Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Proposal for IP convergence sub-layer**
Date Submitted	**2000-10-30**
Source(s)	Carl Eklund Nokia P.O. Box 407 FIN-00045 Nokia Group Voice: +358943761 Fax: +358943766851 mailto:carl.eklund@nokia.com
Re:	Specific open issues
Abstract	The IP convergence layer maps IP packets on MAC connections
Purpose	
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." 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>.

Scope

This document defines a Service Specific Convergence Sublayer (SSCS) layer for transporting Internet Protocol (IP) version 4 and 6 packets over an IEEE 802.16 air interface.

References

RFC792 Transmission Control Protocol
RFC Internet Protocol
RFC768 User Datagram protocol
RFC2469 Internet Protocol v6
http://www.isi.edu/in-notes/iana/assignments/protocol-numbers

Overview

The IP convergence resides on top of 802.16 MAC layer. It provides a method to transport IP packets over the radio interface by adapting service requests for transmission and reception of IP packets to the bearer services offered by the MAC. It also provides a way for the BS to configure packet classifiers in the SSs in order to support IP QoS.
The from the point of view of the IP network the 802.16 network appears a single router or a part thereof, with every SS acting as an intelligent linecard while the BS acts a ‘central route processor’ and a linecard.

IP convergence sub-layer

Functionality

IP SSCS provides the capability to transfer IP SSCS SDU between the IP SSCS of the BS and one or more IP SSCSs of SSs over the 802.16 network.
It is the task of the IP SSCS to map the IP packets to the connections and services of the MAC layer. IP SSCS SDUs coming from the higher layer are mapped onto different MAC transport connections based on the IP source and destination addresses, the Protocol field(v4) or the Next Header field (v6), the source and destination port numbers (for applicable protocols) and Type Of Service(v4) or the Traffic Class (v6). The IP SSCS functions are performed on an IP SSCS-PDU basis. The IP SSCS accepts two kinds of IP packets namely IPv4 and IPv6 packets.

Transport of IP packets

An IP packet is transported in the payload section of one or more MAC PDUs. The CSI bit in the MAC header must be set to zero.

Selectors

IPv4 packets are mapped to MAC connections based the on the contents of the IPv4 header[1]. The selectors for IPv4 are listed in Table 1 .

1. The outermost header in case of IP in IP tunneling.

IPv6 packets are mapped to MAC connections based on contents of the IPv6 chain of headers[1]. The selectors for IPv6 are listed in Table 2 . For IPv6 packets it should be noted that that the Next

Field in IPv4 header	Length	Search type
Source Address	4 Bytes	Longest Prefix Match
Destination Address	4 Bytes	Longest Prefix Match
Protocol	1 Byte	Exact Match
Type of Service	1 Byte	Exact Match
Source port number	2 Bytes	Range Match
Destination port number	2 Bytes	Range Match

Header field is the one indicating the payload protocol.

Field in IPv6 header	Length	Search type
Source Address	4 Bytes	Longest Prefix Match
Destination Address	4 Bytes	Longest Prefix Match
Next Header[a]	1 Byte	Exact Match
Traffic Class	1 Byte	Exact Match
Source port number	2 Bytes	Range Match
Destination port number	2 Bytes	Range Match

a. The Next Header field defining the acting as the selector is the one indicating the payload protocol in the IPv6 header chain.

Filters

A filter is a set of conditions on every selector. Each filter is identified by a 2 byte Filter ID. The Filter IDs are unique within an instance of the IP convergence sub-layer.

Default conditons on the selectors

The default condition on the the selectors are listed in Table 3 .

Selector	Default
Source Address	Ignore

1. The outermost chain of headers in case of IP in IP tunneling.

Selector	Default
Destination Address	Ignore
Protocol	Ignore
TOS/Traffic class	Ignore
Source port number	Ignore
Destination port number	Ignore

IP Convergence sublayer specific messages

A set of IP Convergence sublayer messages is defined to support real time signaling between the IP convergence layers in the BS and SS. These messages are carried in Convergence Sublayer PDUs with the Convergence Sublayer Indicator (CSI) bit set in the MAC header.
The first byte of the message indentifies the type of message as listed in Table 4 . The rest of the message is TLV encoded. The encodings are local to the IP convergence sublayer and are definded below.

