INTERNATIONAL TELECOMMUNICATION UNION

**RADIOCOMMUNICATION STUDY GROUPS**

**Document 4B/123-E**
**Document 8D/462-E**
**16 February 2007**
**English only**

Source: Document 8F/TEMP/479(Rev.3)

## Working Party 8F

# LIAISON STATEMENT TO RELEVANT EXTERNAL ORGANIZATIONS AND WORKING PARTY 8A

(COPY TO WORKING PARTIES 4B AND 8D)

## On the preliminary draft new Report ITU-R M.[IP CHAR] "Key technical and operational characteristics for access technologies to support IP applications over land mobile systems" in response to Question ITU-R 223-1/8

Working Party 8F would like to thank External Organizations (EOs) and Working Party 8A for their liaison statements (Docs. 8F/1051, 1052, 1064 and 1113) on the development of a joint WP 8A/8F PDN Report ITU-R M.[IP CHAR] "Key technical and operational characteristics for access technologies to support IP applications over land mobile systems".

WP 8F has editorially updated the joint WP 8A/8F PDN Report ITU-R M.[IP CHAR] "Key technical and operational characteristics for access technologies to support IP applications over mobile systems" received from WP 8A, taking into account comments from the relevant External Organizations. ITU-R WP 8F also discussed the title of the Report and concluded that it should include the idea of "land mobile systems" so that the title of the Report can appropriately reflect the content.

WP 8F noted that the Report is now complete and decided to send it to the 20th meeting of WP 8A for a final editorial check and subsequent submission to the 8th meeting of Study Group 8 in June 2007 for adoption. The preliminary draft new Report is provided in the Attachment 1 to this liaison statement.

WP 8F would like to thank the relevant External Organizations and WP 8A for the fruitful cooperation for the development of the Report ITU-R M.[IP CHAR] in response to Question 223-1/8.

**Attachment:** 1

**Contact (for EOs):**

Colin LANGTRY
Counsellor, ITU-R Study Group 8
E-mail: colin.langtry@itu.int

**Contact (within ITU):**

Hitoshi YOSHINO
NTT DoCoMo Inc.
Research laboratories
Hikarino-oka 3-5
Yokosuka-shi
KANAGAWA 239-8536
Japan
Tel: +81 468 40 3555
Fax: +81 468 40 3789
E-mail: yosino@mlab.yrp.nttdocomo.co.jp

# Attachment 1

Source: Document 8F/TEMP/478(Rev.2)

JOINT WP 8A/ WP 8F PRELIMINARY DRAFT NEW REPORT
ITU-R M.[IP CHAR]

## Key technical and operational characteristics for access technologies to support IP applications over land mobile systems

(Question ITU-R 223-1/8)

### 1 Introduction

With the high demand for Internet Protocol (IP) applications growing consistently at such high rates, the need to develop more efficient systems able to support new internet features will be a necessity.

It is anticipated that users' demands for mobile services are increasing with greater diversity and complexity for the mobile communications market. Diverse and complex services are expected to have quite different traffic characteristics and QoS levels in comparison to voice traffic or text. In addition, increasing demands on multimedia services causes further more complexity in designing and developing the future mobile systems. Future mobile technologies should support diverse services with different traffic characteristics which are pervasive regardless of air interface technologies. IP applications are accepted as one of solutions to provide affordable and compatible services as used in wired communication systems. Therefore, IP applications over mobile systems will be important in the future due to global interoperability.

IP applications over mobile systems are supported by existing standards that use IP to send data. However, to support enhanced IP applications over mobile systems such as seamless delivery of multimedia data services, several significant technical characteristics in the radio interface and access networks should be considered.

The All IP Network (AIPN) is an IP-based network providing common capabilities that are independent to the type of service being provided and the access system being used. Convergence to IP technology within the AIPN system design should be considered for the system as a whole with minimum duplication of functionality.

During the initial stages of AIPN introduction it is likely that earlier systems and terminals will exist in parallel with AIPNs.

Therefore, the AIPN should be able to support access networks containing Circuit Switched (CS) terminals and accommodate access systems based on CS.

Interworking and interconnection with CS networks should be provided.

The AIPN should be designed to enable efficient coexistence with earlier PS domains.

### 2 Scope

This Report defines the essential technical and operational characteristics needed to support IP applications over mobile systems.

# 3 References

## 3.1 Related ITU-R Recommendations and Reports

Recommendation ITU-R M.1079 – Performance and quality of service requirements for IMT-2000 access networks

Recommendation ITU-R M.1741 – Methodology for deriving performance objectives and its optimization for IP packet applications in the mobile-satellite service.

Recommendation ITU-R S.1711 – Performance enhancements of transmission control protocol (TCP) over satellite networks (pre-published)

Recommendation ITU-R M.1645 – Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000

Report ITU-R F.2058 – Design techniques applicable to broadband fixed wireless access (FWA) systems conveying Internet protocol (IP) packets or asynchronous transfer mode (ATM) cells.

## 3.2 IETF

The following references provide supporting information and do not refer to specific implementations.

IETF RFCs are available from the IETF web site, http://www.ietf.org/rfc.

RFC 791, Internet Protocol, Sept. 1981.

RFC 793, Transmission Control Protocol, September 1981.

RFC 1035, Domain Names - Implementation and Specification, November 1987.

RFC 1661, The Point-to-Point Protocol (PPP), July 1994.

RFC 2002 IP Mobility support, October 1996.

RFC 2068, Hypertext Transfer Protocol -- HTTP/1.1, January 1997.

RFC 2131, Dynamic Host Configuration Protocol, March 1997.

RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, December 1998.

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

RFC 3545 Koren, et al, “Enhanced Compressed RTP(CRTP) for links with High Delay, Packet Loss and Reordering”, July 2003.

## 4 Definition

AIPN: A collection of entities that provide a set of capabilities for the provision of IP services to users based on IP technology where various access systems can be connected. The AIPN provides a set of common capabilities (including mobility, security, service provisioning, charging and QoS) which enable the provision of services to users and connectivity to other external networks. An AIPN requires one or more connected access systems to allow users to access the AIPN.

Mobile IPv4: Provides mobility support for IPv4.

Mobile IPv6: Provides mobility support for IPv6.

## 5 Abbreviations

| | |
|---|---|
| AAA | Authentication, Authorization, and Accounting |
| AIPN | All IP Network |
| BR | Border Router |
| CN | Correspondent Node |
| DHCP | Dynamic Host Control Protocol |
| E2E QoS | End-to-End Quality of Service |
| HA | Home Agent |
| HAAA | Home AAA |
| HDB | Home Data Base |
| IETF | Internet Engineering Task Force |
| IMS | IP Multimedia Subsystem |
| LAC | Link Access Control |
| MAC | Media Access Control |
| MIPv4 | Mobile IPv4 |
| MIPv6 | Mobile IPv6 |
| MMD | Multi-Media Domain |
| MS | Mobile Station |
| PDF | Policy Decision Function |
| PDSN/AGW | Packet Data Serving Node/ Access Gateway |
| PDU | Protocol Data Unit |
| PPP | Point-to-Point Protocol |
| SLA | Service Level Agreement |
| VAAA | Visited AAA |
| VDB | Visited Data Base |
| P-CSCF | Proxy-Call Session Control Function |
| PDSN | Packet Data Serving Node |
| S-CSCF | Serving-Call Session Control Function |
| RAN | Radio Access Network |

# 6 Basic capabilities

## 6.1 Key characteristics

### 6.1.1 Technical characteristics

Essential key characteristics to support IP applications over mobile systems include:

– Compatibility
– Transparency
– Scalability and efficiency
– Security
– High speed burst traffic
– Low cost per bits
– Seamless Delivery Services
– Various Grade of Services.

IP applications over mobile systems must be able to remain compatible to all levels used for the standard non-mobile IP applications. IP applications over mobile systems should therefore remain "invisible" for higher level protocols and applications. Higher layers should continue to function normally even while the mobile has altered its point of attachment to the network. As new features are developed, the sub-network (subnet) should also function with maximum efficiency and minimum complexity.

As the user rates of mobile communications increase, IP applications over mobile systems should be scalable over the large numbers utilizing the Internet. These subnets should also be able to provide support for advanced internet features as Multicasting and Quality of Service (QoS). Identification during attachment, authentication and authorization are required in order to protect against remote attacks. As information is transmitted from node to node, the location of a mobile node must be authenticated to maintain security.

### 6.1.2 Operational characteristics

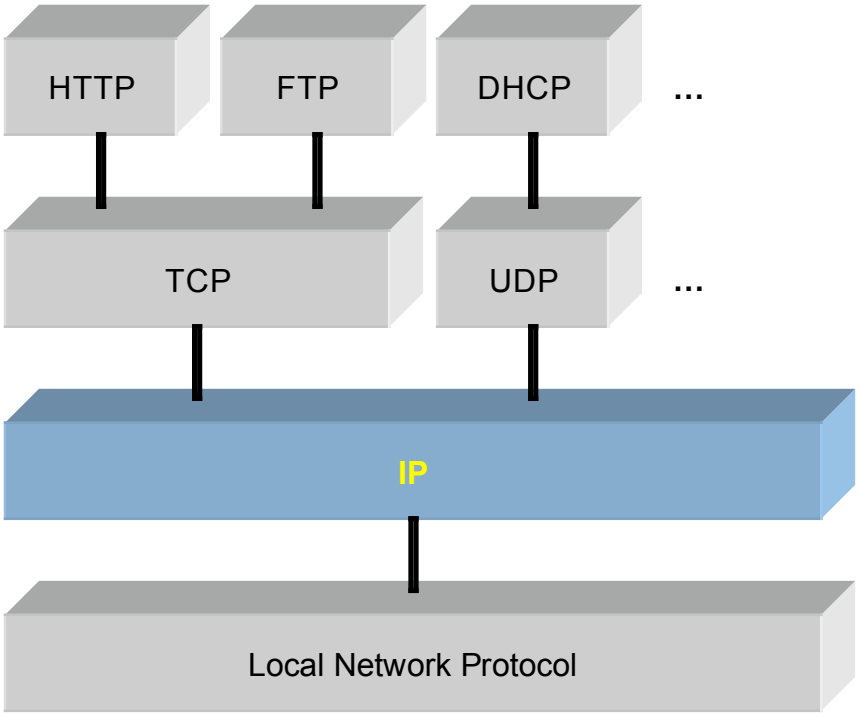
The AIPN should be under the control of the operator of the AIPN. The AIPN should provide common mechanisms for the AIPN operator to control access to and usage of AIPN resources.

## 6.2 Encapsulation

The Internet Protocol Version 4, IPv4, is described in IETF RFC 791. Internet Protocol Version 6, IPv6, is described in IETF RFC 2460. The following Figure illustrates the protocol hierarchy.

FIGURE 6.2.1

**Protocol hierarchy**




All IP application related data is exchanged between hosts in IP packets. For example, the Hypertext Transfer Protocol (RFC 2068) protocol data unit, PDU, is encapsulated in a Transmission Control Protocol (RFC 793) PDU, which is encapsulated in an IP PDU, and then finally in a local network PDU. In the context of mobile systems, the local network may be considered the radio interface.

## 6.3 Address management

To participate effectively in an IP network, a device must possess an IP address. IP packets are routed based on the destination address field within the packet header.

IPv4 addresses are 32-bit binary numbers. Most commonly, they are expressed by considering the 32 bits as four octets, converting each octet to decimal, then separating these numbers with dots to create dotted decimal notation. For example, the address 17.112.152.32 is the dotted decimal notation of:

00010001 01110000 10011000 00100000
00010001 01110000 10011000 00100000

IPv6 addresses are 128-bit binary numbers. If these addresses are expresses in human readable form they are most commonly expressed in hexadecimal with colons to aid legibility, for example:

fe80:0000:0000:0000:020a:95ff:fef3:2e91.

In order to interwork between internet and wireless systems, the mapping between IP addresses and MAC addresses should be considered. For example, IP address of 255.255.255.255 is mapped to the MAC address of ff:ff:ff:ff:ff:ff for data broadcasting in wireless LAN systems.

## 6.4 Maximum Transmission Units (MTUs) and IP fragmentation

IPv4 packets (datagrams) vary in size, from 20 bytes (the size of the IPv4 header alone) to a maximum of 65 535 bytes. Subnets need not support maximum-sized (64 kB) IP packets, as IP provides a scheme that breaks packets that are too large for a given subnet into fragments that travel as independent IP packets and are reassembled at the destination. The maximum packet size supported by a subnet is known as its Maximum Transmission Unit (MTU).

## 6.5 Multicasting/Broadcasting

The Internet model includes "multicasting", where IP packets are sent to all the members of a multicast group. Multicast is an option in IPv4, but a standard feature of IPv6. IPv4 multicast is currently used by multimedia, teleconferencing, gaming, and file distribution (web, peer-to-peer sharing) applications, as well as by some key network and host protocols (e.g., RIPv2, OSPF, NTP). IPv6 additionally relies on multicast for network configuration (DHCP-like autoconfiguration) and link-layer address discovery (replacing ARP). In the case of IPv6, this can allow autoconfiguration and address discovery to span across routers, whereas the IPv4 broadcast-based services cannot without ad-hoc router support.

AlternativelyMBMS (Multimedia Broadcast and Multicast Service) has been developed in mobile systems. The broadcast mode in MBMS differs from the multicast mode in that there is no specific requirement to activate or subscribe to the MBMS in broadcast mode. The broadcast mode is intended to efficiently use radio/network resources e.g. data is transmitted over a common radio channel. Data is transmitted in the broadcast service area as defined by the network. The reception of the traffic in the broadcast mode is not guaranteed.

## 6.6 Bandwidth on Demand (BoD) Subnets

Some subnets allow a number of subnet nodes to share a channel efficiently by assigning transmission opportunities dynamically. Transmission opportunities are requested by a subnet node when it has packets to send. The subnet schedules and grants transmission opportunities sufficient to allow the transmitting subnet node to send one or more packets (or packet fragments). These subnets are referred to as Bandwidth on Demand (BoD) subnets.

## 6.7 Bandwidth asymmetries

Some subnets may provide asymmetric bandwidth (or may cause TCP packet flows to experience asymmetry in the capacity) and the Internet protocol suite will generally still work fine. However, there is a case when such a scenario reduces TCP performance. Since TCP data segments are "clocked" out by returning acknowledgments, TCP senders are limited by the rate at which ACKs can be returned. Therefore, when the ratio of the available capacity of the Internet path carrying the data to the bandwidth of the return path of the acknowledgments is too large, the slow return of the ACKs directly impacts performance. Since ACKs are generally smaller than data segments, TCP can tolerate some asymmetry, but as a general rule, designers of subnets should be aware that subnets with significant asymmetry can result in reduced performance, unless issues are taken to mitigate this (RFC3449).

Several strategies have been identified for reducing the impact of asymmetry of the network path between two TCP end hosts, e.g., (RFC3449). These techniques attempt to reduce the number of ACKs transmitted over the return path (low bandwidth channel) by changes at the end host(s), and/or by modification of subnet packet forwarding. While these solutions may mitigate the performance issues caused by asymmetric subnets, they do have associated cost and may have other implications. A fuller discussion of strategies and their implications is provided in (RFC3449).

## 7 Quality-of-Service (QoS) considerations

Some of the general requirements for QoS should include:

– End-to-end QoS.

– Wide range of QoS-enabled services.

– End-to-end QoS should be supported within the local domain and across different network domains as well.

– Appropriate levels of QoS should be maintained even when internet features, such as multicasting is applied.

The QoS network architecture should be flexible enough to support different QoS control mechanisms, which are defined in different access technology environments. The network should be able to provide mechanisms which could perform traffic and congestion control. Traffic control would include functions such as network resource management, packet marking, traffic shaping, and packet scheduling. Congestion control refers to functions which include packet discarding or explicit congestion notification. The network should also provide methods in which to negotiate QoS at both transport and service layers, and allow dynamic alterations of the QoS parameters. The network should allow operators to implement QoS policy control, where the policy-based management would be extended across multiple domains to ensure QoS.

It is generally recognized that specific service guarantees are needed to support real-time multimedia, toll-quality telephony, and other performance-critical applications[1]. For some important services with strict end-to-end QoS requirements, such as conversational speech or streaming video, the QoS should be assured in case of integrated networking with different IP network domains or backbone networks. Most likely this would be ensured on a per service basis of specific flows of IP packets having been identified by the service.

There are at least two architectural approaches to providing mechanisms for QoS support in the Internet. The IP Integrated Services (Intserv) (RFC1633) is a working group formed to standardize a new resource allocation architecture and new service models for the internet. The Intserv model includes two main components: the traffic control and the ReSerVation Protocol. Flows are identified by a flow specification (flowspec), which creates a stateful association between individual packets by matching fields in the packet header. Capacity is reserved for the flow, and appropriate traffic conditioning and scheduling is installed in routers along the path. The ReSerVation Protocol (RSVP) (RFC2205) (RFC2210) is usually, but need not necessarily be, used to install the flow QoS state. RSVP is a control signalling protocol which requires the introduction of states for specific information flows, although reservation states are “soft” in that they are regularly renewed by messages sent from the initiator of the reservation request. If not renewed, the reservations are timed-out.

Intserv defines two services, in addition to the Default (best effort) service.

1) Guaranteed Service (GS) (RFC2212) offers hard upper bounds on delay to flows that conform to a traffic specification (TSpec). It uses a fluid-flow model to relate the TSpec and reserved bandwidth (RSpec) to variable delay. Non-conforming packets are forwarded on a best-effort basis.

2) Controlled Load Service (CLS) (RFC2211) offers delay and packet loss equivalent to that of an unloaded network to flows that conform to a TSpec, but no hard bounds. Non-conforming packets are forwarded on a best-effort basis.

---

[1] Recommendation ITU-R M.1079 “Performance and quality of service requirements for IMT-2000 access networks”.

The other architectural approach is called the IP Differentiated Services (Diffserv) (RFC2475). This is an alternative resource allocation scheme, which provides service differentiation by dividing the traffic into different classes at the edge of a network by nodes classified as boundary nodes.
A boundary node classifies each incoming packet into a particular traffic class. Diffserv provides a scalable approach, but it in itself does not provide guaranteed QoS. Diffserv does not make any per-flow reservations. Rather, it provides QoS for aggregates of flow. Resources are assured by the prioritization for traffic classes.

Mobile systems face inherent tradeoffs between delay, throughput, reliability, and cost.
Some subnets have parameters that manage bandwidth, internal connection state, and the like. Therefore, the following subnet capabilities may be desirable, although some might be trivial or moot if the subnet is a dedicated point-to-point link.

1) The subnet should have the ability to reserve bandwidth for a connection or flow and schedule packets accordingly.
2) Bandwidth reservations should be based on a one- or two-token bucket model, depending on whether the service is intended to support constant-rate or bursty traffic.
3) If a connection or flow does not use its reserved bandwidth at a given time, the unused bandwidth should be available for other flows.
4) Packets in excess of a connection or flow's agreed rate should be forwarded as best-effort or discarded, depending on the service offered by the subnet to the IP layer.
5) If a subnet contains error control mechanisms (retransmission and/or FEC), it should be possible for the IP layer to influence the inherent tradeoffs between uncorrected errors, packet losses, and delay. These capabilities at the subnet/IP layer service boundary correspond to selection of more or less error control and/or to selection of particular error control mechanisms within the subnet.
6) The subnet layer should know, and be able to inform the IP layer, how much fixed delay and delay jitter it offers for a flow or connection. If the Intserv model is used, the delay jitter component may be best expressed in terms of the TSpec/RSpec model described in (RFC2212).
7) Support of the Diffserv class selectors (RFC2474) suggests that the subnet might consider mechanisms that support priorities.

## 8 End to end requirements for AIPN with access system

### 8.1 Introduction

The AIPN with access system should be capable of fulfilling certain end-to-end characteristics requirements. These requirements, if met by the system, will enable good end-user performance for a variety of end-user services including, but not limited to:

– Real-time, interactive applications, e.g., voice, video and real-time gaming applications.
– Non-real time, interactive applications, e.g., Web browsing, remote login, chat.
– Media streaming applications.
– Conversational services.

The present requirement applies to the entire end-to-end path from the user terminal to the other end-host or server including radio network, core network, and backbone network processing, buffering and propagation delays. Since the delay depends on the location of the end-host, the requirements should be considered as preferred values when the user is within the same continent.

