Project	**IEEE 802.16 Broadband Wireless Access Working Group**
Title	Ethernet/IEEE 802.3 Annex for the 802.16.1 Air Interface Specification
Date Submitted	2000-11-05
Source	Glen Sater Motorola Inc. 8220 E. Roosevelt Street, M/D R1106 Scottsdale, AZ 85257 Voice: 480-441-8893 Fax: 480-675-2116 E-mail: g.sater@motorola.com
Re:	802.16.1 Call for Comments: Session #10, Document 80216-00/01r1
Abstract	This document defines a convergence process for Ethernet and IEEE 802.3 bearer traffic that utilizes the core MAC functionality as currently defined in the draft air interface, document 80216-00/01r4.
Purpose	To provide the necessary text to be inserted Annex into the current draft of the standard to support Ethernet/IEEE 802.3 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. Portions of this document are reprinted with permission from Cable Television Laboratories, Inc.
IEEE Patent Policy	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures (Version 0.9) <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." 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/letters.html>.

Annex A

(normative)

Ethernet/IEEE 802.3 Convergence Sub-Layer

The Ethernet/IEEE 802.3 Convergence Layer (CL) resides on top of the 802.16 MAC layer. The CL performs the following functions, utilizing the services of the MAC layer:

a) Classificiation of the Ethernet/802.3 PDU into the appropriate Connection
b) Suppression of payload header information
c) Delivery of the resulting SDU to the M-SAP associated with the Service Flow for transport to the peer M-SAP
d) Receipt of the PDU from the peer M-SAP
e) Rebuilding of any suppressed payload header information

The CL is responsible for delivering the PDU to the appropriate M-SAP. The MAC is responsible for delivery of the PDU to peer M-SAP in accordance with the QoS, fragmentation, concatenation and other transport functions associated with a particular connection’s service flow characteristics.

A.1 MAC Service Definition

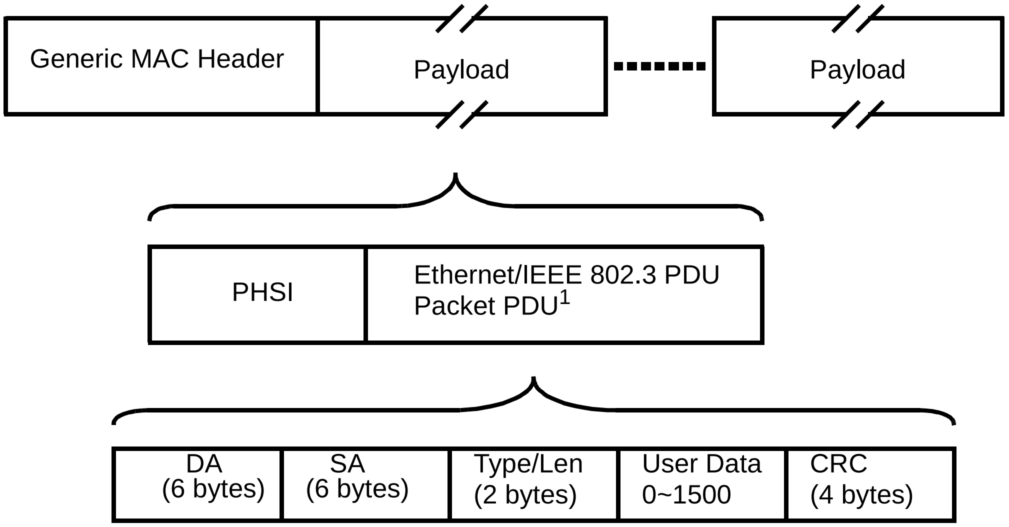
<TBD>

A.2 MAC SDU Format

Ethernet/IEEE 802.3 frames shall be encapsulated in the MAC PDU format as illustrated in Figure A.1. Each MAC PDU shall consist of the standard Generic MAC Header followed by one or more Ethernet/IEEE 802.3 Payloads. Each payload consists of an Payload Header Suppression Index (PHSI) field followed by the actual Ethernet/IEEE 802.3 frame. A value of zero in the PHSI indicates no payload header suppression has been applied to the frame. Otherwise the value is in the index identifying the rules for suppression. This index is mapped to equivalent rules at BS and SS peers to allow for re-construction of suppressed information.

The CSI bit of the Generic MAC Header shall always be set to 0 for this convergence sub-layer.

.



[1]Frame size is limited to 1518 bytes in the absence of VLAN tagging. Cooperating devices which implement IEEE 802.1Q VLAN tagging MAY use a frame size up to 1522 bytes

Figure A.1—MAC PDU Formats

A.3 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. Downstream Classifiers are applied by the BS to packets it is transmitting and Upstream Classifiers are applied at the SS. Figure A.2 and Figure A.3 illustrate the mappings discussed above.

