advertised in its Discover Beacon that it does not support Proxy Networking, it should never receive the CP_PROXY_APPOINT.REQ MME. If it does receive it, it should send a CP_PROXY_APPOINT.CNF message with Result = Failed.

Table 1161: CP_PROXY_APPOINT.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
ReqType	0	1	Request Type
ReqID	1	1	Request ID
GLID	2	1	GLID

Num HSTA	3	1	Number of HSTA Information Fields (=N) 0x00 = no hidden STAs information provided. 0x01 = one hidden station information provided, and so on.
HSTA SA[1]	4 - 9	6	MAC address of the first HSTA
HSTA TEI[1]	10	1	TEI of the first HSTA
HSTA State[1]	11	1	State of the first HSTA.
...			
HSTA SA[N]	-	6	MAC address of the last HSTA
HSTA TEI[N]	-	1	TEI of the last HSTA
HSTA State[N]	-	1	State of the last HSTA.

ReqType

The ReqType field indicates the different types of request. If the ReqType = Add, the PCo shall send the PH_PROXY_APPOINT.IND message to each HSTA in the list.

Table 1162: ReqType

ReqType Value	Interpretation
0x00	“Add”: This MME is used to assign HSTA(s) to the PCo or PSTA. (A PSTA shall become a PCo.)
0x01	“Delete”: This MME is used to un-assign HSTA(s) from a PCo. (The HSTA(s) may have left the AVLN or been re-assigned to a different PCo.)
0x02	“Update”: This MME is used to update information about HSTA(s) that is (are) under the control of a PCo.
0x03	“Shutdown”: This MME is used to un-assign all HSTAs from a PCo and request the PCo to stop being a PCo.
0x04 to 0xFF	Reserved

ReqID

The ReqID field is set by the sender of this MME such that the same value is not recently used between the sender and the receiver of this MME.

GLID

The GLID field specifies the GLID value where the PCo shall transmit Proxy Beacons. This field shall be ignored if ReqType field is “Shutdown.”

Num HSTA

The Num HSTA field specifies the number of HSTA information fields that are included in this MME.

HSTA SA[1] to HSTA SA[N]

The HSTA SA field is the MAC address of the HSTA concerned. This field shall be ignored if ReqType field is “Shutdown.”

HSTA TEI[1] to HSTA TEI[N]

The HSTA TEI field is the TEI of the HSTA concerned. This field shall be ignored if ReqType field is “Shutdown.”

HSTA State[1] to HSTA STATE[N]

The HSTA State field indicates the state of the HSTA concerned. This field shall be ignored if ReqType field is “Shutdown” or “Delete.”

Table 1163: HSTA State

HSTA State Value	Interpretation
0x00	“Associated”: The HSTA is associated with the AVLN and is assigned a TEI.
0x01	“Authenticated”: The HSTA is authenticated (and associated) with the AVLN and has obtained the NEK.
0x02 to 0xFF	Reserved

CP_PROXY_APPOINT.CNF

The CP_PROXY_APPOINT.CNF message is sent by a PSTA or PCo to the CCo in response to a received CP_PROXY_APPOINT.REQ message.

Table 1164: CP_PROXY_APPOINT.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
ReqID	0	1	Request ID
Result	1	1	Result

ReqID

The ReqID field in the CP_PROXY_APPOINT.CNF message is copied from the ReqID field in the corresponding CP_PROXY_APPOINT.REQ message.

Result

Table 1165: Result

Result Value	Interpretation
0x00	Success
0x01	Failed (no resources or Proxy Networking not supported)

0x02 to 0xFF	Reserved

PH_PROXY_APPOINT.IND

The PH_PROXY_APPOINT.IND message is sent by a PSTA or PCo to an HSTA to indicate that the PCo is responsible for the HSTA. Since the HSTA does not yet know its TEI, the PH_PROXY_APPOINT.IND shall be addressed to the broadcast TEI and the HSTA's MAC address.

Table 1166: PH_PROXY_APPOINT.IND Message

Field	Octet Number	Field Size (Octets)	Definition
PCo SA	0 - 5	6	MAC address of the PCo
PCo TEI	6	1	TEI of the PCo
CCo SA	7 - 12	6	MAC address of the CCo
CCo TEI	13	1	TEI of the CCo
GLID	14	1	GLID where Proxy Beacons will be transmitted.

PCo SA

The PCo SA field specifies the MAC address of the PCo.

PCo TEI

The PCo TEI field is set to the TEI of the PCo that shall transmit Proxy Beacons for the new HSTA.

CCo SA

The CCo SA field specifies the MAC address of the PCo.

CCo TEI

The CCo TEI field specifies the TEI of the CCo.

GLID

The GLID field specifies the GLID where the PCo shall transmit Proxy Beacons.

CP_PROXY_WAKE.REQ

The CP_PROXY_WAKE.REQ may be sent by a PCo to request exit from Network Power Saving Mode when it detects transmission from HSTA. The Message field for the MME is NULL.

For more information, refer to Section 7.11.

CCo - CCo

All Management Messages between CCos of Neighbor Networks are unencrypted.

NN_INL.REQ and NN_INL.CNF

Networks List (INL) of another CCo. When a CCo receives an NN_INL.REQ message, it must reply with an NN_INL.CNF message. The NN_INL.REQ and NN_INL.CNF messages are unencrypted.

Table 1167: NN_INL.REQ and NN_INL.CNF Message

Field	Octet Number	Field Size (Octets)	Definition

MyTEI	0	1	TEI of the sender of this message (a non-zero value)
MyNumSlots	10	1	Number of Beacon Slots in the Beacon Region of the sender Short Network Identifier of the sender of this message The four LSBs of this field contain the SNID (refer to
MySNID/Access	1	1	Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.
MyNID	2 – 8	7	Network Identifier of the sender of this message. This field is Ignored if MyTEI=0x00. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.
MyNumAuthSTAs	9	1	Number of authenticated STAs in the AVLN, including the CCo.

NumInfo	13	1	Number of Beacon Slot Information Records (N) that follow this one. 0x00 = none.
MyNumSlots	10	1	Number of Beacon Slots in the Beacon Period (Neg) of this sender. This field is Ignored if MyTEI=0x00. 0x00 = one Beacon Slot, and so on 0x08 - 0xFF = reserved
MySlotID	11	1	SlotID where the sender of this message transmits its Beacon. This field is Ignored if MyTEI=0x00. 0x00 = first Beacon Slot, and so on 0x08 - 0xFF = reserved
MyCoordStatus	12	1	Coordinating Status of the Sender 0x00 = unknown 0x01 = Non-Coordinating Network 0x02 = Coordinating, Group status unknown 0x03 = Coordinating Network in the same Group as this CCo 0x04 = Coordinating Network not in the same Group as this CCo 0x05 – 0xFF = reserved

NumInfo	13	1	Number of Beacon Slots in the Beacon Region (N).
NumSlots_1	22	1	Slot number of the Beacon Slot of the sender candidate.
			Short Network Identifier of the first network that the sender can detect.
SNID/Access_1	14	1	The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.
NID_1	15 - 21	7	Network Identifier of the first network that the sender can detect. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.

NumSlots_1	22	1	Number of Beacon Slots in the Beacon Region of the first network that the Coordinator can detect. 0x00 = one Beacon Slot, and so on 0x08 - 0xFF = reserved
CoordStatus_1	26	1	Number of Beacon Slots in the Beacon Region of the first network that the Coordinator can detect. 0x00 = one Beacon Slot, and so on 0x08 - 0xFF = reserved
SlotID_1	23	1	SlotID where the first network that the sender can detect transmits its Beacon. 0x00 = first Beacon Slot, and so on 0x08 - 0xFF = reserved
			Offset between the
Offset_1	24 - 25	2	Beacon Regions of the sender of this message and the first network that it can detect, measured in units of AllocationTimeUnit. Offset = start time of sender's Beacon Region minus start time of receiver's Beacon Region (modulo) Beacon Period. 0x0000 = zero or in the same Group 0x0001 = one AllocationTimeUnit, and so on

NID_N	-	7	Network Identifier of the Network that 0x00 = unknown 0x01 = Non-Coordinating Network 0x02 = Coordinating, Group status unknown
CoordStatus_1	26	1	0x03 = Coordinating Network in the same Group as this CCo 0x04 = Coordinating Network not in the same Group as this CCo 0x05 – 0xFF = reserved
…	…	…	…
SNID/Access_N	-	1	Short Network Identifier of the last network that the sender can detect. The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.

NID_N	-	7	Network Identifier of the last network that the sender can detect. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.
CoordStatus_N	-	1	Coordinating Status of the last network that the sender can detect. 0x00 = unknown
NumSlots_N	-	1	Number of Beacon Slots in the Beacon Region of the last network that the sender can detect. 0x00 = one Beacon Slot, and so on 0x08 - 0xFF = reserved
SlotID_N	-	1	SlotID where the last network that the sender can detect transmits its Beacon. 0x00 = first Beacon Slot, and so on 0x08 - 0xFF = reserved
Offset_N	-	2	Offset between the Beacon Regions of the sender of this message and the last network that it can detect, measured in units of AllocationTimeUnit. 0x0000 = zero or in the same Group 0x0001 = one AllocationTimeUnit, and so on

CoordStatus_N MySNID/Access	1	1	Proposed SNID of the Network 0x00 – Main Network 0x01 – Neighboring Network 0x02 – Sub-Network 0x03 – Coordinating Network 0x04 – Proxy Coordinating Network not in the same Group as this CCo 0x05 – 0xFF = reserved
NN_NEW_NET.REQ			

The NN_NEW_NET.REQ message is sent by a new CCo to the CCos in its INL to request to set up a new network. The message contains the Beacon Slot number.

The Offset field is set to 0 if the message is sent to a CCo of the same group (i.e., with the same system timing). Otherwise, the Offset field is calculated as the start time of the Beacon Region of the sender minus the start time of the Beacon Region of the receiver.

The NN_NEW_NET.REQ message is unencrypted.

Table 1168: NN_NEW_NET.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
MyTEI	0	1	Proposed TEI of the sender.

MySlotID	11	1	Proposed SNID of the sender. The four MSBs of this field contain the SNID (refer to Section 4.4.1.4. The four MSBs of this field shall be set to 0x0 if the network is
MySNID/Access	1	1	in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.
ReqID	2	1	Request ID. Set by sender so that the same value was not used recently.
MyNID	3-9	7	Proposed NID of the sender. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.
MyNumSlots	10	1	Proposed number of Beacon Slots in the Beacon Region. 0x00 = one Beacon Slot, and so on 0x08 - 0xFF = reserved

MySlotID	11	1	SNID of the sender The proposed SlotID to be used by the sender in the Beacons. The MSB of this field shall be set to 0x0 if the network is unsecured, or 0x1 if it is a Access network
MySNID/Access	1	1	0x00 – 0x07 – SNID of the sender 0xff – the sender is not in a network
Offset	12-13	2	Time offset between the Beacon Regions of the sender and the receiver, in units of AllocationTimeUnit. 0x0000 = zero or in the same Group 0x0001 = one AllocationTimeUnit, and so on

NN_NEW_NET.CNF

The NN_NEW_NET.CNF message is sent by a CCo to another CCo in response to a received NN_NEW_NET.REQ message. If the request is accepted, the Result field shall be set to “successful” and the Information field shall be set to the Beacon Period structure of the sender of this message. In addition, the CCo shall not change its schedule until it receives an NN_NEW_NET.IND message from the new CCo. If the request is rejected, the Result field shall be set to “unsuccessful SNID”, “unsuccessful SlotID” or “unsuccessful, not in the same Group”. When the Result is “unsuccessful SNID” or “unsuccessful SlotID”, the Information shall be set to proposed acceptable SNID or SlotID value. The message is unencrypted.

Table 1169: NN_NEW_NET.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
MyTEI	0	1	TEI of the sender.

MySNID/Access	1	1	SNID of the sender The four LSBs of this field contain the SNID (refer to Section 4.4.1.4. The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.
ReqID	2	1	Request ID. Copied from the ReqID field of the NN_NEW_NET.REQ message.
Result	3	1	0x00 = successful (seeTable 11-70) 0x01 = unsuccessful SNID (see Table 11-71) 0x02 = unsuccessful SlotID (see Table 11-72) 0x03 = unsuccessful, not in the same Group (Information field is null) 0x04 – 0xFF = reserved
Information	-	Var	Information field. The format of this fields depends on the Result

Table 1170: Format of Information Field when Result = 0x00 (Successful)

Field	Octet Number	Field Size (Octets)	Definition

Num	0	1	Number of Region Types to Follow (=N) 0x00 = zero Region Types 0x01 = one Region Type, and so on
Type[1]	1	1	First Region Type (refer to Section 4.4.3.15.4.3.2. The four LSBs of this field contain the Region Type (refer to Section 4.4.3.15.4.3.2. The four MSBs shall be set to 0x0.
EndTime[1]	2 - 3	2	End time of first Region Type, in units of AllocationTimeUnit 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on
…	…	…	…
Type[N]	-	1	Last Region Type The four LSBs of this field contain the Region Type (refer to Section 4.4.3.15.4.3.2. The four MSBs shall be set to 0x0.
EndTime[N]	-	2	End time of last Region Type, in units of AllocationTimeUnit. 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on

Table 1171: Format of Information Field when Result = 0x01 (Unsuccessful SNID)

Field	Octet Number	Field Size (Octets)	Definition
SlotID[N]	N	1	Last SlotID Proposed
Num	0	1	Number of Proposed SNIDs to follow (=N) 0x00 = none 0x01 = one, and so on
			0x08 - 0xFF = reserved
SNID[1]	1	1	First SNID Proposed The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0.
…	…	…	…
SNID[N]	-	1	Last SNID Proposed The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0.

Table 1172: Format of Information Field when Result = 0x02 (Unsuccessful SlotID)

Field	Octet Number	Field Size (Octets)	Definition
Num	0	1	Number of proposed SlotIDs to Follow (=N) 0x00 = None, 0x01 = One and so on.
SlotID[1]	1	1	First SlotID Proposed 0x00 = first Beacon Slot, and so on 0x08 - 0xFF = reserved
…	…	…	…

[illegible]	[illegible]	1	[illegible]

NN_NEW_NET.IND

The NN_NEW_NET.IND message is sent by the new CCo (which sent the NN_NEW_NET.REQ message) to the CCo's in its INL to confirm whether the request to set up a new network is successful or canceled.

If at least one NN_NEW_NET.CNF message with a Result field not equal to Success is received, the new CCo will send a NN_NEW_NET.IND message with Status field equal to Cancel to networks in its INL that have replied with a NN_NEW_NET.CNF message with Result field equal to Success.

Alternatively, if the NN_NEW_NET.CNF messages received all have the Result field equal to Success; the new CCo will send an NN_NEW_NET.IND message with Status field equal to Go to all the CCo's in its INL. The NN_NEW_NET.IND message is unencrypted.

Table 1173: NN_NEW_NET.IND Message

Field	Octet Number	Field Size (Octets)	Definition
MyTEI	0	1	Proposed TEI of the sender
MySNID/Access	1	1	Proposed SNID of the Sender The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.

ReqID	2	1	0x00 = Request 0x01 – 0xFF = Copied from the ReqID field of the **NN_NEW_NET.REQ** message
MySlotID	3	1	Proposed SlotID to be used by the sender
Status	3	1	0x00 = go 0x01 = cancel 0x02 – 0xFF = reserved

NN_ADD_ALLOC.REQ

The NN_ADD_ALLOC.REQ message is sent by a CCo to other CCo's in its INL to request to share additional bandwidth. The message contains the proposed schedules to be used by the CCo. Each schedule is specified by a start time and an end time, using the start time of the sender's Beacon Region as a reference. The NN_ADD_ALLOC.REQ message is unencrypted.

Table 1174: NN_ADD_ALLOC.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
MyTEI	0	1	TEI of the Sender
MySNID/Access	1	1	SNID of the Sender The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.
ReqID	2	1	Request ID. Set by sender so that the same value was not used recently.

StartTime_n	3	2	0x00 = index of the last scheduled Slot 0x01 - 0x07 = proposed Slot ID to be used by the sender to transmit its Beacons. 0x00 = first Beacon Slot, and so on 0x08 - 0xFF = reserved
MySlotID	3	1	
Offset	4 - 5	2	Time offset between the Beacon Regions of the sender and the receiver, in units of AllocationTimeUnit 0x0000 = zero or in the same Group 0x0001 = one AllocationTimeUnit, and so on
Num	6	1	Number of Schedules to Follow 0x00 = none 0x01 = one and so on
StartTime_1	7 - 8	2	Start time of the first schedule being requested, in units of AllocationTimeUnit 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on
EndTime_1	9 - 10	2	End time of the first schedule being requested, in units of AllocationTimeUnit 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on
…	…	…	…

ReqID StartTime_n	2 -	1 2	Request ID copied from the ReqID field Start time of the last schedule being requested, in units of AllocationTimeUnit 0x0000 = zero
			0x0001 = one AllocationTimeUnit, and so on
EndTime_n	-	2	End time of the last schedule being requested, in units of AllocationTimeUnit 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on

NN_ADD_ALLOC.CNF

The NN_ADD_ALLOC.CNF message is sent by a CCo to another CCo in response to a received NN_ADD_ALLOC.REQ message. The message is unencrypted.

Table 1175: NN_ADD_ALLOC.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
MyTEI	0	1	TEI of the sender.
MySNID/Access	1	1	SNID of the sender. The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.

ReqID	2	1	Request ID. Copied from the ReqID field of the **NN_ADD_ALLOC.REQ** message.
Result	3	1	Result 0x00 = success 0x01 = failure 0x02 - 0xFF = reserved

NN_ADD_ALLOC.IND

The NN_ADD_ALLOC.IND message is sent by a CCo (which sent the NN_ADD_ALLOC.REQ message) to the CCo's in its INL to confirm whether the bandwidth request is successful or canceled. If at least one NN_ADD_ALLOC.CNF message with a Result field not equal to Success is received, the CCo will send an NN_ADD_ALLOC.IND message with Status field equal to Cancel to all its neighbors that have replied with a NN_ADD_ALLOC.CNF message with Result field equal to Success.

Alternatively, if the NN_ADD_ALLOC.CNF messages received all have the Result field equal to Success; the CCo will send an NN_ADD_ALLOC.IND message with Status field equal to Go to all the CCo's in its INL.

The NN_ADD_ALLOC.IND message is unencrypted.

Table 1176: NN_ADD_ALLOC.IND Message

Field	Octet Number	Field Size (Octets)	Definition
MyTEI	0	1	TEI of the sender.
MySNID/Access	1	1	SNID of the sender. The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.

ReqID MySlotID	2 3	1 1	Request ID = 0x00 – 0x07 = Copied from the ReqID field of the **NN_ADD_ALLOC.REQ** message.
Status	3	1	0x00 = go 0x01 = cancel 0x02 – 0xFF = reserved

NN_REL_ALLOC.REQ

The NN_REL_ALLOC.REQ message is sent by a CCo to the CCos of its INL to request to release part or all of its Reserved Regions. The message contains the schedules to be released. Each schedule is specified by a start time and an end time, using the start time of the CCo's Beacon Region as a reference. The NN_REL_ALLOC.REQ message is unencrypted.

Table 1177: NN_REL_ALLOC.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
MyTEI	0	1	TEI of the sender.
MySNID/Access	1	1	SNID of the Sender The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.
ReqID	2	1	Request ID Set by sender so that the same value was not used recently.

StartTime_n	3	2	Start time of the last schedule to be released by this sender
MySlotID	3	1	0x00 - 0x07 = proposed Slot ID to be used in order to transmit its Beacons. 0x00 = first Beacon Slot, and so on 0x08 - 0xFF = reserved
Offset	4 - 5	2	Time offset between the Beacon Regions of the sender and the receiver, in units of AllocationTimeUnit. 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on
Num	6	1	Number of Schedules to Follow 0x00 = none 0x01 = one, and so on
StartTime_1	7 - 8	2	Start time of the first schedule to be released, in units of AllocationTimeUnit. 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on
EndTime_1	9 - 10	2	End time of the first schedule to be released, in units of AllocationTimeUnit. 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on
…	…	…	…

ReqID	2	1	Request ID of the last schedule to be released from the ReqID field
StartTime_n	-	2	Start time of the last schedule to be released, in units of AllocationTimeUnit. 0x0000 = zero
			0x0001 = one AllocationTimeUnit, and so on
EndTime_n	-	2	End time of the last schedule to be released, in units of AllocationTimeUnit. 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on

NN_REL_ALLOC.CNF

The NN_REL_ALLOC.CNF message is sent by a CCo to another CCo in response to a received NN_REL_ALLOC.REQ message. The message is unencrypted.

Table 1178: NN_REL_ALLOC.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
MyTEI	0	1	TEI of the sender.
MySNID/Access	1	1	SNID of the Sender The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.

ReqID SlotID	2 3	1 1	Request ID. Copied from the ReqID field of the NN_REL_ALLOC.REQ message.
			Result 0x00 = success
Result	3	1	0x01 = failure 0x02 – 0xFF = reserved

NN_REL_NET.IND

The NN_REL_NET.IND message is sent by a CCo to the CCo's of its INL to release all its Reserved Regions and shut down the network. The NN_REL_NET.IND message is unencrypted.

Table 1179:NN_REL_NET.IND Message

Field	Octet Number	Field Size (Octets)	Definition
MyTEI	0	1	TEI of the sender.
MySNID/Access	1	1	SNID of the Sender The four LSBs of this field contain the SNID (refer to Section 4.4.1.4). The four MSBs of this field shall be set to 0x0 if the network is in-home, or 0x1 if it is an Access network. The Access field in HomePlug AV delimiters (refer to Section 4.4.1.3) can be used to determine whether a network is an in-home or an Access network.
ReqID	2	1	Request ID Set by sender so that the same value was not used recently.

SlotID StartTime_n	3 -	1 2	Slot ID used by the last schedule reserved, in beacons. 0x00 = first Slot, and so on 0x08 - 0xFF = reserved
			Time offset between
Offset	4 - 5	2	the Beacon Regions of the sender and the receiver, in units of AllocationTimeUnit. 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on
Num	6	1	Number of Schedules to Follow 0x00 = none 0x01 = one and so on
StartTime_1	7 - 8	2	Start time of the first schedule reserved, in units of AllocationTimeUnit. 0x0000 = zero or in the same Group 0x0001 = one AllocationTimeUnit, and so on
EndTime_1	9 - 10	2	End time of the first schedule reserved, in units of AllocationTimeUnit. 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on
…	…	…	…

StartTime_n	-	2	Start time of the last schedule reserved, in units of AllocationTimeUnit. 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on
EndTime_n	-	2	End time of the last schedule reserved, in units of AllocationTimeUnit. 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on

Station – Station
CM_UNASSOCIATED_STA.IND
Table 1180: CM_UNASSOCIATED_STA.IND Message

Field	Octet Number	Field Size (Octets)	Definition
NID	0 - 6	7	**Network ID** The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.
CCo Capability	7	1	**CCo Capability** The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in Section 4.4.3.15.4.6.2. The six MSBs of this field shall be set to 0b000000.

CM_ENCRYPTED_PAYLOAD.IND

The CM_ENCRYPTED_PAYLOAD.IND MME exists in two forms. In the standard form, it carries an encrypted payload used by the key distribution protocols described in this specification. However, when PID is 0x04, the fields marked “Encrypted Payload” in Table 1181 are not processed by the MAC; the entire MME is simply passed uninterpreted to and from the Higher Layer Entity (HLE). Also, the 16-octet field ordinarily used to carry the IV shall be used to carry an Universally Unique Identifier (UUID).

Note: The HLE may use the PEKS for its own purposes in this case.

Table 1181. CM_ENCRYPTED_PAYLOAD.IND Message

Field	Octet Number	Field Size (Octets)	Definition
			Payload Encryption
PEKS	0	1	Key Select (**Unencrypted**) The four LSBs of this field contain the PEKS. The four MSBs shall be set to 0x0.
AVLN Status	1	1	AVLN status of source. (**Unencrypted**)
PID	7	1	Protocol ID (**Unencrypted**)
PRN	8 - 9	2	Protocol Run Number (**Unencrypted**)
PMN	10	1	Protocol Message Number (**Unencrypted**)
IV or UUID	-	16	AES encryption Initialization Vector or Universally Unique Identifier (UUID) when PID=0x04 (**Unencrypted**)
Len	-	2	Length of MM, in octets (**Unencrypted**)
RF	-	0-15	Random Filler: A random number (between 0 and 15) of random filler octets included in Encrypted Payload to make

Padding RF	- -	0 - 15 0-15	Random Filler of Encrypted Payload to (128 bit boundary) Length (in octets) of random filler octets included in Encrypted Payload to make
			position of Protocol fields unpredictable (**Encrypted Payload**) – not present when PID=0x04.
MM or HLE Payload	-	Var	MM (Management Message – refer to Section 11.1) can be any legal Management Message except CM_ENCRYPTED_ PAYLOAD.IND (**Encrypted Payload**) – uninterpreted HLE payload when PID=0x04.
CRC	-	0 or 4	Checksum on MME (**Encrypted Payload**) – not present when PID=0x04.
PID	-	0 or 1	Protocol ID (**Encrypted Payload**) – not present when PID=0x04.
PRN	-	0 or 2	Protocol Run Number (**Encrypted Payload**) – not present when PID=0x04.
PMN	-	0 or 1	Protocol Message Number (**Encrypted Payload**) – not present when PID=0x04.

0x04		Associated with an AVLN but not PCo	No adjustment of Encrypted Payload to
Padding	-	0 - 15	128 bit boundary (**Encrypted Payload**) – not present when PID=0x04.
RFLen		0 or 1	0x00 – 0x0F = Length of Random Filler (Bit numbers are before encryption and after decryption). (**Encrypted Payload**) 0x10 – 0xFF = reserved - not present when PID=0x04.

Payload Encryption Key Select (PEKS)

Payload Encryption Key Select (PEKS) is the Index of the Encryption Key used for encrypting MME Payloads. It is not to be confused with the EKS, which appears in the FC to identify the Encryption Key used for PBBs (segments). This field is 4 bits long. Except for PEKS=0x0 or 0xF, it is only unambiguous when it is associated with the MAC address of the STA on the other end of the Link (i.e., the transmitter uses the ODA to resolve the PEKS; the receiver uses the OSA to resolve the PEKS). A PEKS=0xF indicates No Key (i.e., the payload is not encrypted).

Table 1182: Payload Encryption Key Select Interpretation

AVLN Status Value	Interpretation
0x0	Destination STA's DAK (AES 128 bit key)
0x1	NMK known to STA (AES 128 bit key)
0x2 – 0xE	Identifies TEKs (AES 128 bit keys)
0xF	No KEY (used when the requested Encryption Key is not provided or the payload is sent in the clear)

AVLN Status

The AVLN Status field specifies the current association status and capabilities of the sending station.

Table 1183: AVLN Status Interpretation

AVLN Status Value	Interpretation
0x00	Unassociated and Level-0 CCo Capable.
0x01	Unassociated and Level-1 CCo Capable
0x02	Unassociated and Level-2 CCo Capable
0x03	Unassociated and Level-3 CCo Capable

0x04	Associated with an AVLN but not PCo Capable
0x05	Associated with an AVLN and PCo Capable
0x06-0x7	Reserved
0x08	CCo of an AVLN
0x09 – 0xFF	Reserved

Protocol ID (PID)

The Protocol ID (PID) field identifies the purpose of the protocol that is being transmitted in the encryption payload. Except when PID=0x04, the PID appears twice within the message, once in the unencrypted portion of the message and once in the encrypted portion of the message. For more information, refer to Section 7.10.8.

Table 1184: Protocol ID Interpretation

PID Value	Interpretation
0x00	Authentication request by new STA.
0x01	Provision authenticated STA with new NEK by CCo
0x02	Provision STA with NMK using DAK
0x03	Provision STA with NMK using UKE
0x04	HLE protocol
0x05 – 0xFF	Reserved

Protocol Run Number (PRN)

The Protocol Run Number (PRN) field contains a random number that was generated at the beginning of this particular run and is used to distinguish between different runs of the same protocol. Except when PID=0x04, the PRN appears twice within the message, once in the unencrypted portion of the message and once in the encrypted portion of the message.

Protocol Message Number (PMN)

The Protocol Message Number (PMN) field is a sequential counter of the number of messages within the current protocol run, including this one. Except when PID=0x04, the PMN appears twice within the message, once in the unencrypted portion of the message and once in the encrypted portion of the message.

Initialization Vector (IV) or Universally Unique Identifier (UUID)

When PID=0x04, this field is a 128-bit universally unique identifier (UUID). Otherwise, it is the Initialization Vector (IV) used for AES-128. Refer to Section 7.10.8.

Length (Len)

The length field indicates the length in octets of the encapsulated Management Message (i.e., not including the other seven fields in the encrypted portion). When PID=0x04, it is the length in octets of the HLE Payload.

Random Filler (RF)

Between 0 and 15 octets of random data are placed in the Random Filler (RF) field. This field is not present when PID=0x04.

Management Message (MM) or HLE Payload

When PID=0x04, this field takes up all of the MME after the Len field, and is not interpreted by the STA. Otherwise, it contains the MAC Management Message encapsulated and encrypted in the CM_ENCRYPTED_PAYLOAD.IND MME. Only the CM_ENCRYPTED_PAYLOAD.IND MME is not allowed as the encapsulated MME.

Cyclic Redundancy Check (CRC)

The Cyclic Redundancy Check (CRC) is the CRC-32 described in Section 4.2.1. It shall cover the Encapsulated MM Entry. The CRC field is not present when PID=0x04.

Protocol ID (PID - Encrypted)

The PID encrypted field shall exactly match the value of the PID field in the unencrypted part of the MME. This field is not present when PID=0x04.

Protocol Run Number (PRN - Encrypted)

The PRN encrypted field shall exactly match the value of the PRN field in the unencrypted part of the MME. This field is not present when PID=0x04.

Protocol Message Number (PMN - Encrypted)

The PMN encrypted field shall exactly match the value of the PMN field in the unencrypted part of the MME. This field is not present when PID=0x04.

Padding - Encrypted

Padding is between 0 and 15 octets of random data as needed to bring the total length of the encrypted portion of the MME to a multiple of 128 bits for AES-128 encryption. Its length is determined by the length of the RF and the MM fields. This field is not present when PID=0x04.

RF Length (RFLen - Encrypted)

RF Length indicates the length of the Random Filler in octets, and is a uniform random number between 0 and 15. This field is not present when PID=0x04.

CM_ENCRYPTED_PAYLOAD.RSP

Table 1185: CM_ENCRYPTED_PAYLOAD.RSP Message

Field	Octet Number	Field Size (Octets)	Definition
Result	0	1	Result
PID	1	1	Protocol ID
PRN	2 - 3	2	Protocol Run Number

Result

This message is never sent to indicate success. If the CM_ENCRYPTED_PAYLOAD.IND is successful, the message embedded in it is the one that could provoke a response that would generally be embedded in another CM_ENCRYPTED_PAYLOAD.IND message. This message will indicate either a failure to correctly receive the MME or an aborted protocol run. Since either side of the protocol run may abort, this message may be sent by the same STA that sent the CM_ENCRYPTED_PAYLOAD.IND MME.

Table 1186: Result Field Interpretation

Result Value	Interpretation
0x00	Success. (never used)
0x01	Failure
0x02	Abort
0x03 – 0xFF	Reserved

CM_SET_KEY.REQ
The CM_SET_KEY.REQ message usually is embedded within the encrypted payload of a CM_ENCRYPTED_PAYLOAD.IND message. However, it may be sent by a CCo without being embedded to a STA as the first message in the NEK key distribution protocol to initialize the NEK. It may also be sent by the HLE over the H1 interface without being embedded to the CL to change the NMK.

Table 1187: CM_SET_KEY.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
Key Type	0	1	Key Type
			Random number that
My Nonce	1 - 4	4	will be used to verify next message from other end; in encrypted portion of payload.
Your Nonce	5 - 8	4	Last nonce received from recipient; it will be used by recipient to verify this message; in encrypted portion of payload.
PID	9	1	Protocol for which Set Key is asserted Note: This is included since MMEs are not always in an encrypted payload) Refer to Section 11.5.2.3 for information.
PRN	10 - 11	2	Protocol Run Number (refer to Section 11.5.2.4)
PMN	12	1	Protocol Message Number (refer to Section 11.5.2.5)
CCo Capability	13	1	The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in

CCo Capability	13	1	The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in Section 4.4.3.15.4.6.2. The six MSBs of this field are set to 0b000000
NID	14 – 20	7	Network ID to be associated with the key distributed herein. The 54 LSBs of this field contain the NID (refer to Section 3.4.3.1). The two MSBs shall be set to 0b00.
NewEKS	21	1	New Encryption Key Select or New Payload Encryption Key Select depending upon value of Key Type The four LSBs of this field contain the PEKS (refer to Section 11.5.2.1) or EKS (refer to Section 4.4.1.5.2.8). The four MSBs shall be set to 0x0.
NewKEY	var	0 or 16	New Key (none or 128-bit AES Key)

Key Type

The Key Type field appears in many different MMEs and Primitives. In all cases, the values are the same, although not all values are permitted in all messages. Interpretation of this field is defined in Table 11-88. The following restrictions apply for the Key Type for the CM_SET_KEY.REQ message.

