| | |
|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** |
| Title | **Packet Convergence Sublayer for 802.16.1 Air Interface Specification** |
| Date Submitted | **2001-01-16** |
| Source(s) | Ken Stanwood, Stanley Wang, and Robert Johnson<br>Ensemble Communications<br>9890 Towne Centre Dr.<br>San Diego, CA 92121<br>Voice: (858) 404-6559<br>Fax: (858) 458-1401<br>mailto:ken@ensemblecom.com<br>mailto:stanley@ensemblecom.com<br>mailto:robert@ensemblecom.com |
| Re: | IEEE 802.16.1-01/02 : Call for Comments on IEEE 802.16.1/D1-2000 |
| Abstract | This document defines a Convergence Sublayer for packet-based variable-length bearer traffic that utilizes the MAC Common Part Sublayer functionality. |
| Purpose | To provide the necessary text for the Packet Convergence Sublayer, in support of packet-based variable-length bearer traffic. |
| Notice | This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor grants a free, irrevocable license to the IEEE to incorporate text contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16. |
| Patent Policy and Procedures | The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing the standard."<br>Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>. |

# Packet Convergence Sublayer for 802.16.1 Air Interface Specification

Ken Stanwood, Dr. Stanley Wang, Robert Johnson
Ensemble Communications

## Overview

The IEEE 802.16 Packet Convergence Sublayer (CS) resides on top of the IEEE 802.16 Media Access Control (MAC) *Common Part Sublayer* (CPS). The Packet CS is responsible for accepting variable-length packets from its Upper Layers and delivering CS Protocol Data Units (PDU) to the appropriate MAC-CPS Service Access Point (SAP). The MAC-CPS creates its Protocol Control Information (i.e. MAC header in this case) and is responsible for delivery of MAC PDUs to its peer MAC-CPS according to the Quality of Service (QOS) requirements of the particular Service Flow (SF).

The PKT CS utilizes the services provided by the MAC-CPS and performs the following functions:

- Classification or Direct Mapping of Packet CS SDUs to MAC Service Flows/CIDs.
- Payload Header Suppression and Restoration.
- Delivery to MAC SAP.
- Receipt from MAC SAP.

## References

[IEEE00] IEEE 802.16 , "Draft Standard for Air Interface for Fixed Broadband Wireless Access Systems," IEEE 802.16.1/D1-2000, December 2000.

[ISO94] ISO, "Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model," ISO/IEC 7498-1:1994.

Other References are TBD

## Definitions

**Base Station (BS)**: A generalized equipment set providing connectivity, management, and control of Subscriber Stations.

**Connection Identifier (CID)**: A unidirectional, MAC layer address that identifies a connection connecting equivalent peers of SS's and BS's MAC layers.

**Management Information Base (MIB)**: A structured set of objects, which are readable or modifiable via a network management protocol.

**Payload Header Suppression (PHS)**: The process of suppressing the repetitive portion of payload headers at the sender and restoring the headers at the receiver.

**Payload Header Suppression Field (PHSF)**: A string of bytes representing the header portion of a PSU in which one or more bytes will be suppressed (i.e. a snapshot of the uncompressed PDU header inclusive of suppressed and unsuppressed bytes).

**Payload Header Suppression Index (PHSI)**: An 8-bit mask that indicates which bytes in the PHSF to suppress, and which bytes to not suppress.

**Payload Header Suppression Rule (PHSR)**: A ser of TLV’s that apply to a specific PHS Index.

**Payload Header Suppression Size (PHSS)**: The length of the Suppressed Field in bytes. This value is equivalent to the number of bytes in the PHSF and also the number of valid bits in the PHSM.

**Payload Header Suppression Valid (PHSV)**: A flag that tells the sending entity to verify all bytes that are to be suppressed.

**Protocol Data Unit (PDU)**: A data unit generated by a particular protocol layer for its next lower layer.

**Service Access Point (SAP)**: The point in a protocol stack where services of a lower layer are available to the next higher layer.

**Service Data Unit (SDU)**: A data unit handed to a particular protocol layer from the layer above it.

**Service Flow (SF)**: A Service Flow is a unidirectional flow of MAC Service Data Units on a connection that provides a particular Quality of Service.

**Subscriber Station (SS)**: A generalized equipment set providing connectivity between subscriber equipment and a Base Station.

## Abbreviations and Acronyms

| | |
|---|---|
| ATM | Asynchronous Transfer Mode |
| BS | Base Station |
| CID | Connection Identifier |
| CPS | Common Part Sublayer |
| CPT | CS Pass Through |
| CS | Convergence Sublayer |
| MAC | Media Access Control |
| MIB | Management Information Base |
| PCI | Protocol Control Information |
| PDU | Protocol Data Unit |
| PHS | Payload Header Suppression |
| PHSF | Payload Header Suppression Field |
| PHSI | Payload Header Suppression Index |
| PHSM | Payload Header Suppression Mask |
| PHSS | Payload Header Suppression Size |
| PHSR | Payload Header Suppression Rule |
| PHSV | Payload Header Suppression Verify |
| PPP | Point-to-Point Protocol |
| QoS | Quality of Service |
| SAP | Service Access Point |
| SDU | Service Data Unit |
| SF | Service Flow |
| SS | Subscriber Station. |
| TLV | Type Length Value. |
| USG | Unsolicited Grant Service. |

## Changes to the Existing Draft Standard

In order to support the specification defined in this Packet CS contribution, certain aspects of the existing draft standard (*see* [IEEE00]) shall be modified. This section details all necessary changes and the rationales for the changes.

# Additional Definitions and Acronyms

## Additional definitions

1. On page 20, line 44 add the following definitions:
   **Payload Header Suppression (PHS)**: The process of suppressing the repetitive portion of payload headers at the sender and restoring the headers at the receiver.
   **Payload Header Suppression Field (PHSF)**: A string of bytes representing the header portion of a PSU in which one or more bytes will be suppressed (i.e. a snapshot of the uncompressed PDU header inclusive of suppressed and unsuppressed bytes).
   **Payload Header Suppression Index (PHSI)**: An 8-bit mask that indicates which bytes in the PHSF to suppress, and which bytes to not suppress.
   **Payload Header Suppression Rule (PHSR)**: A ser of TLV's that apply to a specific PHS Index.
   **Payload Header Suppression Size (PHSS)**: The length of the Suppressed Field in bytes. This value is equivalent to the number of bytes in the PHSF and also the number of valid bits in the PHSM.
   **Payload Header Suppression Valid (PHSV)**: A flag that tells the sending entity to verify all bytes that are to be suppressed.
   **Protocol Data Unit (PDU)**: A data unit generated by a particular protocol layer for its next lower layer.
2. On page 21, line 1 add the following definition:
   **Service Data Unit (SDU)**: A data unit handed to a particular protocol layer from the layer above it.

Note that the definitions for PDU and SDU are per ISO/IEC 7498 standard (*see* [ISO94]).

## Additional acronyms

3. On page 21, line 62 add the following acronyms:

| | |
|---|---|
| CPS | Common Part Sublayer |
| CPT | CS Pass Through |

4. On page 22, line 42 add the following acronym:

| | |
|---|---|
| PCI | Protocol Control Information |

5. On page 22, line 45 add the following acronyms:

| | |
|---|---|
| PHS | Payload Header Suppression. |
| PHSF | Payload Header Suppression Field |
| PHSI | Payload Header Suppression Index |
| PHSM | Payload Header Suppression Mask |
| PHSS | Payload Header Suppression Size |
| PHSR | Payload Header Suppression Rule |
| PHSV | Payload Header Suppression Verify |

6. On page 22, line 50 add the following acronym:

| | |
|---|---|
| PPP | Point-to-Point Protocol |

7. On page 22, line 58 add the following acronym:

| | |
|---|---|
| SF | Service Flow |

# Changes to the MAC Common Part Sublayer Service Definition

## Changes to existing MAC-CREATE-CONNECTION service primitives

In addition to the parameters currently specified for the MAC-CREATE-CONNECTION.*request* service primitive (*see* 6.1.1.1 of [IEEE00]), the parameters listed in Table 1 shall be included in the service primitive.

**Table 1**: Changes to MAC-CREATE-CONNECTION.request service primitive

| Parameter | Values | Comment |
|---|---|---|
| Packing On/Off Indicator | 0 = packing off<br>1 = packing on | Default is 0. |
| Length Indicator | 0 – variable-length SDUs<br>1 – fixed-sized SDUs | Default is 0. Used by packing to determine the number of SDUs in the PDU. |
| Fixed SDU Length | 0-255 – packing must be in this multiple of bytes | The only valid values for ATM CS are 48 and 50 when PHS is on, and 53 when PHS is off.<br>This field is undefined for the Packet CS. |

### Changes to existing MAC-CHANGE-CONNECTION service primitives

In addition to the parameters currently specified for the MAC-CHANGE-CONNECTION.*request* service primitive (*see* 6.1.1.5 of [IEEE00]), the same parameters added to the MAC-CREATE-CONNECTION.*request* service primitive (*see* Table 1) shall be included in the service primitive.

### Changes to existing MAC-DATA service primitives

In addition to the parameters currently specified for the MAC-DATA.*request* and MAC-DATA.*indication* service primitives (*see* 6.1.1.10 and 6.1.1.11 of [IEEE00]), the parameter listed in Table 2 shall be included in these service primitives:

**Table 2**: Changes to MAC-DATA service primitives

| Parameter | Values | Comment |
|---|---|---|
| CS Pass Through (CPT) | 3 bits, CS dependant | CPT bits are currently undefined for the Packet CS. |

### Additional MAC CPS service primitives

There is no new MAC CPS service primitive defined.