It is possible for a packet to fail to match the set of defined classifiers. In this case, the CL may either associate the packet with a default CID or discard the packet. The action taken is vendor specific. Note that the default CID SHALL be created and managed by the CL since the specification does force the creation of such a connection for the purposes of user data transport.

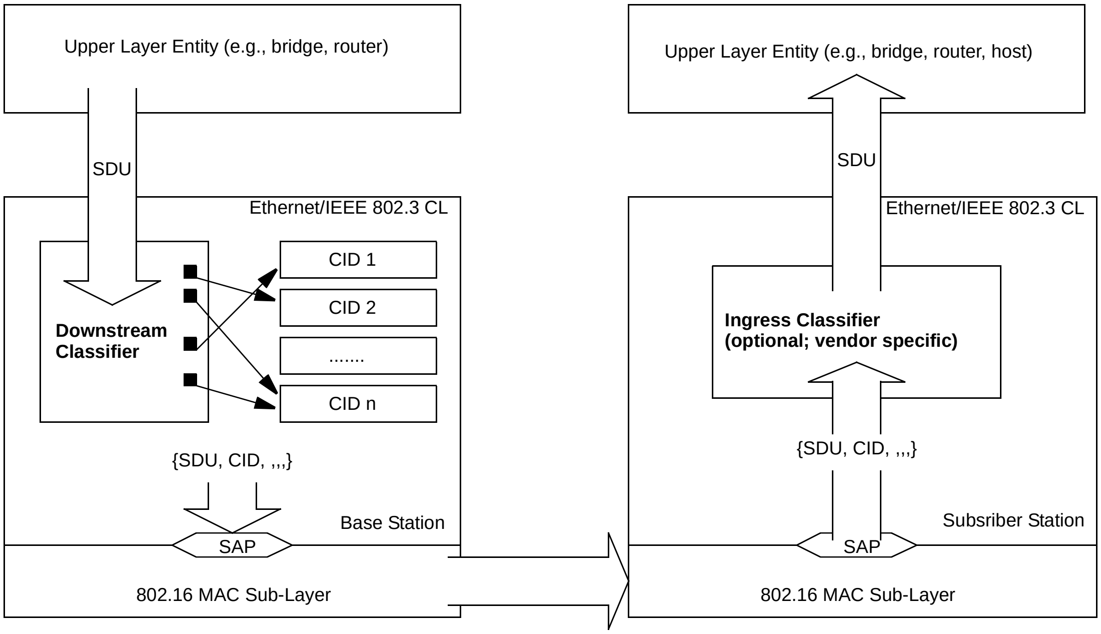


Figure A.2—Classification and CID Mapping (BS to SS)

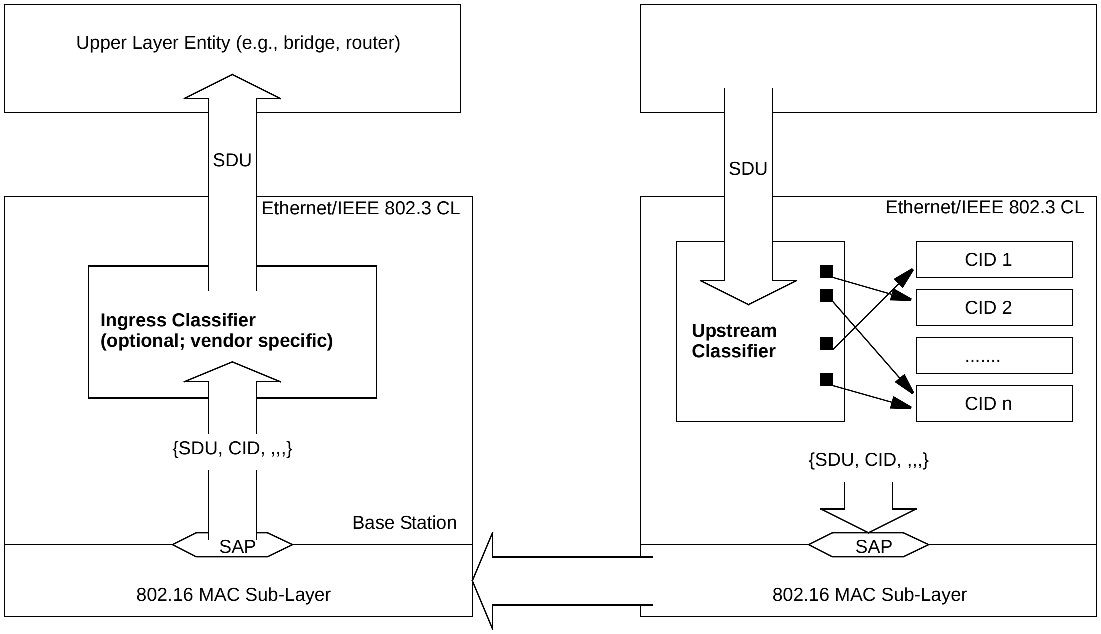


Figure A.3—Classification and CID Mapping (SS to BS)

A.3.1 Classification within the CL

SS and BS Packet Classification consists of multiple Classifiers. Each Classifier contains a priority field which determines the search order for the Classifier. The highest priority Classifier SHALL be applied first. If a Classifier is found in which all parameters match the packet, the Classifier SHALL forward the packet to the corresponding Service Flow. If no Classifier is found in which all parameters match the packet then the packet is classified to the Primary Service Flow.