## 8.2 Delay characteristics

The TCP sender bases its retransmission timeout (RTO) on measurements of the round trip delay experienced by previous packets. This allows TCP to adapt automatically to the very wide range of delays found on the Internet. If the path delay variance is high, TCP sets an RTO that is much larger than the mean of the measured delays. If the packet loss rate is low, the large RTO is of little consequence, as timeouts occur only rarely. Conversely, if the path delay variance is low, then TCP recovers quickly from lost packets; again, the algorithm works well. However, when delay variance and the packet loss rate are both high, these algorithms perform poorly, especially when the mean delay is also high.

Because TCP uses returning acknowledgments as a “clock” to time the transmission of additional data, excessively high delays (even if the delay variance is low) also affect TCP’s ability to fully utilize a high-speed transmission pipe. It also slows the recovery of lost packets, even when delay variance is small.

Mobile systems should therefore minimize all three parameters (delay, delay variance, and packet loss) as much as possible. Often these parameters are inherently in conflict. For example, on a mobile radio channel, retransmission (ARQ) and/or forward error correction (FEC) can be used to trade off delay, delay variance, and packet loss in an effort to improve TCP performance. While ARQ increases delay variance, FEC does not. However, FEC (especially when combined with interleaving) often increases mean delay, even on good channels where ARQ retransmissions are not needed and ARQ would not increase either the delay or the delay variance.

The tradeoffs among these error control mechanisms and their interactions with TCP can be quite complex, and are the subject of much ongoing research. It is therefore recommend that mobile systems provide as much flexibility as possible in the implementation of these mechanisms, and provide access to them as discussed above in the section on Quality of Service.

## 8.3 Round-trip delay requirement

The round-trip delay requirement for small IP packets (0 payload) should be defined such that it will enable real-time applications at good quality when both end-hosts reside within the same continent.

Acceptable value is 50-70 ms average round-trip delay.

## 8.4 Packet loss requirement

The packet loss at the IP layer requirement should be defined such that it will enable a certain maximum download data rate for TCP based applications when both end-hosts reside within the same continent and the radio conditions are preferable.

Acceptable value is 0.001% in good radio conditions but maximum 0.1% packet loss ratio.

NOTE 1 – The maximum value for packet loss may also be sufficient for UDP applications.

## 8.5 Delay jitter requirement

The delay jitter requirement should be defined such that it will not harm real-time applications and will not cause significant TCP degradation due to spurious timeouts.

Acceptable value for delay jitter is 25 ms (for real-time gaming), for TCP based download applications occasional bursts of up to 50 ms are still tolerated.

# 9 Supporting mobility

## 9.1 Introduction

Internet users are increasingly mobile. Not only are many Internet nodes laptop computers, but pocket organizers and mobile embedded systems are also becoming nodes on the Internet. These nodes may connect to many different access points on the Internet over time, and they expect this to be largely transparent to their activities. Except when they are not connected to the Internet at all, and for performance differences when they are connected, they expect that everything will "just work" regardless of their current Internet attachment point or local subnet technology.

Changing a host's Internet attachment point involves one or more of the following steps.

First, if use of the local subnet is restricted, the user's credentials must be verified and access granted. There are many ways to do this. A trivial example would be an "Internet café" that grants physical access to the subnet for a fee. Subnets may implement technical access controls of their own. It is common practice for both cellular telephone and Internet service providers (ISPs) to agree to serve one another's users; RADIUS (RFC2865) is the standard method for ISPs to exchange authorization information.

Second, the host may have to be reconfigured with IP parameters appropriate for the local subnet. This usually includes setting an IP address, default router, and domain name system (DNS) servers.

On multiple-access networks, the Dynamic Host Configuration Protocol (DHCP) (RFC2131) is almost universally used for this purpose. On PPP links, these functions are performed by the IP Control Protocol (IPCP) (RFC1332).

Third, traffic destined for the mobile host must be routed to its current location. This roaming function is the most common meaning of the term "Internet mobility".

Internet mobility can be provided at any of several layers in the Internet protocol stack, and there is ongoing debate as to which is the most appropriate and efficient. Mobility is already a feature of certain application layer protocols; the Post Office Protocol (POP) (RFC1939) and the Internet Message Access Protocol (IMAP) (RFC3501) were created specifically to provide mobility in the receipt of electronic mail.

Mobility can also be provided at the IP layer (RFC3344). This mechanism provides greater transparency, viz., IP addresses that remain fixed as the nodes move, but at the cost of potentially significant network overhead and increased delay because of the sub- optimal network routing and tunneling involved.

Some subnets may provide internal mobility, transparent to IP, as a feature of their own internal routing mechanisms. To the extent that these simplify routing at the IP layer, reduce the need for mechanisms like Mobile IP, or exploit mechanisms unique to the subnet, this is generally desirable. This is especially true when the subnet covers a relatively small geographic area and the users move rapidly between the attachment points within that area. Examples of internal mobility schemes include Ethernet switching and intra-system handover in cellular telephony.

However, if the subnet is physically large and connects to other parts of the Internet at multiple geographic points, care should be taken to optimize the wide-area routing of packets between nodes on the external Internet and nodes on the subnet. This is generally done with "nearest exit" routing strategies. Because a given subnet may be unaware of the actual physical location of a destination on another subnet, it simply routes packets bound for the other subnet to the nearest router between the two. This implies some awareness of IP addressing and routing within the subnet. The subnet may wish to use IP routing internally for wide area routing and restrict subnet -specific routing to constrained geographic areas where the effects of suboptimal routing are minimized.

Key AIPN capabilities are characterized as follows:

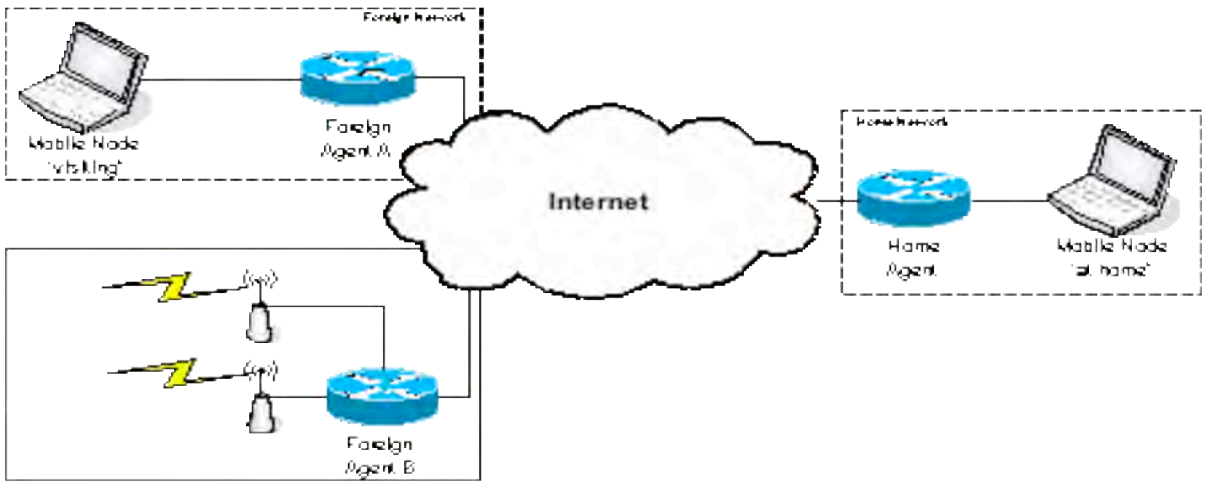
– Able to accommodate fixed access systems and to inter-work with fixed networks in order to provide seamless services over fixed/mobile converged networks, e.g. charging and providing supplementary services.
– Able to support end-user, terminal and session mobility.
– Able to provide seamless terminal mobility within and across access systems. The user should experience no disruption in the service due to terminal mobility.
– Able to maintain a service during a change in access system, with no perceivable interruption from a user perspective.
– Able to support adaptation of services to the capabilities provided by the access systems during terminal mobility.
– Able to support terminal mobility based on criteria including radio conditions, service requirements, user preferences and operator policies.
– Able to notify end users of the degradation in cases when there is a degradation in service quality due to terminal mobility.
– Able to provide appropriate mechanisms to enable users to connect to the AIPN through multiple access systems.
– Able to support handover between CS voice services and AIPN equivalent services (e.g. Voice over IP).

## 9.2 Mobile IP

The IETF have developed mobility support for IP, generically referred to as Mobile IP. In this document we refer to MIPv4 and MIPv6 when appropriate to distinguish between mobility support for IPv4 and IPv6. Figure 9.2.1 depicts the general architecture of MIPv4.

FIGURE 9.2.1

**General architecture of MIPv4**



A brief description of an example implementation of MIPv4 is as follows:

Mobile Node: A node that can change it's point-of-attachment from one link to another by, for example, moving between geographic locations, while maintaining ongoing communications. The mobile node uses only its "permanent" IP address – that address assigned by its home network.

Home Agent: Resides in the home network; maintains a security relations ship with the foreign agent in the visited network; intercepts packets destined to the mobile node's home address and "tunnels" them to mobile node via the foreign agent.

Foreign Agent: Resides in the visited network; maintains a security relationship with the home agent in the home network; acts as the default router for the mobile node while visiting; de-tunnels packets relayed from the home agent.

Further details may be found in RFC 2002.

When IP applications are supported over a mobile system, the mobile node may change its point of attachment by moving between geographic locations, causing the radio sub-system to handover to another cell site. This may or may not cause a handover to a different foreign agent.

### 9.3 Mobility & Handover

The system should support mobility across the cellular network and should be optimized for low mobile speed from 0 to 15 km/h. Higher mobile speed between 15 and 120 km/h should be supported with high performance. Mobility across the cellular network should be maintained at speeds from 120 km/h to 350 km/h (or even up to 500 km/h depending on the frequency band). Voice and other real-time services supported in the CS domain in previous systems should be supported via the PS domain with at least equal quality as supported by previous systems (e.g. in terms of guaranteed bit rate) over the whole of the speed range.

The impact of intra system handovers on quality (e.g. interruption time) should be less than or equal to that provided by CS domain handovers in previous systems.

Mobile speed above 250 km/h, such as a high-speed train environment, represents a special case. In such case a special scenario applies for issues such as mobility solutions and channel models. For the physical layer parameterization the system should be able to maintain the connection up to 350 km/h, or even up to 500 km/h depending on the frequency band.

The system should also support techniques and mechanisms to optimize delay and packet loss during intra system handover.

The wireless network system for future mobile communication may be vary, according to radio network topology, it can be divided into cellular network, distributed network, etc, on the other hand, according to the working function, the mobile user should have the ability to identify multiple radio access system connected IP network, and fast handover freely in different radio access system actively/passively.

## 10 Security requirements

### 10.1 Introduction

There are several security issues related to supporting IP applications whether the applications are run over a mobile system or not. Charging for an application often requires the user to be authenticated to ensure the user is allowed to access the application. In addition, the user may also need to authenticate the application to ensure that personal details, e.g. user's current location or

bank details, are not revealed to the wrong application. Many applications will also have the need to encrypt and protect the integrity of the data that is exchanged between the mobile and application. This ensures that the data sent between the mobile and application can not be read by a man-in-the-middle or modified without it being detected by the receiving party.

The following general objectives should be considered in IP applications over mobile systems:

– Confidentiality
– Integrity
– Accountability
– Availability
– Non-repudiation
– Privacy

## 10.2 Authentication

During the process of handover between foreign agents, it should be avoided that new foreign agents which have not yet been authorized receive data sent from previous FA to the mobile node. For some agent handover algorithms, it is possible that an attacker be provided with an opportunity to act as a pseudo new foreign agent to intercept and capture the data which should normally be transmitted to the mobile node, if the new foreign agent send a "binding update" message to the previous foreign agent before getting the authentication from the mobile node; so it is required that new foreign agents should get the authentication from mobile node first to enhance the security performance of handovers between agents. Mobile nodes could send a "registration request" message to the new foreign agent and simultaneously send a "binding update" message to the previous foreign agent and inform it to cache the data. Subsequently the mobile node performs the authentication procedure with the new foreign agent; and the cached data would be transferred from the previous FA to the new one if the authentication is valid so that a smooth and safe handover mechanism is achieved.

Also, security should be considered along with route optimization. Mobile IP finds a solution to the problem of triangular routing; a mobile node could inform its correspondent node of the care-of address so as to communicate with it without passing through the home agent. But under this circumstance interactive authentication is required for both the mobile node and its correspondent node; in other words, a pair of secret keys are needed. On the other hand, allocating a pair of secret keys for every mobile node and its correspondent node would not be feasible when there are a great amount of mobile nodes and correspondent nodes; but it is practicable to assign a pair of secret keys for every mobile node and its HA.

## 10.3 Privacy

Privacy is a fundamental component of security. Privacy can be viewed as the right of individuals to protect the collection and storage of information related to them and to control the disclosure of that information. By extension, privacy may also be associated with certain technical means (e.g. cryptography) to safeguard from unauthorized disclosure to anyone other than the intended parties, so that only the explicitly authorized parties can interpret the content exchanged among them.

Privacy and confidentiality are terms often used synonymously. However, it should be noted that ITU-T Recommendation X.805 differentiates privacy and data confidentiality. Privacy relates to the protection of the association of the identity of users and the activities performed by them (i.e. online purchase habits, Internet sites visited, etc), whereas, data confidentiality specifically relates to the protection against unauthorized access to data contents(i.e. encryption, access control lists, and file permissions are methods often used to provide data confidentiality.)

The term Privacy is referenced in several ITU-T Recommendations, including F.115, H.235, J.160, Q.1531, X.800, and X.805.

Location privacy and anonymity of the mobile node (MN), i.e. preventing the tracing of mobile user's point of attachment to some network, and identity concealment have gotten a little attention. This service has a great significance especially in wireless network which is more vulnerable to eavesdropping attack than wired network. The disclosure of the MN's location and identity allows unauthorized entities to track down its moving history, which can be a serious violation of privacy.

Fulfilling the security requirement is not the only condition for the successful deployment of mobile IP. Considering the usage of foreign network resources by a MN, it can be easily expected that a foreign network will require the MN to pay for network use. Hence, it is another issue to have a incontestable payment protocol. The payment protocol must make sure that it doesn't reveal location history of a MN as normal payments reveal the payer (HA) and payee (FA). Otherwise, the HA can know the foreign networks that the MN visited.

While providing location privacy and anonymity, the protocol must support revocable privacy rather than perfect privacy. In case of serious crime on communication or dispute on payment, the location history and identity must be revealed.

A rather different threat associated with the mobility management schemes is that of location privacy. For example, route optimization and per-host micromobility protocols might allow a correspondent to tell from a user's care-of address that they are away. It is very important that any mobility protocol is considered from a security point of view, to make sure that it does not have any obvious weaknesses that can be exploited and also that it does not open up a new security hole in another protocol.

Voice privacy can be provided in mobile systems by means of a private code or other means, and it is provided on the traffic channels only. All calls are initiated using the public code but the mobile station user may request voice privacy during or after call setup.

Information privacy is assured by using encryption mechanisms. In an effort to enhance the authentication process and to protect sensitive subscriber information, the method is provided to encrypt. If absolute location privacy is required, the mobile node can create a tunnel to its home agent. All datagrams destined for correspondent nodes will appear to emanate from the home network, and it will make it difficult for hackers to pinpoint the location of the mobile node. Implementing IPsec for mobile IP is to protect the redirected packets sent from or to a mobile node against active/passive attack. In addition, this mechanism also helps packets sent by mobile nodes to traverse the firewall of the visiting or home network.

## 10.4 Technical aspects concerning security

### 10.4.1 Tunnelling mechanism

Employ tunnelling mechanism instead of source routing. Source routing has the disadvantage of insecurity other than complicated realization and large overhead. An attacker could use a fake care-of address as a media destination address so as to prevent the mobile node from obtaining the useful information. But mobile IPv6 could use routing header to realize source routing safely.

### 10.4.2 Employing IPSec

IPSec (Internet Protocol Security) was developed by the IETF. It is an integral part of IPv6 and has also been "backwards fitted" to IPv4. IPSec is made up of two components, which are IP Authentication Header (AH) and the Encapsulating Security Payload (ESP); they could carry out the functions of authentication of the IP header and the payload, integrity checking, non-repudiation and encryption of IP header and payload. These mechanisms are designed to be algorithm-independent. This modularity permits selection of different sets of algorithms without affecting other parts of the implementation. IPSec is a kind of standardized security associations which could provide security guarantee on link layer and transport layer; service providers could implement security strategy according to the service level agreement(SLA) established with users so as to make the management of security associations easier. Moreover, there is only one security association required between the foreign network in which the mobile node is located and the home network; therefore the expansibility of security management is greatly improved.

### 10.4.3 Configuration of firewalls

Configuration of firewalls should be based upon specific requirements. Firewalls could protect the information in private networks against unauthorized visits from illegal nodes. Packet filtering firewall has the property of high speed, independency on applications and low-price. But the configuration of this kind of firewall is complicated. And the leakage of mainframe's IP address in the private network could not be avoided; also, suspicious behaviours could not be recorded. Application-level firewalls normally use a mainframe connected to a router as a relay mainframe; which can support more sophisticated security strategy and has a simple configuration. Private networks could be shielded by the firewall, but would suffer lower speed and the possibility of unable to provide connection with legal mobile node. Firewall with secure tunneling could be used to set up VPNs on public networks to enhance the internet level security. Secure tunnel (built up with IPSec) which could pass through the Internet, combined with previous firewalls, could make up a strengthened VPN security system. On the original end of the secure tunnel, the transmitting node has IP data packets encrypted and encapsulated to be IPSec packets which would subsequently be transmitted through the tunnel to the receiving node, which would decrypt the received IPSec packets and resume them into the original IP packets.

### 10.4.4 Balance between security and complexity

Complexity of protocol realization should also be considered along with the improvement of security. It is required by the diversity of services that various security mechanisms be adopted in order to distribute various security level guarantee to different users; but too many security strategies may cause the problem that the management of the system becomes greatly complicated. To simplify the security management, it is feasible to limit mobile nodes from foreign links to visit specific resources. Security could also be strengthened by means of developing FA's intelligentized level, for instance, add ACLs (Access Control Lists) which are commonly used to filter IP packets to FAs (Foreign Agents) and demand mobile nodes to hold certificates to communicate with FAs.

## 11 Service architecture

The service architecture provides a secure, extensible framework under network operator control. It supports efficient, flexible deployment of end-to-end IP applications. This architecture includes infrastructure elements for service processing, subscriber databases, media gateways and servers, and nodes for policy and charging control, as well as the terminals themselves. Real-time multimedia IP services may be provided as well as less challenging services like streaming and interactive services like messaging.

# 12 Interoperability and interworking

## 12.1 Introduction

The AIPN should provide a high level of basic system performance including low communication delay, low connection set-up time and high communication quality.

The AIPN should provide efficient usage of system resources. In particular, the scarcity of the radio resource should be respected within the AIPN by ensuring that radio resources are utilized as efficiently as possible. The AIPN should also support effective usage of power resources within mobile terminals by minimizing the impact on mobile terminal battery life (standby and active).

The AIPN should be able to accommodate a vast number of terminals and users as well as be able to support a wide variety of diverse devices. Examples of terminals that should be supported by the AIPN include terminals which main purpose is to include a sensor/RF tag, household appliances/media players with a wireless communication module, as well as traditional mobile terminals. Identification, addressing, and routing schemes within the AIPN should be provided to support this communication environment; in particular the AIPN should support naming and addressing schemes for a given user/session.

The AIPN should be able to efficiently support a variety of traffic models e.g. user-to-user, user-to-multicast and traffic models generated by ubiquitous services.

The AIPN should provide functionality as appropriate to support international roaming with other AIPNs.

The AIPN should provide appropriate mechanisms to support independent operation of services, AIPN, and/or access systems.

## 12.2 Legacy systems

Constant technological change often weakens the communication services value of legacy systems, which have been developed over the years through huge investments. Despite the availability of more cost-effective technology, legacy systems continue to provide a competitive advantage through supporting special communication services and containing invaluable knowledge and historical data.

In contrast to modern distributed and layered architectures; legacy systems execute communication services policies and decisions. They are characterized by rigid, predefined process flows, which make integration with user relationship management software and Internet-based business applications torturous and sometimes impossible.

