DELIVERABLE D6.1

Report on existing group call solution

Title of Contract	Seamless Communication for Crisis Management
Acronym	SECRICOM
Contract Number	FP7-SEC-218123
Start date of the project	1st September 2008
Duration	44 months, until 30th April 2012
Date of preparation	
Author(s)	Aurel Machalek , Wojciech Dymowski, Dr A Aldabbagh,
Responsible of the deliverable	Aurel Machalek
Email	aurel.machalek@uni.lu
Reviewed by:	Wojciech Dymowski, Dr A Aldabbagh
Status of the Document:	Final
Version	1.0
Dissemination level (select)	PU Public
	PP Restricted to other programme participants (including the Commission Services)
	RE Restricted to a group specified by the consortium (including the Commission Services)
	CO Confidential, only for members of the consortium (including the Commission Services)

Contents

List of Figures

1. Summary

There are a lot of research papers, publications, articles, web information devoted to the new Internet protocol IPv6. In Secricom project and especially in this Deliverable D6.1 we don´t want to repeat known information, that´s why common information about IPv6 are used just as a neccessary base and used in most efficient way. The structure of this document follows topics from DoW of Secricom project Work Package 6. We can mention topics as:

- Unicast, multicast
- QoS needs
- SIP
- End - to – end security

More detailed frame of structure represent Tasks of WP6, concrete T6.1 and T6.2. Task 6.1 is focused to Existing IPv6 enabled PTT solutions, including topics for analyze:

- existing hardware- (e.g. IP phones) and software solutions,
- other than IPv6-enabled solutions,
- QoS support,
- security mechanisms.

Task 6.2. includes these topics to be analyzed:

- QoS in heterogeneous IP-networks,
- DiffServe-based QoS-enabled protocols (IntServ, MPLS, etc.)

The frame of this Deliverable reflex mentioned DoW and of course we have to focused on principals what we can use in future development. These ideas are based on communication between partners involved in WP6.

Novelty in Deliverables D6.1 from our point of view:

- Structured analyse of PTT solutions through IPv6 view in Chapter 1
- Adding overview of HIP protocol to Chapter 6, what is protocol between IPv4 and IPv6 with strong mobility and security features. This give as chance to developed unique communication solution and have some outputs from HIP and IPv6 comparison,
- Last Chapter focused on the Best practice of IPv6 use in safety services, here we mentioned one of the running EU FP6 projects - U2010 and specially part of using IPv6, this give us chance to build new solutions on the best practice in IPv6 safety solution,
- Annex 1 – unique work published on Internet, which gave no doubts why we have to focused in our work in Secricom project on IPv6,
- Annex 2 – added a part of IPv6 Ready Test Specification Management prepared by IPv6 Forum. In Secricom project we are interesting to pass these rules.

2. Group call solution

2.1 Open Mobile Alliance

2.1.1 Introduction

The Open Mobile Alliance (OMA) is an industry forum with nearly 400 members representing the entire mobile industry value chain, including the telecommunications, information technology, and content industries. The OMA focuses on developing market-driven, interoperable mobile service enablers for the rapidly converging communications, entertainment, and media worlds. OMA digital rights management (DRM) systems are important examples of such enablers. Although they have been developed for the mobile market, these systems assume network and bearer-agnostic delivery of the content over Internet Protocol (IP). This assumption makes OMA DRM systems suitable for use in any environment where the content is delivered over IP, which is true of a very wide array of applications. In this article, we overview the OMA DRM systems, position them in the larger context of DRM work, and describe their most important features.

2.1.2 Push-to-Talk over Cellular (PoC)

The modern Push-to-Talk technologies have developed from the traditional "Walkie-Talkies" provided by Land Mobile Radio (LMR) network where circuit-switching is typically involved in the calling process. The advent of new technologies, such as Voice over IP(VoIP) and IP Multimedia Subsystem (IMS), have boosted the packet-switching Push-to-talk over Cellular (PoC) available for commercial deployment. PoC is based on a half-duplex communication mode over mobile networks: a user presses a dedicated button and starts to talk after a talk indication is given; while the others listen and have the right to speak only when the floor is idle. A channel is established at the beginning of the call and it is reserved only for the duration of talk spurts due to the nature of the IP technology instead of for an entire call session in a traditional circuit-switching network. PoC v2.0 will allow audio (e.g. speech, music), video (without audio component), still image, text (formatted and non-formatted) and file share with a single recipient (1-to-1) or between groups of receipents as in a group chat session. On Figure 1 example of 1-many PoC Group Session (voice transmission) was shown:

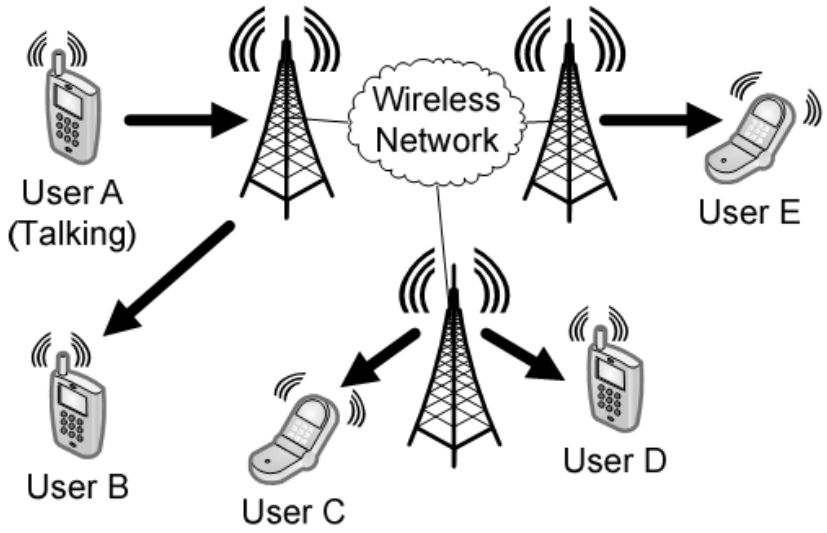

Figure 1: 1-many PoC Group Session

2.1.3 Architecture of PoC

The Open Mobile Alliance (OMA), a standardization organization, has developed technical specifications for application and service enablers independently of the underlying network. The PoC working group in OMA has released the approved version PoC 1.0 in June 2006 and the draft version PoC 2.0 in December 2006. Figure 2 shows the architecture and the Signaling between entities for PoC service based on. OMA defines the presence service as a service enabler that manages the collection and dissemination of presence information over mobile networks. A full spectrum of PoC service capabilities is suggested in OMA by using and interacting with presence and other enablers. In Fig. 2, blue bold boxes are the PoC functional entities and black bold boxes are the presence functional entities. The colors of arrows indicate different protocols over the interface between two entities. PoC client software for PoC service, watcher and presence source application software for Presence service, and Extensible Markup Language (XML) Document Management Client (XDMC) for XDM service are located on UE. PoC client performs registration with IMS core network; publishes PoC setting; allows PoC session initiation, participation and release; and generates and sends talk bursts. Presence source is an entity to provide presence information about a presentity (such as a PoC user) and watcher is an entity to request presence information of others. XDMC is an entity to provide access to any XDM Server (XDMS).

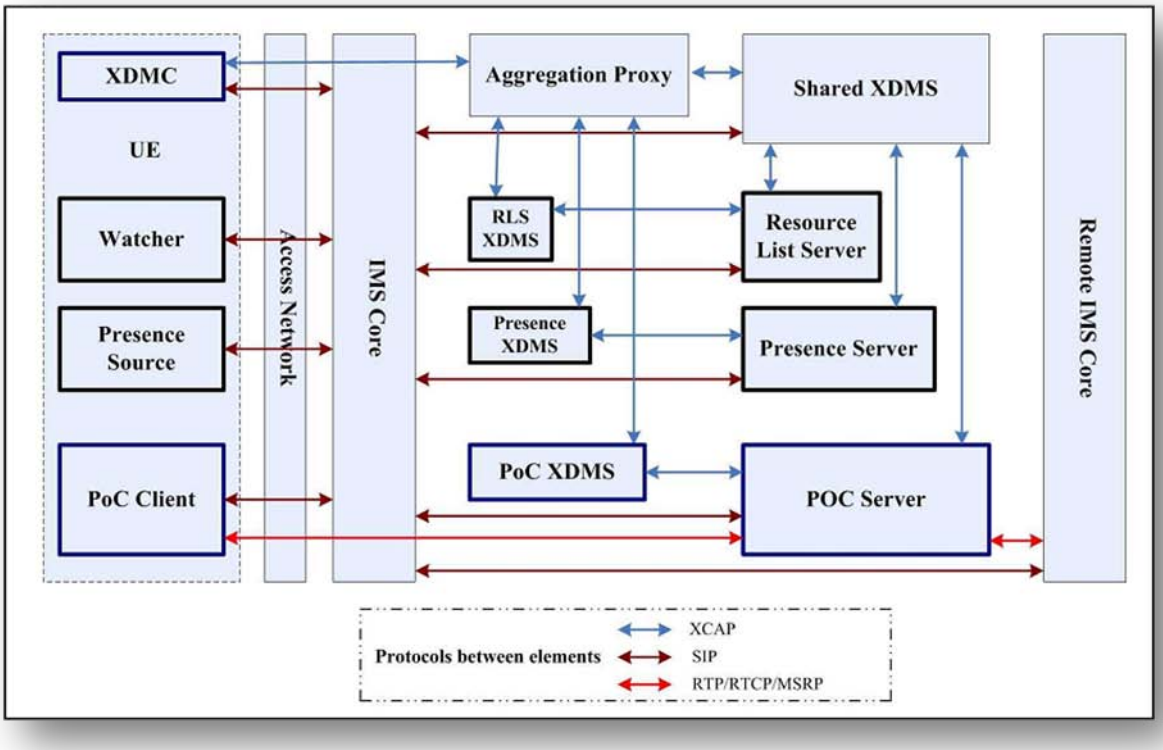

Figure 2: PoC Architecture

2.1.4 IP addressing considerations

Due to the nature of PoC and the fact that PoC uses SIP, the UE, the IMS Core, and the PoC Server have to be in the same address space. Thus for example, if private IPv4 addresses are used, the UE, P-CSCF, and the PoC Server have to have an interface in the same private IP address domain. Hence, NAT cannot be used on the Is and It interfaces. In the inter-connected PoC network case, the inter-connected operators have to be in the same IP address space. In practise this means that the inter-connection has to use public IP address

space. The public IP addresses can be either IPv4 or IPv6. This annex concentrates on describing the possible scenarios for the IP address domains. Figure 3 shows a case where the inter-operator network is using IPv4. The operator internal networks can either use private or public addresses as the operator internal network can basically be isolated from the inter-connect network. However, in the case of IPv4, typically public IPv4 addresses cannot be allocated to the UEs due address scarcity and private IPv4 addresses are used instead. The P-CSCF and the PoC Server have interfaces in the same domain as the UE. The P-CSCF and the PoC server have also interfaces in the same addressing domain as the S-CSCF. The IMS Core has an element on the border of the intra-operator address space, and the inter-operator address space. That element can be either an I-CSCF or the S-CSCF that is multi-homed.

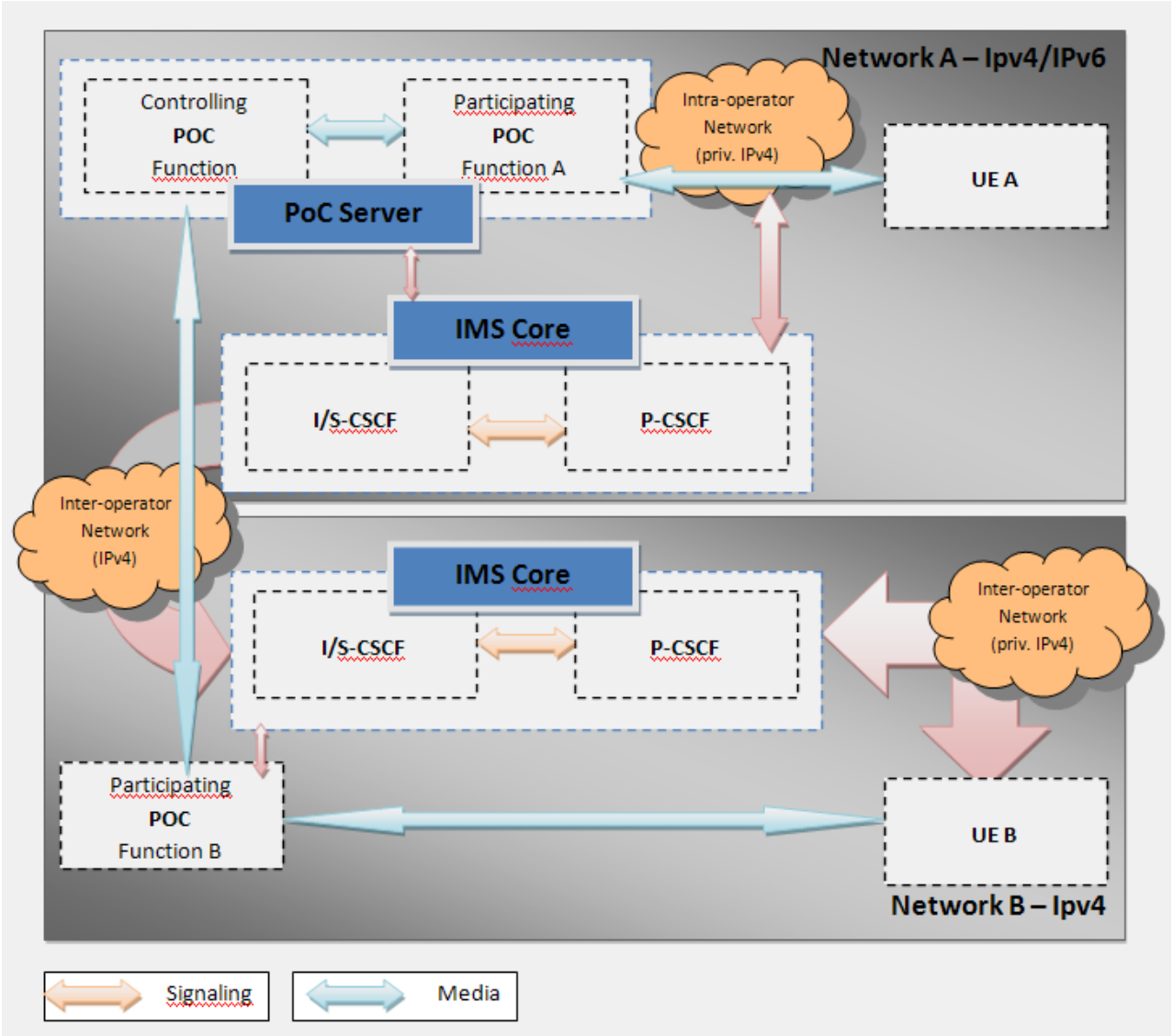

Figure 3: Inter-operator network is based on IPv4

Figure 4 shows a case where the inter-operator network is using IPv6. The operator internal network IP version and address space is independent of the inter-operator network IP version as the operator internal network can basically be isolated from the inter-connect network. The P-CSCF and the PoC Server have interfaces in the same domain as the UE. The P-CSCF and the PoC server have also interfaces in the same addressing domain as the S-CSCF. The IMS Core has an element on the border of the intra-operator address space, and the inter-operator address space. That element can be either an I-CSCF or the S-CSCF that is multi-homed.

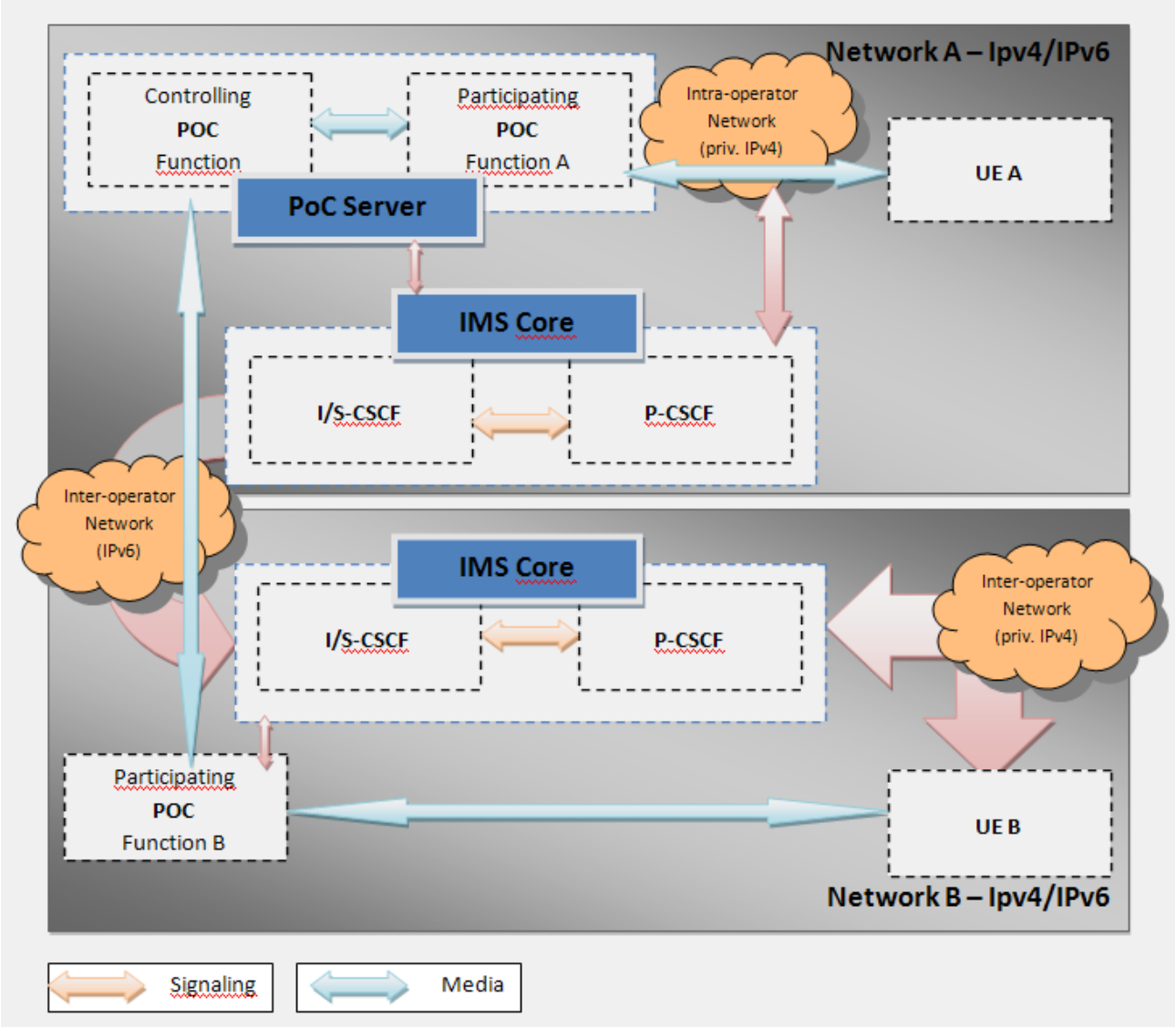

Figure 4: Inter-operator network is based on IPv6

As different vendors equipment may be IPv6 enabled at different time periods, some operators may not support IPv6 on the NNI (Network to Network Interface, an interface which specifies Signaling and management functions between two networks) from the beginning. Hence, the interworking between different kinds of deployment has to be assured by choosing the IP version, which is available. Practically, IPv4 will be chosen if IPv6 is not available for either end of the communication, otherwise IPv6 is used. The decision is done between two peers in a communication.

Figure 5 shows an example of an environment where there are users from different environments participating in a PoC session. In this case, the controlling PoC Server is dual-stack. The session setup is done between the individual participating server and the controlling server.

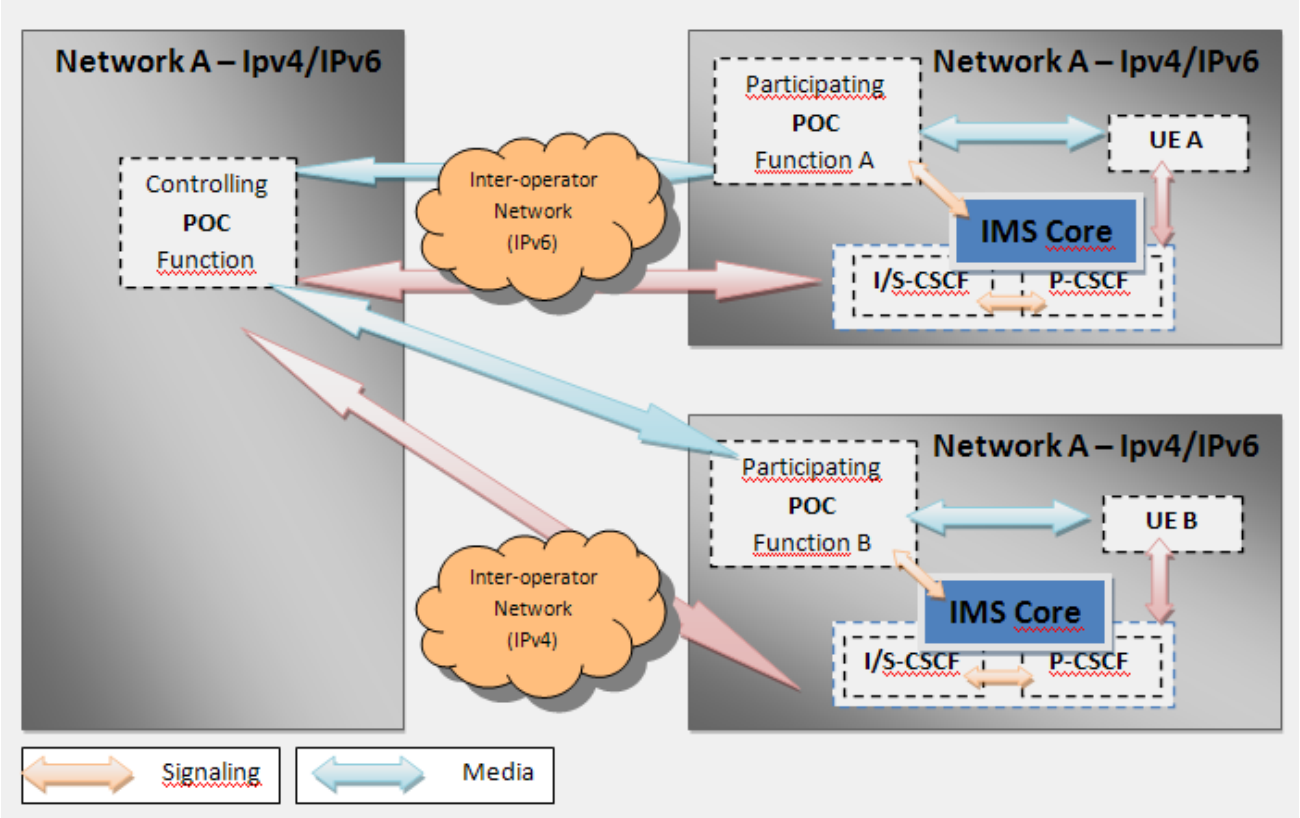

Figure 5: Case where users are from different environments

2.2 PoC and QoS

2.2.1 Introduction

In June 2003, an Agreement for Technology Cooperation for Push-To-Talk over Cellular (PoC) (the "Consortium Agreement") was executed between Ericsson, Motorola, Nokia, Siemens, and AT&T Wireless Services, Inc. to develop interim standards for Push-To-Talk over Cellular applications. As part of the the Consortium Agreement, participants agreed to post the Consortium Phase 2 Specifications and Documentation on their individual company Internet sites.