Key Types DAK and HASH KEY are never permitted.

Key Type NEK, Nonce-only, and TEK are not permitted when this MME is passed across the H1

			interface. Key Type NEK is only allowed across the PHY interface if it is embedded in a CM_ENCRYPTED_PAYLOAD.IND message as described in Section 7.10.4; otherwise, the message received from the PHY interface shall be ignored. Key Type TEK is only allowed across the PHY interface if it is embedded in a CM_ENCRYPTED_PAYLOAD.IND message as described in Section 7.10.3.4; otherwise, the message received from the PHY interface shall be ignored. Key Type NMK is only allowed across the PHY interface if it is embedded in a CM_ENCRYPTED_PAYLOAD.IND message as described in Section 7.10.3; otherwise, the message received from the PHY interface shall be ignored.
Your Nonce	5 – 8	4	Last nonce received from recipient; it will

Table 1188: Key Type Interpretation

Key Type Value	Interpretation
0x00	DAK (AES-128) (never used)
0x01	NMK (AES-128)
0x02	NEK (AES-128)
0x03	TEK (AES-128)
0x04	HASH KEY (Random-3072)
0x05	Nonce Only (no key)
0x06 – 0xFF	Reserved

NID

When Key Type = NMK, the NID field holds the NID to associate with the NMK, and the Security Level of the NMK shall be set to the SL of the NID in the CM_SET_KEY.REQ message. This SL must be compatible with the key distribution method used (refer to Section 7.10.3.1). Normally, the NID will match the sender's NID.

New_EKS

New EKS holds the EKS or the PEKS value associated with the key that is being set.

CM_SET_KEY.CNF

Table 1189. CM_SET_KEY.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
Result	0	1	0x00 = success 0x01 = failure 0x02 – 0xFF = reserved
My Nonce	1 – 4	4	Random number that will be used to verify next message from other end; in encrypted portion of payload.

Your Nonce	5 – 8	4	Last nonce received from recipient; it will be used to by recipient to verify this message; in encrypted portion of payload.
PID		1	Protocol for which Set Key is confirmed Note: This is included since MMEs are not always in an encrypted payload. Refer to Section 11.5.2.3 for more information.
PRN		2	Protocol Run Number (refer to Section 11.5.2.4)
PMN		1	Protocol Message Number (refer to Section 11.5.2.5)
CCo Capability		1	The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in Section 4.4.3.13.4.6.2. The six MSBs of this field are set to 0b000000

CM_GET_KEY.REQ

The CM_GET_KEY.REQ message usually is embedded within the encrypted payload of a CM_ENCRYPTED_PAYLOAD.IND message. However, it is also sent unencrypted as the first message in the UKE key distribution protocol to generate a TEK.

Table 1190: CM_GET_KEY.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
Request Type	0	1	Request Type 0x00 = direct 0x01 = relayed 0x02 - 0xFF = reserved

Requested Key Type	1	1	Requested Key Type Interpretation of this field is the same as in Section 11.5.4.1.
NID	3 - 9	7	Network ID of transmitter or NID of AVLN that transmitter wishes to join. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.
My Nonce	10 - 13	4	Random number that will be used to verify next message from other end (Required for all methods)
PID	14	1	Protocol ID
PRN	15-16	2	Protocol Run Number
PMN	17	1	Protocol Message Number
HASH KEY	18–var	var	Hash Key is present only when Requested Key Type is HASH KEY.

Request Type

Request Type indicates whether or not the request is relayed through a proxy.

Requested Key Type

The Requested Key Type field indicates the type of key requested. Interpretation of this field is defined in Table 11-90. The following restrictions apply for the Key Type for the CM_GET_KEY.REQ message.

Key Types DAK, TEK, and Nonce Only are never permitted.

Only Key Types NEK and HASH KEY are permitted over the PHY interface.

Key Type NEK is only allowed across the PHY interface if it is embedded in a CM_ENCRYPTED_PAYLOAD.IND message as described in Section 7.3.3; otherwise, the message received from the PHY interface shall be ignored.

Only Key Type NMK is permitted across the H1 interface.

NID

The NID field is the Network ID of the AVLN that the STA wants to join.

CM_GET_KEY.CNF

The CM_GET_KEY.CNF message usually is embedded within the encrypted payload of a CM_ENCRYPTED_PAYLOAD.IND message. However, it is also sent unencrypted as the second message in the UKE key distribution protocol to generate a TEK.

Table 1191: CM_GET_KEY.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
EKS	17	1	EKS or PEKS value depending upon Key Type. The four LSBs of this
Result	0	1	Result 0x00 = key granted 0x01 = request refused 0x02 = unsupported method/key type
			0x03 - 0xFF = reserved
Requested KeyType	1	1	Requested Key Type Interpretation of this field is the same as in Section 11.5.4.1.
My Nonce	2 - 5	4	Random number that will be used to verify next message from other end; in encrypted portion of payload.
Your Nonce	6 - 9	4	Last nonce received from recipient; it will be used to by recipient to verify this message; in encrypted portion of payload.
NID	10 - 16	7	Network ID of STEI STA The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.

EKS	17	1	EKS or PEKS value depending upon Key Type The four LSBs of this field contain the PEKS (refer to Section 11.5.3.11) or EKS (refer to Section 4.4.1.5.2.8). The four MSBs shall be set to 0x0. If nonce-only, set to 0x0F
PID	18	1	Protocol ID
PRN	19 - 20	2	Protocol Run Number
PMN	21	1	Protocol Message Number
Key	22 - var	var	Encryption or Hash Key

Requested Key Type

The Requested Key Type field indicates the type of key requested. Interpretation of this field is defined in Table 11-91. The following restrictions apply for the Key Type for the CM_GET_KEY.CNF message.

Key Types DAK, TEK, and Nonce Only are never permitted.

Only Key Types NEK and HASH KEY are permitted across the PHY interface.

Key Type NEK is only allowed across the PHY interface if it is embedded in a CM_ENCRYPTED_PAYLOAD.IND message as described in Section 7.3.3; otherwise, the message received from the PHY interface shall be ignored.

Only Key Type NMK is permitted across the H1 interface.

CM_SC_JOIN.REQ

Table 1192: CM_SC_JOIN.REQ Message

Field	**Octet Number**	**Bit Number**	**Field Size (Bits)**	**Definition**
CCo Capability	0	0 – 1	2	The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in Section 4.4.3.13.4.6.2.
RSVD		2-7	6	Reserved

CM_SC_JOIN.CNF

Table 1193: CM_SC_JOIN.CNF Message

Field	Octet Number	Bit Number	Field Size (Bits)	Definition

PCo Status		6	1	0b0 = STA is not a PCo 0b1 = STA is a PCo
NID	0	0 - 7	56	The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.
AVLN Status	7	0	1	0b0 = not authenticated with an AVLN 0b1 = authenticated with an AVLN
CCo Capability		1 – 2	2	The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in Section 4.4.3.13.4.6.2.
Proxy Network Capability		3	1	0b0 = does not support Proxy Networking 0b1 = fully supports Proxy Networking
Backup CCo Capability		4	1	0b0 = STA does not support Backup CCo function 0b1 = STA supports Backup CCo function
CCo Status		5	1	0b0 = STA is not the CCo 0b1 = STA is the CCo

PCo Status		6	1	0b0 = STA is not a PCo 0b1 = STA is a PCo
Backup CCo Status		7	1	0b0 = STA is not a Backup CCo 0b1 = STA is a Backup CCo

CM_CHAN_EST.IND

A STA uses this MME to send a new Tone Map to another STA. The STA receiving this MME should use the new Tone Map on subsequent transmissions.

Notes:

- The Tone Map field might not be present in the CM_CHAN_EST.IND message. A NEWTMI_AV value of 0x000 indicates the message was sent to update the interval information or to "refresh" the list of valid TMIs (i.e., keep them from becoming stale).
- The (NTMI_AV, TMI_AV[0], … , TMI_AV[L-1]) fields in CM_CHAN_EST.IND indicate the list of Tone Maps that are valid at the receiver (i.e., the STA that generated the CM_CHAN_EST.IND message). This list contains the set of Tone Maps that the receiver is expecting the transmitter to use subsequent to reception of this Management Message.
    - The receiver can still be required to decode MPDUs received with a TMI_AV that is not contained in the valid Tone Map list. For example, if the CM_CHAN_EST.IND contains a new Tone Map, TmiAvNew, that is intended to replace an existing Tone Map, TmiAvOld, the valid Tone Map list will not contain TmiAvOld. It is recommended the receiver keep the Tone Map associated with TmiAvOld until the transmitter starts using TmiAvNew or TmiAvOld becomes stale
    - The list shall also include the Default Tone Map Index.
    - A transmitter shall discontinue use of Tone Maps that are not included in the valid Tone Map list. If the valid Tone Map list is empty (i.e., NTMI = 0x00) the transmitter shall restart the initial channel estimation process (refer to Section 5.2.6.1.1).
- The (NINT, {ET[0], TMI_AV[0]}, … , {ET[M-1], TMI_AV[M-1]}) fields indicate intervals of time where each of the Tone Maps needs to be used. These intervals must cover the entire nominal Beacon Period length (i.e., 33.33 ms. or 40 ms. for 60/50 Hz). Therefore, the end time of the last interval shall be greater than or equal to the length of the Beacon Period.
- This message can be quite long, as the TMD (Tone Map Data) field is 4b x 917 tones = 458.5 octets long (binary encoding) when the default Tone Mask is used. When all carriers are turned on, Tone Map Data is 4b x 1155 tones = 577.5 octets long (binary encoded).
- INT_TMI_AV = 0xFF indicates an Unusable Interval.

• INT_TMI_AV = 0xFE indicates that an AC line cycle adapted Tone Map is not available for a particular Interval.			

Table 1194: CM_CHAN_EST.IND Message

Field	Octet Number	Field Size (Bits)	Definition
MaxFL_AV	0 - 1	16	Maximum number of Channel Adapted Tone Maps that the receiver can support on this channel (i.e., from the destination STA of this message to this station that generated this message). This number does not include any of the ROBO Tone Maps.
MAXTM	6	8	Maximum FL_AV that the receiver is capable of receiving, in multiples of 1.28 sec.
RIFS_AV_OneSym	2	8	Response Interframe Spacing for MPDUs with one OFDM Symbol
RIFS_AV_TwoSym	3	8	Response Interframe Spacing for MPDU with two OFDM Symbols
RIFS_AV_G2Sym	4	8	Response Interframe Spacing for MPDUs with more than two OFDM Symbols
RESPT	5	8	Response Type 0x00 –Default Tone Map transmitted as part of Initial Channel Estimation 0x01 – others 0x02-0xFF – reserved

SCL_CP MAXTM	8 6	8 8	Maximum number of Channel Adaptation MPDUs that the receiver can support on this channel. The value is determined by the STA and is constant. 0x00 = zero, (i.e., receiver is currently not capable of generating any Tone Maps) 0x01 = one, and so on
CP_TMI_AV	7	8	TMI_AV of Default Tone Map for Use in the CP The five LSBs of this field contain the TMI_AV (refer to Section 4.4.1.5.2.13. The three MSBs shall be set to 0b000. HomePlug GREEN PHY stations shall set this field to one of the ROBO Tone Maps.

NTMI_AV	10	8	Number of intervals during the Validation Period 0x00 = transmitter should send Sound MPDUs in intervals without an AC line cycle adapted Tone Map. 0x01 – MAX_TONE_MAP = number of intervals without an AC line cycle adapted Tone Map. 0xFF = reserved
SCL_CP	8	8	0x01 = transmitter should send MPDUs modulated using Default Tone Map in intervals without an AC line cycle adapted Tone Map. 0x02 – 0xFF = reserved
SCL_CFP	9	8	Sound Control during Contention Free Period 0x00 = transmitter should send Sound MPDUs in intervals without an AC line cycle adapted Tone Map. 0x01 = transmitter should send MPDUs modulated using Default Tone Map in intervals without an AC line cycle adapted Tone Map. 0x02 – 0xFF = reserved

NTMI_AV	10	8	Number of entries in the Valid TMI_AV List – L 0x00 = zero 0x01 = one, and so on up to MAX_TONE_MAPS
TMI_AV[0]	11	8	TMI_AV #0 The five LSBs of this field contain the TMI_AV (refer to Section 4.4.1.5.2.13. The three MSBs shall be set to 0b000.
...			
TMI_AV[L-1]	-	8	TMI_AV #L-1 The five LSBs of this field contain the TMI_AV (refer to Section 4.4.1.5.2.13. The three MSBs shall be set to 0b000.
NINT	-	8	Number of Intervals – M 0x00 = zero 0x01 = one, …, 0x20 = 32. 0x21 – 0xFF = reserved
ET[0]	-	16	End Time of first interval, in multiples of AllocationTimeUnit 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on The start time of the first interval is the same as Beacon Period Start Time.

INT_TMI_AV[0]	-	8	0x00 - 0x1F = TMI_AV of the AC line cycle adapted Tone Map for use in last interval (refer to Section 4.4.1.5.2 for the notes above). 0x20 - 0xFD = reserved
NEWTMI_AV	-	8	A value of 0x00 shall indicate that no new
...	-		
ET[M-1]	-	16	End Time of last interval, in multiples of AllocationTimeUnit 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on The start time of the M^{th} interval is the same as the end time of $(M-1)^{th}$ interval.
INT_TMI_AV[M-1]	-	8	0x00 - 0x1F = TMI_AV of the AC line cycle adapted Tone Map for use in last interval 0xFF, 0xFE = refer to the notes above. 0x20 - 0xFD = reserved

CBD_LEN	-	16	Number of Carrier Bit Loading Data Entries - The five LSBs of this field contain the value of CBD_LEN (refer to Section 4.4.1.5.2.13.
NEWTMI_AV	-	8	The three MSBs shall be set to 0b000. A value of 0x00 shall indicate that no new Tone Map is contained in this message. In such cases, the remainder of the fields in this message are not present.
CPF	-	8	CP Flag for the new Tone Map 0x00 = shall not be applied in the CP 0x01 = may be applied in the CP 0x02-0xFF = reserved
FECTYPE	-	8	FEC Type/Code Rate
GIL	-	8	Guard Interval Length
CBD_ENC	-	8	Carrier Bit Loading Data Encoding 0x00 = Carrier Bit Loading Data with Binary Encoding 0x01 = Carrier Bit Loading Data with Run Length Encoding 0x02-0xFF = reserved

CBD_LEN	-	16	Number of Carrier Bit Loading Data entries - N 0x000 = none 0x001 = one and so on.
CBD[0]	-	4	Carrier Bit Loading Data [0]
…			
CBD[N-1]	-	4	Carrier Bit Loading Data [N-1]
PAD	-	4	Optional 4-bit pad to make the CM_CHAN_EST.IND message an integral number of octets

MaxFL_AV

MaxFL_AV indicates the maximum value of the FL_AV that the receiver is capable of receiving, in multiple of 1.28 sec. MaxFL_AV shall be a value in the range 0x07A2 to 0x0FFF, inclusive.

Note: A value of 0x07A2 indicates MaxFL_AV of 2501.12 sec.

RIFS_AV_OneSym

RIFS_AV_OneSym indicates the Response Interframe Spacing to be used for unicast MPDU transmissions with negotiated TMs (i.e., TMI_AV in the range 0b00100 – 0b11111) containing one OFDM Symbol. The interpretation of this field is shown in Table 11-95.

RIFS_AV_TwoSym

RIFS_AV_TwoSym indicates the Response Interframe Spacing to be used for unicast MPDU transmissions with negotiated TMs (i.e., TMI_AV in the range 0b00100 – 0b11111) containing two OFDM Symbol. The interpretation of this field is shown in Table 11-95.

RIFS_AV_G2Sym

RIFS_AV_G2Sym indicates the Response Interframe Spacing to be used for unicast MPDU transmissions with negotiated TMs (i.e., TMI_AV in the range 0b00100 – 0b11111) containing more than two OFDM Symbols. The interpretation of this field is shown in Table 11-95.

All ROBO modulated MPDUs shall use a Response Interframe Spacing of RIFS_AV_default.

Table 1195: RIFS_AV, RIFS_AV_OneSym, and RIFS_AV_TwoSym Interpretation

RIFS_AV_OneSym, RIFS_AV_TwoSym, RIFS_AV_G2Sym Value	Interpretation
0x00 – 0x17	Reserved
0x18 – 0x7D	Response Interframe Spacing, in multiples of 1.28 μsec
0x7E – 0xFF	Reserved

FEC Type/Code Rate (FECTYPE)
The FEC Type/Code Rate is an 8-bit field that indicates the FEC type and code rate for the corresponding Tone Map.
Table 1196: FEC Type/Code Rate Interpretation

FECTYPE Value	Interpretation
0x00	½ rate Turbo Convolution Encoder coding
0x01	16/21 rate Turbo Convolution Encoder coding (not required for GREEN PHY)
0x02 - 0xFF	Reserved

Guard Interval Length (GIL)
The Guard Interval Length (GIL) field is an 8-bit field that encodes the length of the guard interval used on symbols transmitted using this Tone Map. Three GI lengths are supported, as in Table 11-97.

Table 1197: Guard Interval Length Interpretation

GIL Value	Length of Guard Interval
0x00	GI_{417}
0x01	GI_{567}
0x02	GI_{3534}
0x03 - 0xFF	Reserved

Carrier Bit Loading Data Encoding (CBD_ENC)
The Carrier Bit Loading Encoding (CBD_ENC) field is an 8-bit field that indicates the encoding used for presenting the modulation level for all unmasked carriers.
Table 1198: CBD_ENC Interpretation

CBD_ENC Value	Interpretation
0x00	Binary Encoding is used
0x01	Run Length Encoding is used
0x02- 0xFF	Reserved

Carrier Bit Loading Data (CBD)
Carrier Bit Loading Data contains a list of Modulation Types for every unmasked carrier. The format of the data may be Binary Encoding or Run Length Encoding.
Binary Encoding (CBD_ENC=0x00)
In Binary Encoding, each 4-bit Modulation Type field indicates the modulation of each unmasked carrier, starting from the lowest frequency carrier. The total number of entries shall equal the total number of unmasked carriers. Masked carriers are not included.
Table 1199: Interpretation of Modulation Type

Modulation Type	Interpretation
0x0	Empty Tone (refer to Section 3.5.1). Empty tones are not modulated with data.
0x1	BPSK

0x2	QPSK
0x3	8-QAM
0x4	16-QAM
0x5	64-QAM
0x6	256-QAM
0x7	1024-QAM
0x8 - 0xF	Reserved

Run Length Encoding (CBD_ENC=0x01)

Run Length Encoding can be applied to the Binary Encoded Tone Map Data to reduce the number of octets required to indicate modulation information on each unmasked carrier.

Note: CBD_LEN is equal to the total number of nibbles after Run Length Encoding has been applied.

Run Length Encoding is applied starting from the lowest frequency unmasked carrier. For each run of one or more carriers that use the same modulation, there will be an entry that provides the modulation and the length of the run. The entry may be one, two, or three nibbles long. The first nibble will always have its most-significant bit equal to zero. Any additional nibbles in the entry will always have their most-significant bit equal to one.

The first nibble indicates the Modulation Type, as shown in Table 11-100 If the next unmasked carrier has a different modulation, then this ends the entry. If only the next unmasked carrier has the same modulation, then this also ends the entry (and the next carrier's modulation is encoded in the same way, using the binary encoding). If there are K adjacent unmasked carriers with the same modulation, and 2<K<11, then the next nibble encodes the run length as shown in Table 11-101. If there are K adjacent unmasked carriers with the same modulation, and 10<K<75, then the next two nibbles encode the run length as shown in Table 11-101.

If the run length is greater than 74, then another entry is used to encode the remaining carrier modulations in the run.

Table 11100: Single Nibble Run Length Interpretation

Single Nibble Run Length Value	Interpretation
0x8	Run length = 3
0x9	Run length = 4
0xA	Run length = 5
0xB	Run length = 6
0xC	Run length = 7
0xD	Run length = 8
0xE	Run length = 9
0xF	Run length = 10

Table 11101: Two Nibble Run Length Interpretation

Two Nibble Run Length Value	Interpretation
0x88	Run length = 11
0x89	Run length = 12

	0x8A	Run length = 13	Number of entries in
	…	…	the Valid TMI_AV
	0xFE	Run length = 73	List – L
NTMI_AV	0xFF	Run length = 74	0x00 = zero
CM_TM_UPDATE.IND	1	8	0x01 = one and so on

The Tone Map Update Indication message is used to modify a subset of unmasked carriers of a Tone Map. The updated Tone Map is assigned a new Tone Map Index. The index of the tone to update field in CBUD[0..N-1] is the index of the unmasked carrier, where the first unmasked carrier is index 0, and the maximum index value is the total number of unmasked carriers minus one. An index value i corresponds to the i+1 unmasked carrier entry of the Carrier Bit Loading Data (CBD) in the Channel Estimation Indication (refer to Section 11.5.10.8.1).

Notes:

- This index does not include masked carriers.
- The (NTMI_AV, TMI_AV[0], … , TMI_AV[L-1]) fields indicate the list of Tone Maps that are valid at the receiver (refer to Section 11.5.12).
- The (NINT, {ET[0], INT_TMI_AV[0]}, … , {ET[M-1], INT_TMI_AV[M-1]}) fields indicate intervals of time where each of the Tone Maps needs to be used (refer to Section 11.5.10).
- Tone Map Update Indication is intended for Tone Map updates only when the size of this message is smaller than a Channel Estimation Indication.
- INT_TMI_AV = 0xFF indicates an Unusable Interval.
- INT_TMI_AV = 0xFE indicates that an AC line cycle adapted Tone Map is not available for a particular Interval.
- The Old Tone Map (i.e., OLD TMI_AV) used to generate the updated Tone Map (i.e., New TMI_AV) might or might not be invalidated by the receiver. In all cases, the list of valid Tone Maps shall be used by the transmitter to determine which Tone Maps are invalidated.

Table 11102: Tone Map Update Information

Field	Octet Number	Field Size (Bits)	Definition
CP_TMI_	0	8	TMI of Default Tone Map The five LSBs of this field contain the TMI_AV (refer to Section 4.4.1.5.2.13. The three MSBs shall be set to 0b000.

INTNTMI_AV [0]	1	8	Number of Entries in the Valid TMI_AV List – L 0x00 = zero 0x01 = one and so on up to MAX_TONE_MAPS
TMI_AV [0]	2	8	TMI_AV #0 The five LSBs of this field contain the TMI_AV (refer to Section 4.4.1.5.2.13. The three MSBs shall be set to 0b000.
…			
TMI_AV [L-1]	-	8	TMI_AV #L-1 The five LSBs of this field contain the TMI_AV (refer to Section 4.4.1.5.2.13. The three MSBs shall be set to 0b000.
NINT	-	8	Number of Intervals – M 0x01 = one, , …, 0x20 = 32 0x21 – 0xFF = reserved
ET[0]	-	16	End Time of first interval, in multiples of AllocationTimeUnit 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on The start time of the first interval is the same as Beacon Period Start Time.

INT_TMI_AV [0]	-	8	0x00 – 0x1F = TMI_AV of Tone Map resulting after Update. The 5 LSBs of this field contain the TMI_AV of Tone Map for use in first interval. 0xFF, 0xFE = refer to the notes above 0x20 - 0xFD = reserved
...			
NEW TMI_AV	-	8	End Time of last interval, in multiples of AllocationTimeUnit 0x0000 = zero 0x0001 = one AllocationTimeUnit, and so on The start time of the M^{th} interval is the same as the end time of $(M-1)^{th}$ interval.
ET[M-1]	-	16	
INT_TMI_AV [M-1]	-	8	0x00 – 0x1F = TMI_AV of Tone Map for use in first interval 0xFF, 0xFE = refer to the notes above. 0x20 - 0xFD = reserved
OLD TMI_AV	-	8	TMI_AV of the Tone Map to update The 5 LSBs of this field contain the TMI_AV (refer to Section 4.4.1.5.2.13). The three MSBs shall be set to 0b000.

NEW TMI_AV	-	8	TMI_AV of the Tone Map resulting after updates. The 5 LSBs of this field contain the TMI_AV (refer to Section 4.4.1.5.2.13. The three MSBs shall be set to 0b000. A value of 0x00 shall indicate that no new Tone Map is contained in this message. In such cases, the remainder of the fields in this message are not present and the OLD TMI_AV field shall be ignored.
CPF	-	8	CP Flag for the new Tone Map 0x00 = shall not be applied in the CP 0x01 = may be applied in the CP 0x02-0xFF = reserved
FECTYPE	-	8	New FEC Type/Code Rate
GIL	-	8	New Guard Interval Length
CBUD_LEN	-	16	Number of the Carrier Bit Loading Update Data Entries - N 0x0000 = no CBUD field (i.e., only changes to FEC type & guard interval length) 0x0001 = one CBUD field, and so on.

CBUD[0]	-	16	Carrier Bit Loading Update Data [0] b0 - b11 = index of tone to update b12 - b15 = modulation type (refer to Table 11-99)
…			
CBUD[N-1]	-	16	Carrier Bit Loading Update Data [N-1] b0 - b11 = index of tone to update b12 - b15 = modulation type (refer to Table 11-99)_

CM_AMP_MAP.REQ

A STA uses this MME to send a new amplitude map to another STA. The STA receiving this MME shall adjust the amplitude of each unmasked carrier according to the new amplitude map and its amplitude map on all subsequent transmissions. Each 4-bit AMDATA field indicates the TX Amplitude Reduction of each unmasked carrier, starting from the lowest frequency carrier. The total number of entries shall equal the total number of unmasked carriers. Note that masked carriers are not included. The interpretation of the 4-bit AMDATA field for each unmasked carrier is shown in Table 324. The default value for AMDATA for each unmasked carrier is 0b0000 (no reduction).

Reception of a CM_AMP_MAP.REQ message shall cause the STA to respond with a CM_AMP_MAP.CNF message.

Table 11103: Amplitude Update Indication

Field	Octet Number	Field Size (Bits)	Definition
AMLEN	0 - 1	2	Number of Amplitude Map Data Entries – N 0x0000 = zero 0x0001 = one, and so on
AMDATA[0]	-	4	Amplitude Map Data – First Unmasked Carrier
…	…		…
AMDATA[N-1]	-	4	Amplitude Map Data – Last Unmasked Carrier

CM_AMP_MAP.CNF

A STA shall generate a CM_AMP_MAP.CNF message in response to the corresponding

CM_AMP_MAP.REQ.			Number of Bridged Destinations = L
NBDA	1	1	0x00 = none

Table 11104: CM_AMP_MAP.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
ResType	0	1	Response Type 0x00 = success 0x01 = failure 0x02 - 0xFF = reserved

CM_BRG_INFO.REQ

CM_BRG_INFO.REQ is a request to provide Bridging Information. The message field for this MME is NULL.

CM_BRG_INFO.CNF

The CM_BRG_INFO.CNF message contains the set of stations to which the current station is acting like a bridge.

Table 11105: Bridging Information Response

Field	Octet Number	Field Size (Octets)	Definition
BSF	0	1	Bridging Station Flag 0x00 = this station does not perform bridging functions and the remaining fields are not valid. 0x01 = this station does perform bridging functions and the remainder of the fields are valid. 0x02 – 0xFF = reserved
BIVF	-	Var	Indicates the Number of Stations for which the station is bridging. The format of this field is shown in Table 11-106) .

Table 11106: Bridging Information Variable Field (BIVF)

Field	Octet Number	Field Size (Octets)	Definition
BTEI	0	1	STEI of the Bridge

NBDA	1	1	Number of Bridged Destinations L belonging to the connection. The value of this field is described in Section 6.3.
BDA[0]	2 - 7	6	Bridged Destination Address
...	…	…	…
BDA[L-1]	-	6	Bridged Destination Address - (L-1)
Classifier Rule Set	-	Var	This field shall always be set to 0x00 – to identify packets belonging to the 0x01 – connection. And so on

Bridge TEI (BTEI)

The Bridge TEI field is the STEI of the AV Bridge that is sending the Bridging Information Response message.

Number of Bridge Destination Addresses (NBDA)

The Number of Bridge Destination Addresses field corresponds to the number of BDA fields included in the message.

Bridged Destination Address [i] (BDA[i])

The Bridged Destination Address [i] field carries the 48-bit address of the *i*th station to which the station is bridging.

CM_CONN_NEW.REQ

The CM_CONN_NEW.REQ message is a request from the station that is initiating the Connection to the terminating station(s) to add a new Connection.

Table 11107: CM_CONN_NEW.REQ Message

Field Name	Octet Number	Field Size (Octets)	Description
CID	12 - 13	2	Connection Identifier of the Connection being negotiated (refer to Section 5.2.1.4.2)
CSPEC	-	Var	Connection Specification of the new Connection. The interpretation of this field is the same as in Section 7.8.1.

Classifier Rule Set	-	Var	Classifier Rule Set to identify packets belonging to the connection. The format of this field is described in Section 6.3. This field shall always be present. When there is no reverse link, the Number of Classifier Rules shall be set to 0x00 to indicate that there is no classifier rule. When there is a reverse link, a valid Classifier Rule Set shall be present.

CM_CONN_NEW.CNF

The CM of the terminating STA of a Connection sends the CM_CONN_NEW.CNF message to indicate whether the corresponding CM_CONN_NEW.REQ was accepted or not.

Table 11108: CM_CONN_NEW.CNF Message

Field Name	Octet Number	Field Size (Octets)	Description
CID	0 - 1	2	This field is the Connection ID of the Connection being negotiated (refer to Section 5.2.1.4.2)
Proposed CSPEC LLID-R	- 2	Var 1	Proposed CSPEC indicating the CSPEC that the CM is currently capable of supporting. Reverse Local Link ID This field shall be set to 0x00, if the Reverse Link is not present.
Result	3	1	Specifies the result of the Connection request. 0x00 = success 0x01 = failure – Classifier Rule Set cannot be supported 0x02 = failure – Classifier resources are not available 0x03 = failure – Maximum connection limit of the STA is reached 0x04 = failure – other. In this case, a Proposed CSPEC may be present 0x05 – 0xFF = reserved

Proposed CSPEC	-	Var	Proposed CSPEC indicating the CSPEC that the CM is currently capable of supporting. This field is only present when Result is set to 0x04. When this field is present and a valid Proposed CSPEC is not included, this field shall be 2 octets long with a value of 0x0000 (i.e., CSPEC_LEN = 0x0000). When a valid Proposed CSPEC is included, the interpretation of this field is the same as in Section 7.8.1.

CM_CONN_REL.IND

The CM_CONN_REL.IND message is used to indicate the release of a Connection. This message is sent to all stations that are part of the Connection.

Table 11109: CM_CONN_REL.IND Message

Field Name	Octet Number	Field Size (Octets)	Description
CID	0 - 1	2	Connection ID of the Connection being released (refer to Section 5.2.1.4.2).
Reason Code	2	1	Specifies the Cause of the Release 0x00 = normal release 0x01 = release due to violation of CSPEC, Violated CSPEC field is present 0x02 – 0xFF = reserved
Violated CSPEC	-	Var	Violated CSPEC indicating the fields of the CSPEC that are violated. This field is only present when Reason Code is set to 0x01. When this field is present and a valid Violated CSPEC is not included, this field shall be 2 octets long, with a value of 0x0000 (i.e., CSPEC_LEN = 0x0000). When a valid Violated CSPEC is included, the interpretation of this field is the same as in Section7.8.1.

CM_CONN_REL.RSP

The CM_CONN_REL.RSP message is transmitted in response to the corresponding

CM_CONN_REL.IND message. This message indicates successful release of a Connection.

Table 11110: CM_CONN_REL.RSP Message

Field Name	Octet Number	Field Size (Octets)	Description
Result	2	1	Result of the Connection Modification Request 0x00 – success 0x01 – failed
CID	0 - 1	2	Connection ID of the Connection that is released (refer to Section 5.2.1.4.2).

CM_CONN_MOD.REQ

The CM_CONN_MOD.REQ message is used to initiate Connection reconfiguration. It contains a proposal for the revised CSPEC.