Type	Message Name	Message description
0	ADD_FLTR	Add Filter
1	ADD_ACK	Add acknowledge
2	RM_FLTR	Remove Filter
3	RM_ACK	Remove acknowledge
4-255	Reserved	

Add filter message (ADD_FLTR)

The ADD_FLTR message is sent by a BS to a SS to add filter to the SS convergence layer classifier. The parameters are (as defined in <add reference to Encodings..>):

Filter ID. Mandatory parameter. If a filter with this ID already exists it is replaced by the filter defined in the ADD_FLTR message.
IP version. Mandatory parameter
Source address prefix. Optional. Reverts to default if omitted.
Destination address prefix. Optional. Reverts to default if omitted.
Protocol/Next header ID. Optional. Reverts to default if omitted.
Source port number range. Optional. Reverts to default if omitted.
Destination port number range. Optional. Reverts to default if omitted.
TOS/Traffic class. Optional. Reverts to default if omitted.
Connection ID. Mandatory parameter.
HMAC digest if privacy enabled

Add acknowledge (ADD_ACK)

The ADD_ACK message is sent by the SS in resonse to a ADD_FLTR message.The parameters are (as defined in <reference to section on encodings>):

Filter ID. Mandatory parameter.
Condition Code. Mandatory

Remove Filter (RM_FLTR)

The RM_FLTR message is sent by the BS to the SS remove filters from the SS convergence layer classifier. The parameters are (as defined in <reference to section on encodings>):

Filter ID. Mandatory parameter. Appears once for each filter to be removed.
HMAC Digest if privacy enabled

Remove acknowledge (RM_ACK)

The RM_ACK message is sent by the SS in resonse to a RM__FLTR message.The parameters are (as defined in <reference to section on encodings>):

Filter ID. Mandatory parameter.
Condition Code. Mandatory

Encodings for IP convergence sublayer message parameters

Filter ID

The Filter ID. This value is unique within each instance of the IP convergence layer.

Type	Length	Value
0	2	Filter ID

IP version

This record indictes the IP version. Allowed values are 4 and 6.

Type	Length	Value
1	1	IP version.

Source address prefix

This record specifies the source address prefix part of a classifier against which the source address field in the IP header is matched. The prefix is always given as a 32-bit number for IPv4 and a

Type	Length	Value
2	5 or 17	Prefix length, Prefix

128-bit number for IPv6. Only the Prefix length most significant bits of the Prefix are utilized for classification purposes.

Destination address prefix

This record specifies the source address prefix part of a classifier against which the destination address field in the IP header is matched. The prefix is always given as a 32-bit number for IPv4

Type	Length	Value
3	5 or 17	Prefix length, Prefix

and a 128-bit number for IPv6. Only the Prefix length most significant bits of the Prefix are utilized for classification purposes.

Protocol/Next Header identifier

For IPv4 this record specifies the value against which the Protocol field of the IP header is compared. For IPv6 the this field specifies the value against which the Next Header field in the IPv6 chain of headers indicating the type of payload is compared.

Type	Length	Value
4	1	Protocol ID

The encoding of the protocol numbers is that defined by IANA in <reference to iana URL as stated in the references>.

Source port number range

This parameter specifies a range of source port numbers against which the appropriate field in the payload protocol header is matched. The field to be matched is defined separately for each

Type	Length	Value
5	4	start of range, end of range

protocol. The definitions are listed in Table 5 .

Protocol	Relevant field in header	Reference document
TCP	Source port	RFC792
UDP	Source port	RFC768
SCTP	Source port	

Destination port number range

This parameter specifies a range of source port numbers against which the appropriate field in the payload protocol header is matched. The field to be matched is defined separately for each

Type	Length	Value
6	4	start of range, end of range

protocol. The definitions are listed in Table 6 .