The packet classification table contains the following fields:

a) Priority — determines the search order for the table. Higher priority Classifiers are searched before lower priority Classifiers.
b) IP Classification Parameters — zero or more of the IP classification parameters (IP TOS Range/ Mask, IP Protocol, IP Source Address/Mask, IP Destination Address/Mask, TCP/UDP Source Port Start, TCP/UDP Source Port End, TCP/UDP Destination Port Start, TCP/UCP Destination Port End).
c) LLC Classification Parameters — zero or more of the LLC classification parameters (Destination MAC Address, Source MAC Address, Ethertype/SAP)
d) IEEE 802.1P/Q Parameters — zero or more of the IEEE classification parameters (802.1P Priority Range, 802.1Q VLAN ID)
e) 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, BWA MAC sublayer service interface). SNMP-based operations can view Classifiers that are added via dynamic operations, but can not modify or delete Classifiers that are created by dynamic operations. The format for classification table parameters defined in the configuration file, registration message, or dynamic signaling message is contained in Section A.5.1.

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.

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 CL may also be aware of the particular Connections in the MAC Sublayer, and may have assigned the Packet directly to a Connection. In these cases, a user data Packet is considered to be directly associated with a Connection as selected by the upper layer and/or CL.

A.4 Payload Header Suppression

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 downstream examples are given. The following definitions are used:

Table A.1—Payload Header Suppression Definitions

PHS	Payload Header Suppression	Suppressing an initial byte string at the sender and restoring the byte string at the receiver.
PHS Rule	Payload Header Suppression Rule	A set of TLV's that apply to a specific PHS Index.
PHSF	Payload Header Suppression Field	A string of bytes representing the header portion of a PDU in which one or more bytes will be suppressed (i.e., a snapshot of the uncompressed PDU header inclusive of suppressed and unsuppressed bytes).
PHSI	Payload Header Suppression Index	An 8-bit value which references the suppressed byte string.
PHSM	Payload Header Suppression Mask	A bit mask which indicates which bytes in the PHSF to suppress, and which bytes to not suppress.
PHSS	Payload Header Suppression Size	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.
PHSV	Payload Header Suppression Verify	A flag which tells the sending entity to verify all bytes which are to be suppressed.

A.4.1 Overview

In Payload Header Suppression, a repetitive portion of the payload headers of the Ethernet/IEEE 802.3 SDU is suppressed by the sending entity and restored by the receiving entity. On the uplink, the sending entity is the SS and the receiving entity is the BS. On the downlink, the sending entity is the BS and the receiving entity is the SS. Each SDU is prefixed with a Payload Header Suppression Index (PHSI) which references the Payload Header Suppression Field (PHSF).

The sending entity uses Classifiers to map packets into a Service Flow. The Classifier 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 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 which change such as IP sequence numbers, and still suppressing bytes which 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 which 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.

A.4.1.1 Example Applications

a) A Classifier on an upstream 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 which identifies this VoIP media flow. For the upstream case, 42 bytes of payload header are verified and suppressed, and a 1 byte prefix containing the PHSI is added to every packet in that media flow.

b) A Classifier which 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 existence of the PHSI extended header will indicate the choice made, the simple CID/PHSI lookup at the receiving entity will always yield the correct result.

c) A Classifier on an upstream Service Flow which identifies all 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.

A.4.1.2 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 0-1 illustrates the following procedure.

A packet is submitted to the SS Ethernet/802.3 CL. The SS applies its list of Classifier rules. A match of the rule will result in an 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 SDU to the M-SAP for transport on the uplink.

When the packet is received by the BS, the BS will determine the associated CID by examination of the generic MAC header. The BS sends the PDU to the M-SAP associated with that CID. The receiving Ethernet/802.3 CL uses the CID and the PHSI to look up PHSF, PHSM, and PHSS. The BS reassembles the packet and then proceeds with normal packet processing. The reassembled 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.