Legacy modernization is crucial for organizations spending too much to maintain the communication services value of their outdated information systems. Also driving the need for change is the industry's movement toward new mobile communication platforms. The new system paradigms leverage a component-based, distributed computing model capable of automating communication services internally or with partners via mobile IP

Several options exist for modernizing legacy systems, defined as any monolithic communication system that's too difficult and expensive to modify to meet new and constantly changing users requirements. Which technique ranging from software update and legacy wrapping to permanent, solutions such as automated migration or replacing the system with the instead of hardware board. which is also more complex.

On the other hand, a variety of options exist, including replacing the system with a packaged application or non-intrusive measures. Each of the approaches makes sense under certain circumstances. The latter methods provide quick and inexpensive access to legacy functionality, while the former can eliminate legacy applications in which the code quality is too poor to migrate.

The solution to the legacy system problem can be provided by a cooperative network, and by systems built over generic IP networking technologies. The key points are that the system should be layered on demand, encourage reuse of independent modularized functional blocks, support multiple services and service creation, ensure consistent end-to-end connectivity across different access technologies, and cooperate in terms of network control, operations, and maintenance. The architecture shall include the endpoints of communications as part of the communications system, and should provide a secure and trusted environment in which network functions are performed; the network should self-organize dynamically.

## 13 Transmission efficiency

The cost and limited availability of spectrum requires that the wireless technology transporting the IP traffic be as efficient as possible.

At the physical layer the measure of spectral efficiency is bits per second/Hz of spectrum used. Optimizing this requires a careful design of the system to minimize overhead and exploit the different QoS requirements of IP applications, the variability of the wireless channel, and the mobility of multiple users in the network.

Above the physical layer, the spectral efficiency for IP applications is maintained by using protocols with low overhead such as compression protocols. In particular, IP header compression protocols for IP multimedia such as RObust Header Compression, specified in IETF RFC 3095 and Enhanced Compressed RTP, specified in IETF RFC 3545 offer a crucial role in efficiency.

## 14 Example of multi-media applications

The wide range of multimedia applications that run over IP networks requires that the wireless system be designed to support all the particular requirements of each application.

### 14.1 Voice-over-IP (VoIP) over mobile systems

Following are the advantages of carrying voice over IP versus conventional circuit-switched voice services:

1) The packetization of voice allows the voice codec and network to jointly exploit variations in the amount of information in the speech signal to reduce the data rate that is needed while not sacrificing voice quality.
2) The flexibility of the IP transport and intelligent-client architecture of IP networks allows the timely introduction of rich and new supplementary services that can be used with the voice services.

In the future, as the use of VoIP applications becomes more and more widespread, the enablement of voice services based on wireless IP will be essential.

VoIP services over mobile systems will have to overcome the following challenges:

– Good QoS support over several different network technologies.
– Real-time service insists strict delay and packet loss requirements over packet switched networks.

– Factors Influencing Speech Quality:
  – Impairment of audio quality due to audio processing.
  – Delay, Jitter, and Loss of packets.
  – Wireless environment are characterized by fluctuations in transmission quality.
  – Physical layer leads to highly error-prone environment.
  – Wireless links generally offer lower bandwidth compared to wireline links.
  – Packet losses due to bit errors.
– Mean Opinion Score (MOS).

### 14.2 Web surfing

The web-surfing experience is no longer limited to static webpages described by markup languages. With the increasing use of downloaded executable applets and scripts, the web surfing multimedia experience has expanded beyond still images to dynamic animation. The richness of these downloaded applications requires downloading of larger clips for execution in the user's web browser.

### 14.3 Streaming audio and video

Streaming audio applications generally require medium amounts of bandwidth with a bound on the amount of total jitter experienced at the receiver. Streaming video requires higher bandwidth with similar bounds on the jitter.

Since streaming applications are generally not real time, the transport of streaming traffic typically does not require immediate delivery. However, to limit the size of the de-jitter buffer required in mobile terminals and reduce tune-in delay for broadcast streaming services, the jitter must be bound by the network.

### 14.4 Digital video telephony

Video telephony is one of the most challenging IP applications to support since it requires high bandwidth, low latency, and low jitter.

## 15 Summary

Mobile communication systems should support diverse and complex services with different traffic characteristics and QoS levels. IP applications over mobile systems is one of promising technologies to provide affordable and compatible services as used in wired communication systems.

This Report has outlined key technical and operational characteristics to support IP applications over mobile systems from various aspects, in particular: it has

– introduced the key capabilities of the All IP Network (AIPN) which is an IP-based network providing common capabilities that are independent to the type of service being provided and the access system being used;
– identified key characteristics to support IP applications over mobile networks and provided general characteristics for diverse QoS support;
– further described in detail, amongst those characteristics, end-to-end characteristics for AIPN with access system, including delay characteristics, round-trip delay, packet loss and the jitter of the delay;

– addressed mobility support for IP and handover since supporting mobility is becoming more important due to the wide spread of laptop computers and other mobile embedded devices;
– identified the general characteristics and discussed related technologies to ensure security, as the demands are increasing for IP applications over a mobile system that equip security functions;
– discussed the issues on interoperability and interworking as well as transmission efficiency since the efficient use of system resources becomes more important, particularly scarce radio resource;
– finally provided some examples of multi-media IP applications that run over a mobile system and discussed their characteristics.

**Appendices**

The following 9 appendices illustrate specific applications and provide valuable information in terms of validation of the characteristics listed in the main body of this Report.

# Appendix 1

# Description of some specific IP applications over mobile systems

## 1 Introduction

Section 2 contains information on features currently available in 3GPP[2], whereas Section 3 deals with future developments currently under study.

## 2 Features currently available

### 2.1 IP Multimedia Subsystem (IMS)

In Release 5, IMS architecture has been developed in order to provide multimedia services based on IETF developed protocols SIP/SDP and provide service enablers in order to provide services developed within and outside of 3GPP (e.g. enable 3rd party service integration with IMS). The architecture for IMS enables delivery of services like speech, video, combinational services, presence, IMS messaging etc. IMS also provides the infrastructure for easy service development; for example, Push to Talk over Cellular (PoC) is one example of the usage of IMS in order to deliver a specific service and ability to charge for these services independent of PS domain charging.

Additional functions available via IMS are necessary enablers to support PoC, IMS messaging, and Presence services. By combining the support of messaging with other IMS service capabilities, such as Presence, new rich and enhanced messaging services for the end users can be created such as Instant Messaging, Chat, Store and Forward Messaging with rich multimedia components. The concept of presence, whereby users make themselves "visible" or not "visible" to other parties of their choice, a services such as group and private "chats" to take place. Presence is an attribute related to mobility information, and provides a different capability to be exploited by other services. The concept of presence enables other multimedia services to exploit this key enabler to support other advanced multimedia services and communications. See also TS 23.228 – "IP Multimedia Subsystem (IMS); Stage 2".

### 2.2 End to end QoS procedures and service based local policy control

In Release 5, end to end QoS architecture for UMTS networks and interworking with external network procedures have been developed over the PS domain, where interworking may be achieved by:

– signalling along the flow path (e.g. RSVP, LDP);

– packet marking or labelling along the flow path (e.g. DiffServ, MPLS);

– interaction between Policy Control and/or Resource Management elements;

– Service Level Agreements enforced by the border routers between networks.

Service based local policy provides mechanism for binding media, policy control over the media (and UMTS bearer) based on the session information from IMS signalling, charging correlation and gating function using a token based approach that requires terminal support.

---

2 More detailed information is provided at http://www.3gpp.org.

## 2.3 Supporting mobility

In 3GPP specifications 23.060 and 29.060, the procedures and protocol details for GPRS Tunnelling protocol (GTP) operation are specified. GTP provides mobility within a GPRS network including one or several access types, e.g. WCDMA RAN, GSM/Edge RAN, and GAN.

The Mobile Station (MS) set up a connection towards an external IP network though activating a PDP context. At activation of a PDP context an MS is able to use either a static IP Address or a dynamically assigned IP Address belonging to its GPRS domain in the MS's home or visited IMT-2000 WCDMA network. The MS selects the IP PoP at PDP Context activation through a configured or default Access Point Name (APN) regardless of whether the MS has a static or dynamic IP Address. The MS keep its PDP context (IP PoP) and maintain the IP Address persistent throughout the packet data session even when handing off between radio networks connected to separate SGSNs.

Fast handover mechanisms in the context of both intra-SGSN and inter-SGSN handover are supported. At inter-SGSN handover, pre-establishment of tunnels to the new serving SGSN are set up prior to the handover and forwarding of packets from the old serving SGSN to the new serving SGSN is supported. The mechanisms are referred to as SRNS Relocation for inter-SGSN mobility within a WCDMA RAN and PS Handover for inter-SGSN mobility between a WCDMA RAN and a GSM/Edge RAN. The fast handover minimizes data loss when the MS is handing off between radio network controllers s connected to separate SGSNs.

## 2.4 Support for IPv6

Cooperation with IETF has resulted in achieving improved support of IPv6 PDP contexts in the PS domain.

## 2.5 IP Transport in UTRAN

In Release 99 and Release 4, only ATM can be used at the transport layer in the various interfaces. This Work Item introduces the possibility to use IP at the transport layer in the Iub, Iur, Iu-Ps and Iu-Cs interfaces, as an alternative to ATM. However, the use of ATM at the link layer under IP is not precluded.

The introduction of IP as a transport protocol in the radio network does not imply an end to end IP network; the UE may be given an IP address by the higher layers, but it will not be part of the UTRAN IP network (which is private), and packets will be encapsulated in the corresponding User Plane protocol.

The Work Item has made a choice for the protocols to transport the Radio and Signalling bearers over IP. Different solutions are adopted: UDP is used in the User plane in the three interfaces, and SCTP with additional protocols is used for the Signalling bearers. With respect to the IP version, IPv6 is mandatory and IPv4 is optional, although a dual stack is recommended.

Additionally, the Work Item resulted in decisions on QoS and interworking with ATM transport networks:

– Diffserv is the mechanism to provide different service levels, and several alternatives are allowed for the traffic flow classification. It is allowed also that the QoS differentiation can be provided either on a hop-by-hop basis or on a edge-to-edge basis.

– Interworking with Release 99/Release 4 and Release 5 ATM nodes is required, and it can be accomplished via a dual stack, a logical interworking function or a separate interworking unit.

## 2.6 RObust Header Compression functionality (ROHC)

Under the Release 4, the ROHC was introduced. Its benefit is an important reduction in header overhead, simply because the fields of the headers of IP packets are either constant or changing in a known pattern. Hence it is possible to send only information regarding the nature of the changing fields of those headers. This leads to a reduction in the size of header, from 40 octets into only few octets while the payload is around 30 octets for some applications (e.g. IP based voice applications) and with IP version 4, and from about 60 octets to only few octets with IP version 6. This translates directly into bandwidth efficiency. The ROHC scheme is claimed to be more suited to cellular environment and changing links than the previous compression schemes. RFC3095 "RObust Header Compression (ROHC)" is the IETF proposal for IP header compression specially designed for real time IP services over wireless links. ROHC was included in the Release 4 of UTRAN as one of the compression schemes to be provided by the PDCP (Packet Data Convergence Protocol) sublayer in the RNC. As ROHC is part of the PDCP layer, there is a compressor and decompressor pair in the RNC and a corresponding pair in the UE. During SRNS relocation the source RNC gives the role of the serving RNC (SRNC) to the target RNC, therefore compressor/decompressor have to be relocated as well. The straightforward solution in place in Release 4 was to initialise the header compression in both peers after relocation, which results in problems like high probability of lost speech frames. This could be avoided by not initialising compression but continuing it in the target SRNC from the place in which the compression ended in the source SRNC. The required changes to perform RFC3095 context relocation in the SRNS context relocation were introduced in Release 5. In order to perform the ROHC relocation, RANAP messages that carry RAB contexts during SRNS relocation are updated to carry also the ROHC/RFC3095 contexts for each RAB. The ROHC context IE to be transferred is defined in the RRC protocol specification. "RFC3095 Context Info" container to RANAP information elements "Forward SRNS Context" and "RANAP Relocation Information" were added to RANAP. Further details can be found in TR 25.844 ("Radio Access Bearer Support Enhancements") and in TR 25.860 ("Radio Access Bearer Support Enhancements") in TR 25.844 – "Radio Access Bearer Support Enhancements" and TR 25.860 – "Radio Access Bearer Support Enhancements" respectively.

## 2.7 IMS signalling flag

IMS signalling traffic is carried by an interactive PS RAB. In order to enable UTRAN to apply special handling of "signalling RABs" compared to other interactive PS RABs, a signalling "flag" was introduced as an additional level of QoS for Interactive traffic RABs.

## 2.8 High Speed Downlink Packet Access (HSDPA) and enhanced uplink

As enhancements of the support for packet data transmission in Release 99/Release 4, the Release 5 radio-interface specification includes enhanced features for HSDPA, allowing for highly efficient downlink packet-data transmission with peak data rates up to 14 Mbit/s and simultaneous high-speed packet data and other services such as speech on the single carrier. Furthermore, the Release 6 radio-interface specification includes features for Enhanced Uplink access allowing for improved capacity and coverage, data rates up to more than 4 Mbit/s, and uplink radio-interface delay less than 10 ms.

## 2.9 Multimedia Broadcast and Multicast Services (MBMS)

The Release 6 radio-interface specification includes a radio access network architecture providing efficient support for MBMS, i.e. allowing for multimedia content distribution to groups of users over a point-to-multipoint bearer.

## 2.10 Flow based charging

Supporting Release 6 Flow Based Charging was developed for GPRS, allowing more granular and flexible charging principles and mechanism for PS domain, this is applicable to both On line and Off line charging cases and allows operators to activate/deactivate charging rules on PDP contexts according to their own policies. This function uses IETF developed Diameter protocols and provides support of such functions as (see also TS 23.125 – "Overall high level functionality and architecture impacts of flow based charging; Stage 2"):

– Identification of the service data flows that need to be charged individually (e.g. at different rates), and those that can be handled as an aggregate.

– Provision and control of charging rules per PDP context on service data flow level.

– Reporting of service data flow level byte counts (for volume based charging) and service data flow durations (for time based charging) based on the PDP context level.

– Event indication according to on-line charging procedures (e.g. sending AAA Accounting Stop) and, optionally, following this particular event, taking appropriate actions on service data flow(s) according to the termination action.

– Event indication and event monitoring and following this particular event, taking the appropriate on-line charging actions.

## 2.11 WLAN-UMTS interworking

In Release 6, interworking of WLAN enables 3GPP–WLAN Interworking so as to extend 3GPP services and functionality to the WLAN access environment. The 3GPP–WLAN Interworking System provides bearer services allowing a 3GPP subscriber to use a WLAN to access 3GPP PS based services. The following functionalities have been specified:

– Provide the interworking WLAN with a means of Access, Authentication and Authorization (AAA) through the 3GPP System, which allows WLAN UEs to access WLAN and the locally connected IP network (e.g. Internet).

– Provide WLAN UEs with IP bearer capability to access PS based services which are provided by PLMN.

For further details, see also TS 23.234 – "3GPP system to Wireles Local Area Network (WLAN) interworking; System description".

## 2.12 Voice Call Continuity (VCC)

During the course of Release 6, TS 23.234 (3GPP system to Wireless Local Area Network (WLAN) interworking: System description) was developed that provides the possibility to offer VoIP over WLAN interworking with IMS.

# 3 Release 7 (current) developments

**Enhancements on IMS:** Currently 3GPP is conducting various studies in order to enhance the IMS system enabling improved performance for the overall 3GPP system in order to deliver real-time services like Multimedia Telephony, PoC etc., improved support for applications via communication service identifiers and providing support for Globally Routable User Agent URI in IMS.

**IMS Multimedia Telephony:** The IMS Multimedia Telephony Service provides real time bidirectional conversational transfer of speech, video or optionally other types of data using basic IMS system concepts. The IMS Multimedia Telephony communication is point to point between

terminals communicating, or a terminal and a network entity. This communication is usually symmetrical, but in special cases the media components present in each direction may be different, or they may be the same but with different bit rates and Quality of Service.

An IMS Multimedia Telephony communication can start with only one type of media and additional types of media may or may not be added by the users as the communication progress. Therefore a particular IMS Multimedia Telephony communication may consist of only one type of media, e.g. speech.

**SMS/MMS over generic 3GPP IP access**: The overall objective is to enhance the 3GPP specifications to support delivery of SMS and MMS over WLAN and any other 3GPP IP access in a manner which guarantees existing SMS and MMS services are not degraded. This specification also describes the means to deliver the content of IMS Messages (i.e. a SIP MESSAGE) to non-IMS users as SMS messages, as well as means to deliver the content of SMS messages to IMS users as IMS Messages (i.e. SIP MESSAGEs) See draft TS 23.204– "Support of SMS and MMS over generic 3GPP IP access".

**Combinational services**: Many operators regard IMS as a key feature. However, there remain issues with the efficiency of transferring Voice over IP over the radio interface, and, with the capability of the GSM radio interface to handle VoIP. Additionally, operators are interested in techniques to smooth the rollout and accelerate the take-up of IMS. As a result of this, a study was started to study the techniques for delivering IMS services using CS bearers for real-time media components. The study covered the different solutions for offering existing IMS simultaneous services (real time media + non real -time media) especially in GERAN, where conversation PS spectrum efficiency is too low. The study resulted in the creation of the specification TS 23.279– "Combining Circuit Switched (CS) bearers with IP Multimedia Subsystem (IMS)".

It describes the architectural details to combine CS services and IMS services (CSI) for using them in parallel between the same two users in a peer-to-peer context. It also provides a detailed description of how capabilities and identities are exchanged to enable the combination of CS and IMS services between the same two UEs.

Current specification includes the following capabilities that enable the combination of CS and IMS services:

– Radio capability exchange.
– SIP based UE terminal capability exchange.
– MSISDN number exchange in SIP.
– Establishing an IMS session in parallel to an ongoing CS call between the same two UEs.
– Establishing a CS call in parallel to an ongoing IMS session between the same two users UEs.

The individual CS call or IMS service that are combined are described in their respective specifications. Additional aspects of CSI interworking including how to handle terminating aspects of the CS and IMS components of the service is currently being studied.

**Evolution of policy control and charging (PCC):** For Release 7 a harmonization of SBLP and FBC that have been developed within 3GPP is ongoing together with addition of an access agnostic approach. The access agnostic approach, moving away from the GPRS focused Release 6 FBC/SBLP, will enable re-use of PCC for other access types (eg I-WLAN, PacketCable, SAE). The harmonization is essential when optimizing real-time interactions of the GGSN (and gateways of other IP Connectivity Access Networks), and optimizing the real-time control architecture of 3GPP in general. Goal is also to study how differentiation based on end-user subscription classes can be achieved. In addition it should be studied how non-QoS policy control functions (e.g. service

authorization, control of redirect functions etc.) fits in the harmonized architecture. These aspects are important in order to fully capitalize on the new core network capabilities that have been developed. See the draft TS 23.203 – "Evolution of policy control and charging".

**System enhancements for fixed broadband access to IMS:** The standardization of the Next Generation Network (NGN) is addressed by a number of SDOs, e.g. ETSI and ITU-T. 3GPP recognizes that external standards organizations are in the process of defining NGN session control using IMS as a platform. This embeds IMS as the framework for advanced services for many types of operators. Enhancements of the 3GPP specifications needed for IMS to meet the NGN requirements is close to completion, TS 23.228 has been updated to capture the architectural enhancements.

**Architectural enhancements for end-to-end Quality of Service (QoS):** The work investigates possible solutions to enhance the end-to-end QoS architecture as currently specified in 3GPP TS 23.207 to achieve improved end-to-end QoS in the case of interworking with IP network domains or backbone networks that provide IP QoS mechanisms and enhanced interworking with other next generation networks. Within this study, emerging QoS standardization efforts from TISPAN, ITU-T, and the IETF should be taken into account. See also TR 23.802 – "Architectural enhancements for end-to-end Quality of Service (QoS)". This work has been completed with the following conclusion and recommended to further changes to 3GPP specifications for now due to this specific study:

"The current interconnection model for 3GPP networks is described in GSMA PRD IR.34 [36] and this model takes a pragmatic approach to QoS, relying simply on overprovisioning and marking of User Plane IP packets (using DiffServ) to exchange QoS information (i.e. as per Release 99). According to GSMA, IMS deployment in the near term will rely on this approach, together with SLAs, to deliver QoS on inter-PLMN networks. Such solution is described in Annex A.2.1 and A.2.2 of TS 23.207 [4] and presented in Section 5.2.3 of the TR.

It is generally recognized that in the future new interconnection models may be needed, e.g., to accommodate increased adoption of IP based services and/or support interfacing to other Next Generation Networks and/or when the committed SLAs cannot be met, although the timing and the details of such need is not currently well understood."

