Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Comment Resolution Details**	
Date Submitted	**2001-09-13**	
Source(s)	Carl Eklund	Voice: +348504836566
	Nokia Research Center	Fax:+358718036851
	P.O.BOX 407	mailto:carl.eklund@nokia.com
	FIN-00045 Nokia Group, Finland	
Re:	IEEE Sponsor Ballot of IEEE P802.16/D4-2001	
Abstract	Adds specific detail to comment resolutions	
Purpose	For use in conjunction with comment resolution database	
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 material 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." 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>.	

This document replaces page 343 line 38 to page 356 line 57

0.0.0.0.1 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
[24/25].100.6	1	0 — DSC Add Classifier 1 — DSC Replace Classifier 2 — DSC Delete Classifier

0.0.0.0.2 Classifier Error Parameter Set

This field defines the parameters associated with Classifier Errors.

Type	Length	Value
[24/25].100.8	*n*	Compound

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

The Classifier Error Parameter Set is returned in DSA-RSP and DSC-RSP messages to indicate the recipient's response to a Classifier establishment request in a DSA-REQ or DSC-REQ message.

On failure, the sender shall include one Classifier Error Parameter Set for each failed Classifier requested in the DSA-REQ or DSC-REQ message. Classifier Error Parameter Set for the failed Classifier shall include the Error 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 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 DSA-REQ or DSC-REQ messages.

0.0.0.0.2.1 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
[24/25].100.8.1	*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.

0.0.0.0.2.2 Error Code

This parameter indicates the status of the request. A non-zero value corresponds to the Confirmation Code as described in 11.4.11. A Classifier Error Parameter Set shall have exactly one Error Code within a given Classifier Encoding

Subtype	Length	Value
[24/25].100.8.2	1	Confirmation code except okay (0)

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.

0.0.0.0.2.3 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
[24/25].100.8.3	*n*	Zero-terminated string of ASCII characters

Note: The length *n* includes the terminating zero.

0.0.0.0.3 Packet Classification Rule

This compund parameter contains the parameters of the classification rule. All parameters pertaining to a specific classification rule shall be included in the same Packet Classification Rule compound parameter.

Type	Length	Value
[24/25].100.9	*n*	Compound

0.0.0.0.3.1 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.

Classifiers may have priorities in the range 0 - 255 with the default value being 0.

Type	Length	Value
[24/25].100.9.1	1	1 — 65535

0.0.0.0.3.2 IP Type of Service/DSCP Range and Mask

The values of the field specify the matching parameters for the IP ToS/DSCP 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
[24/25].100.9.2	3	tos-low, tos-high, tos-mask

0.0.0.0.3.3 Protocol

The value of the field specifies a list of matching values for the IP Protocol field. For IPv6 [RFC 2460] this refers to next header entry in the last header of the IP header chain. The encoding of the value field is that defined by IANA in [IANA]. If this parameter is omitted, then comparison of the IP header Protocol field for this entry is irrelevant.

Type	Length	Value
[24/25].100.9.3	n	prot1, prot2,...prot n

0.0.0.0.3.4 IP Masked Source Address

The value of the field specifies a list of IP source address, address mask pairs. An IP packet with IP source address “ip-src” matches this parameter if src = (ip-src AND smask). If this parameter is omitted, then comparison of the IP packet source address for this entry is irrelevant.

Type	Length	Value
[24/25].100.9.4	n* 8 (IPv4) or n*32 (IPv6)	src 1, smask 1, ..., src n, smask n

0.0.0.0.3.5 IP Destination Address

The value of the field specifies a list of IP destination address, address mask pairs. An IP packet with IP destination address “ip-dst” matches this parameter if dst = (ip-dst AND dmask). If this parameter is omitted, then comparison of the IP packet destination address for this entry is irrelevant.

Type	Length	Value
[24/25].100.9.5	n* 8 (IPv4) or n*32 (IPv6	dst 1, dmask 1, ..., dst n, dmask n

0.0.0.0.3.6 Protocol Source Port Range

The value of the field specifies a list of non-overlapping ranges of protocol source port values. Classifier rules with port numbers are protocol specific i.e. a rule on port numbers without a protocol specification must not be defined. An IP packet with protocol port value “src-port” matches this parameter if sportlow <= src-port <= sporthigh. If this parameter is omitted the protocol sourceport is irrelevant. This parameter is irrelevant for protocols without port numbers.

