INTERNATIONAL TELECOMMUNICATION UNION

RADIOCOMMUNICATION STUDY GROUPS

Document 8A/IEEE-2-E
Document 8F/IEEE-1-E
8 March 2006
English only

Received: **TECHNOLOGY**

Subject: Question ITU-R 223-1/8

Institute of Electrical and Electronics Engineers (IEEE)

KEY TECHNICAL AND OPERATIONAL REQUIREMENTS FOR ACCESS TECHNOLOGIES TO SUPPORT IP APPLICATIONS OVER MOBILE SYSTEMS

This contribution was developed by IEEE Project 802, the Local and Metropolitan Area Network Standards Committee ("IEEE 802"), an international standards development committee organized under the IEEE and the IEEE Standards Association ("IEEE-SA").

The content herein was prepared by a group of technical experts in IEEE 802 and industry and was approved for submission by the IEEE 802.16 Working Group on Wireless Metropolitan Area Networks, the IEEE 802.18 Radio Regulatory Technical Advisory Group, and the IEEE 802 Executive Committee, in accordance with the IEEE 802 policies and procedures, and represents the view of IEEE 802.

IEEE thanks ITU-R for the liaison statement in Document IEEE 802.16-05/056 requesting input for the progression of the work toward the development of a PDNR ITU-R M.[IP CHAR] ("Key technical and operational requirements for access technologies to support IP applications over mobile systems") in response to Question ITU-R 223-1/8, which WP 8F is developing in close co-operation with WP 8A.

We have reviewed the document with interest and we have developed a description of the relevant capabilities of the IEEE 802.16 standard based on the outline of the sections in the main body of Annex A of the PDNR ITU-R M.[IP CHAR].

Proposal

We propose a new attachment to Annex A, summarising the implementation of relevant technical and operational requirements for access technologies to support IP capabilities of IEEE 802.16 systems.

Attachment 1

Use of IEEE 802.16 access networks to support IP applications in the mobile service

Introduction

IEEE Std 802.16-2004 [1] as amended by IEEE Std 802.16e-2005 [2], hereafter referred to as the IEEE 802.16 standard, specifies an air interface (including the medium access control layer and multiple physical layer specifications) of BWA systems supporting multiple services. Included is support for subscriber stations moving at vehicular speeds to specify a mobile broadband wireless access (BWA) system. Functions to support higher layer handover between base stations or sectors are specified. Mobile operation is limited to licensed bands suitable for mobility below 6 GHz. The standard enables rapid worldwide deployment of innovative, cost-effective, and interoperable multivendor BWA products and networks, including mobile networks supporting IP applications.

This Attachment summarises the relevant capabilities of the IEEE 802.16 standard based on the outline of the sections in the main body of Annex A, illustrating how the IEEE 802.16 standard meets the key technical characteristics for the All IP Network that are essential in supporting IP applications in the mobile service.

It should be noted that the IEEE 802.16 standard provides the basic lower layer transport capabilities and other features used to create, control and manage an All IP Network, but the standard does not describe all operational or support aspects necessary for deployment of a fully functional All IP Network. These additional aspects, built on the IEEE 802.16 capabilities, are addressed through the activities of the WiMAX Forum and are described in another Attachment to this Annex.

Scope and structure of IEEE 802.16 standard

Figure 1 illustrates the reference model and scope of this standard. The Medium Access Control (MAC) layer comprises three sublayers. The Service-Specific Convergence Sublayer (CS) provides any transformation or mapping of external network data, received through the CS service access point (SAP), into MAC SDUs received by the MAC Common Part Sublayer (CPS) through the MAC SAP. This includes classifying external network service data units (SDUs) and associating them to the proper MAC service flow identifier (SFID) and connection identifier (CID). It may also include such functions as payload header suppression (PHS). Multiple CS specifications are provided for interfacing with various protocols. The internal format of the CS payload is unique to the CS, and the MAC CPS is not required to understand the format of or parse any information from the CS payload.