PoC Release 2.0 – UE Provisioning V2.0.7 is part of the Consortium Phase 2 Specifications and Documentation, describes the following parts:

- The general provisioning overview
- The Over The Air Provisioning (OTA provisioning) architecture and functionality.

2.2.2 OTA provisioning parameters

PoC UE Provisioning uses several configuration parameters that should be provided by OTA provisioning. OTA provisioning should contain minimum of 6 characteristics:

- 1 NAPDEF characteristic (this is used for normal GPRS configuration as it is currently used) NAPDEF (Network Access Point DEFinitions) characteristic contains information about access points. NAPDEF defines how a mobile device can set up a network connection, either via circuit-

switched data or GPRS. For every NAPDEF referred to by an APPLICATION characteristic, an access point is created on the device.

- 1 PXLOGICAL characteristic
  Logical proxies (the PXLOGICAL characteristic) have a number of physical instances, i.e., physical proxies. Each logical proxy has a name, an unique ID, a startpage URL, and some parameters like port number values that are shared between all physical instances of the logical proxy.
- 4 extended APPLICATION characteristics

Separate APPLICATION characteristic elements should be used for each specific service as follows: Basic IMS client functionality (IMS), PoC, Presence (PS) and Group Management (GLMS). For this reason, each service (APPLICATION) must have an application ID registered at OMNA. The mapping to OTA provisioning data model to one of these six mentioned characteristics (application IDs) is given by the prefix of parameter name and PXLOGICAL is prefixed with PXIMS.

Generally, a network access (e.g. GPRS) must be provided for the possibility to connect to the PoC network (IMS Core, Presence Server, GLMS and PoC Server). Configuration of the network access is not in a scope of this document. PoC configuration uses the NAPID of the configured network access.

Existing parameters

Internal Parameter name	**Possible values (example)**	**Description**	**Optionality (mandatory /optional)**	**OMA data model mapping in provisioning document**
POC.Napid	String (e.g. POCNAP)	Network Access Point ID identifying the PoC GPRS profile used for PoC network access.	Mandatory	NAPDEF.NAPID, PXLOGICAL.PXPHYSICAL.TONAPID, APPLICATION.TO-NAPID

2.2.3 PoC defined parameters

The list of parameters which were identified as required on *PoC List Management and Do-Not-Disturb* and *PoC Signaling Flows*. The parameter names are according to these documents with prefix added for simple matching to correct OTA provisioning characteristics.

2.2.4 Implementation PoC in various access networks

Generally the PoC implementation should work in an access network that delivers a throughput of 7.2 kbps or more.

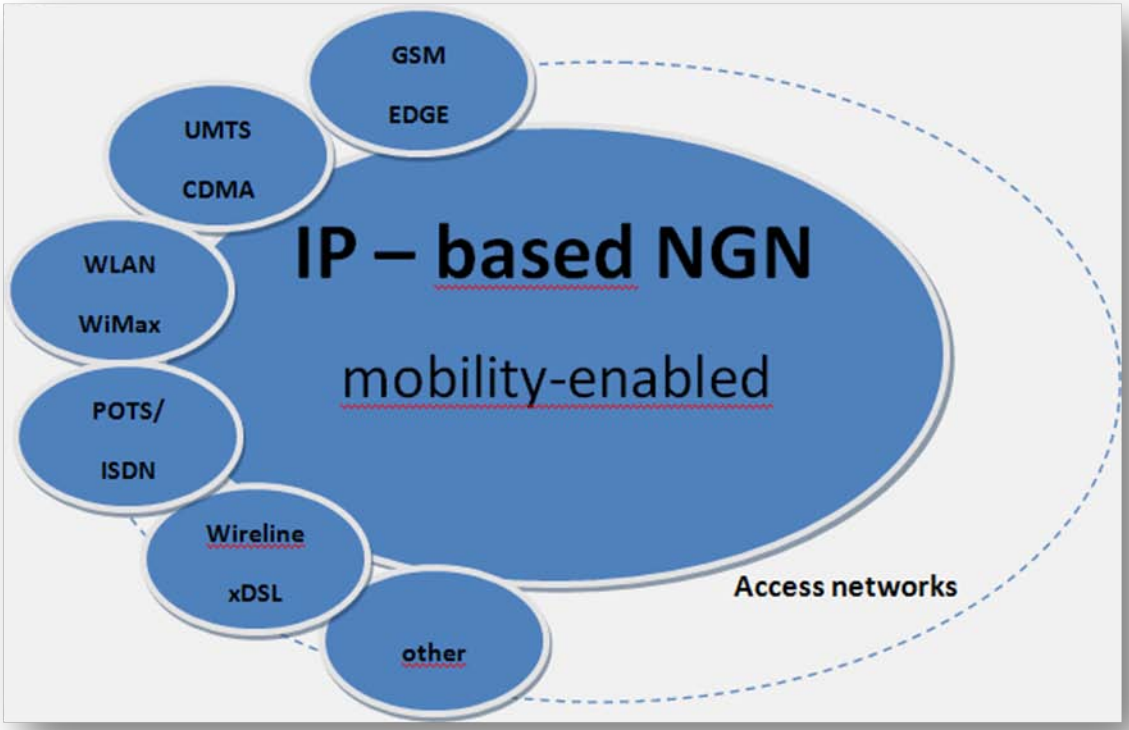

Figure 6: Implementation PoC in various access networks

The access network can be UMTS, GSM, WLAN, DSL, etc. OMA service enablers utilize 3GPP/3GPP2 IMS core network to deal with authentication, authorization, routing, charging, signaling compression, address-translation, and interworking. The Session Initiation Protocol (SIP) is used for the session control. Application servers, such as PoC server, Presence Server, and Resource List Server, are inserted into the SIP Signaling path .

2.3 IPv6 and PoC

2.3.1 Technology preview

The phone needs to include a PoC client and user interface (embedded or loaded), it also has to support SIP protocol and VoIP features. The sendering phone sends packet data to a PoC server, as manifolded if it is a group call. The core network consists of PoC Call Processor and PoC Register network elements which are connected to GPRS or EDGE network.

Session Initiation (SIP) protocol is an application layer protocol for creating, modifying and terminating sessions with one or more participants. It also enables a terminal to register its current address to a proxy so that other users are able to reach it with a textual address; it includes also authentication and authorization. The voice packets are transported with Real-time Transport Protocol (RTP).

Internet Protocol Multimedia Subsystem (IMS) is a platform that may be used by operators to quickly develop and deploy multimedia services for 2.5G and 3G mobile networks. This platform contains a SIP application server on which mobile data services like Push-To-Talk over Cellular and telephone conferencing are based on in the future. The servers handle session and group control, VoIP streaming, stream control, provisioning and management of users and groups.

2.3.2 Always-On Capability Permits Push-to-Talk Applications

Applications that are always able to accept a connection from a host on the Internet are known as “always on”, and IPv6 is ideally suited to such applications. The availability of trillions of IP addresses will allow billions of data phones, handheld PDAs, home appliances, and other devices to connect continuously to the Internet. Push to talk is one such promising always-on application. Users simply press a button on their cell phones, and they are almost instantaneously connected to another party or a talk group.

Implementing application layer Mobile IPv6 in 2G and 3G mobile networks primarily requires application layer IPv6 support from the network, the installation of a Home Agent (HA) router in the home network, the use of mobile terminals supporting Mobile IPv6 and the implementation of IP security. Further, Mobile IPv6 is a highly feasible mechanism for implementing static IPv6 addressing for mobile terminals. In this case, the Mobile IPv6 home address is the static address and the mobile node can always be reached using the same globally unique IPv6 address, independent of its current location. Many applications and services, such as Push-To-Talk, need static IP addresses/static user identity.

2.3.3 Mixed support of IPv6 and IPv4 in a group talk session

The same principle applies also when determine the IP address space when IP version 4 is used. Since the IP version 6 is optional a network supporting IP version 6 also supports IP version 4. Figure 7 and 8 illustrate how the originating side determines which IP version that shall be used during a talk session (according to Motorola).

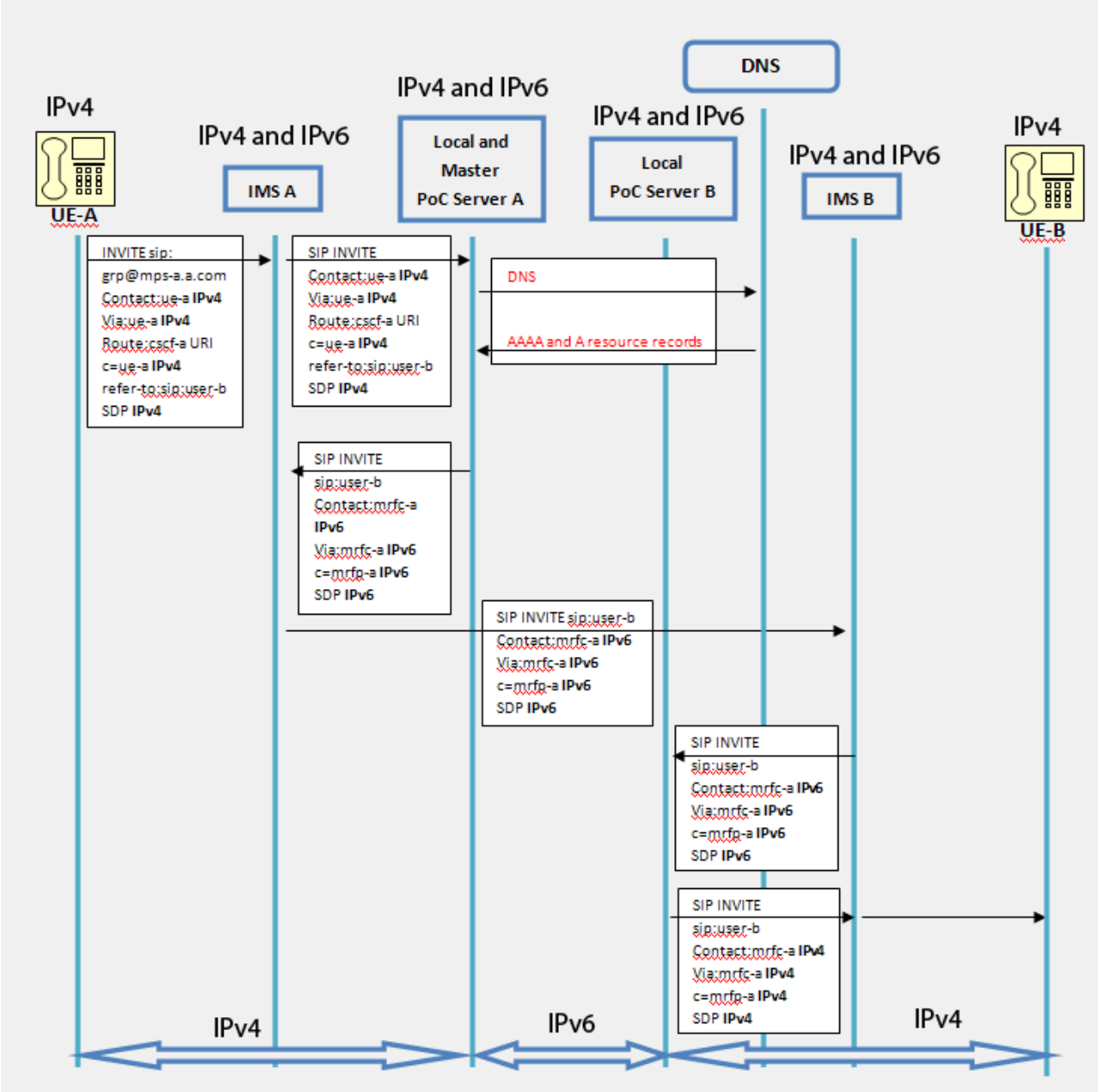

Figure 7: Both sides supports both IPv6 and IPv4

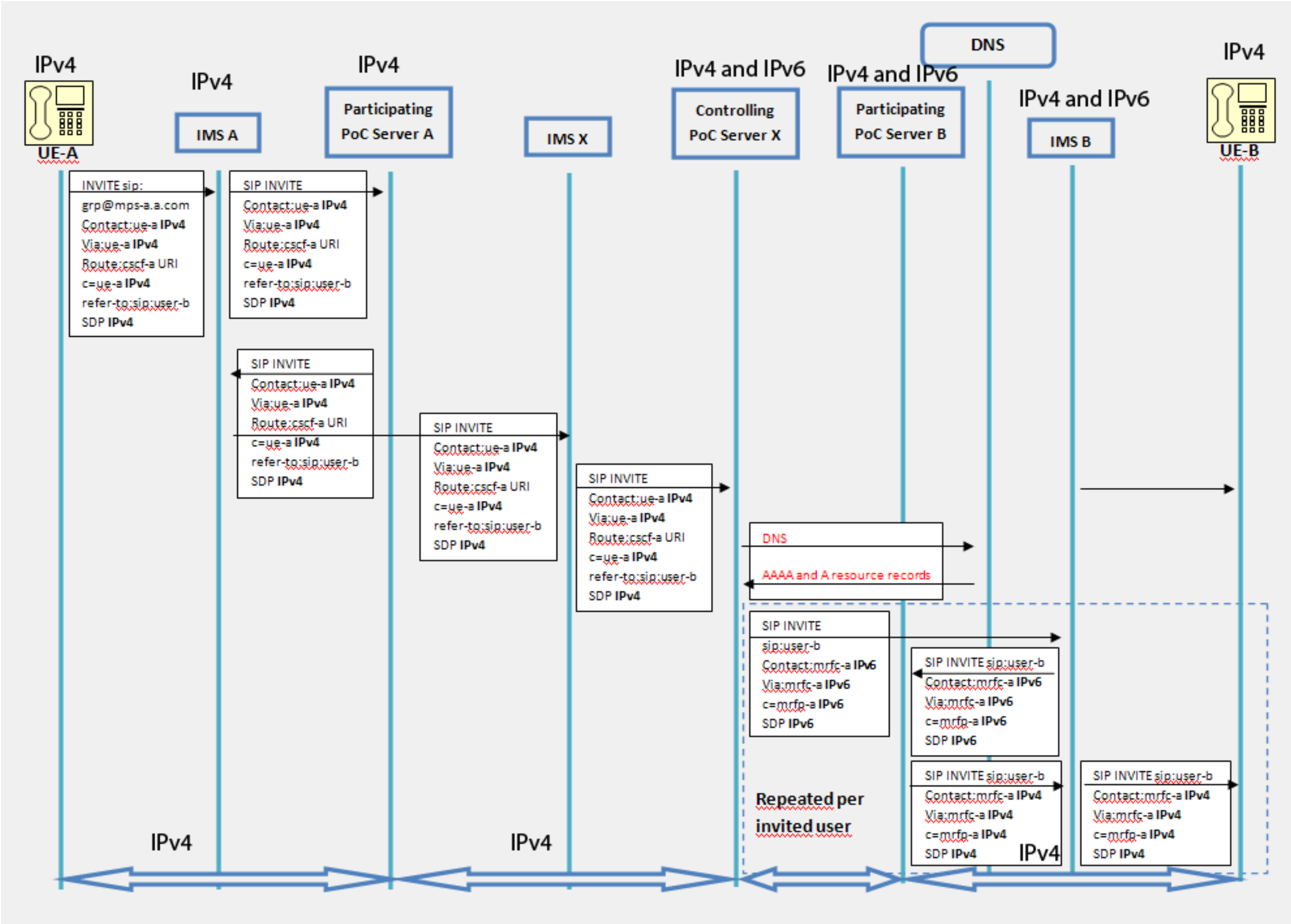

Figure 8: Mixed support of IPv6 and IPv4 in a group talk session

2.3.4 PoC and NATs

- Even though PoC connections use a PoC server in the network, private addresses cause problems similar to other SIP signaling cases.
- UDP inactivity timers are used with NATs and cause some problems:
    - ➢ The mobile would need to send keep-alive packets to every used public UDP socket in about 30 seconds. This generates unnecessary “overhead” traffic and would be very bad for the battery life.
    - ➢ The mobiles could easily use up all of the operators public IPv4-addresses due to the refreshments, the public UDP ports can’t be assigned to new mobiles.
    - ➢ Thus, for performance reasons, NATs should not be used for PoC.

2.3.5 Other benefits coming from implement IPv6

The clear benefit of IPv6 is that it brings savings in battery consumption. Cellular phones are often behind NATs. Applications that keep connections open for a long time need to keep UDP mappings in NATs alive by sending keep alive messages roughly every 30 seconds. Always-on applications are emerging and becoming popular in cellular phones, thus further increasing amount of applications that need to have connections constantly open. Increased load also to network due all those keep-alives. Sending of NAT keep-alives once in 30 seconds decreases cellular phone standby time by several days. Problem is more severe in 3GPP technology than with WLAN, as in 3GPP it is more resource consuming to bring radio interface up. NAT keep-alives are a big problem.

Example: for Nokia Push-to-Talk (PoC) application it is required that there is no NATs between terminal and the PoC server. This is because PoC uses UDP protocol, which does not contain sessions like TCP/IP, and thus assigns the port to another user after certain inactivity time. This would require terminals sending “keeping – alive - messages” in frequent manner to NAT which would generate unnecessary traffic and would be bad for the battery consumption.

2.4 IMS and PoC

2.4.1 Introduction

The IP Multimedia Subsystem (IMS) is an architectural framework for delivering internet protocol (IP) multimedia services. It was originally designed by the wireless standards body 3rd Generation Partnership Project (3GPP), as a part of the vision for evolving mobile networks beyond GSM. Its original formulation (3GPP R5) represented an approach to delivering "Internet services" over GPRS. This vision was later updated by 3GPP, 3GPP2 and TISPAN by requiring support of networks other than GPRS, such as Wireless LAN, CDMA2000 and fixed line. The last version of IMS is release 8, published at 5th June 2008.

2.4.2 Architecture of IMS

The IP Multimedia Core Network Subsystem is a collection of different functions, linked by standardized interfaces, which grouped form one IMS administrative network. Figure 9 shows block scheme of IMS.

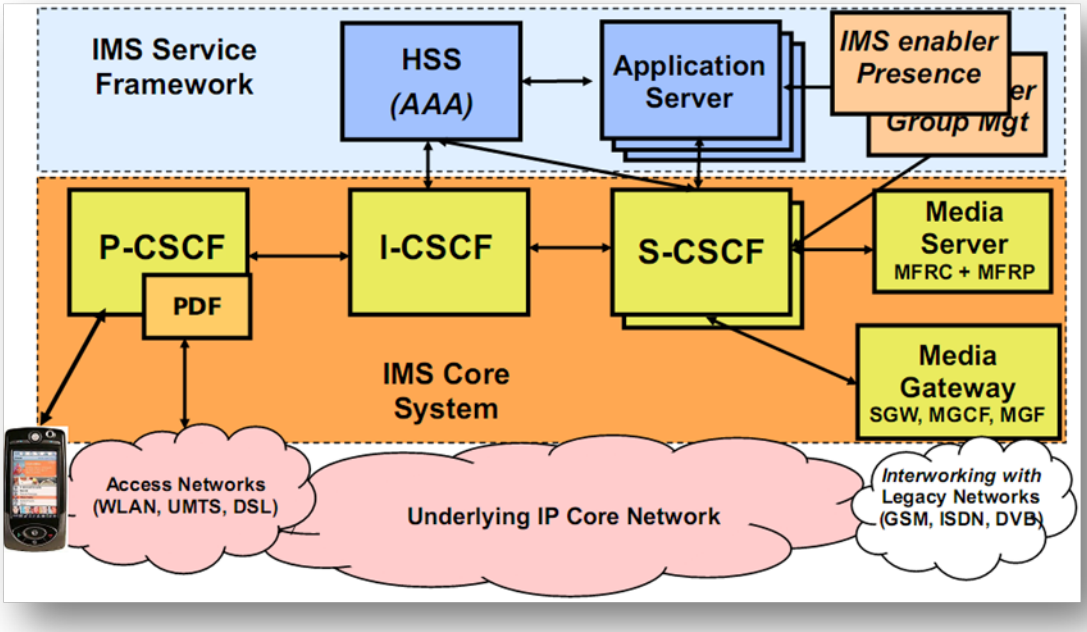

Figure 9: 3GPP IMS Architecture: IMS Core and Applications

2.5 QoS support in IMS

2.5.1 Introduction

It is commonly accepted that the future of telecommunications will be based on the convergence of fixed and mobile technologies, interworking existing IP Connectivity Access Networks (IP-CAN) with an all IP core. This increasing trend towards all-IP based network architectures has benefits for both subscribers and network operators. Network costs are greatly reduced by the maintenance of a single core network and the convergence of fixed and mobile technologies allows for far better service integration. The Third Generation Partnership Project (3GPP) standardized the IP Multimedia Subsystem (IMS) as a subsystem of UMTS to facilitate a smooth transition from the Circuit Switched (CS) to the Packet Switched (PS) domain; it is essentially an overlay architecture that allows multimedia service provisioning across both wired and wireless IP-CANs. 3GPP2 has also adopted this architecture for use on top of their Multimedia Domain and Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN) is utilizing the IMS for multimedia service provisioning in their Next Generation Network (NGN) architecture.

The realization of an all IP core requires careful thinking due to the complexity of the signaling, Quality of Service (QoS), security and mobility issues handled by the previous CS technologies, and with IP traditionally a ‘‘best effort’’ technology, QoS becomes particularly important. Customer uptake is heavily dependent on end user experience, and with the increasing viability of IMS, a comprehensive management framework is needed.

The IMS uses end to end signaling for service based session establishment and also makes decisions based on policies for enforcing QoS on the access routers. Given the growth in importance of QoS, many recent research works provide solutions to the QoS problem, however these and 3GPP standardization efforts do not address or specify how the requests are processed or mapped within the IMS architecture. The objective of this article is to highlight critical unresolved issues within the standardized IMS QoS provisioning mechanisms and to propose a decision making/ mapping solution for managing QoS in different scenarios.

2.5.2 Policy Based QoS Provisioning

3GPP has adopted Policy Based Network Management (PBNM) for QoS provisioning in the IMS. This system was chosen to manage resources on both the session and bearer levels in a tight but flexible manner decoupling the core network components and procedures from the subtleties of the access technologies. PBNM allows a network operator to make resource allocation decisions based on high level policies without interfering with IP-CAN specific management. A critical component in this architecture is a logical entity that has a northbound interface to the Signaling plane and a southbound interface to the bearer plane to provide linkage and synchronization between the two planes. Such an intermediate node has been de fined under several standards and given different functional names including Policy Server, Resource and Admission Control Function (RACF) and Bandwidth Manager; in the 3GPP release 6 IMS architecture such an element is called Policy Decision Function (PDF). When a User Equipment (UE) (Fig. 10) sets up an IMS session it sends SIP messages via IMS proxies .

