Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**ROHC Classification Changes**
Date Submitted	**2008-01-24**
Source(s)	Muthaiah Venkatachalam Intel Corp. Phillip Barber Huawei Technologies Co.	E-mail: muthaiah.venkatachalam@intel.com pbarber@huawei.com
Re:	P802.16Rev2/D2, LB26a
Abstract	The current IEEE 802.16 REV2/D2 draft includes a revised method for conducting classification of Protocol SDUs that include ROHC headers. This revised method was introduced as part of the uncompleted Corrigenda process and attempts to make ROHC classification outside the scope of the 802.16 standard. While the motivation for this revised method is to some degree understandable, it has several flaws that are addressed in this contribution.
Purpose	Adoption toward REV2/D3
Notice	*This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups*. It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who 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	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.

Title of Contribution

Muthaiah Venkatachalam and Phillip Barber
Intel Corp. and Huawei Technologies Co.

Problem:

The current IEEE 802.16 REV2/D1 draft includes a revised method for conducting classification of Protocol SDUs that include ROHC headers. This revised method was introduced as part of the uncompleted Corrigenda process and attempts to make ROHC classification outside the scope of the 802.16 standard.

While the motivation for this revised method is to some degree understandable, it has several flaws including:

- the remedy was incomplete; did not modify all locations in the standard to consistently apply the remedy

- the objective of the revised method was to move the classification out of the 802.16 MAC; this is somewhat understandable in that ROHC removes most if not all of the usual identifying elements in a Protocol SDU header normally used for packet classification in the 802.16 MAC CS; but it is problematic in that it requires separate treatment of Protocol SDUs at ingress into the CS_SAP, requiring that Protocol SDUs that include ROHC headers NOT be classified by an 802.16 mechanism, requiring the Service API for the CS_SAP to inspect the headers and direct them away from the CS_SAP (in an undefined manner) and ingress into the 802.16 MAC (again in an undefined manor); it is not useful to have Protocol SDU ingress into the 802.16 protocol stack undefined.

Remedy 1:

Modify the language of section 5.2.7.1 & 5.2.7.2 for classification of Protocol SDUs that include ROHC headers to provide a method to do classification within the 802.16 MAC CS using a method similar to that used by GPCS, that is by use of a classification method outside the 802.16 standard but integrated into the 802.16 MAC CS through use of an indexing method.

In P802.16REV2/D2, page 38, line 53, modify the text as:

5.2.7 IP-header-compression-specific part

The CS supports SDUs in two formats that facilitate robust compression of IP and higher layer headers. These formats are ROHC (RFC 3095) and ECRTP (RFC 3545) and are referred to as the Compressed-IP-header~~IP-header compression~~ CS PDU formats.

5.2.7.1 Compressed-IP-header CS PDU

The formats of the compressed-IP-header CS PDU are mapped to ~~MSDU~~MAC SDUs according to Figure 19~~21~~ (when header suppression is enabled at the connection, but not applied to the CS PDU) or Figure 20~~22~~ (with header suppression on the uncompressed Ethernet portion of an IP-over-802.3/Ethernet PDU). In the case where PHS is not enabled, PHSI field shall be omitted.

PHSI = 0	IEEE 802.3/Ethernet PDU with COMPRESSED-IP-Header ~~+ payload~~ or IP Packet (including header) with COMPRESSED-IP-Header

Figure 19~~21~~— IEEE 802.3/Ethernet CS PDU format, with IP-over-802.3Ethernet, or IP CS PDU format with compressed-IP-header and without header suppression

PHSI! = 0	Header-Suppressed IEEE 802.3/Ethernet PDU with COMPRESSED-IP-Header + payload

Figure 2022—IEEE 802.3/EthernetIP CS PDU format, with IP-over-802.3/Ethernet, with both compressed-IP-header and Ethernet header part header suppression

5.2.7.2 Compressed-IP-header classification rules

The term 'ROHC channel' is defined in RFC3095 and further clarified in RFC3759. The 802.16 standard does not attempt to redefine the definition of 'ROHC Channel'.