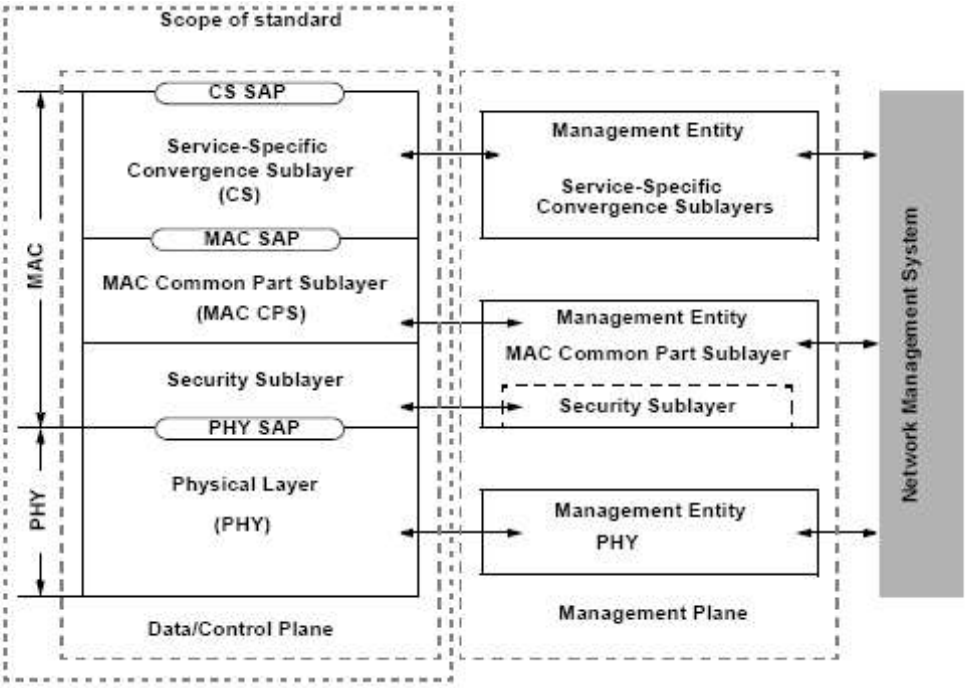

Figure 1—IEEE Std 802.16 protocol layering, showing SAPs

Convergence sublayers

The convergence sublayers specified in the IEEE 802.16 standard are listed below:

Packet, IPv4
Packet, IPv6
Packet, 802.3/Ethernet
Packet, 802.1Q VLAN
Packet, IPv4 over 802.3/Ethernet
Packet, IPv6 over 802.3/Ethernet
Packet, IPv4 over 802.1Q VLAN
Packet, IPv6 over 802.1Q VLAN
ATM
Packet, 802.3/ethernet with ROHC header compression
Packet, 802.3/ethernet with ECRTP header compression
Packet, IP2 with ROHC header compression
Packet, IP2 with ECRTP header compression

The packet CS (required to support IP applications) resides on top of the IEEE Std 802.16 MAC CPS. The CS performs the following functions, utilizing the services of the MAC:

a) Classification of the higher-layer protocol PDU into the appropriate transport connection

b) Suppression of payload header information (optional)

c) Delivery of the resulting CS PDU to the MAC SAP associated with the service flow for transport to the peer MAC SAP

d) Receipt of the CS PDU from the peer MAC SAP

e) Rebuilding of any suppressed payload header information (optional)

The sending CS is responsible for delivering the MAC SDU to the MAC SAP. The MAC is responsible for delivery of the MAC SDU to peer MAC SAP in accordance with the QoS, fragmentation, concatenation, and other transport functions associated with a particular connection's service flow characteristics. The receiving CS is responsible for accepting the MAC SDU from the peer MAC SAP and delivering it to a higher-layer entity.