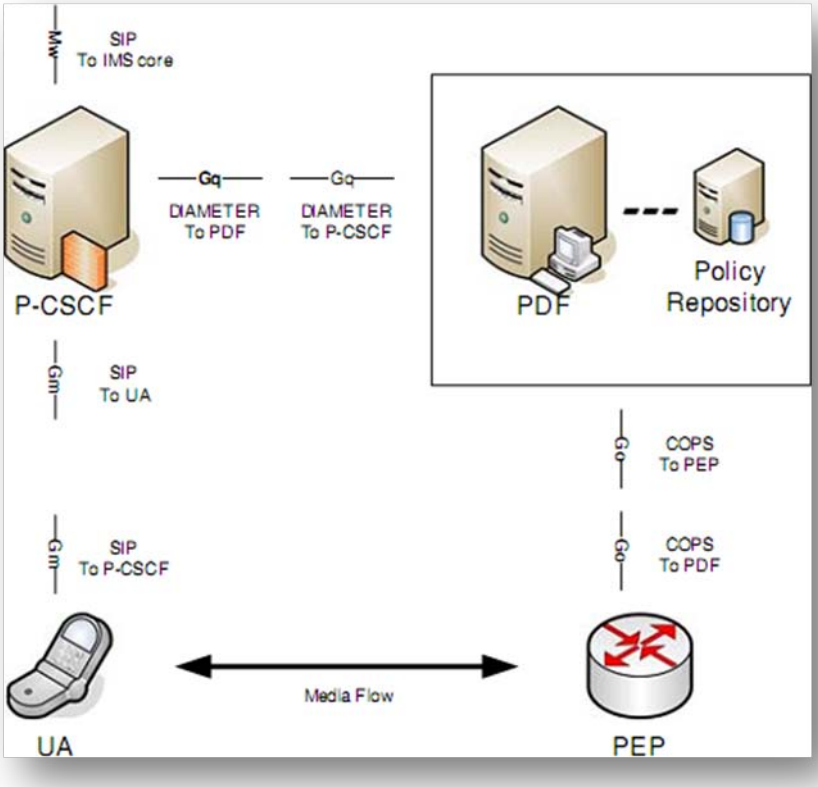

Figure 10: Policy Based QoS Provisioning within the 3GPP IMS

As the first point of contact within the IMS the Proxy-Call Session Control Function (P-CSCF) examines these messages and, where possible, translates the Session Description Protocol (SDP) field of the SIP messages into service information. This service information is conveyed to the PDF using a specialized DIAMETER interface known as the Gq interface. Upon receipt of service information the PDF consults a repository of pre-stored policies and makes a decision whether or not to allow the session to proceed. Based on these pre-stored policies the PDF assigns QoS parameters to each session and must map these parameters to configuration information specific to the IP-CAN in the bearer level. These QoS configuration parameters are pushed to entities that enforce QoS within the bearer level known as Policy Enforcement Points (PEP). The PEP acts as a gate that allows authorized IP flows to use network resources, but drops unauthorized flows; this is known as policy based admission control. The interface between the PDF and the PEP is known as the Go interface and uses the Common Open Policy Service Protocol (COPS) to transfer policy information.

2.6 Measurments of PoC

The main goal of the following measurements, performed by engineers from Fujitsu Labs of America, Inc. and Personal Systems Research Center, Fujitsu Labs LTD is to investigate the performance of PoC system over commercial 3G networks. The performances were measured in the US. PoC system aims to provide high flexibility to a wide range of business solutions and operate independent of the underlying network. Thus the investigation results of different network characteristics generate important information to improve our PoC system. Three major carriers in the US are selected, two of which provide 1xEV-DO (Evolution-Data Optimized) services while the other one provides UMTS/HSDPA (Universal Mobile Telecommunications System and High Speed Downlink Packet Access). Several empirical studies of PoC performance have been conducted over 2.5G networks and some architectural studies of PoC in 3G networks have been investigated in the past.

2.6.1 System configuration and evaluation items

The testbed of PoC measurements is composed PCs shown in Figure 11

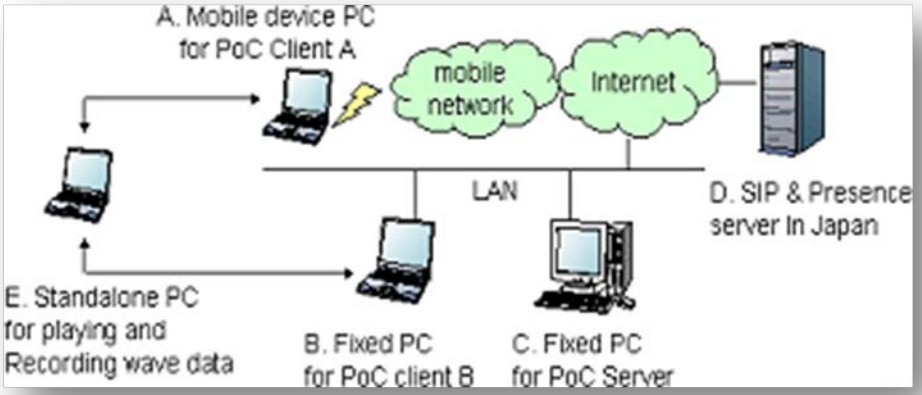

Figure 11. Enviroment for PoC evaluation

PC[1] A is the mobile device running PoC Client software. The other PoC Client (PC B) is attached to the same LAN as the PoC Server (PC C). PC D is another SIP & Presence Server located in Japan. Finally, PC E is a machine simply playing and recording sound to measure the voice latency. The details of the operations measuring uplink voice latency are illustrated in Figure 12.

[1] To case evaluation, PC Clients are used in the experiment despite the PoC client operates on PDA and Smartphone as well.

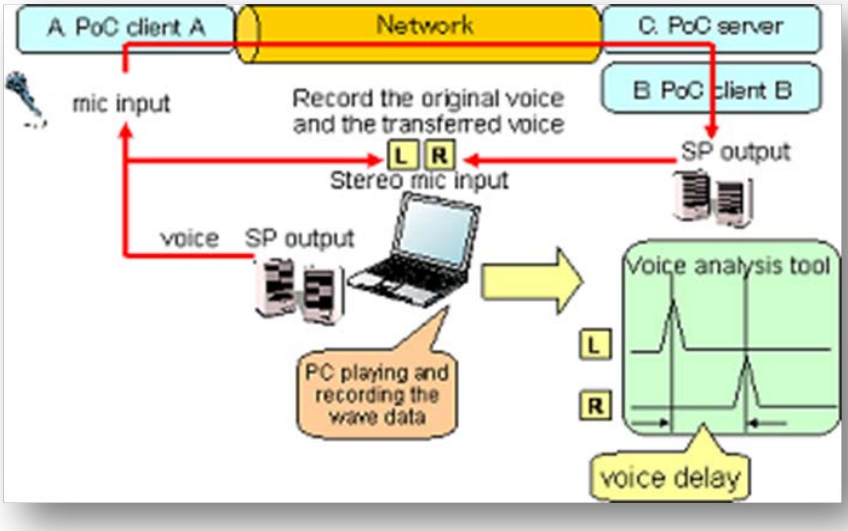

Figure 12. Enviroment setup for evaluation of uplink voice latency

The stereo sound wave originating from PC E is split into left and right channel signals. The right channel signal travels through PoC Client A, the Internet, PoC Server, PoC Client B, and finally back to the recording machine (PC D). The voice latency is determined by comparing the waveform of left and right channels.

Besides voice latency, two other performance metrics are control latency and voice quality. Control latency describes the delays encountered when performing actions such as starting a PoC session and floor arbitration. More specifically, four items of control latency are considered:

- **PoC Start to Okay:** The time between sending PoC start and receiving OK from PoC server.
- **PoC Start to Join**: The time between sending PoC start and receiving other participants' join information. At this moment, the initiating user can start to talk.
- **Floor Request:** The time between sending floor request and receiving floor information.
- **Floor Release:** The time between sending floor release and receiving floor information.

2.6.2 PoC Control Latency

The results of the control latency test based on 20 samples are show in Table 1.

Item	A	B	C
PoC Start to Okay	1116	1247	1342
PoC Start to Join	1540	1683	1794
Floor Request	882	807	905
Floor Release	878	880	986

Table 1: Control latency results (unit: ms)

The control latency values are generally larger than RTT mainly because of the extra RTT between PoC Server in the US and SIP & Presence Server in Japan.

2.6.3 PoC Voice Latency

The second test measures the voice latency in both directions using two codecs, GSM6.10 and AMR, over several frame times (20, 40, 60, 80, 100, 120, 200, 240, 300, and 400ms). The results of the voice latency test using AMR and GSM6.10 codec are shown in Figure 13 and Figure 14, respectively. It is clear that downlink performance is almost identical for all three networks when the frame time is small, and continues to be similar even with larger frame times. In terms of uplink performance it appears that larger frame times lead to a linear increase in delay, but more variation is seen when the size is 120ms or shorter.

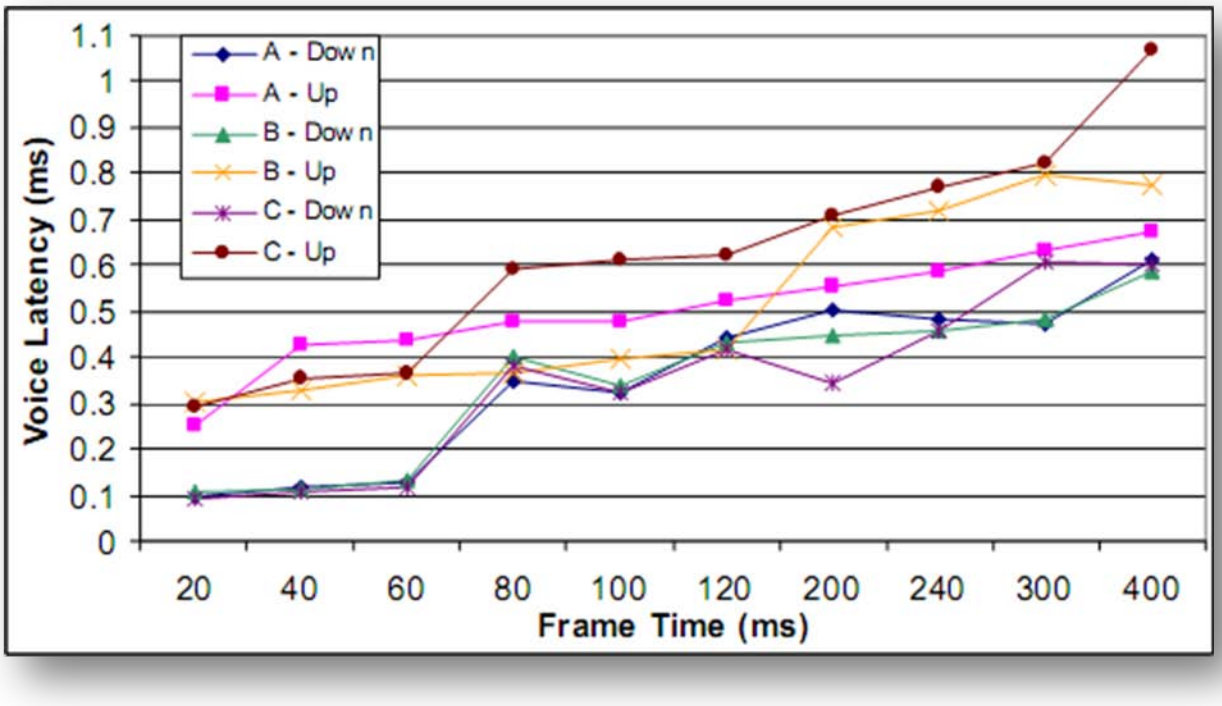

Figure 13. Voice latency using the AMR half rate (4.75kbps) cosec

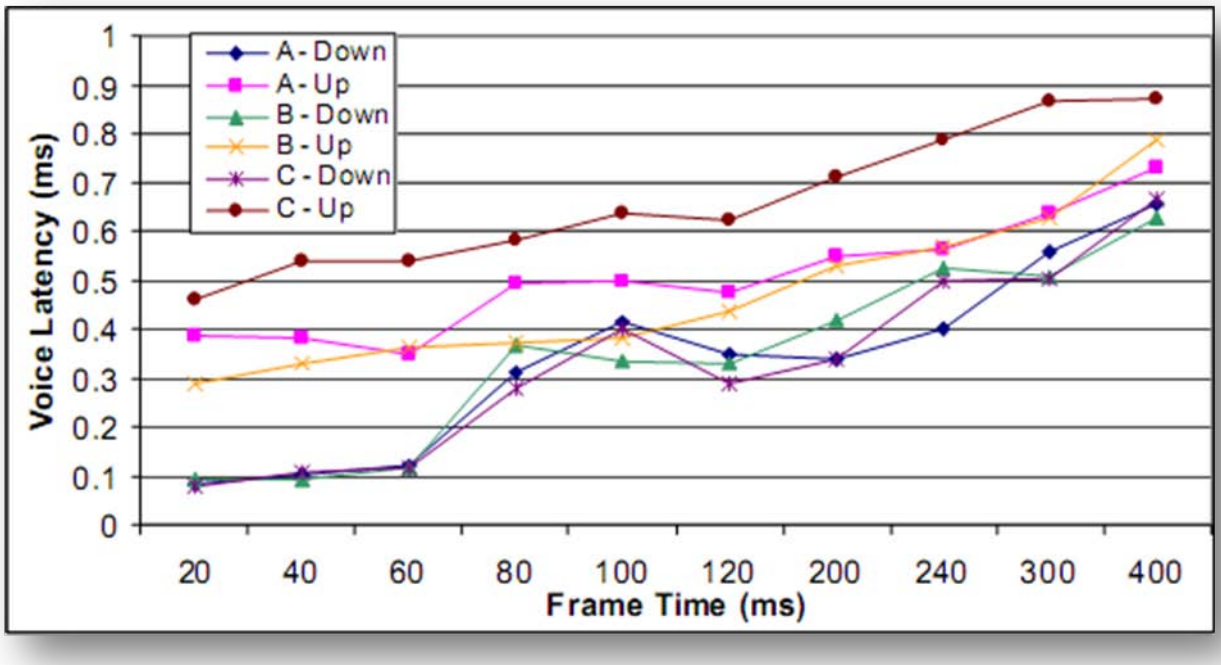

Figure 14: Voice latency using the GSM6.10 (13.2kbps) codec

Several important characteristics of PoC traffic are identified. First, the downlink voice delay is shorter than uplink delay. Second, longer frames also undergo longer latency. Third, there is no apparent difference in the results of AMR and GSM6.10 codec. The results are quite intuitive and can be explained in the following. Voice latency is constituted by two components: data frame time and packet propagation time. Data frame time is the period in which the wave samples are buffered in the sender. Waves carried in a long data frame need to wait for long time before being transmitted. Data frame time can be seen as the base of voice latency. On the contrary, packet propagation time is determined by both packet payload length and link bandwidth. In particular, there exists a significant difference between uplink and downlink bandwidth resulting in the difference of uplink and downlink voice latency. But since the data rate of both GSM6.10 and AMR codecs is small compared to the offered bandwidth in both uplink and downlink, the difference of voice latency in AMR and GSM6.10 is not so obvious. Finally, one interesting phenomenon is also observed in the steep increase of voice latency from 60 to 80 ms in all three networks.

2.6.4 PoC Voice Quality

The third test measures the quality of the voice data after passing through the PoC system. This test is also taken in both directions using both codecs and used the same frame times as the second test. A 30 second speech sample is used in the test and then rated on a scale of one to five where five is the highest quality and one is the lowest similar to Mean Opinion Score (MOS). More detailed descriptions of each score are listed in Table 2. Note that the interpretation of the results is subjective and reviewed by two listeners.

	Description
1	The recording is virtually useless. Much static, lost words or unclear words appear in the speech and it is hard to understand the speaker.
2	The recording is severely degraded but still intelligible.
3	All sentences can be recognized. Only a moderate level of quality degradation is observed.
4	Only a small number of problems can be heard in the recording.
5	Almost no problems exist in the recording.

Table 2: Description of voice quality scores

The results of voice quality using AMR and GSM6.10 are presented in Figure 15 and Figure 16, respectively. Basically, the voice recordings are understandable using either codec and any frame time for both directions. However, some combinations of these parameters offer a much clearer and pleasant listening experience than others. In general, the downlink tests sound excellent due to the additional bandwidth. The sound quality of higher frame time recordings are better despite the noticeably larger impact of packet losses made on these tests. In other words, a smoothing mechanism is applied to generate better voice quality when the buffering waves are longer. But once a long frame is lost, it is more difficult to recover cleanly from the loss. The trade-off between sound quality and frame loss is a key factor to determine the frame time. In addition, the impact of codec to voice quality is not so obvious though GSM6.10 provides slightly better quality than AMR.

A trade-off exists between the AMR and GSM6.10 codec. AMR with higher compression rate and shorter data size results in smaller voice latency. On the other hand, GSM 6.10 usually generates better voice quality provided that sufficient bandwidth is available. Therefore, PoC system might need to change codec depending on various conditions.

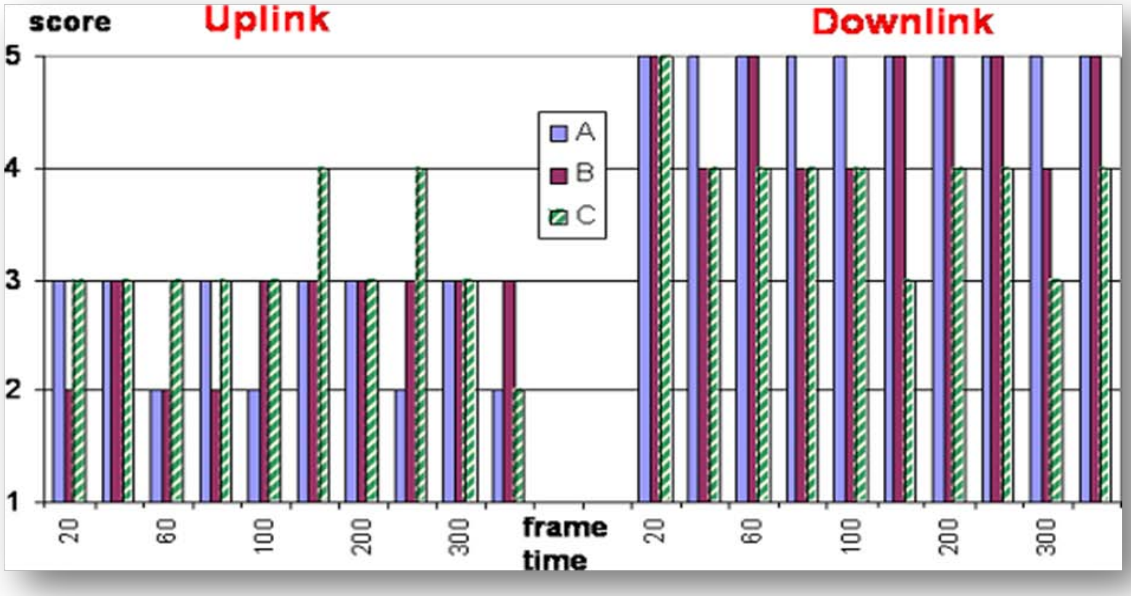

Figure 15. Results of voice quality using the AMR codec

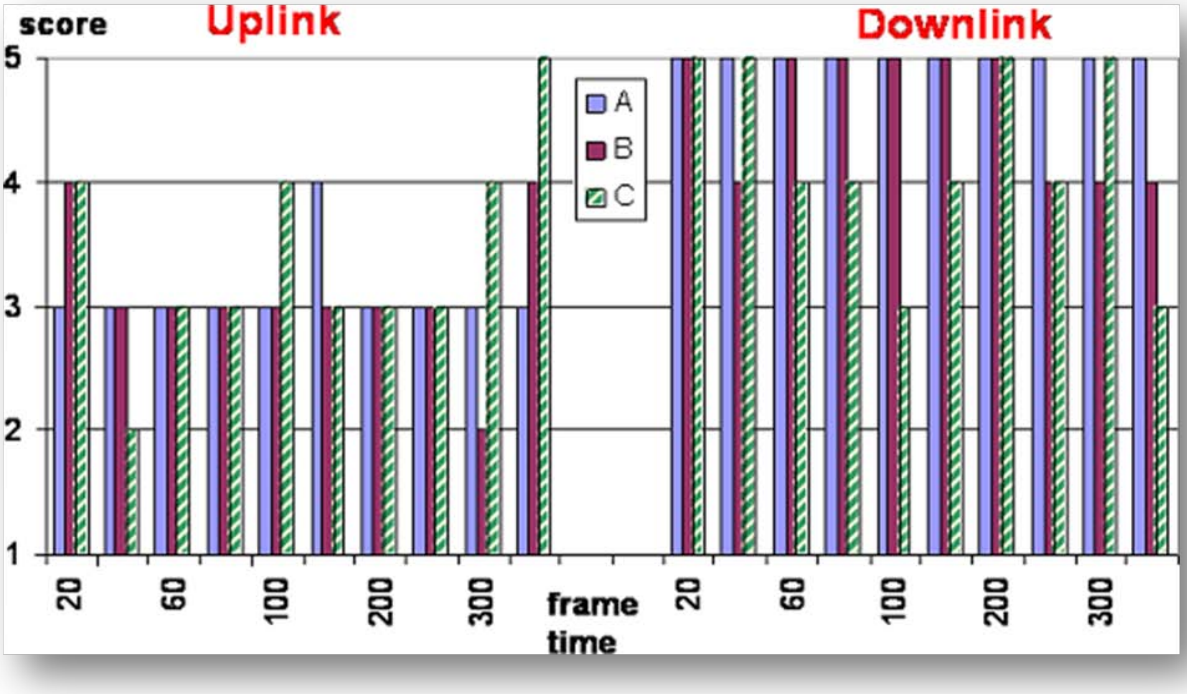

Figure 16. Results of voice quality using the GSM6.10 codec

2.6.5 Summary

From above empirical study results, the performance of PoC in 3G networks is generally better than PoC services offered by US carriers, which exhibit 1-2 seconds session initiation latency and 1-3 seconds voice latency. Additionally the carriers' PoC solutions are optimized for their own networks, but through this evaluation we have shown our PoC system achieves excellent performance at any 3G networks.

2.7 Traffic Routing and Switching

2.7.1 Routing of IPv4/v6 Traffic

The routing of IP traffic is one of the major elements of the Internet and its protocol and without this crucial element the networking capability of the internet would not be possible.

The internet itself is made up from smaller sub-networks each of which is assigned a unique network address. Sub-networks are inter-connected using IP routers, and each sub-network can contain a number of IP nodes each of which is assigned a unique IP address. A node must have a unique IP address for it to communicate over the internet. In simple terms, an IP node places in a data packet the IP address of the destination node it wishes to communicate with as well as its own IP address and the message it wishes to send. Once formed, the packet is sent over the network, which in turns handles the delivery of the packet to its intended destination.

IP routers are devices that move traffic packet by packet from one sub-network in to another after inspecting the destination IP address in each packet to determine whether the packet requires forwarding onto another sub-network, and if so to which immediate sub-network it is to be forwarded.

In order to accomplish traffic routing, the routing device construct a routing table which contains details of all the sub-networks the router has learnt during its course of operation and how the delivery of packets destined to each of the sub-networks is are to be carried out. Thus, the routing process interrogates the

routing table for each packet received in order to determine the correct route through which the packet is to be dispatched.
Because the routing table can grow to large sizes, the routing process has been found to be inefficient from network capacity view point – this is especially true for high-speed networks carrying multi-media traffic.
In addition, by its nature, routing is a hop-by-hop traffic forwarding process. In general, hop-by-hop routing is unable to permit absolute QoS traffic guarantees because of its late binding of network resources such as link and switch capacity to packet flows. This is effect has a detrimental impact on latency/jitter sensitive applications such as audio and video.

2.7.2 Switching of IPv4 Traffic and QoS: MPLS

In recent years, the trends toward distributed networking and converging voice and video applications onto the wide area networks have pushed network designers to a newer technology called Multiprotocol Label Switching (MPLS) which appends an IP packet with a 32 bit label that instructs the routers in an IP network how to switch the packet without examining the packet's contents, thus permitting the IP packet to traverse a network more quickly than with a routing protocol.
MPLS labels fit between Layer 2 and 3 of the protocol stack and provide information on how to

1) Establish a switched path through an IP network
2) Identify packets that share a common classification for transport and
3) Set the Quality of Service (QoS) the packets should receive.