In Release 7 End-to-End QoS support for I-WLAN has also been introduced.

**Voice Call Continuity (VCC):** There is the possibility to support the most prevalent GSM service (voice calls) over IMS via alternative IP Connectivity Access Networks (IP-CAN), e.g. I-WLAN, when there is coverage. By developing the capability to support seamless voice call continuity between the CS Domain and an I-WLAN, an operator would be able to provide relief to the GSM/UMTS radio resources and increase service revenue. Study on such aspects were performed with the following requirements: the study shall identify the impacts to the current 3GPP specifications to support real-time voice continuity when moving between the GSM/UMTS CS Domain and IMS domain using an IP Connectivity Access Network (e.g. 3GPP IP access over I-WLAN and PS domain).

– The study does not introduce new requirements for ISIM and USIM.
– The study should minimize impacts on existing 3GPP specifications.
– The study shall not require changes to radio systems (e.g., UTRAN/GERAN or 802.xx, etc.).

The specification work has started on VCC (see draft TS 23.206 – "Voice Call Continuity between CS and IMS ") based on the feasibility study conclusion documented in TR 23.806 – "Voice Call Continuity between CS and IMS Study".

## 4 Future developments

With enhancements already incorporated in the 3GPP Specifications, the 3GPP radio-access technology will be highly competitive for several years. However, to ensure competitiveness in an even longer time frame, i.e. for the next 10 years and beyond, a long-term evolution of the 3GPP radio-access technology needs to be considered. This is the scope of the Study Item on Evolved UTRA and UTRAN: the SI sheet can be found in SI sheet for "Evolved UTRA and UTRAN". Currently two TR are being developed: one on the feasibility study for Evolved UTRA and UTRAN and the second one focusing on the requirements for Evolved UTRA and UTRAN. Within this framework a number of advanced techniques will be considered; the study of some of those has been already initiated (e.g., OFDM - see SI sheet for "Analysis of OFDM for UTRAN enhancement").

IMS is considered to be crucial for the development of multimedia-based 3G networks. In order to make the deployment of IP based multimedia services economically viable in a 3G environment, it is necessary to ensure that the Radio Access Bearers used to support these services are optimized. RABs for IMS support are already defined in 3GPP UTRAN Rel5. However, these RABs may need to be optimized, in order to ensure a commercially viable deployment of IMS services. Work is ongoing in the scope of the Radio Access Bearer Support Enhancements WI, to analyse UTRAN Rel5 and look at different optimization proposals to improve the support of IMS in Release 6 or later. The work have been focused on VoIP specifically, since it is where the optimization is most needed when comparing a non optimized IMS speech call and a R99 CS speech call.

Currently work has either started or will be starting on the following aspects of architecture development:

**All-IP Network (AIPN):** The AIPN is a common IP-based network that provides IP-based network control and IP transport. This includes the provision of IP-based mobility control of the high quality appropriate for cellular networks (i.e. no degradation in performance compared to other cellular mobility mechanisms) that is not dependent upon specific access or transport technologies, or IP version. It is the aim of the AIPN to provide a seamless user experience for all services within and across the various access systems. As well as across multiple diverse terminals a user may possess. Interworking with external IP networks (e.g. Internet) and legacy networks (e.g. PSTN) is provided and functionality at the edge of the network enables support of different access systems and legacy equipment. See also SI sheet for "All-IP Network" and TR 22.978 – "All-IP network (AIPN) feasibility study".

**3GPP System architecture evolution:** The objective of this feasibility study is to develop a framework for an evolution or migration of the 3GPP system for a higher-data-rate, lower-latency, packet-optimized, multi-RAT, access technology. The focus of this work will be on the PS domain with the assumption that voice services are supported in this domain. The main objectives is to address the following aspects:

– Overall architecture impacts stemming from activities requirements developed from TSG-RAN Study Item on Radio Evolution. The architectural developments should take into account the targets for the evolution of the radio-interface.
– Overall architecture impacts stemming from the work in SA1 on an All-IP Network (AIPN) (see TS 22.258).
– Overall architecture aspects of supporting mobility between heterogeneous access networks, including 3GPP and non-3GPP access networks, such as service continuity.

Migration aspects should be taken into account for the above, i.e. how to migrate from the existing to or evolve to any new architecture. The overall architectural impacts for System Architecture Evolution study is being conducted within 3GPP SA2; for details see TR 23.882 – "3GPP system architecture evolution (SAE): Report on technical options and conclusions"

# Appendix 2

## Location based information services for mobile internet systems

### 1 Introduction

With the convergence of wireless communications and wireless Internet-based networks, wireless Internet broadcasting technologies and services have been actively developed. For Internet-broadcasting service, multicasting technology is the best solution. However, IP multicasting has not been widely deployed due to the lack of multicasting nodes in the Internet and the fundamental concerns related to scalability, reliability, and congestion control. So, instead of multicasting, unicast protocol has been often employed to deliver the broadcast datagram to individual user, one by one. However, as the number of users increase, so do the network traffic and the server load, even to the extent as to bring down some broadcasting server.

In particular, complex protocols between terminals and gateways are needed to support multicasting function in the mobile network. Overall, the current multicasting schemes and the current multicasting addressing are mainly focused on the "pull" operation of the broadcasted data. Additionally, the users need either to know a-priori, or search for the specific web site addresses, when a particular piece of information is needed. Moreover, the users also need to manipulate the settings of his terminal to function in a particular mobile environment.

### 2 The location based information service technology for mobile Internet system

The IP specification defines that the IP address of all 1's represent subnet-level broadcast; i.e., such datagrams are delivered to all the nodes on the subnet. The broadcasting datagram cannot reach nodes beyond the subnet; otherwise, it would result in network-wide flooding and severe congestion.

Using a unicast protocol, a broadcasting server in the Internet can carry broadcast data to an edge router, to a base station, or an Access Point, which are located at the edge of Internet and which are connected to a subnet of terminals. Then broadcasting to all the nodes in the subnet is possible using subnet-level broadcasting. Thus, this technology integrates subnet-level broadcasting operation with unicast routing, where the unicast routing is from a server to an edge router with a unique IP address, and can be applied to all kind of wireless systems which use Internet as core network.

FIGURE A2-1

**The network configuration of location based information service system**

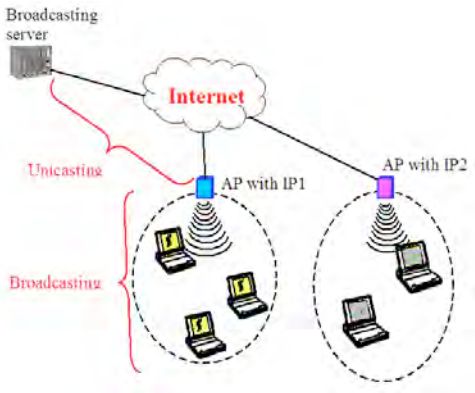


Figure A2-1 shows the network configuration of the location based information service system for wireless Local Area Network (LAN). Wireless LAN networks have been extensively deployed worldwide at a large rate, with almost all of the APs connected to the Internet by a LAN or by an x-Digital Subscriber Line (xDSL). APs are non-mobile and have their own unique IP addresses for operation and maintenance purposes. Thus such an IP address identifies the location of the AP. A broadcasting server maintains the list of IP addresses and their corresponding location information. First, using unicast routing, the broadcasting server sends the broadcasting datagram to a destination IP address, which corresponds to the specific location. The AP with that IP address receives the datagram, and by reading the protocol number and the port number, the AP identifies the datagram as a broadcasting datagram. For broadcasting services, UDP should be used (UDP's protocol number is 17) instead of TCP, and port number should be defined for this applications (e.g., 44555). After the datagram has been identified as a broadcasting datagram, the AP replaces the destination IP address of the datagram to all 1's and resends the datagram on the local radio subnet, after the IP checksum field is recalculated. When the datagram is sent to the subnet, the destination Media Access Control (MAC) layer address should also be set as broadcast address, for channel efficiency in the subnet. For Ethernet and for Wireless LAN, the broadcast address is all 1's of 48bits. On the terminal side, all the associated wireless terminal receivers in the radio zone of the AP receive the MAC frame, and bypass the datagram to the IP layer, because of the MAC address of all 1's. The IP layer passes the datagram on to the UDP layer without filtering, due to the IP address of all 1's. The broadcast data packet is then finally delivered to the application according to the pre-defined UDP port number. The scheme, allows the user to receive the broadcasted data with the information related to the user's location, without the user's need to know the IP address of the data server.

To implement the above Internet location-dependent broadcasting, edge routers, base stations, and Access Points need to be able to translate IP addresses (of course, with associated operations, such as checksum recalculation). In particular, the base stations or the Access Points should identify the broadcasting datagrams and to replace the destination IP address of the broadcasting datagrams to all 1's. The checksum, which covers the IP datagram header, needs to be recalculated and the IP datagram is then broadcasted on the subnet with the MAC-layer broadcast address.

IP datagram broadcast to the subnet does not require the knowledge of the local subnet IP address or the IP addresses of the nodes on the subnet. All of the nodes in the subnet can receive the IP datagram, without any prior configuration of the nodes or of the broadcasting server, such as IP address, subnet mask, gateway address, domain name server address, and web site addresses of interest. Moreover, there is no need for registration to receive the location-based information. The scheme operates in the "push" mode, similar to broadcasting radio stations; i.e., users turn on their terminals and are able to listen to a particular channel. As IP address is not needed at the receiver, IP address assignment protocol, like Dynamic Host Configuration Protocol (DHCP) is not needed and the scheme supports unlimited number of receivers in a subnet. Also, as the server sends broadcasting datagram not to each receiver but to edge routers, base stations, or Access Points only, the broadcasting traffic and the server load are reduced considerably. For location-based information and traffic information services, the broadcasting contents should depend on the location of the base station or the Access Point. In contrast, traditional multicasting schemes, which provide the same contents to all of base stations or Access Points, are unable to support such location-based broadcasting services. By comparing current Internet broadcasting services using unicast protocol, not only the Internet traffic is reduced, but also the local traffic in a subnet or a cell is considerably decreased. Finally, as already pointed out, the proposed scheme implements "push" type of services using broadcasting technology; so neither users and nor service providers need to know the users' locations, eliminating the problem of the privacy of users' location information.

## 2.1 Triggering location based information service

The technology is simple and easy to implement and to use. However, even if there is no user in radio zone, the server would still send the data to the base station or the Access Point. This would result in some inefficiency.

An AP can broadcast announcement messages repetitively to the mobile terminals in its radio zone. When a terminal enters the radio zone and receives the announcement message from the AP, the terminal transmits broadcast request datagram to the AP, with destination IP address of all 1s, UDP protocol, and pre-defined port number. The AP receives and recognizes the triggering datagram and sends a broadcast request datagram to the server by unicast routing. When the server receives the broadcast request datagram, it starts a timer and begins sending the broadcasting data to the AP. In the absence of future triggering datagrams from the AP, the server ceases to send the broadcasting data after the timer expires. Thus, for a terminal to continue to receive broadcasting data, the terminal has to periodically send the triggering datagram to the AP.

The AP periodically sends out its setup information, which is constantly received by the terminals and which consists of the AP announcement messages, AP identification, the list of current or available broadcast channels, and the remaining time until timer expiration (of each broadcast contents). When a terminal moves from one location to another, by listening to the setup information of a local AP, the terminal is able to recognize the new AP. If a required broadcasting channel is not among the currently broadcasted channels, then the terminal sends a triggering datagram. By employing the optional triggering datagrams with some added complexity, the unnecessary broadcasting traffic can be eliminated and the network utilization can be improved.

## 2.2 The repetitive information service and data filtering

Some data do not change frequently and it is often the case that such data need to be received once by a terminal and refreshed infrequently.

As a terminal moves throughout a radio zone of an AP, the time to receive any particular data is limited by the size of the zone and by the velocity of the moving terminal. For a user to be able to listen to particular data at least once in a zone, the data should be broadcast repetitively in the zone. This can be implemented by storing the data in the AP and the control fields of the header of the broadcasting data (to be used by the AP) should include the broadcasting duration, the broadcasting data priority, and the re-broadcasting period. When the AP receives the broadcasting data, it first analyzes the header field and stores the broadcasting data with the control fields of the header.

The location-based information data sent from the broadcasting server to the APs would typically be of very large volume. Moreover, such data could change periodically. As the broadcasting data is not requested by the terminal but rather pushed into the terminal, if all such data were to be displayed on a terminal, it would be very difficult for a user to identify the pieces of data which are of interest to the user. By categorizing the broadcasting data in the control field of the header, the user's terminal can selectively display on the terminal only those parts which are of interest to the user. The advantage of such a selective "push" scheme, as is the case with the non-selective scheme, is that the user does not have to know the actual web site address of the broadcasting server; the terminal simply automatically selects the information of interest to the user. Once the basic information is received and displayed on the user's terminal, he can now easily navigate to the corresponding web site by clicking on the appropriate links.

## 2.3 Data indexing

In this technology, the terminal needs to examine every datagram to identify those with information needed by the user. Such an operation could represent a significant overhead the terminals in which the lack of processing power and battery capacity are crucial factors. If AP were to provide broadcasting information about the data in advance of the actual broadcasting for every broadcasting contents or service, such as the times at which the data will be broadcasted, the port number, or even particular IP/MAC addresses, the terminals could then reject broadcasting frames of no interest, without processing those frames at the MAC and IP layers.

More specifically, every broadcasting content would be broadcasted via pre-determined MAC address, IP address, and port number. Thus, every MAC frame received from the AP with address that the user does not want should be abandoned at the MAC layer of the terminal. It would save the processing power and the battery power at the terminal, as compared with the case when the frame is abandoned at higher layers. This operation can also be done at the IP layer using IP address; however, it is most efficient as a lower layer operation.

Time indexing for broadcasting method has already been proposed at the MAC protocol level to save power consumption. In the same way, broadcasting scheduling on IP layer level is possible. When broadcasting server and AP send location based information to terminals, it should contain broadcasting times of each broadcasting contents. The terminals then know when the broadcasting data is going to be transmitted and can turn on the receiver at the indicated time. Using such a scheme, power consumption and processing load can be reduced significantly.

FIGURE A2-2

**Examples of some main data formats**

| broadcast_signal frame | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| signal_header | | | | broadcast_info | | | | | | | |
| packet_class | repetition_period | BS_id | location_id | broadcast_current | | | | | broadcast_avail | urgent_info | |
| | | | | info_class | req_period | prog_id | MAC/IP/port addr | broadcast_period | the same to broadcast_current | | |

| broadcast_data frame | | | | | |
|---|---|---|---|---|---|
| data_header | | | | | payload_data |
| packet_class | req_req | prog_id | BS_id | location_id | |

| broadcast_req frame | |
|---|---|
| subscriber_info | prog_id |

## 3 Examples of applications

The location based information service technology can be used for providing location-specific information to users based on the position of their associated AP. The applications could be categorized as *Location Based Services (LBS), Private Broadcasting Services (PBS),* and *Digital Multimedia Broadcasting Services (DMBS)*.

- Examples of *Location Based Services* applications:
  - Location based geographic information services
  - Location based community news
  - Location based shopping information services
  - Location based tourist information services
  - Emergency guide services
  - Traffic information services

As user moves into a radio zone, the user can receive location-specific information without the knowledge of the user's position information. This is very convenient for drivers and pedestrians with limited handling capabilities of complicated web searching. Furthermore, it ensures privacy of users' locations information.

- Examples of *Private Broadcasting Services*:
  - Announcement service in a sports stadium or a theater
  - Conference services
  - Emergency announcements

When many people gather into a place and need the same information, the location-based broadcasting can be a very efficient solution. In particular, wireless LANs with location-based IP broadcasting could be used to implement an unlicensed broadcasting system. For instance, an AP is located at the center of stadium and uses omni-directional antenna, then it might be able to cover the full range of the stadium. One of such applications, the emergency evacuation directions, could be implemented by an AP unit and data storage, while those operate on batteries. Such a system would work without the need for a network connection or power supply.

- *Digital Multimedia Broadcasting Services (DMBS)*
  - E-education services
  - Indoor and outdoor DMB services

The proposed technology supports services much like the common broadcast radio or TV; this user can just turn on the receiver and select the preferred data, especially for multimedia services.

# Appendix 3

## A protocol for improving UDP performance over wireless networks and its application to mobile robot control

### 1 Abstract

The emerging wireless internet (WiBro in Korea) era allows the introduction of many new services. The intelligent mobile robot service is the one of the new services. Wibro can control the robot remotely. In the control, both the on-line real-time and the reliability of control data transmission are very important. Considering the real-time control and data reliability, a new protocol for the robot service has been designed. UDP protocol is described below with some policies that are effective for the mobile robot service. Two flow charts for packet transmission are shown. Finally, comments are made for both the interval time decision making of local retransmitting and another protocol policy for moving users.

### 2 A control protocol for the mobile robot over wireless internet

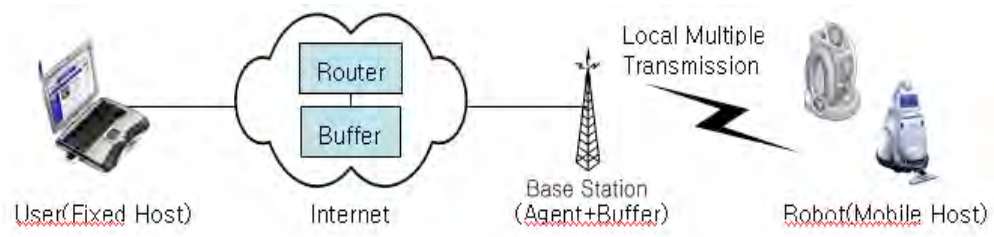
When one controls the remote mobile robot through wireless internet, we must consider the on line real-time and reliability of robot control data transmission. There are two major protocols in internet, TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). In TCP, the protocol divides these data into multiple packets and transmits. After confirming the arrival of the data (receiving the ACK packet), TCP transmits the next packet. The TCP protocol takes more time than UDP. Because the TCP is particularly targeted at the wired networks, a packet loss is assumed to be caused by the network congestion. In the wireless environment, the chance of losing packets due to transmission bit errors is not negligible. Transmissions are especially prone to bursty packet error. Therefore the TCP protocol is not proper for application to real-time control of the robot.

We selected the protocol UDP for robot real-time control through wireless internet. The UDP also has some problems. UDP is prone to error even though the protocol is speedy. In this contribution, to overcome the problem, we adopt some policies (algorithms) under UDP. Both robot control data transmission under priority condition in wired links and using multiple transmissions in wireless links can make the mobile robot act on time correctly.

Figure A3-1 shows the network environment consisting of wired links and wireless links. The user can control remotely the mobile over wireless internet.

FIGURE A3-1

**The protocol of network and mobile robot**



The robot control data and links are defined as follows:

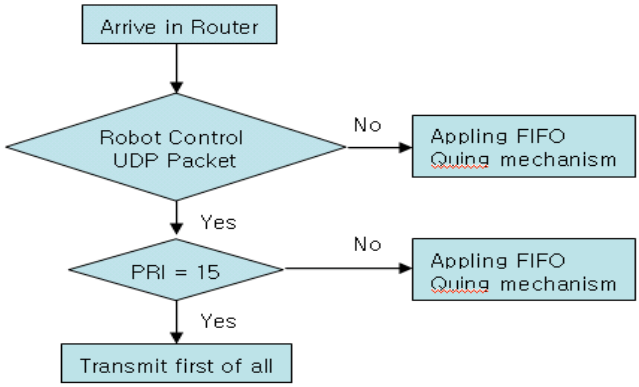
Robot control data: Simple command to order the robot move or do some work. Example: key inputs on mobile phone panel, key inputs on computer keyboard.

Wired links : To accomplish the real time transmission of the UDP packet for robot control and overcome congestion packet loss, set the priority field (PRI) of the IP packet as 15(IPv6). The node (router) serves the arrived packet of robot control data with PRI 15 first of all.

Wireless links: To exclude transmission congestion loss of robot control data in wireless links (which have essential difficulties), copy the robot control UDP packet at the base station and transmit multiple times to the robot. The length of wireless link is usually shorter than wired links. So the delay time of wireless links is of a brief duration compared with transmission time of wired links.