A single ROHC channel, which may have multiple ROHC contexts, shall have a one-to-one mapping to a single service Flow flow (SFID). Since there is a one-one mapping between a ROHC channel and an SF ID, there is no need to have any additional classifiers associated with that Service Flow. The method of associating a ROHC channel with a Service Flow is left to the implementation. One or more ROHC channels can be established for an SS.

ROHC classification is the classification of MAC SDUs that include ROHC headers. For ROHC classification purposes, relevant ROHC headers include only ROHC headers that compress portions of an IP header, which may include an IP header as part of IP-over-802.3/Ethernet, where such compression would make all or part of the IP header unusable for IP CS or IEEE 802.3/Ethernet CS classification purposes. ROHC classification shall be done on MAC SDUs only when ingressing via the ROHC_SAP.

ROHC classification uses the SS MAC Address and SFID parameters presented as part of the ROHC primitive to directly and uniquely map the data packets to the service flow. The method of upper layer application assignment of the SS MAC Address and SFID to the data packet is outside the scope of this standard.

For a service flow mapped to a ROHC Channel, the ROHC parameters associated with the ROHC Channel and used in the upper ROHC compression layer to configure the service shall be negotiated by including the ROHC Parameter Payload TLV (11.13.38) in the DSx-REQ/RSP messages.

In order to facilitate higher layer classification of data packets to assign the ROHC classification index, when the service to be carried over the ROHC CS identified service flow is IP-over-Ethernet or IP then the service flow encodings transmitted to create the flow should include those IP specific classification parameters (11.13.19.3.4.2 through 11.13.19.3.4.7, and 11.13.19.3.4.16) necessary to assist the higher layer application in formulating classification rules.
For a Service Flow mapped to a ROHC Channel, the ROHC parameters associated with the ROHC Channel shall be negotiated by including the ROHC Parameter Payload TLV (11.13.38) in the DSA-REQ/RSP messages (for a new Service Flow creation) or the DSC-REQ/RSP messages (for an existing Service Flow).

5.2.7.3 ROHC SAP parameters

ROHC classification uses the ROHC_SAP, an instance of the logical CS SAP. The ROHC_SAP parameters enable the upper layer protocols to generically pass information to the ROHC classifier so that ROHC classification does not need to interpret upper layer protocol headers in order to map the upper layer data packets into proper 802.16 MAC connections.
Since the SAP parameters are explicit, the parsing portion of the classification process is the responsibility of the upper layer. The parameters relevant for the ROHC_SAP data path primitive ROHC_DATA.request are described in sections 5.2.7.3.1.

Service flow ID (SFID)

Unique identifier to identify a unidirectional service flow for an SS. The higher layer application shall map the combination of SFID and SS MAC Address directly to a MAC connection ID. During connection/service flow establishment, the 802.16 control plane function shall provide the higher layer application the mapping information.
SS MAC Address:
48-bit unique identifier used by SS.
LENGTH:
Number of bytes in DATA.
DATA:
The payload delivered by the upper layer to the ROHC classification, or by the ROHC classification to the upper layer.

5.2.7.3.1 ROHC_DATA.request
Function:
This primitive defines the transfer of data from the upper layer to the ROHC_CS.
Semantics of the service primitive:
The parameters of the primitive are as follows:

ROHC_DATA.request
(

Service Flow ID,
SS MAC Address
length,
data

)
The parameters Service Flow ID, SS MAC Address, length, and data are described in section 5.2.7.3.
When generated:
This primitive is generated by an upper layer protocol when a protocol SDU requiring ROHC classification is to be transferred to a peer entity or entities.
Effect of receipt:
The receipt of this primitive causes ROHC classification to map the Service Flow ID and SS MAC Address to a unidirectional service flow and a connection. ROHC classification invokes MAC functions, for example the MAC SAP (an example MAC SAP definition is provided in Annex C) to effect transfer of the SDU to the MAC layer.

Remedy 2:

Modify the language of section 5.2.3.1 to clarify that PHS still operates even in the presence of compression of the IP header so long as no part of the PHSF is being compressed.

In P802.16REV2/D2, page 33, line 38, modify the text as:
5.2.3.1 PHS operation
SS and BS implementations are free to implement PHS in any manner as long as the protocol specified in this subclause is followed. Figure 12 illustrates the following procedure.