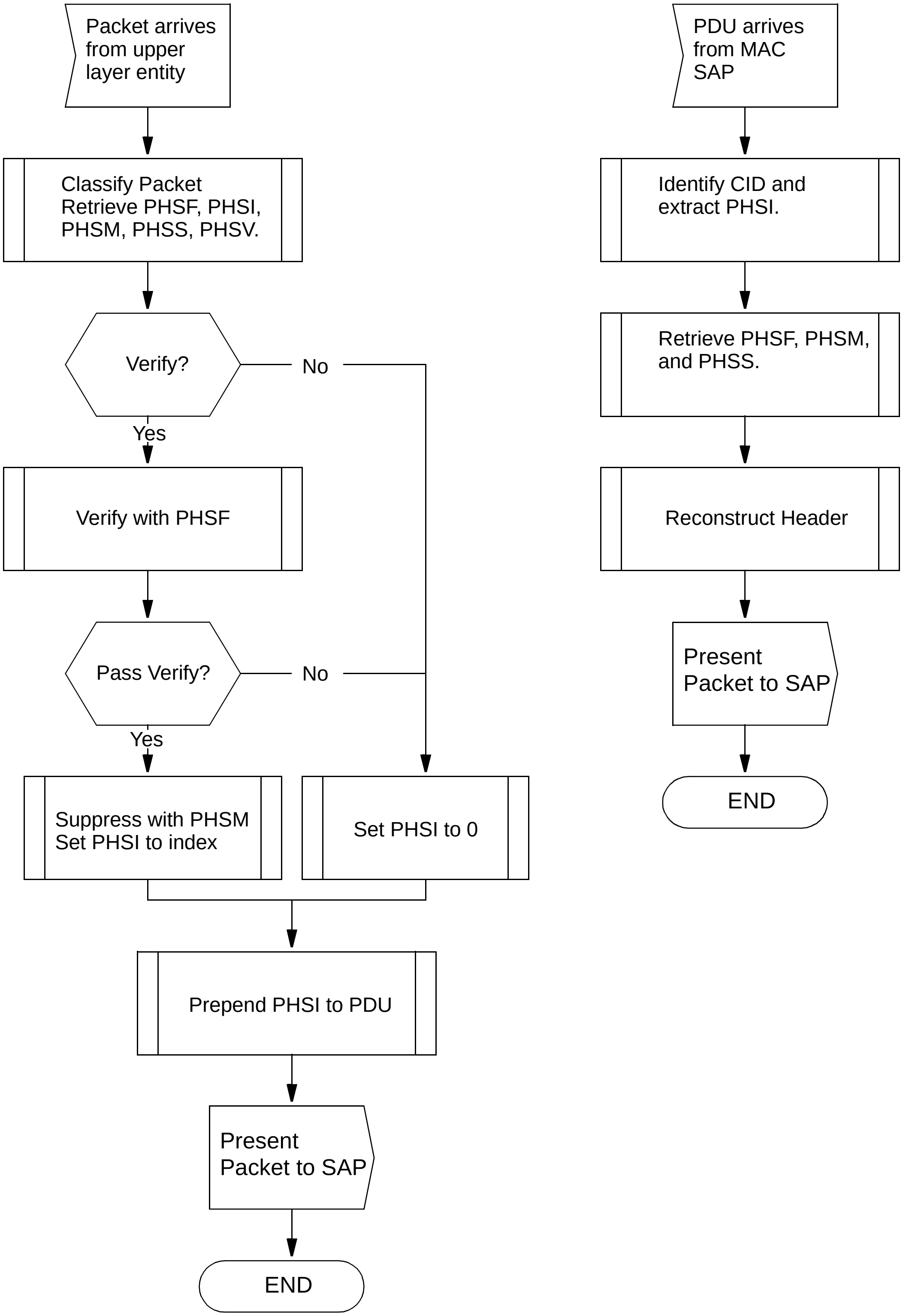

Packet arrives from upper layer entity
Classify Packet Retrieve PHSF, PHSI, PHSM, PHSS, PHSV.
Verify?
No
Yes
Verify with PHSF
Pass Verify?
No
Yes
Suppress with PHSM Set PHSI to index
Set PHSI to 0
Prepend PHSI to PDU
Present Packet to SAP
END
PDU arrives from MAC SAP
Identify CID and extract PHSI.
Retrieve PHSF, PHSM, and PHSS.
Reconstruct Header
Present Packet to SAP
END

Figure A.4—Payload Header Suppression Operation

A similar operation occurs on the downlink. The BS applies its list of Classifiers. A match of the Classifier will result in a Downstream Service Flow 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 SDU to the M-SAP for transport on the uplink.

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 CL. The CL then uses the PHSI to lookup PHSF, PHSM, and PHSS. The SS reassembles the packet and then proceeds with normal packet processing.

Figure A.5 demonstrates packet suppression and restoration when using PHS masking. Masking allows only bytes which do not change to be suppressed. Note that the PHSF and PHSS span the entire Suppression Field, included suppressed and unsuppressed bytes.