FIGURE A3-2

**Flow chart of data processing at wired links**

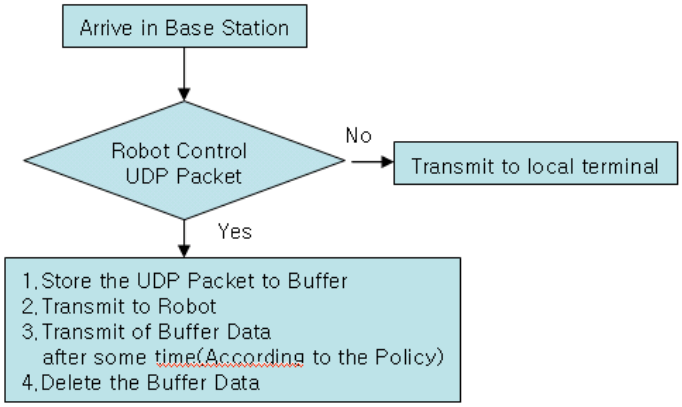



In wired links, packet loss is low and speedy transmission is possible. We selected the UDP protocol for robot control data transmission. If the router receives the UDP robot control packet (with PRI=15 in Ipv6), the router must immediately transmit the packet first of all. In wireless link base stations, whether the received packet is robot control UDP or not, one copies the packet and transmits multiple times or transmits the packet as it is.

…

FIGURE A3-3

**Flow chart of data processing at base station of wireless links**




In Figure A3-3, there might be many policies. If a packet loss occurs at the wireless link and there is a chance that the loss is noticed by the application, one can choose the interval time. For example, packet losses can be noticed by receiving ACK packets in the application layer. Then the local retransmission interval time can be defined after the receiving the ACK packet.

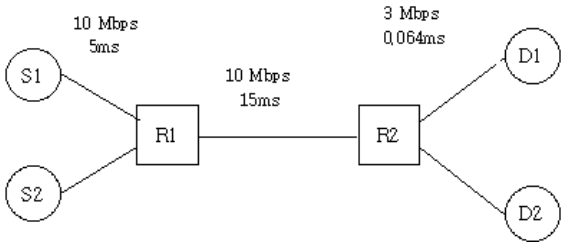
The protocol which is about network consisting of mobile links between user and internet. In this case, the condition is more complicated than the links between a base station and the robot.

## 3 Simulation Method

The simulation network configuration is shown in Figure A3-4. Two sources S1 and S2 are connected to a router R1 through 10 Mbit/s and 5 ms delay links. Router R1 is connected to R2 through a 10 Mbit/s and 15 ms delay link. Destination D1 is connected to the router R2 via 3 Mbit/s, 0.064 ms delay link. The link between the router R2 and destination D1 is made wireless link with packet errors. Traffic to evaluate the performance is connected to the source S1, and background traffic is connected to the source S2 and generates the bottle-neck link between the router R1 and the router R2. The source S1 sends data to the destination D1, the source S2 the destination D2. The traffic connected to the source S1 is generated by a CBR (Constant Bit Rate) traffic with a packet size 50 bytes and the time interval 0.1 second. The background traffic connected to the source S2 is a CBR traffic with a packet size 500 bytes and its rates 5 Mbit/s, 10 Mbit/s, and 20 Mbit/s. The packet error rate of the wireless link is varied to test the performance of various methods under different loss environments. The schemes we compared include base TCP, UDP, and the duplicate transmission method considering the priority which is proposed in this document.

FIGURE A3-4

**Simulation network configuration**




## 4 Simulation results and Analysis

Our experiments were simulated using the ns-2 simulator from the Lawrence Berkely Laboratory. The major metrics we used to evaluate the proposals are packet delay and packet loss. The packet delay in TCP is defined as the time difference between the transmitted packet and the acknowledged packet. The packet delay in UDP is defined as the time difference between the transmitted packet and the received packet. The packet loss is defined the packet which is not successfully received at the receiver. The performance metrics of three schemes under two packet error rates are shown.

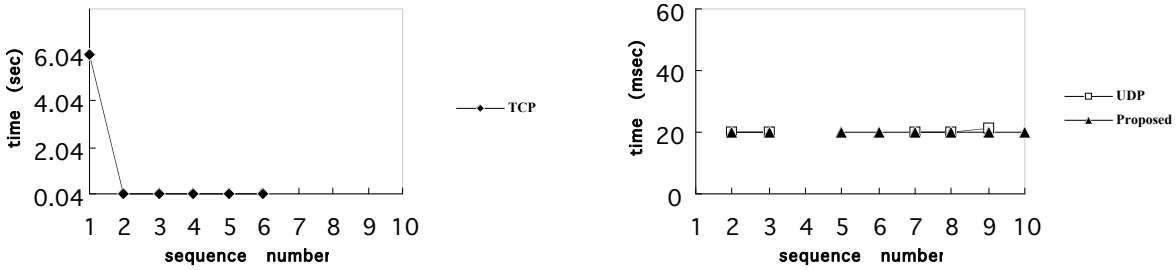
Figure A3-5 shows the results under the packet error rate 10 % of the wireless link between the router R2 and the destination D1. Figure A3-5(a) shows the result under the transmission rate 5 Mbit/s of the source S2. From the Figure A3-5(a) the packet delay of TCP packet of the sequence number 1 is 6 seconds. This result is expected from the retransmissions which are caused by the packet loss. After the packet of the sequence number 7 there are cases that the acknowledged packet has not arrived at the source S1. In UDP there are packet losses of the sequence numbers 4, 5, 6, and 10. In the proposed method the sequence numbers are 1 and 4.

Figure A3-5(b) shows the result under the transmission rate 10 Mbit/s of the source S2. From the Figure A3-5(b) we can see that the packet delay of TCP follows a similar pattern to the results in Figure A3-2(a), while after the packet of the sequence number 5 there are cases that the acknowledged packet has not arrived at the source S1. The packet delay of UDP and the proposed scheme is about 20 ms, and both schemes have a packet loss in the sequence number is 1.

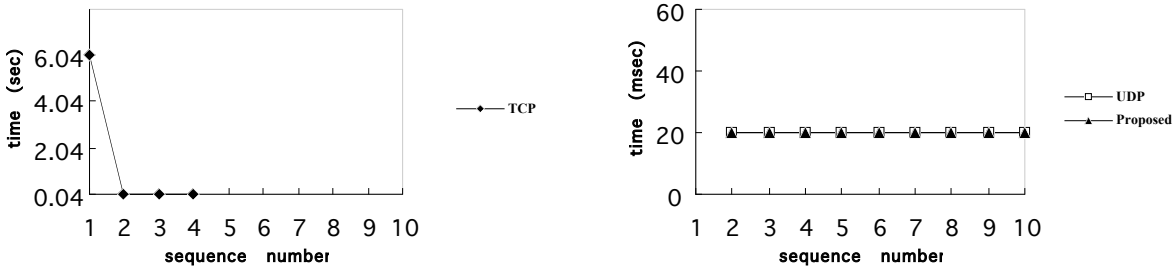
Figure A3-5(c) shows the result under the transmission rate 20 Mbit/s of the source S2. From the Figure A3-5(c) we can see that the packet delay of TCP follows a similar pattern to the results in Figure A3-5(a), while after the packet of the sequence number 3 there are cases that the acknowledged packet has not arrived at the source S1. The packet delay of UDP and the proposed scheme is about 20 ms. In UDP there are packet losses of the sequence numbers 1, 2, 5, and 10. In the proposed method the sequence number is 1.

FIGURE A3-5

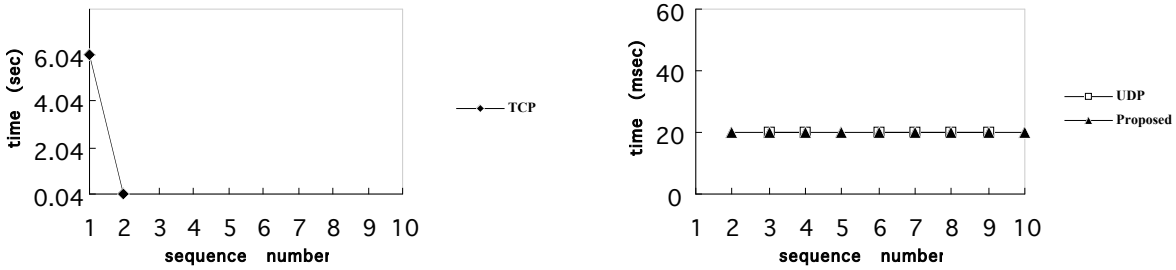
**Packet delay and packet loss under the packet error rate 10%**




(a)




(b)




(c)

# 5 Technical and operational requirements for the internet robot control service protocol

## 5.1 Technical requirements for real-time robot control Internet services in mobile systems

### 5.1.1 Mapping

– UDP protocol should be considered for real-time control of robot as well TCP.

– Retransmission or multi transmission strategies for reliable transmission of robot control data should be considered.

– All the classes of IP addresses should be clearly mapped into proper data link or MAC layer addresses of mobile system, in downlink and uplink.

– Identification and routing schemes within the robot control services network should be provided to support the communication environment.

– Efficient traffic models for robot service should be supported.

– International roaming for overseas mobile users should be supported.

### 5.1.2 Real-time mobile system control channel assignment

– A real-time control channel should be assigned in the data link layer in downlink and uplink for proper robot control data transmission.

### 5.1.3 Robot control protocol procedure

– An appropriate protocol procedure for robot control command transmission at wired links should be supported.

– An appropriate protocol procedure for robot control command transmission at wireless links should be supported.

– A priority field for the IP packet such as 15(Ipv6) should be considered for speedy transmission.

– The local retransmission interval time should be considered and defined such that it enables real-time applications.

### 5.1.4 QoS

– Reliable/best effort real-time robot system control service should be supported. Some of the requirements for QoS should include the end(User)-to-end(Mobile system) QoS.

– Control command data transmission reliability should be maintained even when robot control multicasting is applied.

– Transmission real-time QoS should be supported within the wired links and across wireless links as well.

### 5.1.5 Mobility management

– Seamless handover should be supported.

– Mobility should be supported for IPv4 and IPv6.

## 5.2 Operational requirements for real-time robot control Internet services in mobile systems

### 5.2.1 Functions of network nodes in mobile system

– The nodes should support QoS control according to the number of users, and the robot service provider.

– The nodes should support accounting and authentication.

– The nodes should support a translation function of the IP address, port number and protocol number.

– The nodes should support an encapsulation function with the robot service center.

– IP applications over robot systems should be scalable over the large numbers accessing the service servers.

– Standardized network management interfaces should be supported.

– Power saving capabilities for data transmitting should be supported.

– Paging capabilities for the mobile systems should be supported.

– IP applications over mobile systems can be considered as the distributed architecture: Intelligence distributed in the network (computing) and mobile systems (sensing and action).

– The capability of load balancing should be supported.

### 5.2.2 Applications

– A wide range of services should be supported.

– Many applications for mobile systems over wireless networks can be considered as follows:

  • Multimedia mobile machine tele-control service (tele-operation service): networked home appliance control.

  • Tele-gardening service: Tele-gardening using Internet and a mobile-controlled system (robot)

  • Tele-game service: Network based humanoid robot and mobile robot fighting game

  • Tele-education service: Network based remotely-controlled mobile machine teaching system

  • Tele-babysitting service: Networked mobile system between caller (mother) and receiver (baby).

# Appendix 4

# IP application support in IMT-2000 CDMA multi-carrier

## 1 Introduction

The essential technical and operational characteristics needed to support IP applications over mobile systems are as varied as the applications that may be supported over the Internet Protocol (IP). In the following sections, the basic capabilities required to support IP applications are illustrated and expanded upon to demonstrate how IMT-2000 CDMA multi-carrier supports various multi-media applications.

## 2 Basic capabilities

### 2.1 Introduction

The Internet can be modelled as a collection of hosts interconnected via transmission and packet switching facilities. The most basic technical characteristic in the support of IP applications is the ability to convey data towards its intended recipient. A mobile system is typically involved in the final delivery of data to the intended recipient. This process may be further segmented into the encapsulations of IP packets for transport, and the ability to identify and route to the intended recipient.

### 2.2 Encapsulation

An IMT-2000 CDMA multi carrier system encapsulates the IP packet for transmission of the air interface using the general architecture defined in 3GPP2[3] C.S0001, which includes: the physical layer specified in 3GPP2 C.S0002; the MAC in 3GPP2 C.S0003; the LAC in 3GPP2 C.S0004; and upper layer signalling in 3GPP2 C.S0005.

The High Rate Packet Data Air Interface defined in 3GPP2 C.S0024 supports data rates up to 3.1 Mbit/s in the downlink and 1.8 Mbit/s in the uplink. Work is ongoing to support much higher peak data rates by combining up to 15 1.25 MHz channels.

### 2.3 Address management

In IMT-2000 CDMA multi-carrier, IP addresses are assigned to mobile stations automatically using one of two mechanisms. The first mechanism uses the Point-to-Point Protocol, PPP, see for example IETF RFC 1661 and other references in 3GPP2 X.S0011. The second method uses the Dynamic Host Control Protocol, DHCP, see for example IETF RFC 2131 and other references in 3GPP2 X.S0011.

IP Addresses are typically invisible to subscribers via a mechanism that maps user-friendly names to IP addresses. IMT-2000 CDMA multi-carrier supports the Domain Name System, DNS, for name to address translation, see for example IETF RFC 1035 and other references in 3GPP2 X.S0011.

---

[3] More detailed information is provided at http://www.3gpp2.org.

# 3 Quality of service considerations

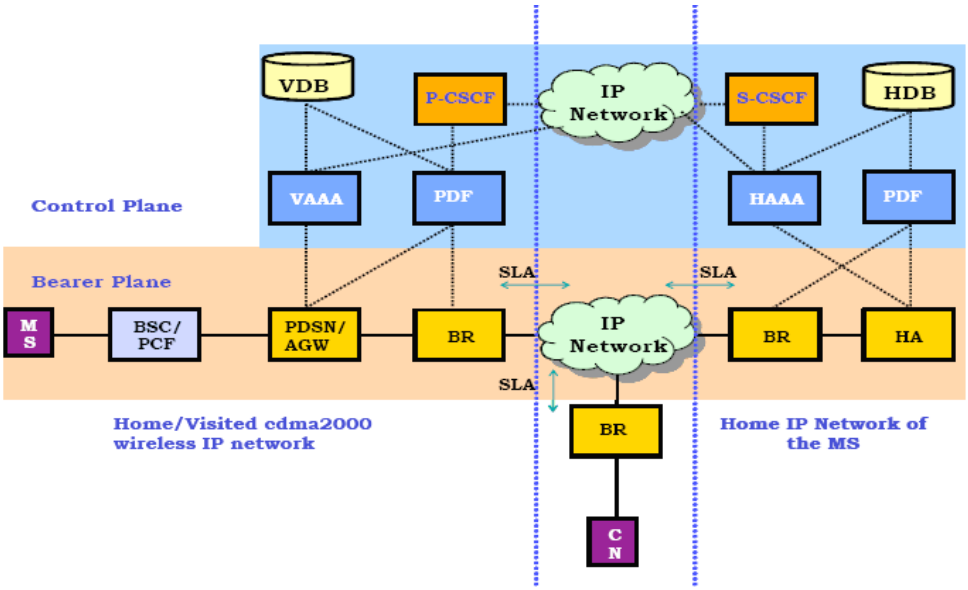
## 3.1 Introduction

The following information provides background information related to Quality of Service (QoS) considerations for an IMT-2000 CDMA multi-carrier wireless IP network and is derived from 3GPP2 S.R0079.

Requirements are defined to enable an IMT-2000 CDMA multi-carrier wireless IP network to provide End to End (E2E) QoS between a mobile station and a correspondent node. The E2E QoS network reference model involves several IP nodes. The two end points are the MS and the correspondent node (CN). The intervening networks span across an IMT-2000 CDMA multi-carrier wireless IP network that includes the radio link, the intermediate IP network, and the Edge IP network of the correspondent node. The E2E reference model can be viewed as a set of consecutive networks. The Figure below depicts an example of the E2E QoS architecture. (Note: the Figure below is for reference purposes only. It does not imply that all network elements shown are necessarily involved with E2E QoS.) E2E QoS may be provided by explicit management of QoS on the consecutive networks, or by provisioning, or a combination of both.

FIGURE A4-1

**QoS reference model**




The availability of E2E QoS functionality in the IMT-2000 CDMA multi-carrier wireless IP network provides the following benefits:

– E2E QoS would enable users to launch a variety of applications and experience their associated benefits in the wireless mobility context.

– E2E QoS would enable IMT-2000 CDMA multi-carrier wireless IP network providers to offer a variety of services and benefit from their associated revenue streams.

The following provides an example of an approach to E2E QoS in the IMT-2000 CDMA multi-carrier wireless IP network: The E2E QoS support in the IMT-2000 CDMA multi-carrier wireless IP network may be provided via one or more instances of a packet data service. The types of instances of a packet data service are identified as a main service instance or an auxiliary service

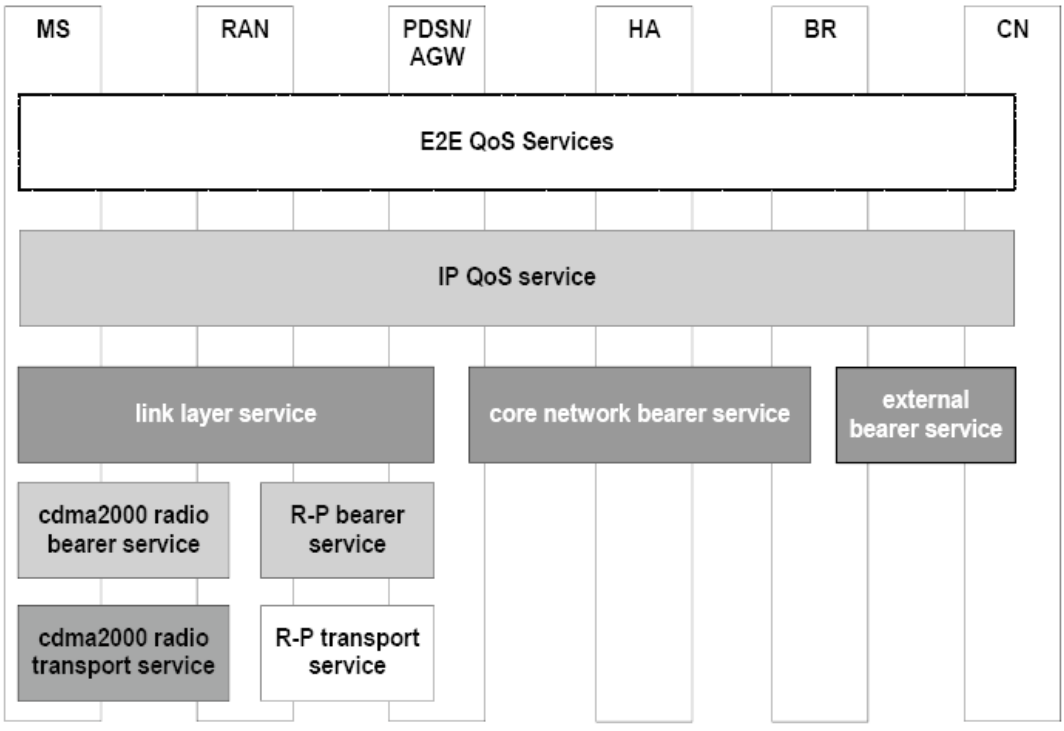
instance. In the IMT-2000 CDMA multi-carrier wireless IP network, the radio resources should be allocated per service instance. In this context the purpose of a main service instance is used to provide resources in the IMT-2000 CDMA multi-carrier wireless IP network to meet the QoS requirements for the applications that may only require Best-Effort QoS support. However, to meet the QoS demands of applications that require better than Best Effort QoS, an auxiliary service instance can be used. The resource allocation for an auxiliary service instance is selective and is based on a characterization of QoS requirements associated with an application. One or more auxiliary service instances may be established by the MS based on the number of applications in use for an MS each requiring different QoS.

## 3.2 The IMT-2000 CDMA multi-carrier E2E QoS bearer services

The E2E QoS support in the IMT-2000 CDMA multi-carrier wireless IP network attempts to reserve the necessary resources to ensure that the requested QoS requirements for a user's application are satisfied. If the necessary resources are not available in the IMT-2000 CDMA multi-carrier wireless IP network, an attempt should be made to negotiate a lower QoS. The following figure shows the different bearer services in a IMT-2000 CDMA multi-carrier network to satisfy subscriber's E2E QoS requests.