Table 11111: CM_CONN_MOD.REQ Message

Field Name	Octet Number	Field Size (Octets)	Description
CID	0 - 1	2	Local Connection ID of the Connection being negotiated (refer to Section 5.2.1.4.2).
Modified CSPEC	-	Var	Modified CSPEC containing the (complete) new CSPEC that is requested for the Connection. The interpretation of this field is the same as in Section 7.8.1.

CM_CONN_MOD.CNF

The CM_CONN_MOD.CNF message indicates whether the corresponding CM_CONN_MOD.REQ was successful.

Table 11112: CM_CONN_MOD.CNF Message

Field Name	Octet Number	Field Size (Octets)	Description
CID	0-1	2	Connection ID of the Connection being negotiated (refer to Section 5.2.1.4.2)

Result	2	1	Request Type 0x00 = request to provide information for all active 0x01 = failed, Proposed SCPED field is present 0x02 – 0xFF = reserved
ReqType	0	1	Proposed CSPEC indicating the CSPEC that the CM is currently capable of supporting. This field is only present when Result is set to 0x01. When this field is present
Proposed CSPEC	-	Var	and a valid Proposed CSPEC is not included, this field shall be 2-octets long with a value of 0x0000 (i.e., CSPEC_LEN = 0x0000). When a valid Proposed CSPEC is included, the interpretation of this field is the same as in Section 7.8.1.

CM_CONN_INFO.REQ

The **CM_CONN_INFO.REQ** message is a request to provide the information on ongoing Connections that are either initiated or terminated at the STA. This message can be sent by any STA in the AVLN to any other STA.

Table 11113: CM_CONN_INFO.REQ Message

Field Name	Octet Number	Field Size (Octets)	Description

ReqType	0	1	Request Type 0x00 = request to provide information for all active Connections 0x01 = request to provide information for a Connection with the specified CID 0x02 = request to provide information for a Connection to which the specified Global Link belongs 0x03 - 0xFF = reserved
CID	1 - 2	2	Connection Identifier of the Connection for which the Connection information is requested. This field is only valid when ReqType is set to 0x01.
GLID	3	1	Global Link Identifier for which the associated Connection information is requested This field is only valid when ReqType is set to 0x02.

CM_CONN_INFO.CNF

The CM_CONN_INFO.CNF message is generated in response to the corresponding CM_CONN_INFO.REQ. CM_CONN_INFO.CNF contains the information about the source, destination, connection identifier, link identifiers and CSPEC of the Connection(s).

LID-R	5	1	Link ID of the

For Connections with only local links, the CSPEC shall include CM-to-CM QoS and MAC Parameters for both forward (if any) and reverse (if any) links.
For Connections that are initiated by the STA and containing Global Links, the CSPEC shall include CM-to-CM and CM-to-CCo QoS and MAC Parameters for both forward (if any) and reverse (in any) links.
For Connections that are not initiated by the STA and containing Global Links, the CSPEC shall include CM-to-CM QoS and MAC parameters for both forward (if any) and reverse (in any) links.

Table 11114: CM_CONN_INFO.CNF Message

Field Name	Octet Number	Field Size	Description
NumConn	7	1	Number of Connections = N 0x00 = no active connections or Unknown Connection Identifier or Unknown GLID 0x01 = one ConnInfo Field, 0x02 = two ConnInfo Fields, and so on
ConnInfo[1]	-	Var	Connection Information
…			
ConnInfo[N]	-	Var	Connection Information

Table 11115: Format of ConnInfo

Field Name	Octet Number	Field Size	Description
CID	0 - 1	2	Connection Identifier of the Link (refer to Section 5.2.1.4.2)
STEI	2	1	TEI of the source STA.
DTEI	3	1	TEI of the sink STA.
LID-F	4	1	Link ID of the Forward Link. A value of 0x00 is used to indicate that this field is invalid.

LID-R	5	1	Link ID of the Reverse Link. A value of 0x00 is used to indicate that this field is invalid.
CSPEC	-	Var	Connection Specification

CM_STA_CAP.REQ

The CM_STA_CAP.REQ message is a request to provide the station capabilities. The message field for this management message is NULL.

CM_STA_CAP.CNF

The CM_STA_CAP.CNF message is generated in response to the corresponding CM_STA_CAP.REQ.

Table 11116: CM_STA_CAP.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
AVVersion	0	1	HomePlug AV Version. AV 1.1 and GREEN PHY stations shall set this field to 0x00. Other values are reserved.
MACAddr	1 - 6	6	MAC Address
OUI	7 - 9	3	Organizationally Unique Identifier
AutoConnect	10	1	Auto Connect Capability 0x00 = Auto Connect Service not supported 0x01 = Auto Connect Service supported 0x02 - 0xFF = reserved
Smoothing	11	1	Smoothing Capability 0x00 = Smoothing Service not supported 0x01 = Smoothing Service supported 0x02 - 0xFF = reserved

TwoSymFC CCoCapability	17 12	1 1	CCo Capability The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in Section 4.4.3.15.4.6.2. The six MSBs of this field are set to 0b000000
ProxyCapable	13	1	Proxy Capability 0x00 = not capable of being a Proxy Coordinator 0x01 = capable of being a Proxy Coordinator 0x02 - 0xFF = reserved
BackupCCo	15	1	Backup CCo-capable 0x00 = Backup CCo capability not supported 0x01 = Backup CCo capability supported 0x02 - 0xFF = reserved
SoftHandOver	16	1	Soft Hand Over Support 0x00 = Soft Handover not supported 0x01 = Soft Hand Over supported 0x02 - 0xFF = reserved

TwoSymFC	17	1	Two Symbol Frame Control 0x00 = not supported 0x01 = supported 0x02 - 0xFF = reserved
MaxFL_AV	18 - 19	2	Maximum value of FL_AV that the station is capable of supporting in multiples of 1.28 sec. 0x00 = zero 0x01 = 1.28 sec, and so on
Bidirectional Bursting	23	1	Bidirectional Bursting Capability 0x00 = not supported 0x01 = supported 0x02 - 0xFF = reserved
HomePlug1.1Cap	20	1	Ability to Support Enhanced Coexistence with HomePlug 1.1 0x00 = not capable of supporting HomePlug 1.1 coexistence 0x01 = capable of supporting HomePlug 1.1 coexistence 0x02 – 0xFF = reserved
HomePlug1.0Interop	21	1	HomePlug 1.0.1 Interoperability 0x00 = not capable of interoperating with HomePlug 1.0.1 0x01 = capable of interoperating with HomePlug 1.0.1
RegulatoryCap	22	1	Capability of Operating in Various Regulatory Domains 0x00 = North America only 0x01 - 0xFF = reserved

NumNWs Bidirectional Bursting	0 23	1 1	Number of AVLNs Bidirectional Bursting Capability 0x00 = not capable of supporting Bidirectional Bursts 0x01 = capable of supporting Bidirectional Bursting. Only supports CFP Bidirectional Bursts ending with SACK 0x02 = capable of supporting Bidirectional Bursting. Supports CFP Bidirectional
			Bursts that either end with a SACK or a Reverse SOF. 0x03-0xFF = reserved
ImplementationVer	24 - 25	2	Implementation Version This field is defined by the chip and/or product manufacturers. It is intended to facilitate interoperability testing.

CM_NW_INFO.REQ

The CM_NW_INFO.REQ message is a request to provide the list of AVLNs to which the STA is a member and the relevant information about the AVLN. The message field for this management message is NULL.

CM_NW_INFO.CNF

CM_NW_INFO.CNF message is generated in response to the corresponding CM_NW_INFO.REQ.

Table 11117: CM_NW_INFO.CNF Message

Field	Octet Number	Field Size (Octets)	Definition

SNID	7	1	Short Network Identifier. If STA is a member of any AVLN, then the least-significant 4 bits of this field contain the SNID assigned to the STA by the AVLN's CCo. 0x00 = not a member of any AVLN 0x01 = member of one AVLN and so on. If STA is member of multiple networks, NWINFO[0] contains the information about the AVLN whose PHY Clock the STA is tracking (refer to Section 5.5.4.1).
NumNWs	0	1	Number of AVLNs that the STA is a member of.
NWINFO[0]	-	Var	Network Information of the first AVLN (refer to Table 11-118)
…			
NWINFO[N-1]	-	Var	Network Information of the last AVLN (refer to Table 11-118)

Table 11118: NWINFO Field Format

Field	Octet Number	Field Size (Octets)	Definition
NID	0 - 6	7	Network Identifier The least-significant 54 bits of this field contains the NID of the AVLN. The remaining 2 bits are set to 0b00.

SNID	7	1	Short Network Identifier The least-significant 4 bits of this field contains the Short Network Identifier. The remaining 4 bits are set to 0x0
TEI	8	1	Terminal Equipment Identifier of the STA in the AVLN
StationRole	9	1	Role of the station in the AVLN 0x00 = STA 0x01 = Proxy Coordinator 0x02 = CCo 0x03 – 0xFF = reserved
CCo_MACAddr	10 - 15	6	MAC Address of the CCo of the network.
Access	16	1	Access Network 0x00 = This NID corresponds to an in-home network 0x01 = This NID corresponds to an Access Network 0x02 - 0xFF = reserved
NumCordNWs	17	1	Number of Neighbor Networks that are coordinating with the AVLN 0x00 = none (Un-Coordinated mode) 0x01 = one Coordinating network, and so on

CM_GET_BEACON.REQ

The CM_GET_BEACON.REQ message is a request to provide the Beacon Payload field of a recently received Central Beacon or Proxy Beacon (if station cannot hear the Central Beacon) of an

AVLN to which the STA is a member.			Request Type 0x00 = request to provide the manufacturer-set NID of the STA 0x01 = request to provide the user-set NID of the STA 0x02 = request to provide the HFID of the Network, whose network identifier is contained in the NID field 0x03 = request to set the user-set HFID of the STA to the value indicated in the HFID
Table 11119: CM_GET_BEACON.REQ Message			
Field	Octet Number	Field Size (Octets)	Definition
NID	0 - 6	7	Network Identifier of the AVLN to which the STA is a member. The least significant 54 bits of this field contains the NID. The remaining two bits are set to 0b00.
ReqType	0	1	

CM_GET_BEACON.CNF

The CM_GET_BEACON.CNF message is generated in response to the corresponding CM_GET_BEACON.REQ. The format and interpretation of the fields in this message are same as shown in Table 4-52 “Beacon Payload Field” and Table 4-52b “Assignment of Previously Reserved Beacon Payload Fields for GREEN PHY” except tjat the Octet Pad and Beacon Payload Check Sequence fieldsare not included.

CM_HFID.REQ

The CM_GET_HFID.REQ message is a request to provide the Human Friendly Identifier of a STA or an AVLN.

Table 11120: CM_HFID.REQ Message

Field	Octet Number	Field Size (Octets)	Definition

NID	-	0 or 6	Network Identifier The least significant 54 bits of this field contain the NID. The remaining 2 bits are set to 0. This field is only present when ReqType is 0x01 or 0x02
ReqType	0	1	0x00 = request to provide the HFID of the STA 0x01 = request to provide the user-set HFID of the STA 0x02 = request to provide the HFID of the Network, whose network identifier is contained in the NID field 0x03 = request to set the user-set HFID of the STA to the value indicated in the HFID field 0x04 = request to set the HFID of the Network, whose network identifier is contained in the NID field, to the value indicated in the HFID field. 0x05 - 0xFF = reserved Note: This message must be sent to the CCo of an AVLN to set the HFID of the Network

NID	-	0 or 6	Network Identifier The least-significant 54 bits of this field contains the NID. The remaining two bits are set to 0b00. This field is only present when ReqType is set to 0x02 or 0x04.
HFID	-	0 or 64	Human Friendly Identifier This field is only present when ReqType is set to 0x03 or 0x04.

CM_HFID.CNF

The CM_HFID.CNF message is generated in response to the corresponding CM_HFID.REQ.

Table 11121: CM_HFID.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
ResType	0	1	Response Type 0x00 - 0x04 = success, with value indicating the Request's Req Type 0xFF = failure 0x05 - 0xFE = reserved
HFID	-	0 or 64	Human Friendly Identifier of the STA or AVLN This field is always present. When Res Type is fail, the current value is returned.

CM_MME_ERROR.IND

CM_MME_ERROR.IND message shall be generated by a station upon the reception of MME that it does not support. This message may also be generated in response to the reception of a supported MME with invalid MME field(s).

Table 11122: CM_MME_ERROR.IND Message

Field	Octet Number	Field Size (Octets)	Definition
NumSTAs	7	1	Number of AV STAs in the AVLN = L
ReasonCode	0	1	Reason Code 0x00 = MME not Supported 0x01 = supported MME with invalid MME fields 0x02 = unsupported feature 0x03 - 0xFF = reserved
RX_MMV	1	1	Management Message Version of the received MME
RX_MMTYPE	2-3	2	Management Message Type of the received MME
InvalidByteOffset	4-5	2	Byte Offset of first or only invalid field in MME. This field is only valid when the Reason Code is set to 0x01. 0x00 = first Octet of the MME 0x01 = second Octet of the MME, and so on.

CM_NW_STATS.REQ

The CM_NW_STATS.REQ message is a request to provide the network statistics. The message field for this management message is NULL.

CM_NW_STATS.CNF

The CM_NW_STATS.CNF message is generated in response to the corresponding CM_NW_STATS.REQ. This message contains the list of all associated and authenticated STAs in the AVLN and the physical layer data rates to all those stations.

Table 11123: CM_NW_STATS.CNF Field Format

Field	Octet Number	Field Size (Octets)	Definition

NumSTAs	7	1	Number of AV STAs in the AVLN = L 0x00 = None, 0x01 = One, and so on.
DA[0]	-	6	MAC Address of the STA – 0
AvgPHYDR_TX[0]	-	1	Average PHY Data Rate in Mega Bits per second from STA to DA[0]. 0x00 = unreachable/ unknown 0x01 = 1 Mbps, and so on
AvgPHYDR_RX[0]	-	1	Average PHY Data Rate in Mega Bits per second from DA[0] to STA. 0x00 = unreachable/ unknown 0x01 = 1 Mbps, and so on
…			
DA[L-1]	-	6	MAC Address of STA – (L-1)
AvgPHYDR_TX[L-1]	-	1	Average PHY Data Rate in Mega Bits per second from STA to DA[L-1]. 0x00 = unreachable/ unknown, 0x01 = 1 Mbps, and so on
AvgPHYDR_RX[L-1]	-	1	Average PHY Data Rate in Mega Bits per second from DA[L-1] to STA. 0x00 = unreachable/ unknown 0x01 = 1 Mbps, and so on

LID	9	1	Link Identifier This field is valid only

CM_LINK_STATS.REQ
CM_LINK_STATS.REQ is a request to provide statistics for a Link that is associated with a Connection, or for Priority based Links or Management Links.

Table 11124: CM_LINK_STATS.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
ReqType	0	1	Request Type 0x00 = reset statistics for the corresponding Link 0x01 = get statistics for the corresponding Link 0x02 = get and reset statistics for the corresponding Link 0x03 - 0xFF = reserved
ReqID	1	1	Request Identifier The ReqID field is set by the sender of this MME such that the same value is not recently used between the sender and the receiver of this MME. Request ID is used to bind this request with the corresponding response.
NID	2-8	7	Network Identifier of the STA(s) whose Connection statistics are being requested. The least-significant 54 bits of this field contains the NID. The remaining 2 bits are set to 0b00.

LID	9	1	Link Identifier This field is valid only when the Mgmt_Flag is set to 0x00.
LinkStats TLFlag	- 10	Var 1	Transmit Link Flag 0x00 = transmit Link 0x01 = receive Link 0x02 - 0xFF = reserved
Mgmt_Flag	11	1	Management Link 0x00 = not management Link 0x01 = management Link 0x02 - 0xFF = reserved
DA/SA	12-17	6	Indicate the Destination MAC Address when TLFlag is set to 0x00. Indicate the Source Mac Address when TLFlag is set to 0x01.

CM_LINK_STATS.CNF

CM_LINK_STATS.CNF is generated in response to the corresponding CM_LINK_STATS.REQ.

Table 11125: CM_CONN_STATS.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
ReqID	0	1	Request Identifier copied from the corresponding request
ResType	1	1	Response Type 0x00 = success 0x01 = failure 0x02 - 0xFF = reserved

LinkStats	-	Var	Link Statistics for the Link. The format of this field depends on whether the Link is a “Transmit Link” or a “Receive Link” as shown in Table 11-126 and Table 11-127.

Table 11126: LinkStats Field Format for Transmit MFS

Field	Octet Number	Field Size (Octets)	Definition
BeaconPeriodCnt	0 - 1	2	Counter indicating the number of Beacon Periods over which Link statistics are collected 0x00 = zero 0x01 = one Beacon Period 0x02 = two Beacon Periods, and so on Note: The statistics collection may begin in the middle of a Beacon Period. In such cases, the partial Beacon Period is counted as the first Beacon Period.
Tx_NumMSDUs	2 - 5	4	Number of MSDUs Received from HLE 0x00000000 = none 0x00000001 = one, and so on
Tx_Octets	6 - 9	4	Number of Octets of MSDU Payload Received from HLE 0x00000000 = none 0x00000001 = one octet, and so on

Tx_NumSegs	10 - 13	4	Number of Segments That were Generated 0x00000000 = none 0x00000001 = one, and so on
Tx_NumSeg_Suc	14 - 17	4	Number of Segments That were successfully delivered. 0x00000000 = none 0x00000001 = one, and so on
Tx_NumSeg_Dropped	18 - 21	4	Number of Segments that were Dropped 0x00000000 = none 0x00000001 = one, and so on
Tx_NumPBs	22 - 25	4	Number of PBs Handed Over to the PHY for Transmission 0x00000000 = None 0x00000001 = one, and so on
Tx_NumMPDUs	26 - 29	4	Number of MPDUs That were Transmitted 0x00000000 = none 0x00000001 = one, and so on
Tx_NumBursts	30 - 33	4	Number of Bursts That were Transmitted 0x00000000 = zero 0x00000001 = one, and so on
Tx_NumSACKs	34 - 37	4	Number of MPDUs that were successfully acknowledged (i.e., SACK with MFSRsp set to ACK). 0x00000000 = none 0x00000001 = one, and so on

LatBin[N] NumLatBins	- 38	4 1	Number of BBs in Which Latency Information is Collected = N 0x00 = not available, In this case, the reminder of the fields are not present.
			0x01 = invalid 0x02 = two latency bins 0x03 = three latency bins and so on.
LatBinGran	39	1	Granularity of Latency Bin. 0x00 = one Beacon Period 0x01 = one millisecond 0x02 = two milliseconds 0x03 = and so on
LatBin(0)	40 - 43	4	Number of PBs successfully transmitted with a latency in the range [0 to LatBinGran] 0x00000000 = none 0x00000000 = one, and so on
LatBin(1)	-	4	Number of PBs successfully transmitted with a latency in the range (LatBinGran to 2* LatBinGran) 0x00000000 = none 0x00000001 = one, and so on
…			

Rx_NumSeg_Suc LatBin[N]	10 - 13 -	4 4	Number of SDs Segments Successfully Transmitted with a Latency > LatBinGran*(N-1) 0x00000000 = none
			0x00000001 = one, and so on

Table 11127: LinkStats Field Format for Receive MFS

Field	Octet Number	Field Size (Octets)	Definition
BeaconPeriodCnt	0 - 1	2	Counter indicating the number of Beacon Periods over which Link statistics are collected 0x00 = none 0x01 = one Beacon Period 0x02 = two Beacon Periods and so on. Note: The statistics collection may begin in the middle of a Beacon Period. In such cases, the partial Beacon Period is counted as the first Beacon Period.
Rx_NumMSDUs	2 - 5	4	Number of MSDUs Successfully Received 0x00000000 = none 0x00000001 = one, and so on
Rx_Octets	6 - 9	4	Number of Octets of MSDU Payload Successfully Received 0x00000000 = none 0x00000001 = one octet, and so on

Rx_NumSeg_Suc	10 - 13	4	Number of Segments that were successfully received. 0x00000000 = none 0x00000001 = one, and so on
Rx_NumSeg_Missed	14 - 17	4	Number of Segments that were missed. 0x00000000 = none 0x00000001 = one, and so on
Rx_NumPBs	18 - 21	4	Number of PBs that were handed over from the PHY to the MAC. 0x00000000 = none 0x00000001 = one, and so on
Rx_NumBursts	22 - 25	4	Number of Bursts That were Transmitted 0x00000000 = zero, 0x00000001 = one, and so on
Rx_NumMPDUs	26 - 29	4	Number of MPDUs That were Received. 0x00000000 = none 0x00000001 = one, and so on
NumICV_FAILS	30 - 33	4	Number of Received MAC Frame for which ICV Failed 0x00000000 = none 0x00000001 = one, and so on

- CM_STA_IDENTIFY.REQ (GREEN PHY)

The CM_STA_IDENTIFY.REQ message is a request to provide the STA identification information. The message field for this management message is NULL.

- CM_STA_IDENTIFY.CNF (GREEN PHY)

The CM_STA_IDENTIFY.CNF **message** is generated in response to the corresponding CM_STA_IDENTIFY.REQ. This message contains the GREEN PHY Capability and/or the version of HomePlug AV supported.

Table 11128: CM_STA_IDENTIFY.CNF Field Format

Field	Octet Number	Field Size (Octets)	Definition
Repeating and Routing Capability of GREEN PHY Capability	3 0	1 1	Repeating and Routing Capability of the station 0x00 – STA is not GREEN PHY Capability 0x01 – STA is HomePlug GREEN PHY 1.0 Capable 0x02-0xFF -- Reserved
Power Save Capability	1	1	Power Save Capability of the station 0x00 – STA has no Power Save Capability 0x01 – STA is Power Save Capable 0x02-0xFF -- Reserved
GP Preferred Allocation Capability	2	1	GP Preferred Allocation Capability of the station 0x00 – STA has no Capability to respect GP Preferred Allocation 0x01 – STA has Capability to respect GP Preferred Allocation 0x02-0xFF -- Reserved

EF Repeating and Routing Capability	- 3	Var 1	Repeating and Routing Capability 0x00 – STA does not support Repeating and Routing 0x01 – STA supports Repeating and Routing 0x02-0xFF -- Reserved
			Reserved
HomePlug AV Version	4	1	Version of HomePlug AV supported by the station 0x00 – HPAV 1.1 station 0x01 – 0xFE Reserved for future use 0xFF – Not a HPAV Station
EFL	5	1	Extended Fields Length 0x00 = No Extended Field 0x01 = 1 Octet extended Field, and so on

EF	-	Var	Extended Fields Extended Fields enable extensions to the contents of this MME. This field is expected to be used by future versions of HomePlug AV and Green PHY. This field is ignored by Green PHY 1.0 stations

- CM_STA_IDENTIFY.IND (GREEN PHY)

The CM_STA_IDENTIFY.IND **message** is sent from a GREEN PHY Station or a Station supporting versions of HomePlug AV greater than 1.1 that has just associated and authenticated with a CCo to convey its GREEN PHY Station Type or the version of HomePlug AV to the CCo. The format of this message is the same as the CM_STA_IDENTIFY.CNF message in Section 11.5.38.

- CM_STA_IDENTIFY.RSP (GREEN PHY)

The CM_STA_IDENTIFY.RSP message is sent by the CCo to the STA to confirm the reception of the CM_STA_IDENTIFY.IND message.

The message field for this message is NULL.

- CM_ROUTE_INFO.REQ (GREEN PHY)

The **CM_ROUTE_INFO**.REQ message is a request to provide the distant vector information. The message field for this management message is NULL.

- CM_ROUTE_INFO.CNF (GREEN PHY)

CM_ROUTE_INFO.CNF is generated in response to the corresponding **CM_ROUTE_INFO**.REQ and provides the requesting STA information from the LRT. This message shall contain an entry for every STA identified in the TEI Map except itself.

Table 11129: CM_ROUTE_INFO.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
NumEntries	0	1	Number of entries = L 0x00 = None, 0x01 = One, and so on.
UDTEI[0]	1	1	Ultimate destination TEI[0] for the MAC Frame

RDR[0]	2	1	RDR for UDTEI[0] from the LRT, which indicates the data rate from the STA sending this message to the UDTEI[0]
RNH[0]	3	1	RNH for UDTEI[0] from the LRT, which indicates the number of hops from the STA sending this message to the UDTEI[0] 0x00 = direct communication (1 hop) 0x01 = 2 hops, and so on
UDTEI[1]	4	1	Ultimate destination TEI[1] for the MAC Frame
RDR[1]	5	1	RDR for UDTEI[1] from the LRT, which indicates the data rate from the STA sending this message to the UDTEI[1]
RNH[1]	6	1	RNH for UDTEI[1] from the LRT, which indicates the number of hops from the STA sending this message to the UDTEI[1] 0x00 = direct communication (1 hop) 0x01 = 2 hops, and so on
...			
UDTEI[L-1]	3L+1	1	Ultimate destination TEI[L-1] for the MAC Frame

RDR[L-1]	3L+2	1	RDR for UDTEI[L-1] from the LRT, which indicates the data rate from the STA sending this message to the UDTEI[L-1]
RNH[L-1]	3L+3	1	RNH for UDTEI[L-1] from the LRT, which indicates the number of hops from the STA sending this message to the UDTEI[L-1] 0x00 = direct communication (1 hop) 0x01 = 2 hops, and so on

-
-
-
-
-
-

Route Data Rate (RDR[i])
The Route Data Rate (RDR) is encoded using the same method as used for the BLE (see Section 4.4.1.5.2.10), except that the rate encoded as **0x00** shall be used to indicate an unreachable UDTEI. A UDTEI shall be reported as unreachable to a neighbor if either no path to that UDTEI is known, or if the neighbor is the next STA in the path to that UDTEI (split horizon with poison reverse). Thus any RDR that is less than or equal to the RDR encoded as **0x01** shall be reported as **0x01**.

- CM_ROUTE_INFO.IND (GREEN PHY)

CM_ROUTE_INFO.IND message has the same format as **CM_ROUTE_INFO.**CNF and is sent to other STAs in the AVLN when there is a significant change in the LRT information. This message shall

include an entry for every entry in the LRT that changed significantly and may include an entry for every STA identified in the TEI Map except itself.

- CM_UNREACHABLE.IND (GREEN PHY)

CM_UNREACHABLE.IND is generated when a STA becomes unreachable. It is sent if the STA was reachable directly but is no longer directly reachable, or in response to receipt of a **CM_UNREACHABLE**.IND MME from the STA that is the current Next TEI for the now unreachable STA. This message shall contain an entry for every newly unreachable STA.

Table 11130: CM_ROUTE_INFO.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
UnrchTS	0-3	4	Value of the NTB when the STA was found unreachable
NumEntries	4	1	Number of entries = L 0x00 = reserved, 0x01 = One, and so on.
UDTEI[0]	5	1	Unreachable ultimate destination TEI[0]
UDTEI[1]	6	1	Ultimate destination TEI[1] for the MAC Frame
...			
UDTEI[L-1]	L+5	1	Ultimate destination TEI[L-1] for the MAC Frame

-
-

Unreachable Time Stamp (UnrchTS)

The 32-bit Unreachable Time Stamp (UnrchTS) Time Stamp field is the value of the NTB at the STA that first reported the newly unreachable STA as unreachable. It is copied verbatim by all STAs that generate a new **CM_UNREACHABLE**.IND MME because of receiving a **CM_UNREACHABLE**.IND MME.

- CM_SLAC_PARM.REQ (GREEN PHY)

CM_SLAC_PARM.REQ is generated by the HLE of an PEV to request the parameters for the SLAC protocol from the EVSE(s). The format of this message is shown in Table below.

Table 11131: CM_SLAC_PARM.REQ Message

Field	Octet Number	Field Size (Octets)	Definition

APPLICATION_TYPE	0	1	Application Type 0x00 : PEV-EVSE Association 0x01-0xFF: Reserved
SECURITY_TYPE	1	1	Security in M-Sound Messages 0x00: No Security 0x01: Public Key Signature 0x02-0xFF: Reserved
RunID	2-9	8	Run identifier of sender
CipherSuiteSetSize	10	1	**Cipher Suite Set Size** Number of supported cipher suites N. This field is only present when SECURITY_TYPE = 0x01
CipherSuite [1]	11-12	2	**Cipher Suite 1** First supported cipher suite. This field is only present when SECURITY_TYPE = 0x01
…	…	…	…
CipherSuite [N]	Var	2	**Cipher Suite N** Nth supported cipher suite. This field is only present when SECURITY_TYPE = 0x01

-

APPLICATION TYPE
This field identifies the context in which the SLAC process is being carried out. If the value is 0x00, then it is being used for PEV-EVSE matching. All other values are reserved. his field

indicates the MAC address of the GP STA(s) with which the STA should initiate the SLAC Process. If this MAC Address is set to the broadcast address (i.e., **0xFFFFFFFFFFFF**), the STA shall initiate the SLAC process with all of the GP STAs in the network using broadcast MPDUs.

SECURITY TYPE

This field indicates whether the sender prefers Secure SLAC for PEV-EVSE matching. If the value is 0x00, Secure SLAC is not desired, if the value is 0x01, Secure SLAC is requested. All other values are reserved.

RUN IDENTIFIER

This field is a value generated by the sender, unique for the sender. This field shall be chosen to be as unique as possible for each SLAC protocol run.

CIPHER SUITE SET SIZE

This field is an unsigned integer that specifies the number of cipher suites listed in the remainder of the message. If Secure SLAC is supported, this field shall be set to 0x01 (i.e., one Cipher Suite supported). Values of Cipher Suite set size greater than 1 are reserved for future use.

CIPHER SUITE [1] to CIPHER SUITE [N]

This field indicates a cipher suite supported by the sender and which may be used by another station sending signed messages to it or requesting encrypted messages from it.

PEVs and EVSEs that support secure SLAC shall set Cipher Suite to 0x00 to indicate that they support the following suite,

- ECDSA-with-SHA256 for signature (RFC 5754)
- Specify enveloped data using ephemeral-static ECDH key agreement algorithm for AES-128 key, dhSinglePass-stdDH-sha256kdf-scheme and id-aes128-wrap algorithm (RFC 5753),
- Specify enveloped data encryption using id-aes128-CBC (RFC 3565)

Note: The underlying cryptographic algorithms used in Cipher Suite 0x00 are required in SEP 2.0 (i.e., ECC Cipher Suite).

- CM_SLAC_PARM.CNF (GREEN PHY)

CM_SLAC_PARM.CNF is generated by the HLE of a EVSE GP STA in response to the corresponding **CM_SLAC_PARM.REQ**. During the SLAC Process, a GP STA shall transmit M-SOUND MPDUs to a target GP STA (i.e., M-SOUND_TARGET) so that the target GP STA can measure the attenuation profile (ATTEN_PROFILE) of the received signal. The format of this MME is as shown in Table 11-132.

Table 11132: CM_SLAC_PARM.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
M-SOUND_TARGET	0-5	6	Indicates the MAC address of the GP STA with which the STA shall initiate the Signal Level Attenuation Characterization Process.

NUM_SOUNDS	6	1	Indicates the number of M-SOUND MPDUS transmitted by the GP STA during the Signal Level Attenuation Characterization Process.
Time_Out	7	1	Indicates the amount of time within which the GP STA will complete the transmission of SOUND MPDUs during the Signal Level Attenuation Characterization Process. The time is in multiples of 100 msec. 0x00 – 0 msec 0x01 – 100 msec 0x02 – 200 msec, and so on.
RESP_TYPE	8	1	Indicates whether the recipient of the SOUND MPDUs shall communicate the signal attenuation characteristic profile data to the HLE or another GP STA. 0x00 – HLE of the STA 0x01 – Another GP STA 0x02 – 0xFF – Reserved

FORWARDING_STA	9-14	6	Indicates the MAC address of the GP STA to which the STA(s) participating in the SLAC Process shall forward the signal attenuation characteristic profile data. This field is valid only if RESP_TYPE is set to 0x01
APPLICATION_TYPE	15	1	Application Type 0x00 : PEV-EVSE Association 0x01-0xFF: Reserved
SECURITY_TYPE	16	1	Security in M-Sound Messages 0x00: No Security 0x01: Public Key Signature 0x02-0xFF: Reserved
RunID	11-18	8	Run identifier of sender
CipherSuite	19-20	2	**Cipher Suite** Selected cipher suite. This field is only present when SECURITY_TYPE = 0x01

•

M-SOUND_TARGET
This field indicates the MAC address of the GP STA(s) with which the STA should initiate the SLAC Process. If this MAC Address is set to the broadcast address (i.e., **0xFFFFFFFFFFFF**), the STA shall initiate the SLAC process with all of the GP STAs using multi-network broadcast MPDUs.
NUM_SOUNDS
This field indicates the maximum number of M-SOUND MPDUs transmitted by the STA during the SLAC Process.
Time_Out

This field indicates the time within which the STA completes transmit of SOUND MPDUs during the SLAC Process. The time is represented here in multiples of 100 msecs.			
RESP_TYPE			
SECURITY_TYPE	1	1	Security in M-Sound Messages 0x00: No Security

This field indicates the behavior of the GP STA(s) participating in the SLAC Process upon processing the M-SOUND MPDUs. The GP STA shall transmit the Signal Level Attenuation Profile data obtained from processing the M-SOUND MPDUs to the HLE if the field is set to **0x00** or to another GP STA if the field is set to **0x01**.