### Specific changes to the existing document

The following changes to the existing draft standard (*see* [IEEE00]) shall be made:

8. On page 28, line 59 replace "traffic parameters" with "service flow parameters".
9. On page 28, line 60 add the following lines:
   packing indicator,
   length indicator,
   fixed SDU length,
10. On page 29, line 16 add the following paragraphs:
    The packing indicator specifies whether packing is on/off for a given Service Flow.
    The length indicator specifies whether the SDUs on the Service Flow are fixed length or variable length.
    The fixed SDU length specifies the length of the SDU for a fixed-length SDU Service Flow.
11. On page 30, line 1 replace "traffic parameters" with "service flow parameters".
12. On page 34, line 38 add the following line:
    CS pass through,

13. On page 34, line 52 add the following paragraph:
    The CS pass through specifies the 3-bit information passed by the CS. It is to be placed in the CPT field of the MAC-CPS PDU header.
14. On page 35, line 29 add the following line:
    CS pass through,

## Changes to the Service Specific Convergence Sublayer

### Specific changes to the existing document

The following changes to the existing draft standard (*see* [IEEE00]) shall be made:

15. On page 24, line 23 replace sections 5.2 and 5.3 with the content from this Packet CS contribution starting with “Reference Model” and ending with “Common Sublayer” (inclusive).
16. The TLV addition/replacement exercise for the “TLV Encodings” section in this contribution is left as TBD (see “Appendix A: Open Issues in this contribution).

## Changes to the MAC Layer Protocol Architecture

### Changes to the MAC PDU header

To allow better integration with the CS, the following change to the MAC-CPS PDU header shall be made:

Use three (3) of the reserved bits for *CS Pass Through* (CPT) of information.

### Specific changes to the existing document

The following changes to the existing draft standard (*see* [IEEE00]) shall be made:

17. On page 37, line 13 change the uplink MAC header format to include a new 3-bit field. Label the new field "CPT" and place it after the "PDE" field. Reduce the length of "Reserved" field from 6 bits to 3 bits.
18. On page 37, line 56 change the downlink MAC header format to include a new 3-bit field. Label the new field "CPT" and place it after the "PDE" field. Reduce the length of "Reserved" field from 6 bits to 3 bits.
19. On page 39, line 19 add the following new row to the table:

| | | |
|---|---|---|
| CPT | 1 | This field allows the Convergence Sublayer to pass service specific information to the MAC-CPS. |

## Packing, Fragmentation and/or Concatenation

Information contained in this section is informative. Functions described in this section shall be defined in the MAC-*Common Part Sublayer* (MAC-CPS) specification (*see* 6.2.1.3 and 6.2.1.4 of [IEEE00]). Details on *Payload Header Suppression* (PHS) as related to the Packet CS, are defined in this Packet CS contribution.

### Packed Mode vs. Single-SDU Mode

Packing refers to the process by which several SDUs are packed into one PDU payload in order to reduce the overhead due to *Protocol Control Information* (PCI), i.e., PDU headers and trailers. In *Packed Mode* (PM), one or more MAC-CPS SDUs, each of which contains a single Packet CS PDU with or without PHS, are packed into one single MAC-CPS PDU. Note that packing can be done independent of PHS (i.e., with or without PHS).

In *Single-SDU Mode* (SSM), each MAC-CPS SDU occupies the entire MAC-CPS PDU payload. Note that PM and SSM are mutually exclusive and that authority to use either PM or SCM is provisioned during connection establishment.

### Fragmentation

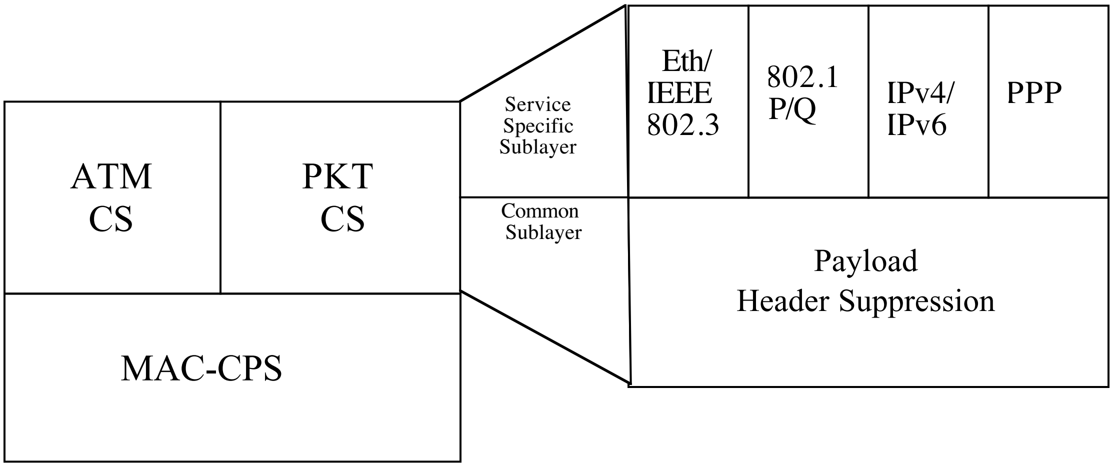
Fragmentation is the process by which a MAC SDU is divided into one or more MAC PDU payloads. This process is undertaken to allow efficient use of available bandwidth. The authority to fragment MAC SDUs is provisioned when the connection is created. For the Packet CS, MAC-CPS fragmentation must always be enabled (see the MTU Considerations section in this Packet CS contribution).

### Concatenation

Concatenation is the process by which multiple MAC-CPS PDUs are concatenated into one single uplink or downlink burst. Since each MAC-CPS PDU is identified by a unique CID, the receiving MAC-CPS entity (at either a BS or SS) is able to reassemble one or multiple received PDUs to the original SDU and present the SDU to the correct instance of MAC-CPS SAP.

## Reference Model

The following reference model expands on the 802.16.1 System Reference Model to illustrate the logical entities that may be present in the Packet CS.



## Generic PDU Format

| | |
|---|---|
| PHSI<br>(1 Byte)<br>(Optional) | Packet CS Payload |

- Payload Header Suppression Index (PHSI): may/may not be present in Packet CS PDU, based on the on/off state of the given Service Flow's Payload Header Suppression Indicator (TLV).
- Packet CS Payload: per service type specific payload (see Service Specific Sublayer).

## Maximum Transfer Unit (MTU) Considerations

The MAC-CPS provides the SDU fragmentation service to the Packet CS, and MUST be enabled for variable-length SDU service (see MAC-CPS). Since the MAC-CPS fragmentation service is always enabled for MAC-CPS variable-length SDU service, the MAC-CPS does not pose any MTU requirements on the Packet CS. In other words, the Packet CS may send to the MAC-CPS SAP up to the maximum Packet CS PDU length for the given service type (including Packet CS control information like the PHSI Byte).

## Service Specific Sublayer

## Classification

A classifier is a set of matching criteria applied to each packet entering the BWA network. It consists of some packet matching criteria (destination IP address, for example), a classifier priority, and a reference to a CID. If a packet matches the specified packet matching criteria, it is then delivered to the SAP with for delivery on the connection defined by the CID. The Service Flow characteristics of the connection provide the QoS for that packet.

Several Classifiers may all refer to the same Service Flow. The classifier priority is used for ordering the application of Classifiers to packets. Explicit ordering is necessary because the patterns used by Classifiers may overlap. The priority need not be unique, but care SHALL be taken within a classifier priority to prevent ambiguity in classification. The highest priority Classifier SHALL be applied first. Downstream Classifiers are applied by the BS to packets it is transmitting, and Upstream Classifiers are applied at the SS. Figure (TBD) and Figure (TBD) illustrate the mappings discussed above.

It is possible for a packet to fail to match the set of defined classifiers. In this case, the Packet CS Service Type may either associate the packet with it's assigned default CID or discard the packet, but the action taken SHALL be configurable for each Packet CS Service Type (FFS: assignment of Packet CS Service Type default CID may be accomplished via a Classification TLV that specifies "default-forwarding", -or- the default CID may be simply a low-priority classification rule that matches all traffic for the specific Packet CS Service Type.).

The packet classification table contains the following fields:

- Priority -- determines the search order for the table. Higher priority Classifiers are searched before lower priority Classifiers.
- Ethernet/IEEE 802.3 Classification Parameters --zero or more of the Ethernet/IEEE 802.3 classification parameters (Destination MAC Address, Source MAC Address, Ethertype/SAP).
- IEEE 802.1P/Q Parameters -- zero or more of the IEEE 802.1P/Q classification parameters (802.1P Priority Range, 802.1Q VLAN ID).
- IPv4/IPv6 Classification Parameters -- zero or more of the IP classification parameters (Ipv4 TOS Range/Mask, Ipv4 Protocol, Ipv4 Source Address/Mask, Ipv4 Destination Address/Mask).
- TCP/UDP Classification Parameters -- TCP/UDP Source Port Start, TCP/UDP Source Port End, TCP/UDP Destination Port Start, TCP/UCP Destination Port End).
- Service Flow Identifier -- identifier of a specific flow to which this packet is to be directed.

Classifiers can be added to the table either via management operations (configuration file, registration, and SNMP), or via dynamic operations (dynamic signaling, MAC-CPS SAP).

SNMP-based operations can view Classifiers that are added via dynamic operations, but cannot modify or delete Classifiers that are created by dynamic operations. The format for classification table parameters defined in the configuration file, or dynamic signaling message is contained in Section (TBD).

Typically, an outgoing user data Packet is submitted by an Upper Layer protocol (such as the forwarding bridge of a SS) for transmission on the MAC interface. The packet is compared against a set of Classifiers. The matching Classifier for the Packet identifies the corresponding Service Flow via the Service Flow ID (SFID). In the case where more than one Classifier matches the packet, the highest Priority Classifier is chosen.