By its nature, traffic switching is an end-to-end explicit routing process, where pre-calculated routes such as in source routing are necessary to permit early binding of resources to the flows and hence to achieve the desired QoS guarantees.
It is accepted that MPLS provide an efficient form of QoS and a good vehicle for traffic engineering. Indeed, explicit routing is generally used to improve path controllability; eliminate loop paths; support QoS on demand; and implement policy routing and traffic engineering.

2.7.3 IPv6 Intrinsic Support for MPLS: Flow Labels

MPLS has been a form of a bolt-on mechanism added to IPv4 in order to provide efficient QoS and increased network capacity. On the other hand, IPv6 designers recognised the power of MPLS from its evident popularity, and hence incorporated an MPLS like feature in the organic fabric of the protocol. Specifically, IPv6 includes a "flow label" in its specifications and thus provides the means by which IPv6-capable routers can recognise the end-to-end flow to which transmitted packets belong. Whilst similar to the service offered by MPLS, this capability is intrinsic with the IP rather than an add-on which help for better implementation and deployment.

3 Overview of existing hardware and software solutions with IPv6 support

3.1 Mobile Internet Protocol v6 - MIPv6

Mobile IPv6 allows an IPv6 node to be mobile - to arbitrarily change its location on an IPv6 network—and still maintain existing connections. When an IPv6 node changes its location, it might also change its link. When an IPv6 node changes its link, its IPv6 address might also change in order to maintain connectivity. There are mechanisms to allow for the change in addresses when moving to a different link, such as stateful and stateless address autoconfiguration for IPv6. However, when the address changes, the existing connections of the mobile node those are using the address assigned from the previously connected link cannot be maintained and are ungracefully terminated.

The key benefit of Mobile IPv6 is that even though the mobile node changes locations and addresses, the existing connections through which the mobile node is communicating are maintained. To accomplish this, connections to mobile nodes are made with a specific address that is always assigned to the mobile node, and through which the mobile node is always reachable. Mobile IPv6 provides Transport layer connection survivability when a node moves from one link to another by performing address maintenance for mobile nodes at the Internet layer.

MIPv6 is defined by:

- Mobility Support in IPv6 (June 2004)
- Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents

Goals of IPv6 mobility:

- Always on IP connectivity,
- Roaming between different L2 technologies (WLAN, WiMAX, GSRP, fixed),
- Roaming between different (sub)networks (Huge WLAN deployments mostly use different L3 subnets),
- Application continuity (Session persistence),
- Static IP Adresses for mobile nodes,
- Mobile devices may act as servers,
- Bootstrapping MIPv6 - No static configuration of Home Agent (A router on the home network which represents the Mobile Node while it's not attached with the home network) address and Home Adress on mobile nodes,
- Network mobility (NEMO) (Instead of node mobility) IETF working group with focus on mobile networks (e.g. prefix delegation)
- Mobile adhoc networks (MANET) - Interworking of Mobile Ad-hoc networks and Mobile IPv6 Networks:
    - Mobile node roaming in between MIPv6 and MANET
    - MANET roaming as a MIPv6 client
- Signaling and Handoff Optimization
    - Fast Handovers for Mobile IPv6 (FMIPv6)
    - Hierachical MIPv6 mobility management (HMIPv6)

- Cryptographically generated (IPv6) addresses

Mobile Node can prove that it owns its Home Address by including its public key in the binding update and by signing the resulting message (No public key infrastruture needed).

3.2 Cisco Systems

Cisco IPICS Push-to-Talk Management Center

The Cisco IP Interoperability and Collaboration System (IPICS) Push-to-Talk Management Center (PMC) client is a Microsoft Windows-based application that enables push-to-talk (PTT) functionality for PC users. It allows users to communicate over and monitor broadcasts of multiple channels of communications at the office or from a remote site.

The Cisco IPICS PMC client extends communications of existing PTT radio channels or broadcast networks. With this system, users can participate in multiple channels of communication. The ability for users to also respond to incidents or emergencies by using a Cisco IPICS PMC on their PCs, boosts organizational responsiveness as well as operational efficiency and effectiveness.

Cisco IPICS PMC users can be added to new communication channels as incidents or needs arise. Users have communication access not only to PTT radio channels, but also other online IPICS PMC users, phones users, or virtual talk groups (VTGs) made up of multiple channels and communication device types, such as mobile phones and IP phones. An operations manager or dispatcher remotely manages the availability of these channels, allowing for quick and efficient response to escalating events.

An integral component of Cisco IPICS, the Cisco IPICS PMC is a licensed application hosted by the Cisco IPICS Server. The Cisco IPICS PMC works in conjunction with the server to receive its configuration, updates and upgrades, management, authentication, and alert tone distributions. Other Cisco IPICS system components include the IPICS Policy Engine, IPICS Phone Client, IPICS Operational Views (Ops Views), Land Mobile Radio (LMR) gateways, Router Media Service (RMS) gateways, and Session Initiation Protocol (SIP) telephony gateways.

Cisco IPICS is a systems-level, network-based solution for voice interoperability. It takes full advantage of open IP standards and IP network infrastructure for better flexibility, scaling, and security.

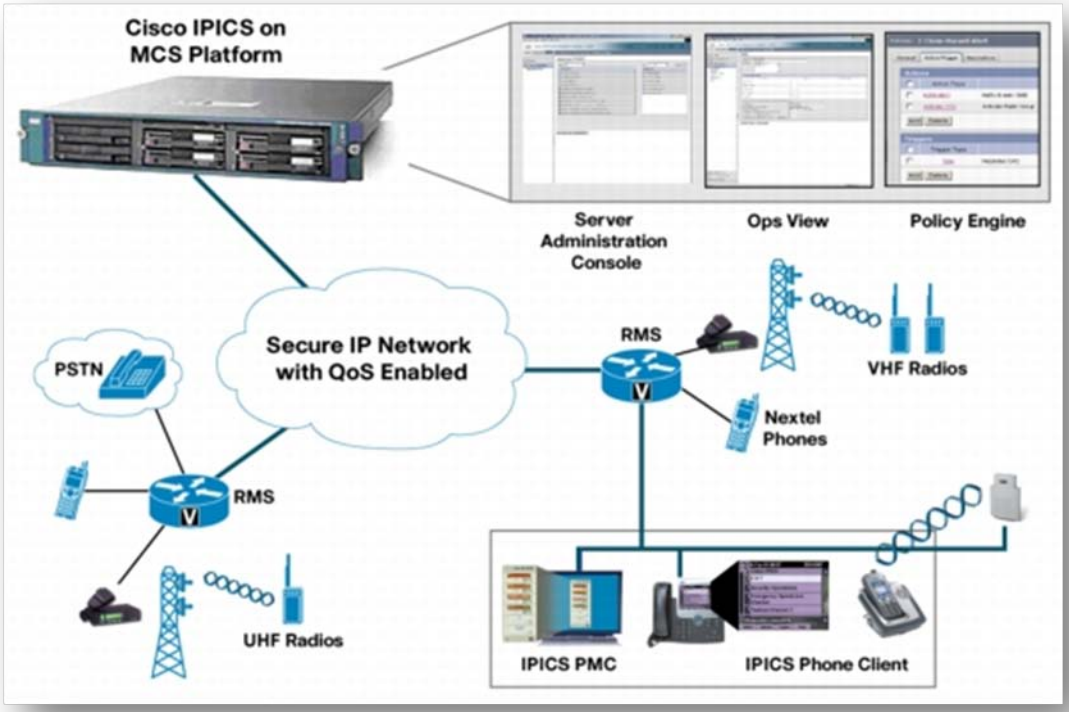

Figure 17: Cisco IPICS Solution

3.2.1 Cisco Unified Wireless IP Phone 7921G

Cisco IP Phone 7921G is example of IP phone supporting Push-to-Talk:

Figure 18: Cisco IP Phone 7921G

This second-generation wireless IP phone supports a host of calling features and voice-quality enhancements, including:

- IEEE 802.11a, b, and g standards that allow customers to use the phone in the 2.4 GHz or 5 GHz bands

- Built-in speakerphone capabilities
- A functional combination charger and speakerphone
- Dedicated mute and volume keys, and separate Application button that can support Push-to-Talk via Extensible Markup Language (XML)
- Battery life about 200 hours standby time or 15.5 hours talk time
- High durability for all business environments
- Exceptional voice quality with support for wideband audio
- Diversity antenna for better RF coverage
- Support for wide range of enterprise applications through XML
- Wireless security features including LEAP, PEAP, EAP-FAST, EAP-TLS, WPA, WPA2, CCKM, WEP, TKIP/MIC, AES
- Voice security features including Certificates, Secure Real-Time Protocol (SRTP), and Transport Layer Security (TLS)
- Quality of service features including WMM, TSPEC, EDCA, QBSS

3.3 Nokia Mobile Device IPv6 Support

Network layer IPv6 support in:

- Nokia Series 40 (S40) and Series 60 (S60) platforms - Nokia 6630, 6680, 6681, 6280, 7270, 7710
- Nokia Nseries devices: N70, N71, N80, N90, N91, N92, N95
- Nokia Eseries devices: E50, E60, E61, E65, E70
- Nokia Communicator: 9500, 9300, 9300i (WLAN)
- IPv4/IPv6 dual-stack in Symbian since 7.0s, 8.0 and 9.1

Application layer support for IPv6:

- All IMS applications support IPv6
- SIP stack supports both IPv4 and IPv6 - IPv6 supported for all SIP applications like Video Sharing, PoC. Nokia 6680 was used in GSMA SIM/IMS trials in both Europe and Asia
- S60 and S80 includes IPv6 support exists all basic applications: Email, Web browser, Real-one player, etc.

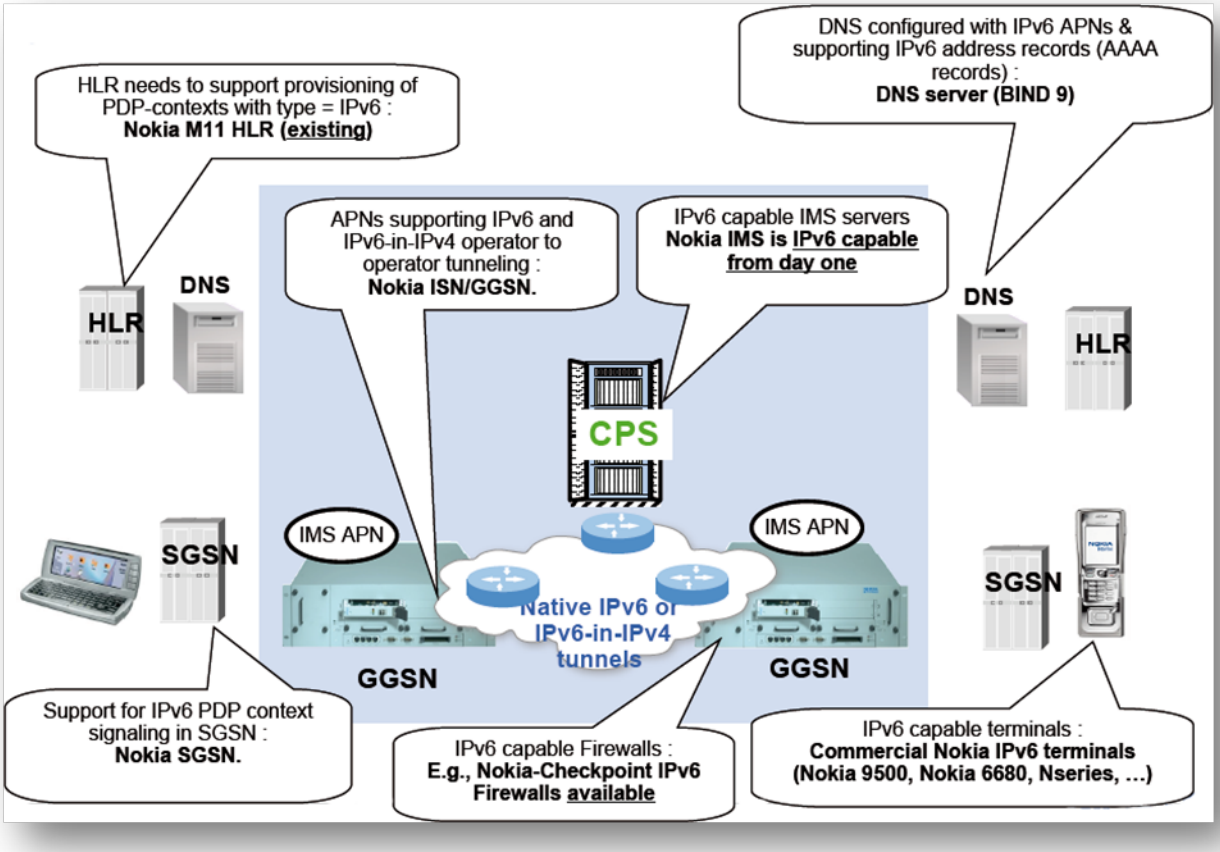

Figure 19: Nokia Networks IPv6 Support

3.4 Voice over Wireless Lan solution by Nortel

3.4.1 Introduction

Voice over Wireless LAN (VoWLAN) represents the coming together of two important and rapidly growing technologies — WLAN and IP Telephony. By seamlessly integrating the IP Telephony system with WLAN infrastructure, users are provided with high-quality mobile voice and data communications throughout the workplace.

Nortel co. gives a VoWLAN solution for users to roam from floor to floor in a building, or around a specified area, while still remaining accessible and connected through a lightweight device. With their own, easy to handling, multi-function handsets integrated into WLAN infrastructure, workers have the ability to stay in constant contact.

WLAN Handsets reside on the WLAN with other wireless devices using Direct Sequence Spread Spectrum (DSSS) radio technology. They operate over an 802.11b WLAN providing users with a WLAN IP Telephony extension off your existing PBX or IP Telephony Call Server. WLAN handsets are not the only way to provide VoWLAN. Soft-clients for handhelds extend mobile voice and data communications to a selection of personal communications devices that may already be in use in the enterprise. Handsets can integrate into existing LAN infrastructure to reduce the costs of implementation.

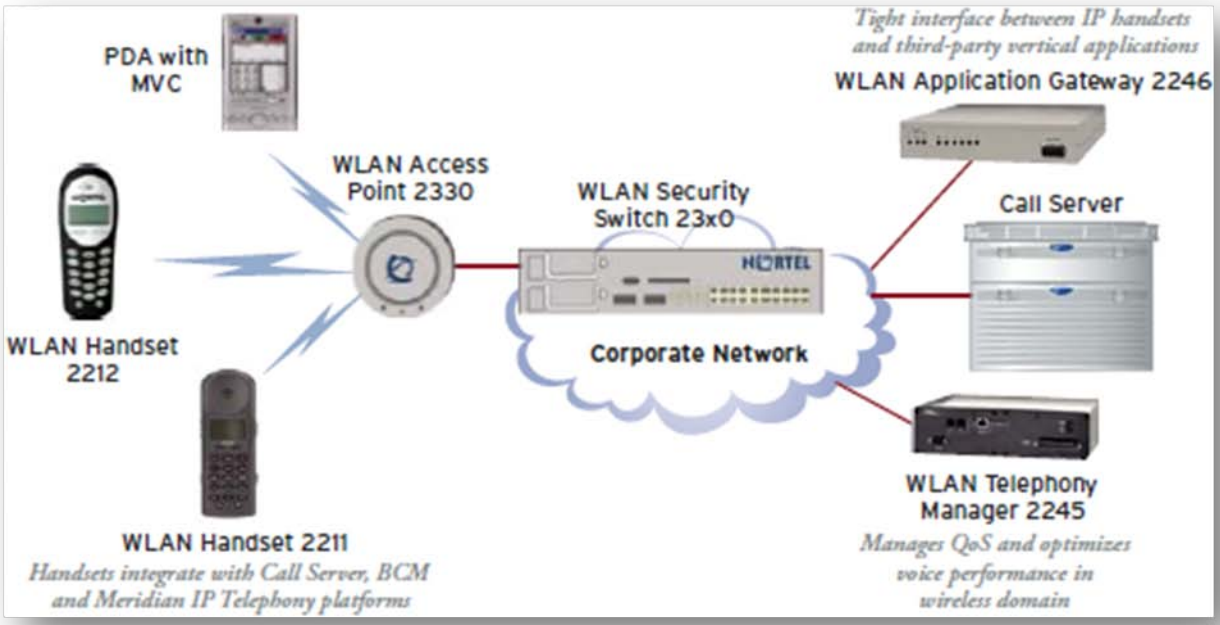

Figure 20: Implementation of VoWLAN with Nortel devices

WLAN Handset most important features:

- Call Forward
- Call Park / Call Park Retrieve
- Call Pickup
- Conference
- Group Call

- Message Waiting Indication / Voice Mail Access
- Quality of Service
- Supports digital and native IP interfaces to most major telephony switches
- Push-to-Talk mode (model 2211 only)
- Integrated TFTP client DHCP or static IP addressing

3.4.2 Nortel WLAN Handset 2211

The industrial-grade design of the WLAN 2211 handset is engineered for demanding environments such as healthcare and manufacturing. It has all the capabilities of the WLAN Handset 2210 and exclusive features such as Push-to-Talk functionality, which allows broadcast communication between employees, eliminating the need for two-way radios or walkie-talkies. The PTT functionality uses IP multicast addresses, requiring that multicasting be enabled on the subnet.

3.4.3 Soft Clients for handhelds

The Nortel Multimedia Communication Server (MCS) 5100 enables businesses to augment existing voice and data infrastructures with advanced IP-based multimedia and collaborative capabilities. The wireless client for RIM handhelds supported in Multimedia Communication Server 5100 Release 3.5 brings new tools to the mobile worker with SIP-based multimedia communications including presence, instant messaging and click-to-call — together with the traditional RIM productivity services organizer and e-mail applications. This client is supported on BlackBerry 6xxx and 7xxx devices including the newly introduced 7270 for campus-based communications.

The BlackBerry is a wireless handheld device introduced in 1999 as a two-way pager. In 2002, the more commonly known smartphone was released, which supports push e-mail, mobile telephone, text messaging, internet faxing, web browsing and other wireless information services. It is an example of a convergent device. Some models (currently, those manufacturers for use with iDEN – Integrated Digital Enhanced Network - networks such as Nextel and Mike) also incorporate a Push-to-Talk feature. The BlackBerry solution is approved and used by: White House, American Congress, US Army, US Air Force, The Government of Canada (also local authorities), members of Government of Poland, The Netherlands, Germany and Austria, police and fire services in many European countries.

3.5 Sprint Nextel Dispatch Solution

3.5.1 Optimal interoperability for public safety

One of the major issues facing the public sector is the inability of emergency service workers including traditional “first responders” to communicate with one another when the need arises.

The Nextel National Network serves as the ideal solution to complement existing LMR systems in USA. Unlike those of other cellular carriers, the Nextel network is actually a nationwide digital 800 MHz trunked radio system. This differentiation provides tremendous possibilities for the public sector and first responders. The following diagram highlights a very important point about the Nextel National Network.

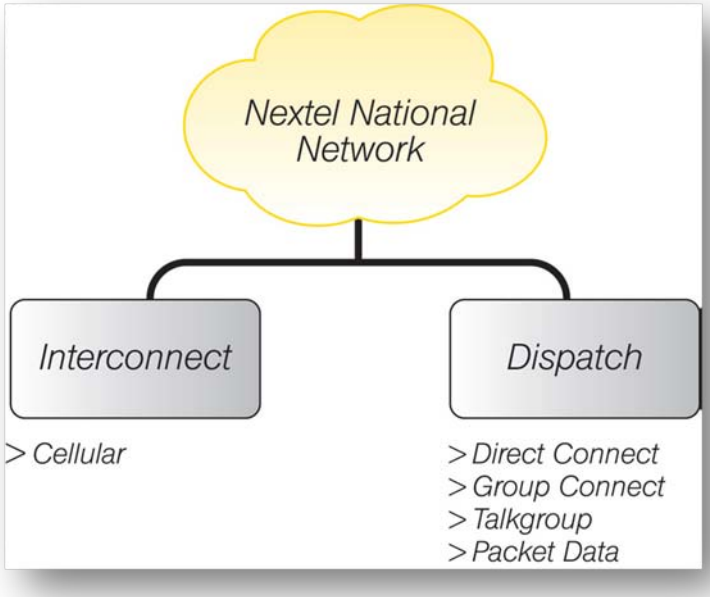

Figure 21: Dispatch services on a dedicated, private network

3.5.2 VoIP-Based Dispatch Solutions

Over the past decade Voice over IP (VoIP) has matured and evolved into to a reliable, secure solution for Public Safety dispatch communications. As VoIP has been applied to dispatch communications it's become known throughout the industry as Radio Over IP (RoIP). VoIP dispatch systems result in very cost effective radio communication solutions that make use of a customer's existing private IP and radio networks. Because communications utilizes IP, there are absolutely no boundaries or confines – a dispatch operator can be anywhere his/her job requires them to be, even if they're mobile. Additionally, a dispatch operator has the ability to communicate with and establish interoperability between any and all radio systems that are part of the solution.

Interoperability is not limited to Nextel and LMR systems; VoIP can effectively connect telephone systems, intercom systems and satellite based push-to-talk services for dispatch communications regardless of geographic territory. VoIP is also a very user friendly, flexible and scalable tool. A basic solution would include a Windows-based PC to run the dispatch client, an IP to Radio interface and some number of radio control stations (or access radios). This configuration can scale very easily to include any number of client PCs, any number of radio interfaces and the number of end users is virtually unlimited. Finally, because IP is fundamentally a distributed architecture, these solutions can be built as redundant and fault tolerant as needed with no single point of failure.

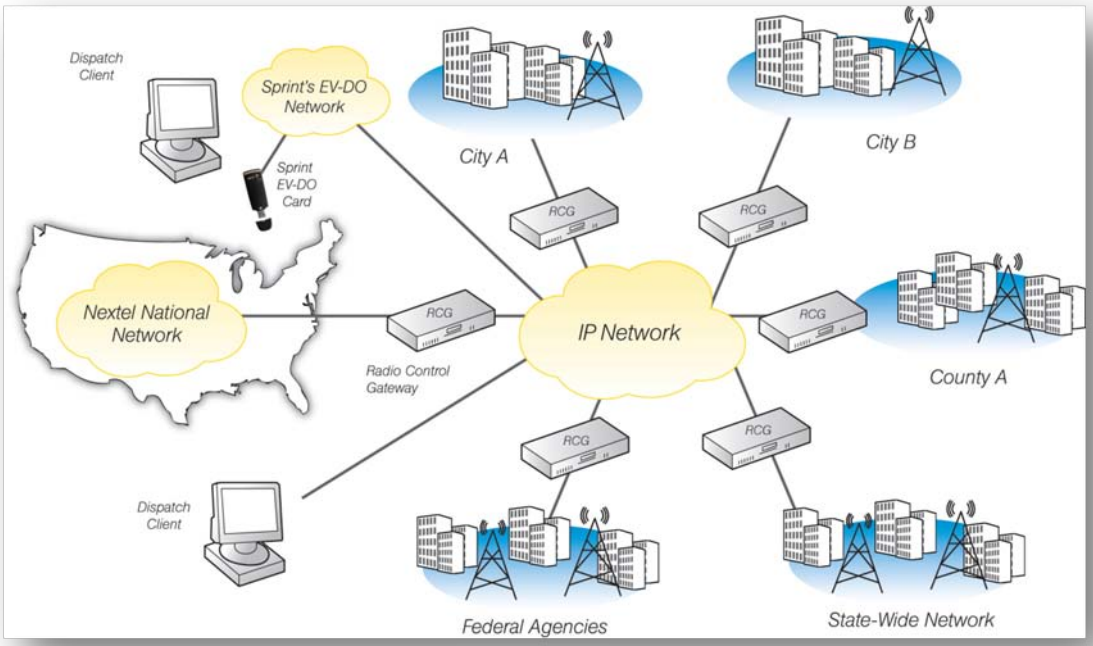

Figure 22. Dispatch VoIP: Increased Redundancy, Mobility and Interoperability

3.5.3 Nationwide interoperability and emergency response support

Critical to the success of any interoperability plan is communications between local, regional, state and federal responding agencies – regardless of jurisdiction, discipline or location. The solution must be flexible enough to be useful on a daily basis, but ubiquitous enough to span the broadest range of agencies, geographies and applications. One critical point that has been identified at a number of large-scale events is that there is a need for another way to communicate if the primary radio system fails or becomes overloaded. Integrating the Nextel nationwide radio network with regional private radio systems creates system of systems – essentially a radio system overlay that can be integrated into any and all radio systems.