FORWARDING_STA

This field is set to the MAC address of the GP STA to which the STA(s) participating in the SLAC process shall transmit the Signal Level Attenuation Profile data to. This field is valid only when the **RESP_TYPE** is set to **0x01**.

APPLICATION TYPE

This field identifies the context in which the SLAC process is being carried out. If the value is 0x00, then it is being used for PEV-EVSE matching. All other values are reserved.

SECURITY TYPE

This field indicates whether the sender supports Secure SLAC for PEV-EVSE matching. If the SECURITY_TYPE in **CM_SLAC_PARM.REQ** is set to 0x00, then this field shall be set to 0x00. If the SECURITY_TYPE in **CM_SLAC_PARM.REQ** is set to 0x01 (i.e.., public key signature), and the Green PHY station supports one of the Cipher Suites provided in the **CM_SLAC_PARM.REQ**, then this field shall be set to 0x01.

RUN IDENTIFIER

RUN IDENTIFIER in this message shall be copied from the corresponding field in **CM_SLAC_PARM.REQ**.

CIPHER SUITE

If the SECURITY_TYPE is set to 0x01 (i.e., public key signature), then this field shall be set to 0x0000.

- CM_START_ATTEN_CHAR.IND (GREEN PHY)

A Green PHY STA that initiates a SLAC shall transmit **CM_START_ATTEN_CHAR.IND** to indicate to the target STAs (i.e., indicated by the SOUND_TARGET in the preceding **CM_SLAC_PARM.CNF**) that the SLAC Process is starting. This MME is generated in response to a **CM_SLAC_PARM.CNF**. This message shall be transmitted in multi-network broadcast mode. The Green PHY STA shall transmit this MME multiple times to increase the probability of reception of this MME by all the STAs in the network. The format of this MME is shown in Table 11-133

Table 11133: CM_START_ATTEN_CHAR.IND Message

Field	Octet Number	Field Size (Octets)	Definition
APPLICATION_TYPE	0	1	Application Type 0x00 : PEV-EVSE Association 0x01-0xFF: Reserved

SECURITY_TYPE	1	1	Indicates the Security Mode within which the CM_SLAC_PARM.CNF message is sent. 0x00 – No Security 0x01 – Public Key Signature 0x02-0xFF – Reserved
ACVarField	1	var	Variable Field

•

APPLICATION TYPE

This field identifies the context in which the SLAC process is being carried out. Its interpretation is the same as in 11.5.45.1.

SECURITY TYPE

This field indicates whether or not Secure SLAC is used, as in 11.5.45.2.

ACVarField

If Security Type = 0x01, then it is CMS-formatted signed contents, with the contents given in Table XXX below. If Security Type = 0x00, then it is the contents given in Table 11-134 below without CMS formatting.

Table 11134: CM_START_ATTEN_CHAR.IND Message

Field	Octet Number	Field Size (Octets)	Definition
NUM_SOUNDS	0	1	Indicates the number of SOUND MPDUS transmitted by the GP STA during the Signal Level Attenuation Characterization Process.

Time_Out	1	1	Indicates the amount of time within which the GP STA will complete the transmission of SOUND MPDUs during the Signal Level Attenuation Characterization Process. The time is in multiples of 100 msec. 0x00 – 0 msec; 0x01 – 100 msec; 0x02 – 200 msec, and so on.
RESP_TYPE	2	1	Indicates whether the recipient of the SOUND MPDUs shall communicate the signal attenuation characteristic profile data to the HLE or another GP STA. 0x00 – HLE of the STA 0x01 – Another GP STA 0x02 – 0xFF - Reserved
FORWARDING_STA	3 – 8	6	Indicates the MAC address of the GP STA to which the STA(s) participating in the SLAC Process shall forward the signal attenuation characteristic profile data. This field is valid only if RESP_TYPE is set to 0x01

RunID	11-18	8	Run identifier of sender

NUM_SOUNDS
The interpretation of this field is same as 11.5.46.2. It shall be set to the same value as indicated in NUM_SOUNDS field of the corresponding **CM_SLAC_PARM.CNF** MME.
Time_Out
The interpretation of this field is same as 11.5.46.3. It shall be set to the same value as indicated in Time_Out field of the corresponding **CM_SLAC_PARM.CNF** MME. The recipient(s) of this MME shall start a timer that is set to Time_Out duration (refer to Section 5.2.9).
RESP_TYPE
The interpretation of this field is same as in 11.5.46.4. It shall be set to the same value as indicated in **RESP_TYPE** field of the corresponding **CM_SLAC_PARM.CNF** MME.
FORWARDING_STA
The interpretation of this field is same as in 11.5.46.5. It shall be set to the same value as indicated in **FORWARDING_STA** field of the corresponding **CM_SLAC_PARM.CNF** MME.
RUN IDENTIFIER
This field shall be copied from the corresponding **CM_SLAC_PARM.CNF** message.

- CM_ ATTEN_CHAR.IND (GREEN PHY)

CM _ATTEN_CHAR.IND is transmitted by M-SOUND_TARGET STA(s) (i.e., EVSEs) in the SLAC Process. A GP Station processes the received M-SOUND MPDUs and builds a signal attenuation profile. As soon as it receives NUM_SOUNDS SOUND MPDUs as described in **CM_START_ATTEN_CHAR.IND** or the timer maintained by the STA expires, the EVSE shall transmit **CM _ATTEN_CHAR.IND** to the PEV**.** Table 11-Y1 describes the various fields in the message.
Table 11135: CM_ ATTEN_CHAR.IND Message

Field	Octet Number	Field Size (Octets)	Definition
APPLICATION_TYPE	0	1	Application Type 0x00 : PEV-EVSE Association 0x01-0xFF: Reserved
SECURITY_TYPE	1	1	Security in M-Sound Messages 0x00: No Security 0x01: Public Key Signature. 0x02-0xFF: Reserved
ACVarField	-	var	Attenuation Characteristics Variable Field

•

APPLICATION TYPE
This field identifies the context in which the SLAC process is being carried out. Its interpretation is the same as in 11.5.45.1.
SECURITY TYPE
This field indicates whether or not Secure SLAC is used, as in 11.5.45.2.
ACVarField
This field contains the actual attenuation characteristic values. If Security Type = 0x01, then it is CMS-formatted signed contents, with the contents given in Table 11-Y2 below. If Security Type = 0x00, then it is the contents given in Table 11-Y2 below without CMS formatting.

Table 11-136: CM_ ATTEN_CHAR.IND ACVarField Contents

Field	Octet Number	Field Size (Octets)	Definition
SOURCE_ADDRESS	0 – 5	6	The MAC Address of the GP STA initiating the SLAC Process
RunID	6-13	8	The run identifier of the station that sent the M-Sounds
SOURCE_ID	14-30	17	The unique identifier of the station that sent the M-Sounds
RESP_ID	31-47	17	The unique identifier of the station that is sending this message
NumSounds	48	1	Number of M-Sounds used in generating the ATTEN_PROFILE 0x00 – No M-Sounds were received 0x01 – 1 M-Sound was received, and so on
ATTEN_PROFILE	-	var	Signal level attenuation profile

SOURCE_ADDRESS
This field contains the MAC address of the GP STA initiating the SLAC Process.
RUN IDENTIFIER
This field contains the Run Identifier given in the **CM_START_ATTEN_CHAR.IND** message by the GP STA initiating the SLAC Process.

SOURCE IDENTIFIER This field contains the unique identifier of the GP STA initiating the SLAC Process. If Secure SLAC is used for PEV-EVSE matching, this shall be the VIN of the PEV, as used in the public key certificate of the PEV. Otherwise it shall be all zeroes.			
AAG[N]	-	1	Average Attenuation of Group – N 0x00 = 0dB, 0x01 =
RESPONDER IDENTIFIER This field contains the unique identifier of the GP STA initiating the SLAC Process. If Secure SLAC is used for PEV-EVSE matching, this shall be the unique, assigned identification number of the EVSE, as used in the public key certificate of the EVSE. Otherwise it shall be all zeroes.			
NumSounds Number of M-Sounds (NumSounds) field indicates the number M-Sounds that were received and processed for generating the ATTEN_PROFILE. An EVSE that receives a **CM_START_ATTEN_CHAR.IND** but fails to receive any M-Sounds that can be used for generating the ATTEN_PROFILE shall send **CM_ATTEN_CHAR.IND** message with NumSounds set to zero. This will enable the PEV to determine that the EVSE failed to provide a valid ATTEN_PROFILE due to lack of M-Sounds, and take appropriate action. PEV shall ignore the ATTEN_PROFILE field when NumSounds is set to 0x00.			
ATTEN_PROFILE This field contains the signal level attenuation profile between the GP STA whose MAC address is described in **SOURCE_ADDRESS** and the GP STA transmitting this MME. The GP station divides the set of unmasked carriers (as described in Section 3.6.7) into groups of sixteen carriers, starting from the carrier with lowest frequency. For each group, the average attenuation of the carrier in the group is provided. Depending on the number of unmasked carriers, the last group may have lesser than 16 carrier. In such cases, the average attenuation shall be computed only on the available unmasked carriers within the last group. The format of ATTEN_PROFILE is shown in Table 11-137.			

Table 11137: ATTEN_PROFILE field format

Field	Octet Number	Field Size (Octets)	Definition
NumGroups	6	1	Number of Groups (=N) 0x00 = 0 Octets, 0x01 = 1 Octet, and so on
AAG[1]	-	1	Average Attenuation of Group – 1 0x00 = 0dB, 0x01 = 1dB, 0x02 = 2 dB and so on.
…			

AAG[N]	-	1	Average Attenuation of Group – N 0x00 = 0dB, 0x01 = 1dB, 0x02 = 2 dB and so on.

- CM_ ATTEN_CHAR.RSP (GREEN PHY)

CM _ATTEN_CHAR.RSP is transmitted by the PEV in response to the corresponding **CM_ATTEN_CHAR.IND** from the EVSE. Table 11-138 describes the various fields in the message.

Table 11138: CM_ ATTEN_CHAR.RSP Message

Field	Octet Number	Field Size (Octets)	Definition
APPLICATION_TYPE	0	1	Application Type 0x00 : PEV-EVSE Association 0x01-0xFF: Reserved
SECURITY_TYPE	1	1	Security in M-Sound Messages 0x00: No Security 0x01: Public Key Signature. 0x02-0xFF: Reserved
ACVarField	-	var	Attenuation Characteristics Variable Field

-

APPLICATION TYPE

This field identifies the context in which the SLAC process is being carried out. Its interpretation is the same as in 11.5.45.6.

SECURITY TYPE

This field indicates whether or not Secure SLAC is used, as in 11.5.45.7.

ACVarField

This field contains the response. If Security Type = 0x01, then it is CMS-formatted signed contents, with the contents given in Table 11-139 below. If Security Type = 0x00, then it is the contents given in Table 11-139 below without CMS formatting.

Table 11139: CM_ ATTEN_CHAR.CNF ACVarField Contents

Field	Octet Number	Field Size (Octets)	Definition
SOURCE_ADDRESS	0 – 5	6	The MAC Address of the GP STA initiating the SLAC Process

RunID CipherSuiteSetSize	6-13 6	8 1	Run Identifier Cipher Suite Set Size
			The unique identifier of the station that sent the M-Sounds
SOURCE_ID	14-30	17	
RESP_ID	31-47	17	The unique identifier of the station that is sending this message
Result	-	var	0x00 – Success 0x01-0xFF - Reserved

SOURCE_ADDRESS
This field contains the MAC address of the GP STA initiating the SLAC Process.
RUN IDENTIFIER
This field contains the Run Identifier given in the **CM_START_ATTEN_CHAR.IND** message by the GP STA initiating the SLAC Process.
SOURCE IDENTIFIER
This field contains the unique identifier of the GP STA initiating the SLAC Process. If Secure SLAC is used for PEV-EVSE matching, this shall be the VIN of the PEV, as used in the public key certificate of the PEV. Otherwise it shall be all zeroes.
RESPONDER IDENTIFIER
This field contains the unique identifier of the GP STA initiating the SLAC Process. If Secure SLAC is used for PEV-EVSE matching, this shall be the unique, assigned identification number of the EVSE, as used in the public key certificate of the EVSE. Otherwise it shall be all zeroes.

- CM_ PKCS_CERT.REQ (GREEN PHY)

CM_PKCS_CERT.REQ is optional for PEVs and EVSEs, mandatory if public key certificates are supported. It is used to request a public key certificate of the target named by the MAC address parameter. The rest of its parameters describe the ciphersuites that the sender supports.
Table 1113140: CM_ PKCS_CERT.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
Target MAC	0 - 5	6	**Target MAC address** Unicast MAC address of the station for which the public key certificate is desired.

CipherSuiteSetSize	6	1	**Cipher Suite Set Size** Number of supported cipher suites N.
CipherSuite1	7-8	2	**Cipher Suite 1** First supported cipher suite.
…	…	…	…
CipherSuiteN	Var	2	**Cipher Suite N** Nth supported cipher suite.

- CM_ PKCS_CERT.CNF (GREEN PHY)

CM_PKCS_CERT.CNF is optional for PEVs and EVSEs, mandatory if public key certificates are supported. It is used to respond to a request for a public key certificate of the target named by the MAC address parameter in the **CM_PKCS_CERT.REQ**.

Table 1114132: CM_ PKCS_CERT.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
Target MAC	0 - 5	6	**Target MAC address** MAC address of the station for which the public key certificate is provided.
Status	var	1	**Status of Confirmation** 0x00 =Success; certificate included 0x01 = Failure; certificate of unsupported ciphersuite type 0x02 = Failure; PKCS not supported 0x03-0xFF = Reserved

CipherSuite	var	2	**Cipher Suite** Cipher suite of certificate.
CertLength	var	2	**Certificate Length** Unsigned integer length in octets of certificate that follows
CertLength	var	2	**Certificate Length** Unsigned integer length in octets of certificate that follows 0x0000=0, 0x0001=1, etc.
Certificate Package	var	var	**Certificate Package** Certificate of target MAC using named cipher suite, encoded using RFC 5246 encoding as null signed message. Optionally include certificate list and CRL lists as needed.

- CM_ PKCS_CERT.IND (GREEN PHY)

CM_PKCS_CERT.IND is optional for PEVs and EVSEs, mandatory if public key certificates are supported. It is used to provide a public key certificate of the target named by the MAC address parameter in the request.

Table 1114133: CM_ PKCS_CERT.IND Message

Field	Octet Number	Field Size (Octets)	Definition
Target MAC	0 - 5	6	**Target MAC address** MAC address of the station for which the public key certificate is provided.
CipherSuite	var	2	**Cipher Suite** Cipher suite of certificate.

CertLength	var	2	**Certificate Length** Unsigned integer length in octets of certificate that follows 0x0000=0 , 0x0001=1, etc.
Status	var	1	**Status** 0x00 = Success; certificate accepted 0x01 = Failure; certificate of unsupported ciphersuite type 0x02 = Failure;
Certificate Package	var	var	**Certificate Package** Certificate of target MAC using named cipher suite, encoded using RFC 5246 encoding as null signed message. Optionally include certificate list and CRL lists as needed.

- CM_ PKCS_CERT.RSP (GREEN PHY)

CM_PKCS_CERT.RSP is generated in response to the corresponding **CM_PKCS_CERT.IND** when ODA in the **CM_PKCS_CERT.IND** is a unicast MAC Address.
CM_PKCS_CERT.RSP is optional for PEVs and EVSEs, mandatory if public key certificates are supported. It is used to respond optionally to **CM_PKCS_CERT.IND** message holding a public key certificate of the target named by the MAC address parameter in the indication.

Table 1114134: CM_ PKCS_CERT.RSP Message

Field	Octet Number	Field Size (Octets)	Definition
Target MAC	0 - 5	6	**Target MAC address** MAC address of the station for which the public key certificate is provided.

SECURITY_TYPE	1	1	**Security Type of Response Messages** 0x00: No Security 0x01: Public Key Signature.
Status	var	1	**Status of RM Sounds** 0x00 = Success; certificate accepted 0x01 = Failure; certificate of unsupported ciphersuite type 0x02 = Failure; PKCS not supported 0x03-0xFF = Reserved
CipherSuiteSetSize	var	0 or 1	**Cipher Suite Set Size** Number of supported cipher suites N.
CipherSuite1	var	0 or 2	**Cipher Suite 1** First supported cipher suites.
…	…	…	…
CipherSuiteN	var	0 or 2	**Cipher Suite N** Nth supported cipher suites.

- CM_ MNBC_SOUND.IND (GREEN PHY)

CM_MNBC_SOUND.IND is used as part of SLAC protocol to estimate the attenuation profile of a transmission from an PEV at EVSEs.

Table 1114135: CM_ MNBC_SOUND.IND Message

Field	Octet Number	Field Size (Octets)	Definition
APPLICATION_TYPE	0	1	Application Type 0x00 : PEV-EVSE Association 0x01-0xFF: Reserved

SECURITY_TYPE	1	1	0x00: No Security 0x01: Public Key
Sender ID	1 - 17	17	Sender's Station Identification
MSVarField	-	var	M-Sound Variable Field

-
-
-
-
-

APPLICATION TYPE
This field identifies the context in which the SLAC process is being carried out. Its interpretation is the same as in 11.5.45.6.
SECURITY TYPE
This field indicates whether or not Secure SLAC is used, as in 11.5.45.7.
MSVarField
This field contains the sender information. If Security Type = 0x01, then it is CMS-formatted signed contents, with the contents given in Table XXX below. If Security Type = 0x00, then it is the contents given in Table XXX below without CMS formatting.

Table 1114136: CM_ MNBC_SOUND.IND Message MSVarField Contents

Field	Octet Number	Field Size (Octets)	Definition

Sender ID	1 - 17	17	**Sender's Identification** If APPLICATION_TYPE=0x00 then Sender ID is PEV's VIN code.
Cnt	18	1	**Countdown Counter** Countdown counter for number of Sounds remaining; 0x00=0, 0x01=1, etc.
RunID	19-34	16	**Run Identifier** This value shall be the same as the one sent in the CM_START_ATTEN_CHAR.IND message by this sender.
Rnd	35-50	16	**Random Value** Random value

SENDER IDENTIFIER
This field contains the unique identifier of the GP STA sending the M-Sound. If Secure SLAC is used for PEV-EVSE matching, this shall be the VIN of the PEV, as used in the public key certificate of the PEV. Otherwise it shall be all zeroes.
CNT
This field contains a count-down counter. Its value shall be less than the value of NUM_SOUNDS given in the **CM_START_ATTEN_CHAR.IND** message, and shall be decremented on each M-Sound sent. It indicates the number of M-Sound messages remaining to be sent.
RUN IDENTIFIER
This field contains the Run Identifier given in the **CM_START_ATTEN_CHAR.IND** message by the GP STA initiating the SLAC Process.
RND
This field contains a random value.

- CM_VALIDATE.REQ (GREEN PHY)

CM_VALIDATE.REQ is used in PEV-EVSE association as part of out-of-band Validation (refer Section 13.8.1.4).

Table 1114137: CM_VALIDATE.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
SignalType	0	1	**Signal Type** 0x00 = PEV S2 toggles on CPLT line 0x01-0xFF = reserved for future use
VRVarField	1-var	var	**Validate Request Variable Field**

Table 1114138: VRVarField when SignalType is set to 0x00

Field	Octet Number	Field Size (Octets)	Definition
Timer	1	1	**Timer Value** 0x00 = 100ms 0x01 = 200msec, and so on
Result	2	1	**Result Code** 0x00 = Not Ready 0x01 = Ready 0x02 = Success 0x03 = Failure

- CM_VALIDATE.CNF (GREEN PHY)

CM_VALIDATE.CNF is used in PEV-EVSE association as part of out-of-band Validation (refer Section 13.8.1.4).

Table 1114139: CM_VALIDATE.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
SignalType	0	1	**Signal Type** 0x00 = PEV S2 toggles on CPLT line 0x01-0xFF = reserved for future use
VCVarField	2-var	var	**Validate Confirm Variable Field**

Table 11140: VCVarField when SignalType is set to 0x00

Field	Octet Number	Field Size (Octets)	Definition
ToggleNum	1	1	**Number of detected Toggle Sequences** 0x00 = No detected toggle 0x01 = 1 0x02 = 2, and so on
Result	2	1	**Result Code** 0x00 = Not Ready 0x01 = Ready 0x02 = Success 0x03 = Failure

- CM_SLAC_MATCH.REQ (GREEN PHY)

CM_SLAC_MATCH.REQ is mandatory for PEVs and EVSEs, optional otherwise. It is used by the PEV to indicate to an EVSE that it is connected to it through a charging cordset. It may be signed or unsigned.

Table 11151: CM_SLAC_MATCH.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
APPLICATION_TYPE	0	1	**Application Type** 0x00 : PEV-EVSE Association 0x01-0xFF: Reserved
SECURITY_TYPE	1	1	**Security in M-Sound Messages** 0x00: No Security 0x01: Public Key Signature. 0x02-0xFF: Reserved
MVFLength	2-3	2	**Match Variable Field Length** Unsigned integer length in octets of variable field that follows 0x0000=0, 0x0001=1, etc.

MatchVarField	-	var	**Match Variable Field** Interpretation depends on SECURITY_TYPE Unencrypted, unsigned contents if SECURITY_TYPE = 0x00 CMS formatted message if SECURITY_TYPE= 0x01

-
-
-

APPLICATION TYPE
This field identifies the context in which the SLAC process is being carried out. Its interpretation is the same as in 11.5.45.1.
SECURITY TYPE
This field indicates whether or not Secure SLAC is used, as in 11.5.45.2.
MVFLength
This field is an unsigned integer indicating the length of the Match Variable Field.
Match Variable Field
This field contains the SLAC match information. If Security Type = 0x01, then it is CMS-formatted signed contents signed with the PEV's signing key, with the contents given in Table 11-152 below. If Security Type = 0x00, then it is the contents given in Table 11-152 below without CMS formatting.
Table 11152: Content of CM_SLAC_MATCH.IND Var Field

Field	Octet Number	Field Size (Octets)	Definition
PEV ID	1 - 17	17	**PEV Identification** VIN code of PEV
PEV MAC	18-23	6	**PEV MAC** MAC address of PEV

EVSE ID	23-40	17	**EVSE Identification Field** EVSE identification number Interpretation depends on
EVSE MAC	41-46	6	**EVSE MAC** MAC address of EVSE
MatchVarField	-	var	**Match Variable Field**
RunID	47-62	16	**Run Identifier** Identifier given by PEV in the CM_STAR_ATTEN_CHAR.IND message

- CM_ SLAC_MATCH.CNF (GREEN PHY)

CM_SLAC_MATCH.CNF is mandatory for PEVs and EVSEs, optional otherwise. It is used to indicate that an PEV and an EVSE have been matched. It may be signed or unsigned.

Table 11141: CM_ SLAC_MATCH.CNF Message

Field	Octet Number	Field Size (Octets)	Definition
APPLICATION_TYPE	0	1	Application Type 0x00 : PEV-EVSE Association 0x01-0xFF: Reserved
SECURITY_TYPE	1	1	Security in M-Sound Messages 0x00: No Security 0x01: Public Key Signature. 0x02-0xFF: Reserved
MVFLength	2-3	2	**Match Variable Field Length** Unsigned integer length in octets of variable field that follows 0x0000=0, 0x0001=1, etc.

MatchVarField	-	var	**Match Variable Field** Interpretation depends on SECURITY_TYPE Unencrypted, unsigned contents if SECURITY_TYPE = 0x00 CMS formatted message if SECURITY_TYPE= 0x01

•

APPLICATION TYPE
This field identifies the context in which the SLAC process is being carried out. Its interpretation is the same as in 11.5.45.6.
SECURITY TYPE
This field indicates whether or not Secure SLAC is used, as in 11.5.45.7.
MVFLength
This field is an unsigned integer indicating the length of the Match Variable Field.
Match Variable Field
This field contains the SLAC match information. If Security Type = 0x01, then it is CMS-formatted enveloped contents encrypted with the PEV's public key, whose contents are CMS-formatted signed contents signed with the EVSE's signing key, with the contents given in Table 11-154 below. If Security Type = 0x00, then it is the contents given in Table 11-154 below without CMS formatting.
Table 11142: Content of CM_SLAC_MATCH.CNF Var Field

Field	Octet Number	Field Size (Octets)	Definition
PEV ID	1 - 17	17	**PEV Identification** VIN code of PEV
PEV MAC	18-23	6	**PEV MAC** MAC address of PEV
EVSE ID	23-40	17	**EVSE Identification** EVSE identification number

EVSE MAC	41-46	6	**EVSE MAC** MAC address of EVSE
RunID	47-62	16	**Run Identifier** Identifier given by PEV in the CM_STAR_ATTEN_CHAR.IND message
NID	63-70	8	**Network ID** NID of matching EVSE
NMK	71-86	16	**Network Membership Key** NMK of matching EVSE if content type is encrypted, all zeroes otherwise.

- **CM_SLAC_USER_DATA.REQ (GREEN PHY)**

The **CM_SLAC_USER_DATA.REQ** is generated by the HLE of a GP to carry user data related to SLAC. User data is carried in fields call TLVs (Type, Length and Value).

Table 11155: CM_SLAC_USER_DATA.REQ Message

Field	Octet Number	Field Size (Octets)	Definition
Broadcast_TLV	0	3	Octets 0 and 1 are set to 0x0200 Octet 2 is: 0x00 = Send the MME using unicast, 0x01 = Send the MME using within the AVLN broadcast 0x02 = Send the MME using multi-network broadcast
TLVs	3	Var	TLVs – May be empty.
End_of_data_TLV	3 + length(Var)	2	Set to 0x0000 (i.e. TLV_TYPE=0 and TLV_STR_LEN=0)

.

Broadcast_flag

The user data may need to be sent as Multi-Network Broadcast. In such cases, the MAC needs to know that this message has to be sent as Multi-Network broadcast as the typical behavior of the MAC is to send any broadcast MSDUs or unicast MSDUs as broadcast or unicast within the AVLN. Essentially, this field enables the MAC to route the packet to the proper queue.

User_data_TLVs

The TLVs Field contains zero or more user defined TLVs.

Table 11-156: TLVs Field

Field	Octet Number	Field Size (Octets)	Definition
TLV_1	0	2 + TLV_STR_LEN_1	First TLV. May only be the only TLV in the TLVs Field.
	…		
TLV_N		2 + TVL_STR_LEN_N	Last TLV. N maybe 1 or more.

TLV

Table 11-157: TLV Field

Field	Octet Number	Field Size	Definition
TLV_TYPE	0-1	7-bits	Set to 127.
TLV_STR_LEN		9-bits	Length of TLV information string field
TLV_INFO_STR	3	TVL_STR_LEN	Sequence of TVL_STR_LEN octets.

TLV_TYPE

The TLV_TYPE field for organizationally defined TLVs is always set to 127. The values 0-126 are reserved.

TLV_STR_LEN

The TLV_STR_LEN field is set to the number of octets in the TLV_INFO_STR field. For organizationally defined TLVs TLV_STR_LEN field is 4 octets (OUI + SUBTYPE) plus the number of octets in INFO_STR. See below.

TLV_INFO_STR

Table 11-158: TLV_INFO_STR Field

Field	Octet Number	Field Size (Octets)	Definition

OUI	0	3	organizationally unique identifier (OUI)
SUBTYPE	3	1	organizationally defined subtype
INFO_STR	4	TVL_STR_LEN - 4	organizationally defined information string

OUI

The OUI field shall contain the organization's OUI as defined in Clause 9 of IEEE 802 [4].

Subtype

The organizationally defined subtype field contains a unique subtype value assigned by the defining organization. Defining organizations are responsible for maintaining listings of organizationally defined subtypes in order to assure uniqueness.

INFO_STR

The organizationally defined information string is a sequence of octets that is interpreted as the defining organization desires.

End_of_data_TLV

The End_of_data_TLV field is a two octet all zero TLV that is used to mark the end of the sequence of TLVs in the MME.

- **CM_SLAC_USER_DATA.CNF (GREEN PHY)**

CM_SLAC_USER_DATA.CNF is generated by the HLE of a GP STA in response to the CM_SLAC_USER_DATA.REQ received from the MAC of the STA.

The format of CM_SLAC_USER_DATA.CNF is the same as CM_SLAC_USER_DATA.REQ (see 11.5.59). The Broadcast_flag is set to the same value as was received in the CM_SLAC_USER_DATA.REQ.

Manufacturer-Specific Messages

Manufacturer-specific messages are messages used by equipment manufacturers to implement the primitives at the H1, M1, or other interfaces. The format and use of manufacturer-specific messages are manufacturer dependent.

The difference between manufacturer-specific and vendor-specific messages (Section 11.7) is that manufacturer-specific messages shall never be transmitted over the powerline.

Vendor-Specific Messages

Vendor-specific messages are used by implementers of STAs ("vendors") to enhance the functionality of the system when exchanged between STAs designed by the same vendor. The first three octets of the Vendor-Specific Management Message Entry shall contain the IEEE-assigned OUI as described in reference [4]. The bit and octet order of the OUI here and elsewhere in this specification is identical to the bit and octet order of the MAC address as described in Section 4.1.2. The remaining fields in these messages are defined by the vendor.

Vendor-specific messages may be transmitted over the powerline.
Table 11143: Vendor-Specific MME Fields

Field	Octet Number	Field Size (Octets)	Definition
OUI	0 – 2	3	Organizationally Unique Identifier
Vendor Defined	-	Var	Vendor defined

Service Access Point Primitives

Convergence Layer Information

As with HomePlug AV, to provide an easy-to-use yet robust and powerful interface to the application, HomePlug GREEN PHY implements a Convergence Layer (CL) that shields the application from the complexities of the MAC and PHY. Figure 22 shows the relationship of the CL to the rest of the HomePlug-GREEN PHY system.

H1 and M1 Interfaces

The CL is bounded on the top by the H1 Interface and on the bottom by the M1 Interface (see Figure 21).

As with HomePlug AV, the H1 Interface is the boundary between the HLEs entities above the H1 Interface (e.g., AV or GREEN PHY Control applications, HomePlug-GREEN PHY management entities, Ethernet protocol stacks and Bridges) and the CL. The HLEs communicate with the CL through SAPs at the H1 Interface. The CL implements Protocol Adaptation Layers (PALs) to service the SAPs and exchange data with the HLEs.

The M1 Interface is the boundary between the CL and the MAC. There is a single SAP at the M1 interface that the CL uses to pass data received from HLEs to the MAC. Control Information does not pass across the M1 interface (i.e., there are no M1 primitives for control) because the control plane is monolithic.

Protocol Adaptation Layers (PALs)

Within the CL, entities called Protocol Adaptation Layers (PALs) provide services to the HLEs. The services include Connection management-and-control function, as well as data transport.

The functions provided by the PALs include:

Reformatting messages received from the H1 SAPs and passing them down to the M1 SAPs.

Reformatting messages received from the M1 SAPs and passing them up to the H1 SAPs.

Providing services such as Connection management and address management.

Providing information and statistics.

Service Access Points (SAPs)

The PALs expose SAPs at the H1 interface to communicate with the HLEs.

Similarly, at the M1 interface, the MAC exposes a SAP for the CL to use for data transport. As mentioned above, there are no SAPs and primitives for control messaging.

Primitives

Primitives are the instantiation of the SAPs that are visible from the outside. They are akin to an

Application Program Interface (API) and, in an implementation, will become an API. However, in the system specification (this document), they are basic outlines that identify the information that must flow to and from the PAL to ensure that the designer has available the information on which it depends. Occasionally, several parameters in a primitive may be identified as optional, with a note that at least one of them must appear. In this case, depending on the implementation of the PAL, the designer may select which one to implement, but must implement at least one. Furthermore, the specification of a parameter for a primitive identifies information that must flow. It does not require that the parameter actually exist as a distinct parameter in the implementation so long as the information is conveyed in a way that is well known to both the PAL and the outside entity.	This is an optional parameter. If it is supplied, it may have one of the following values: **Request local confirm:** the higher layer requests an AV_DATA.CNF primitive to indicate the success or failure of this .REQ primitive. **Confirm not requested:** The higher layer does not require a .CNF primitive for
Confirm (optional)	

H1 SAPs

Each PAL provides a SAP at the H1 Interface to allow the HLEs access to the capabilities they require to utilize the PLC system (e.g., establishing and managing Connections, sending data, and so on). These Higher Layer Entities include applications, bridges, and so on.