The Classifier matching a packet MAY be associated with a Payload Header Suppression Rule. A PHS Rule provides details on how header Bytes of a Packet PDU can be omitted, replaced with a Payload Header Suppression Index for transmission and subsequently regenerated at the receiving end. PHS Rules are indexed by the combination of {SFID, PHSI}. When a Service Flow is deleted, all Classifiers and any associated PHS Rules referencing it SHALL also be deleted.

## Direct Mapping

If a packet has already been determined by Upper Layer policy mechanisms to be associated with a particular Service Class Name/Priority combination, that combination associates the packet with a particular Connection directly. The Packet CS/Upper Layer may also be aware of the particular Connections in the MAC-CPS, and may have assigned the packet directly to a Connection based on management operations (i.e. port-based direct mapping) or dynamic operations (signaling at the SS Customer network may have triggered a DSA message towards the BS, so there is a Direct Mapping between the Upper Layer “tag” and the SF/CID). In these cases, a packet is considered to be Directly Mapped with a Connection as selected by the Upper Layer and/or Packet CS.

The Direct Mapping for a packet MAY be associated with a Payload Header Suppression Rule. A PHS Rule provides details on how header Bytes of a Packet PDU can be omitted, replaced with a Payload Header Suppression Index for transmission and subsequently regenerated at the receiving end. PHS Rules are indexed by the combination of {SFID, PHSI}. When a Service Flow is deleted, the Direct Mapping and any associated PHS Rules referencing it SHALL also be deleted.

## Service Types

The following sections cover the service-specific details and considerations related to the transport and management of the Packet CS supported services. With regard to service type support, the following requirements SHALL be met:

The Ethernet Packet CS Service Type SHALL be supported by the BS and SS, for use with the MAC-CPS Secondary CID.

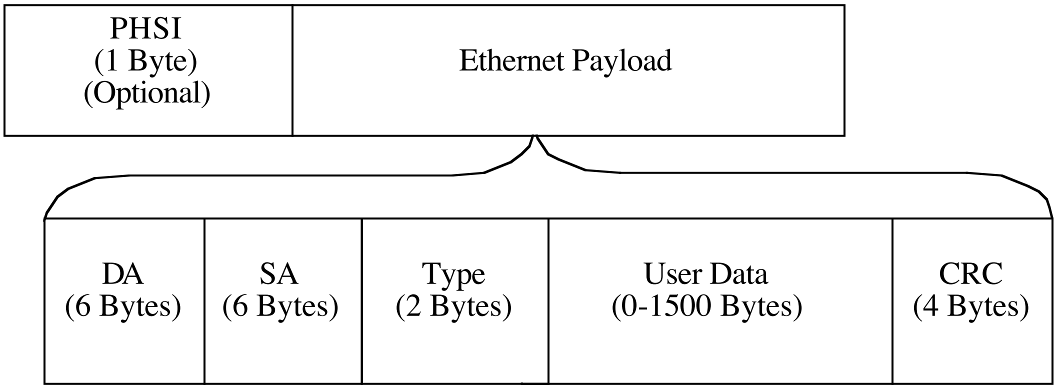
Other Packet CS Service types MAY be supported as needed for a particular deployment of the 802.16 system. It is expected that a set of “CS Service Profiles” will be created to help interoperability in specific target markets, and limit the number of required feature sets on a particular 802.16 system implementation (BS or SS).

## Ethernet/IEEE 802.3

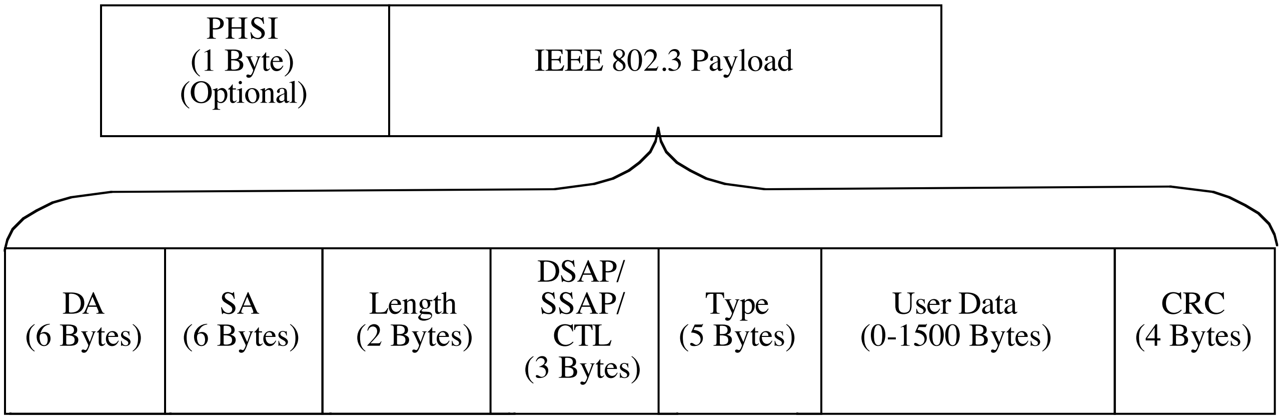
## Data/Control Plane

### *PDU Format*

**Ethernet**



**IEEE 802.3**



### *SDU Classification*

Ethernet/IEEE 802.3 SDUs may be Classified (as opposed to Direct Mapping) using the following categories of classifiers (see the appropriate classification subsection for the associated classification TLVs):

- Ethernet/IEEE 802.3 Classifiers
- IP Classifiers
- TCP/UDP Classifiers
- Vendor Specific Classifiers

### *SDU Direct Mapping*

Ethernet/IEEE 802.3 SDUs may be Directly Mapped (as opposed to Classified) by an Upper Layer Protocol entity. Some examples of Direct Mapping of Ethernet/IEEE 802.3 SDUs to SFs/CIDs are the following:

- Direct Mapping of Ethernet interface to/from SF/CID.
- Direct Mapping of PPP over Ethernet (PPPoE) Session Id to/from SF/CID.

### *Payload Header Suppression Considerations*

## Management Plane

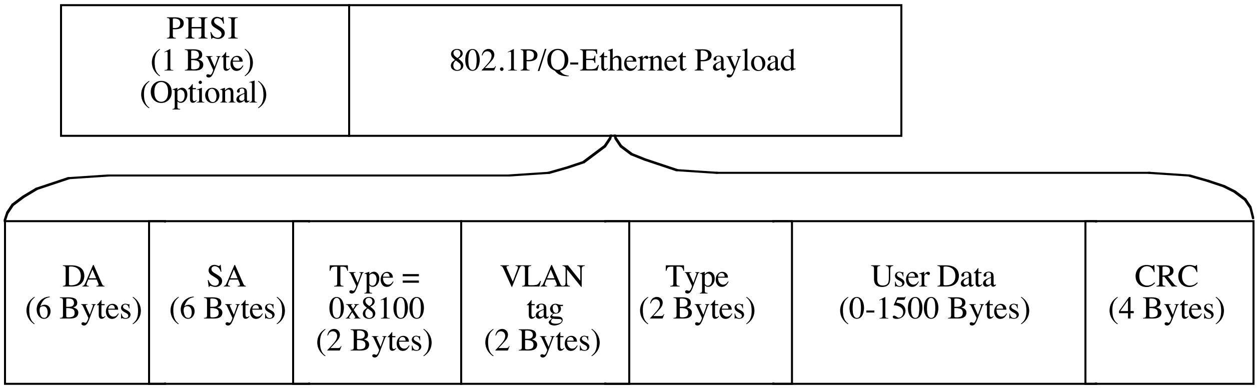
### *MIB Definitions (TBD)*

**802.1P/Q**

## Data/Control Plane

### *PDU Format*

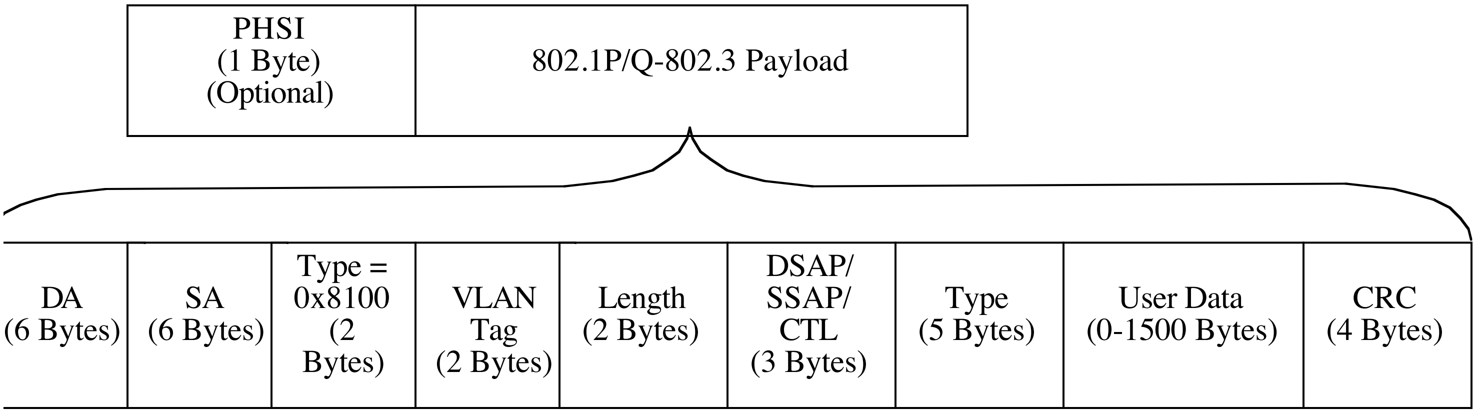
**Ethernet Frame-Mode**



| PHSI<br>(1 Byte)<br>(Optional) | 802.1P/Q-Ethernet Payload |
|---|---|

| DA<br>(6 Bytes) | SA<br>(6 Bytes) | Type =<br>0x8100<br>(2 Bytes) | VLAN<br>tag<br>(2 Bytes) | Type<br>(2 Bytes) | User Data<br>(0-1500 Bytes) | CRC<br>(4 Bytes) |
|---|---|---|---|---|---|---|