The packet CS is used for transport for all packet-based protocols.

Packet Header Suppression (PHS)

IEEE 802.16 supports Packet Header Suppression (PHS). In PHS, a repetitive portion of the payload headers of the higher layer is suppressed in the MAC SDU by the sending entity and restored by the receiving entity. Implementation of PHS capability is optional. On the uplink, the sending entity is the Subscriber Station (SS) and the receiving entity is the Base Station (BS). On the downlink, the sending entity is the BS and the receiving entity is the SS. If PHS is enabled at MAC connection, each MAC SDU is prefixed with a 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 PHS 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 shall not be changed. To change the value of a PHSF on a service flow, a new PHS 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 Payload Header Suppression Valid (PHSV) option to verify or not verify the payload header before suppressing it. PHS has also a Payload Header Suppression Mask (PHSM) option to allow select bytes not to be suppressed. The PHSM facilitates suppression of header fields that remain static within a higher-layer session (e.g. IP addresses), while enabling transmission of fields that change from packet to packet (e.g. IP Total Length).

The BS shall assign all PHSI values just as it assigns all connection identifier (CID) values. Either the sending or the receiving entity shall specify the PHSF and the Payload Header Suppression Size (PHSS). This provision allows for preconfigured headers or for higher level signalling protocols outside the scope of this standard to establish cache entries.

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

MAC common part sublayer and support for IP

For the Point to Multipoint (PMP) mode the downlink, from the BS to the user, operates on a PMP basis. The IEEE Std 802.16 wireless link operates with a central BS and a sectorized antenna that is capable of handling multiple independent sectors simultaneously. Within a given frequency channel and antenna sector, all stations receive the same transmission, or parts thereof. The BS is the only transmitter operating in this direction, so it transmits without having to coordinate with other stations, except for the overall time division duplexing (TDD) that may divide time into uplink and downlink transmission periods. The downlink is generally broadcast. In cases where the DL-MAP does not explicitly indicate that a portion of the downlink subframe is for a specific SS, all SSs capable of listening to that portion of the downlink subframe shall listen. The SSs check the CIDs in the received PDUs and retain only those PDUs addressed to them.

Subscriber stations share the uplink to the BS on a demand basis. Depending on the class of service utilized, the SS may be issued continuing rights to transmit, or the right to transmit may be granted by the BS after receipt of a request from the user.

In addition to individually addressed messages, messages may also be sent on multicast connections (control messages and video distribution are examples of multicast applications) as well as broadcast to all stations.

Within each sector, users adhere to a transmission protocol that controls contention between users and enables the service to be tailored to the delay and bandwidth requirements of each user application. This is accomplished through four different types of uplink scheduling mechanisms. These are implemented using unsolicited bandwidth grants, polling, and contention procedures. Mechanisms are defined in the protocol to allow vendors to optimize system performance by using different combinations of these bandwidth allocation techniques while maintaining consistent interoperability definitions. For example, contention may be used to avoid the individual polling of SSs that have been inactive for a long period of time.

The use of polling simplifies the access operation and guarantees that applications receive service on a deterministic basis if it is required. In general, data applications are delay tolerant, but real-time applications like voice and video require service on a more uniform basis and sometimes on a very tightly-controlled schedule.

The MAC is connection-oriented. For the purposes of mapping to services on SSs and associating varying levels of QoS, all data communications are in the context of a transport connection. Service flows may be provisioned when an SS is installed in the system. Shortly after SS registration, transport connections are associated with these service flows (one connection per service flow) to provide a reference against which to request bandwidth. Additionally, new transport connections may be established when a customer's service needs change. A transport connection defines both the mapping between peer convergence processes that utilize the MAC and a service flow. The service flow defines the QoS parameters for the PDUs that are exchanged on the connection.