A parallel method of communications allows for logistical conversations to take place without interfering with the main public safety radio systems. This parallel concept also offers a way to interconnect agencies that are not affiliated with public safety but are essential to successful mitigation of large-scale emergencies/events.

During the catastrophic events at the Pentagon and the World Trade Center for example, primary public safety radio systems were overwhelmed with radio traffic, sometimes rendering them ineffective. In both of these cases the use of Nextel Direct Connect was very important to first responder operations.

Figure 24 shows an example of large-scale, unified, multi-agency, multi-jurisdictional incident command. In this example, users of LMR systems and Nextel handsets can be coordinated seamlessly and interconnected as needed, in real time. In this example, a federal agency resource is contacted using Nextel Direct Connect and patched to the on-scene incident commander under the control of Emergency Dispatch Operations.

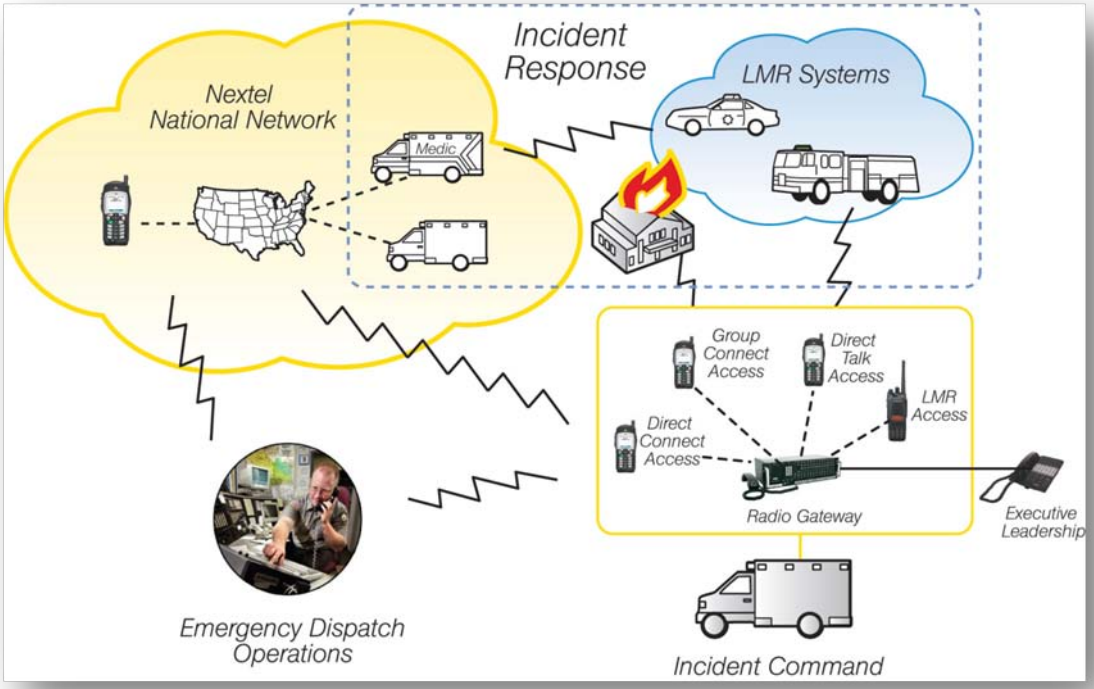

Figure 23: Incident Response and Command

3.5.4 Tactical/incident command interoperability

To address the challenges of on-scene command and control, Sprint has partnered with industry leading manufacturers of radio cross-connect devices. These solutions greatly improve the Incident Commander's ability to achieve on-scene, real-time interoperable communications. Under the control of Incident Command, Nextel Direct Connect and Group Connect services can be interconnected with Land Mobile Radio users as needed.

One extremely powerful benefit of this solution is the ability to bridge (patch) Nationwide Nextel Direct Connect calls into local/regional, first responder talkgroups. For example, during an emergency situation, federal agencies using Nextel Direct Connect can communicate directly with local agencies communicating on LMR talkgroups, Nextel Talkgroups or both. Agency interconnectivity can be accomplished under the control of Incident Command or Dispatch Operations. Figure 25 shows how Nextel Direct Connect can be combined with both Land Mobile Radio talkgroups and Nextel Talkgroups.

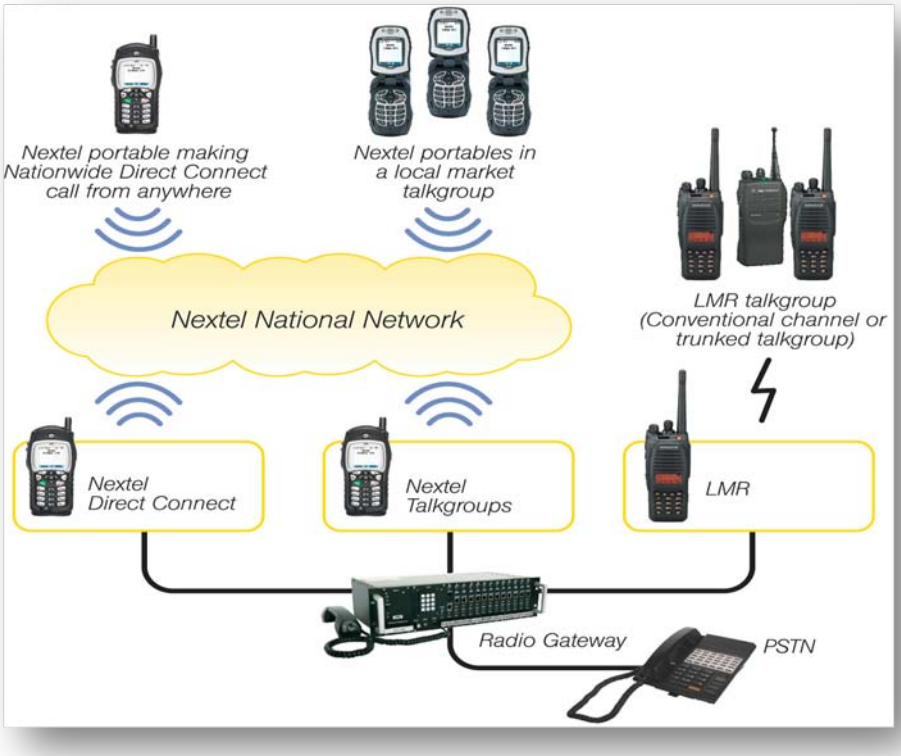

Figure 24: Combining Nextel Direct Connect, Nextel Talkgroups and Land Mobile Radio Talkgroups and/or Channels

3.5.5 Communications assurance in times of crisis

Sprint can provide rapid, temporary increases in capacity and coverage in response to major events across the country. This increase in coverage and capacity can be provided at our existing cell sites, at the local level or through our Emergency Response Team (ERT). Sprint's ERT supports high-volume, short notice equipment needs of our customers with its substantial inventory of COW's (Cell-sites On Wheels), SatCOLTs (Satellite Cell-sites On Light Truck), microwave facilities, ruggedized handsets, and command-and-control solutions based on radio interconnect devices. Sprint's implementation managers and engineers are accustomed to deploying communications infrastructure both within and outside traditional cellular network coverage areas.

3.6 Requirements for critical networks formed by Alcatel-Lucent

3.6.1 Introduction

Designing a public safety network is a complex undertaking. Each public safety agency has specific needs based on operational objectives. Alcatel-Lucent take notice that deploying a network has many constraints, including geographic location, terrain, regulatory framework and spectrum availability and all these factors must be considered when designing the network. Reducing response times, while coordinating emergency personnel, is essential to public safety. The foundation for coordination is an integrated, mission-critical mobile communications network that is reliable and secure and can be upgraded with new services and capabilities as needed. Although individual agencies require their own network, the challenge is ensuring integrated communications across multiple agencies, enabling coordinated intervention by an array of first responders.

Many public service organizations have existing, analog-based voice networks and need to migrate to new networks with IP capabilities. These agencies must ensure a smooth transition from their legacy systems to a digital Private Mobile Radio solution based on industry standards such as Terrestrial Trunked Radio (TETRA) or APCO 25. To operate effectively, first responders require crucial, large bandwidth services, such as, real-time video surveillance, mobile interactive video and remote database access. For many organizations, the solution is to deploy a separate wireless broadband network using mass-market radio access technologies such as WiMAX or CDMA.

3.6.2 A solution

An example of a standards-based mission-critical broadband wireless infrastructure is the Alcatel-Lucent public safety solution based on CDMA2000® 1xEV-DO Revision A (DO Rev A). DO Rev A meets the special requirements of mission-critical first responder high-speed data communications. Operating in the 700 MHz band, DO Rev A dramatically exceeds the limited range of solutions deployed in the 4.9 GHz public safety band (approximately 300 yards or less with line-of-site coverage). Broadband technologies in the 700 MHz band range up to 29 kilometers (depending on the terrain) in urban, suburban and rural environments, ensuring lower cost, higher capacity coverage per square kilometer. And, broadband delivers the speeds and low latency needed to support real-time multimedia communications (Figure 26).

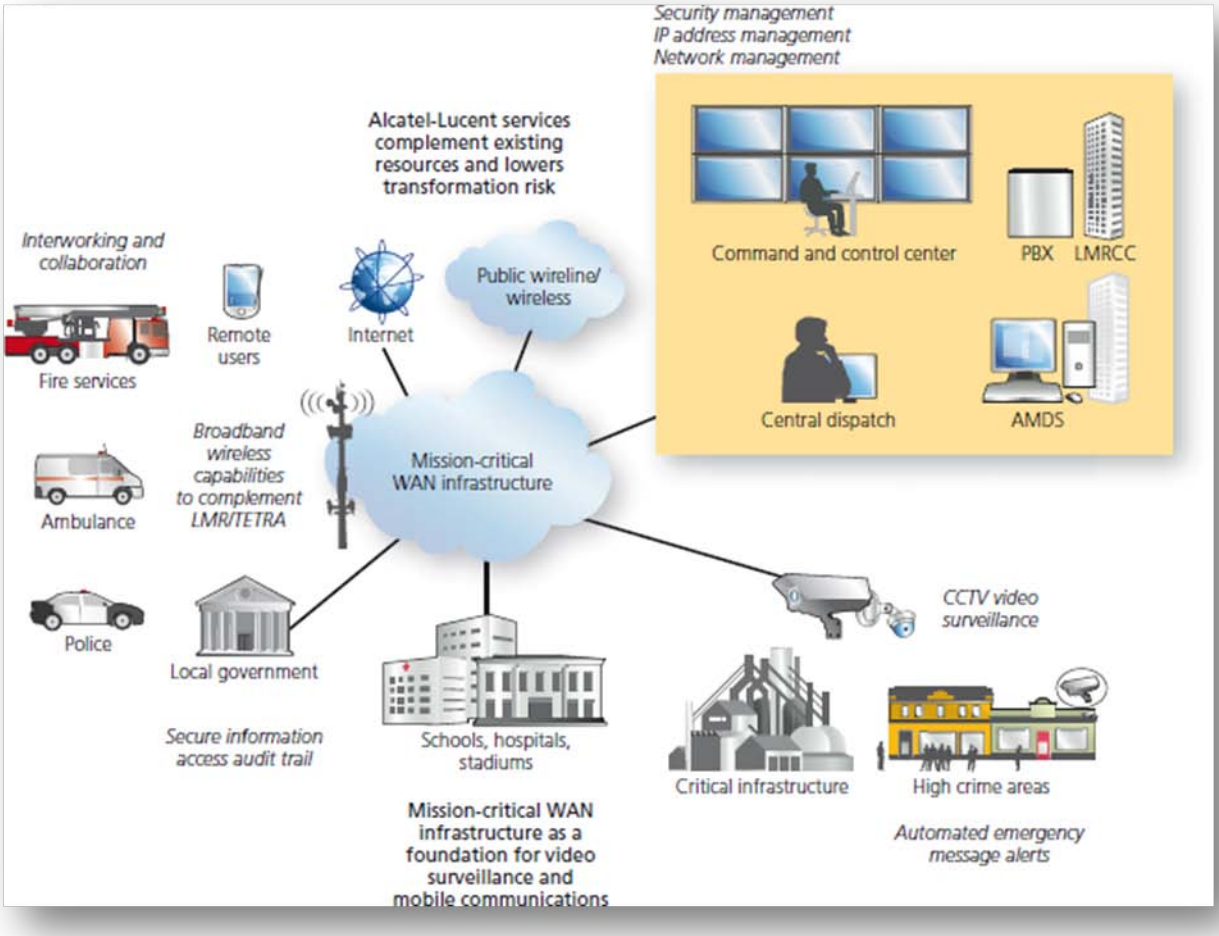

Figure 25. Mission-critical WAN infrastructure for public safety applications

With peak transmission rates up to 3.1 Mb/s, DO Rev A technology supplements existing LMR (Land Mobile Radio) networks supporting a range of advanced multimedia services, such as streaming video, multimedia messaging, web access and backup push-to-talk service.

The standards-based CDMA solution leverages the economies of scale of commercial 3G network deployment and allows interoperability between public safety broadband and commercial 3G wireless networks. As commercial CDMA networks evolve to 4G, the public safety 700 MHz solution will integrate and leverage the improved capabilities of new technologies such as LTE (Long Term Evolution).

Key to the broadband wireless solution is the fixed wide area network (WAN) that connects the antennae sites. This mission-critical infrastructure enables reliable broadband traffic between antennae sites and fixed locations with scalability to support evolving and growing information flow. A combination of microwave, IP/MPLS and optical technologies are often utilized in this infrastructure. In addition, this WAN enables the consolidation of traffic from the agency's fixed sites and mobile first responders for increased efficiency and flexibility.

3.7 Assured Delivery of Business Critical Applications

By design, IP provides both guaranteed and non-guaranteed packet delivery. The choice is often made by the business application developer depending on requirements, network latency/capacity and the environment in which the application is to be used. Also, some of the applications are general purposes in nature and hence it is difficult for a designer to predict the manner by which application will be used and the environment where it would be deployed. In practice, it is often the case that business applications are deployed in areas for which they were not designed. For example, the designer may elect to design the application on a fast errorless LAN. However, application deployment may subsequently be over wireless links with varying capacity and latency.

For critical business operations, it is possible for an application that provides no traffic delivery guarantees to be deployed or the application may not reliably function over the given network. Clearly, due to its design or the nature of its deployment, the application will lead to an increased risk to the business operation of which the application is a part.

One solution is to re-design the offending application itself. However, such solution is either impractical or costly. Another solution concept is presented in Figure 27, where four IP sub-networks contain applications whose traffic is required to be assured. By their design, these end IP sub-networks use routing device as their means of connectivity to the wide area network. In this case, each sub-network is shown to have three connections to the WAN and hence policy-based (PB) multi-bearer routing (MBR) becomes a necessity if elements of resilience are to be deployed. It is possible to extend the policy-based multi-bearer routing to also provide for traffic delivery assurance. Thus, the indicated traffic-delivery assurance routing (TDAR) in Figure 27 combines both the functionality of an MBR and a TDAR, where the both share the same PB configuration mechanism.

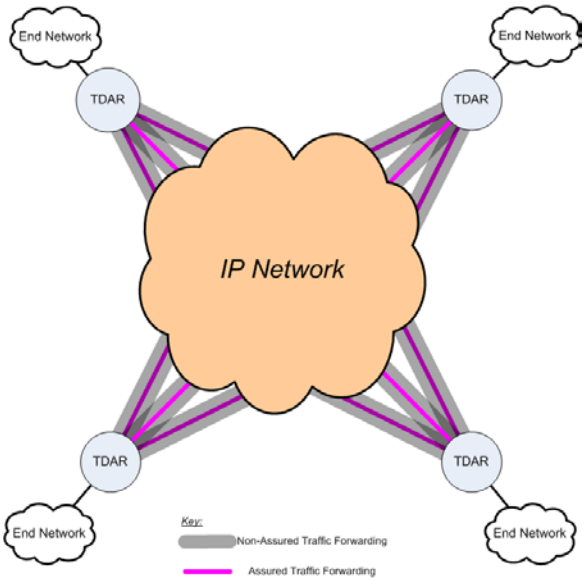

Figure 27: Policy-Based Traffic Delivery Assurance Routing (TDAR)

3.8 TETRA

TETRA (TErrestial Trunked RAdio; formerly known as Trans European Trunked RAdio) is a set of digital trunked mobile radio standards covering different technology aspects (such as air interfaces, network interfaces and its services and facilities). It was developed since 1992 by the European Telecommunications Standards Institute. The main target was to enable independent manufacturers to develop devices (infrastructure and radio terminals products) which would fully interoperate within each other. TETRA is the only official European Standard for digital Professional Mobile Radio (PMR).

In Europe, for public emergency services European Radio communications Committee (ERC)[2] reserved the common radio width 380-385MHz / 390-395Mhz for the trunking systems compatible with TETRA. Those systems by using this radio width are commonly known as TETRA-E. For Private Mobile Radio (PMR) and Public Access Mobile Radio (PAMR) the radio width of 410-420MHz / 420-430MHz and 450-460MHz / 460-470MHz is used in Europe. Elsewhere, the 800MHz band is mostly used.

3.8.1 TETRA system architecture

TETRA is allowing effectively transmitting through the radio carrier speech and data in packed or circuit switched mode. Essential requirement of this system is the possibility of cooperation of this system used by different authorities. Overview of TETRA architecture is show bellow.

[2] ERC Decision of 7 March 1996 on the harmonized frequency band to be designated for the introduction of the Digital Land Mobile System for the Emergency Services (ERC/DEC/(96)01) http://www.erodocdb.dk/Docs/doc98/Official/Pdf/DEC9601E.pdf

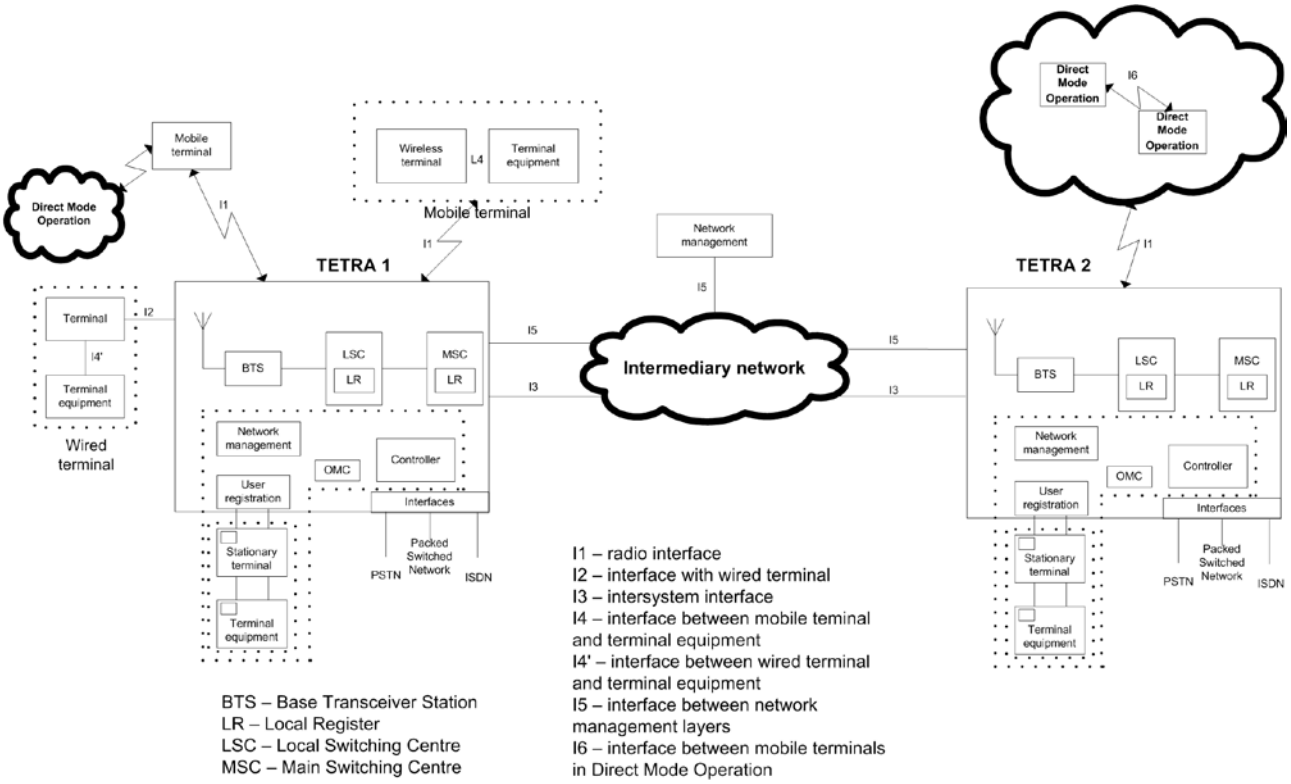

Figure 28: TETRA network architecture

Tree main parts can be distinguished: terminals, base stations and part of network commutation. In commutation part are located the main and local switchboards. Local switchboards are dependent of the main switchboard. Their role is to cooperate between controllers in modern telephone switchboards and controllers in base stations in GSM. Commutation part contains the user registration, exploitation and network maintain center. This part also contains mediate modules which supports cooperation with external set of devices, like PSTN, ISDN or packed switched networks. The base stations are connected to local switchboards.

In TETRA system we can distinguish two types of terminals – mobile and stationary, which are typically used by DYSPOZYTOR SYSTEMU. As in GSM, the terminals can support the basics functions like speech transmission, and others services like data transmission. The TETRA network can be connected with others TETRAs operator networks.

Beside Direct Mode Operation (DMO) between terminals it is possible to use the terminals as a gateway or repeater (as shown below).