**IEEE 802.3 Frame-Mode**



| PHSI<br>(1 Byte)<br>(Optional) | 802.1P/Q-802.3 Payload |
|---|---|

| DA<br>(6 Bytes) | SA<br>(6 Bytes) | Type =<br>0x8100<br>(2<br>Bytes) | VLAN<br>Tag<br>(2 Bytes) | Length<br>(2 Bytes) | DSAP/<br>SSAP/<br>CTL<br>(3 Bytes) | Type<br>(5 Bytes) | User Data<br>(0-1500 Bytes) | CRC<br>(4 Bytes) |
|---|---|---|---|---|---|---|---|---|

### *SDU Classification*

802.1P/Q SDUs may be Classified (as opposed to Direct Mapping) using the following categories of classifiers (see the appropriate classification subsection for the associated classification TLVs):

- 802.1P/Q Classifiers
- Ethernet/IEEE 802.3 Classifiers
- IP Classifiers
- TCP/UDP Classifiers
- Vendor Specific Classifiers

### *SDU Direct Mapping*

802.1P/Q SDUs may be Directly Mapped (as opposed to Classified) by an Upper Layer protocol entity. Some examples of Direct Mapping of 802.1P/Q SDUs to SFs/CIDs are the following:

- Direct Mapping of 802.1P/Q LAN interface to/from SF/CID.

### *Payload Header Suppression Considerations*

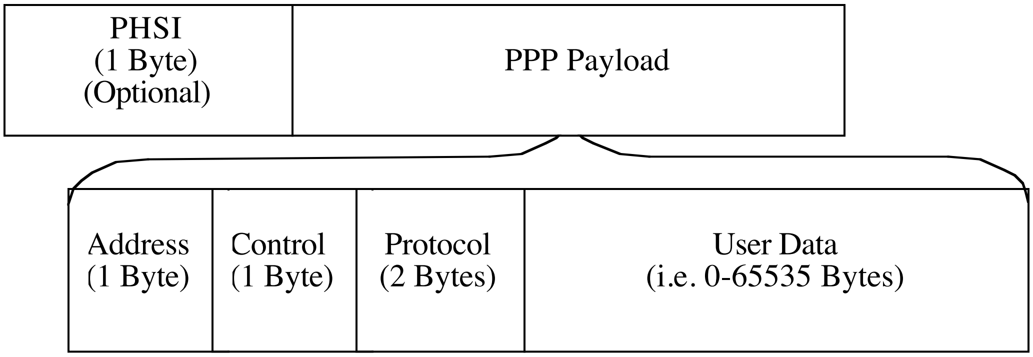
## Management Plane

### *MIB Definitions (TBD)*

# PPP

## Data/Control Plane

### *PDU Format*



NOTE: The maximum length for the PPP Payload User Data field depends on the PPP payload type. Since IP is a typical payload type for PPP sessions, the maximum IP payload length of 65535 Bytes is used as an example. See the Maximum Transfer Unit (MTU) Considerations section for further details.

### *SDU Classification*

In general, PPP SDUs must not be reordered. Since PPP SDU Classification to different SFs/CIDs will result in PPP packet reordering, PPP SDU Classification for purposes of selecting different SFs/CIDs for any single PPP session is not supported (see SDU Direct Mapping). Note that this implies a single PPP session maps one-to-one with a SF/CID.

### *SDU Direct Mapping*

PPP SDUs may be Directly Mapped (as opposed to Classified) by an Upper Layer Protocol entity. Some examples of Direct Mapping of PPP SDUs to SFs/CIDs are the following:

- Direct Mapping of HDLC/PPP interface to/from SF/CID.
- Direct Mapping of PPP over Ethernet (PPPoE) Session Id to/from SF/CID.

### *Payload Header Suppression Considerations*

The Packet CS PHS MAY be configured to suppress/restore the PPP frame header fields, as well as repetitive header Bytes in the PPP Payload's "User Data" field. With regard to Packet CS PHS, there are a few PPP-specific transport considerations, as noted below.

The PPP Link Control Protocol (LCP) has the ability to negotiate the compression/removal of the Address/Control Fields and Protocol Field (ACFC/PFC LCP negotiation) in the PPP frame header. PPP also supports the negotiation of a compression protocol to be used for the end-to-end compression of the PPP "User-Data" field (see PPP Compression Control Protocol, and related IETF documents). The PPP compression protocols may operate with or without the PPP Address/Control and Protocol fields present in the PPP frame header.

When the Packet CS Payload Header Compression service is enabled for a PPP SF direction (upstream/downstream), PPP LCP ACFC/PFC MUST be disabled in the same direction of the PPP link (PPP

LCP is negotiated independently on both ends of the PPP link, as are SFs). This is to ensure correct operation with the Packet CS Payload Header Compression service, and correct operation with already-compressed PPP streams.

When Packet CS PHS service is disabled, the Packet CS imposes no special considerations/restrictions regarding PPP transport, other than those as specified in the SDU Classification section.

The default for Packet CS PHS for PPP SFs SHALL be disabled.

Example PPP LCP ACFC/PFC end-to-end configuration:

- PPPoE: ACFC LCP option MUST not be requested, MUST be rejected. PFC LCP option is NOT RECOMMENDED (IETF RFC 2516).

## Management Plane

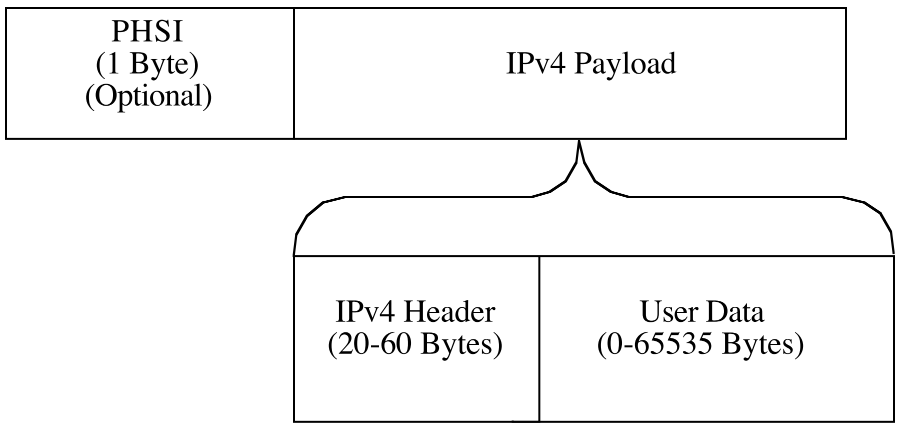
### *MIB Definitions (TBD)*

# IP

## Data/Control Plane

### *PDU Format*

**Ipv4 Format**

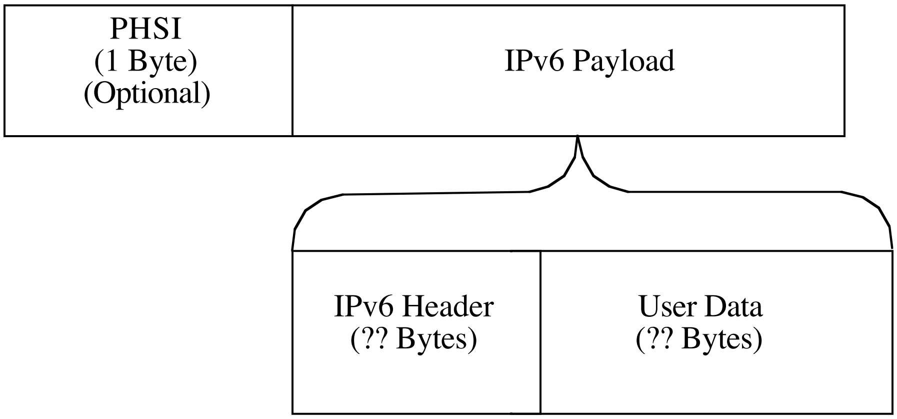


**Ipv4 Header Fields (Mandatory Fixed Portion-20 Bytes)**

- Version (4 bits)
- Header Length (4 bits)
- Type of Service (8 bits)
- Total Length (16 bits)
- Identification (16 bits)
- Reserved Flag (1 bit)
- Don’t Fragment (1 bit)
- More Fragments (1 bit)
- Fragment Offset (13 bits)
- Time to Live (8 bits)
- Protocol (8 bits)
- Header Checksum (16 bits)
- Source Address (32 bits)
- Destination Address (32 bits)

**Ipv6 Format**

The IPv6 format is For Future Study.



**Ipv6 Header Fields (Mandatory Fixed Portion-?? Bytes)**

The IPv6 header fields are For Future Study.

- Version (4 bits)
- Traffic Class (8 bits)
- Flow Label (20 bits)
- Payload Length (16 bits)
- Next Header (8 bits)
- Hop Limit (8 bits)
- Source Address (128 bits)
- Destination Address (128 bits)

### *SDU Classification*

IP SDUs may be Classified (as opposed to Direct Mapping) using the following categories of classifiers (see the appropriate classification subsection for the associated classification TLVs):

- IP Classifiers
- TCP/UDP Classifiers
- Vendor Specific Classifiers

### *SDU Direct Mapping*

IP SDUs may be Directly Mapped (as opposed to Classified) by an Upper Layer Protocol entity. Some examples of Direct Mapping of IP SDUs to SFs/CIDs are the following:

- Direct Mapping of HDLC/IP interface to/from SF/CID.
- Direct Mapping of Multi-Protocol Label Switching (MPLS) “shim” label to/from SF/CID.