Protocol	Relevant field in header	Reference document
TCP	Destination port	RFC792
UDP	Destination port	RFC768
SCTP	Destination port	

TOS/Traffic class

This parameter specified a set of TOS/Traffic class values.

Type	Length	Value
7	N	value1,valueTOS2 ...,valueN

Connection ID

This parameter specifies the MAC connection over which the flow matching the filter shall transported.

Type	Length	Value
7	2	CID

Condition code

This parameter reports the condition code resulting from an add/remove filter operation.

Type	Length	Value
8	1	Condition code

Allowed values are

0 Filter added successfully
1 Filter modified successfully
2 Add failed, Cannot accomodate new filter

3 Unknown parameter
4 Filter removed successfully
4 Remove failed, no such filter
5 Remove successful.No filters in classifier

HMAC digest

Shall be the final parameter in the list if present. The HMAC digest calculated over all message

Type	Length	Value
9	20	A 160-bit SHA hash

parameters not including the digest itself.

Convergence sublayer configuration parameter file encodings

Convergence sublayer specific information is communicated during registration in configuration files using the parameter defined in < reference to section currently 2.3.8>. The sub-index for the IP convergence layer configuration file paramters is [99].3.

Filter definition

This parameter defines a filter for the classifier. The value is in itself a list of subindexed TLVs.

Type	Length	Value
[99.3].0	n	List of TLVs defining the filter

The mandatory fields in the filter definitions are : Filter ID, IP version and CID. In the absence of a selector condition definition the selector is ignored.

Filter ID

The Filter ID. This value is unique within each instance of the IP convergence layer.

Type	Length	Value
[99.3.0].0	2	Filter ID

IP version

This record indictes the IP version. Allowed values are 4 and 6.

Type	Length	Value
[99.3.0].1	1	IP version.

Source address prefix

This record specifies the source address prefix part of a classifier against which the source address field in the IP header is matched. The prefix is always given as a 32-bit number for IPv4 and a

Type	Length	Value
[99.3.0].2	5 or 17	Prefix length, Prefix

128-bit number for IPv6. Only the Prefix length most significant bits of the Prefix are utilized for classification purposes.

Destination address prefix

This record specifies the source address prefix part of a classifier against which the destination address field in the IP header is matched. The prefix is always given as a 32-bit number for IPv4

Type	Length	Value
[99.3.0].3	5 or 17	Prefix length, Prefix

and a 128-bit number for IPv6. Only the Prefix length most significant bits of the Prefix are utilized for classification purposes.

Protocol/Next Header identifier

For IPv4 this record specifies the value against which the Protocol field of the IP header is compared. For IPv6 the this field specifies the value against which the Next Header field in the IPv6 chain of headers indicating the type of payload is compared.

Type	Length	Value
[99.3.0].4	1	Protocol ID

The encoding of the protocol numbers is that defined by IANA in <reference to iana URL as stated in the references>.

Source port number range

This parameter specifies a range of source port numbers against which the appropriate field in the payload protocol header is matched. The field to be matched is defined separately for each

Type	Length	Value
[99.3.0].5	4	start of range, end of range

protocol. The definitions are listed in Table 5 .

Protocol	Relevant field in header	Reference document
TCP	Source port	RFC792
UDP	Source port	RFC768
SCTP	Source port	

Destination port number range
This parameter specifies a range of source port numbers against which the appropriate field in the payload protocol header is matched. The field to be matched is defined separately for each

Type	Length	Value
[99.3.0].6	4	start of range, end of range

protocol. The definitions are listed in Table 6 .

Protocol	Relevant field in header	Reference document
TCP	Destination port	RFC792
UDP	Destination port	RFC768
SCTP	Destination port	

TOS/Traffic class
This parameter specified a set of TOS/Traffic class values.

Type	Length	Value
[99.3.0].7	N	value1,valueTOS2 ...,valueN

Connection ID
This parameter specifies the MAC connection over which the flow matching the filter shall transported.

Type	Length	Value
[99.3.0].7	2	CID