Protocol Adaptation Layer (Data Plane)

Ethernet II-Class (ETH) SAP

The Ethernet II-class SAP supports applications using Ethernet II class packets, including IEEE 802.3 with or without IEEE 802.2 (LLC), IEEE 802.1H (SNAP) extensions, and/or VLAN tagging. Jumbo Ethernet frames (up to 8992 octets) may optionally be supported for connection-oriented services. Jumbo Ethernet frames are not allowed for connectionless service.

ETH_SEND.REQ

The ETH_SEND.REQ primitive is used by the HLE to initiate a data transfer. This request includes the entire IEEE 802.3 frame.

Table 121: ETH_SEND.REQ Primitive

Primitive	ETH_SEND.REQ
Parameter Name	Description
Destination Address	The 48-bit MAC address of the destination STA
Source Address	The 48-bit MAC address of the source STA.
CID (optional)	Connection ID: will simplify classification if HLE can provide (refer to Section 5.2.1.4.2).
Request ID (optional)	Request ID is an identifier generated by HLE to uniquely identify the request.

Confirm (optional) Result	This primitive shall be issued by the PAL in response to an ETH_SEND.REQ primitive. The Result parameter shall have one of the following values: **Request local confirm**: the higher layer requested a .CNF primitive for this packet. **Acknowledged**: the requested packet was successfully delivered and acknowledged. **Timeout**: the requested packet was discarded after a period of time without receiving an acknowledgement. **Confirm not requested**: The higher layer did not request a .CNF primitive for this packet. **No Connection Available**: the request could not be completed because no connection was available to generate the .CNF if desired.
Priority (optional)	The priority at which packet should be sent (refer to Section 13.1). The priority field will be ignored for packets which are carried on a
	Connection.
Data	The payload that is passed from the upper layers for transmission.
Informative Text The optional parameters that might be received from the HLE are not part of a standard Ethernet frame. The way they will be passed from the HLE is an implementation option. The Priority parameter may be passed as a VLAN tag within the Data parameter or via some other mechanism.	

ETH_SEND.CNF

The ETH_SEND.CNF primitive is used by the PAL to notify the HLE of the results of the ETH_SEND.REQ primitive.

Table 122: ETH_SEND.CNF Primitive

Primitive	ETH_SEND.CNF
Parameter Name	Description
CID (optional)	Connection ID (may be ignored by HLE). Refer to Section 5.2.1.4.2.
Request ID (optional)	Request ID associated with the corresponding ETH_SEND.REQ

Result	This primitive returns the results of a .REQ primitive. The Result parameter may have one of the following values: **Acknowledged**: the requested packed was successfully delivered to the receiving DEV. **Timeout**: the requested packet was discarded after a period of time (never acknowledged or delivery errors). **No Connection Available**: the requested packet could not be delivered because no Connection existed to the destination STA. **Parameter Error**: errors in the primitive made it impossible to deliver the requested packet.

ETH_RECEIVE.IND

The ETH_RECEIVE.IND primitive is used by the CL in the receiving STA to notify the HLE that data has been received via an ETH_SEND.REQ primitive. This indication includes the entire IEEE 802.3 frame.

Table 123: ETH_RECEIVE.IND Primitive

Primitive	ETH_RECEIVE.IND
Parameter Name	Description
Destination Address	The 48-bit MAC address of the destination STA. This parameter should always be the MAC address of this STA.
Source Address	The 48-bit MAC address of the source STA
Data	The packet that is passed to the upper layers.
CID (optional)	Connection ID (refer to Section 5.2.1.4.2).
Reception Status (optional)	This parameter indicates the status of the received data. . This parameter may have one of the following values: **Valid**: the AV_data_octets were successfully received **Non-continuous**: the lower layers have detected that there is one or more missing packets **Out of order**: this packet is not in sequential order **Excessive delay**: this packet is older than the maximum delay specified for this stream.
Arrival Timestamp (optional)	The Arrival Time Stamp (ATS). Refer to Section 12.3.2.1.

Informative Text
The optional parameters that can be passed to the HLE are not part of a standard Ethernet frame. The way they will be passed to the HLE is an implementation option. One option is to pass the parameters in a control packet, either immediately before or after the primary data packet. Alternatively, the HLE can contain a hardware solution or a customized Ethernet stack that accepts the additional parameters.

Control SAP Service

The Control SAP enables the HLEs to:

Create and manage Connections

Monitor status and statistics

Support vendor-specific primitives

Initialize the STA

Obtain or set encryption keys

APCM_CONN_ADD.REQ

APCCM_CONN_ADD.REQ is a request from the HLE to the CM to add a new Connection.

Table 124: APCM_CONN_ADD.REQ Primitive

Primitive	APCM_CONN_ADD.REQ

Parameter Name	Description
Original Source Address	The address of the DEV originating the data carried on this Connection
Original Destination Address	The address of the DEV to which this Connection is directed
Request ID	An identifier generated by HLE to uniquely identify the request.
CSPEC	Connection Specification of the new Connection. The interpretation of this field is the same as in Section 7.8.1.
Classifier Rule Set(s)	Information needed to configure the Classifier on this STA for this Connection (e.g., source Internet Protocol (IP) address, source IP port, destination IP address, destination IP port). Refer to Section 6.2 for details on the Classifier Rule Set(s).

APCM_CONN_ADD.CNF

APCM_CONN_ADD.CNF is generated by the CM in response to the corresponding APCM_CONN_ADD.REQ. This primitive indicates whether the Connection request was successful.

Table 125: APCM_CONN_ADD.CNF Primitive

Primitive	APCM_CONN_ADD.CNF
Parameter Name	Description
CID	The unique CID of this Connection (refer to Section 5.2.1.4.2)
Original Source Address	The address of the DEV originating the data carried on this Connection
Original Destination Address	The address of the destination station side of this new stream.
Result	The Result parameter may have one of the following values: Success: the ADD operation was successful. Failure: the ADD operation failed.
Request ID	Request ID associated with the corresponding APCM_CONN_ADD.REQ
Rejecting Station(s) MAC Addresses [ ]	This is an optional field that is present if the new Connection failed. This field contains the MAC addresses of the station(s) that rejected the Connection.
Proposed CSPEC	Proposed CSPEC indicating the CSPEC that the CM is currently capable of supporting, if the new Connection failed. If it is not included, the failure was for a reason not related to an inability to support the CSPEC. The interpretation of this field is the same as in Section 7.8.1.

APCM_CONN_ADD.IND

APCM_CONN_ADD.IND is an indication from the CM to the HLE of the new Connection that is being requested.

Table 126: APCM_CONN_ADD.IND Primitive

Primitive	APCM_CONN_ADD.IND
Parameter Name	Description
CID	The unique CID of this Connection (refer to Section 5.2.1.4.2)
Init. MAC Addr	MAC address of the STA initiating the Connection
Term. MAC Addr	MAC address of the terminating STA(s)
CSPEC	Connection Specification of the new Connection. The interpretation of this field is the same as in Section 7.8.1.

APCM_CONN_ADD.RSP

APCM_CONN_ADD.RSP is a response from the HLE to the CM for the corresponding APCM_CONN_ADD.IND.

Table 127: APCM_CONN_ADD.RSP Primitive

Primitive	APCM_CONN_ADD.RSP
Parameter Name	Description
CID	The unique CID of this Connection (refer to Section 5.2.1.4.2)
Result	The Result parameter may have one of the following values: Success: the ADD operation was successful. Failure: the ADD operation failed.
Proposed CSPEC	Proposed CSPEC indicating the CSPEC that the HLE is currently capable of supporting if the new Connection failed. If it is not included, the failure was for a reason not related to an inability to support the CSPEC. The interpretation of this field is the same as in Section 7.8.1.
Rejecting Station(s) MAC Addresses [ ]	This is an optional field that is present if the new Connection failed. This field contains the

APCM_CONN_MOD.REQ

Table 128: APCM_CONN_MOD.REQ Primitive

Primitive	APCM_CONN_MOD.REQ
Parameter Name	Description
CID	The unique CID of this Connection (refer to Section 5.2.1.4.2)
Modified CSPEC	Modified CSPEC containing the new CSPEC that is requested for the Connection. The interpretation of this field is the same as in Section 7.8.1.

APCM_CONN_MOD.CNF

Table 129: APCM_CONN_MOD.CNF Primitive

Primitive	APCM_CONN_MOD.CNF
Parameter Name	Description
CID	The unique CID of this Connection (refer to Section 5.2.1.4.2)
Result	The Result parameter may have one of the following values: Success: the MODIFY operation was successful. Failure: the MODIFY operation failed.

Rejecting Station(s) MAC Addresses [ ]	This field contains the MAC addresses of the HE STA(s) that rejected the connection modification. This field may optionally be included when the Proposed CSPEC failed. If CSPEC
Proposed CSPEC Proposed CSPEC	Proposed CSPEC containing the CSPEC that can be supported, if the connection modification failed. If it is not included, the failure was for a reason not related to an inability to support the CSPEC. The
	interpretation of this field is the same as in Section 7.8.1.

APCM_CONN_MOD.IND

Table 1210: APCM_CONN_MOD.IND Primitive

Primitive	APCM_CONN_MOD.IND
Parameter Name	Description
CID	The unique CID of this Connection (refer to Section 5.2.1.4.2)
Modified CSPEC	Modified CSPEC containing the new CSPEC that is requested for the Connection. The interpretation of this field is the same as in Section 7.8.1.
Cause	Cause for the connection reconfiguration CCo initiated HLE initiated Others

APCM_CONN_MOD.RSP

Table 1211: APCM_CONN_MOD.RSP Primitive

Primitive	APCM_CONN_MOD.RSP
Parameter Name	Description
CID	The unique CID of this Connection (refer to Section 5.2.1.4.2)
Result	The Result parameter may have one of the following values: Success: the MODIFY operation was successful. Failure: the MODIFY operation failed.

Proposed CSPEC	Proposed CSPEC indicating the CSPEC that the HCE is currently capable of supporting, if this connection modification failed. This field may optionally be included when the Connection was terminated by the CCo due to insufficient bandwidth. If it is included, the failure was for a reason not related to an inability to support the CSPEC. The interpretation of this field is the same as in Section 7.8.1.

APCM_CONN_REL.REQ

Table 1212: APCM_CONN_REL.REQ Primitive

Primitive	APCM_CONN_REL.REQ
Parameter Name	Description
CID	The unique CID of this Connection (refer to Section 5.2.1.4.2)

APCM_CONN_REL.CNF

Table 1213: APCM_CONN_REL.CNF Primitive

Primitive	APCM_CONN_REL.CNF
Parameter Name	Description
CID	The unique CID of this Connection (refer to Section 5.2.1.4.2)

APCM_CONN_REL.IND

Table 1214: APCM_CONN_REL.IND Primitive

Primitive	APCM_CONN_REL.IND
Parameter Name	Description
CID	The unique CID of this Connection (refer to Section 5.2.1.4.2)
Reason Code	Specifies the cause of the release. Normal release Release due to violation of CSPEC Insufficient Bandwidth Requested by another station within the AVLN that is not part of the connection.
Releasing Station MAC Address	This field contains the MAC addresses of the station that initiated the release of the Connection.

Informative Text The HLE may require a distributed, synchronized clock for other reasons (e.g., surround-sound audio, where all speakers must be closely synchronized). The HLE may also require a synchronized clock for other reasons. Implementers are encouraged to provide a clock that is more accurate than the 25 MHz clock (or clock over). The method by which the recovered clock is provided to the HLE is an implementation option. Providing the recovered clock via a software call interface is desirable for the HLE in order to support applications such as HDTV and “audiophile-quality” audio.	Proposed CSPEC indicating the CSPEC that the CCo is currently using for synchronous application support. This field may optionally be included to indicate the CSPEC that is not supported by the HLE. If included, the value provided for the HLE is an implementation specific decision for the HLE.
Violated CSPEC The implementer is encouraged to provide, at a minimum, a “recovered clock” signal (such as a processor interrupt signal) to the HLE on reception of the Beacon. With this signal, the ability to read the time value broadcast within the Beacon, and its own clock, the HLE can make its own clock recovery function.	Violated CSPEC is an optional field that is present when the Connection is released due to a CSPEC violation. This field contains the fly of the CSPEC that are violated.

APCM_GET_NTB.REQ

The APCM_GET_NTB.REQ primitive is used by the HLE to request the Network Time Base from the CCo or its estimate, NTB_STA, from a non-CCo STA (refer to Section 5.5.5).

Table 1215: APCM_GET_NTB.REQ Primitive

Primitive	APCM_GET_NTB.REQ
Parameter Name	Description
	<This message does not require any parameters.>

APCM_GET_NTB.CNF

The APCM_GET_NTB.CNF primitive is used by the CL to provide the current Network Time Base to the HLE. The Network Time Base can be used to support the end-to-end smoothing requirements specified in Section 6.7.3. The APCM_GET_NTB.CNF primitive is optional.

Informative Text

The HLE may require a distributed, synchronized clock for synchronous applications (e.g., surround-sound audio, where all speakers must be closely synchronized). The HLE may also require a synchronized clock for other reasons.

Implementers are encouraged to provide a clock that is monotonically increasing (except at roll over). The method by which the recovered clock is provided to the HLE is an implementation option.

Providing the recovered clock via a software call is insufficient for demanding AV applications such as HDTV and “audiophile-quality” audio.

The implementer is encouraged to provide, at a minimum, an "immediate signal" (such as a processor interrupt signal) to the HLE on reception of the Beacon. With this signal and the ability to read the time value broadcast within the Beacon, the HLE can make its own clock recovery function.

For a more fully featured implementation, the implementer is encouraged to supply the recovered clock to the HLE. In this context, the term “recovered clock” means a 32-bit 25 MHz clock that is phase locked to the CCo's reference clock via the time value broadcast in the Beacon. The recovered clock in the local PLC H/W should be readable by the HLE at any time.

The accuracy required of the recovered clock relative to the CCo's clock depends on the application that will be using the clock. It is assumed that the implementer will specify an accuracy (e.g., ±0.5 µsec or ±10 µsec) rigorous enough to satisfy their target market.

Table 1216: APCM_GET_NTB.CNF Primitive

Primitive	APCM_GET_NTB.CNF
Parameter Name	Description
Network Time Base	32-bit value of NTB (refer to Section 5.5)

APCM_AUTHORIZE.REQ

The APCM_AUTHORIZE.REQ primitive is used to instruct a STA to authorize another STA to join its AVLN using DAK-based distribution of the NMK. A Request ID is included to match the corresponding APCM_AUTHORIZE.CNF in case multiple such requests are initiated in parallel.

Table 1217: APCM_AUTHORIZE.REQ Primitive

Primitive	APCM_AUTHORIZE.REQ
Parameter Name	Description
Request	Authorize STA
Request ID	Request ID for asynchronous confirmation
DAK	DAK to be used for NMK Provisioning
ODA	MAC address of STA to authenticate, if known
NMK	Network Management Key to distribute (or indicate to use current NMK)
NID	Network Identifier (including Security Level) to associate with this NMK, or indicate to use the default NID

SL	Security Level of New NMK (values = HS or SC) – Only included if default NID is used

Support for explicit delivery of NMK and non-default NID is optional. Support for authorization using the current NMK and NID is mandatory. The SL of the NID shall be compatible with the SL of the NMK being distributed. The current NMK shall not be distributed using a different Security Level. This primitive shall include either the NID or the SL field, but not both.

APCM_AUTHORIZE.CNF

The APCM_AUTHORIZE.CNF primitive is used by a STA to inform the HLE of the results of its request to authorize another STA to join its AVLN using DAK-based distribution of the NMK. The Request ID shall match the Request ID used in the corresponding APCM_AUTHORIZE.REQ primitive. This confirmation shall only be sent when the protocol terminates due to successful completion, timeout, or abort. Timeout may be due to TEK lifetime expiration, or it may be due to a persistent lack of response to the DAK-encrypted initial message.

Table 1218: APCM_AUTHORIZE.CNF Primitive

Primitive	APCM_AUTHORIZE.CNF
Parameter Name	Description
Request ID	Request ID of the APCM_AUTHORIZE.REQ to which this is a confirmation
Result	Result = Authorization Complete No Response Protocol aborted
ODA	MAC address of STA authorized

APCM_AUTHORIZE.IND

The APCM_AUTHORIZE.IND primitive is used by a STA to inform the HLE that it has been authorized by another STA to join its AVLN using DAK-based distribution of the NMK. This indication shall only be sent when the protocol terminates due to successful completion, TEK lifetime timeout, or abort.

Table 1219: APCM_AUTHORIZE.IND Primitive

Primitive	APCM_AUTHORIZE.IND
Parameter Name	Description
ODA	MAC address of STA that sent DAK-Encrypted MME
NID	Network ID of AVLN that sent DAK-Encrypted MME
Status	Status = Authorization Complete Protocol aborted

APCM_GET_SECURITY_MODE.REQ

Table 1220: APCM_GET_SECURITY_MODE.REQ Primitive

Primitive	APCM_GET_SECURITY_MODE.REQ
Parameter Name	Description
	<This message does not require any parameters.>

APCM_GET_SECURITY_MODE.CNF

Table 1221: APCM_GET_SECURITY_MODE.CNF Primitive

Primitive	APCM_GET_SECURITY_MODE.CNF
Parameter Name	Description
Result	Success | Fail
Security Mode	Secure | Simple-Connect | SC-Add | SC-Join

APCM_SET_SECURITY_MODE.REQ

Table 1222: APCM_SET_SECURITY_MODE.REQ Primitive

Primitive	APCM_SET_SECURITY_MODE.REQ
Parameter Name	Description
Security Mode	Secure | Simple-Connect | SC-Add | SC-Join

APCM_SET_SECURITY_MODE.CNF

Table 1223: APCM_SET_SECURITY_MODE.CNF Primitive

Primitive	APCM_SET_SECURITY_MODE.CNF
Parameter Name	Description
Result	Success | Fail

APCM_GET_NETWORKS.REQ

Table 1224: APCM_GET_NETWORKS.REQ Primitive

Primitive	APCM_GET_NETWORKS.REQ
Parameter Name	Description
	<This message does not require any parameters.>

APCM_GET_NETWORKS.CNF

Table 1225: APCM_GET_NETWORKS.CNF Primitive

Primitive	APCM_GET_NETWORKS.CNF
Parameter Name	Description
NNSTA	Number of Networks Found = N
NID[1]	NID of AVLN 1
STATUS(1)	Status of AVLN 1 = Joined | Not Joined – have NMK | Not Joined – no NMK | Blacklisted
CMAC[1]	MAC address of AVLN 1's CCo
HFID[1]	HFID of AVLN 1
…	
NID[N]	NID of AVLN N
STATUS(N)	Status of AVLN N

CMAC[N]	MAC address of AVLN N's CCo
HFID[N]	HFID of AVLN N

APCM_SET_NETWORKS.REQ

Table 1226: APCM_SET_NETWORKS.REQ Primitive

Primitive	APCM_SET_NETWORKS.REQ
Parameter Name	Description
NID	Network ID
Request Type	Join Now | Leave Now | Blacklist | Rehabilitate

APCM_SET_NETWORKS.CNF

Table 1227. APCM_SET_NETWORKS.CNF Primitive

Primitive	APCM_SET_NETWORKS.CNF
Parameter Name	Description
	<This message does not require any parameters.>

APCM_GET_NEWSTA.REQ

Table 1228. APCM_GET_NEWSTA.REQ Primitive

Primitive	APCM_GET_NEWSTA.REQ
Parameter Name	Description
	<This message does not require any parameters.>

APCM_GET_NEWSTA.CNF

Table 1229: APCM_GET_NEWSTA.CNF Primitive

Primitive	APCM_GET_NEWSTA.CNF
Parameter Name	Description
NNSTA	Number of newSTAs = N
MAC[1]	MAC address of newSTA 1
HFID-MFG[1]	Manufacturer-set HFID of newSTA 1
HFID-USER[1]	User-set HFID of newSTA 1
…	
MAC[N]	MAC address of newSTA N
HFID-MFG[N]	Manufacturer-set HFID of newSTA N
HFID-USER[N]	User-set HFID of newSTA N

APCM_GET_NEWSTA.IND

Table 1230: APCM_GET_NEWSTA.IND Primitive

Primitive	APCM_GET_NEWSTA.IND
Parameter Name	Description
NNSTA	Number of newSTAs = N
MAC[1]	MAC address of newSTA 1
HFID-MFG[1]	Manufacturer-set HFID of newSTA 1
HFID-USER[1]	User-set HFID of newSTA 1

…	
MAC[N]	MAC address of newSTA N
HFID[N]	HFID of newSTA N
HFID-MFG[N]	Manufacturer-set HFID of newSTA N
HFID-USER[N]	User-set HFID of newSTA N

APCM_SET_KEY.REQ

The APCM_SET_KEY.REQ primitive is used by the HLE to set the NMK of its STA. Reception of this primitive causes the STA to leave its existing AVLN (if it is part of an AVLN) and restart its power-on network procedure (refer to Section 7.1). This may also be accomplished by sending the CM_SET_KEY.REQ MME over the H1 interface, destined for the STA's MAC address.

Table 1231: APCM_SET_KEY.REQ Primitive

Primitive	APCM_SET_KEY.REQ
Parameter Name	Description
NMK	New Network Membership Key
NID	Network Identifier (including Security Level) to associate with this NMK, or indicate to use the default NID
SL	Security Level of New NMK (values = HS or SC) - Only included if default NID is used

Support for explicit delivery of NMK and non-default NID is optional. Support for the default NID is required. This primitive shall include either the NID or the SL field, but not both.

APCM_SET_KEY.CNF

Table 1232: APCM_SET_KEY.CNF Primitive

Primitive	APCM_SET_KEY.CNF
Parameter Name	Description
Result	Success | Fail

APCM_GET_KEY.REQ

The APCM_GET_KEY.REQ primitive is used by the HLE to obtain the NMK of its STA.

Table 1233:. APCM_GET_KEY.REQ Primitive

Primitive	APCM_GET_KEY.REQ
Parameter Name	Description
	<This message does not require any parameters.>

APCM_GET_KEY.CNF

The APCM_GET_KEY.CNF primitive is used by the STA to provide its NMK to its HLE.

Table 1234: APCM_GET_KEY.CNF Primitive

Primitive	APCM_GET_KEY.CNF
Parameter Name	Description
NID	Network Identifier associated with this NMK (including the Security Level)
NMK	Network Membership Key

APCM_STA_RESTART.REQ The APCM_STA_RESTART.REQ primitive is used by the HLE to restart the STA. Upon restarting, the STA initiates the power-on network procedure (see Section 7.1). There are no parameters for this primitive. APCM_STA_RESTART.CNF The APCM_STA_RESTART.CNF primitive is generated by the STA in response to the corresponding APCM_STA_RESTART.REQ.	The Result parameter may have one of the following values: **Success**: the SET_TONE_MASK operation was successful. **Failure**: the SET_TONE_MASK operation

Table 1235. APCM_STA_RESTART.CNF Primitive

Primitive	APCM_STA_RESTART.CNF
Parameter Name	Description
Result	Success | Fail

APCM_NET_EXIT.REQ

The APCM_NET_EXIT.REQ primitive is used by the HLE to request the STA to leave the AVLN to which it is belongs (if any). If the STA is part of an AVLN, it follows the procedure described in Section 7.3.6 for leaving the AVLN. Upon leaving the AVLN, the STA will not rejoin the AVLN until it is powered down and restarted or until it receives an APCM_SET_KEY.REQ or APCM_STA_RESTART.REQ primitive. There are no parameters for this primitive.

APCM_NET_EXIT.CNF

Table 1236. APCM_NET_EXIT.CNF Primitive

Primitive	APCM_NET_EXIT.CNF
Parameter Name	Description
Result	Success | Fail

APCP_SET_TONE_MASK.REQ

The APCP_SET_TONE_MASK.REQ primitive is used to set the tone mask for the station (refer to Section 3.6.7).

Table 1237: APCP_SET_TONE_MASK.REQ Primitive

Primitive	APCP_SET_TONE_MASK.REQ
Parameter Name	Description
Tone Mask	This parameter indicates masked carriers from carrier number 74 through 1228 (1.8 MHz to 30 MHz)

APCP_SET_TONE_MASK.CNF

Table 1238: APCP_SET_TONE_MASK.CNF Primitive

Primitive	APCP_SET_TONE_MASK.CNF
Parameter Name	Description

Tone Mask	The Result parameter may have one of the following values: **Success**: the SET_TONE_MASK operation was successful. **Failure**: the SET_TONE_MASK operation failed.

APCM_STA_CAP. REQ

The APCM_STA_CAP.REQ primitive is a request from HLE to provide the station capabilities. There are no fields present in this primitive.

APCM_STA_CAP.CNF

The APCM_STA_CAP.CNF primitive is generated in response to the corresponding APCM_STA_CAP.REQ. The fields present in this primitive are same as the fields in CM_STA_CAP.CNF (refer to Section 11.5.25).

APCM_NW_INFO.REQ

The APCM_NW_INFO.REQ primitive is a request from HLE to provide the list of AVLNs to which the STA is a member and the relevant information about the AVLN. There are no fields present in this primitive.

APCM_NW_INFO.CNF

The APCM_NW_INFO.CNF primitive is generated in response to the corresponding APCM_NW_INFO.REQ. The fields present in this primitive are same as the fields in CM_NW_INFO.CNF (refer to Section 11.5.27).

APCM_LINK_STATS.REQ

The APCM_LINK_STATS.REQ primitive is a request from HLE to provide statistics for a Link that is associated with a Connection, or for Priority based Links or Management Links. The fields present in this primitive are same as the fields in CM_LINK_STATS.REQ (refer to Section 11.5.35).

APCM_LINK_STATS.CNF

The APCM_LINK_STATS.CNF primitive is generated in response to the corresponding APCM_LINK_STATS.REQ. The fields present in this primitive are same as the fields in CM_LINK_STATS.CNF (refer to Section 11.5.36).

APCM_GET_BEACON.REQ

The APCM_GET_BEACON.REQ primitive is a request to provide the Beacon Payload field of a recently received Central Beacon or Proxy Beacon (if station cannot hear the Central Beacon) of an AVLN to which the STA is a member. The fields present in this primitive are same as the fields in CM_GET_BEACON.REQ (refer to Section 11.5.28).

APCM_GET_BEACON.CNF

The APCM_GET_BEACON.CNF primitive is generated in response to the corresponding APCM_GET_BEACON.REQ. The fields present in this primitive are same as the fields in CM_GET_BEACON.CNF (refer to Section 11.5.29).

APCM_GET_HFID.REQ

The APCM_GET_HFID.REQ primitive is a request from HLE to provide the Human Friendly Identifier of a STA or an AVLN. The fields present in this primitive are same as the fields in

CM_HFID.REQ (refer to Section 11.5.30). APCM_GET_HFID.CNF			**Encryption Key**
PP_EKS	**Bit string**	**N/A**	

The APCM_GET_HFID.CNF primitive is generated in response to the corresponding APCM_HFID.REQ. The fields present in this primitive are same as the fields in CM_HFID.CNF (refer to Section 11.5.31).

APCM_SET_HFID.REQ

The APCM_SET_HFID.REQ primitive is a request from HLE to set the user-defined Human Friendly Identifier of a STA or an AVLN. The only field present in this primitive is the HFID (up to 64 octets – refer to Section 7.3.1.2).

APCM_SET_HFID.CNF

The APCM_SET_HFID.CNF primitive is generated in response to the corresponding APCM_HFID.REQ. It indicates success or failure.

APCM_SET_HD_DURATION.REQ (GREEN PHY)

The **APCM_SET_HD_DURATION**.REQ primitive is used to set the Hold Down Duration (HD_Duration) system parameter (refer to Section 5.8.1.1). A STA shall be capable of Hold Down Durations from zero to 30 seconds.

Table 1239: APCP_SET_TONE_MASK.REQ Primitive

Primitive	APCP_SET_TONE_MASK.REQ
Parameter Name	Description
HD_Duration	This parameter indicates Hold Down Duration

APCM_SET_HD_DURATION.CNF (GREEN PHY)

The **APCM_SET_HD_DURATION.**CNF primitive confirms setting of the Hold Down Duration (HD_Duration) system parameter.

APCM_ UNASSOCIATED_STA.IND (GREEN PHY)

The **APCM_UNASSOCIATED_STA.IND** primitive is used by a STA to inform the HLE that a **CM_UNASSOCIATED_STA.IND** has been received. The fields present in this primitive are same as the fields in **CM_UNASSOCIATED_STA.IND** (refer to Section 11.5.1).

APCM_SC_JOIN.REQ (GREEN PHY)

The **APCM_SC_JOIN.REQ** primitive is used by a STA to inform the HLE that a **CM_SC_JOIN.REQ** has been received. The fields present in this primitive are same as the fields in **CM_SC_JOIN.REQ** (refer to Section 11.5.8).

APCM_SC_JOIN.CNF (GREEN PHY)

The **APCM_SC_JOIN.CNF** primitive is used by the HLE to inform the STA that it should send a **CM_SC_JOIN.CNF**. The fields present in this primitive are same as the fields in **CM_SC_JOIN.CNF** (refer to Section 11.5.9).

APCM_SET_PPKEYS.REQ (GREEN PHY)

The APCM_SET_PPKEY.REQ primitive is used by the HLE to set the security parameters for a point-to-point encrypted connection (PP-EKS and PPEK). Reception of this primitive causes the STA to store this information, encrypt all future transmissions to the indicated STA using this information, and use these keys to attempt to decrypt and verify MAC Frames received from the indicated station.

The APCM_SET_PPKEY.REQ primitive is generated by the HLE

Table 1240: APCM_SET_PPKEYS.REQ Primitive

Name	Type	Valid range	Description

PP_EKS	**Bit string**	**N/A**	**Encryption Key Select for Point to Point encryption key select**
PPEK	**Bit string**	**N/A**	**Point-to-Point Encryption Key**
Other MAC	**MAC address**	**Any valid individual Ethernet address**	**MAC address of other STA**

If the value of the new PPEK is all zeros, then the current PPEK for that MAC is discarded along with the PP_EKS.

APCM_SET_PPKEYS.CNF (GREEN PHY)

This primitive is used to inform the HLE of the results of the APCM_SET_PPKEYS.REQ.

This primitive is generated by the STA in response to a MLME_APCM_SET_PPKEYS.REQ

Table 1241: APCM_SET_PPKEYS.CNF Primitive

Name	Type	Valid range	Description
ResultCode	**Enumeration**	**SUCCESS, FAIL**	Indicates the results of the corresponding .request primitive.

APCM_SET_CCo.REQ (GREEN PHY)

The **APCM_SET_CCo.REQ** primitive is used by the HLE to configure a Green PHY station to be always CCo, never a CCo or automatically determine whether it should become a CCo.

Table 1242: APCM_SET_CCo.REQ Primitive

Primitive	APCP_SET_CCo.REQ
Parameter Name	Description
SET_CCo_MODE	• This parameter indicates whether the station is • Always a CCo. In this case, the station will not join other AVLNs as a STA • Never a CCo. In this case, the station will never become the CCo of an AVLN • Auto CCo. In this case, the station may act either as a CCo or STA of an AVLN

APCM_SET_CCo.CNF (GREEN PHY)

The **APCM_SET_CCo.**CNF primitive is generated in response to the corresponding **APCM_SET_CCo.**REQ. This primitive indicates successful configuration of the station based on the **APCM_SET_CCo.**REQ.

APCM_CONF_SLAC.REQ (GREEN PHY)
The **APCM_CONF_SLAC.REQ** primitive is used by the HLE to configure SLAC Protocol at a Green PHY station.
Table 1243: APCM_CONF_SLAC.REQ Primitive

Primitive	APCP_CONF_SLAC.REQ
Parameter Name	Description
SLAC_CONF	• This parameter indicates the SLAC Configuration at a Green PHY station • Disable SLAC: The Green PHY station will not transmit or receive any SLAC related messages • Enable SLAC functions associated with the transmitter of M-Sounds and to disable SLAC functions associated with receiver of M-Sounds • Enable SLAC function associated with the receiver of M-Sounds and to disable SLAC functions associated with transmitter of M-Sounds

APCM_CONF_SLAC.CNF
The **APCM_CONF_SLAC.CNF** primitive is generated in response to the corresponding **APCM_CONF_SLAC.REQ**. This primitive indicates successful configuration of the station based on the **APCM_CONF_SLAC.REQ**.