Type	Length	Value
[24/25].100.9.6	n*4	sportlow 1, sporthigh2,...,sportlow n, sporthigh n

0.0.0.0.3.7 Protocol Destination Port Range

The value of the field specifies a list of non-overlapping ranges of protocol destination port values. Classifier rules with port numbers are protocol specific i.e. a rule on port numbers without a protocol specification shall not be defined. An IP packet with protocol port value “dst-port” matches this parameter if dportlow <=

dst-port <=dporthigh. If this parameter is omitted the protocol destination port is irrelevant. This parameter is irrelevant for protocols without port numbers.

Type	Length	Value
[24/25].100.9.7	n*4	dportlow 1, dporthigh2,...,dportlow n, dporthigh n

0.0.0.0.3.8 Ethernet Destination MAC Address

The values of the field specifies a list of matching destination MAC address, adress mask pairs. An Ethernet packet with destination MAC address "etherdst" matches this parameter if dst = (etherdst AND msk). If this parameter is omitted, then comparison of the Ethernet destination MAC address for this entry is irrelevant.

Type	Length	Value
[24/25].100.9.8	n*12	dst 1, msk 1, ... , dst n, msk n

0.0.0.0.3.9 Ethernet source MAC Address

The values of the field specifies a list of matching source MAC address, adress mask pairs. An Ethernet packet with source MAC address "etherdst" matches this parameter if dst = (etherdst AND msk). If this parameter is omitted, then comparison of the Ethernet source MAC address for this entry is irrelevant.

Type	Length	Value
[24/25].100.9.9	n*12	src 1, msk 1, ... , src n, msk n

0.0.0.0.3.10 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 SDUs 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 SDUs using the IEEE 802.2 encapsulation format [IEEE802.2] 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 SDU 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
[24/25].100.9.10	3	type, eprot1, eprot2

0.0.0.0.3.11 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 an 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
[24/25].100.9.11	2	pri-low, pri-high Valid Range: 0 — 7 for pri-low and pri-high

0.0.0.0.3.12 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. leftmost) 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 an 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
[24/25].100.9.12	2	vlan_id1, vlan_id2

0.0.0.0.3.13 Associated Payload Header Suppression Index

The Associated Payload Suppression Index has a value between 1 and 255 which shall mirror the PHSI value of a payload header suppression rule. Packets matching the Packet Classification Rule containing the Associated Payload Header Suppression Index parameter shall undergo PHS according to the corresponding PHS rule.

Type	Length	Value
[24/25].100.9.13	1	index value

0.0.0.0.3.14 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 11.4.10).

Type	Length	Value
[24/25].100.9.255	*n*	

0.0.0.0.3.15 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
[24/25].100.10	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.

0.0.0.0.3.16 Payload Header Suppression Error Parameter Set

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

Type	Length	Value
[24/25].100.11	*n*	compound field

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

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

0.0.0.0.3.17 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
[24/25].100.11.1	1	Payload Header Suppression Encoding Subtype in Error

0.0.0.0.3.18 Error Code

This parameter indicates the status of the request. A non-zero value corresponds to the Confirmation Code as described in 11.4.11. A Payload Header Suppression Error Parameter Set shall have exactly one Error Code within a given Payload Header Suppression Encoding.

Type	Length	Value
[24/25].100.11.2	1	Confirmation code except okay(0)

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.

0.0.0.0.3.19 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 SS 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
[24/25].100.11.3	*n*	Zero-terminated string of ASCII characters

The length *n* includes the terminating zero.

0.0.0.0.4 Payload Header Suppression Rule

This field defines the parameters associated with a Payload Header Suppression Rule.

Type	Length	Value
[24/25].100.12	*n*	

0.0.0.0.4.1 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. The uplink and downlink PHSI values are independent of each other.

Type	Length	Value
[24/25].100.12.1	1	index value

0.0.0.0.4.2 Payload Header Suppression Field (PHSF)

The PHSF is string of bytes containing the header information to be suppressed by the sending CL and reconstructed by the receiving CL. The MSB of the string corresponds to first byte of the CL-SDU.

Type	Length	Value
[24/25].100.12.2	*n*	string of bytes suppressed

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

0.0.0.0.4.3 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
[24/25].100.12.3	*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 I 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.

0.0.0.0.4.4 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
[24/25].100.12.4	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.

0.0.0.0.4.5 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
[24/25].100.12.5	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.

0.0.0.0.4.6 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 shall be discarded.

Type	Length	Value
[24/25].100.12.255	*n*	