The concept of a service flow on a transport connection is central to the operation of the MAC protocol. Service flows provide a mechanism for uplink and downlink QoS management. In particular, they are integral to the bandwidth allocation process. An SS requests uplink bandwidth on a per connection basis (implicitly identifying the service flow). Bandwidth is granted by the BS to an SS as an aggregate of grants in response to per connection requests from the SS.

Transport connections, once established, may require active maintenance. The maintenance requirements vary depending upon the type of service connected. For example, unchannelized DS1 services require virtually no connection maintenance since they have a constant bandwidth allocated periodically. Channelized DS1 services require some maintenance due to the dynamic (but relatively slowly changing) bandwidth requirements if compressed, coupled with the requirement that full bandwidth be available on demand. IP services may require a substantial amount of ongoing maintenance due to their bursty nature and due to the high possibility of fragmentation. As with connection establishment, modifiable connections may require maintenance due to stimulus from either the SS or the network side of the connection.

Finally, transport connections may be terminated. This generally occurs only when a customer's service requirements changes. The termination of a transport connection is stimulated by the BS or SS.

All three of these transport connection management functions are supported through the use of static configuration and dynamic addition, modification, and deletion of service flows.

Addressing and connections in Point to Multipoint mode in the Data/Control plane

Each SS shall have a 48-bit universal MAC address, as defined in IEEE Std 802-2001 [3]. This address uniquely defines the SS from within the set of all possible vendors and equipment types. It is used during the initial ranging process to establish the appropriate connections for an SS. It is also used as part of the authentication process by which the BS and SS each verify the identity of the other.

Connections are identified by a 16-bit CID. At SS initialization, two pairs of management connections (uplink and downlink) shall be established between the SS and the BS and a third pair of management connections may be optionally generated. The three pairs of connections reflect the fact that there are inherently three different levels of QoS for management traffic between an SS and the BS. The basic connection is used by the BS MAC and SS MAC to exchange short, time-urgent MAC management messages. The primary management connection is used by the BS MAC and SS MAC to exchange longer, more delay-tolerant MAC management messages. The standard specifies which MAC Management messages are transferred on which of these two connections. Finally, the Secondary Management Connection is used by the BS and SS to transfer delay tolerant, standards-based (e.g. Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), SNMP, etc.) messages. These messages are carried in IP datagrams. Messages carried on the Secondary Management Connection may be packed and/or fragmented. Use of the secondary management connection is required only for managed SS.

The connection identifier (CID's) for these connections shall be assigned in messages. The message dialogs provide three CID values. The same CID value is assigned to both members (uplink and downlink) of each connection pair.

For bearer services, the BS initiates the set-up of connections based upon the provisioning information distributed to the BS. The registration of an SS, or the modification of the services contracted at an SS, stimulates the higher layers of the BS to initiate the setup of the connections.

The CID can be considered a connection identifier even for nominally connectionless traffic like IP, since it serves as a pointer to destination and context information. The use of a 16-bit CID permits a total of 64K connections within each downlink and uplink channel.

Requests for transmission are based on these CIDs, since the allowable bandwidth may differ for different connections, even within the same service type. For example, an SS unit serving multiple tenants in an office building would make requests on behalf of all of them, though the contractual service limits and other connection parameters may be different for each of them.

Many higher-layer sessions may operate over the same wireless CID. For example, many users within a company may be communicating with Transmission Control Protocol (TCP)/IP to different destinations, but since they all operate within the same overall service parameters, all of their traffic is pooled for request/grant purposes. Since the original local area network (LAN) source and destination addresses are encapsulated in the payload portion of the transmission, there is no problem in identifying different user sessions.

The type of service and other current parameters of a service are implicit in the CID; they may be accessed by a lookup indexed by the CID.

IP Header compression

The Convergence sublayer supports SDUs in two formats that facilitate robust compression of IP and higher layer headers. These formats are ROHC (RFC 3095 [4]) and ECRTP (RFC 3545 [5]) and are referred to as the IPheader-compression CS PDU format.