FIGURE A4-2

**QoS architecture**




**E2E QoS Service**: The application layer QoS between the end hosts identifies the QoS requirements, for example via SIP/SDP signalling protocol. The QoS requirements from application layer are mapped down to create a network layer session. The mobile terminal then establishes a

link layer connection suitable for support of the network layer session. The QoS parameters received from the application layer are mapped to the corresponding IP layer signalling parameters as well as the link layer parameters.

**IP QoS Service:** In the E2E scenario, the mobile terminal can use the IP QoS service to control the QoS at the local and remote access networks, and DiffServ to control the IP QoS through the backbone IP network. Any IETF defined IP QoS signalling protocol can be used for different services. The entities that are supporting the IP QoS signalling should act according to the IETF specifications for IntServ and IntServ/DiffServ interworking. In addition to provision of E2E QoS Service and via IP QoS Service, QoS requirements may also be determined based on operator local policy/SLA.

**Link Layer Service:** The Link layer service currently does not provide any QoS capability. Support for QoS at the PPP layer (or any other link layer protocol that might be used in the future) is FFS.

**External Bearer Service:** The bearer services provided by the external network. e.g., the IP core network that is not owned and operated by the wireless service providers.

**IMT-2000 CDMA multi-carrier Radio Bearer Service:** IMT-2000 CDMA multi-carrier radio bearer services and their associated QoS parameters are defined in 3GPP2 C.S0017 and 3GPP2 C.S0024-A v1.0. This includes both the assured mode and non-assured mode QoS parameters. This service is enabled by the IMT-2000 CDMA multi-carrier radio transport service.

**R-P Bearer service:** The R-P bearer service is concerned with the QoS guarantee for the following service scenario: The bearer resources are allocated on the R-P interface in an attempt to meet the QoS requirements received from the mobile user as allowed by the network.

**Core network bearer service:** The core network in the IMT-2000 CDMA multi-carrier wireless IP network provides this type of bearer service between PDSN/AGW and BR.

**IMT-2000 CDMA multi-carrier Radio Transport Service:** This service is provided by the IMT-2000 CDMA multi-carrier physical layer that is categorized by the QoS classes and parameters based on the stringent requirements of the physical channels (FCH, DCCH, SCH, etc.). Note that the MAC/Multiplex sublayer has to map the radio bearer QoS parameters (logical channel) onto the physical channel QoS parameters. The radio transport layer service is concerned with the physical radio channel payload data units produced and consumed by the IMT-2000 CDMA multi-carrier radio bearer service plus any signalling associated with those radio channels, e.g., common channel signalling, and call control messages and OAM. The radio transport service QoS should not be dependent on the definition of the radio bearer service QoS, or any higher-layer QoS definitions.

**R-P Transport Service**: The service provided by the R-P transport network to guarantee delivery of the R-P bearer services within their specified QoS limits.

## 4 Supporting mobility

In 3GPP2 X.P0011-C, the requirements and procedures for Mobile IPv4 operation are specified based on a set of RFCs (including RFC 2002). The Mobile Station (MS) is able to use either a static Home Address or a dynamically assigned Home Address belonging to its Home Agent (HA) in the MS's home IMT-2000 CDMA multi-carrier network. The MS has a static HA address assigned regardless of whether the MS has a static or dynamic Home Address. The MS is able to maintain the Home Address persistent throughout the packet data session even when handing off between radio networks connected to separate PDSNs.

Mobile IPv4 operation is enhanced to support the scenario where the MS requests dynamic HA assignment in addition to dynamic Home Address assignment. A fast handover in the context of an inter-PDSN handover enables the MS's data traffic to traverse through the anchored PDSN even when the MS has moved to a radio network connected to a new serving PDSN. A tunnel is established between the anchored and serving PDSNs to transport the MS's data traffic. The fast handover minimizes data loss when the MS is handing off between radio networks connected to separate PDSNs.

Work is ongoing towards 3GPP2 X.P0011-D, in which the requirements and procedures for Mobile IPv6 operation are specified based on a set of IETF RFCs (including RFC 3775). The MS is able to use either a static or dynamically Home Address and/or HA. The MS is able to maintain the Home Address persistent throughout the packet data session even when handing off between radio networks connected to separate PDSNs. Mobile IPv6 operates in two distinct operation modes: Bi-directional tunnel mode and Route Optimized mode. If bi-directional tunnel mode is used, all the MS's data traffic traverses through the MS's HA. If Route Optimized mode is used between the MS and a corresponding node, the data traffic exchanged between the two by-passes the HA and thus avoids the so-called triangular routing.

## 5 Security considerations

### 5.1 Introduction

There are several security issues related to supporting IP applications whether the applications are runover a mobile system or not.

### 5.2 3GPP2 Security features

Each 3GPP2 subscription has a User Identity Module (UIM), which can be either an integral part of the mobile or be removable. The UIM is a secure module that holds subscription information along with cryptographic keys, which are used to provide secure access to the network. For example, for MMD (see section 6), the keys in the UIM are used to provide mutual authentication between the user and network, when a user registers. Keying material derived from this authenticated is then used to integrity protect all further signalling traffic between the mobile and MMD and hence provide the mobile with secured access to services using MMD. The latest release of the specification (currently under development) will also provide confidentiality protection of this traffic.

3GPP2 is also developing a system called the Generic Bootstrapping Architecture. The major aim of this is to provide keying material to secure a variety of applications that run between the mobile and the network. The keying material is derived from the cryptographic keys that are already on the UIM.

## 6 Service architecture

### 6.1 Introduction

The service architecture provides a secure, extensible framework under network operator control.

### 6.2 MMD overview and references

3GPP2 has adopted the IP Multimedia Subsystem (IMS) as the basis for the service architecture. 3GPP2's Multi-Media Domain (MMD) includes IMS and the IMT-2000 CDMA multi-carrier packet data network. The 3GPP2 MMD network provides third generation capabilities and is based

on IETF protocols, including SIP, SDP, Diameter, and Mobile IP. It describes the system elements, interfaces, protocol specifications and procedures to provide the complete specification for the MMD core network.

### 6.3 MMD and regulatory features

MMD supports features that certain administrations may require, such as lawful surveillance of signalling and bearer traffic. MMD will also be extended to support VoIP with GPS-assisted position location for emergency services. IP applications over mobile systems should support the relevant specifications in this area.

## 7 Inter-working

### 7.1 Introduction

With the goal of providing a seamless user experience, IMT-2000 CDMA multi carrier extends support for IP applications to other wireless systems.

### 7.2 Wireless Local Area Networks

IMT-2000 CDMA multi-carrier supports inter-working with Wireless LAN networks, with the intent of extending support for IP applications to the Wireless LAN environment while maintaining authentication and accounting aspects. The work has involved cooperation with IETF, and initial publication of 3GPP2 X.S0028 is pending completion of the RFC process in the IETF. Work is continuing to enhance the user experience with access to native services and seamless handover.

### 7.3 GPRS

Support for IP applications is extended to a subscriber that has roamed into a GPRS network via the protocols and procedures defined in 3GPP2 X.S0034.

## 8 Spectral efficiency

The cost and limited availability of spectrum requires that the wireless technology transporting the IP traffic be as efficient as possible.

At the physical layer the measure of spectral efficiency is bits per second/Hz of spectrum used. Optimizing this requires a careful design of the system to minimize overhead and exploit the different QoS requirements of IP applications, the variability of the wireless channel, and the mobility of multiple users in the network. The IMT-2000 CDMA multi-carrier air interface is designed to do this by making use of multi-user diversity and intelligent schedulers.

Outlined in 3GPP2 C.S0024-A v1.0, IMT-2000 CDMA multi-carrier technology allows schedulers to quickly and efficiently favour users where the network is able to deliver more overall throughput while meeting the QoS requirements of users currently in less favorable radio conditions. Recognizing that IP applications require different levels of QoS, the IMT-2000 CDMA multi-carrier system design allows the scheduler to exploit this range of requirements and the variation in the wireless channel conditions among multiple users to maximize the delivery of throughput in the given spectrum. The system also allows the operator to dynamically balance throughput of a sector with delivered QoS requirements (e.g. throughput vs. latency).

Above the physical layer, the spectral efficiency for IP applications is maintained by using protocols with low overhead such as compression protocols. In particular, IP header compression protocols for IP multimedia such as RObust Header Compression, specified in IETF RFC 3095 and IMT-2000 CDMA multi-carrier-optimized header compression with zero-byte overhead detailed in 3GPP2 C.S0047-0 v1.0 are incorporated into the IMT-2000 CDMA multi-carrier system for this purpose.

## 9 Example multi-media applications

This section identifies a non-exhaustive list of IP applications that are supported by the IMT-2000 CDMA multi-carrier system standards.

### 9.1 Web-surfing

The QoS requirements for web-surfing generally require bursts of high-bandwidth while allowing for up to 1-2 seconds of latency. As further detailed in 3GPP2 C.S0024-A v1.0, IMT-2000 CDMA multi-carrier EV-DO system exploits the lax latency requirement of this kind of application to improve the overall throughput of the system. The scheduler is able to efficiently choose from among many users in diverse and varying radio conditions to favour those that maximize sector throughput while meeting the latency constraints for all web surfing users.

### 9.2 Voice-over-IP

The IMT-2000 CDMA multi-carrier system provides a range of service options and technologies for packetizing VoIP traffic that achieve the above advantages while carrying VoIP traffic over the air interface. The IMT-2000 CDMA multi-carrier 1x service options outlined in 3GPP2 C.S0063-0 v1.0 provide the same level of latency over the air interface as conventional circuit switched services while eliminating IP header overhead in the VoIP media traffic. The conventional IMT-2000 CDMA multi-carrier circuit-switched voice services already provide good capacity by supporting variable rate frames. The IMT-2000 CDMA multi-carrier 1x VoIP service option 61 provides this same capacity while supporting supplementary services carried over IP described in advantage 2 above.

The IMT-2000 CDMA multi-carrier EV-DO standard, 3GPP2 C.S0024-A v1.0, allows the network operator to trade off VoIP latency vs. sector throughput/voice capacity while sharing the same spectrum with other non-VoIP data applications. ROHC is also supported by the IMT-2000 multi-carrier system to reduce the IP overhead of the VoIP media traffic over IMT-2000 multi-carrier EV-DO.

The end-to-end system design for IMT-2000 CDMA multi-carrier VoIP services are described in 3GPP2 X.P0039-0 v1.0.

### 9.3 Streaming audio and video

The IMT-2000 CDMA multi-carrier standard 3GPP2 X.S0011-D provides procedures for the applications to reserve necessary bandwidth and jitter requirements with the radio network.

3GPP2 C.P0046-0 v1.0 describes how these multimedia streaming services are transported over IMT-2000 CDMA multi-carrier in a means that interoperates with general Internet streaming services.

### 9.4 Digital video telephony

The IMT-2000 CDMA multi-carrier EV-DO system is designed to allow an intelligent scheduler to provide the high bandwidth within the jitter and latency requirements while maximizing the sector throughput under such constraints. Since video telephony requires significant resources it is very important that the system be designed well for this application to minimize the impact on the system capacity and support a reasonable number of video telephony users.

The end-to-end system design for IMT-2000 CDMA multi-carrier Video Telephony services is defined in 3GPP2 X.P0039-0 v1.0.

## 10 Conclusion

In conclusion, significant support exists, and work is ongoing in 3GPP2 to enhance support of IP applications over mobile systems. This Appendix has focused on the key high-level operational and technical characteristics required to support such IP applications over mobile systems including the basic capabilities necessary to support mobility over IP, the Quality of Service features which can be implemented, Service Architecture, Inter-working and the ability to support multimedia applications such as Voice-over-IP.

## 11 References

### 11.1 IETF

IETF RFCs are available from the IETF web site, http://www.ietf.org/rfc.

RFC 791, Internet Protocol, Sept. 1981.

RFC 793, Transmission Control Protocol, September 1981.

RFC 1035, Domain Names - Implementation and Specification, November 1987.

RFC 1661, The Point-to-Point Protocol (PPP), July 1994.

RFC 2068, Hypertext Transfer Protocol -- HTTP/1.1, January 1997.

RFC 2131, Dynamic Host Configuration Protocol, March 1997.

RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, December 1998.

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

### 11.2 3GPP2

Relevant 3GPP2 Technical Specifications are listed below without version numbers. The most recent versions are available from the 3GPP2 web site:
http://www.3gpp2.org/Public_html/specs/index.cfm.

3GPP2 A.S0019, Interoperability Specification (IOS) for Broadcast Multicast Services (BCMCS)

3GPP2 C.S0001, Introduction to cdma2000 Spread Spectrum Systems - Revision D.

3GPP2 C.S0002, Physical Layer Standard for cdma2000 Spread Spectrum Systems.

3GPP2 C.S0003, Medium Access Control (MAC) Standard for cdma2000 Spread Spectrum Systems.

3GPP2 C.S0004, Signalling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum Systems.

3GPP2 C.S0005, Upper Layer (Layer 3) Signalling Standard for cdma2000 Spread Spectrum Systems

3GPP2 C.S0017, Data Service Options for cdma2000 Spread Spectrum Systems

3GPP2 C.S0024, cdma2000 High Rate Packet Data Air Interface Specification.

3GPP2 C.S0032, Recommended Minimum Performance Standards for cdma2000 High Rate Packet Data Access Network.

3GPP2 C.S0033, Recommended Minimum Performance Standards for cdma2000 High Rate Packet Data Access Terminal

3GPP2 C.S0037, Signalling Conformance Specification for cdma2000® Wireless IP Networks.

3GPP2 C.S0039, Enhanced Subscriber Privacy for cdma2000® High Rate Packet Data.

3GPP2 C.S0047, Link-Layer Assisted Service Options for Voice-Over-IP: Header Removal (SO 60) and Robust Header Compression (SO 61).

3GPP2 C.S0054, cdma2000® High Rate Broadcast-Multicast Packet Data Air Interface Specification.

3GPP2 C.S0063 cdma2000 High Rate Packet Data Supplemental Services, March 2005.

3GPP2 X.P0039, Packet Switched Voice (over IP) and Video Telephony Services End-to-end System Design Technical Report.

3GPP2 C.S0046, 3G Multimedia Streaming Services.

3GPP2 S.R0037, IP Network Architecture Model for cdma2000® Spread Spectrum Systems.

3GPP2 S.R0086, IMS Security Framework

3GPP2 X.S0011, cdma2000 Wireless IP Network Standard: Introduction.

3GPP2 X.S0011, cdma2000 Wireless IP Network Standard.

3GPP2 X.S0013, IP Multimedia Subsystem (IMS).

3GPP2 X.S0028, cdma2000 Packet Data Services; Wireless Local Area Network (WLAN) Inter-working.

3GPP2 X.S0034, cdma2000/GPRS Roaming.

# Appendix 5

## The path of IP applications over mobile systems

There is a traditional relation between the existed PLMN, PSTN, and IP network, illustrated in Figure A5-1. The IP network mainly deals with data communications. That is from Recommendation ITU-R M.1079 (Performance and quality of service requirements for IMT-2000 access networks).

FIGURE A5-1

**End-to-end system**

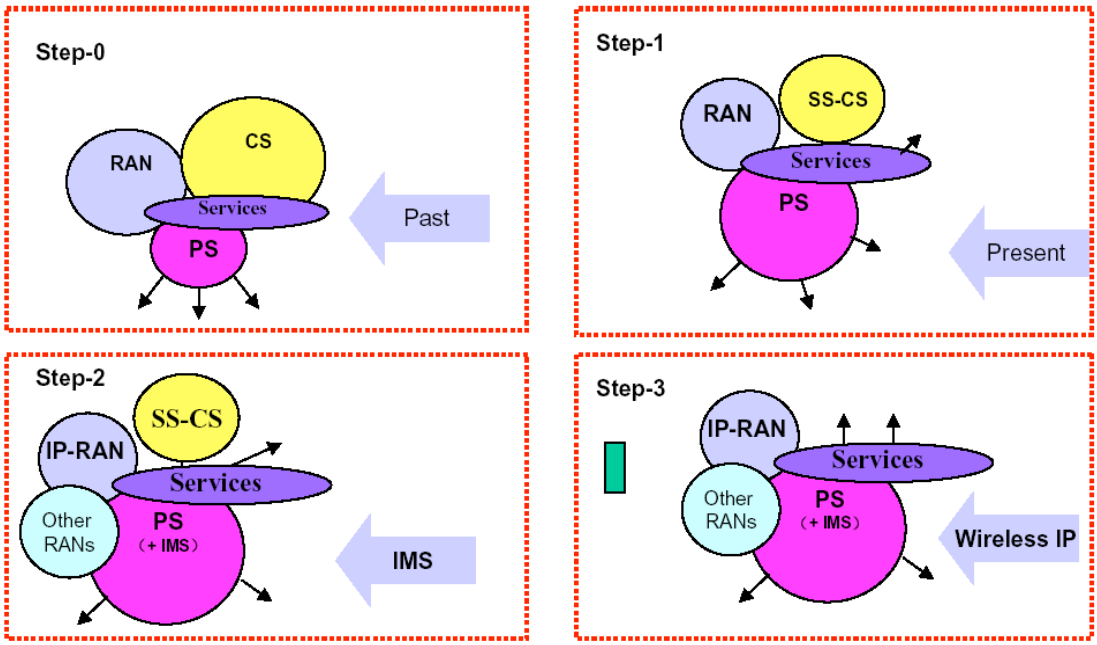

Modern digital technology allows different sectors, e.g. wireline telecom, data, wireless telecom, to be merged together. This convergence is happening on a global scale and is drastically changing the way in which both people and devices communicate. At the center of this process, forming the backbone and making convergence possible, are IP-based networks. IP-based systems offer significant advantages to operators and subscribers, from connectivity across a variety of devices, networks and protocols, to greater flexibility in the management, use and cost of network resources. IP is the guarantee of openness of the beyond 3G, which can merge data, voice and multimedia. All the components use IP protocols to provide transport for all types of bearer and signalling information in All-IP network. However, the transformation of the current mobile network to All-IP network architecture cannot happen overnight. IP network is enlarging into the mobile network and fixed network gradually.

For current mobile network, there are core network including Packet Switch (PS) domain, Circuit Switch (CS) domain, Service Deliver Platform (SDP) domain, and radio access network (RAN) domain. Up to now, PS domain and SDP domain have already applied IP technologies, as shown in Figure A5-2. It supports simultaneous use of the circuit-switched voice services and the packet-switched session services. Recently, IP is being utilized to both the carrier network and the signalling network in CS domain gradually, such as R4 in 3GPP and LMSD in 3GPP2. The key enhancements are Transcoder Free Operation (TrFO) and SIGTRAN. In general, there is no big problem if the special IP carrier network, e.g. CN2 of China Telecom, is deployed. The new bearer and signalling interfaces will gently be supported. An IP signalling network would replace the old SS7 telecommunications protocol, IP networks use some bandwidth-expensive mechanisms to achieve reliability.

…

FIGURE A5-2

**IP Evolution in mobile networks**




An individual user can be connected via a variety of different radio access systems to the networks. The interworking between these different access systems could be realized through a common IP-based core network with "optimally connected anywhere, anytime" manner. This IP-based core network shall be open to any service currently used and to be used in the future. The IMS (IP Multimedia Subsystems) based on SIP protocol of an IETF protocol is suggested to be access technology-agnostic so that the IMS may be implemented to not only IMT-2000 access technologies but also other IP access technologies.

– Non-IP-based systems (voice delivery) e.g. GSM, CDMA2000 and WCDMA {2 GHz, WAN, Seamless, Voice/Data, Handset/Computer}.

– IP-based systems (data services) e.g. 802.11 WiFi {2.4 GHz, LAN, Hotpoint, Data/VoIP, Computer/Handset}, and 802.16 WiMax, 802.20 WBMA.

**Consideration of IP RAN**

An All-IP based B3G wireless network has intrinsic advantages over its predecessors. IP tolerates a variety of radio protocols, and lets you design a core network that gives you complete flexibility as to what the access network is. The core network provider can support many different access technologies, WCDMA, CDMA2000, Bluetooth, WiFi, WiMax, and some that we haven't even invented yet, such as some new CDMA protocols.

High rate access technologies, e.g. HSDPA/HSUPA and EV DO A/B, require the IP transmission over RAN. Combination of fixed and mobile access is called Connectivity access network (CAN).