A packet is submitted to the packet CS. The SS applies its list of classification rules. A match of the rule shall result in an UL service flow and CID and may result in a PHS Rule. The PHS Rule provides PHSF, PHSI, PHSM, PHSS, and PHSV. If PHSV is set or not present, the SS shall 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 shall suppress all the bytes in the UL PHSF except the bytes masked by PHSM. The SS shall then prefix the PDU

with the PHSI and present the entire ~~MSDU~~MAC SDU to the MAC SAP for transport on the UL.

When the MAC protocol data unit (MPDU) is received by the BS from the air interface, the BS MAC shall determine the associated CID by examination of the generic MAC header. The BS MAC sends the PDU to the MAC SAP associated with that CID. The receiving packet CS 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 contains bytes from the PHSF. If verification was enabled, then the PHSF bytes equal the original header bytes. If verification was not enabled, then there is no guarantee that the PHSF bytes match the original header bytes.

A similar operation occurs on the DL. The BS applies its list of Classifiers classification rules. A match of the classification shall result in a DL 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 shall verify the Downlink Suppression field in the packet with the PHSF. If they match, the BS shall suppress all the bytes in the Downlink Suppression field except the bytes masked by PHSM. The BS shall then prefix the PDU with the PHSI and present the entire MAC SDU~~MSDU~~ to the MAC SAP for transport on the DL.

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

PHS shall be disabled/made inactive for a packet, and PHSI for the MAC SDU shall be set to zero if any portion of the IP header being used for classification (not including IP-over-IEEE 802.3/Ethernet) is being compressed by an upper layer header compression service such as ROHC or ECRTP. PHS may only be active to suppress the Ethernet portion of the header in a packet with an IP-over-IEEE 802.3/Ethernet header when any portion of the IP part of the header is being compressed by a higher layer compression service.

Figure 13 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.

Remedy 3:
Modify the language of section 11.13.19.1 to disambiguate the CS used by the service flow, and to introduce 'Compressed-IP-header CS' CS use as defined in 5.2.7.

In P802.16REV2/D2, page 1166, line 3, modify as:
11.13.19.1 CS Specification parameter
This parameter specifies the CS that the connection being set up shall use. The CS specified by this parameter implicitly defines the classification method used for this service flow.

Type	Length	Value	Scope
[145/146].28	1	0: GPCS (Generic Packet Convergence Sublayer) 1: Packet, IPv4 (IP CS) 2: Packet, IPv6 (IP CS) 3: Packet, IEEE 802.3/Ethernet CS 4: *Reserved* 5: Packet, IPv4 over IEEE 802.3/Ethernet[a]	DSA-REQ

| | | (IEEE 802.3/Ethernet CS)
6: Packet, IPv6 over IEEE 802.3/Ethernet[a] (IEEE 802.3/Ethernet CS)
7: *Reserved*
8: *Reserved*
9: ATM
10: Packet, IEEE 802.3/Ethernet[a] with ROHC header compression (Compressed-IP-header CS)
11: Packet, IEEE 802.3/Ethernet[a] with ECRTP header compression (Compressed-IP-header CS)
12: Packet, IP[b] with ROHC header compression (Compressed-IP-header CS)
13: Packet, IP[b] with ECRTP header compression (Compressed-IP-header CS)
14: Packet, IP CS[b]
15–255 *Reserved* | |

[a]Classifiers for IEEE 802.1Q VLAN tags may be applied to service flows of this CS type.
[b]SDUs for service flows of this CS type may carry either IPv4 or IPv6 in the header-compressed payload.

Remedy 4:

Modify the language to increase clarity of usage. Specify that the payload data is used by ROHC for configuration parameter transfer through lower layer.

In P802.16REV2/D2, page 1184, line 13, modify as:

11.13.38 ROHC Parameter Payload

This attribute contains the payload used in the upper ROHC compression layer to configure the service. The MAC layer does not interpret this attribute.

Type	Length	Value	Scope
[145/146].47	*variable*	ROHC Parameter Payload	DSA-REQ, DSA-RSP DSC-REQ, DSC-RSP