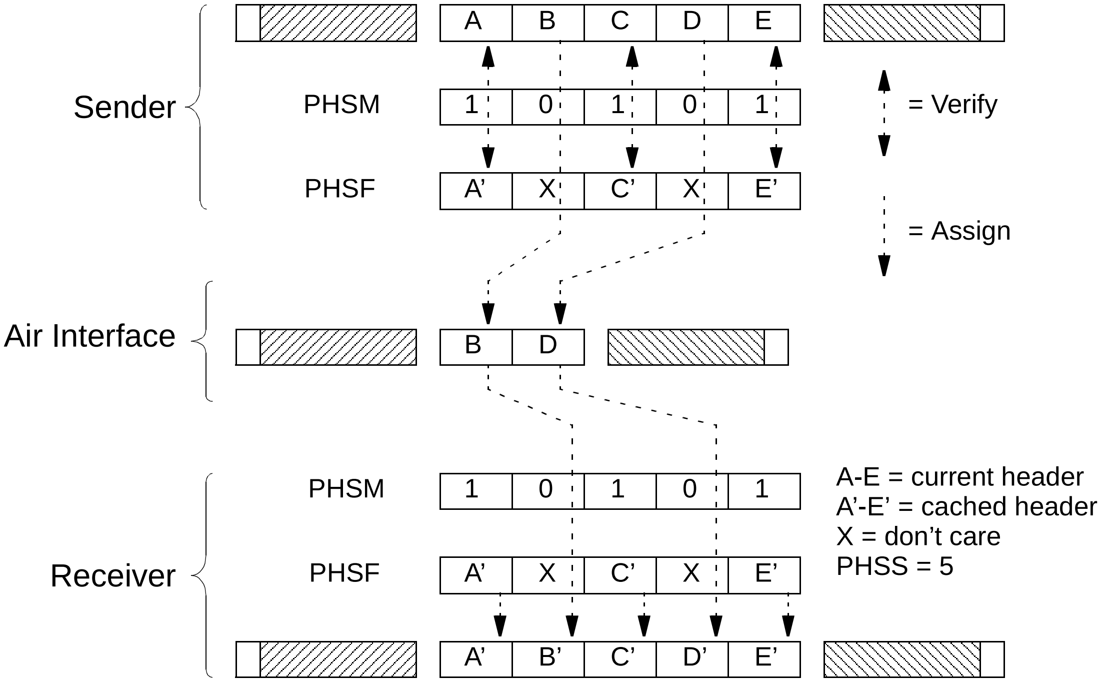


Figure A.5—Payload Header Suppression with Masking

A.4.1.3 Signaling

Payload Header Suppression requires the creation of three objects:

a) Service Flow
b) Classifier
c) 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 A.6 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 the header fields to be suppressed will be known. The values of some of the fields (e.g., 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.

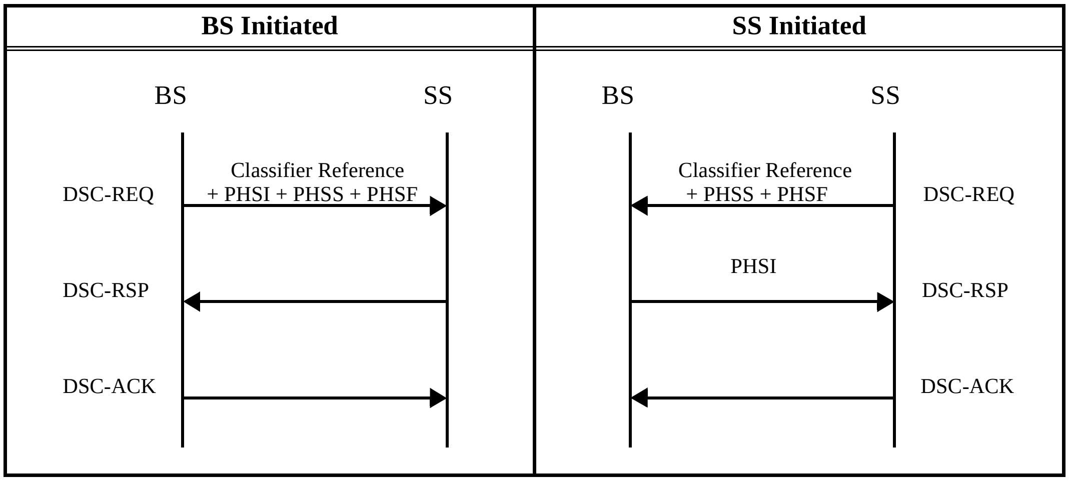
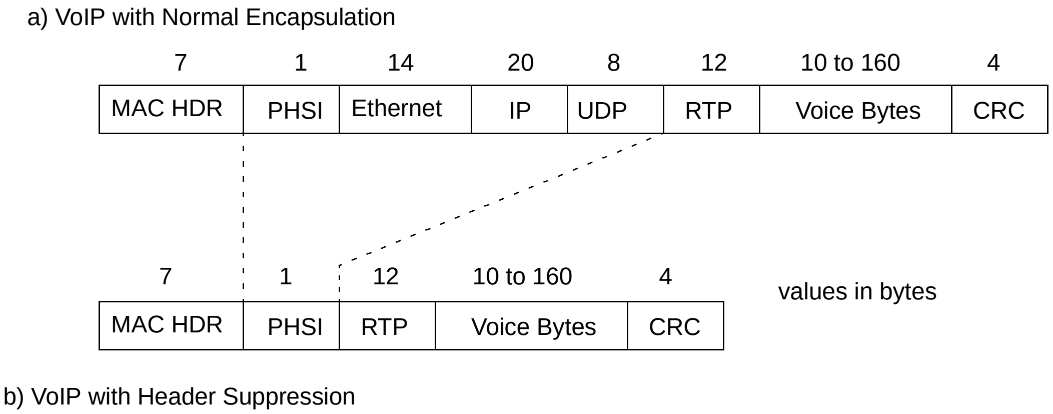