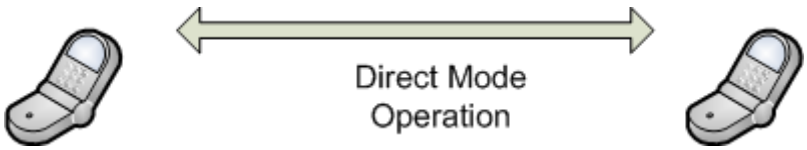

Figure 29: Direct Mode Operation

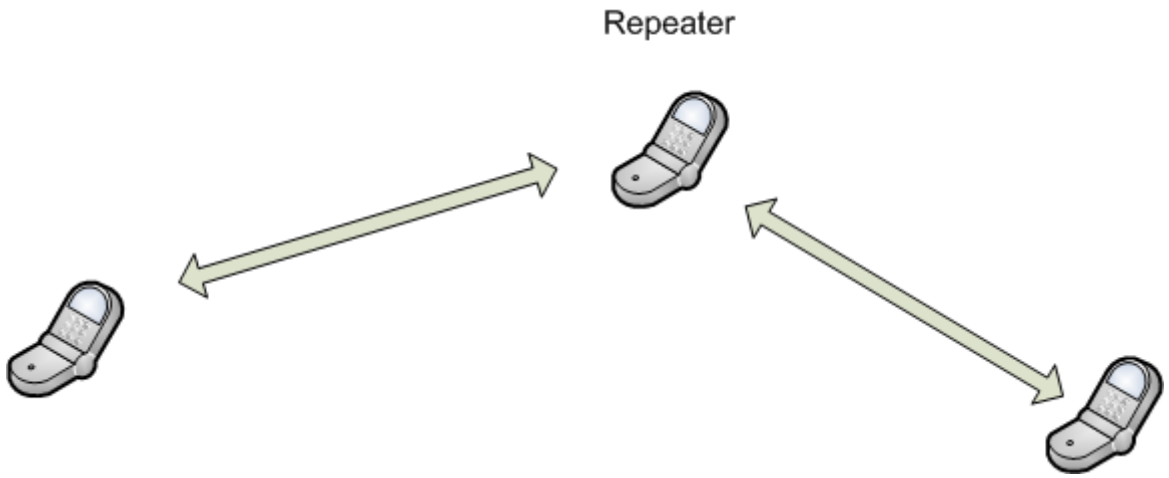

Figure 30: Communication thru repeater

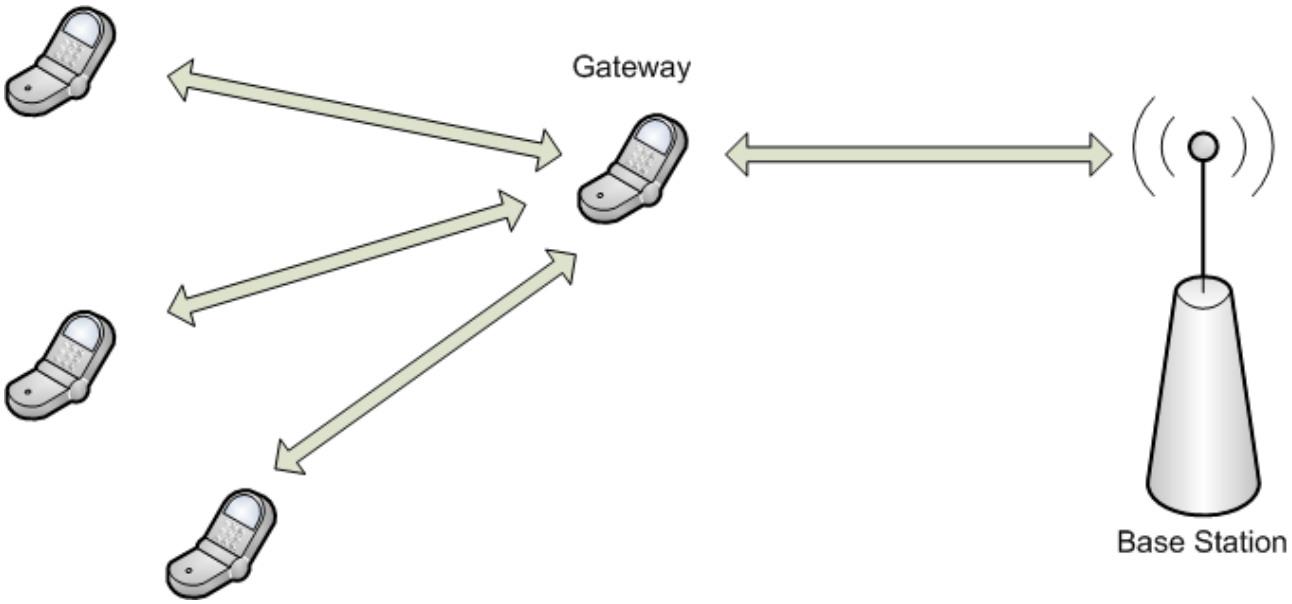

Figure 31: Communication thru Gateway

3.8.2 Radio channel

As frequency spectrum resource is very limited, effective usage is very important. As GSM, TETRA is based on mixed channel access method – TDMA and FDMA. Allotted to the users radio width is divided into 25kHz channels, and every channel has frame structure for four speech channels. As a result, the effective radio width used for a single speech transmission is 6.25kHz. Analogues system typically uses 25kHz or 12.5kHz carrier, so TETRA is 2 or 4 times more effective. On top of that, digital technology provides better area coverage. Another pros of using the same carrier width is an easier migration from analogues systems to TETRA. Transmission at radio channel uses π/4 DQPSK modulation. Speech signals are sampled at 8kbps; compressed with a vocoder creates a data stream of 4,8. The summary bandwidth at one carrier is 19.2 kbps (36kbps with protective coding). The ALOHA algorithm is used for channel access. Both point – to – point and point – to – multipoint transfer can be used. Main TETRA features are shown bellow.

Parameter	*Value*
Modulation	π/4 DQPSK
Spacing	25 kHz
Number of channel at one carrier	4
Channel access method	FDMA/TDMA
Total bandwidth at one carrier	19.2 kbps
Total bandwidth at one carrier (with protective coding)	36 kbps
Modulation rate	18 kbauds
Algorithm used for channel access	ALOHA
Time needed to set up a connection	Less than 300 ms
Time needed to switch between base stations	Less than 1 s
Terminal power output	1, 3, 10 W
Cells size	Several dozen km
Terminal maximum speed	Less than 200 kmph

3.8.3TETRA System modes

TETRA standards defines two main modes:

- Voice plus Data (TETRA V+D) – support voice and data transmission.
- Packet Optimized Data (TETRA POD) – supports only data transmission.

TETRA V+D is circuit switched network; speech is transmitted in previously described radio channels. The bandwidth for data transmission is associated "as needed" - from one to four time slots can be used at a carrier, which gives a bandwidth from 4.8kbps to 19.2 kbps. It shall be noticed, that TETRA V+D support direct connection between terminals, without intermediary devices (eg. base station).

TETRA POD is optimized for data transmission and shall be used in application, where a speech transmission is not required. At this mode, system can work in connection or connectionless oriented mode. This mode also supports traffic priorities, as well as unicast and multicast packet flow with bandwidth up to 19.2kbps.

3.8.4 Network procedures in the TETRA system

Each intercommunication system to function well needs many network procedures. In TETRA system we define such procedures as:

- Switching channels between base stations.
- Change of the area location by mobile station.
- Terminal migration into other TETRA network.
- Terminal identification.
- Session commencement and finalizing.

- Assigned user to terminal.
- On terminal request interrupting and starting information transition on downstream.

Those procedures in many aspects are similar to GSM procedures. They are used in standard TETRA as described below.

Similar as in GSM, decision about cell switching is made by the terminal based on the strength and quality of signals received from neighbour base stations. If terminal is found outside network area in within its registered, it can use the other operators resources, if allowed (depending on TETRA operators agreements).

Very important aspect of TETRA standard, especially if used by such authorities as Police, Army etc. is a system security to prevent unauthorized access to the services and information, as well as stolen terminals usages. Each time a terminal is registered in the system, the identification procedure is made. Those methods are similar as in GSM. They help the identification and localization of stolen terminals. User before accessing the network must authorize himself by using identification card or password. This enhances system security and allow user to use different terminals.

3.8.5 Services

The main services available in TETRA are:

- Multicast Or unicast, half duplex or full duplex speech transmission.
- Data transmission, encrypted or not, with a various level or error correction codes.
- Maximum bandwidth between 9.6kbps (with strongest error correction codes) to 28.8kbps (without error correction codes).
    - Data transmission - 7.2/14.4/21.6/28.8 kbps
    - Protected data transmission – 4.8/9.6/14.4/19.2 kbps
    - Strongly protected data transmission – 2.4/4.8/7.2/9.6 kbps
- Packed data transmission, with or without acknowledges.
- Call redirection.
- Call restriction (incoming or outgoing, from or to specified group of users).
- User groups managing.
- Short Data Service (SDS) and status messaging.
- Support for Value Added Services (VAS).
- Immediate, simultaneous connectivity to a subgroup of users.
- Priorities.

- Storing messages for temporary unavailable users, and delivering it when a user log on into network.
- Discrete listing (A privileged user can eavesdrop other users calls).

3.8.6 Air – Ground – Air

The TETRA Air-Ground-AIR (TETRA AGA) services have been developed to provide similar TETRA services to devices in the air, on a water and on a ground. TETRA AGA support basic services such as video and data or mobility management, but are not supporting TETRA High Speed Data (TAPS/TEDS).

The specification of air and naval propagation environments relates on for example less attenuation, so the cell radius can be significantly larger than at urban or suburban environments. The Air – Ground - Air service changes the TDMA frames properties, which allows to maximizing mobile reception from 58 to 83. The side effect of such change is a reduction of total available bandwidth per km^2. It also resolves problem of switching between large cells (larger, but with less capability - what better suits the naval and air needs) and ordinary ones (where the traffic is much larger) by reducing or denying to switch from ordinary to AGA cells, to ensure the quality of service to designated users.

From initiation of Baltic countries - Finland, Estonia, Sweden and Norway there are attempts to use TETRA system in naval communications. In Gulf of Finland Tetra system is already in use in VIRVE, which is the commencement of naval networks in the coast. Network VIRVE is using original bandwidth of TETRA system – 450MHz. Other concept allowing the coexistence of both technologies at the same time (TETRA with currently used FM communication system) using the same radio width of 156-174MHz; which would allow smooth migration.

3.9 TETRA2 (TEDS)

The evolution of TETRA standards lead to broadband services. TETRA Release 2 (TEDS – TETRA Enhanced Data Service) offers improvements as:

- Minimum bandwidth of 50kbps (on the edge of cell).
- Simultaneous data and voice transmission.
- Reduction of maximum terminals power output to 1W for mobile terminals and 3W for nomadic terminals.
- Prioritization for speech transmission.
- Multiple modulation types:
    - 4 QAM – on the edge of cell.
    - 16 QAM – for medium bit rate.
    - 64 QAM for high bit rate.
    - π/4 DQPSK for control transmission.

- D8PSK

- Varied types of radio width – 25, 50, 100 and 150 kHz.
- Parallel Concatenated Convolution Coding (PCCC).

3.10 Existing TETRA implementation

- VIRVE (Finland's public safety network), covering 350,000 km^2 is one of the largest TETRA public safety network. It operates since 1998.
- Hong Kong Police uses TETRA since a year 2000; this network coverage the whole Hong Kong.
- Used during Olympic Games in Beijing 2008, providing secure and seamless communication for nearly 90.000 people involved in organization and setting up to 1.6 million calls a day.
- Beijing Government's Just Top network (China).
- RAKEL (Sweden – under construction now) is planned to cover 450,000km^2, and will become the world's largest PMR system.
- Krakowski Szybki Tramwaj (Cracow, Poland) – the TETRA system have developed In a public communications system in cooperation legacy VHF system, sharing the same radio width.

4. IPv6 multitasking

Previous chapter analyzed all group solutions. In this chapter we like to focused of IPv6 multitasking possibilities, what Secricom project will used in own solution. First part of this chapter is tutorial of IPv6 necessary for understanding IPv6, second part looks at multicast specific issues.

4.1 IPv6 facilities

The IPv6 is nowgaining momentum as an improved network layer protocol. There is a lot of commercial interest and activity in Europe and Asia, and as of press time, there was also some traction in the United States. For example, the U.S. Department of Defense (DoD) announced that from October 1, 2003, all new developments and procurements needed to be IPv6 capable; the DoD.s goal was to complete the transition to IPv6 for all intra- and internetworking across the agency by 2008. In 2005, the U.S. Government

Accountability Office (GAO) recommended that all agencies become proactive in planning a coherent transition to IPv6. The expectation is that in the next few years, a transition to this new protocol will occur worldwide.

The current version of IP, IPv4, has been in use for almost 30 years and exhibits some challenges in supporting emerging demands for address space cardinality, high-density mobility, multimedia, and strong security. This is particularly true in developing domestic and defense department applications utilizing peer-to-peer networking.

IPv6 offers the potential of achieving the scalability, reacheability, end-to-end interworking, QoS, and commercial-grade robustness for data as well as for Voice Over IP (VoIP), IPTV distribution, and triple-play networks; these capabilities are mandatory mileposts of the technology if it is to replace the Time Division Multiplexing (TDM) infrastructure around the world.

IPv6 was initially developed in the middle 90s of last century because of the anticipated need for more end-system addresses based on anticipated Internet growth, encompassing mobile phone deployment, smart home appliances, and billions of new users in developing countries (e.g., in China and India). New technologies and applications such as VoIP, “always-on access” (e.g., DSL and cable), Ethernet to- the-home, converged networks, and evolving ubiquitous computing applications will be driving this need even more in the next few years. A converged network utilizing IPv6 supports both local- and wide-area components as well as private and carrier-provided communications domains; the IPv6/IPv4 network can support video delivery, VoIP, Internet, intranet, and wireless services.

Basic Network Address Translation (NAT) is a method by which IP addresses (specifically IPv4 addresses) are transparently mapped from one group to another.

Specifically, private “nonregistered” addresses are mapped to a small set (as small as 1) of public registered addresses; this impacts the general addressability, accessibility, and “individuality” of the device. Network Address Port Translation (NAPT) is a method by which many network addresses and their TCP/UDP ports are translated into a single network address and its TCP/UDP ports. Together, these two methods, referred to as traditional NAT, provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses.

NAT is a short-term solution for the anticipated Internet growth phenomenon and a better solution is needed for address exhaustion. There is recognition that NAT techniques make the internetworking, the applications, and even the devices more complex and this means a cost overhead. The expectation is that

IPv6 can make IP devices less expensive, more powerful, and even consume less power; the power issue not only is important for environmental reasons but also improves operability (e.g., longer battery life in portable devices, such as mobile phones).

Corporations and government agencies will be able to achieve a number of improvements with IPv6. IPv6 can improve a firm´s intranet, with benefits such as follows:

- Expanded addressing capabilities
- Serverless autoconfiguration ("plug-and-play") and reconfiguration
- More efficient and robust mobility mechanisms
- End-to-end security, with built-in, strong IP layer encryption, and authentication
- Streamlined header format and flow identification
- Enhanced support for multicast and QoS
- Extensibility—improved support for feature options/extensions

While the basic function of IP is to move information across networks, IPv6 has more capabilities built into its foundation than IPv4. A key capability is the significant increase in address space. For example, all devices could have a public IP address, so that they can be uniquely tracked. Today, inventory management of dispersed Information Technology (IT) assets cannot be achieved with IP mechanisms; during the inventory cycle, someone has to manually verify the location of each desktop computer.With IPv6, one can use the network to verify that such equipment is there; even non-ITequipment in the field can also be tracked, by having an IP address permanently assigned to it. IPv6 also has extensive automatic configuration (autoconfiguration) mechanisms and reduces the IT burden, thereby making configuration essentially plug-and-play.

4.2 Overview of IPv6

IP was designed in the 1970s for the purpose of connecting computers that were in separate geographic locations. Computers on a campus were connected by means of local networks, but these local networks were separated into essentially stand-alone islands.

Internet, as a name to designate the protocol and more recently the worldwide information network, simply means "internetwork," that is, a connection between networks. In the beginning, the protocol had only military use, but computers from universities and enterprises were quickly added. The Internet as a worldwide information network is the result of the practical application of IP, that is, the result of the interconnection of a large set of information networks . Starting in the early 1990s, developers realized that the communication needs of the 21st century needed a protocol with some new features and capabilities while at the same time retaining the useful features of the existing protocol.

While link-level communication does not generally require a node identifier (address) since the device is intrinsically identified with the link-level address, communication over a group of links (a network) does require unique node identifiers (addresses). The IP address is an identifier that is applied to each device connected to an IP network. In this setup, different elements taking part in the network (servers, routers, user computers, etc.) communicate among each other using their IP address as an entity identifier. In IPv4, addresses consist of four octets. For ease of human conversation, IP addresses are represented as

separated by periods, for example, 166.74.110.83, where the decimal numbers are a shorthand (and corresponds to) the binary code described by the byte in question (an 8-bit number takes a value in the 0–255 range). Since the IPv4 address has 32 bits there are nominally 2^{32} different IP addresses (approximately four billions nodes if all combinations are used).

IPv6 is the Internet´s next-generation protocol, which was at first called IPng ("Internet Next Generation"). The IETF developed the basic specifications during the 1990s to support a migration to a new environment. IPv6 is defined in RFC 2460, which obsoletes RFC 1883. (The "version 5" reference was employed for another use – an experimental real-time streaming protocol, and to avoid any confusion, it was decided not to use this nomenclature.)

4.3 Some of IPv6 benefits

IPv4 has proven, by means of its long life, to be a flexible and powerful networking mechanism. However, IPv4 is starting to exhibit limitations, not only with respect to the need for an increase of the IP address space, driven, for example, by new populations of users in countries such as China and India and by new technologies with "always connected devices" (DSL, cable, networked PDAs, 2.5G/3G mobile telephones, etc.), but also in reference to a potential global rollout of VoIP. IPv6 creates a new IP address format, so that the number of IP addresses will not exhaust for several decades or longer even though an entire new crop of devices are expected to connect to Internet.

IPv6 also adds improvements in areas such as routing and network autoconfiguration. Specifically, new devices that connect to the Internet will be "plug-and-play" devices. With IPv6 one is not required to configure dynamic nonpublished local IP addresses, the gateway address, the subnetwork mask, or any other parameters. When plugged into the network, the equipment automatically obtains all requisite configuration data.

The advantages of IPv6 can be summarized as follows:

Scalability: IPv6 has 128-bit addresses versus 32-bit IPv4 addresses. With IPv4, the theoretical number of available IP addresses are $2^{32}–10^{10}$. IPv6 offers a 2_{128} space. Hence, the number of available unique node addresses is $2^{128}–10^{39}$.

Security: IPv6 includes security in its specifications such as payload encryption and authentication of the source of the communication.

Real-time applications: To provide better support for real-time traffic (e.g., VoIP), IPv6 includes "labeled flows" in its specifications. By means of this mechanism routers can recognize the end-to-end flow to which transmitted packets belong. This is similar to the service offered by MPLS, but it is intrinsic with the IP mechanism rather than an add-on. Also, it preceded this MPLS feature by a number of years.

Plug-and-play: IPv6 includes a plug-and-play mechanism that facilitates the connection of equipment to the network. The requisite configuration is automatic.

Mobility: IPv6 includes more efficient and enhanced mobility mechanisms, particularly important for mobile networks.

Optimized protocol: IPv6 embodies IPv4 best practices but removes unused or obsolete IPv4 characteristics. This results in a better optimized IP.

Addressing and routing: IPv6 improves the addressing and routing hierarchy.

Extensibility: IPv6 has been designed to be extensible and offers support for new options and extensions.

4.4 Addressing classes of IPv4

With IPv4, the 32-bit address can be represented as AdrClass|netID|host. The network portion can contain either a network ID or a network ID and a subnet. Every network and every host or device has a unique address, by definition. The traditional IPv4 address classes were as follows:

Traditional Class A address: Class A uses the first bit of the 32-bit space (bit 0) to identify it as a Class A address; this bit is set to 0. Bits 1 – 7 represent the network ID and bits 8 – 31 identify the PC, terminal device, or host/server on the network. This address space supports 2_7_2¼126 networks and approximately 16 million devices (2_{24}) on each network. By convention, the use of an “all 1s” or “all 0s” address for both the network ID and the host ID is prohibited (which is the reason for subtracting the 2 above).

Traditional Class B address: Class B uses the first 2 bits (bit 0 and bit 1) of the 32-bit space to identify it as a Class B address; these bits are set to 10. Bits 2 – 15 represent the network ID and bits 16 – 31 identify the PC, terminal device, or host/ server on the network. This address space supports 2_{14}_2¼16,382 networks and 2_{16}_2¼65,134 devices on each network.

Traditional Class C address: Class C uses the first 3 bits (bit 0, bit 1, and bit 2) of the 32-bit space to identify it as a Class C address; these bits are set to 110. Bits 3 – 23 represent the network ID and bits 24 – 31 identify the PC, terminal device, or host/server on the network. This address space supports about 2 million networks (2_{21} – 2) and 2_8 – 2¼254 devices on each network.

Traditional ClassDaddress: This class is used for broadcasting and/ormulticasting: wherein all devices on the network receive the same packet. Class D uses the first 4 bits (bit 0, bit 1, bit 2, and bit 3) of the 32-bit space to identify it as a ClassDaddress; these bits are set to 1110.

Classless Interdomain Routing (CIDR), described in RFC 1518, RFC 1519, and RFC 2050, is yet another mechanism that was developed to help alleviate the problem of exhaustion of IP addresses and growth of routing tables. The concept behind CIDR is that blocks of multiple addresses (for example, blocks of Class C address) can be combined, or aggregated, to create a larger classless set of IP addresses, with more hosts allowed. Blocks of Class C network numbers are allocated to each network service provider; organizations using the network service provider for Internet connectivity are allocated subsets of the service provider´s address space as required.

These multiple Class C addresses can then be summarized in routing tables, resulting in fewer route advertisements. The CIDR mechanism can also be applied to blocks of Class A and B addresses. All of this assumes, however, that the institution in question already has an assigned set of public, registered IP addresses; it does not address the issue of how to get additional public, registered, globally unique IP addresses.

4.5 Network Address Translation in IPv4

IPv4 addresses can be from an officially assigned public range or from an internal intranet private (but not globally unique) block. Internal intranet addresses may be in the ranges of 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. In the internal intranet private address case, a NAT function is employed to map the internal addresses to an external public address when the private-to-public network boundary is crossed.

This, however, imposes a number of limitations, particularly since the number of registered public addresses available to a company is almost invariably much smaller (as small as 1) than the number of internal devices requiring an address.

As noted, IPv4 theoretically allows up to 2_{32} addresses, based on a four-octet address space. Public, globally unique addresses are assigned by the IANA. IP addresses are addresses of network nodes at layer 3; each device on a network (whether the Internet or an intranet) must have a unique address. In IPv4, it is a 32-bit (4-byte) binary address used to identify a host.s network ID. It is represented by the nomenclature a.b.c.d (each of a, b, c, and d being from 1 to 255.

Examples are 167.168.169.170, 232.233.229.209, and 200.100.200.100. The problem is that during the 1980s many public registered addresses were allocated to firms and organizations without any consistent control. As a result, some organizations have more addresses than they actually need, giving rise to the present dearth of available “registerable” layer 3 addresses. Furthermore, not all IP addresses can be used due to the fragmentation described above.

One approach to the issue would be a renumbering and a reallocation of the IPv4 addressing space. However, this is not as simple as it appears since it requires worldwide coordination efforts. Moreover, it would still be limited for the human population and the quantity of devices that will be connected to the Internet in the medium-term future . At this juncture, and as a temporary and pragmatic approach to alleviate the dearth of addresses, NAT mechanisms are employed by organizations and even home users. This mechanism consists of using only a small set of public IPv4 addresses for an entire network to access the Internet. The myriad of internal devices are assigned IP addresses from a specifically designated range of Class A or Class C addresses that are locally unique but are duplicatively used and reused within various organizations. In some cases (e.g., residential Internet access use via DSL or cable), the public IP address is only provided to a user on a time-lease basis, rather than permanently.