IP wireless environment would further reduce costs for service providers by ushering in an era of real equipment interoperability. Wireless service providers would no longer be bound by single-system vendors of proprietary equipment. Future CAN will be integrated with all IP core network to

interwork with other RANs including legacy RANs. Generally, 3G systems are regarded as non-IP based wireless access. But IP RAN emerges in R5 of 3GPP and EV DO of 3GPP2. SDOs are doing a study on access network re-design to support an IP based access network.

Generally, the RAN has the following features:

– IP RAN architecture becomes flat, all with IP bearing.

– Districted control makes some function reconfigure, e.g. the functions of RNC is weaken, its functions give to BTS.

– Maximize synergy among various transport infrastructure elements e.g., gateways, routers, etc.

– Intelligently splitting control and user planes to dynamically allocate capacity based on service demands.

FIGURE A5-3

**IP vision**

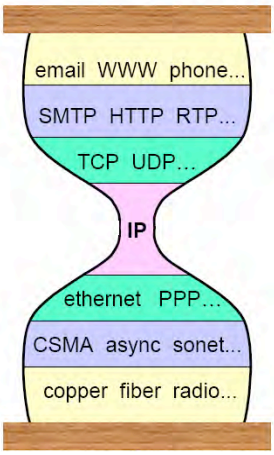



Figure A5-3 shows the vision of everything over IP and IP over everything. Everything over IP means IP network can bear various services. IP over every thing means IP may be transported over various media, such as fiber and radio.

**IP over air interface**

Dedicated allocation of physical resource such as circuit-switching transmission may take an advantage in terms of QoS guarantee but this causes inefficiency for low data rate or silent period of variable data rate services due to waste of radio resources. Then data for the services can be divided into IP packet, and each is transmitted through wireless medium.

Unfortunately, normal IP headers contribute a large overhead to the payload; for example, for VoIP, a packet has a total IP/UDP/RTP header size of 40 octets in IP v4 and 60 octets in IP v6. The size of the payload may be as low as 15-20 octets. Then the need to reduce header size for efficiency is obvious, especially for wireless links. Several methods (e.g. RFC2507/2508) have been proposed to reduce the header size. However, wireless links have characteristics that make header compression less efficient. They have to be robust enough to perform well in an environment with high bit error and packet loss rates. Robust header compression (ROHC) was proposed to conserve bandwidth in

the narrow radio spectrum, reduce the packet loss rate over unreliable wireless link, and then to improve voice quality. This compression method was defined in the ongoing RFC3095, as part of the so-called packet data convergence protocol (PDCP) layer. All these tend to make IP spectrum efficient from the inefficient state.

For IP mobile network, there exist mobility and handover problems:

– Mobile IP supports macro mobility well. IETF proposes the Cellular IP to realize micro and pico mobility as the complement of the Mobile IP.

– A handover in any IP-based mobile network is a complex procedure. Typically, it takes quite a long time before the new access router gets the parameters describing the flow states associated with an incoming mobile node, trying to enable media independent seamless handover of a data session between 802.3/11/16, 3GPP, and 3GPP2. It is more difficult to attempt CS to VoIP seamless handover. Since mobile Internet will be always-on, operators realize the need for IP v6 addressing due to limited IP v4 address availability. In the future, both IP v4 and IP v6 users have to be accessed to applications and services on IP v4 networks.

# Appendix 6

# Support of IP protocol with DECT

## 1 Introduction

This Appendix describes the 2 basic ways in DECT to support IP services.

1) Interwork the IP protocol in the fixed part as specified in TS 102 265, DECT access to IP based networks.
2) Transparent transport of the IP packets across the air interface as specified in EN 301 649, DECT Packet Radio Service (DPRS).

The case (A) is described in section 2 and the case (B) is described in section 3 of this Appendix.

## 2 DECT access to IP based networks

The TS 102 265 profile specifies the DECT interworking with IP networks. The profile specifies in particular DECT interworking with Session Initiation Protocol (SIP) and Mobile IP service. It is based and develops further the findings of the TR 102 010.

In regard to Mobile IP, IP addressing associated with the “Fixed Termination” (FT) and/or with the “Portable Termination” (PT) is specified. In regard to SIP interworking, Voice over IP (VoIP) and multimedia sessions are covered. In the case of voice, the VoIP is terminated in the FT and “normal” GAP based voice is used over the DECT air interface.

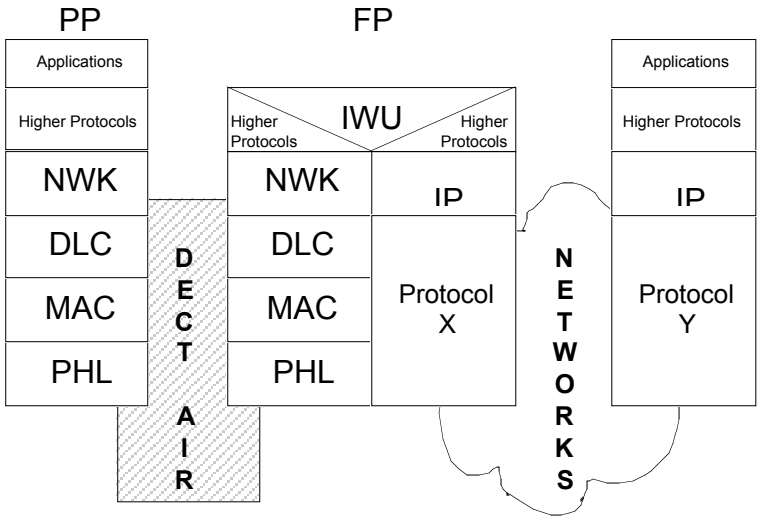
### 2.1 Reference configuration

Figure A6-1 describes the case when the IP protocol is terminated in the FP. This configuration may be preferable especially in the case of a DECT voice IP telephone (this does not exclude messaging or other data only services). Some issues that need consideration here in regard to providing interoperability between FPs and PPs are, e.g. unified way of transmitting the voice samples or other media streams to the PP and interaction with the signalling protocol use by the VoIP (e.g. SIP).

…

FIGURE A6-1

**Reference configuration 2 (IP terminated at the FP)**

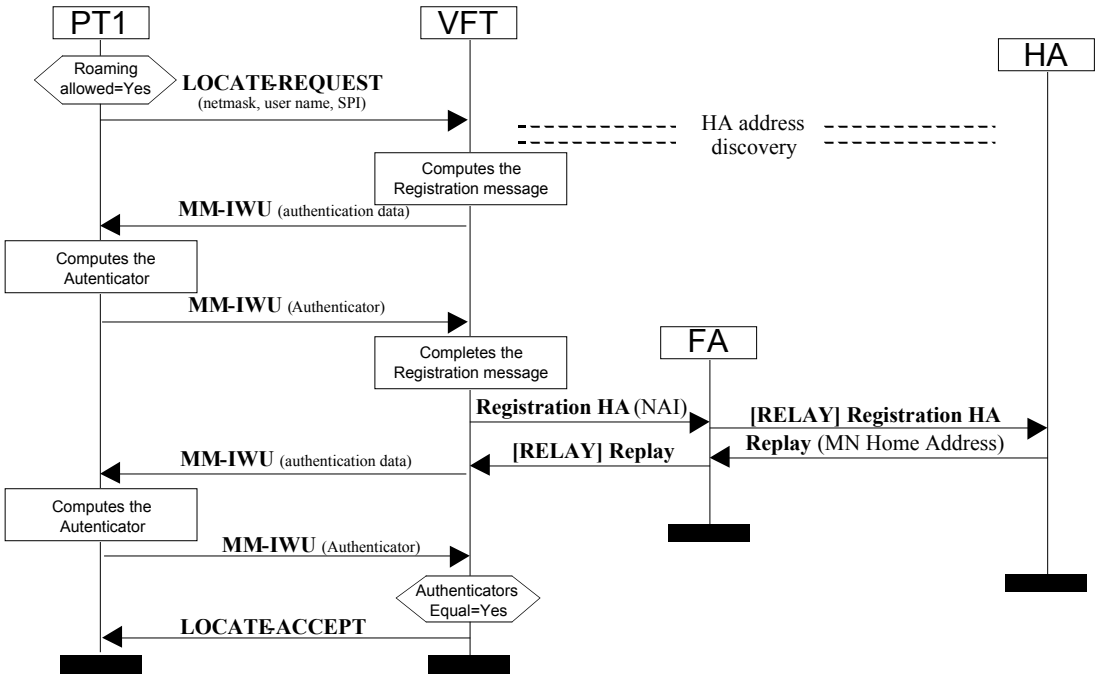



## 2.2 IP-Roaming

The TS 102 265 specifies how the DECT procedures can be used to support roaming based on "Mobile IP". Figure A6-2 shows an example of a complete Portable Part IP roaming registration procedure.

FIGURE A6-2

**Successful PP mobile IP roaming registration (PT auth)**



## 2.3 SIP Interworking

SIP is an application-layer signalling protocol that can establish, modify, and terminate interactive multimedia sessions over IP between intelligent terminals with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. It is a clear text client/server protocol using Uniform Resource Locators (URL) for addressing (in this sense having a lot in common with HyperText Transfer Protocol (HTTP)).

SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types (users may move between endpoints, they may be addressable by multiple names, and they may communicate in several different media - sometimes simultaneously). SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers.

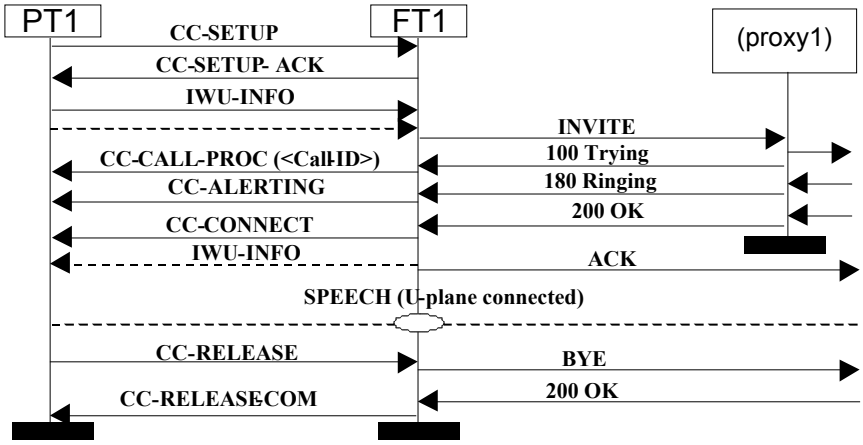
SIP runs on top of several different transport protocols enabling Internet endpoints called user agents (UA) to discover one another and to agree on a characterization of a session they would like to share. For locating prospective session participants, and for other functions, SIP enables the creation of an infrastructure of network hosts (called proxy servers) to which user agents can send registrations, invitations to sessions, and other requests.

A user agent represents an end system. In the context of the TS 102 265 a User Agent comprises a DECT Fixed Part and a DECT Portable Part and the UA activities may be provided either by the Fixed Part or by the Portable Part. As a Fixed Part can serve a number of Portable Parts, each tandem of the Fixed Part and a Portable Part may, but need not, represent an independent UA, i.e. the Fixed Part may be engaged in a number of different UAs, whereas a Portable Part may be engaged only in one UA at a time.

The Figure A6-3 gives an example how DECT can support a SIP session establishment and termination.

FIGURE A6-3

**Successful SIP session establishment and termination Outgoing call (GAP)**



In the case of an incoming (e.g. Voice over IP) call, the attempt of a SIP session establishment (i.e. the arrival of an INVITE message) will be detected at the FT side. This, if the desired session is acceptable, will result into an incoming call establishment towards the PT.

Based on the user's Address-Of-Record (AOR) and the session description (if provided) the FT shall determine which PT to call. If session description is not provided and the user (identified by its AOR) has used multiple PTs (e.g. for different types of media) the FT should ring all PTs and the one that the user answers first should determine the session media description. Alternatively a PT may be chosen as a default.

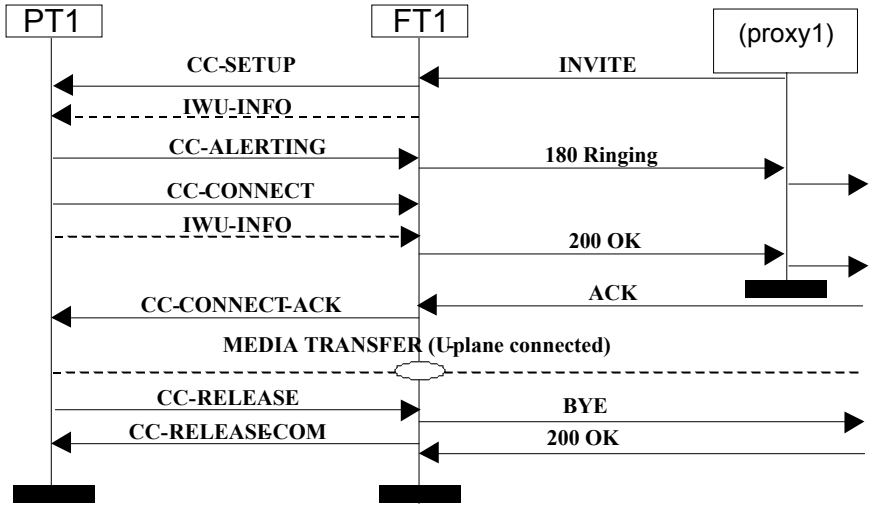
When accepting the call the user may, if media description is suggested, accept or suggest modification to the type of media indicated in the session description. As soon as all the necessary information is collected the FT shall map it to a 200 OK message.

If session description was first suggested by the called party, the acceptance of it (ACK message) shall be provided into the {CC-CONNECT-ACK} message.

An example of the mapping between the DECT incoming call establishment and release procedures and the SIP session establishment and termination procedures is provided in Figure A6-4.

FIGURE A6-4

**Successful SIP session establishment and termination Incoming call**




## 3 DECT Packet Radio Service (DPRS)

The DECT Packet Radio Service, DPRS, EN 301 649 specifies common features and services for all packet data applications. This profile also serves as a base specification for other data profiles.DPRS does not contain GAP speech functionality but whenever needed (e.g. Call Control and Mobility Management procedures) it refers to the procedures defined in GAP, all additional procedure support necessary for data applications is explicitly specified in DPRS.

Interworking with V.24 interfaces, Ethernet, Token Ring LANs, direct interworking with Internet Protocol (IP) and PPP and, a Generic media encapsulation protocol allowing for various different media protocols to utilize one transport have been defined.

The standard contains specifications for applications for which a high degree of data integrity is necessary and includes connection oriented bearer services. A set of fast suspend and resume procedures is provided to overcome the drawbacks in regard to resource utilization that can be identified in most of the connection oriented service.

DPRS also extends the data stream service into environments, such as public services, where significant mobility is a characteristic. This service may be used to provide interworking with a voice-band modem service over public networks such as PSTN or ISDN.

Annexes to the DPRS specify a set of services that can be provided. There are two types of services:

– Frame Relay Service includes transport of protocols with user-delimited frames. DPRS defines the following frame-relay services:
  1) IEEE 802.3 (Ethernet).
  2) IEEE 802.5 (Token Ring).
  3) Internet Protocol (IP).
  4) Point to Point Protocol (PPP).
  5) Generic media encapsulation protocol.
– Character Oriented service incorporates a packet assembling and disassembling (PAD) functionality to transport a stream data. DPRS incorporates the following Character Oriented services:
  – V.24 (asynchronous data).

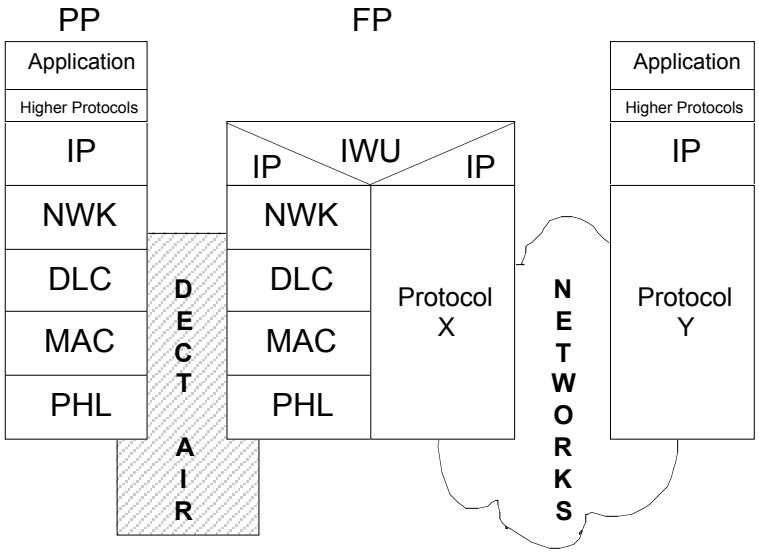
USB interworking is provided as well.

### 3.1 Reference configuration (transparent IP transport)

Figure A6-5 shows the transparent transport of the IP protocol across the Fixed Part and the termination of the IP protocol in the PP.

FIGURE A6-5

**Reference configuration 2 (IP terminated at the PP)**



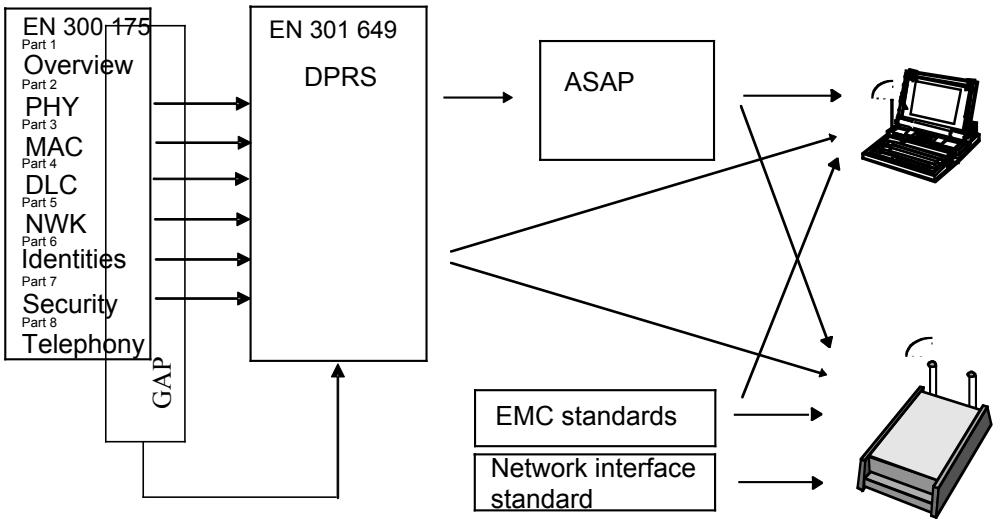
## 3.2 Application Specific Access Profiles

Application Specific Access Profiles (ASAPs) identify a specific application scenario and select a subset of DPRS services for such applications.

The relationship between the standards and DPRS is shown in Figure A6-6.

FIGURE A6-6

**Standards relating to DPRS**




The following 2 subsections describe ASAPs for Ethernet and V.24 Interworking.

### 3.2.1 Ethernet interworking

TS 101 942 defines a data Application Specific Access Profile (ASAP) intended for enterprise, small office and home office (SOHO) and Home (residential/private) markets combining a selection of Ethernet Interworking DECT-DPRS data services. The TS 102 014 specify the Ethernet ASAP Test Specification (PTS) and the TS 102 013 (2 parts) specify the Ethernet ASAP requirement list and profile specific Implementation Conformance Statement (ICS) *pro forma* respectively.

The aim of TS 101 942 is to guarantee a sufficient level of interoperability and to provide an easy route for development of DECT DATA LAN applications.

### 3.2.2 V.24 Interworking

TS 101 947 defines a data Application Specific Access Profile (ASAP) intended for enterprise, small office and home office (SOHO), and, home (residential/private) markets combining a selection of V.24 Interworking DECT-DPRS data services. The TS 102 012 specify the V.24 ASAP Test Specification (PTS) and the TS 102 011 (2 parts) specify the V.24 ASAP requirement list and profile specific Implementation Conformance Statement (ICS) pro forma respectively.

The aim of TS 101 947 is to guarantee a sufficient level of interoperability and to provide an easy route for development of DECT DATA simple cable replacement applications.

## 4 Summary

This Appendix gives a brief description how DECT can support IP applications and which DECT standards have been developed in this area. It has been demonstrated, that DECT is suitable for supporting VoIP and SIP. The transport medium is used very efficiently. Both methods, the transparent transport and the interworking of IP, are specified.