Figure A.6—Payload Header Suppression Signaling Example

A.4.1.4 Payload Header Suppression Example

A Service Class with the Service Class Name of “G711-UL-UGS-HS-42” is established which is intended for G.711 VoIP traffic on the uplink and is mapped to a service flow using UGS 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 A.7 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.



a) VoIP with Normal Encapsulation

b) VoIP with Header Suppression

Figure A.7—Payload Header Suppression Example

Figure A.7a shows a normal RTP packet carried on an upstream channel. The MAC layer overhead consists of the 7 byte generic MAC header, a PHSI field (set to 0), 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 A.7b 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.

A.5 Common Radio Frequency Interface Encodings

A.5.1 Encodings for Configuration and MAC-Layer Messaging

The following type/length/value encodings SHALL be used in both the configuration file, in SS registration requests and in Dynamic Service Messages. All Ethernet/IEEE 802.3 specific TLVs are prefixed begin with a Type value of 100. Other Type values are defined for other CLs; refer to ***<TBD: Insert cross-reference to Section 2.3.8, Convergence Sub-Layer Parameter Encodings, of document IEEE 802.16-00/01r4>***.

The following configuration settings SHALL be supported by all SSs which are compliant with this specification.

A.5.1.1 Configuration File and Registration Settings

These settings are found in the configuration file and, if present, SHALL be forwarded by the SS to the BS in its Registration Request.

A.5.1.1.1 Upstream Packet Classification Configuration Setting

This field defines the parameters associated with one entry in an upstream traffic classification list.

Type	Length	Value
100.22	n	

A.5.1.1.2 Downstream Packet Classification Configuration Setting

This field defines the parameters associated with one Classifier in an downstream traffic classification list.

Type	Length	Value
100.23	n	

A.5.1.1.3 Payload Header Suppression

This field defines the parameters associated with Payload Header Suppression.

Type	Length	Value
100.26	n	

A.5.1.1.4 Maximum Number of Classifiers

This is the maximum number of Classifiers that the SS is allowed to have active.

This is necessary when using deferred activation since the number of provisioned Service Flows may be high and since each Connection might support multiple Classifiers. Provisioning represents the set of Connections the SS can choose between, however, it may still be desirable to limit the number of simultaneously admitted Classifiers applied to this set. This parameter provides the ability to limit the size of that set.

Type	Length	Value
100.28	2	Maximum number of simultaneous admitted classifiers

The default value is 0 — no limit.

A.5.1.2 Configuration-File-Specific Settings

These settings are found in only the configuration file. They SHALL NOT be forwarded to the BS in the Registration Request.

A.5.1.3 Registration-Request/Response-Specific Encodings

These encodings are not found in the configuration file, but are included in the Registration Request. Some encodings are also used in the Registration Response.

The SS SHALL include SS Capabilities Encodings in its Registration Request. If present in the corresponding Registration Request, the BS SHALL include SS Capabilities in the Registration Response.

A.5.1.3.1 SS Capabilities Encoding

The value field describes the capabilities of a particular SS, i.e., implementation dependent limits on the particular features or number of features which the modem can support. It is composed from a number of encapsulated type/length/value fields. The encapsulated sub-types define the specific capabilities for the modem in question. Note that the sub-type fields defined are only valid within the encapsulated capabilities configuration setting string.

Type	Length	Value
100.5	n	

The set of possible encapsulated fields is described below.

A.5.1.3.1.1 Payload Header Suppression Support

If the value field is a 1 the SS requests payload header suppression support from the BS.

Type	Length	Value
100.5.4	1	1 or 0

A.5.1.3.1.2 Optional Filtering Support

The fields shows the optional filtering support in the SS.

Type	Length	Value
100.5.9	1	Packet Filtering Support Array bit #0: 802.1P filtering bit #1: 802.1Q filtering bit #2-7: reserved SHALL be set to zero

A.5.2 Quality-of-Service-Related Encodings

A.5.2.1 Packet Classification Encodings

The following type/length/value encodings SHALL be used in both the configuration file, registration messages, and Dynamic Service messages to encode parameters for packet classification and scheduling.

The following configuration settings SHALL be supported by all SSs which are compliant with this specification.

A.5.2.1.1 Upstream Packet Classification Encoding

This field defines the parameters associated with an upstream Classifier.