### *Payload Header Suppression Considerations*

## Management Plane

### *MIB Definitions (TBD)*

# Common Sublayer

# Payload Header Suppression

## Data/Control Plane

The overview section explains the principles of Payload Header Suppression. The subsequent sections explain the signaling for initialization, operation, and termination. Finally, specific upstream and down-stream examples are given.

## Overview

In Payload Header Suppression, a repetitive portion of the payload headers of the Packet CS SDU is suppressed by the sending entity and restored by the receiving entity. When PHS is enabled for a SF/CID, each SDU is prefixed with a Payload Header Suppression Index (PHSI) that references the Payload Header Suppression Field (PHSF).

The sending entity uses Classifiers or Direct Mapping to map packets into a Service Flow. The Classifier or Direct Mapping uniquely maps packets to its associated Payload Header Suppression Rule. The receiving entity uses the Connection Identifier (CID) and the PHSI to restore the PHSF. Once a PHSF has been assigned to a PHSI, it cannot be changed. To change the value of a PHSF on a Service Flow, a new Payload Header Suppression Rule SHALL be defined, the old rule is removed from the Service Flow, and the new rule is added. When a Classifier or Direct Mapping is deleted, any associated PHS rule SHALL also be deleted.

PHS has a PHSV option to verify or not verify the payload before suppressing it. PHS also has a PHSM option to allow select Bytes not to be suppressed. This is used for sending Bytes that change such as IP sequence numbers, and still suppressing Bytes that do not change.

The BS SHALL assign all PHSI values just as it assigns all CID values. Either the sending or the receiving entity SHALL specify the PHSF and PHSS. This provision allows for pre-configured headers, or for higher level signaling protocols outside the scope of this specification to establish cache entries. PHS is intended for unicast service, and is not defined for multicast service.

It is the responsibility of the higher-layer service entity to generate a PHS Rule that uniquely identifies the suppressed header within the Service Flow. It is also the responsibility of the higher-layer service entity to guarantee that the Byte strings being suppressed are constant from packet to packet for the duration of the Active Service Flow.

### *Example Applications*

- A Classifier on an upstream Ethernet Service Flow which uniquely defines a Voice-over-IP (VoIP) flow by specifying Protocol Type of UDP, IP SA, IP DA, UDP Source Port, UDP Destination Port, the Service Flow Reference, and a PHS Size of 42 Bytes. A PHS Rule references this Classifier providing a PHSI value that identifies this VoIP media flow. For the upstream case, 42 Bytes of payload header PHS are verified and suppressed, and a 1 byte prefix containing the PHSI is added to every packet in that media flow.
- A Classifier that identifies the packets in a Service Flow, of which 90% match the PHSR. Verification is enabled. This may apply in a packet compression situation where every so often compression resets are

done and the header varies. In this example, the scheduling algorithm would allow variable bandwidth, and only 90% of the packets might get their headers suppressed. Since the PHSI extended header value will indicate the choice made, the simple CID/PHSI lookup at the receiving entity will always yield the correct result.

- A Classifier on an upstream Service Flow which identifies all Ethernet IP packets by specifying Ethertype of IP, the Service Flow ID, a PHSS of 14 Bytes, and no verification by the sending entity. In this example, the BS has decided to route the packet, and knows that it will not require the first 14 Bytes of the Ethernet header, even though some parts such as the Source Address or Destination Address may vary. The SS removes 14 Bytes from each upstream frame (Ethernet Header) without verifying their contents and forwards the frame to the Service Flow.

## Operation

To clarify operational packet flow, this section describes one potential implementation. SS and BS implementations are free to implement Payload Header Suppression in any manner as long as the protocol specified in this section is followed. Figure (TBD) illustrates the following procedure.

### *Uplink*

A packet is submitted to the SS Packet CS. The SS may apply a list of Classifier rules or use Direct Mapping to retrieve the Upstream Service Flow, CID, and a PHS Rule. The PHS Rule provides PHSF, PHSI, PHSM, PHSS, and PHSV. If PHSV is set or not present, the SS will compare the Bytes in the packet header with the Bytes in the PHSF that are to be suppressed as indicated by the PHSM. If they match, the SS will suppress all the Bytes in the Upstream Suppression Field except the Bytes masked by PHSM. The SS will then prefix the frame with the PHSI and present the entire PDU to the MAC-CPS SAP for transport on the uplink.

When the BS receives the packet, the BS will determine the associated CID by examination of the generic MAC header. The BS sends the encapsulated SDU to the MAC-CPS SAP associated with that CID. The receiving Packet CS uses the CID and the PHSI to look up PHSF, PHSM, and PHSS. The BS restores the packet and then proceeds with normal packet processing. The restored packet will contain Bytes from the PHSF. If verification was enabled, then the PHSF Bytes will equal the original header byes. If verification was not enabled, then there is no guarantee that the PHSF Bytes will match the original header Bytes.

<TBD: Insert Figure A.4 in Ethernet CS contribution 802.16.1c-00/18>

### *Downlink*

A packet is submitted to the BS Packet CS. The BS may apply a list of Classifier rules or use Direct Mapping to retrieve the Downstream Service Flow, CID, and a PHS Rule. The PHS Rule provides PHSF, PHSI, PHSM, PHSS, and PHSV. If PHSV is set or not present, the BS will verify the Downstream Suppression Field in the packet with the PHSF. If they match, the BS will suppress all the Bytes in the Downstream Suppression Field except the Bytes masked by PHSM. The BS will then prefix the frame with the PHSI and present the entire PDU to the MAC-CPS SAP for transport on the downlink.

The SS will receive the packet based upon the CID Address filtering within the MAC. The SS receives the PDU and then sends it to the Packet CS. The Packet CS then uses the PHSI to lookup PHSF, PHSM, and PHSS. The SS restores the packet and then proceeds with normal packet processing.

Figure (TBD: Figure A.5 in Ethernet CS contribution 802.16.1c-00/18) demonstrates packet suppression and restoration when using PHS masking. Masking allows only Bytes that do not change to be suppressed. Note that the PHSF and PHSS span the entire Suppression Field, included suppressed and unsuppressed Bytes.

## Signaling

Payload Header Suppression requires the creation of three objects:

1. Service Flow.
2. Classifier (when Classification, as opposed to Direct Mapping is used).
3. Payload Header Suppression Rule.

These three objects MAY be created in separate message flows, or MAY be created simultaneously.

PHS Rules are created with Registration, DSA, or DSC messages. The BS SHALL define the PHSI when the PHS Rule is created. PHS Rules are deleted with the DSC or DSD messages. The SS or BS MAY define the PHSS and PHSF.

Figure (TBD: A.6 in Ethernet CS contribution 802.16.1c-00/18) shows the two ways to signal the creation of a PHS Rule.

It is possible to partially specify a PHS rule (in particular the size of the rule) at the time a Service Flow is created. As an example, it is likely that when a Service Flow is first provisioned a portion of the header fields to be suppressed will be known. The values of the rest of the fields (i.e. IP addresses, UDP port numbers, etc.) may not be known and would be provided in a subsequent DSC as part of the activation of the Service Flow (using the "Set PHS Rule" DSC Action). If the PHS Rule is being defined in more than one step, each step, whether it is a registration request or a DSC, SHALL contain both the Service Flow ID (or reference) and a PHS index to uniquely identify the PHS rule being defined.

## Case Study

A Service Class with the Service Class Name of "ETH-G711-UL-USG-HS-42" is established which is intended for G.711 VoIP traffic on the uplink and is mapped to a service flow using USG scheduling. When Classifiers are added to the flow, a PHSS value of 42 is included which explicitly states that the first 42 Bytes of the frame in that flow SHALL be verified, suppressed, and restored.

Figure (TBD: Figure A.7 in Ethernet CS contribution 802.16.1c-00/18) shows the encapsulation used in the upstream with and without Payload Header Suppression. An RTP Voice over IP Payload without IPSEC is used as a specific example to demonstrate efficiency.

Figure (TBD: Figure A.7a in Ethernet CS contribution 802.16.1c-00/18) shows a normal RTP packet carried on an upstream channel. The MAC layer overhead consists of the 7 Byte generic MAC header, the 14 Byte Ethernet Header, and the 4 Byte Ethernet CRC trailer. The VoIP payload uses a 20 Byte IP header, an 8 Byte UDP header, and a 12 Byte RTP header. The voice payload is variable and depends upon the sample time and the compression algorithm used.

Figure (TBD: Figure A.7b in Ethernet CS contribution 802.16.1c-00/18) shows the same payload with Payload Header Suppression enabled. In the upstream, Payload Header Suppression begins with the first Byte after the PHSI field. The 14 Byte Ethernet header, the 20 Byte IP header, and the 8 Byte UDP header have been suppressed, and the one Byte PHSI field is set, for a net reduction of 42 Bytes. In this example of an established VoIP connection, these fields remain constant from packet to packet, and are otherwise redundant.

### Management Plane

## MIB Definitions (TBD)

## TLV Encodings

## MAC-CPS TLVs

### Fixed-Length vs. Variable-Length SDU Indicator

The value of this parameter specifies whether the SDUs on the Service Flow will be fixed length or variable length. The parameter is used only if packing is on for the Service Flow. The default value is 0, i.e., variable-length SDUs.

| Type | Length | Value | Scope |
|---|---|---|---|
|  | 1 | 0 = variable-length SDUs<br>1 = fixed-length SDUs<br><br>default = 0 |  |

For the Packet CS, if this TLV is present in the configuration/registration or dynamic signaling messages, the value MUST be set to 0 (i.e. variable-length SDUs).