M1 SAPs
MAC Service Definition
Overview
The MAC provides two types of service:
Connection-Oriented Service (COS)
Connectionless Service (CLS)
Connection-Oriented Service (COS)
A Connection is a logical path between two peer STAs. A Connection may use either of the two MAC schemes:
Scheduled Access (TDMA)
Contention Access (CA)
First, the source and destination STAs set up a Connection between themselves. Information, such as the SAP used, whether in-order delivery is required, and traffic characteristics, are exchanged during the Connection setup process.
A Connection is realized by one more Links that actually carry the data traffic. Two types of Links are supported in HomePlug-AV:
Global Links
Local Links

Global Links use the Contention-Free Region and have dedicated bandwidth allocations from the CCo. The CCo is involved in the link-setup procedures. The source and destination STAs can request sufficient bandwidth from the CCo to guarantee QoS.
Local Connection s use the CP, and do not involve the CCo in the Connection setup or bandwidth-allocation process. They are used for connection-oriented applications that are not bandwidth demanding, but would like to support, for example, in-order delivery.
The GLID and LLID are used to identify Global Links and Local Links, respectively. Packets received can be delivered to the appropriate SAP at the destination STA based on the GLID or LLID.
Connectionless Service (CLS)
Connectionless Service (CLS) is used mainly for bursty traffic that does not have a strict QoS requirement. Prior connection setup between the source and destination STAs is not required. Packets are transmitted using CSMA/CA in the CP. Four reserved values of LLIDs are used to identify Connectionless Services. Sufficient information is carried inside the packets themselves for the destination STAs to deliver the packets to the appropriate SAP.

MAC Data Service

The MAC data service provides reliable transport of a MSDU from one MAC data service access point to one or more other MAC data service access points.
MD_DATA.REQ
The MD_DATA.REQ primitive requests a transfer of an MSDU from a local MAC Data SAP to a single-peer MAC Data SAP, or multiple-peer Data SAPs in the case of group addresses.
Table 1244: MD_DATA.REQ Primitive

Primitive	MD_DATA.REQ
Parameter Name	Description
Original Destination Address	A 48-bit address of the receiver that is the ultimate destination of this MSDU. The address format follows the corresponding fields described in the IEEE 802.3 standard.
Original Source Address	A 48-bit address of the station from which this MSDU originated. The address format follows the corresponding fields described in the IEEE 802.3 standard.
Convergence Layer SAP Type	A 3-bit field that defines the protocol and other characteristics of the MSDU Payload. 0b000 = Ethernet II-class SAP (refer to Section 12.3.2.1.1) 0b001 - 0b111 = reserved
Link Identifier	An 8-bit field associated with the payload being carried by this MSDU. For a description of the various types of LIDs and how they are used, refer to Section 5.2.1.4.1.

Payload Length	Length in octets of the payload field. The MAC uses this information together with the presence/absence of the ATS in the MAC Frame to calculate the total MAC Frame Length.
Arrival Time Stamp	The value of the sender's Network Time Base at the time when the MSDU Payload arrived at the sender's CL SAP. ATS is used as part of jitter-control mechanism (refer to Section 6.7.3). The presence of ATS is negotiated during connection setup, based on the QoS requirement specified in the CSPEC.
MSDU Payload	The payload field of the MSDU to be transmitted by the MAC sublayer entity. The content of the MSDU's payload depends on the CL SAP that generated the MSDU. MSDU is an optional field and shall only be present when there is no Management Message present in the primitive.
Management Message	Contains the management information. The organization of the Management Message shall follow the format described in Chapter 11. Management Message is an optional field and shall be present only when there is no MSDU Payload present in the primitive. MD_DATA.REQ primitive shall contain either MSDU Payload or Management Message, but not both.

MSDU Payload for Ethernet II-Class SAP

Ethernet II-class SAP shall carry the entire IEEE 802.3 frame in the MSDU Payload field. This includes the Original Destination Address, Original Source Address, Optional VLAN Tag, Ethertype/Length, and Data fields present in the Ethernet frame.

Figure 121: MSDU Payload Format for Ethernet II-Class SAP

MD_DATA.CNF

The MD_DATA.CNF primitive acknowledges the receipt of the MD_DATA.REQ and indicates the result of the requested transmission.

Table 1242: MD_DATA.CNF Primitive

Primitive	MD_DATA.CNF
Parameter Name	Description
Status	Indicates whether the associated MD_DATA.REQ was successful

MD_DATA.IND
The MD_DATA.IND primitive indicates a transfer of an MSDU to a local MAC Data SAP from a single-peer MAC Data SAP.
Table 1243: MD_DATA.IND Primitive

Primitive	MD_DATA.REQ
Parameter Name	Description
Original Destination Address	A 48-bit address of the receiver that is the ultimate destination of this MSDU. The address format follows the corresponding fields described in the IEEE 802.3 standard.
Original Source Address	A 48-bit address of the station from which this MSDU originated. The address format follows the corresponding fields described in the IEEE 802.3 standard.
Convergence Layer SAP Type	The interpretation of this field is the same as the corresponding CL SAP Type in Section 12.3.2.1.
Link Identifier	The interpretation of this field is the same as the corresponding Link Identifier in Section 12.3.2.1.
Payload Length	Length of the payload (i.e., MSDU Payload or MM Message), in octets
Arrival Time Stamp	The interpretation of this field is the same as the corresponding Arrival Time Stamp in Section 12.3.2.1.
MSDU Payload	The interpretation of this field is the same as the corresponding MSDU Payload in Section 12.3.2.1.
Management Message	The interpretation of this field is the as the corresponding Management Message in Section 12.3.2.1.

MAC Management Service
For information about the MAC Management Service, refer to Section 5.2.

Appendices
Priority Mapping (Informative)
The current version of the IEEE 802.1 standard describes the use of user priorities and access priorities in a bridged-network environment. User priorities are the priorities that a user or application requests be associated with its traffic. Access priorities are the number of differentiated traffic classes that a MAC provides. In subclause 7.7.3, IEEE 802.1D provides the following

mapping of user priorities to traffic classes.

Table 131: Recommended User Priority-to-Traffic Class Mappings

		Number of Available Traffic Classes						
	1	2	3	4	5	6	7	8
User Priority	0 (default)	0	0	0	1	1	1	1	2
	1	0	0	0	0	0	0	0	0
	2	0	0	0	0	0	0	0	1
	3	0	0	0	1	1	2	2	3
	4	0	1	1	2	2	3	3	4
	5	0	1	1	2	3	4	4	5
	6	0	1	2	3	4	5	5	6
	7	0	1	2	3	4	5	6	7

Note: The rationale behind the choice of values in Table 131 is discussed in H.2 of IEEE 802.1D. A consequence of the mapping shown is that frames carrying the default user priority (0) are given preferential treatment relative to user priorities 1 and 2 in HLEs that implement four or more traffic classes.

As with HomePlug AV, GREEN PHY provides four differentiated traffic classes at the PHY level, corresponding to the four channel access priorities. In Table 131, the mapping from column four (highlighted) is recommended, where HomePlug channel access priorities 0 through 3 correspond to traffic classes 0 through 3.

Both HomePlug AV and GREEN PHY QoS functions differentiate between eight levels of user priority, eliminating the need for mapping at the higher layers.

This priority mapping allows both HomePlug AV and GREEN PHY to operate with the industry standard Request for Comments (RFC) 2205 Resource Reservation Protocol (RSVP [16]) and the Internet draft standard Subnet Bandwidth Manager (SBM) to provide differentiated QoS levels for multimedia traffic.

Table 132 is derived from H.2 of IEEE 802.1D and defines the user priorities that should be assigned to application classes.

Table 132: Recommended Application Class-to-User Priority Mappings

User Priority	Application Class
7	a) Network Control — characterized by a “must-get-there” requirement to maintain and support the network infrastructure.
6	b) “Voice” — characterized by less than 10 ms delay, and hence maximum jitter (one-way transmission through the LAN infrastructure of a single campus).
5	c) “Video” or “Audio” — characterized by less than 100 ms delay.

4	d) Controlled Load — important business applications subject to some form of "admission control," be it pre-planning of the network requirement at one extreme to bandwidth reservation per flow at the time the flow is started at the other.
3	e) Excellent Effort — or "CEO's best effort," the best-effort type services that an information-services organization would deliver to its most important customers.
0	f) Best Effort — LAN traffic as we know it today. (This user priority is actually serviced at a higher priority than user priorities 1 and 2 to accommodate legacy entities.)
1,2	g) Background — bulk transfers and other activities that are permitted on the network, but that should not impact the use of the network by other users and applications.

User Experiences (UEs) (Informative)

This informative section describes typical user experiences (UEs) that are supported by HomePlug AV and GREEN PHY. These user experiences reflect the way in which the user interacts with the devices as they are being configured. They will depend upon how the device manufacturer implements the user interface for the device and what configuration is performed before the user installs the device. The various UEs reflect and are supported by underlying protocols that distribute the Network Membership Key (NMK), which defines an AV Logical Network. Possession of the NMK allows a device to join the corresponding AVLN. Two NMK distribution methods (supporting UE2 and UE3) are very secure, while the third (supporting UE4) sacrifices a measure of security for convenience.

Four basic UEs are anticipated:

User plugs devices in a set into the outlets and they connect by themselves

User enters NPW to get a device to join an AVLN (devices with rich user interfaces)

User enters DPW to add another device to an AVLN (at least one device with rich user interface)

User pushes a button on each of two devices to get them to connect to each other

In addition, the manufacturer should provide each device with a reset mechanism (e.g., a reset button) and should provide the user with some indication of the state of the device and the network. If the device supports the Simple Connect mechanism (refer to Section 13.2.4) using button presses, and only has one button, then it is recommended that only a long duration button press be interpreted as "Reset." In this case, reset should cause the device to change Security Level to SL-SC. Care should be taken to shield the button from inadvertent presses, and a button press sustained for too long should be ignored.

Indication to the user of the state of the device and the network may be done with one or more

LEDs, with one or more colors. As a minimum, the device should indicate:
That the power is on.
Whether the device detects other traffic on the power line.
Whether the device is part of an AVLN.
Which security mode the device is in (i.e., SL-HS or SL-SC).
Feedback indicating an error when a user presses the button when the device is in SL-HS is also desirable.

UE1 – Preconfigured Set of Devices

A manufacturer may package several devices as a set (e.g., a home theater audio component set). In this case, the manufacturer may choose to set the NMK on all devices in the set to the same value. Since all the devices have the same NMK out of the box, the user need only plug them in for all the devices to discover one another and form an AVLN without user intervention.
If the Security Level is set to SL-HS, then it is recommended that the manufacturer derive the NMK from a random NPW, and that the NPW be included in the packaging. This is so that the user can add new devices to the network using UE2. UE4 will not be possible.
If the Security Level is set to SL-SC, then the user can employ Simple Connect methods (UE4) to add new devices. UE2 will not be possible.
Regardless of Security Level, if one or more of the devices has a user interface that allows the user to enter the DPW of a new device, then UE3 is also available.
This mechanism provides very high security for the devices in the pre-packaged set, as long as no other devices are added, even if the Security Level of the network is SL-SC. For networks at SL-SC, adding devices to the network using Simple Connect (UE4) exposes the network to possible compromise.
Note: This approach has the drawback that a user who purchases multiple such sets and installs them without any user intervention will create one AVLN per set of devices. This will cause proliferation of AVLNs, neighbor networks, use up Beacon slots, and create unnecessary overhead in AVLN management. The user should be advised to add new devices to an existing AVLN, even when they come as a preconfigured set.

Informative Text
Manufacturers are cautioned against shipping large numbers of devices with the same NPW and hence, NMK. All populations of such devices capable of communicating with one another will attempt to form a single AVLN, which will degrade performance considerably if the network is physically dispersed enough to have hidden nodes, particularly if there are multiple layers of hidden nodes.

UE2 – Network Password Entry

A device that has a user interface suitable for entry of alphanumeric characters can allow the user to select and enter a Network Password (NPW). If there are other devices already in an AVLN, then the user must know the NPW of the existing network to cause the new device to join the existing AVLN. The Security Level for the new device will be SL-HS, so UE4 will not be possible for devices in this network.
This approach is very secure for key distribution, since the NMK is never sent over the network.

However, human selection of the NPW can expose networks formed in this manner to password-guessing attacks. It is therefore recommended that human selected passwords be much longer than the minimum length of 12 characters.

UE3 – Device Password Entry

If an AVLN has a device with a user interface suitable for entry of alphanumeric characters, the user can enter the Device Password (DPW) of a device the user wishes to add to the AVLN. The DPW is a unique alphanumeric string set by the manufacturer and provided with the device (e.g., with the documentation and/or printed on a label attached to the device itself). The user needs only to enter the DPW in the appropriate text box to cause the device on which the DPW is entered to distribute the NMK to the device whose DPW is entered, causing it to join the existing network. This distribution method is very secure (as long as the DPW is not easily guessable) and is supported for both security levels.

UE4 – Simple Connect (Button Push)

To support easy connection of devices packaged separately that might not have rich user interfaces (i.e., capable of character entry) supporting UE2 or UE3, both HomePlug AV and GREEN PHY support the Simple Connect experience. Generically, the user presses a button on one device, then presses a button on another device within a short amount of time to cause these two devices to join the same network. While the amount of time a device remains promiscuous is the vendor's choice, the recommended range for this vulnerable time is between 30 seconds and two minutes, with one minute as the default value. Under some circumstances, a vendor may elect a value outside this range, or even to provide the choice of duration to the user.

This mechanism trades off convenience for users and low-cost user interfaces for lowered security. Simultaneous execution of this mechanism can cause networks to admit stations other than those desired by the user, and sufficiently equipped and sophisticated attackers can compromise the key exchange itself, so this is only recommended for non-sensitive information applications.

While this experience is described below by the user pushing buttons, a device with richer interface may have a menu selection that is equivalent to pushing a button and may be more specific about whether a device is to keep its current NMK ("Add" the other device) or discard its current NMK ("Join" the other device). The descriptions below assume a single button that the user presses briefly to indicate the desire for two devices to join with each other in a common network.

Note that a device that has an NMK-HS shall be configured to ignore button presses, as the NMK-HS must not be distributed using UKE (the protocol underlying the Simple Connect experience). In this case, the user must first change the Security Level of the device (by changing its NMK or resetting) before the device will respond to the button presses and permit the Simple Connect experiences.

UE4a – Two New Devices Form a New Network Using SC

When a user has two devices that are not already part of a network, the user needs only to press the button on one device, then press the button on the other device within a reasonable amount of time. The time constraint is determined by the manufacturer, but 1-2 minutes should be typical. As long as no other devices have their buttons pushed as this process continues, the two devices should detect one another and form a new AVLN.

In the unlikely event that one or both of the devices is "recruited" by some third device (e.g., a

neighbor is adding devices using Simple Connect at the same time), the user may reset the device(s).

UE4b – Adding a New Device to an Existing Network Using SC

When the user wishes to add a new device to an existing network, the user must press the button on the new device, and press the button on a device that is already in the desired network. The two devices should quickly detect one another and the device in the existing network should share the NMK of that network with the new device. The order in which the buttons are pressed does not matter, but they should be pressed within the time constraint(s) set by the manufacturer(s).

UE4c – Adding Multiple New Devices Using SC Chaining

To add several new devices to an existing network using the button-push mechanism described in Section 13.2.4, the user must press two buttons for each new device (the button on the new device, and the button on a device that is already in the desired network). A vendor may implement a mode of operation in which a device in the network remains promiscuous until some period of time elapses in which new devices are added .This allows the user to press the button once on one device in the network, then press the button on each new device once.

Changing Security Levels on a Device

Since networks are defined by their NMKs, and NMKs are associated with a Security Level that determines how they may be distributed, the user may find that a device is using an NMK with a Security Level that is incompatible with their needs. This is the case when a device is configured to use Simple Connect, but the user desires a greater level of security. Conversely, a user may have a device that has an NMK-HS, and consequently ignores button presses (except for "Reset"). In each of these cases, the user needs to be able to change the SL of the device. It is possible to do this through a menu selection in a device with a rich user interface, but may be done in other ways also.

Changing SL-HS to SL-SC

When a user has a device with an NMK-HS, it must not distribute the NMK-HS using UKE (the protocol underlying Simple Connect experience). Thus the device shall ignore "Join" and "Add" button presses (and should indicate an error to the user if they are pressed). To cause the device to enter Simple Connect Mode, the user may:

- Specify a Security Level mode change to SL-SC from the user interface.
- Enter the device's DPW on another device that is in SL-SC (the other device must have a rich user interface).
- Reset the device using a "Reset" button or menu selection.

In all cases, the device will discard its old NMK and either receive a new one (case 2) or generate a new NMK (cases 1 and 3).

Changing SL-SC to SL-HS

When a user has a device that is in SL-SC but wishes the device to be in SL-HS, the user may:

- Specify a Security Level mode change to SL-HS from the user interface.
- Enter an NPW and specify SL-HS (the device must have a rich user interface).
- Enter the device's DPW on another device that is in SL-HS (the other device must have a rich user interface).

As when changing from SL-HS to SL-SC, the device will discard its old NMK-SC and either generate a new one (case 1) or receive the NMK-HS (cases 2 and 3). If an NMK-HS is generated,

the device may do this by generating a random NPW first, from which the NMK-HS is then derived. At the option of the manufacturer, this NPW may be displayed to the user in order that it can be used in UE2 with other devices.

Security State Transition Diagrams

This section describes the state machine for security and key management.

State Definitions for Security Protocol State Machine

Figure 131 and following provide diagrams showing security state transitions and their triggers. In these figures, detailed states of the protocols are not shown.

An Unassociated STA may create its own AVLN due to:

Failure to detect any Beacons

Detection of another Unassociated STA that has a matching NID

When in the DAK-encrypted NMK provisioning protocol, detection of another STA in SC-Join that is less CCo-capable

When in SC-Join, detection of another STA in SC-Join that is less CCo-capable

These cases are not distinguished in the diagrams.

Figure 131: State Transition Diagram for HS Security Level

Figure 132: State Transition Diagram for Simple-Connect Security Level

Test Vectors

The HomePlug AV specification includes a set of transmit test vectors that provide a variety of examples of MAC Frames and MPDUs, as well as a sample Matlab implementation of an AV transmit PHY.

These vectors are distributed as a ZIP file called AVVectors v1.1.zip. This file should be verified to be a true copy of the original by checking the Message Digest using SHA256 as specified in FIPS 180-2 (refer to Section 1.1).

Table 13-2b: Test Vectors

Filename	SHA-256 Message Digest
AVVectors v1.1.zip	437ce9d1e0c70255ee1f81aca96a6ab920a7827 b177011c4c9598f8c116c9ca6

In the ZIP file, there is a directory called \AVVectors\PHY that contains the sample PHY model. The directory \AVVectors\Work contains the various transmit test vectors, inputs, and outputs. Also included is a readme.txt file that explains the inputs and outputs used in the vectors. For more information about the AV vectors, refer to the readme.txt file.

For reference, the MatLab vectors were run with MatLab v7.0.1 using the MatLab Communications Toolbox. All input files are in plain text format. Output files are provided in MatLab .MAT format as well as in plain text.

The test vectors and the PHY model contained in the AVVectors v1.1.zip file shall be treated as Normative.

Example Hashed NMK, Hashed NID, and NMK Provisioning MME Using DAK

11	66	C5		AES Key [88

Table 13-3 shows examples of passwords hashed to AES Encryption Keys with AES octet number 0 corresponding to the leftmost octet (byte array position 0) of the hashed key octet string. Table 13-4 shows an example NID hashed from the NMK in Table 13-3. Table 13-4 and Table 13-5 show an example MME provisioning the NMK with the DAK mechanism. Table 13-4 shows an example of a CM_SET_KEY.REQ message that contains the NMK from Table 13-3. Table 13-6 shows an example CM_ENCRYPTED_PAYLOAD.IND message where the CM_SET_KEY.REQ payload MME from Table 13-5 is encrypted with the DAK from Table 13-3.

Note: The “Test Value” column in Table 13-5 and Table 13-6 indicates the test values in hexadecimal format, starting from the least-significant octet. For example, the OSA field in these examples has a value of 004647484950. The least-significant and most-significant octets in the field are 0x00 and 0x50, respectively.

Table 133: Example AES Encryption Keys Hashed from Passwords

Octet	NMK-HS	DAK	Description	Description	Description
	“HomePlugAV0123”	“DAK_Password”	Key Octet Order	AES Key order for Encrypted Payload	AES Key order for PBB Encryption
0	B5	EE	Leftmost Key Octet	AES Key [0 - 7]	AES Key [7 - 0]
1	93	7F		AES Key [8 - 15]	AES Key [15 - 8]
2	19	57		AES Key [16 - 23]	AES Key [23 - 16]
3	D7	88		AES Key [24 - 31]	AES Key [31 - 24]
4	E8	E2		AES Key [32 - 39]	AES Key [39 - 32]
5	15	A0		AES Key [40 - 47]	AES Key [47 - 40]
6	7B	21		AES Key [48 - 55]	AES Key [55 - 48]
7	A0	C9		AES Key [56 - 63]	AES Key [63 - 56]
8	01	99		AES Key [64 - 71]	AES Key [71 - 64]
9	B0	46		AES Key [72 - 79]	AES Key [79 - 72]
10	18	9A		AES Key [80 - 87]	AES Key [87 - 80]

11 FMI	66	2 C5	Fragmentation Management	AES Key [88 - 95]	AES Key [95 - 88]
12	9C	2A		AES Key [96 - 103]	AES Key [103 - 96]
13	CE	F3		AES Key [104 - 111]	AES Key [111 - 104]
14	E3	0A		AES Key [112 - 119]	AES Key [119 - 112]
15	0D	06	Rightmost Key Octet	AES Key [120 - 127]	AES Key [127 - 120]

Table 134: Example NID Offset Hashed from NMK-HS with Appended Security Level

Octet	NID	Description
0	0x02	Leftmost Octet of 52 Bit Hashed NID Offset
1	0x6B	
2	0xCB	
3	0xA5	
4	0x35	
5	0x4E	
6	0x18	Left Nibble = 0x1 HS Security Level Right Nibble = 0x8, the rightmost nibble of the 52 Bit NID offset

Table 135: Example CM_SET_KEY.REQ Message Provisioning NMK Using the DAK

Field	Field Size (Octets)	Definition	Example Value (Left Octet = LSByte)
ODA	6	Original Destination Address	003132333435
OSA	6	Original Source Address	004647484950
VLAN Tag	0 or 4	IEEE 802.1Q VLAN Tag (optional)	None
MTYPE	2	0x88e1 (IEEE-assigned Ethertype)	88e1
MMV	1	Management Message Version	01
MMTYPE	2	Management Message Type	0860 CM_SET_KEY.REQ

FMI	2	Fragmentation Management Information	0000
Key Type	1	Key Type	01 NMK (AES-128)
My Nonce	4	Random number that will be used to verify next message from other end; in encrypted portion of payload.	00112233
Your Nonce	4	Last nonce received from recipient; it will be used by recipient to verify this message; in encrypted portion of payload.	44332211
PID	1	Protocol for which Set Key is asserted Note: This is included since MME is not always in encrypted payload. Refer to Section 11.5.2.3 for information.	02 Provision STA with NMK using DAK
PRN	2	Protocol Run Number (refer to Section 11.5.2.4)	2D37
PMN	1	Protocol Message Number (refer to Section 11.5.2.5)	03
CCo Capability	1	The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in Section 4.4.3.15.4.6.2. The six MSBs of this field are set to 0b000000	02 Level-2 CCo Capable

NID	7	Network ID of transmitting STA The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.	026BCBA5354E18 NID from Table 134: Example NID Offset Hashed from NMK-HS with Appended Security Level
NewEKS	1	New Encryption Key Select or New Payload Encryption Key Select depending upon value of Key Type The four LSBs of this field contain the PEKS (refer to Section 11.5.2.1) or EKS (refer to Section 4.4.1.5.2.8). The four MSBs shall be set to 0x0.	01 NewEKS is ignored when Key Type is NMK
NewKEY	0, 16 or 384	New Key (none, 128-bit AES Key or 3072-bit Hash Key)	B59319D7E8157BA001B018669CCEE30D NMK from Table 13-3

Table 136: Example CM_ENCRYPTED_PAYLOAD.IND Message Provisioning NMK Using the DAK

Field	Field Size (Octets)	Definition	Example Value (Left Octet = LSByte)
ODA	6	Original Destination Address	003132333435
OSA	6	Original Source Address	004647484950
VLAN Tag	0 or 4	IEEE 802.1Q VLAN Tag (optional)	None
MTYPE	2	0x88e1 (IEEE-assigned Ethertype)	88e1
MMV	1	Management Message Version	01

MMTYPE		2		Management Message Type	0660 CM_ENCRYPTED_PAYLOAD.IND
FMI		2		Fragmentation Management Information	0000
PEKS RF		1 0-15	Random Filler: A number (between 0 and 15) of random filler octets included in Encrypted Payload to make position of	Payload Encryption Key Select (**Unencrypted**) The four LSBs of this field contain the PEKS. The four MSBs shall be set to 0x0.	00 Destination STA's DAK (AES 128 bit key)
AVLN Status		1		AVLN status of source. (**Unencrypted**)	05 Associated with an AVLN and PCo Capable
PID		1		Protocol ID (**Unencrypted**)	02 Provision STA with NMK using DAK
PRN		2		Protocol Run Number (**Unencrypted**)	2D37
PMN		1		Protocol Message Number (**Unencrypted**)	03
IV		16		AES Encryption Initialization Vector (**Unencrypted**)	FEDCBA9876543210FEDCBA9876543210
Len		2		Length of MM, in octets (**Unencrypted**)	3900 Length of CM_SET_KEY.REQ

RF	0-15	Random Filler: A number (between 0 and 15) of random filler octets included in Encrypted Payload to make position of Protocol fields unpredictable (**Encrypted Payload**)	2468ACE035	**DAK used for Encryption:** EE7F5788E2A021C999469AC52AF30A06 from Table 133 **Encrypted Payload:** A9A887CA49530931BB7360AD22B284619EAFB1078A318564A90BD1D3E629B7BD008A626840B13DBDDC3E26E512331F9E67CC44187681F653D0DBE18FBB0ED9DF095CC6B89F21657B203ED6593635663C
MM	Var	MM (Management Message – refer to Section 11.1) can be any legal Management Message except CM_ENCRYPTED_PAYLOAD.IND (**Encrypted Payload**)	See CM_SET_KEY.REQ above	
CRC	4	Checksum on MME (**Encrypted Payload**)	F1662820	

PID	1	Protocol ID (**Encrypted Payload**)	02 Provision STA with NMK using DAK	
PRN	2	Protocol Run Number (**Encrypted Payload**)	2D37	
PMN	1	Protocol Message Number (**Encrypted Payload**)	03	
Padding	Var	To adjust size of Encrypted Payload to 128-bit boundary (**Encrypted Payload**)	ACBCD2114D AE1577C6	
RFLen	1	0x00 – 0x0F = Length of Random Filler (Bit numbers are before encryption and after decryption). (**Encrypted Payload**) 0x10 – 0xFF = reserved	05	

Example of NMK Provisioning Using UKE Mechanism

Table 137: CM_GET_KEY.REQ Provisioning NMK Using UKE – Message 1 through Table 1312: CM_ENCRYPTED_PAYLOAD.IND Provisioning NMK Using UKE – Message 4 show example messages provisioning the NMK using the UKE mechanism.

Table 137: CM_GET_KEY.REQ Provisioning NMK Using UKE – Message 1 is Message-1, **CM_GET_KEY.REQ,** containing the first Hash Key.

Table 138: CM_GET_KEY.CNF Provisioning NMK Using UKE – Message 2 is Message-2, CM_GET_KEY.CNF, containing the second Hash Key and the PEKS of the TEK that is generated.

Table 139: CM_SET_KEY.REQ Provisioning NMK Using UKE – Payload of Message 3 and Table 1310: CM_ENCRYPTED_PAYLOAD.IND Provisioning NMK Using UKE –

Message 3
 together are an example of Message 3, the MME provisioning the NMK. Table 139: CM_SET_KEY.REQ Provisioning NMK Using UKE – Payload of Message 3
 is the CM_SET_KEY.REQ MME. Table 1310: CM_ENCRYPTED_PAYLOAD.IND Provisioning NMK Using UKE – Message 3
 shows the CM_ENCRYPTED_PAYLOAD.IND MME that carries the CM_SET_KEY.REQ. The payload of the CM_ENCRYPTED_PAYLOAD.IND is encrypted with the TEK that was generated from the Hash Keys and whose PEKS was set by the sender of Message 2.
Table 1311: CM_SET_KEY.CNF Provisioning NMK Using UKE – Payload of Message 4
 and Table 1312: CM_ENCRYPTED_PAYLOAD.IND Provisioning NMK Using UKE – Message 4
 together are an example of Message 4, the MME acknowledging the receipt of the NMK. Table 1311: CM_SET_KEY.CNF Provisioning NMK Using UKE – Payload of Message 4
 is the CM_SET_KEY.CNF MME. Table 1312: CM_ENCRYPTED_PAYLOAD.IND Provisioning NMK Using UKE – Message 4
 shows the CM_ENCRYPTED_PAYLOAD.IND MME that carries the CM_SET_KEY.CNF. The payload of the CM_ENCRYPTED_PAYLOAD.IND MME is encrypted with the NMK.
CM_GET_KEY.REQ
Table 137: CM_GET_KEY.REQ Provisioning NMK Using UKE – Message 1

Field	Field Size (Octets)	Definition	Example Value (Left Octet = LSByte)
ODA	6	Original Destination Address	003132333435
OSA	6	Original Source Address	004647484950
VLAN Tag	0 or 4	IEEE 802.1Q VLAN Tag (optional)	None
MTYPE	2	0x88e1 (IEEE-assigned Ethertype)	88e1
MMV	1	Management Message Version	01
MMTYPE	2	Management Message Type	0C60 CM_GET_KEY.REQ
FMI	2	Fragmentation Management Information	0000
Request Type	1	Request Type 0x00 = direct 0x01 = relayed 0x02 - 0xFF = reserved	00 direct

Requested Key Type	1	Requested Key Type Interpretation of this field is the same as in Section 11.5.4.1.	00010203040506070 04 8090A0B0C0D0E0F Hash Key 101112131415161 71 (Random-3072) 8191A1B1C1D1E1F
NID	7	Network ID of transmitter or NID of AVLN that transmitter wants to join. The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two MSBs shall be set to 0b00.	20212223242526272 8292A2B2C2D2E2F 30313233343536373 8393A3B3C3D3E3F 40414243444546474 8494A4B4C4D4E4F 50515253545556575 8595A5B5C5D5E5F 60616263646566676 8696A6B6C6D6E6F 70717273747576777
My Nonce	4	Random number that will be used to verify next message from other end (required for all methods).	8797A7B7C7D7E7F FFEEDDCC
PID HASH KEY	1 var	Hash Key is present only when Requested Key Type is HASH KEY	03 Protocol ID Provision STA with NMK using UKE
PRN	2	Protocol Run Number	AB34
PMN	1	Protocol Message Number	01

HASH KEY	var	Hash Key is present only when Requested Key Type is HASH KEY	00010203040506070 8090A0B0C0D0E0F 10111213141516171 8191A1B1C1D1E1F 20212223242526272 8292A2B2C2D2E2F 30313233343536373 8393A3B3C3D3E3F 40414243444546474 8494A4B4C4D4E4F 50515253545556575 8595A5B5C5D5E5F 60616263646566676 8696A6B6C6D6E6F 70717273747576777 8797A7B7C7D7E7F 80818283848586878 8898A8B8C8D8E8F 90919293949596979 8999A9B9C9D9E9F A0A1A2A3A4A5A6 A7A8A9AAABACA DAEAFB0B1B2B3B 4B5B6B7B8B9BAB BBCBDBEBFC0C1 C2C3C4C5C6C7C8C 9CACBCCCDCECF D0D1D2D3D4D5D6 D7D8D9DADBDCD DDEDFE0E1E2E3E4 E5E6E7E8E9EAEBE CEDEEEFF0F1F2F3 F4F5F6F7F8F9FAF BFCFDFEFF000102 030405060708090A0 B0C0D0E0F1011121 31415161718191A1 B1C1D1E1F2021222 32425262728292A2 B2C2D2E2F3031323 33435363738393A3 B3C3D3E3F4041424