A number of protocols can have trouble travel through a NAT device and hence the use of NAT implies that many applications (e.g., VoIP) cannot be used effectively in all instances. As a consequence, these applications can only be used in intranets. Examples include the following:

Multimedia applications such as videoconferencing, VoIP, or video-on-demand/ IPTV do not work smoothly through NAT devices. Multimedia applications make use of RTP and Real-Time Control Protocol (RTCP). These in turn use UDP with dynamic allocation of ports and NAT does not directly support this environment.

Kerberos authentication needs the source address and the source address in the IP header is often modified by NAT devices.

IPSec is used extensively for data authentication, integrity, and confidentiality. However, when NAT is used, IPSec operation is impacted, since NAT changes the address in the IP header.

Multicast, although possible in theory, requires complex configuration in a NAT environment and hence, in practice, is not utilized as often as could be the case.

The need for obligatory use of NAT disappears with IPv6.

4.6 Construction of IPv6

IPv6 interfaces can have multiple addresses that have different reachability scopes. For example, a node may have a link-local address, a site-local address, and a global address. Note: IPv6 actually has possible 15 scopes, as hex 0 to hex F; some of these scopes are unused.

Like IPv4, IPv6 is a connectionless, unreliable datagram protocol used primarily for addressing and routing packets between hosts. Connectionless means that a session is not established before exchanging data. Unreliable means that delivery is not guaranteed. IPv6 always makes a best effort attempt to deliver a packet. An IPv6 packet might be lost, delivered out of sequence, duplicated, or delayed. IPv6 per se does not attempt to recover from these types of errors. The acknowledgment of packets delivered and the recovery of lost packets is done by a higher layer protocol, such as TCP. From a packet forwarding perspective IPv6 operates just like IPv4. An IPv6 packet, also known as an IPv6 datagram, consists of an IPv6 header and an IPv6 payload.

The IPv6 header consists of two parts, the IPv6 base header and optional extension headers. Functionally, the optional extension headers and upper layer protocols, for example, TCP, are considered part of the IPv6 payload. IPv4 headers and IPv6 headers are not directly interoperable: hosts and/or routers must use an implementation of both IPv4 and IPv6 in order to recognize and process both header formats. This gives rise to a number of complexities in the migration process between the IPv4 and the IPv6 environments.

However, techniques have been developed to handle these migrations.

4.7 Autoconfiguration of IPv6

Autoconfiguration is a new characteristic of IPv6 that facilitates network management and system setup tasks by users. This characteristic is often called “plug-and-play” or “connect-and-work.” Autoconfiguration facilitates initialization of user devices: after connecting a device to an IPv6 network, one or several IPv6 globally unique addresses are automatically allocated.

The “autoconfiguration” process is flexible but it is also somewhat complex. The complexity arises from the fact that various policies are defined and implemented by the network administrator. Specifically, the administrator determines the parameters that will be assigned automatically. At a minimum (and/or when there is no network administrator), the allocation of a link-local address is often included. The link-local address allows communication with other nodes placed in the same physical network.

Note that “link” has somewhat of a special meaning in IPv6, as follows: a communication facility or medium over which nodes can communicate at the link layer, that is, the layer immediately below IPv6. Examples are Ethernets (simple or bridged); PPP links; an X.25 packet-switched network, a frame relay network or a cell relay/ATM network, and internet(working) layer (or higher layer) “tunnels,” such as tunnels over IPv4 or IPv6 itself.

Two autoconfiguration basic mechanisms exist: stateful and stateless. Both mechanisms can be used in a complementary manner and/or simultaneously to define parameter configurations.

Stateless autoconfiguration is also described as “serverless.” Here, the presence of configuration servers to supply profile information is not required. In this environment, manual configuration is required only at the host level and a minimal configuration at the router level is occasionally needed. The host generates its own address using a combination of the information that it possesses (in its interface or network card) and the information that is periodically supplied by the routers. Routers determine the prefix that identifies

networks associated to the link under discussion. The “interface identifier” identifies an interface within a subnetwork and is often, and by default, generated from the MAC address of the network card. The IPv6 address is built combining the 64 bits of the interface identifier with the prefixes that routers determine as belonging to the subnetwork. If there is no router, the interface identifier is self-sufficient to allow the PC to generate a link-local address. The link-local address is sufficient to allow the communication between several nodes connected to the same link (the same local network).

Stateful configuration requires a server to send the information and parameters of network connection to nodes and hosts. Servers maintain a database with all addresses allocated and a mapping of the hosts to which these addresses have been allocated, along with any information related with all requisite parameters. In general, this mechanism is based on the use of DHCPv6.

Stateful autoconfiguration is often employed when there is a need for rigorous control in reference to the address allocated to hosts (in stateless autoconfiguration the only concern is that the address be unique). Depending on the network administrator policies, it may be required that some addresses be allocated to specific hosts and devices in a permanent manner; here, the stateful mechanism is employed on this subset of hosts, but the control of the remaining parameters and/or nodes could be less rigorous. In some environments there are no policy requirements on the importance of the allocated addresses. In this situation the stateless mechanism can be used.

IPv6 addresses are “leased” to an interface for a fixed established time (including an infinite time). When this “lifetime” expires, the link between the interface and the address is invalidated and the address can be reallocated to other interfaces. For the suitable management of address expiration time, an address goes through two states (stages) while it is affiliated to an interface:

(a) At first, an address is in a “preferred” state, so its use in any communication is not restricted.

(b) After that, an address becomes “deprecated,” indicating that its affiliation with the current interface will (soon) be invalidated.

While it is in deprecated state, the use of the address is discouraged, although it is not forbidden. However, when possible, any new communication (for example, the opening of a new TCP connection) must use a preferred address. A deprecated address should only be used by applications that already used it before and in cases where it is difficult to change this address to another address without causing a service interruption.

To insure that allocated addresses (granted either by manual mechanisms or by autoconfiguration) are unique in a specific link, the link duplicated address detection algorithm is used. The address to which the duplicated address detection algorithm is being applied to is designated (until the end of this algorithmic session) as an “attempt address.” In this case, it does not matter that such address has been allocated to an interface and received packets are discarded.

Next, we describe how an IPv6 address is formed. The lowest 64 bits of the address identify a specific interface and these bits are designated as “interface identifier.” The highest 64 bits of the address identify the “path” or the “prefix” of the network or router in one of the links to which such interface is connected. The IPv6 address is formed by combining the prefix with the interface identifier.

It is possible for a host or device to have IPv6 and IPv4 addresses simultaneously. Most of the systems that currently support IPv6 allow the simultaneous use of both protocols. In this way, it is possible to support

communication with IPv4-only networks as well as IPv6-only networks and the use of the applications developed for both protocols. This technique is commonly known as dual stack.

Is it possible to transmit IPv6 traffic over IPv4 networks via tunneling methods. This approach consists of "wrapping" the IPv6 traffic as IPv4 payload data: IPv6 traffic is sent "encapsulated" into IPv4 traffic, and at the receiving end this traffic is parsed as IPv6 traffic. Transition mechanisms are methods used for the coexistence of IPv4 and/or IPv6 devices and networks. For example, an "IPv6-in-IPv4 tunnel" is a transition mechanism that allows IPv6 devices to communicate through an IPv4 network. The mechanism consists of creating the IPv6 packets in a normal way and encapsulating them in an IPv4 packet. The reverse process is undertaken in the destination machine, which deencapsulates the IPv6 packet.

There is a significant difference between the procedures to allocate IPv4 addresses, which focus on the parsimonious use of addresses (since addresses are a scarce resource and should be managed with caution), and the procedures to allocate IPv6 addresses, which focus on flexibility. ISPs deploying IPv6 systems follow the Regional Internet Registries (RIRs) policies relating to how to assign IPv6 addressing space among their clients. RIRs are recommending ISPs and operators allocate to each IPv6 client a /48 subnetwork; this allows clients to manage their own subnetworks without using NAT. (The implication is that the need for NAT disappears in IPv6.) In order to allow its maximum scalability, IPv6 uses an approach based on a basic header, with minimum information. This differentiates it from IPv4 where different options are included in addition to the basic header. IPv6 uses a header "concatenation" mechanism to support supplementary capabilities. The advantages of this approach include the following:

The size of the basic header is always the same and is well known. The basic header has been simplified compared with IPv4, since only 8 fields are used instead of 12. The basic IPv6 header has a fixed size, hence, its processing by nodes and routers is more straightforward. Also, the header´s structure aligns to 64 bits, so that new and future processors (at least 64 bits) can process it in a more efficient way.

Routers placed between a source point and a destination point (that is, the route that a specific packet has to pass through) do not need to process or understand any "extension headers." In other words, in general, interior (core) points of the network (routers) only have to process the basic header, while in IPv4 all headers must be processed. This flow mechanism is similar to the operation in MPLS yet precedes it by several years.

There is no limit to the number of options that the headers can support (the IPv6 basic header is 40 octets in length, while the IPv4 one varies from 20 to 60 octets, depending on the options used).

In IPv6, interior/core routers do not perform packet fragmentation, but the fragmentation is performed end to end. Fragmentation can be done by using the extension headers. That is, source and destination nodes perform, by means of the IPv6 stack, the fragmentation of a packet and the reassembly, respectively.

The fragmentation process consists of dividing the source packet into smaller packets or fragments.

A "jumbogram" is an option that allows an IPv6 packet to have a payload greater than 65,535 bytes. Jumbograms are identified with a 0 value in the payload length in the IPv6 header field and include a jumbo payload option in the hop-by-hop option header. It is anticipated that such packets will be used, in particular, for multimedia traffic.

This preliminary overview of IPv6 highlights the advantages of the new protocol and its applicability to a whole range of applications, including VoIP.

4.8 Coexistence and migration

Migration is expected to be fairly complex. Initially, internetworking between the two environments will be critical. Existing IPv4 endpoints and/or nodes will need to run dual-stack nodes or convert to IPv6 systems. Fortunately, the new protocol supports IPv4-compatible IPv6 addresses, which is an IPv6 address format that employs embedded IPv4 addresses. Tunnelling, will play a major role in the beginning:

There are a number of requirements that are typically applicable to an organization wishing to introduce an IPv6 service:

- The existing IPv4 service should not be adversely disrupted (e.g., as it might be by router loading of encapsulating IPv6 in IPv4 for tunnels).
- The IPv6 service should perform as well as the IPv4 service (e.g., at the IPv4 line rate and with similar network characteristics).
- The service must be manageable and be able to be monitored (thus tools should be available for IPv6 as they are for IPv4).
- The security of the network should not be compromised due to the additional protocol itself or weakness of any transition mechanism used.
- An IPv6 address allocation plan must be drawn up.

Well-known interworking mechanisms include the following (RFC2893):

Dual IP layer (also known as dual stack): A technique for providing complete support for both IPs—IPv4 and IPv6—in hosts and routers.

Configured tunnelling of IPv6 over IPv4: Point-to-point tunnels made by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures.

Automatic tunnelling of IPv6 over IPv4: A mechanism for using IPv4-compatible addresses to automatically tunnel IPv6 packets over IPv4 networks.

Tunnelling techniques include the following (RFC2893):

IPv6-over-IPv4 tunnelling: The technique of encapsulating IPv6 packets within IPv4 so that they can be carried across IPv4 routing infrastructures.

Configured tunnelling:

IPv6 - over - IPv4 tunnelling where the IPv4 tunnel endpoint address is determined by configuration information on the encapsulating node. The tunnels can be either unidirectional or bidirectional. Bidirectional configured tunnels behave as virtual point-to-point links.

Automatic tunnelling: IPv6-over-IPv4 tunnelling where the IPv4 tunnel endpoint address is determined from the IPv4 address embedded in the IPv4-compatible destination address of the IPv6 packet being tunnelled.

IPv4 multicast tunnelling: IPv6-over-IPv4 tunnelling where the IPv4 tunnel end point address is determined using Neighbour Discovery (ND). Unlike configured tunnelling this does not require any address

configuration, and unlike automatic tunnelling it does not require the use of IPv4-compatible addresses. However, the mechanism assumes that the IPv4 infrastructure supports IPv4 multicast.

4.9 IPv6 Multicast

Next, we focus on multicast issues, including layer 3 addressing. Note at this juncture that IPv6 multicast does not support DM.

4.10 IPv6 Multicast Addresses

Figure 31a depicts the IPv6 multicast address. In IPv6, multicast addresses begin with the format prefix 1111 1111 (FF in hex). The format prefix is followed by two fields, each 4 bits long: flags and scope. The flag field T initially indicated whether the address was

permanent or transient. RFC3306 added a P (prefix) flag; this flag allows part of the group address to include the source networks unicast prefix, which creates a globally unique group address. The R flag is used to indicate that the RP address is embedded in the group address; with embedded RP, the flags R, P, and Tare set to 1. The scope is a subset of the network, as discussed earlier. The remaining 112 bits of the IPv6 address are the group ID.

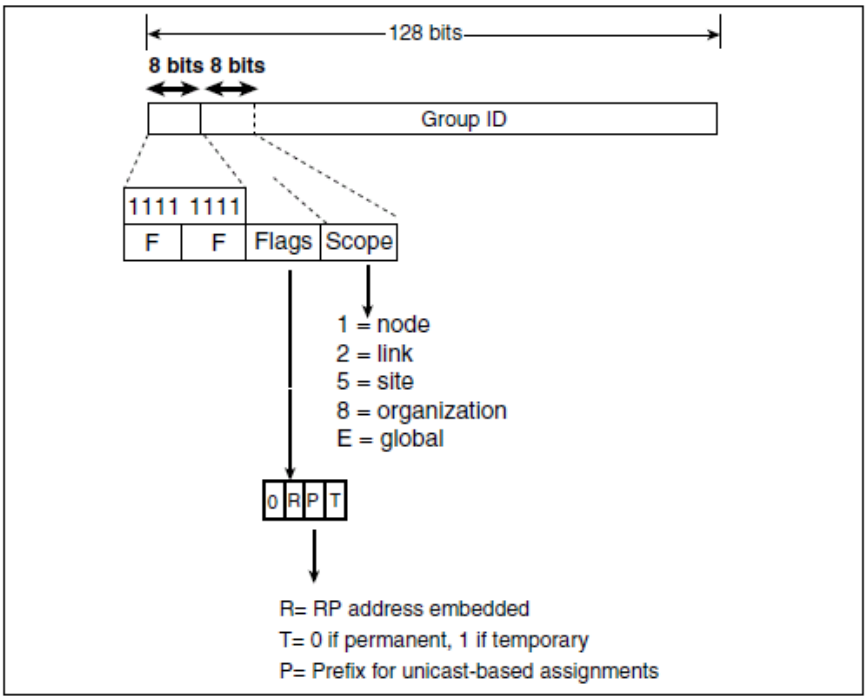

Figure 31a: IPv6 Multicast Addressing

4.11 MAC Layer Addresses

MAC layer addresses consist of 24 bits for the Organizational Unit Identifier (OUI) and 24 bits for the serial number of the Ethernet NIC. For a multicast environment the MAC address format uses a special OUI. The OUI for IPv4 multicast is 00:00:5E with the least significant bit most significant octet set and with only half of this address space allocated to IP multicast. The implication of the fact that only 23 bits are available for the group address means a potential address overlap at layer 2. A different OUI format is used for IPv6

multicast. The leading two octets are set to hex 33-33, and the remaining four octets are available for address mapping from the last 32 bits of the 128-bit IPv6 multicast address. See Figure 31b for an example.

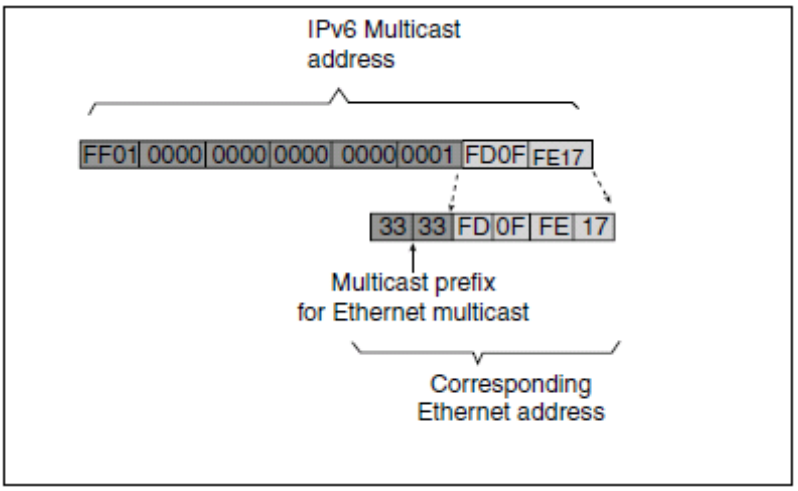

Figure 31b: IPv6 Multicast Address Mapping to derive an Ethernet address

4.12 Signaling

Just as is the case in IPv4, IPv6 hosts (receivers) must signal a router with its desire to receive data from a specific group. IPv6 multicast does not use IGMP but rather uses MLD. MLDv1 is similar to IGMPv2, and MLDv2 is similar to IGMPv3.

4.13 RP Aproaches

Recall that in PIM - SM (Protocol Independent Multicast - Sparse-Mode) sources must send their traffic to an RP (Rendezvous Point) ; this traffic is in turn forwarded to receivers on a shared distribution tree. In IPv6, auto-RP is not currently available; however, there is a BSR (Bootstrap Router)for IPv6; also there is static configuration of an RP (embedded RP). Static use is acceptable in the intradomain, but not within the interdomain. Embedded RP is a viable solution for those applications that cannot leverage SSM and that require a PIM SM model to interoperate across multiple domains . Embedded RP uses the R flag discussed above: when the flags R, P, and T are set to 1, this indicates that the RP address is embedded in the group address.

5. Quality of Service and QoS enabled protocols

According the T6.2 of DoW of Secricom projects is our aim find a common method to deal with QoS in heterogeneous IP-networks. Similar to the ToS field of the IPv4 header, the traffic class field is available to identify and distinguish between different classes or priorities of IPv6 packets. Furthermore, other than DiffServe-based QoS-enabled protocols (IntServ, MPLS, etc.) needs to be analyzed and compared to inherent mechanisms of IPv6.

QoS, especially in the Internet, is proving hard to provide. QoS was actually included in the first versions of IP – the TOS bits in the IP packet header were designed to allow a user to indicate to the network the required QoS. Yet, to date, there is very little QoS support in the Internet. One of the problems appears to be in defining what is QoS and what the network should do.

5.1 Current IP QoS mechanism

Despite the fact that the need to provide QoS is a major issue in current Internet development, the Internet itself today does already provide some QoS support. The main elements in common use today are the Transmission Control Protocol (TCP), Explicit Congestion Notification (ECN) and the Real Time Protocol (RTP). This section reviews these mechanisms, with particular emphasis on their behaviour in a wireless network supporting mobile terminals.

5.1.1 TCP IP

The Transmission Control Protocol, TCP, is a well-known protocol that manages certain aspects of QoS, specifically loss and data corruption. It provides reliable data transport to the application layer. We will consider first how it provides this QoS service, and then consider the problems that wireless can present to the TCP service.

TCP operates end to end at the transport layer. Data passed to the transport module are divided into segments, and each segment is given a TCP header and then passed to the IP module for onward transmission. The transport layer header is not then read until the packet reaches its destination.

The main elements of a TCP header for QoS control are the sequence number and checksum. When the TCP module receives a damaged segment, this can be identified through the checksum, and the damaged segments discarded. Data segments that are lost in the network are identified to the receiving module through the (missing) sequence numbers. In both cases, no acknowledgement of the data will be returned to the sender, so the data will be re-transmitted after a timer expires at the sending node. The sequence numbers also enable the receiver to determine whether any segments have been duplicated, and they are used to order the incoming segments correctly. Receivers can provide flow control to the sender to prevent any receiver node buffer over-runs, by entering the 'window size', or maximum number of bytes, that the receiver can currently handle. The sender must ensure that there is not so much data in transit at any one time that loss could occur through a receiver buffer overflow. To keep data flowing, receivers will send a minimum of TCP ACK messages to the sender, even if there is no data flow from receiver to sender.

TCP requires an initial start- up process that installs state in client and receiver about the transmission – this state defines a virtual circuit. This state essentially identifies the two ends of the connection (IP address and TCP port identifier) and indicates the initial starting values for the sequence numbers. This is needed to ensure that repeat connections to the same destinations are correctly handled.

In addition to ensuring that its data rate does not cause a receiver buffer overflow, the sender is also responsible for preventing network router buffer overflow. TCP achieves this network congestion control by slowing down the data transmission rate when congestion is detected. This helps prevent data loss due to queue overflows in routers. To achieve this, the sender maintains a second window size that reflects the state of the network. The sender determines this window size by gradually increasing the number of segments that it sends. Initially, the sender will send only one segment. If this is acknowledged before the timer expires, it will then send two segments. The congestion window grows exponentially until a timeout occurs, indicating congestion.

TCP requires neither network-based call admission control nor any support in routers, but it makes some assumptions about the nature of routers and transmission networks. In particular, this protocol assumes that transmission loss rates are small, so the overhead of end-to-end retransmission of corrupted packets is not an issue. It further assumes that loss is primarily caused by network buffer overflows. It can be thought of as having an out-ofband, hard-state signaling protocol – the TCP handshake. The end terminals have traffic conditioning capabilities – they measure the traffic flow, and on identification of network problems, they can act on the traffic, essentially reducing the data transmission rate.

5.1.2 QoS of wireless TCP

Whilst the higher-level protocols should be independent of the link layer technology, TCP is typically highly optimised, based on assumptions about the nature of the link, which are not true in wireless networks.

The congestion control algorithm assumes specifically that losses and delays are caused by congestion. In a fixed network, if losses or delays are encountered, this implies a congested router. In this situation, the sender should reduce the level of congestion losses by slowing down its sending rate. This will reduce the required number of re-transmissions, thus giving more efficient use of the network whilst being fair to other users of the network. In a wireless network, losses occur all the time, independently from the data rate. Thus, slowing down does not alleviate the loss problem, and simply reduces the throughput. In a general network, there may be both wireless and fixed sections, and neither the sender nor receiver can know where losses have occurred and, therefore, what action should be taken on detection of losses. Since many wireless networks have a circuit-oriented link layer, any problems with TCP efficiency directly cause overall inefficient use of the link.

In the presence of frequent losses, the congestion avoidance algorithms have also been shown to produce throughputs inversely proportional to the round triptime. This is a problem as many wireless links have large latencies (as a result of the loss management required), and this problem would be compounded for mobile-to-mobile communications. Essentially, the reason for this is that the slow start algorithm and loss-recovery mechanisms both rely on the sender having data acknowledged – the time to obtain the acknowledgements depends upon the round-trip time. This result has been formally proven, but can be understood from Figure 32, which illustrates the behaviour of the slow-start algorithm. This shows that, after a loss, the rate of growth of the congestion window (and hence the data throughput) is directly related to the round triptime. If losses are regular, this process will be repeated.

Whilst link layer error management, such as ARQ, can greatly improve the error rate of the wireless link, it achieves this with a cost of variable delay. TCP implementations use timers held by the sender to indicate when an ACK should have appeared in response to a transmission. If the timer expires, the sender knows to re-transmit the segment. Whilst the sender may attempt to set the timer based upon measurement of the round-trip time, it is difficult to do this accurately in a wireless network because of the random nature of

the losses and ARQ-induced delays. It is possible, therefore, that the same segment is in transmission twice as the link layer attempts to send the segment across the link uncorrupted, whilst the sender has assumed that the packet is lost and has re-transmitted it. This is wasteful of bandwidth.