### Packing On/Off Indicator

The value of this parameter specifies whether or not packing is turned on or off for a connection. The default is off.

| Type | Length | Value | Scope |
|---|---|---|---|
|  | 1 | 0 = packing off<br>1 = packing on<br><br>default = 0 |  |

## Packet CS Service TLVs

### Service Capabilities

The Packet CS Service Capabilities TLVs allow the BS and SS to communicate the supported subset of Packet CS services during SS registration. The SS SHALL include the Packet CS Service Capabilities TLVs in the REG-REQ message to indicate to the BS the subset of Packet CS services the SS supports. The BS SHALL include the Packet CS Service Capabilities TLVs in the REG-RSP message to indicate to the SS the subset of SS services the BS supports. For example, the BS MAY simply clear bits in the SS's Packet CS Service Capabilities bit-mask, to indicate to the SS the requested services that are not supported by the BS.

The Ethernet Packet CS Service Type SHALL be supported by the BS and SS, for use with the MAC-CPS Secondary CID.

Other Packet CS Service types MAY be supported as needed for a particular deployment of the 802.16 system. It is expected that a set of “CS Service Profiles” will be created to help interoperability in specific target markets, and limit the number of required feature sets on a particular 802.16 system implementation (BS or SS).

The Packet CS Service Capabilities value field is a bit-mask indicating the various Packet CS Service Types.

| Type | Length | Value | Scope |
|---|---|---|---|
| | 4 or 8<br><br>4: Allows 32 Packet CS Service Types.<br><br>8: Allows 64 Packet CS Service Types. | Bit-mask<br><br>Bit 0 – Ethernet<br>Bit 1 -- IEEE 802.3<br>Bit 2 – 802.1P<br>Bit 3 – 802.1Q<br>Bit 4 -- PPP<br>Bit 5 – IPv4<br>Bit 6 – IPv6 | |

FFS: what about adding/removing hardware to SS w/o REG-REQ? Should the SS be able to re-submit its CS Service Capabilities (i.e. in new/existing message?).

### Service Type

The Packet CS Service Type TLV allows the BS and SS to communicate during SF establishment, the requested service for the given SF. The BS and SS SHALL include the Packet CS Service Type TLVs in the REG-REQ/DSA-REQ messages to indicate to the peer the requested service type for the SF.

The Packet CS Service Type TLV is encoded as a variable-length octet string of length n. Each byte in the octet string represents the service layering, starting from the outermost encapsulation and ending with the innermost encapsulation that makes sense to convey for the given SF. The value for each byte in the octet string is the bit-position value as indicated in the Packet CS Service Capabilities TLV.

The outermost Packet CS Service Type for the given SF SHALL be indicated in the given Packet CS Service Type TLV. Additional service layering MAY be indicated as appropriate for the given SF, using the Packet CS Service Type TLV encoding rules.

The rational for the Packet CS Service Type encoding is the following:

1.) The 802.1P/Q service has 2 different framing formats. The correct framing mode can easily be indicated using this method, as well as the 802.1P or 802.1Q modes.
2.) Knowing the relative service layering apriori to the application of classifiers to the given SF (if any), allows the originator of the classification encodings to perform a sanity check on the classifiers to ensure that they make sense for the given service layering before requesting their application to the given SF via DSC signaling.

## Service Type Examples

1.) 802.1P service with IEEE 802.3 framing: Byte 0 = 1 (IEEE 802.3), Byte 1 = 2 (802.1P), Length = 2
2.) IPv4/PPP service: Byte 0 = 4 (PPP), Byte 1 = 5 (IPv4), Length = 2
3.) PPP raw transport service: Byte 0 = 4 (PPP), Length = 1 (i.e. compressed PPP streams, etc.)
4.) PPPoE service: Byte 0 = 0 (Ethernet), Byte 1 = 4 (PPP), Length = 2
5.) Ethernet over PPP service using the PPP Bridging Control Protocol: Byte 0 = 4 (PPP), Byte 1 = 0 (Ethernet), Length = 2
6.) IPv4/Ethernet service: Byte 0 = 0 (Ethernet), Byte 1 = 5 (IPv4), Length = 2
7.) IPv6 service: Byte 0 = 6, Length = 1

| Type | Length | Value | Scope |
|---|---|---|---|
| | n | Variable-length octet string of length n. | |

# Packet CS Classification TLVs

## General SDU Classifier TLVs

### Classifier Reference

The value of the field specifies a reference for the Classifier. This value is unique per Dynamic Service message, or configuration file.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].1 | 1 | 1-255 | |

### Classifier Identifier

The value of the field specifies an identifier for the Classifier. This value is unique to per Service Flow. The BS assigns the Classifier Identifier.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].3 | 2 | 1-65535 | |

### Classifier Rule Priority

The value of the field specifies the priority for the Classifier, which is used for determining the order of the Classifier. A higher value indicates higher priority.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].4 | 1 | 0-255 | |

Classifiers that appear in Configuration files and Registration messages MAY have priorities in the range 0 –255 with the default value 0. Classifiers that appear in DSA/DSC message SHALL have priorities in the range 64-191, with the default value 64.

### Classifier Activation State

The value of this field specifies whether this classifier should become active in selecting packets for the Service Flow. An inactive Classifier is typically used with an AdmittedQoSParameterSet to ensure resources are available for later activation

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].5 | 1 | 0 – Inactive<br>1—Active<br>The default value is 1 – activate the classifier. | |

## Classifier Activation Signal

This field SHALL only be used in Dynamic Service Change messages that originate from the BS and which affect the Active parameter set. It is not present in any other Service Flow signaling messages.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].6 | 1 | 1 — Activate/Deactivate Classifier on Request<br>2 — Activate/Deactivate Classifier on Ack.<br>The default value is (FFS) | |

This field directs the modem to change its upstream transmission characteristics to match those in the DSC either immediately on receiving the DSC-Request, or only after receiving the DSC-Ack. In particular, it signals the time of (de-) activation of any classifiers that are changed by this DSC exchange.

## Classifier Dynamic Service Change Action

When received in a Dynamic Service Change Request, this indicates the action that should be taken with this classifier.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].7 | 1 | 0 — DSC Add Classifier<br>1 — DSC Replace Classifier<br>2 — DSC Delete Classifier | |

## Classifier Error Encodings

This field defines the parameters associated with Classifier Errors.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].8 | n | | |

A Classifier Error Parameter Set is defined by the following individual parameters: Errored Parameter, Confirmation Code and Error Message.

The Classifier Error Parameter Set is returned in REG-RSP, DSA-RSP and DSC-RSP messages to indicate the recipient’s response to a Classifier establishment request in a REG-REQ, DSA-REQ or DSC-REQ message. On failure, the sender SHALL include one Classifier Error Parameter Set for each failed Classifier requested in the REG-REQ, DSA-REQ or DSC-REQ message. Classifier Error Parameter Set for the failed Classifier SHALL include the Confirmation Code and Errored Parameter and MAY include an Error Message. If some Classifier Sets are rejected but other Classifier Sets are accepted, then Classifier Error Parameter Sets SHALL be included for only the rejected Classifiers. On success of the entire transaction, the RSP or ACK message SHALL NOT include a Classifier Error Parameter Set.

Multiple Classifier Error Parameter Sets MAY appear in a REG-RSP, DSA-RSP or DSC-RSP message, since multiple Classifier parameters may be in error. A message with even a single Classifier Error Parameter Set SHALL NOT contain any other protocol Classifier Encodings (e.g. IP, 802.1P/Q).

A Classifier Error Parameter Set SHALL NOT appear in any REG-REQ, DSA-REQ or DSC-REQ messages.

### *Classifier Errored Parameter*

The value of this parameter identifies the subtype of a requested Classifier parameter in error in a rejected Classifier request. A Classifier Error Parameter Set SHALL have exactly one Errored Parameter TLV within a given Classifier Encoding.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].8.1 | n | Classifier Encoding Subtype in Error | |

If the length is one, then the value is the single-level subtype where the error was found, e.g. 7 indicates an invalid Change Action. If the length is two, then the value is the multi-level subtype where there error was found (i.e. 9-2 indicates an invalid IP Protocol value).

### *Classifier Error Code*

This parameter indicates the status of the request. A non-zero value corresponds to the Confirmation Code as described in ***<TBD>***. A Classifier Error Parameter Set SHALL have exactly one Error Code within a given Classifier Encoding.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].8.2 | 1 | Confirmation code | |

A value of okay(0) indicates that the Classifier request was successful. Since a Classifier Error Parameter Set is only applies to errored parameters, this value SHALL NOT be used.

### *Classifier Error Message*

This subtype is optional in a Classifier Error Parameter Set. If present, it indicates a text string to be displayed on the SS console and/or log that further describes a rejected Classifier request. A Classifier Error Parameter Set MAY have zero or one Error Message subtypes within a given Classifier Encoding.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].8.3 | n | Zero-terminated string of ASCII characters. | |

Note: The length N includes the terminating zero.
Note: The entire Classifier Encoding message SHALL have a total length of less than 256 characters.

### Ethernet/IEEE 802.3

This field defines the parameters associated with Ethernet/IEEE 802.3 packet classification.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].10 | n | | |

### Destination Ethernet Address

The value of the field specifies the matching value for the Ethernet destination address. An Ethernet packet with Ethernet destination address "EtherDst" matches this parameter if Dst = (EtherDst AND EtherDstMask), where "EtherDstMask" is the parameter from Section (TBD). If this parameter is omitted, then comparison of the Ethernet destination address for this entry is irrelevant.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].10.1 | 6 | dst1, dst2, dst3, dst4, dst5, dst6 | |

### Destination Ethernet Address Mask

The value of the field specifies the mask value for the Ethernet destination address, as described in Section (TBD). If this parameter is omitted, then the default Ethernet destination address mask is 255.255.255.255.255.255.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].10.2 | 6 | dmask1, dmask2, dmask3, dmask4, dmask5, dmask6 | |

### Source Ethernet Address

The value of the field specifies the matching value for the Ethernet source address. An Ethernet packet with Ethernet source address "EtherSrc" matches this parameter if Src = (EtherSrc AND EtherSrcMask), where "EtherSrcMask" is the parameter from Section (TBD). If this parameter is omitted, then comparison of the Ethernet source address for this entry is irrelevant.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].10.3 | 6 | src1, src2, src3, src4, src5, src6 | |

### Source Ethernet Address Mask

The value of the field specifies the mask value for the Ethernet source address, as described in Section (TBD). If this parameter is omitted, then the default Ethernet source address mask is 255.255.255.255.255.255.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].10.4 | 6 | smask1, smask2, smask3, smask4, smask5, smask6 | |

## Ethertype/IEEE 802.2 SAP

type, eprot1, and eprot2 indicate the format of the layer 3 protocol ID in the Ethernet packet as follows:

If type = 0, the rule does not use the layer 3 protocol type as a matching criteria. If type = 0, eprot1, eprot2 are ignored when considering whether a packet matches the current rule.