Note that the same subtype fields defined are valid for both the encapsulated upstream and downstream packet classification configuration setting string. These type fields are not valid in other encoding contexts.

Type	Length	Value
100.22	n	

A.5.2.1.2 Downstream Packet Classification Encoding

This field defines the parameters associated with a downstream Classifier.

Note that the same subtype fields defined are valid for both the encapsulated upstream and downstream flow classification configuration setting string. These type fields are not valid in other encoding contexts.

Type	Length	Value
100.23	n	

A.5.2.1.3 General Packet Classifier Encodings

A.5.2.1.3.1 Classifier Reference

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

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

A.5.2.1.3.2 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 Packet Classifier Identifier.

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

A.5.2.1.3.3 Service Flow Reference

The value of the field specifies a Service Flow Reference that identifies the corresponding Service Flow.

In all Packet Classifier TLVs that occur in any message where the Service Flow ID is not known (e.g. CPE-initiated DSA-REQ and REG-REQ) this TLV SHALL be included. In all Packet Classifier TLVs that occur in a DSC-REQ and BS-initiated DSA-REQ messages the Service Flow Reference SHALL NOT be specified.

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

A.5.2.1.3.4 Service Flow Identifier

The value of this field specifies the Service Flow ID that identifies the corresponding Service Flow.

In Packet Classifier TLVs where the Service Flow ID is not known, and this TLV SHALL NOT be included (e.g. CPE-initiated DSA-REQ and REG-REQ). In Packet Classifier TLVs that occur in a DSC-REQ and BS-initiated DSA-REQ message, the Service Flow ID SHALL be specified.

Type	Length	Value
[22/23].4	4	1 - 4,294,967,295

A.5.2.1.3.5 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.

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.

Type	Length	Value
100.[22/23].5	1	

A.5.2.1.3.6 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
100.[22/23].6	1	0 — Inactive 1 — Active

The default value is 1 — activate the classifier.

A.5.2.1.3.7 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
100.[22/23].7	1	0 — DSC Add Classifier 1 — DSC Replace Classifier 2 — DSC Delete Classifier

A.5.2.1.3.8 Classifier Error Encodings

This field defines the parameters associated with Classifier Errors.

Type	Length	Value
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.

A.5.2.1.3.9 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.

Subtype	Length	Value
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 e.g. 9-2 indicates an invalid IP Protocol value.

A.5.2.1.3.10 Error Code

This parameter indicates the status of the request. A non-zero value corresponds to the Confirmation Code as described in ***<TBD: Insert cross-reference to Section <TBD>, of document IEEE 802.16-00/01r4>***. A Classifier Error Parameter Set SHALL have exactly one Error Code within a given Classifier Encoding.

Subtype	Length	Value
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.

A.5.2.1.3.11 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.

SubType	Length	Value
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.

A.5.2.1.4 IP Packet Classification Encodings

This field defines the parameters associated with IP packet classification.

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

A.5.2.1.4.1 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
100.[22/23].9.1	3	tos-low, tos-high, tos-mask

A.5.2.1.4.2 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
100.[22/23].9.2	2	prot1, prot2

Valid Range
0 — 257

A.5.2.1.4.3 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 A.5.2.1.4.4. If this parameter is omitted, then comparison of the IP packet source address for this entry is irrelevant.

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

A.5.2.1.4.4 IP Source Mask

The value of the field specifies the mask value for the IP source address, as described in Section A.5.2.1.4.3. If this parameter is omitted, then the default IP source mask is 255.255.255.255.

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

A.5.2.1.4.5 IP Destination Address

The value of the field specifies the matching value for the IP destination address. An IP packet with IP destination 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
100.[22/23].9.5	4	dst1, dst2, dst3, dst4

A.5.2.1.4.6 IP Destination Mask

The value of the field specifies the mask value for the IP destination address, as described in Section A.5.2.1.4.5. If this parameter is omitted, then the default IP destination mask is 255.255.255.255.

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

A.5.2.1.4.7 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
100.[22/23].9.7	2	sportlow1, sportlow2

A.5.2.1.4.8 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
100.[22/23].9.8	2	sporthigh1, sporthigh2

A.5.2.1.4.9 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
100.[22/23].9.9	2	dportlow1, dportlow2

A.5.2.1.4.10 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
100.[22/23].9.10	2	dporthigh1, dporthigh2

A.5.2.1.5 Ethernet LLC Packet Classification Encodings

This field defines the parameters associated with Ethernet LLC packet classification.

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

A.5.2.1.5.1 Destination MAC Address

The values of the field specifies the matching parameters for the MAC destination address. An Ethernet packet with MAC destination address “etherdst” matches this parameter if dst = (etherdst AND msk). If this parameter is omitted, then comparison of the Ethernet MAC destination address for this entry is irrelevant.