CM_GET_KEY.CNF		Random number that	

Table 138: CM_GET_KEY.CNF Provisioning NMK Using IKE – Message 2

Field My Nonce	Field Size (Octets)	Definition	Example Value (Left Octet = LSByte)
ODA	6	Original Destination Address	004647484950
OSA	6	Original Source Address	003132333435
VLAN Tag	0 or 4	IEEE 802.1Q VLAN Tag (optional)	None
MTYPE	2	0x88e1 (IEEE-assigned Ethertype)	88e1
MMV	1	Management Message Version	01
MMTYPE	2	Management Message Type	0D60 CM_GET_KEY.CNF
FMI	2	Fragmentation Management Information	0000
Result	1	Result 0x00 = key granted 0x01 = request refused 0x02 = unsupported method/key type 0x03 - 0xFF = reserved	00 key granted
KeyType	1	Key Type (refer to Section 11.5.4.1). Values = NMK (AES-128) | NEK (AES-128) | TEK (AES-128 | HASH_KEY (Random-3072) | nonce-only) are permitted in this message.	04 Hash Key (Random-3072)

My Nonce	4	Random number that will be used to verify next message from other end; in encrypted portion of payload.	33221100
Your Nonce	4	Last nonce received from recipient; it will be used to by recipient to verify this message; in encrypted portion of payload.	FFEEDDCC
NID	7	Network ID of STEI STA The 54 LSBs of this field contain the NID (refer to Section 4.4.3.1). The two security bits shall be set to 0b00.	3F5B4FDC4D3D05
EKS	1	EKS or PEKS value depending upon Key Type The four LSBs of this field contain the PEKS (refer to Section 11.5.2.11) or EKS (refer to Section 4.4.1.5.2.8. The four MSBs shall be set to 0x0. If nonce-only, set to 0x0F.	03 This is the PEKS assigned to the TEK that will generated from the Hash Keys
PID	1	Protocol ID	03 Provision STA with NMK using UKE
PRN	2	Protocol Run Number	AB34
PMN	1	Protocol Message Number	02

Key	var	Encryption or Hash Key	FFFEFDFCFBFAF9 F8F7F6F5F4F3F2F1 F0EFEEEDECEBEA E9E8E7E6E5E4E3E2 E1E0DFDEDDDCD BDAD9D8D7D6D5 D4D3D2D1D0CFCE CDCCCBCAC9C8C 7C6C5C4C3C2C1C0 BFBEBDBCBBBAB 9B8B7B6B5B4B3B2 B1B0AFAEADACA BAAA9A8A7A6A5 A4A3A2A1A09F9E 9D9C9B9A99989796 9594939291908F8E8 D8C8B8A898887868 584838281807F7E7 D7C7B7A797877767 574737271706F6E6 D6C6B6A696867666 564636261605F5E5 D5C5B5A595857565 554535251504F4E4 D4C4B4A494847464 544434241403F3E3 D3C3B3A393837363 534333231302F2E2 D2C2B2A292827262 524232221201F1E1 D1C1B1A191817161 514131211100F0E0 D0C0B0A090807060 50403020100FFFEF DFCFBFAF9F8F7F 6F5F4F3F2F1F0EFE EEDECEBEAE9E8E 7E6E5E4E3E2E1E0D FDEDDDCDBDAD 9D8D7D6D5D4D3D 2D1D0CFCECDCC CBCAC9C8C7C6C5

TEK Computation The TEK used below is computed as outlined in Section 7.10.2.6. The computed TEK = 36 6A 3B 2D 8A 0F C6 DD CA E8 C5 56 36 7D 4B EB		Protocol for which Set Key is asserted Note: This is included since MMs not always is encrypted	
PID	1		

CM_SET_KEY.REQ in CM_ENCRYPTED_PAYLOAD.IND

Table 139 – CM_SET_KEY.REQ Provisioning NMK Using HKE – Payload of Message 3

Field	Field Size (Octets)	Definition	Example Value (Left Octet = LSByte)
ODA	6	Original Destination Address	003132333435
OSA	6	Original Source Address	004647484950
VLAN Tag	0 or 4	IEEE 802.1Q VLAN Tag (optional)	None
MTYPE	2	0x88e1 (IEEE-assigned Ethertype)	88e1
MMV	1	Management Message Version	01
MMTYPE	2	Management Message Type	0860 CM_SET_KEY.REQ
FMI	2	Fragmentation Management Information	0000
Key Type	1	Key Type	01 NMK (AES-128)
My Nonce	4	Random number that will be used to verify next message from other end; in encrypted portion of payload.	FFEEDDCC Note: It is not necessary for a STA generate more than one new nonce within the same protocol run
Your Nonce	4	Last nonce received from recipient; it will be used by recipient to verify this message; in encrypted portion of payload.	33221100

PID	1	Protocol ID (refer to Section 11.5.2.3)	03 Provision STA with NMK using UKE
NewEKS	1	New EKS (refer to Section 11.5.2.6)	01 NMK is encrypted with a DAK
PRN	2	Protocol Run Number (refer to Section 11.5.2.4)	AB34
PMN	1	Protocol Message Number (refer to Section 11.5.2.5)	03
CCo Capability	1	The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in Section 4.4.3.15.4.6.2. The six MSBs of this field are set to 0b000000	02 Level-2 CCo Capable
NID	7	Network ID of transmitting STA The 54 LSBs of this field contain the NID (refer to Section 3.4.3.1). The two MSBs shall be set to 0b00.	3F5B4FDC4D3D05

PEKS NewEKS	1 1	New Encryption Key Select The four LSBs of this field contain the	01 NewEKS is ignored when Key Type is NMK
		PEKS (refer to Section 11.5.2.1) or EKS (refer to Section 4.4.1.5.2.8). The four MSBs shall be set to 0x0.	
NewKEY	0, 16 or 384	New Key (none, 128-bit AES Key or 3072-bit Hash Key)	0088119922AA33BB44CC55DD66EE77FF (NMK)

Table 1310: CM_ENCRYPTED_PAYLOAD.IND Provisioning NMK Using UKE – Message 3

Field	Field Size (Octets)	Definition	Example Value (Left Octet = LSByte)
ODA	6	Original Destination Address	003132333435
OSA	6	Original Source Address	004647484950
VLAN Tag	0 or 4	IEEE 802.1Q VLAN Tag (optional)	None
MTYPE	2	0x88e1 (IEEE-assigned Ethertype)	88e1
MMV	1	Management Message Version	01
MMTYPE	2	Management Message Type	0660 CM_ENCRYPTED_PAYLOAD.IND
FMI	2	Fragmentation Management Information	0000

PEKS		1	Random Filler: A number (between 0 and 15) of random filler octets included in Encrypted Payload to make position of Protocol fields unpredictable (**Encrypted Payload**)	Payload Encryption Key Select (**Unencrypted**) The four LSBs of this field contain the PEKS. The four MSBs shall be set to 0x0.	03 This is the PEKS for the TEK passed in the CM_GET_KEY.CNF MME
AVLN Status		1		AVLN status of source. (**Unencrypted**)	08 CCo of an AVLN
RF		0-15		123456789A	
PID		1		Protocol ID (**Unencrypted**)	03 Provision STA with NMK using UKE
PRN		2		Protocol Run Number (**Unencrypted**)	AB34
PMN		1		Protocol Message Number (**Unencrypted**)	03
IV		16		AES Encryption Initialization Vector (**Unencrypted**)	FEDCBA9876543210FEDCBA9876543210
Len		2		Length of MM, in octets (**Unencrypted**)	3900 Length of CM_SET_KEY.REQ

TEK used for Encryption:
366A3B2D8A0EC6DDCAE8C556367D4BEB

Encrypted Payload:
5332516FB8DCAEBD2D7BA1163409CFB114D35C9FE209269E1CDF9C44DBB161CA33A5E5A70120B47B0A0402C692B99E8C7B0499D1A2A475A480C

RF	0-15	Random Filler: A number (between 0 and 15) of random filler octets included in Encrypted Payload to make position of Protocol fields unpredictable (**Encrypted Payload**)	123456789A	**TEK used for Encryption:** 366A3B2D8A0FC6DDCAE8C556367D4BEB **Encrypted Payload:** 5332516FB8DCAEBD2D7BA1163409CFB114D35C9FE209269E1CDF9C44DBB161CA33A55A70120B47B0A0402C692B99E8C7B0499D1A2A475A480C6F9B0CE8FC70F5C039A9DB5A5783FE8A1AF324FFFDCCE3
MM	Var	MM (Management Message – refer to Section 11.1) can be any legal Management Message except CM_ENCRYPTED_PAYLOAD.IND (**Encrypted Payload**)	See CM_SET_KEY.REQ above	
CRC	4	Checksum on MME (**Encrypted Payload**)	607F75C6	
PID	1	Protocol ID (**Encrypted Payload**)	03 Provision STA with NMK using UKE	

MMTYPE	2	Management Message		
PRN	2	Protocol Run Number (**Encrypted Payload**)	AB34	
PMN	1	Protocol Message Number (**Encrypted Payload**)	03	
Padding	Var	To adjust size of Encrypted Payload to 128-bit boundary (**Encrypted Payload**)	DBF4C91A3CD A2F169B	
RFLen	1	0x00 – 0x0F = Length of Random Filler (Bit numbers are before encryption and after decryption). (**Encrypted Payload**) 0x10 – 0xFF = reserved	05	

CM_SET_KEY.CNF in CM_ENCRYPTED_PAYLOAD.IND

Table 1311: CM_SET_KEY.CNF Provisioning NMK Using UKE – Payload of Message 4

Field	Field Size (Octets)	Definition	Example Value (Left Octet = LSByte)
ODA	6	Original Destination Address	004647484950
OSA	6	Original Source Address	003132333435
VLAN Tag	0 or 4	IEEE 802.1Q VLAN Tag (optional)	None
MTYPE	2	0x88e1 (IEEE-assigned Ethertype)	88e1
MMV	1	Management Message Version	01

MMTYPE	2	The type of this message	0960 CM_SET_KEY.CNF
FMI	2	Fragmentation Management Information	0000
CCo Capability	1	1 = CCo capable 0 = not CCo capable	
Result	1	0x00 = success 0x01 = failure 0x02 – 0xFF = reserved	00
My Nonce	4	Random number that will be used to verify next message from other end; in encrypted portion of payload.	33221100
Your Nonce	4	Last nonce received from recipient; it will be used to by recipient to verify this message; in encrypted portion of payload.	FFEEDDCC
PID	1	Protocol for which Set Key is confirmed Note: This is included since MME not always in encrypted payload) Refer to Section 11.5.2.3 for information.	03 Provision STA with NMK using UKE
PRN	2	Protocol Run Number (refer to Section 11.5.2.4)	AB34
PMN	1	Protocol Message Number (refer to Section 11.5.2.5)	FF

CCo Capability	1	The two LSBs of this field contain the STA's CCo capability. The interpretation of these bits is the same as in Section 4.4.3.13.4.6.2. The six MSBs of this field are set to 0b000000.	02 Level-2 CCo Capable

Table 1312: CM_ENCRYPTED_PAYLOAD.IND Provisioning NMK Using UKE – Message 4

Field	Field Size (Octets)	Definition	Example Value (Left Octet = LSByte)
ODA	6	Original Destination Address	004647484950
OSA	6	Original Source Address	003132333435
VLAN Tag	0 or 4	IEEE 802.1Q VLAN Tag (optional)	None
MTYPE	2	0x88e1 (IEEE-assigned Ethertype)	88e1
MMV	1	Management Message Version	01
MMTYPE	2	Management Message Type	0660 CM_ENCRYPTED_ PAYLOAD.IND
FMI	2	Fragmentation Management Information	0000
PEKS	1	Payload Encryption Key Select (**Unencrypted**) The four LSBs of this field contain the PEKS. The four MSBs shall be set to 0x0.	01 NMK known to STA (AES 128 bit key)
AVLN Status	1	AVLN status of source. (**Unencrypted**)	05 Associated with an AVLN and PCo Capable

PID	1	Protocol ID (**Unencrypted**)	03 Provision STA with NMK using UKE
PRN	2	Protocol Run Number (**Unencrypted**)	AB34
PMN	1	Protocol Message Number (**Unencrypted**)	FF
IV	16	AES Encryption Initialization Vector (**Unencrypted**)	00112233445566778899AABBCCDDEEFF
Len	2	Length of MM, in octets (**Unencrypted**)	2100 Length of CM_SET_KEY.CNF

RF	0-15	Random Filler: A number (between 0 and 15) of random filler octets included in Encrypted Payload to make position of Protocol fields unpredictable (**Encrypted Payload**)	3456789012	**NMK used for Encryption:** 0088119922AA33BB44CC55DD66EE77FF **Encrypted Payload:** 8648E0A97FC3CE46283CE6D43F9C44E38DD55CC469216EACB8D873D7EC1A3369D38CFEC56088072550D6684B0A1C001A
MM	Var	MM (Management Message – refer to Section 11.1) can be any legal Management Message except CM_ENCRYPTED_PAYLOAD.IND (**Encrypted Payload**)	See CM_SET_KEY.CNF above	

CRC	4	Checksum on MME (**Encrypted Payload**)	B1FBF73D	
PID	1	Protocol ID (**Encrypted Payload**)	03 Provision STA with NMK using UKE	
PRN	2	Protocol Run Number (**Encrypted Payload**)	AB34	
PMN	1	Protocol Message Number (**Encrypted Payload**)	FF	
Padding	Var	To adjust size of Encrypted Payload to 128-bit boundary (**Encrypted Payload**)	34	
RFLen	1	0x00 – 0x0F = Length of Random Filler (Bit numbers are before encryption and after decryption). (**Encrypted Payload**) 0x10 – 0xFF = reserved	05	

Third Party Managed Security Deployment Scenarios

To use 3rd party managed security, at least one of the STAs in the network must have HLE software to communicate with the 3rd party security manager know as the Authentication Server (AS). Such a STA is called an Authenticator STA. How the Authenticator communicates with the AS is outside of scope.

There are three ways to authorize a STA (called the Supplicant STA) using a 3rd party security manager:

- DAK
- Push-button
- Direct entry

DAK Authorization

DAK authorization is recommended to be used when the network operator has knowledge of the STAs that will be part of the AVLN (e.g. they own or otherwise supply the STAs). DAK Authorization requires the network operator to know the MAC/DAK pair for all authenticated STAs.

The procedure to authorize a Supplicant STA using DAK Authorization is as follows:

When an Unassociated STA (aka the Supplicant STA) powers-on it broadcasts a CM_UNASSOCIATED_STA.IND MME (see 7.2.1). When an Authenticator STA receives an APCM_UNASSOCIATED_STA.IND, it sends the MAC address of the Supplicant STA to the AS. If the Supplicant STA is known by the AS (i.e., its MAC/DAK pair has been previously registered), then the AS will supply the Authenticator STA the DAK of the Supplicant STA. The Authenticator STA will then use the APCM_AUTHORIZE.REQ/CNF/IND (Section 12.2.2.14/15/16) primitives to pass NMK via DAK to the Supplicant STA.

Push Button Authorization

Push-button Authorization is recommended to be used when the consumer owns the STA and the network operator agrees to authenticate STAs based the STA's MAC address (i.e. the STAs MAC address must be pre-registered with the network operator. The DAK can be kept private to the consumer.

The procedure to authorize a Supplicant STA using Push Button Authorization is as follows:

When an Authenticator STA is placed in a SC-Add state, it waits until it receives an APCM_SC_JOIN.REQ primitive from the Supplicant STA. The Authenticator STA then sends the MAC address of the Supplicant STA to the AS. If this MAC address is know by the AS, the AS will reply to the Authenticator STA with an "OK to join" message. The Authenticator STA then responds with a CM_SC_JOIN.CNF.

Direct Entry Authorization

Direct entry Authorization can be used when a STA is also an Authenticator STA. As the Authenticator STA can communicate directly with the AS, it can authenticate itself to the AS and request the NMK from the AS.

The procedure to authorize a Supplicant STA using Direct Entry Authorization is as follows:

When a STA that is also an Authenticator STA powers-on, it may request the AS for the NMK for the AVLN. When the NMK is received the STA will use the Direct Entry of the NMK procedure (Section 7.10.3.3) to set the NMK.

PEV - EVSE Association (GREEN PHY)

Signal Level Attenuation Characterization (SLAC) enables a station to measure the signal level of its transmission at other stations in the network. It was designed for automotive applications where there may be multiple plug-in electric vehicles (PEV) and Electric

Vehicle Supply Equipment (EVSE). The signal level from a PEV is measured at EVSEs in order to determine uniquely which PEV is plugged in to which EVSE. The process leading to this decision will be called Green PHY PEV-EVSE Association (GreenPPEA). Unique and secure GreenPPEA between a PEV and the EVSE is essential for proper charging and billing purposes. It is not sufficient, however, and higher level processes are needed to authorize the EVSE to supply power to the PEV plugged in to it, and for the correct account to be charged for the received energy (refer to ISO/IEC 15118 series).

Informative Text
Note: Plug-in Electric Vehicles (PEV) is a subcategory of different types of Electric Vehicles (EV). In this application, PEVs plug into an external AC or DC power source, an EVSE, for charging energy. The communications between the PEV and EVSE may be done over the cordset's (SAE J1772) AC "Mains" or "Pilot" signal wires. For more information, see the SAE J2931, IEC61851-1 and related PEV standards.

The basic idea behind the GreenPPEA protocol is illustrated in Figure 13-X. The signals sent by PEV (i.e., Green PHY 1 (GP1)) will reach the EVSE-1 (i.e., GP2) with minimal attenuation. To reach any other EVSE, the PEV signal needs to go through two open contacts and/or PLC pass band (RF) coupling, which significantly reduces the signal strength measured at other EVSE's. Note that wires within the same cable, and even wires in different cables that are sufficiently close and parallel to each other, can experience non-negligible crosstalk, but with significant signal attenuation. PEV-EVSE association exploits this inherent asymmetry in signal strength at different EVSE's to associate (match) the PEV to the EVSE to which it is physically connected through the charging cordset.

Informative Text
Matching means that the PEV has been able to select and associate with the EVSE, which then together establish a private network by exchanging an NID and NMK. Matched devices no longer participate in GreenPPEA, which simplifies the process for other unmatched (available) PEVs and EVSEs.

Figure 13-3: PEV – EVSE Association

During the GreenPPEA protocol, the PEV and the EVSE (or more properly, a charging cable controlled by an EVSE, in case an EVSE has more than one such cable) proceeds through several states. For simplicity, these will be called PEV states and EVSE states.

- The start state for the EVSE is **Unoccupied**, meaning that no PEV is currently plugged in to the EVSE its cable.
- When a PEV plugs in to the EVSE, the EVSE can detect this and transitions to the **Unmatched** state, meaning that a PEV is plugged into it, but the PEV has not yet been

Informative Text

- After PEV and EVSE are matched and have formed an AVLN, the GreenPPEA protocol has completed successfully. Their higher layers then work together, possibly with other devices,

identified reliably.

- When the GreenPPEA protocol completes successfully, the PEV and EVSE is identified reliably, and the EVSE state becomes **Matched**.

When the PEV unplugs from the EVSE, this is detected by the EVSE and its state returns to Unoccupied.

A PEV proceeds through several states, starting with Disconnected. When it is plugged into an EVSE, it also can detect this and it transitions to the Unmatched state, in which it carries out the GreenPPEA protocol. Upon successful completion of the protocol, the PEV enters the Matched state and remains there until it is unplugged.

Only an EVSE in the Unmatched state needs to participate in the GreenPPEA protocol, as an Unoccupied EVSE cannot be the EVSE with which a PEV should be matched, and a Matched EVSE has already identified the PEV plugged into it.

PEV – EVSE Association Procedure

As the SLAC procedure starts, the PEV and EVSE decide whether or not to use Secure SLAC. If Secure SLAC is selected, then all subsequent messages that are optionally signed must be signed for the recipient to accept them, and all messages that are optionally encrypted must be encrypted. The sequence of steps in PEV – EVSE Association procedure is an example of how a procedure could look like. Trigger conditions and decisions may vary from the HLE application, such as the ISO/IEC 15118 series.

Configuration of GP stations in PEV and EVSE: Initialize PEV to never be CCo; Initialize EVSE to always be CCo.

- SLAC: PEV obtains SLAC parameters from the EVSE. PEV sends Multi-Network Broadcast (MNBC) messages (referred to as M-Sounds, i.e., multi-network sounds) in SLAC process; PEV then optionally provides public key security credentials, followed by M-Sounds signed using public key cryptography.
- Match Decision: Each unmatched EVSE processes the M-Sounds, verifying the public key signature if present. Each such EVSE sends the Sounding results to the PEV so that it can make the matching decision, optionally signed and including EVSE certificate.
- Validation: PEV optionally uses Control Pilot validation of the selected EVSE.
- Inform EVSE of Decision: PEV decides which EVSE is attached to it based on the ATTN_PROFILE results from the M-Sounds responses (refer to ISO/IEC 15118-3) and validation results (if used), and sends to that EVSE a matching message, optionally signed.
- Confirm Decision: Selected EVSE sends PEV a confirmation message with NID, NMK, EVSE's MAC address; message is optionally encrypted with the PEV's public key and signed by the EVSE.
- Network Join: PEV joins matching EVSE's AVLN, using NID and NMK supplied by selected EVSE. (Refer to HPGP specification section 7.3.4.1)
- Amplitude Map exchange: Optionally, EVSE and PEV agree on amplitude map.

Informative Text

After PEV and EVSE are matched and have formed an AVLN, the GreenPPEA protocol has completed successfully. Their higher layers then work together, possibly with other devices, to obtain account authorization and supply power, and to confirm power is being received by PEV. Refer to ISO/IEC 15118-3

Configuration of GP stations in PEV and EVSE

GP station in the PEV shall be configured never to become a CCo using the **APCM_SET_CCo.REQ** (Section 12.2.2.57). GP station that is configured to never be a CCo shall not respond to **CM_SC_JOIN.REQ** message from other STAs. PEV shall be configured to only support SLAC functions associated with the transmitter of M-Sounds using **APCM_CONF_SLAC.REQ** (Section 12.2.2.59).

GP station in the EVSE shall be configured to always be a CCo always when the GP station is coupled to the Control Pilot. EVSEs in Unoccupied state shall be configured to not support SLAC functions using **APCM_CONF_SLAC.REQ**.

SLAC

SLAC process enables EVSEs to measure and report the attenuation profile of M-Sound PPDUs transmitted by PEV. The behavior of PEV and EVSE is described in the following sections.

Informative Text

The messages sent during the SLAC process are all sent using multi-network broadcast (MNBC), even if the destination MAC address is unicast. This is necessary because not all EVSEs may belong to the same AVLN, and the PEV needs to reach all EVSEs with which it may be matched. Moreover, the PEV does not even join an AVLN until it is matched, since it has to send messages using MNBC regardless. All EVSEs (and other PEVs) that receive the SLAC messages will filter them according to the MAC address, the message, and their own state. For example, devices that are not EVSEs will ignore the M-Sounds sent by PEVs in this protocol. EVSEs that are unoccupied or are already matched will also discard these messages. Refer to section 5.4.3.

PEV SLAC

The SLAC procedure at the PEV is as follows. Trigger conditions and decisions may vary from the HLE application, such as the ISO/IEC 15118 series.

- PEV-HLE initiates the SLAC protocol by sending **CM_SLAC_PARM.REQ** message. This message requests the EVSE(s) to provide SLAC parameters to be used by the PEV. PEV-HLE will start a timer to track the reception of the corresponding **CM_SLAC_PARM.CNF**. If the **CM_SLAC_PARM.CNF** is not received before the timer expires, the PEV-HLE may reinitiate the SLAC protocol. The fields in the **CM_SLAC_PARM.REQ** shall be set as follows,
- APPLICATION_TYPE shall be set to 0x00 (i.e., Green PHY PEV-EVSE Association).
- By default, HLE shall set the SECURITY_TYPE to 0x00. If the PEV supports Security, SECURITY_TYPE shall be set to 0x01 (i.e., Public Key Signature) and the message shall

include Cipher Suites that are supported by the PEV.

- PEV Green PHY station shall transmit **CM_SLAC_PARM.REQ** message as a multi-network broadcast.
- When the PEV Green PHY station receives a **CM_SLAC_PARM.CNF** message(s), it shall pass it to the PEV-HLE.
- PEV-HLE may receive **CM_SLAC_PARM.CNF** from multiple EVSEs. PEV-HLE may use one or more of the received **CM_SLAC_PARM.CNF** messages for determining the SLAC parameters.
- When the **CM_SLAC_PARM.CNF** indicates that Secure SLAC is required, PEV-HLE shall send a **CM_PKCS_CERT.IND** message. The Target MAC address for this message shall be set to MAC address of the PEV Green PHY station. To ensure reliable reception of this message at all EVSEs, it is recommended that this message be transmitted at least three times by the PEV-HLE. If the **CM_PKCS_CERT.IND** message is larger than 502 Octets, the message shall be fragmented by the HLE (refer to Section 11.1.7).
- PEV Green PHY station shall transmit **CM_PKCS_CERT.IND** message from the HLE using Multi-Network Broadcast.
- To enable reliable reception of **CM_START_ATTEN_CHAR.IND** at all EVSEs, the PEV-HLE shall send at least three **CM_START_ATTEN_CHAR.IND** messages, with the fields reflecting the values of the **CM_SLAC_PARM.CNF** message it received. If Secure SLAC has been selected, then these messages shall be signed. PEV Green PHY station shall transmit **CM_START_ATTEN_CHAR.IND** messages from the HLE using Multi-Network Broadcast.
- The PEV-HLE shall send **CM_MNBC_SOUND.IND** messages. The number of **CM_MNBC_SOUND.IND** messages shall be based on the corresponding NUM_SOUNDS parameter in **CM_SLAC_PARM.CNF**. Each **CM_MNBC_SOUND.IND** message is sent with additional information, including a countdown counter (indicating the number of Sounds remaining to be sent). If Secure SLAC has been selected, then the M-Sound shall be signed by the PEV. If the **CM_MNBC_SOUND.IND** message is larger than 502 Octets, the message shall be fragmented by the HLE (refer Section 11.1.7). PEV Green PHY station shall transmit **CM_MNBC_SOUND.IND** messages using Multi-Network Broadcast.

EVSE SLAC

The SLAC procedure at the EVSE is as follows. Trigger conditions and decisions may vary from the HLE application, such as the ISO/IEC 15118 series.

- When an Unoccupied EVSE-HLE enters the Unmatched state ,it configures the EVSE GP to support only SLAC functions associated with the receiver of M-Sounds using **APCM_CONF_SLAC.REQ**.
- EVSE Green PHY station shall pass any received **CM_SLAC_PARM.REQ** messages to the EVSE-HLE
- Reception of a **CM_SLAC_PARM.REQ** message at an Unmatched EVSE-HLE shall cause the HLE to transmit a **CM_SLAC_PARM.CNF** message to the PEV. The fields in the **CM_SLAC_PARM.CNF** shall be set as follows,
- APPLICATION_TYPE shall be set to 0x00 (i.e., Green PHY PEV-EVSE Association).
- By default, HLE shall set the SECURITY_TYPE to 0x00. If both EVSE and PEV support

Security, SECURITY_TYPE shall be set to 0x01 (i.e., Public Key Signature).

- The RESP_TYPE shall be set to 0x01 and the FORWARDING_STA shall be set to the MAC address of the PEV.
- All other fields shall be set based on the local configuration of EVSE-HLE.
- The Green PHY station in the EVSE shall transmit **CM_SLAC_PARM.CNF** message sent by the HLE to PEV using multi-network broadcast.
- If the EVSE-HLE supports Secure SLAC, then reception of the PEV Public Key shall cause an Unmatched EVSE-HLE to store the associated Public Key for verifying the M-Sound signatures.
- The Green PHY station in the EVSE shall pass any **CM_START_ATTEN_CHAR.IND** messages to the EVSE-HLE.
- Reception of **CM_START_ATTEN_CHAR.IND** message at the EVSE-HLE shall cause EVSE-HLE to start a timer based on the Time_Out field in the message. Expiration of this timer is used as a trigger for generating **CM_ATTN_CHAR.IND**. However, if Secure SLAC has been selected, then the **CM_START_ATTEN_CHAR.IND** message must be signed and the signature verified, or else it is ignored.
- The Green PHY station in the EVSE shall pass any M-Sound messages to the EVSE-HLE along with the Attenuation Profile associated with that message. Signal processing is performed by the PHY, and if the MAC is configured to receive M-Sounds, it passes both the M-Sound message and the Attenuation Profile to the HLE.
- Reception of an M-Sound at the EVSE-HLE shall cause it to process the Attenuation Profile information. The RunID shall match the RunID sent by that PEV in the **CM_START_ATTEN_CHAR.IND** message or else the M-Sound is discarded. If the process is Secure SLAC, EVSE-HLE shall only process M-Sounds with valid public key signatures. The EVSE-HLE shall also track the value Countdown Counter of any PEV whose M-Sounds it receives. For a run (i.e., based on RunID) of the SLAC protocol, this value must be monotonically decreasing, so any M-Sound from a PEV whose Countdown Counter's Cnt value is not less than the smallest value of Cnt received from the PEV shall be discarded.
- If the last M-Sound is received (Cnt=0) or if the timer has expired, the EVSE-HLE shall trigger the generation of **CM_ATTN_CHAR.IND**. This message shall be sent to the PEV, signed if the process is secure. If signed, the EVSE shall first send its public key certificate including its EVSE_ID and attributes that identify it as an EVSE, signed by a certificate authority allowed to identify EVSEs.
- If Secure SLAC is used, EVSE-HLE shall send **CM_PKCS_CERT.IND** message with its Public Certificate. The Target MAC address for this message shall be set to MAC address of the EVSE Green PHY station. To ensure reliable reception of this message by the PEV, it is recommended that this message be retransmitted until a corresponding **CM_PKCS_CERT.RSP** message is received by the PEV-HLE. If the **CM_PKCS_CERT.IND** message is larger than 502 Octets, the message shall be fragmented (refer Section 11.1.7).
- EVSE Green PHY station shall transmit **CM_PKCS_CERT.IND** message from the HLE using Multi-Network Broadcast.

- EVSE-HLE shall send the **CM_ATTN_CHAR.IND** message. If secure SLAC is used, this message shall be signed by the EVSE-HLE using its public key certificate. To ensure reliable reception of this message by the PEV, it is recommended that this message be retransmitted until a corresponding **CM_ATTN_CHAR.RSP** message is received by the PEV-HLE.
- EVSE Green PHY station shall transmit **CM_ ATTN_CHAR.IND** message from the HLE using Multi-Network Broadcast.

Matching Decision at PEV

Matching decision enables the PEV and EVSE to determine which EVSE and PEV they are connected through the charging cordset. The matching decision is the most important part of the Green PHY PEV-EVSE association procedure. The matching decision is made by the PEV based on the **CM_ATTN_CHAR.IND** message that is generated by the EVSE-HLE's as a result of SLAC (refer Section 13.8.1.4.1). These messages shall be signed if the process is secure.

The Matching decision is made by the PEV, with optional validation by the selected EVSE. The process at the PEV is as follows:

- When the timeout as advertised in the **CM_START_ATTEN_CHAR.IND** message expires, the PEV-HLE shall start a timer for receiving results from the EVSEs.
- When the PEV Green PHY station receives a **CM_PKCS_CERT.IND** message, it shall pass it to the PEV-HLE.
- When the PEV HLE receives a **CM_PKCS_CERT.IND** message, if Secure SLAC has been selected it shall validate the certificate as described in Section 9 of ZigBee-11185. If valid, and if the attributes and root certificate authority identify the sender as an EVSE, it shall cache the certificate for use in verifying messages signed by that EVSE.
- When the PEV Green PHY station receives a **CM_ATTEN_CHAR.IND** message, it shall pass it to the PEV-HLE.
- When the PEV-HLE receives a **CM_ATTEN_CHAR.IND** message it shall verify that the RunID matches that of the **CM_START_ATTEN_CHAR.IND** message and store it until it has decided which EVSE is the most likely match for it. If the process is secure, it shall verify the signature on the message and discard it if it is not verified to be from an authorized EVSE.
- When the timer for receiving results from EVSEs expires, the PEV shall consider the ATTN_PROFILE measured at the valid reporting EVSE's and select an EVSE according to ISO/IEC 15118-3.

Validation

When the PEV's HLE determines that association Validation is required, the PEV causes a signal to be sent out-of-band and challenge the EVSE to respond appropriately. Details of the Validation procedure are described in ISO/IEC 15118-3. To facilitate the Validation protocol, Green PHY specification includes two management messages,

- CM_VALIDATE.REQ (refer Section 11.5.55)
- CM_VALIDATE.CNF (refer Section 11.5.56)

Green PHY stations only provide transport service to these CM_VALIDATE.REQ/CNF

messages. Green PHY stations do not interpret or modify the contents of these messages.
The required behavior of PEV Green PHY station is as follows,

- PEV Green PHY station shall transmit **CM_VALIDATE.REQ** message from the HLE using Multi-Network Broadcast
- When the PEV Green PHY station receives a **CM_VALIDATE.CNF** message, it shall pass it to the PEV-HLE

The required behavior of EVSE Green PHY station is as follows,

- When the PEV Green PHY station receives a **CM_VALIDATE.REQ** message, it shall pass it to the PEV-HLE
- EVSE Green PHY station shall transmit **CM_VALIDATE.CNF** message from the HLE using Multi-Network Broadcast

Inform EVSE of Decision

The PEV-HLE shall send the selected EVSE (if any) its decision in a **CM_SLAC_MATCH.REQ** message and request the NID and NMK from the selected EVSE in the **CM_SLAC_MATCH.CNF** reply. If the process is secure, this message is signed by the PEV-HLE. The message shall be resent at least once if a corresponding confirmation message is not received from the selected EVSE. The PEV Green PHY station shall transmit **CM_SLAC_MATCH.REQ** message from the HLE using Multi-Network broadcast.
The selected EVSE's HLE shall verify the RunID as well as the signature on the message if the process is secure, and may request validation before it confirms the matching decision.