If type = 1, the rule applies only to frames which contain an Ethertype value. Ethertype values are contained in packets using the DEC-Intel-Xerox (DIX) encapsulation or the RFC1042 Sub-Network Access Protocol (SNAP) encapsulation formats. If type = 1, then eprot1, eprot2 gives the 16-bit value of the Ethertype that the packet SHALL match in order to match the rule.
If type = 2, the rule applies only to frames using the IEEE 802.2 encapsulation format with a Destination Service (DSAP) other than 0xAA (which is reserved for SNAP). If type = 2, the lower 8 bits of the eprot1, eprot2, SHALL match the DSAP byte of the packet in order to match the rule.

If the Ethernet frame contains an 802.1P/Q Tag header (i.e., Ethertype 0x8100), this object applies to the embedded Ethertype field within the 802.1P/Q header.

Other values of type are reserved. If this TLV is omitted, then comparison of either the Ethertype or IEEE 802.2 DSAP for this rule is irrelevant.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].10.5 | 3 | type, eprot1, eprot2 | |

## IEEE 802.1P/Q

This field defines the parameters associated with IEEE 802.1P/Q packet classification.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].11 | n | | |

## IEEE 802.1P User_Priority

The values of the field specify the matching parameters for the IEEE 802.1P user_priority bits. An Ethernet packet with IEEE 802.1P user_priority value “priority” matches these parameters if pri-low <= priority <= pri-high. If this field is omitted, then comparison of the IEEE 802.1P user_priority bits for this entry is irrelevant.

If this parameter is specified for an entry, then Ethernet packets without IEEE 802.1Q encapsulation SHALL NOT match this entry. If this parameter is specified for an entry on a SS that does not support forwarding of IEEE 802.1Q encapsulated traffic, then this entry SHALL NOT be used for any traffic.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].11.1 | 2 | pri-low, pri-high.<br>Valid Range<br>0 — 7 for pri-low and pri-high | |

## IEEE 802.1Q VLAN_ID

The value of the field specifies the matching value for the IEEE 802.1Q VLAN ID bits. Only the first (i.e. left-most) 12 bits of the specified VLAN ID field are significant; the final four bits SHALL be ignored for comparison. If this field is omitted, then comparison of the IEEE 802.1Q VLAN ID bits for this entry is irrelevant.
If this parameter is specified for an entry, then Ethernet packets without IEEE 802.1Q encapsulation SHALL NOT match this entry. If this parameter is specified for an entry on a SS that does not support forwarding of IEEE 802.1Q encapsulated traffic, then this entry SHALL NOT be used for any traffic.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].11.2 | 2 | vlan_id1, vlan_id2 | |

### PPP

No classification TLV's are supported for the PPP Service Specific Sublayer.

### IP

This field defines the parameters associated with IP packet classification.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].9 | n | | |

## IP Type of Service Range and Mask

The values of the field specify the matching parameters for the IP ToS byte range and mask. An IP packet with IP ToS byte value "ip-tos" matches this parameter if tos-low <= (ip-tos AND tos-mask) <= tos-high. If this field is omitted, then comparison of the IP packet ToS byte for this entry is irrelevant.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].9.1 | 3 | tos-low, tos-high, tos-mask | |

## IP Protocol

The value of the field specifies the matching value for the IP Protocol field [RFC-1700]. If this parameter is omitted, then comparison of the IP header Protocol field for this entry is irrelevant.

There are two special IP Protocol field values: "256" matches traffic with any IP Protocol value, and "257" matches both TCP and UDP traffic. An entry that includes an IP Protocol field value greater than 257 SHALL be invalidated for comparisons (i.e. no traffic can match this entry).

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].9.2 | 2 | prot1, prot2<br>Valid Range<br>0 — 257 | |

## IP Source Address

The value of the field specifies the matching value for the IP source address. An IP packet with IP source address "ip-src" matches this parameter if src = (ip-src AND smask), where "smask" is the parameter from Section (TBD). If this parameter is omitted, then comparison of the IP packet source address for this entry is irrelevant.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].9.3 | 4 | src1, src2, src3, src4 | |

## IP Source Mask

The value of the field specifies the mask value for the IP source address, as described in Section (TBD). If this parameter is omitted, then the default IP source mask is 255.255.255.255.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].9.4 | 4 | smask1, smask2, smask3, smask4 | |

## IP Destination Address

The value of the field specifies the matching value for the IP destination address. An IP packet with IP desti-nation address "ip-dst" matches this parameter if dst = (ip-dst AND dmask), where "dmask" is the parameter from Section A.5.2.1.4.6. If this parameter is omitted, then comparison of the IP packet destination address for this entry is irrelevant.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].9.5 | 4 | dst1, dst2, dst3, dst4 | |

## IP Destination Mask

The value of the field specifies the mask value for the IP destination address, as described in Section (TBD). If this parameter is omitted, then the default IP destination mask is 255.255.255.255.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].9.6 | 4 | dmask1, dmask2, dmask3, dmask4 | |

## TCP/UDP

This field defines the parameters associated with TCP/UDP packet classification.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].x | n | | |

## IP Fragmentation Considerations

Larger IP packets entering into the 802.16 system may have been subject to IP fragmentation.

When applying TCP/UDP classifiers, both the BS and SS SHALL ensure that the TCP/UDP classifiers are not applied to fragmented TCP/UDP payload bytes.

## TCP/UDP Source Port Start

The value of the field specifies the low-end TCP/UDP source port value. An IP packet with TCP/UDP port value “src-port” matches this parameter if sportlow <= src-port <= sporthigh. If this parameter is omitted, then the default value of sportlow is 0. This parameter is irrelevant for non-TCP/UDP IP traffic.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].x.1 | 2 | sportlow1, sportlow2 | |

## TCP/UDP Source Port End

The value of the field specifies the high-end TCP/UDP source port value. An IP packet with TCP/UDP port value “src-port” matches this parameter if sportlow <= src-port <= sporthigh. If this parameter is omitted, then the default value of sporthigh is 65535. This parameter is irrelevant for non-TCP/UDP IP traffic.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].x.2 | 2 | dportlow1, dportlow2 | |

## TCP/UDP Destination Port Start

The value of the field specifies the low-end TCP/UDP destination port value. An IP packet with TCP/UDP port value “dst-port” matches this parameter if dportlow <= dst-port <=dporthigh. If this parameter is omitted, then the default value of dportlow is 0. This parameter is irrelevant for non-TCP/UDP IP traffic.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].x.3 | 2 | dportlow1, dportlow2 | |

## TCP/UDP Destination Port End

The value of the field specifies the high-end TCP/UDP destination port value. An IP packet with TCP/UDP port value “dst-port” matches this parameter if dportlow <= dst-port <= dporthigh. If this parameter is omitted, then the default value of dporthigh is 65535. This parameter is irrelevant for non-TCP/UDP IP traffic.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].x.4 | 2 | dporthigh1, dporthigh2 | |

### Vendor Specific

This allows vendors to encode vendor-specific Classifier parameters. The Vendor ID SHALL be the first TLV embedded inside Vendor Specific Classifier Parameters. If the first TLV inside Vendor Specific Classifier Parameters is not a Vendor ID, then the TLV SHALL be discarded. (Refer to TBD)

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.[22/23].43 | n | | |

## Packet CS Payload Header Suppression TLVs

### General Payload Header Supression TLVs

### PHS Indicator

The value of this parameter specifies whether the SDUs on the Service Flow will have their headers suppressed. The default value is 0, i.e., PHS is off. For the Packet CS, it is expected that end-to-end header suppression/compression, and encryption will be enabled for SFs, so the 802.16 PHS will likely be limited in scope to the outer-most headers, depending on the given Packet CS Service Type.

| **Type** | **Length** | **Value** | **Scope** |
|---|---|---|---|
| | 1 | 0 = PHS is off<br>1 = PHS is on<br>default = 0 | |

### PHS Dynamic Service Change Action

When received in a Dynamic Service Change Request, this indicates the action that SHALL be taken with this payload header suppression byte string.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.26.5 | 1 | 0 — Add PHS Rule<br>1 — Set PHS Rule<br>2 — Delete PHS Rule<br>3 — Delete all PHS Rules | |

The “Set PHS Rule” command is used to add the specific TLV’s for an undefined payload header suppression rule. It SHALL NOT be used to modify existing TLV’s.

When deleting all PHS Rules any corresponding Payload Header Suppression Index SHALL be ignored. An attempt to Add a PHS Rule which already exists is an error condition.

FFS: why can’t “Add PHS Rule” be used in place of “Set PHS Rule” for undefined PHSRs?

## PHS Error Encodings

This field defines the parameters associated with Payload Header Suppression Errors.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.26.6 | n | | |

A Payload Header Suppression Error Parameter Set is defined by the following individual parameters: Errored Parameter, Confirmation Code and Error Message.