Type	Length	Value
100.[22/23].10.1	12	dst1, dst2, dst3, dst4, dst5, dst6, msk1, msk2, msk3, msk4, msk5, msk6

A.5.2.1.5.2 Source MAC Address

The value of the field specifies the matching value for the MAC source address. If this parameter is omitted, then comparison of the Ethernet MAC source address for this entry is irrelevant.

Type	Length	Value
100.[22/23].10.2	6	src1, src2, src3, src4, src5, src6

A.5.2.1.5.3 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
100.[22/23].10.3	3	type, eprot1, eprot2

A.5.2.1.6 IEEE 802.1P/Q Packet Classification Encodings

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

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

A.5.2.1.6.1 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
100.[22/23].11.1	2	pri-low, pri-high

Valid Range
0 — 7 for pri-low and pri-high

A.5.2.1.6.2 IEEE 802.1Q VLAN_ID

The value of the field specify 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
100.[22/23].11.2	2	vlan_id1, vlan_id2

A.5.2.1.6.3 Vendor Specific Classifier Parameters

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 A.5.1.1.7)

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

A.5.2.1.7 Upstream-Specific Classification Encodings

A.5.2.1.7.1 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
100.22.12	1	1 — Activate/Deactivate Classifier on Request 2 — Activate/Deactivate Classifier on Ack

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 which are changed by this DSC exchange.

The default value is 2 for a bandwidth increase. The default value is 1 for a bandwidth decrease. If increase or decrease is ambiguous, then the default value is 2.

A.5.2.2 Service Flow Encodings

The following type/length/value encodings SHALL be used in the configuration file, registration messages, and Dynamic Service messages to encode parameters for Service Flows.

The following configuration settings SHALL be supported by all SSs which are compliant with this specification.

A.5.2.2.1 Payload Header Suppression

This field defines the parameters associated with Payload Header Suppression.

Type	Length	Value
100.26	n	

Note: The entire Payload Header Suppression TLV SHALL have a length of less than 255 characters.

A.5.2.2.1.1 Classifier Reference

The value of the field specifies a Classifier Reference that identifies the corresponding Classifier. (Refer to A.5.2.1.3.1)

Type	Length	Value
100.26.1	1	1 - 255

A.5.2.2.1.2 Classifier Identifier

The value of the field specifies a Classifier Identifier that identifies the corresponding Classifier. (Refer to A.5.2.1.3.2)

Type	Length	Value
100.26.2	2	1 - 65535

A.5.2.2.1.3 Service Flow Reference

The value of the field specifies a Service Flow Reference that identifies the corresponding Service Flow. (Refer to 0.0.0.3.1)

Type	Length	Value
100.26.3	2	1 - 65535

A.5.2.2.1.4 Service Flow Identifier

The value of the field specifies a Service Flow Identifier that identifies the corresponding Service Flow. All downstream PHS Rules SHALL use the Service Flow Identifier of the Primary Downstream Service Flow. (Refer to 0.0.0.3.2)

Type	Length	Value
100.26.4	4	1 - 4,294,967,295

A.5.2.2.1.5 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
100.26.5	1	0 — Add PHS Rule 1 — Set PHS Rule 2 — Delete PHS Rule 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.

A.5.2.2.2 Payload Header Suppression Error Encodings

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

Type	Length	Value
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.

A.5.2.2.2.1 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.

Subtype	Length	Value
100.26.6.1	1	Payload Header Suppression Encoding Subtype in Error

A.5.2.2.2.2 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.

Subtype	Length	Value
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.

A.5.2.2.2.3 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.

SubType	Length	Value
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.

A.5.2.2.3 Payload Header Suppression Rule Encodings

A.5.2.2.3.1 Payload Header Suppression 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 13th 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 implentation 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 = 13th byte of PDU

2nd MSB of PHSF value = 14th byte of PDU
...
nth byte of PHSF (LSB of PHSF value) = (n+13)th byte of PDU

Type	Length	Value
100.26.7	n	string of bytes suppressed

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

A.5.2.2.3.2 Payload Header Suppression Index (PHSI)

The Payload Header Suppression Index (PHSI) has a value between 1 and 255 which 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
100.26.8	1	index value

A.5.2.2.3.3 Payload Header Suppression 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 which vary in value to be excluded from suppression with the constant bytes around them suppressed.

Type	Length	Value
100.26.9	n	bit 0: 0 = don’t suppress first byte of the suppression field 1 = suppress first byte of the suppression field bit 1: 0 = don’t suppress second byte of the suppression field 1 = suppress second byte of the suppression field bit x: 0 = don’t suppress (x+1) byte of the suppression field 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.

A.5.2.2.3.4 Payload Header Suppression 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
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 which 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.

A.5.2.2.3.5 Payload Header Suppression 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
100.26.11	1	0 = verify 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 5.3.7.3)

A.5.2.2.3.6 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 SHALLss be discarded. (Refer to A.5.1.1.7)

Type	Length	Value
100.26.43	n	