# Appendix 7

## General considerations for mobile system configuration to support Internet protocol (IP) applications

### 1 IP architecture requirements for mobile system

An All-IP architecture for mobile system is in fact quite different from the traditional cellular systems that are defined by the network elements, the interfaces between them, and the protocols that run other those interfaces. The IP approach has very weak interfaces and largely concentrates on protocols - typically one protocol providing a single function - which are developed independently and are not tightly integrated to either each other or a particular underlying network structure. Another point is that there are still many blind spot that IP technology currently cannot fill - areas where work still needs to be done to replicate some of the functionality of the tightly integrated/proprietary standards of mobile system.

The architecture of mobile wireless Internet principles would be as follows:

- Embrace internet technologies and services.
- Separation of concerns (service from delivery):
  - Separation of transport and signalling.
  - Separation of mobility management from session control.
  - Aid Operators/ISPs ability to independently upgrade sub-systems.
  - Allow Operators/ISPs to build multi-vendor systems.
- Open all pertinent interfaces:
  - including RAN internal interfaces, core network interfaces.
  - floating transcoder function (not tied to radio access network).
- Independence of wireless access technology:
  - Extend IP transport of traffic and control to BTS.
  - Provide IP end-to-end from terminal for data applications.
  - Inter-technology mobility management (separate mobility management function).
- Global alignment:
  - Eliminate regional/country differences in key interfaces.
  - Globally accessible services.

Interoperability with 2G and non-IP networks and services

- Harmonization across access technologies:
  - Extends from Wireless to Wireline, xDSL, Cable, etc.
- Distributed architecture:
  - Intelligence distributed in the network and end points.
  - Scalable.
- Performance, Quality, Reliability:
  - End-to-end QoS mechanism for any given service.

– The seamless deliverable capability of QoS based on mobile IP, as the terminal moving on different radio networks, the grades of QoS and applied services should be guaranteed based on seamless frequent handover.

– The capability of load balance based on parameterized QoS, with the balance status changing because of the number of balances and intensity twitter of services, it is essential to achieve equilibria of balances in different radio networks.

- Security:
  - Support mutual authentication, confidentiality, integrity and non-repudiation
- O&M:
  - Standardized, compatible network management interfaces.
  - Flexible accounting and billing.
- Services:
  - Support wide range of services, including real-time, non-real-time, multi-media services.
  - Rapid service creation.
  - Support of third party service development.
  - User customization of services.
- Support regulatory requirements:
  - Legal intercept.
  - Number portability.
  - And other regional requirements.

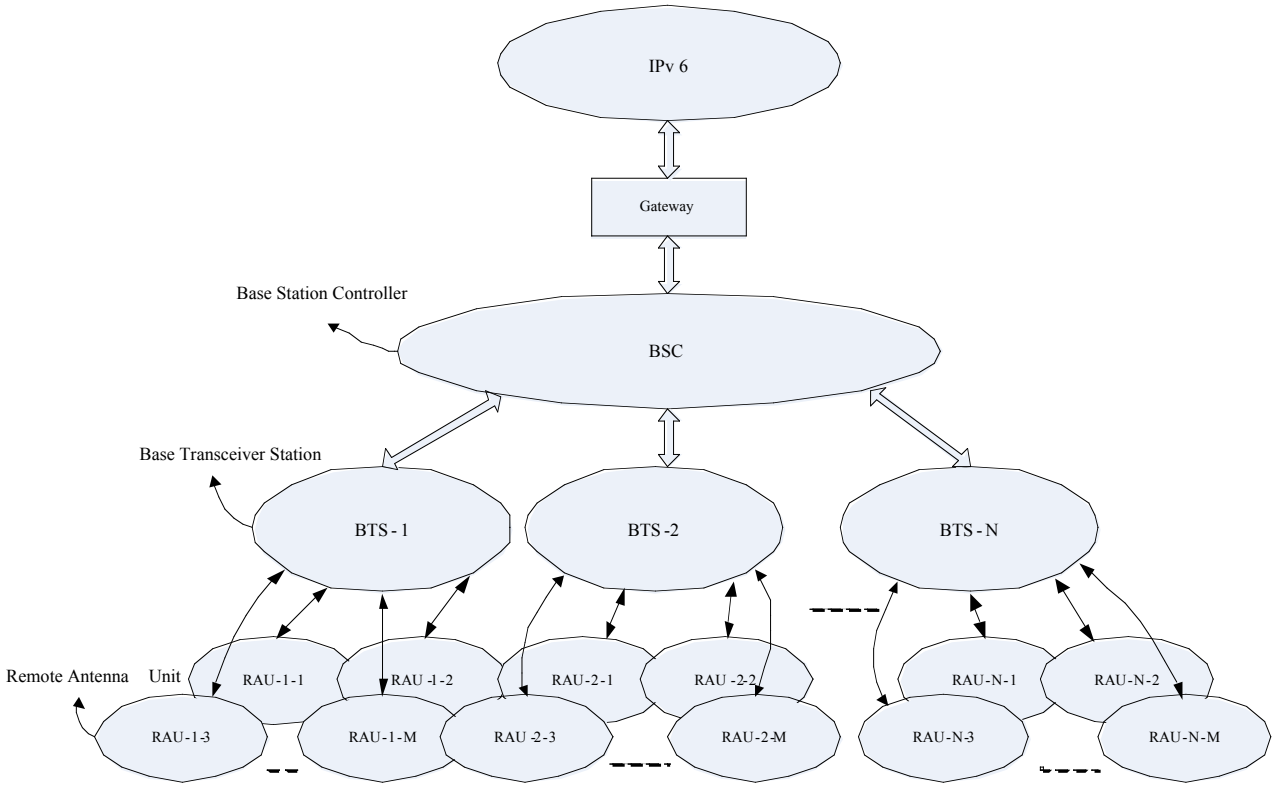
## 2 The architecture of mobile wireless system

Towards meeting the architecture principles, here we give a reference architecture of mobile wireless system as Figure A7-1.

…

FIGURE A7-1

**Architecture of mobile wireless network**




In this mobile wireless network, radio access network mean the traditional cellular mobile wireless network or distributed mobile wireless network .The mobile wireless network would have some characteristics as following:

– Adapting to kinds of multiple accesses (e.g. FDMA, TDMA and CDMA) and prototypes (e.g. IMT-2000, Wi-Fi and WiMAX).

– Resource management is more convenient. Base transceiver station can implement dynamic resource allocation, optimize resource utilizing, which greatly improves spectrum efficiency, and the cell structure by software set-up adapts to different periods of time and service changes in different areas.

– Superior wireless coverage and capacity due to the system's high output power and low uplink noise.

– Industry-leading installation and administrative capabilities.

– Flexible design for handling future technologies and Internet protocols.

– Good cover with the serve district, depressing the handover ratio of the system. When the user moves in a cell, the system needn't handover, though different antennas are utilized.

– Base transceiver station can adjust connecting manners and resource configuration according to service hot spot and service changes. Different antenna groups build up different shapes of serving areas.

– Good separation between the area and the cover after erecting antenna. Agile configuration and adjusted structure through software can meet various services, which makes the heavy network planning easier.

– Base transceiver station and simple remote antenna unit get easy maintenance. At the same time, it enhances the network reliability and economizes cost of maintenance.

## 3 Conclusion

The IP applications related to Core network, RAN, air interface, i.e. for the RAN, should provide the multiplex mobile access configuration. Furthermore, user convenience is highly upgraded, and service providers and network administrators can easily configure the local information network, due to the reduction of traffic of Internet and server, and burden of IP address management.

# Appendix 8

## Use of IEEE 802.16 access networks to support IP applications over mobile systems

### 1 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 Broadband Wireless Access (BWA) systems supporting multiple services. Included is support for subscriber stations moving at vehicular speeds to specify a mobile 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 Appendix summarizes the relevant capabilities of the IEEE 802.16 standard based on the outline of the sections in the main body of the Report, 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 Appendix 9.

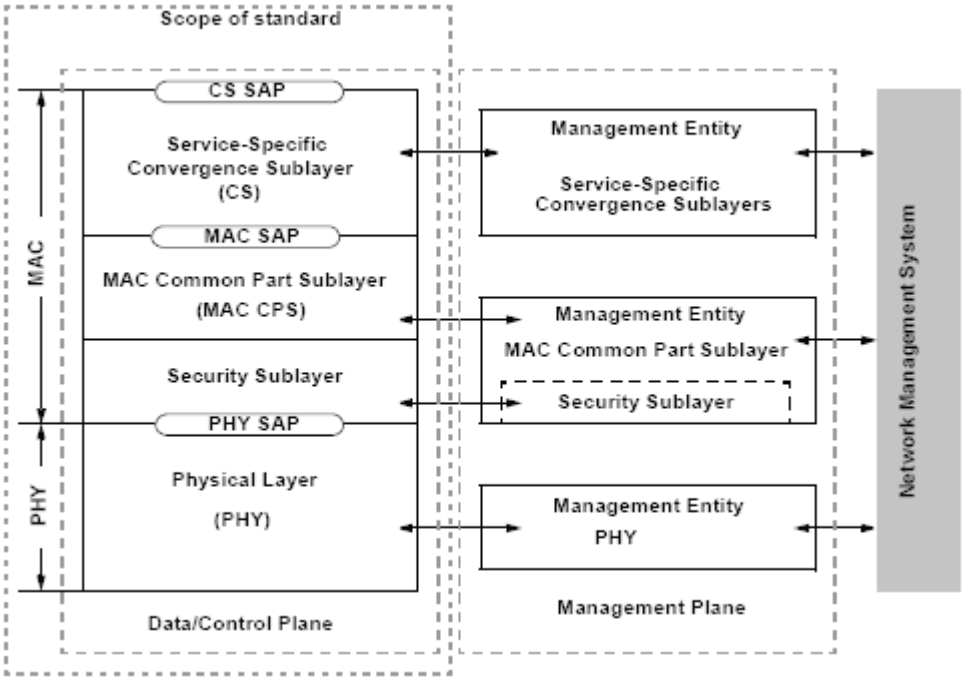
### 2 Scope and structure of IEEE 802.16 standard

Figure A8-1 illustrates the reference model and scope of this standard. The Medium Access Control (MAC) layer comprises three sublayers. The Service-Specific Convergence Sublayer provides any transformation or mapping of external network data, received through the Convergence Sublayer 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 Convergence Sublayer specifications are provided for interfacing with various protocols. The internal format of the Convergence Sublayer payload is unique to the Convergence Sublayer, and the MAC CPS is not required to understand the format of or parse any information from the Convergence Sublayer payload.

…

FIGURE A8-1

**IEEE Std 802.16 protocol layering, showing SAPs**




## 3 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 Convergence Sublayer (required to support IP applications) resides on top of the IEEE Std 802.16 MAC CPS. The Convergence Sublayer 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 Convergence Sublayer PDU to the MAC SAP associated with the service flow for transport to the peer MAC SAP.

d) Receipt of the Convergence Sublayer PDU from the peer MAC SAP.

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

The sending Convergence Sublayer 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 Convergence Sublayer is responsible for accepting the MAC SDU from the peer MAC SAP and delivering it to a higher-layer entity.

The packet Convergence Sublayer is used for transport for all packet-based protocols.

## 4 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.

## 5 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.

## 6 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.

For interworking to Internet services, the relationship between IP address and CID should be specified.

## 7 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 IP header-compression Convergence Sublayer PDU format.

The following parameters are relevant for IEEE Std 802.3/Ethernet Convergence Sublayer 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 (i.e. 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.

## 8 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.

## 9 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 Neighbour BS information acquired from a decoded message, or may make a request to schedule scanning intervals or sleep-intervals to scan, and possibly range, Neighbour 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 2 “Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands” and Corrigendum 1.

[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.

# Appendix 9

# WiMax Forum Mobility Profiles for support of IP applications over mobile systems

## 1 Introduction

IEEE 802.16™ is an emerging suite of standards for Broadband Wireless Access (BWA). IEEE Std 802.16e-2005, an amendment to the IEEE 802.16-2004 ™ base specification, enables combined fixed and mobile operation in licensed frequency bands under 6 GHz. Mobility supported system for WiMAX is called mobile WiMAX (including WiBro). This combination of IEEE Std 802.16-2004 and the 802.16e-2005 amendment is designed as a high-throughput packet data network radio capable of supporting several classes of IP applications and services based on different usage/mobility and business models. To allow such a diverse combination of usage, mobility, and deployment models, the IEEE 802.16-2004 and 802.16e-2005 air interface is designed with a high degree of flexibility and an extensive number of options.

## 2 MAC and PHY functional requirements

All requirements in this clause apply to both BS and MS unless otherwise stated and captures the requirements for QoS and Services support for mobility profiles.

### 2.1 Service class and applications support

The Basic Mobility Profile set shall include all scheduling services and data delivery services defined in IEEE802.16-2004 and 802.16e-2005 so that the following application types can be supported efficiently:

– Real-Time Applications, One-way Streaming, and Conversational Applications, e.g., Audio/Video Streaming, Video Telephony/Conferencing, Interactive Gaming.

– Non-Real-Time Applications, e.g., Web Browsing, FTP, Email, Instant Messaging.

All the capabilities needed to efficiently support VoIP are required at the MS and at the BS.

– When VoIP is supported the system shall use all those features defined in IEEE802.16-2004 and 802.16e-2005 that are needed to ensure the quality of service and capacity for VoIP services.

– When VoIP is supported, specifically silence suppression and header compression suppression should be supported.

### 2.2 Multicast and broadcast services support

– All BSs and MSs should support the Multicast and Broadcast Services (MBS) feature and both single BS transmission and multi-BS simulcast transmission should be supported by the mobility profiles.

– In future releases all BSs and MSs shall support the Multicast and Broadcast Services (MBS) feature and both single BS transmission and multi-BS simulcast transmission shall be supported by the mobility profiles.

### 2.3 QoS control

– The Basic Mobility Profile Set shall include all features and parameters needed for applications level QoS differentiation. Such differentiation shall apply to different applications and packet flows from the same IP address.

– The Basic Mobility Profile Set shall include all features and parameters needed for user-level QoS and Priority differentiation.

## 3 Power saving, idle mode, and paging requirements

– The Basic Mobility Profile Set shall optimize power saving capabilities for all scheduling services and data delivery services, as enabled by any combination of Sleep and Idle Modes.

– The Basic Mobility Profile Set shall include paging capability for all devices.

– The parameters associated with Sleep and Idle modes and Paging shall be defined and adjustable over wide ranges to support the needs of different device types and usage models.

## 4 Security requirements

The WiMAX Forum™ Mobility Profiles shall use security options defined in IEEE 802.16e-2005 to meet the following general requirements:

### 4.1 Threat classes

The basic assumptions that apply to all security threat classes below include the wide availability of commodity MS and BS systems and components, and the wide availability of knowledge on protocols, security measures, and tools.

– Theft of Service: Acquisition of network connectivity and other services without proper authorization and without being detected real-time or in auditing.

– Privacy Compromise: Access to user traffic over wireless links without proper authorization, in real time or via offline analysis.

– Man in the Middle (MitM) attack: Impersonation of the BS to the Subscriber, or two-way impersonation between the BS and the Subscriber. Although MitM is more of an attack method than a threat, it is listed here for clarity in later sections.

– Protocol Denial of Service (DoS): Disruption or degradation of correct protocol operation or exhaustion of system resources by injection, shaping, dropping, shuffling or modification of management traffic. Protocol DoS attacks include, for example, water torture" attacks which force the reception and decoding of unnecessary packets to run down system resources, battery power, etc.

– Device integrity and compliance compromise: Change or violation of device compliance with a certified profile and supported extensions without being detected while or after accessing legitimate network services.

### 4.2 Device authorization

– The WiMAX Forum™ Mobility Profiles shall provide device authorization that provides assurance (via an 802.16e-2005 X.509 device certificate) that the device has been manufactured by a specific recognized WiMAX vendor. The 802.16e-2005 X.509 device certificate shall be unique to each MS.

### 4.3 WiMAX Forum mobility profiles

– In addition to the X.509 device certificate, the MS may have other device credentials installed during provisioning for use in network entry. The additional credentials, if installed, shall be suitable for PKMv2 secure EAP method satisfying the requirements in IETF RFC 3748 and the mandatory criteria listed in Section 2.2 of RFC 4017.

– The method used by the EAP server shall perform mutual authentication in compliance with the PKMv2 specifications. PKMv1 shall not be supported. EAP methods satisfying the requirements of IETF RFC 3748 and the mandatory criteria listed in section 2.2 of RFC 4017 and PKMv2 shall be used.

### 4.4 Network entry of a provisioned MS

– After a device has been provisioned Device and User credentials it shall use the provisioned credentials on all subsequent network entries. The credentials shall use the EAP-in-EAP method as outlined in the 802.16e-2005. The EAP-in-EAP method allows for different AAA servers for Device and User authentication allowing flexibility for various business models and roaming agreements. The credentials used shall allow key exchange within the authenticator domain and expedited handover in the mobility domain (same AK zone).

### 4.5 Encryption of the air link bearer traffic and messages

– The WiMAX Network shall allow CCM-Mode 128-bit AES, AES Key Wrap with 128-bit key to be enabled on any service flow as requested by the MS or BS. For MBS service the WiMAX Network shall allow MBS CTR mode 128 bits AES, no data authentication, AES Key Wrap with 128-bit key to be enabled on any service flow as requested by the MS, or BS shall be supported. This means that BS and MSs must support at least the AES methods available in 802.16e-2005 so that encryption may be invoked on any or all service flows. CMAC should be used for control messages.

## 5 Requirement for MAC convergence sublayer

BS and MS shall support at least one Convergence Sublayer instance at a time. A BS may simultaneously support multiple instances of Convergence Sublayerss. Irrespective of the number of Convergence Sublayers supported, at least one of the supported Convergence Sublayer at the BS and MS shall support the following requirements:

– All BS shall support single host devices.

– All BS shall support multi host devices.

– Multi-host MSs shall support one or more of the following media types on a user facing interface:

  • IEEE 802.3 Ethernet with and without IEEE 802.1Q VLAN tags (see Note 1).

  • IEEE 802.11 with or without a Mobile IP stack on hosts connecting to the gateway.

  • IEEE 802.15 with the ability to manage connectivity to the MS on the device.

– The hosts behind the multi-host MS shall be manageable from the WiMAX network as an option.

– The hosts behind the multi-host MS shall be configurable to authenticate to the network.
– The MS shall be capable of mobile operation even if the form factor favors fixed operation. An example would be a 110 Volt device with Ethernet interface.
– Nothing in the selected sub-layer shall impede handover to or from WiMAX/802.11/3G.
– The Basic Mobility Profile Set, for both MS and BS, shall support both IPv4 and IPv6.
– The Convergence Sublayers selected should conserve airlink resources while supporting all of the requirements.
– The Basic Mobility Profile Set shall support header suppression and compression to maximize throughput efficiency.
– The header compression selected shall reduce the compression-related information feedback across the airlink.
– The choice of header suppression and compression shall support traffic which is forward-link only including broadcast/multicast traffic.

NOTE 1 – Support for Ethernet with and without IEEE 802.1Q VLAN is meant to imply the use of Ethernet and IEEE 802.1Q VLAN as a foundation for offering services. These services could typically use IP on top of Ethernet with IEEE 802.1Q VLAN tags.

The above requirements should be interpreted as neither requiring nor prohibiting the instantiation of multiple Convergence Sublayers types in a MS at a given instance.

The above requirements should be interpreted as neither requiring nor prohibiting dynamic switching between Convergence Sublayers types.

The above requirements should be interpreted as neither requiring nor prohibiting a MS from performing a handover, which involves an instantiation of an additional Convergence Sublayers type that is not already being used before handover.

## 6 Air interface functional requirement for L2 handover

The WiMAX Forum™ Mobility Profile shall include all features and parameters needed to support QoS during handover for all supported applications at Simple Mobility. The future WiMAX Forum™ Mobile Profile Set shall include all features and parameters needed to support QoS during handover for all supported applications at Full Mobility. The Basic Mobility Profile Set shall include all features and parameters needed to maintain radio link security during the handover process. The system shall support Handover between different RF channels of the same or different bandwidths.

## 7 Diversity and multiple antenna support

The MS shall support minimum of two branch receive antenna diversity. The BS shall support a minimum of two branch receive and transmit antenna diversity. Advanced antenna and/or MIMO based features may be supported but future releases using Advanced Antenna and MIMO based features shall be used to meet or exceed the system and link level performance requirements.

_____