The Payload Header Suppression Error Parameter Set is returned in REG-RSP, DSA-RSP and DSC-RSP messages to indicate the recipient's response to a Payload Header Suppression Rule establishment request in a REG-REQ, DSA-REQ or DSC-REQ message.

On failure, the sender SHALL include one Payload Header Suppression Error Parameter Set for each failed Payload Header Suppression Rule requested in the REG-REQ, DSA-REQ or DSC-REQ message. Payload Header Suppression Error Parameter Set for the failed Payload Header Suppression Rule SHALL include the Confirmation Code and Errored Parameter and MAY include an Error Message. If some Payload Header Suppression Rule Sets are rejected but other Payload Header Suppression Rule Sets are accepted, then Payload Header Suppression Error Parameter Sets SHALL be included for only the rejected Payload Header Suppression Rules. On success of the entire transaction, the RSP or ACK message SHALL NOT include a Payload Header Suppression Error Parameter Set.

Multiple Payload Header Suppression Error Parameter Sets MAY appear in a REG-RSP, DSA-RSP or DSC-RSP message, since multiple Payload Header Suppression parameters may be in error. A message with even a single Payload Header Suppression Error Parameter Set SHALL NOT contain any other protocol Payload Header Suppression Encodings (e.g. IP, 802.1P/Q).

A Payload Header Suppression Error Parameter Set SHALL NOT appear in any REG-REQ, DSA-REQ or DSC-REQ messages.

### *PHS Errored Parameter*

The value of this parameter identifies the subtype of a requested Payload Header Suppression parameter in error in a rejected Payload Header Suppression request. A Payload Header Suppression Error Parameter Set SHALL have exactly one Errored Parameter TLV within a given Payload Header Suppression Encoding.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.26.6.1 | n | Payload Header Suppression Encoding Subtype in Error | |

If the length is one, then the value is the single-level subtype where the error was found, e.g. 5 indicates an invalid Change Action. If the length is two, then the value is the multi-level subtype where there error was found (there are no multi-level PHS subtypes currently defined).

### *PHS Error Code*

This parameter indicates the status of the request. A non-zero value corresponds to the Confirmation Code as described in C.4. A Payload Header Suppression Error Parameter Set SHALL have exactly one Error Code within a given Payload Header Suppression Encoding.

| Type | Length | Value | Scope |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 100.26.6.2 | 1 | Confirmation code | |

A value of okay(0) indicates that the Payload Header Suppression request was successful. Since a Payload Header Suppression Error Parameter Set only applies to errored parameters, this value SHALL NOT be used.

### *PHS Error Message*

This subtype is optional in a Payload Header Suppression Error Parameter Set. If present, it indicates a text string to be displayed on the CPE console and/or log that further describes a rejected Payload Header Suppression request. A Payload Header Suppression Error Parameter Set MAY have zero or one Error Message subtypes within a given Payload Header Suppression Encoding.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.26.6.3 | n | Zero-terminated string of ASCII characters. | |

The length n includes the terminating zero.

The entire Payload Header Suppression Encoding message SHALL have a total length of less than 256 characters.

### PHS Field (PHSF)

The value of this field are the bytes of the headers which SHALL be suppressed by the sending entity, and SHALL be restored by the receiving entity. In the upstream, the PHSF corresponds to the string of PDU bytes starting with the first byte after the MAC Header Checksum. For the downstream, the PHSF corresponds to the string of PDU bytes starting with the first byte after the MAC Header Checksum. This string of bytes is inclusive of both suppressed and unsuppressed bytes of the PDU header. The value of the unsuppressed bytes within the PHSF is implementation dependent.

The ordering of the bytes in the value field of the PHSF TLV string SHALL follow the sequence:

Upstream
MSB of PHSF value = 1st byte of PDU
2nd MSB of PHSF value = 2nd byte of PDU
...
nth byte of PHSF (LSB of PHSF value) = nth byte of PDU

Downstream
MSB of PHSF value = 1st byte of PDU
2nd MSB of PHSF value = 2nd byte of PDU
...
nth byte of PHSF (LSB of PHSF value) = nth byte of PDU

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.26.7 | n | string of bytes suppressed | |

The length n SHALL always be the same as the value for PHSS.

### PHS Index (PHSI)

The Payload Header Suppression Index (PHSI) has a value between 1 and 255 that uniquely references the suppressed byte string. The Index is unique per Service Flow in the upstream direction, and unique per CPE in the downstream direction. The upstream and downstream PHSI values are independent of each other.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.26.8 | 1 | index value | |

### PHS Mask (PHSM)

The value of this field is used to interpret the values in the Payload Header Suppression Field. It is used at both the sending and receiving entities on the link. The PHSM allows fields such as sequence numbers or checksums that vary in value to be excluded from suppression with the constant bytes around them sup-pressed.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.26.9 | 1 | bit 0:<br>0 = don't suppress first byte of the suppression field.<br>1 = suppress first byte of the suppression field<br>bit 1:<br>0 = don't suppress second byte of the suppression field<br>1 = suppress second byte of the suppression field<br>bit x:<br>0 = don't suppress (x+1) byte of the suppression field<br>1 = suppress (x+1) byte of the suppression field | |

The length n is ceiling(PHSS/8). Bit 0 is the MSB of the Value field. The value of each sequential bit in the PHSM is an attribute for the corresponding sequential byte in the PHSF.

If the bit value is a "1", the sending entity should suppress the byte, and the receiving entity should restore the byte from its cached PHSF. If the bit value is a "0", the sending entity should not suppress the byte, and the receiving entity should restore the byte by using the next byte in the packet. If this TLV is not included, the default is to suppress all bytes.

### PHS Size (PHSS)

The value of this field is the total number of bytes in the header to be suppressed and then restored in a Service Flow that uses Payload Header Suppression.

| Type | Length | Value | Scope |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 100.26.10 | 1 | number of bytes in the suppression string | |

This TLV is used when a Service Flow is being created. For all packets that get classified and assigned to a Service Flow with Payload Header Suppression enabled, suppression SHALL be performed over the specified number of bytes as indicated by the PHSS and according to the PHSM. If this TLV is not included in a.Service Flow definition, or is included with a value of 0 bytes, then Payload Header Suppression is disabled.

A non-zero value indicates Payload Header Suppression is enabled.

### PHS Verification (PHSV)

The value of this field indicates to the sending entity whether or not the packet header contents are to be verified prior to performing suppression. If PHSV is enabled, the sender SHALL compare the bytes in the packet header with the bytes in the PHSF that are to be suppressed as indicated by the PHSM.

| Type | Length | Value | Scope |
|---|---|---|---|
| 100.26.11 | 1 | 0 = verify<br>1 = don’t verify | |

If this TLV is not included, the default is to verify. Only the sender SHALL verify suppressed bytes. If verification fails, the Payload Header SHALL NOT be suppressed. (Refer to Section TBD)

### Vendor Specific PHS Parameters

This allows vendors to encode vendor-specific PHS parameters. The Vendor ID SHALL be the first TLV embedded inside Vendor Specific PHS Parameters. If the first TLV inside Vendor Specific PHS Parameters is not a Vendor ID, then the TLV SHALL be discarded. (Refer to TBD)

## MAC-CPS SAP Primitive Usage

TBD

## Appendix A : Open Issues

## IPv6 Support

IPv6 sections need to be filled in (Service Specific Sublayer, TLV Encodings).

## PHS

It will be useful to have 2 categories for Payload Header Suppression. Generic PHS, and Service-Specific PHS. Generic PHS is called as such for its multi-service applicability. Service-Specific PHS may be used in special cases for further-optimizing a specific stream of headers, where Generic PHS does not suffice. It may also be the case that Generic PHS and Service-Specific PHS might work together at some level, handling header suppression for different portions of the payload headers.

### Generic PHS

For purposes of allowing future optimization techniques, and to acknowledge implementation vs. optimization trade-offs, it will be useful to have a Generic PHS (GPHS) Capabilities TLV and a GPHS Type TLV. The GPHS Capabilities TLV, used in the registration process, would allow the BS and SS to negotiate the subset of GPHS algorithms that are supported by both the BS and SS. The GPHS Type TLV allows the BS or SS to request the specific GPHS algorithm to be used for a particular SF direction (upstream/downstream). The encoding for the GPHS Capabilities and Generic PHS Type TLVs could use the encoding technique as is used for the Service Capabilities and Service Type TLVs.

The PHS algorithm as is currently defined in this Packet CS contribution would be assigned a name (TBD) and a value (i.e. bit-position in a bit-mask). The GPHS TLVs should then have a type (i.e. by Generic PHS algorithm), and subtypes (for GPHS algorithm-specific information).

It may make sense to reserve a few Convergence Pass-Through (CPT) bits for purposes of GPHS support. The reserved bits could be reused if GPHS is disabled in the particular SF direction, or if the enabled GPHS algorithm on the particular SF doesn't use the GPHS reserved bits (or some portion therein).

### Service-Specific PHS

It is expected that no direct-support for Service-Specific PHS (SSPHS) will be included as part of the Packet CS, as Generic PHS with algorithm negotiation should suffice. SSPHS MAY be signaled via Vendor-Specific TLVs or by MAC-CPS Convergence Pass-Through (CPT) bits (which are not reserved/used by GPHS).

## MAC-CPS SAP Primitive Usage

The MAC-CPS SAP Primitive Usage section needs to be filled in.

## TLV Encoding Section

In the TLV tables, the "Type" field, and "Scope" field needs to be filled in.

## Figures

Figures from Glen Sater's Ethernet CS contribution IEEE 802.16.1c-00/18 would help to clarify the PHS section.

- Figure A.4—Payload Header Suppression Operation.
- Figure A.5—Payload Header Suppression with Masking.
- Figure A.6—Payload Header Suppression Signaling Example.
- Figure A.7—Payload Header Suppression Example.

## References

The References section needs to be filled in.