The following parameters are relevant for IEEE Std 802.3/Ethernet CS classifiers [6]:

> IEEE Std 802.3/Ethernet header classification parameters—zero or more of the IEEE Std 802.3/Ethernet header classification parameters (destination MAC address, source MAC address, Ethertype/SAP).

IP-header-compressed IP over IEEE 802.3/ethernet encapsulation exists to deal with the case where a IP compression function (ie. ROHC or ECRTP) is performed on an IP packet carried in an 802.3/ethernet frame before its ingress to the convergence sublayer (note that the compression function shall not operate on the 802.3/ethernet frame header so that the Ethernet frame header remains intact).

For IP-header compressed IP over IEEE 802.3/ethernet, IP header compression and VLAN headers may be included in the classification. In this case, only the IEEE 802.3/802.1Q and Compressed IP header classification parameters are allowed.

Security sublayer

The security sublayer provides subscribers with privacy, authentication or confidentiality across the broadband wireless network. It does this by applying cryptographic transforms to MPDUs carried across connections between SS and BS.

In addition, the security sublayer provides operators with strong protection from theft of service. The BS protects against unauthorized access to these data transport services by securing the associated service flows across the network. The security sublayer employs an authenticated client/server key management protocol in which the BS, the server, controls distribution of keying material to client SS. Additionally, the basic security mechanisms are strengthened by adding digital-certificate-based SS device authentication to the key management protocol.

If during capabilities negotiation, the SS specifies that it does not support IEEE 802.16 security, step of authorization and key exchange shall be skipped. The BS, if provisioned so, shall consider the SS authenticated; otherwise, the SS shall not be serviced. Neither key exchange nor data encryption is performed.

Handover support

On a mobile network, handover is required to support mobile subscriber stations. The handover (HO) process in which a mobile station (MS) migrates from the air-interface provided by one base station to the air interface provided by another base station is defined in the standard.

An MS shall be capable of performing handover using the procedures defined. The handover process may be used in a number of situations, some examples being:

> When the MS moves and (due to signal fading, interference levels, etc.) needs to change the base station to which it is connected in order to provide a higher signal quality;
>
> When the MS can be serviced with higher QoS at another base station.

The handover decision algorithm is beyond the scope of the standard.

The HO process consists of the stages:

Cell reselection:

> MS may use Neighbor BS information acquired from a decoded message, or may make a request to schedule scanning intervals or sleep-intervals to scan, and possibly range, Neighbor BS for the purpose of evaluating MS interest in handover to potential target BS. The cell reselection process need not occur in conjunction with any specific, contemplated HO Decision.

HO Decision & Initiation:

A handover begins with a decision for an MS to handover from a serving BS to a target BS. The decision may originate either at the MS, or the serving BS. The HO Decision consummates with a notification of MS intent to handover.

Synchronization to Target BS:

The downlink MS shall synchronize to downlink transmissions of Target BS and obtain DL and UL transmission parameters.

Ranging:

The MS and target BS shall conduct Initial Ranging or Handover Ranging. Target BS may make a request to serving BS for information on the MS over the backbone network and serving BS may respond. Regardless of having received MS information from serving BS, target BS may request MS information from the backbone network.

Termination of MS Context:

Termination of MS Context is defined as serving BS termination of context of all connections belonging to the MS and the context associated with them (i.e,. information in queues, ARQ state-machine, counters, timers, header suppression information, etc. is discarded).

References:

1. IEEE 802.16-2004: IEEE Standard for Local and metropolitan area networks: Part 16: Air Interface for Fixed Broadband Wireless Access Systems.

2. IEEE 802.16e-2005: IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems: Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands.

3. IEEE Std 802-2001: 802-2001 IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.

4. RFC 3095 Borman, et al, 'RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP and uncompressed', July 2001.

5. RFC 3545 Koren, et al, 'Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering', July 2003.

6. IEEE Std 802.3-2005: IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks--Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.