Informative Text

The messages sent up until the PEV and EVSE form an AVLN are all sent using multi-network broadcast (MNBC), even if the destination MAC address is unicast. This is necessary because the PEV and the EVSE have not yet joined the same AVLN. Stations that receive the MNBC messages will filter them using the MAC address.

Matching Confirm by EVSE

Once the EVSE-HLE has received the match request from a PEV and optionally has validated that the PEV is connected to it using the charging cordset based procedure described in previous sections, it confirms the decision to the PEV. It also transitions to the Matched state.
The behavior of the EVSE is as follows.

- EVSE-HLE shall send a **CM_SLAC_MATCH.CNF** message that includes an NID and NMK. If Secure SLAC is used, the NID and NMK are newly generated by the EVSE-HLE and this message shall be signed by the EVSE-HLE using its public certificate and encrypted using the PEV's public key.
- EVSE Green PHY station shall transmit **CM_SLAC_MATCH.CNF** message from the HLE using Multi-Network Broadcast.
- EVSE-HLE shall configure the EVSE Green PHY station with the same NMK and default NID that it sent to PEV using the **APCM_SEK_KEY.REQ** primitive. This causes the EVSE to become an unassociated STA waiting for another STA that has the same NMK/NID to join

Informative Text

The purpose of this feature is to allow the PEV to have shared control of the amplitude map, rather than it being controlled solely by the CCo (EVSE). It recognizes an uncertainty that the remote may be sensitive to specific PLC carriers or may generate noise that could interfere with the PLC network. The extensive use of reduced carrier amplitude could reduce the bandwidth supported by the network. In addition, the amplitude map is used to cause the stations to

- Reception of **CM_PKCS_CERT.IND** causes the PEV-HLE to validate and to store the Certificate.
- The Green PHY station at the PEV passes any received **CM_SLAC_MATCH.CNF** to its HLE.
- Reception of **CM_SLAC_MATCH.CNF** causes the PEV-HLE to verify the RunID and the Public Key Signature (if any) of the message. Further, the PEV shall verify that the public key used for signing the **CM_SLAC_MATCH.CNF** is the same as the public key used for signing the **CM_ATTN_CHAR.IND** message from that particular EVSE. If the Public Key Signature is verified or the process is not secure, the PEV-HLE accepts the NID and NMK included in the message, causing it to leave its current network and to join the specified network, entering the Matched PEV state.

Network Join

When the PEV-HLE accepts an NID and NMK from a **CM_SLAC_MATCH.CNF**, it shall configure the PEV Green PHY station with the same NMK and default NID that it received from EVSE in **CM_SLAC_MATCH.CNF** using the **APCM_SEK_KEY.REQ** primitive. This causes the PEV to become an unassociated STA waiting for another STA that has the same NMK/NID to join it to form an AVLN. Likewise, the EVSE-HLE shall configure the EVSE Green PHY station with the same NMK and default NID that it sent to PEV using the **APCM_SEK_KEY.REQ** primitive. This causes the EVSE to become an unassociated STA waiting for another STA that has the same NMK/NID to join it to form an AVLN. The PEV and EVSE form an AVLN using the matching NID/NMK (refer to Section 7.3.4.1)

Amplitude Map exchange

EVSE may optionally provide PEV with its Amplitude Map using **CM_AMP_MAP.REQ** message. PEV may also optionally provide EVSE with its Amplitude Map using **CM_AMP_MAP.REQ**. The transmit power on various carriers used by both Green PHY stations shall be based the minimum of the EVSE's amplitude map and the amplitude map it received from the associated PEV. HLE may configure the Green PHY station with a specific Amplitude Map using **CM_AMP_MAP.REQ** message. The amplitude map of a PEV and EVSE shall be reset to their default amplitude map after the PEV is disconnected from the EVSE.

Informative Text

The purpose of this feature is to allow the PEV to have shared control of the amplitude map, rather than it being controlled solely by the CCo (EVSE). It recognizes an uncertainty that the PEV may be sensitive to specific PLC carriers or may generate noise that could interfere with the PLC network. The extensive use of reduced carrier amplitude could reduce the bandwidth supported by the network. In addition, the amplitude map is used to cause the stations to conform to the regulatory environment in which they operate.

Secure SLAC Overview

Secure SLAC is an optional feature described in Section 13.8.1 that provides enhanced support from security attacks. This section addresses the following limitations of basic SLAC and conversely, the value of using secured SLAC,

- There is no mechanism to validate that M-Sounds are transmitted by the PEV. Malicious PEV's may generate M-Sounds with strong signal that appear to be sent from a legitimate PEV. This can cause an EVSE to record false signal level attenuation values from the legitimate PEV, and cause the legitimate PEV to make the wrong decision and the EVSE possibly to provide the malicious PEV with power.
- There is no mechanism for EVSE to securely communicate its SLAC values to the PEV. Thus a rogue PEV can send the legitimate PEV misleading values that will cause it to make the wrong decision and the EVSE possibly to provide the malicious PEV with power.
- There is no mechanism for the PEV to securely communicate its decision to the selected EVSE. A rogue PEV can send a spoofed message to the EVSE to which it is connected and cause it to provide it with power under the belief that it is providing the legitimate PEV with power.

Secure SLAC uses public key signatures on the M-Sounds to prevent an EVSE from accepting spoofed M-Sounds. Verifying the RunID in each M-Sound, which must match the RunID given in the **CM_START_ATTEN_CHAR.IND** message, prevents a rogue PEV from replaying M-Sounds from the legitimate PEV. Thus the EVSE's will obtain reliable attenuation readings from a legitimate PEV. Neither can a rogue PEV spoof or replay the message from an EVSE containing SLAC data, since these messages are signed by the EVSE and must have a matching RunID, so the legitimate PEV has uncorrupted data on which to base its decision. Through public key signatures and the RunID verification, Secure SLAC also prevents a rogue PEV from spoofing or replaying the message to its EVSE telling it that it has been selected for a legitimate PEV.

Public Key Certificates

Public Key Certificates shall have the format as specified in ZigBee-11185. Public key certificates shall be passed as signed CMS messages (refer to RFC 5652) with null content. All received public key certificates shall be validated as described in Section 9 of ZigBee-11185r05.

The Public Key Certificate for an EVSE shall have an attribute that identifies that certificate holder as an EVSE. Similarly, the Public Key Certificate for a PEV shall have an attribute that identifies that certificate holder as a PEV.

CMS shall also be used to sign and to encrypt messages as needed using the enveloped

data, and the signed data content types.

All CMS messages shall be sent using Distinguished Encoding Rules (DERs) wherever applicable.

All PEVs and EVSEs that support secure SLAC shall support at least DSA with SHA-256, RSA, and AES-128 in CBC mode. ECDSA, ECDH, and AES-256 are recommended. Refer to RFC 3565, RFC 5280, RFC 5480 and RFC 5758.

Exchange of User Data

CM_SLAC_USER_DATA.REQ and **CM_SLAC_USER_DATA.CNF** messages may be used by PEVs and EVSEs to exchange user data as part of SLAC. For example, these messages to be used to shut the charger down or recognize the car has left (e.g. immediate disassociate). The format of these messages is described in Section 11.5.59 and Section 11.5.60.

EVSE Power Save Restrictions

An EVSE with an associated PEV (refer to Section 13.8.1) shall not enter Power Save mode if the PEV is not in Power Save mode.

ISP

ISP Overview

HomePlug GREEN PHY shall follow the requirements stated in the IEEE 1901 specification.
Refer to Chapter 17 “Inter System Protocol” in the IEEE 1901 specification.

ISP BENTRY

HomePlug GREEN PHY shall follow the requirements stated in the IEEE 1901 specification.
Refer to section 7.4.1.4.17.23 “ISP BENTRY” in the IEEE 1901 Specification.

ISP BENTRY: Beacon Entries in Various Beacons

HomePlug GREEN PHY shall follow the requirements stated in the IEEE 1901 specification.
Refer to Table 7-78 “Beacon Entries in Various Beacons” in the IEEE 1901 Specification.

ISP BENTRY: BEHDR Value

HomePlug GREEN PHY shall follow the requirements stated in the IEEE 1901 specification.
Refer to Table 7-77 “Beacon Header Interpretation” in the IEEE 1901 Specification.

ISP BENTRY: ISP MME Types

HomePlug GREEN PHY shall follow the requirements stated in the IEEE 1901 specification.
Refer to Table 7-61 “Management Message Type” in the IEEE 1901 Specification.
Refer also to the following sections in the IEEE 1901 Specification:
Section 7.5.1.2.59 “CC_ISP_DetectionReport.indication”
Section 7.5.1.2.60 “CC_ISP_StartReSync.request”
Section 7.5.1.2.61 “CC_ISP_FinishReSync.request”
Section 7.5.1.2.62 “CC_ISP_ReSyncDetected.indication”
Section 7.5.1.2.63 “CC_ISP_ReSyncTransmission.request”

Coexistence for ISP

HomePlug GREEN PHY shall follow the requirements stated in the IEEE 1901 specification.
Refer to Chapter 16 “Coexistence” in the IEEE 1901 Specification.

Index

1.1 Proxy Coordinator (PCo) Messages
CP_PROXY_APPOINT.CNF, 565
CP_PROXY_APPOINT.REQ, 563
Abbreviations, 2, 12
AC Line Cycle synchronization in Coordinated mode, 438
Access coexistence
bandwidth allocation, 482
bandwidth release, 488
CCo requirements, 480
Flexible frequency division, 490
flexible time division access, 479
sharing resources, 481
STA requirements, 480
using Neighbor Network coordination, 486
using resource from the In-Home Network, 484
Access network resources, 483
Acronyms, 2
Acting as an AV bridge, 249
AES encryption algorithm and mode, 405
AES encryption key automatically, 407
AES encryption key generation, 406
from passwords, 406
Amplitude Map, 88
Association, 331
Association procedure, 481
Authentication
method, 335
Authentication procedure, 482
Authorization methods, 392
Authorization procedure, 482
Auto Connect-initiated reconfiguration, 229
Auto-Connect Service, 314
evaluating data flow, 315
monitoring automatic connections, 317
processing, 316
Automatic retransmission, 283
Auto-selection of CCo, 356

AV Frame Control Interleaver, 42
AVLN
shutting down, 437
AVLN
forming a new, 336
getting more information about, 330
joining an existing, 346
joining or forming, 329
leaving, 352
names, 330
network identifier, 329
overview, 329
removing a station from, 353
selecting a new, 353
Backup CCo and CCo failure recovery, 388
Bandwidth allocation, 384
Bandwidth allocation for access coexistence, 482
Neighbor Network coordination, 486
using resources from the In-Home Networking, 484
Bandwidth Manager, 373
Bandwidth release for access coexistence, 488
Bandwidth release procedure, 437
Bandwidth sharing in coordinated mode, 434
Beacon MAC Protocol Date Unit payload format, 156
Beacon Period configuration, 387
Beacon Period structure, 198, 417
Beacon Period structure, 195
Beacon Period structure
CSMA-Only mode, 202
Beacon Period structure
uncoordinated mode, 204
Beacon Period structure
Coordinated mode, 205
Behavior as a CCo in an AVLN, 327
Behavior as a STA in an AVLN, 326
Bidirectional bursting, 278
Binary numbers, 11
Bit and octet order, 101
Bit and octet transmission order
at the MAC PHY interface, 102
Bridging, 248
acting as an AV bridge, 249

communicating through an AV bridge, 250
Bridging with Quality of Service, 253
Buffer management, 260
Bursting
bidirectional, 278
Capability of CCo, 357
Carrier Bit Loading Data Encoding (CBD_ENC, 598
CC_BEACON_RELIABILITY.CNF, 549
CC0
selecting, 353
selecting for a new AVLN, 353
CCo
Bandwidth Manager, 373
Beacon Period configuration, 387
connection admission control, 386
outage/failure recovery, 389
proxy networking, 364
scheduler and bandwidth allocation, 384
transfer/handover of functions, 358
CCo, 357
auto-selection, 356
order for selection, 357
user-appointed, 354
Channel access, 208
CSMA/CA, 208
TDMA, 210
Channel access mechanism, 195
Channel access priority, 210
Channel estimation, 235, 245
initial, 236
procedure, 235
Channel Interleaver, 49, 52
Channel negotiation, 491
Classifier, 307
configuration, 308
Ethernet SAP Classifier rules, 308
initiated connection setup, 308, 312
CM behavior under inactivity interval, 222
CM_ENCRYPTED_PAYLOAD.IND message encryption, 406
CM_GET_KEY.CNF provisioning NMK using UKE, 698
CM_GET_KEY.REQ provisioning NMK using UKE, 696
CM_SET_KEY.CNF in CM_ENCRYPTED_PAYLOAD.IND, 703

CM_SET_KEY.REQ in CM_ENCRYPTED_PAYLOAD.IND, 700
Coexistence with HomePlug 1.1 and Non-HomePlug powerline networks, 464
Communicating through an AV bridge, 250
broadcast address, 252
Known AV Station, 251
Known Bridged destination, 252
Known DA, 251
Known multicast address, 252
Unknown DA, 252
Unknown multicast address, 252
Unknown unicast destination, 252
Communication between
associated but unauthenticated STAs, 268
STAs not associated with the same AVLN, 269
Communication inside an AVLN, 28
Communication with
broadcast addresses, 252
Known AV Stations, 251
Known Bridged Stations, 252
Known DAs, 251
Known multicast addresses, 252
Unknown DAs, 252
Unknown multicast addresses, 252
Unknown unicast destinations, 252
Computing the lNL allocation, 421
Connection admission control, 386
Connection identifiers, 215, 216, 217
Connection monitoring, 222
Connection reconfiguration, 227
Connection services
connection monitoring, 222
connection reconfiguration, 227
connection setup, 109, 204, 205, 207, 218, 221, 226, 229, 283, 285, 317, 384, 416, 417
connection teardown, 222
Global Link reconfiguration triggered by CCo, 229
Global Link Setup, 221
Connection services for broadcast/multicast, 232
Connection setup, 109, 204, 205, 207, 218, 221, 226, 229, 283, 285, 317, 384, 416, 417
Connection Specification, 21, 373, 384
Connection teardown, 222
Connectionless links, 213
Connectionless Service, 217, 679

Connection-oriented service, 678
Connection-Oriented service, 218
Connections, 211
Connections and network modes, 226
Control SAP Service, 658
Conventions, 11
Convergence layer
functions, 307
Convergence layer information, 653
Coordinated mode, 417, 419
CRC-24, 106
CRC-32, 105
CSMA/CA channel access, 208
CSMA/CA coexistence, 464
CSMA-Only mode, 416
CSPEC reconfigurability, 384
Cyclic Redundancy Check calculation, 105
DAK-encrypted NMK, 348
Data encryption, 275
De-muxing, 314
De-squeeze, 230, 231
Device Access Key, 390
Device Password, 391
Disambiguated TEIs, 333
Discover Process, 361
Diversity Copier, 42
Duplicate Detection, 260
Dynamic channel adaptation, 239
Empty tone filling, 59
Encryption
data, 275
HomePlug AV method, 275
Encryption
CM_ENCRYPTED_PAYLOAD.IND Message, 406
Encryption AES, 405
Encryption key, 390
generation, 406
network, 391
temporary, 392
uses and protocol failures, 403
Encryption Key Change BENTRY, 182
Encryption Key Select, 120, 121

Encryption payload-level, 405
Encryption PHY block-level, 405
End-to-end smoothing, 318
Error Correction
Frame Control Forward, 41
Payload Forward, 43
Ethernet II-class (ETH) SAP, 654
Ethernet SAP Classifier Rule set format, 313
FDMA coexistence management messages, 491
File integrity verification, 2
Flexible Frequency Division Access coexistence, 490
Flexible TDM coexistence with non-HomePlug networks, 492
Flow control, 260
Format of Beacon MAC Protocol Date Unit payload, 156
Format of Long MAC Protocol Date Unit payload, 151
Forming a new AVLN, 336
Forming an AVLN, 329
Fragment management information, 496
Frame Control Forward Error Correction, 41
Framing process, 254
Functional blocks, 25
Generation of AES encryption key, 406
Get full AVLN information, 330
Get full STA information, 331
Global Link reconfiguration
triggered by CCo, 229
Global Link Setup, 221
Global Links, 213
Guard Interval Length, 597
H1 interface, 653
H1 SAPs, 654
Hashed NMK, hashed NID, and NMK provisioning MME using DAK, 691
Hexadecimal numbers, 11
Hidden stations
associating, 366
identifying, 366
HLE-initiated reconfiguration, 229
HomePlug 1.0.1, 444
Carrier Sensing mechanism, 444
compatible frame lengths, 452
contention-free transmissions, 446
link status, 446

prioritizes CSMA/CA, 444
segment bursting, 446
HomePlug 1.0.1/1.1
coexistence mode changes, 450
HomePlug AV coexistence modes
coexistence with HomePlug 1.0.1, 447
HomePlug AV OFDM transceiver, 36
HomePlug AV operation under various regulatory jurisdictions, 32
Hostile connection teardown, 226
Human-friendly station and AVLN names, 330
Incoming traffic
from
the powerline network, 249, 250
from the
bridged network, 250
Informative text, 11
Initial channel estimation, 236
Initialization Vector, 583
Instantiating
a proxy network, 369
Interfering Network List, 420
computing, 421
Interframe spacing, measurement of, 294
Joining an AVLN, 329
Joining an existing AVLN, 346
Key Type, 586, 589, 590, 591
Last symbol padding, 59
Latency effect on teardown messages, 225
Latency effects on Global Link Setup, 221
Leaving an AVLN, 352
Line cycle synchronization, 195, 197
Link identifiers, 214
Links, 211
connectionless, 213
global, 213
local, 213
Local links, 213
Logical networks, 27
Long MAC Protocol Date Unit format, 151
M1 interface, 653
M1 SAPs, 678
MAC

Beacon Period structure, 198
bridging, 248
bridging with Quality of Service, 253
channel access, 208
connection identifiers, 215, 216, 217
connection services
connection monitoring, 222
connection reconfiguration, 227
connection setup, 109, 204, 205, 207, 218, 221, 226, 229, 283, 285, 317, 384, 416, 417
connection teardown, 222
Global Link reconfiguration triggered by CCo, 229
Global Link Setup, 221
Connections, 211
data encryption, 275
encryption
method, 275
framing process, 254
link identifiers, 214
links, 211
connectionless, 213
global, 213
local, 213
MPDU bursting, 276
reassembly, 259
retransmission
automatic, 283
strategies, 285
retransmission, 285
segmentation, 257
transport services, 217
connectionless, 217
connection-oriented, 218
MAC data service, 679
MAC Frame format, 106
MAC Frame header, 107
MAC Frame length, 109
MAC Frame streams, 255
MAC Frame type, 107
MAC Protocol Data Unit
format, 111
format in AV Only mode, 112
format in Hybrid mode, 112

Frame Control fields, 113
Management message format, 493
Management messages
CM_MME_ERROR.IND, 615
CM_NW_STATS.CNF, 616, 621, 622
CM_NW_STATS.REQ, 616, 621
Management messages
CC_ACCESS_NEW.CNF, 552
CC_ACCESS_NEW.IND, 554
CC_ACCESS_NEW.REQ, 552
CC_ACCESS_NEW.RSP, 555
CC_ACCESS_REL.CNF, 556
CC_ACCESS_REL.IND, 556
CC_ACCESS_REL.REQ, 555
CC_ACCESS_REL.RSP, 557
CC_ALLOC_MOVE.CNF, 551
CC_ALLOC_MOVE.REQ, 550
CC_ASSOC.CNF, 542
CC_ASSOC.REQ, 540
CC_BACKUP_APPOINT.CNF, 522
CC_BACKUP_APPOINT.REQ, 521
CC_BEACON_RELIABILITY.REQ, 549
CC_BLE_UPDATE.IND, 559
CC_CCO_APPOINT.CNF, 520
CC_CCO_APPOINT.REQ, 520
CC_DCPPC.IND, 557
CC_DCPPC.RSP, 558
CC_DETECT_REPORT.CNF, 538
CC_DETECT_REPORT.REQ, 537
CC_DISCOVER_LIST.CNF, 526
CC_DISCOVER_LIST.IND, 529
CC_DISCOVER_LIST.REQ, 526
CC_HANDOVER.CNF, 524
CC_HANDOVER.REQ, 523
CC_HANDOVER_INFO.IND, 524
CC_HANDOVER_INFO.RSP, 525
CC_HP1_DET.CNF, 558
CC_HP1_DET.REQ, 558
CC_LEAVE.CNF, 544
CC_LEAVE.IND, 544
CC_LEAVE.REQ, 544
CC_LEAVE.RSP, 545

CC_LINK_INFO.CNF, 522
CC_LINK_INFO.IND, 523
CC_LINK_INFO.REQ, 522
CC_LINK_INFO.RSP, 523
CC_LINK_MOD.CNF, 534
CC_LINK_MOD.REQ, 533
CC_LINK_NEW.CNF, 532, 533
CC_LINK_NEW.REQ, 529
CC_LINK_REL.IND, 536
CC_LINK_REL.REQ, 535
CC_LINK_SQZ.CNF, 535
CC_LINK_SQZ.REQ, 535
CC_RELAY.IND, 548
CC_RELAY.REQ, 547
CC_SET_TEI_MAP.IND, 545
CC_SET_TEI_MAP.REQ, 545
CC_WHO_RU.CNF, 540
CC_WHO_RU.REQ, 539
CM_AMP_MAP.CNF, 603
CM_AMP_MAP.REQ, 603
CM_BRG_INFO.CNF, 604
CM_BRG_INFO.REQ, 604
CM_CHAN_EST.IND, 592
CM_CONN_INFO.CNF, 609
CM_CONN_INFO.REQ, 609
CM_CONN_MOD.CNF, 608
CM_CONN_MOD.REQ, 608
CM_CONN_NEW.CNF, 606
CM_CONN_NEW.REQ, 605
CM_CONN_REL.IND, 607
CM_CONN_REL.RSP, 607
CM_ENCRYPTED_PAYLOAD.IND, 580
CM_ENCRYPTED_PAYLOAD.RSP, 585
CM_GET_BEACON.CNF, 614
CM_GET_BEACON.REQ, 613
CM_GET_KEY.CNF, 590
CM_GET_KEY.REQ, 588
CM_HFID.CNF, 615
CM_HFID.REQ, 614
CM_LINK_STATS.CNF, 559, 560, 561, 562
CM_NW_INFO.CNF, 612
CM_NW_INFO.REQ, 612

CM_SC_JOIN.CNF, 592
CM_SC_JOIN.REQ, 591
CM_SET_KEY.CNF, 588
CM_SET_KEY.REQ, 586
CM_STA_CAP.CNF, 610
CM_STA_CAP.REQ, 610
CM_TM_UPDATE.IND, 600
CM_UNASSOCIATED_STA.IND, 580
CP_PROXY_WAKE.REQ, 567
New_EKS, 587
NN_ADD_ALLOC.CNF, 575
NN_ADD_ALLOC.REQ, 574
NN_INL.CNF, 567
NN_INL.REQ, 567
NN_NEW_NET.CNF, 571
NN_NEW_NET.IND, 573
NN_NEW_NET.REQ, 570
NN_REL_ALLOC.CNF, 577
NN_REL_ALLOC.IND, 575
NN_REL_ALLOC.REQ, 576
NN_REL_NET.IND, 578
Management messages
CM_LINK_STATUS.REQ, 617
Management messages
CM_LINK_STATS.CNF, 618
Management messages
CM_LINK_STATS.CNF, 623
Management messages
CM_LINK_STATS.CNF, 623
Management messages
CM_LINK_STATS.CNF, 624
Management messages
CM_LINK_STATS.CNF, 624
Management messages
CM_LINK_STATS.CNF, 624
Management messages
CM_LINK_STATS.CNF, 648
Management messages
CM_LINK_STATS.CNF, 651
Management messages
manufacturer-specific, 651
Management messages

vendor-specific, 651
Man-in-the-middle security attacks, 411
Manufacturer-specific messages, 651
Mapping, 58
Mapping for
BPSK, QPSK, 8-QAM, 16-QAM, 64-QAM, 256-QAM, 1024-QAM, 66, 69
HomePlug AV Frame Control Coherent QPSK, 66
Matching NIDs, 346
Measurement of interframe spacing, 294
Message nomenclature, 13
Message nomenclature, 14
Method for authentication, 335
M-initiated reconfiguration, 229
MME PAD, 507
Modulation normalization scales, 69
MPDU bursting, 276
MTYPE, 494
Multi-network broadcast, 271
N etwork modes, 226
Negotiation of the channel, 491
Neighbor Network
access coexistence, 486
Neighbor Network instantiation, 424
NEK provisioning, 402
for new STA, 402
for part or all of the AVLN, 402
Network concepts, 27
logical network, 27
physical network, 27
Network Encryption Key, 391
Network identification for AVLN, 329
Network Membership Key, 391
Network operation modes
Coordinated, 417
CSMA-Only, 416
overview, 415
Uncoordinated, 416
Network Password, 391
Network power management, 413
Network reference block diagram, 25
Network Time Base synchronization, 286
NIDs

matching, 346
NMK provisioning using UKE mechanism, 695, 705, 706, 707
Nonces, 390
generation, 408
overview, 392
North American carrier and spectral masks, 86
Order for selection of CCo, 357
Original Destination Address, 494
Original Source Address, 494
Outage/failure recovery, 389
Parameter specifications, 32
Pass phrases, 390
Payload Encryption Key Select, 581
Payload Forward Error Correction, 43
Payload Forward Error Correction Encoder, 43
Payload-level encryption, 405
Phrases, 12
PHY
AV Frame Control Interleaver, 42
Channel Interleaver, 49, 52
clock and Network Time Base synchronization, 286
clock frequency tolerance, 90
Diversity Copier, 42
empty tone filling, 59
last symbol padding, 59
mapping function, 58
Payload Forward Error Correction Encoder, 43
PPDU formats, 37, 38
PPDU structure, 38
puncturing, 47
receiver electrical specification, 97
ROBO Interleaver, 54
ROBO modes, 52
scrambler, 44
spurious transmission, 90
symbol timing, 39, 41
tone mask, 84
transmitter electrical specification, 88
Turbo Convolutional Code Encoder, 41
Turbo Convolutional Encoder, 44
turbo interleaving, 48
PHY

clock correction, 290
PHY block-level encryption, 405
Physical networks, 27
Point-to-point smoothing, 318
Power-On Network Discovery Procedure, 321
PPDU
formats, 37, 38
structure, 38
PPDU formats, 37, 38
Primitives, 654
APCM_AUTHORIZE.CNF, 665
APCM_AUTHORIZE.IND, 666
APCM_AUTHORIZE.REQ, 664
APCM_CONN_ADD.CNF, 658
APCM_CONN_ADD.IND, 659
APCM_CONN_ADD.REQ, 658
APCM_CONN_ADD.RSP, 660
APCM_CONN_MOD.CNF, 661
APCM_CONN_MOD.IND, 661
APCM_CONN_MOD.REQ, 660
APCM_CONN_MOD.RSP, 662
APCM_CONN_REL.CNF, 662
APCM_CONN_REL.IND, 663
APCM_CONN_REL.REQ, 662
APCM_GET_BEACON.CNF, 674
APCM_GET_BEACON.REQ, 674
APCM_GET_HFID.CNF, 674
APCM_GET_HFID.REQ, 674
APCM_GET_KEY.CNF, 671
APCM_GET_KEY.REQ, 671
APCM_GET_NETWORKS.CNF, 668
APCM_GET_NETWORKS.REQ, 667
APCM_GET_NEWSTA.CNF, 669
APCM_GET_NEWSTA.IND, 670
APCM_GET_NEWSTA.REQ, 669
APCM_GET_NTB.CNF, 663
APCM_GET_NTB.REQ, 663
APCM_GET_SECURITY_MODE.ASP, 666
APCM_GET_SECURITY_MODE.CNF, 666
APCM_LINK_STATS.CNF, 674
APCM_LINK_STATS.REQ, 673
APCM_NET_EXIT.CNF, 672

APCM_NET_EXIT.REQ, 672
APCM_NW_INFO.CNF, 673
APCM_NW_INFO.REQ, 673
APCM_SET_HFID.CNF, 675
APCM_SET_HFID.REQ, 674
APCM_SET_KEY.CNF, 671
APCM_SET_KEY.REQ, 670
APCM_SET_NETWORKS.CNF, 668
APCM_SET_NETWORKS.REQ, 668
APCM_SET_SECURITY_MODE.CNF, 667
APCM_SET_SECURITY_MODE.REQ, 667
APCM_STA_CAP.CNF, 673
APCM_STA_CAP.REQ, 673
APCM_STA_RESTART.CNF, 672
APCM_STA_RESTART.REQ, 671
APCP_SET_TONE_MASK.CNF, 673
APCP_SET_TONE_MASK.REQ, 672, 675, 676
ETH_RECEIVE.IND, 656
ETH_SEND.CNF, 655
ETH_SEND.REQ, 655
MD_DATA.REQ, 679
Procedure for
association, 481
authentication, 482
authorization, 482
Protocol Adaptation Layer, 654
Protocol Adaptation Layers, 653
Protocol ID, 582
Protocol layer diagram, 26
Protocol Message Number, 583
Protocol Run Number, 583
Proxy Beacons, 370
Proxy networking, 364
Puncturing, 47
Reassembly, 259
References, 1
Releasing bandwidth, 437
Removing a station from an AVLN, 353
Repetition security attachs, 411
Resisting security attacks, 411
Retransmission, 285
automatic, 283

strategies, 285
ROBO Interleaver, 54
ROBO modes, 52
ROBO-AV mapping, 70
Scheduler allocation, 384
Scheduling policy, 436
SC-Join and SC-Add, 350, 351
Scrambler, 44
Security
authorization methods, 392
Device Access Key, 390
Device Password, 391
encryption keys, 390
goals and containts, 31
Network Encryption Key, 391
Network Membership Key, 391
Network Password, 391
nonces, 390, 392
overview, 31, 389
passwords, 390
Temporary Encryption Key, 392
threat mode, 31
Security attacks, 411
man-in-the-middle, 411
repetition, 411
Security state transition diagrams, 688
Segmentation, 257
Selecting a CCo, 353
Service Access Points, 654
Sharing bandwidth in coordinated mode, 434
Shutting down an AVLN, 437
Smoothing, 317
control, 318
end-to-end, 318
point-to-point, 318
Source-aware bridging, 248
Squeeze, 230, 231
STA behavior after power-on, 323
STAs, 337, 340, 342, 344
Station roles, 30
Stations
getting full STA information, 331

removing from an AVLN, 353
updating with the TEI Map, 335
SubAVLNs, 27
Symbol mapping
8-QAM, 68
except 8-QAM, 67
Symbol timing, 39, 41
SYNCP AV phase reference, 71
System block diagram, 25
System overview, 25
System reference model, 25
TDMA channel access, 210
TEIs
assignment and renewal, 333
disambiguated, 333
leases and renewals, 334
when to stop using, 334
TEK computation, 699
Temporary Encryption Key, 392
Threat mode, 31
Tone maps
intervals, 243
maintenance, 243
Tone mask, 84
transfer/handover of CCo functions, 358
Transport services, 217
connectionless, 217
connection-oriented, 218
Turbo Convolutional Code Encoder, 41
Turbo Convolutional Encoder, 44
Turbo interleaving, 48
Two Unassociated STAs
both in SC-Join, 344
form an AVLN using a DAK-encrypted NMK, 340
one in SC-add and one in SC-Join, 342
with matching NIDs, 337
Unassociated CCo behavior, 325
Unassociated STA behavior, 324
Uncoordinated mode, 416
Universally Unique Identifier, 583
Updating STAs with the TEI MAP, 335
User experiences (UEs) (informative), 683

User-appointed CCo, 354
Vendor-specific messages, 651
Virtual Carrier Sense (VCS) Timer, 209
When to stop using a TEI, 334
Words, 12