Another problem arises because wide-area modern wireless links typically have large latencies and large bandwidths. This means that at any particular time, a large amount of data could be in transit between the sender and receiver. If this value is larger than the receiver window, the sender will need to reduce its transmission rate, lowering the throughput, because the receiver buffer would otherwise run the risk of becoming overflowed. From the example given in RFC2757, for a UMTS network with a bandwidth of 384 kbit/s and a latency of 100 ms making the end-to-end latency 200 ms, the delay bandwidth product would be 76.8 kbits or 9.6 kbytes, compared with a typical receiver buffer or window of only 8 kbytes. Thus, unless TCP implementations are modified to have larger buffers, the data transmission will not fill the available capacity on the network – a terrible waste of expensive UMTS bandwidth.

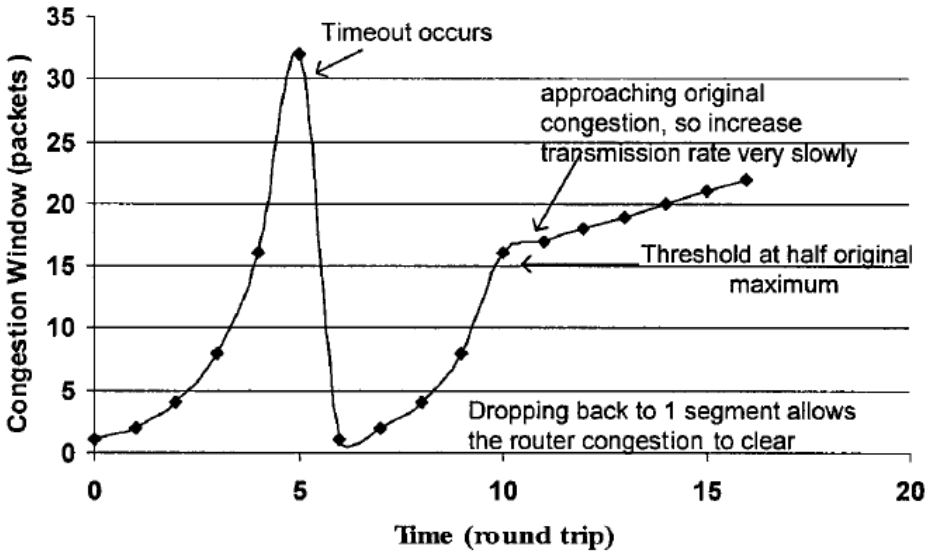

Figure 32: The size of the congestion window

Thus, to summarise the problems of TCP in wireless networks:

- Loss leads to a reduction of sending rate and so reduced throughput, but the loss remains as it was not caused by congestion.
- Loss leads to an initiation of the slow start mechanism. This is slowest to reach a steady state when round-triptimes are large and will never reach a steady state if losses are frequent. This leads to reduced throughput.
- Variable delays lead to inaccurate time-outs, and so extra TCP re-transmissions will be generated, meaning that bandwidth is wasted on unnecessary re-transmissions.
- Large delays also mean that at any one time, a large amount of data will be in transit across the network. Therefore, the sender will have to suspend sending data until the data in transit have cleared the receiver's buffer.

Delay-related problems could be exacerbated on handover, which often increases the delay or even causes short breaks in communication. Ideally, TCP re-transmissions should be delayed during handover to allow the link layer to recover. However, techniques to provide this functionality and other solutions to TCP performance problems are still an area of active research. A large number of solutions to these problems have been proposed. However, many produce knock-on effects. For example, if a TCP proxy is used as a proxy at the boundary between the fixed and wireless networks, the end-to-end semantics of TCP are broken. In addition to changing the semantics of TCP (the ACK does not mean the segment has been received), it then also breaks the IP level security model, and causes problems if the terminal moves away from that proxy. Other solutions may require changes to current TCP implementations, e.g. upgrades to every WWW server. Other ideas may require that a terminal uses different TCP implementations depending upon the physical network it is using for the connection – a severe limitation for vertical handover. Finally, many solutions have been proposed that are not suitable because they may negatively affect the Internet stability, for example by leading to increased levels of bursts of traffic and congestion.

However, some modifications can be made. For example, the slow start process can be speeded up if the slow start initial window size is 2 or 3 segments rather than the traditional 1 segment. This has been accepted as a modification to TCP that does not affect the general stability of the Internet.

Also, since slow start is particularly painful in wireless networks because of the long round-triptimes, techniques should be used that minimise its occurrence as a result of congestion losses. The use of SACK, Selective Acknowledgement, is also recommended. SACK is a technique that speeds up recovery where burst errors have damaged multiple segments – thus, its benefit depends upon the nature of the wireless network. It basically allows for multi- (rather than single) segment loss recovery in one round-triptime.

Whilst TCP proxies have many problems, application level proxies, however, may be of much greater benefit to the wireless environment especially as application layer protocols are often very inefficient. Even in this situation, however, the user must be in control of when and where proxies are used.

5.1.3 Random Early Detection

These are techniques that can be used by the network to reduce the amount of congestion losses, thus improving the quality of service. Random Early Detection (RED) has already been deployed within routers in some parts of the Internet. This technique deliberately discards packets as the queue builds up, providing a form of ‘congestion ahead’ notice to all users. Essentially, by dropping a few packets early on, it is possible to avoid congestion that would otherwise lead to larger numbers of packets being lost.

Within the router, as the average queue length increases, the probability of a packet being dropped increases. Larger packet bursts will experience a larger packet-discard rate, and sustained loads further increase the packetdiscard rates. Thus, TCP sessions with the largest open windows will have a higher probability of experiencing packet drop, causing them to start the congestion avoidance procedure.

Since the larger flows have a greater chance of experiencing packet drops, RED can avoid all the TCP flows becoming synchronised. This happens when the flows all experience congestion at the same time, all cut back, and all start to grow together.

Explicit Congestion Notification is another mechanism to give advance warning of impending congestion. The router can mark, rather than just drop, packets with an explicit Congestion Experienced (CE) bit flag, on

the assumption that the sender will see and react to this. In the case of TCP, the flag information must be echoed back by the receiver. Whilst ECN improves the performance of the network compared with packet drop RED, it requires changes to how TCP and IP operate and so, although it is now fully agreed within the IETF, it is unlikely to be introduced quickly.

5.1.4 RTP

The Real-time Transport Protocol, RTP, again provides end-to-end network transport functions. It provides ordering and timing information suitable for applications transmitting real-time data, such as audio, video, or data, over multicast or unicast network services. Again, we will first consider how it functions and then consider the impact that wireless networks could have on RTP.

RTP requires no support in the network or routers. An initiation stage ensures that traffic descriptors are exchanged so that the end terminals can agree the most suitable traffic encodings. SIP is a suitable protocol for automating this stage. In addition to the RTP header information, RTP is usually run with RTCP, the Real Time Control Protocol. The amount of control data is constrained to be at most 5% of the overall session traffic. RTP is a transport layer protocol that is typically run on top of UDP, extending the basic UDP multiplexing and checksum functionality.

RTP uses packet sequence numbers to ensure that packets are played out in the correct order. RTP headers carry timing information, which enables calculation of jitter. This helps receivers to obtain a smooth playback by suitable buffering strategies. Reception reports are used to manage excessive loss rates as, when high loss rates are detected, the encoding schemes for the data can be changed. For example, if loss is believed to be due to congestion, the bandwidth of transmission should be reduced. In other circumstances, redundant encoding schemes may provide increased tolerance to bit errors within a packet. This information can be delivered to the source through RTCP messages.

The RTCP control messages provide information to enable streams from a single source, such as an audio and video stream, to be synchronised. Audio and video streams in a video-conference transmission are sent as separate RTP transmissions to allow low-bandwidth users to receive only part of the session. The streams are synchronised at the receiver through use of the timing information carried in the RTCP messages and the time stamps in the actual RTP headers. Full stream synchronisation between multiple sources and destinations requires that sources and receivers have timestamps that are synchronised, for example through the use of the network time protocol (NTP).

To prevent interaction between RTP and the lower layers, application frames are typically fragmented at the application level – thus, one RTP packet should map directly into one IP packet.

RTP provides a means to manage packet re-ordering, jitter, and stream synchronisation, and can adapt to different levels of loss. However, it cannot in itself ensure timely delivery of packets to the terminal. This is because it has no control over how long the network takes to process each packet. If real-time delivery or correct data delivery is required, other mechanisms must be used.

5.1.5 RTP Mobility QoS

While RTP is largely independent of mobility, the overall RTP architecture includes elements such as mixer and translator nodes for service scalability and flexibility. If the core network includes several of these components, the mobility of the terminal may lead to situations where the mixer and the translator may change. These nodes have been pragmatically introduced as a means to handle multicast sessions. In large

sessions, it may not be possible for all users to agree on a common data format – for example, if one user has a very-low-bandwidth link and all other users want high-quality audio. Mixers, placed just before the start of a low-bandwidth network can be used to overcome some of these limitations by re-coding speech and multiplexing all the different audio streams into one single stream, for example.

This is done in such a way that the receiver can still identify the source of each element of speech. Translators are used in RTP to overcome some problems caused by firewalls.

5.1.6 RTP wireless QoS

5.1.6.1 Low Battery Power

RTP makes large use of timing information to achieve its full functionality. The clocks used for this need to be synchronised across the network. The Network Time Protocol, NTP is typically used for this. However, for NTP to provide the required high levels of accuracy (approximately in the microsecond range) it could require that the mobile terminal has IP connectivity for significant time periods (hours or days). This is somewhat unrealistic given current battery lifetimes. Therefore, some alternative mechanism to allow quicker convergence to NTP may be useful for mobile nodes. If the base stations were high-level NTP servers, it is possible that good synchronization could be maintained here, which would enable much quicker convergence for the mobile terminals – however, this is a requirement (albeit simple) on mobile networks to provide this additional service to their users.

5.1.6.2 Compressible Flows

For low-bandwidth links, the header overhead of an RTP packet (40 bytes) is often large compared with the data – this is particularly important for Voice over IP traffic (20 bytes of data per packet for a voice packet encoded at 8 kbit/s, packets every 20 ms). In these circumstances, RTP header compression is often used. This is operated on a link-by-link basis. It enables the combined RTP/UDP/IP header to be reduced from 40 bytes to 2 bytes. No information needs to be transmitted to the link layer to achieve this compression.

Because the RTP compression is lossless, it may be applied to every UDP packet, without any concern for data corruption. To save processing, as it is likely that the only traffic that will benefit is RTP, heuristics could be used to determine whether or not the packet is an RTP packet – no harm is done if the heuristic gives the wrong answer. For example, only UDP packets with even port numbers should be processed (RTP always uses an even port number, and the associated RTCP uses the next, odd, port number), and records should be kept of the identity of packets that have failed to compress.

However, this process only works once the data are being transmitted. If the application wants to improve QoS by reserving resources within the network, the application does not know if link-layer compression will be used, and the network layer does not know that compressible data will be transmitted. Thus, an application will request a reservation for the full data bandwidth. This reservation may be refused over the wireless link because of insufficient bandwidth, yet the compressed flow could be easily served.

Without passing application layer information to the link layer, the link layer will need to manage this possibility intelligently. There are two options:

- Allocate for the full bandwidth request initially, but reduce the local linklayer reservation on detection of compressible (usually RTP) traffic. Although this may lead to reservations being refused unnecessarily, it would allow the unused portion of a reservation to be recovered.

- Assume that RTP is used for all delay-sensitive reservation classes, and under-allocate bandwidth accordingly. Since the vast majority of real-time traffic will use RTP, this may be a suitable solution – although the traffic will need to be monitored to detect and correct when this assumption fails.

For all transmissions, not just RTP transmissions, the overhead of the IP packet header can be reduced. A number of header compression schemes do exist, particularly if the underlying link appears as a PPP, point-to-point protocol, link to the IP layer above. However, TCP or RTP header compression is incompatible with network layer encryption techniques. Another possible problem with compression is that even a single bit error in a compressed header could lead to the loss of the entire segment – for TCP, this would lead to the slow start process being triggered. It is assumed that payload compression will take place at the sending nodes, in an effort to reduce the cost to the user of the link (assuming that cost to the user is directly related to bandwidth used).

A limited set of basic QoS functions is already available within the Internet. However, none of these mechanisms can support real-time services, as they cannot ensure timely packet delivery. To do this would require some support by the network itself – the network will need to be responsible for more than just attempted packet delivery. This has been an active research area within the IETF over the last few years, and indeed, some progress has been made over the last year towards introducing QoS into IP networks.

Further, to date, much Internet development has ignored the problems that mobility and wireless could cause. This is also true of many of the newer IETF standards. Although this situation is rapidly changing, some of the problems are fundamental, as to overcome them would require changes to the huge installed base of TCP/IP equipment, so many of the issues are likely to remain for many years. To some extent, it means that innovative solutions to minimize the impact of these problems need to be provided by the wireless link layers. This may be one area in which wireless network solutions may differentiate themselves.

5.2 QoS Mechanism

QoS is a large topic and, as previously indicated, has implications in every part of the system. The first stage in understanding the problem is therefore to attempt to structure the QoS problem into smaller units. This section identifies what the basic elements are, and looks at some of the different design choices that exist for each of the elements.

As part of this, the problem that needs to be considered is: What is the required functionality within the network to provide QoS? The mechanisms that can exist within the routers, to enable the network to provide QoS, are examined later in this chapter. Since network QoS is essentially about giving preferential treatment to some traffic, there need to be mechanisms to negotiate this treatment with the network. This process is covered under a discussion of signaling. Finally, mechanisms are needed that allow the network to ensure that admission to the service is controlled – after all, not every user can have preferential treatment at the same time. Throughout this section, special attention is paid to issues caused by wireless and mobile networks.

5.3 Functionality Required of the Network to Support QoS

Quality of service may require control of a range of features including packet delay, packet loss and packet errors, and jitter. Beyond a basic minimum, QoS is meaningful to a user only if it exists on an end-to-end basis. As an example, the error rate of the data, as finally delivered to the application, is more significant than the error rate at any particular point within the network. As previously discussed, many aspects of QoS, including packet loss, stream synchronisation, and jitter, can be controlled at the terminal through the use of suitable end-to-end layer protocols. As an example, the transmission layer protocol TCP is currently used to control error rates, whilst RTP is used to manage jitter and stream synchronisation. The only parameter that cannot be controlled in such a fashion is the (maximum) delay experienced by a packet across the network. Providing delay-sensitive packet delivery requires co-operation from each element within the network. This leads to a division of responsibility for QoS according to Figure 33.

Whatever functionality is placed within the network to support QoS, this functionality, or its effects, needs to be clearly described to users. In general terms, users can be easily bewildered by a totally flexible system. It may be possible to offer a huge range of services, each with different probabilities of being maintained. However, as described in Chapter 2, UMTS networks define only four classes:

Layer	Example Protocols	Functionality Required
Application		
Transport	TCP, UDP, RTP	Error control, Stream Synchronisation, Jitter Control
Network	DiffServ	Timely Packet delivery
Link	FEC	Timely frame delivery, some error management, orderly frame delivery

Figure 33: Internet Layer Model with QoS protocols and functionality

- Conversational – For applications such as video telephony.
- Streaming – For applications such as concert broadcast.
- Interactive – For applications such as interactive chat, WWW browsing.
- Background – For applications such as FTP downloads.

However, it has been proposed that even these classes could be collapsed into only two – delay sensitive and delay insensitive – as evidence exists, which suggests that only two classes can be truly distinguished within the Internet.

Finally, it is worth stating that just because it is implied here that only delay is important, this does not necessarily mean that only delay will be controlled by the delay-sensitive class. Jitter may be controlled as part of this, either explicitly, or by controlling the maximum delay that traffic experiences. Some effort may also take place to prevent congestion losses in such a class.

5.4 Interaction with the Wireless Link Layer

Although, above, a picture has been drawn with clear separation between layers and functions, life is never so clean-cut, and interactions will exist between different elements. These interactions are most obvious – and most problematic – between the network and link layer. Network layer quality typically manages the router behaviour in order to achieve a certain quality of service. This works well if the link is well behaved – if it has no significant impact on the delay, jitter, or loss that a packet might experience. However, this is not true with a wireless link layer. Furthermore, the simplest method to overcome these problems – bandwidth over-provision – is not practical in general in a wireless environment, as bandwidth is expensive. For example, in the recent UK UMTS spectrum auction, 20 MHz of bandwidth went for 4 billion UK pounds. Therefore, link-layer mechanisms are needed to manage the quality of data transmission across the wireless network. It is important that any quality provided at the network layer is not compromised by the link-layer behaviour. This could occur, for example if the link layer provides some form of re-transmission-based loss management, (such as ARQ) without the network layer being able to control the delay, or if the link layer reorders packets that have been sent for transmission. The next section expands upon these issues that have a significant impact on QoS.

5.4.1 Loss Management

There are a number of problems that wireless networks have that lead to data loss:

Low signal-to-noise ratio

Because base stations are obtrusive and cost money, they are used as sparingly as possible, and that means that at least some links in every cell have very low signal-to-noise ratios, and thus very high intrinsic error rates. Typically, a radio link would have a bit error rate (BER) of 10^{-3} compared with a fibre link with a BER of 10^{-9}.

Radio Errors Come in Bursts

In many other networks, errors are not correlated in any way.

Radio Links Suffer Both Fast and Slow Fading

Fast fading causes the received power, and hence the error rate, to fluctuate as the receiver is moved on a scale comparable with the wavelength of the signal. It is caused by different rays travelling to the receiver via a number of reflections that alter their relative phase (a GSM signal would have a wavelength of 10–20 cm or so). Slow fading – also called shadowing – is caused by buildings and typically extends much further than a wavelength.

There are solutions to these problems. To overcome the high error rates, radio links employ both forward and backward error correction. For example carrying redundant bits enables the receiver to reconstruct the original data packet (Forward Error Correction), whereas Automatic Repeat Request (ARQ) is used to re-transmit lost packets. Where ARQ can be used, the error rates can be reduced sufficiently such that any losses TCP sees are only the expected congestion losses. However, this scheme relies on linklayer re-transmissions and so significantly increases the latency, which can be a problem for real-time traffic.

To counter the problem of burst errors and fast fading, radio systems can mix up the bits and fragment IP packets into smaller frames. Again, this could cause latency problems for real-time traffic.

All these techniques, however, still do not take into account the unpredictable and uncontrollable errors that might occur. An example of such a problem could be when a user of a wireless LAN moves a filing cabinet, or a user of a GSM system is on a train that enters a tunnel. In such situations, the signal level might fall so far into the noise that the session is effectively lost.

Mechanisms also exist so that the wireless transmitters can control to some extent how the errors appear to the terminal. For example, some traffic (such as voice) prefers an even selection of bit errors to whole packet losses.

Certain encoding of video traffic, however, leads to a preference that certain whole video packets are dropped, ensuring that the top priority packets are transmitted uncorrupted. If the link layer knows the type of traffic carried, it can control the loss environment, by using different error correction schemes. However, this requires significant communications between the application and the wireless layer. Exchange of wireless specific information from the application is generally considered as a bad thing.

Higher layers should not communicate with the link layers, and protocols should not be designed to the requirements or capabilities of the link layer. Applications and transport layer protocols should not have 'wireless aware' releases.

So, how can these issues be handled? The error rate on wireless links is so bad that it is a fair assumption that error correction techniques should be used wherever possible. It is assumed that forward error correction is always used on the wireless links to improve the bit error rates. Ideally, for non-real time services, the errors on a link should be controlled to produce an overall error of no more than 1 in 10_6. For real-time service, the errors should be corrected as much as possible within the delay budget. This implies some mechanism for communicating QoS requirements down to the link layers, perhaps using the IP2W interface. Furthermore, to enable wireless loss management techniques to be used, network providers should assume that a significant proportion of any delay budget should be reserved for use within a wireless link.

Scheduler Interactions

Once QoS exists at both the link and network layers, there is a possibility for interactions between the two QoS mechanisms. There is unlikely to be a one-to-one mapping between network and link-layer flows. So, in the general case, thousands of network layer flows may co-exist, whereas there is usually a limit on the number of physical flows that may exist. In the general case, there cannot be a one-to-one mapping between these flows and the queues that are used to put these flows on to the network. With multiple queues at both layers, there will also be scheduling to determine how to serve these queues at both layers. This can cause problems. Consider a simple case where the network has a 'fast' and 'slow' queue for IP packets. The network layer bounds the size of the fast queue (to say 50% of the available bandwidth) to ensure that the slow queue is not starved. If there is a packet in both queues, the fast packet will always be delivered to the link layer before the slow packet. The link layer also has two queues: 'first transmission attempt' and 're-transmission'. These queue link-layer frames (parts of IP packets) and are served in such a way that frames for re-transmission are given a slightly lower priority than 'first attempt' frames. Now, suppose the IP layer sends first a 'fast' packet, which is divided into two frames at the link layer, and then a large TCP packet. The second half of the fast packet fails to be correctly delivered, is queued for re-transmission, and is then blocked for a long time as the large TCP packet is served from the 'first attempt' queue.

Although this is a simplistic scenario, it illustrates the points that:

- The network layer needs a clear understanding of the behaviour of linklayer classes and link-layer scheduling to prevent interactions between the behaviours of the two schedulers.
- The link layer needs QoS classes that support the network requirements.

Again, this implies some mechanism for communicating QoS requirements down to the link layers.

5.5 Mechanisms to Provide Network QoS

When traffic enters a router, the router first determines the relevant output for that traffic and then puts the packet into a queue ready for transmission on to that output link. Traditionally, in routers, traffic is taken (scheduled) from these output queues in a first come, first served basis. Thus, as illustrated in Figure 34, packets can be delayed if there is a large queue. Packets can be lost if the queue is filled to overflowing.

QoS implies some kind of preferential treatment of traffic in routers. This preferential treatment may be allocated on a per-flow or aggregate basis. A flow is an associated sequence of packets flowing between the same source/destination pair – such as a sequence of packets that make up a voice transmission. Individual flows can be aggregated together into a shared class. Per-flow scheduling gives better control of the QoS, enabling firm guarantees to be made about the treatment of the traffic.

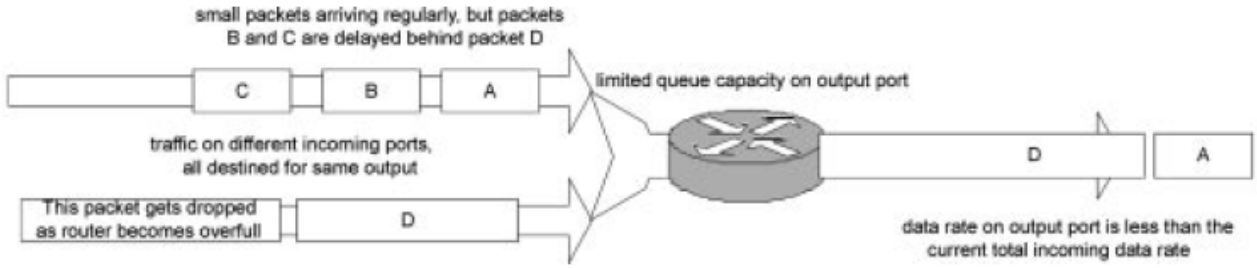

Figure 34: Packet delay

However, this also requires that per-flow state be maintained in every router, and this per-flow state is used to determine the scheduling of packets through the router. This causes scalability problems within the core network, where large numbers of individual flows may co-exist. In the alternative aggregate treatment, traffic on entry to the network is placed into one of a few traffic classes. All traffic in any class is given the same scheduling treatment. This solution gives better scalability and can also reduce the complexity of scheduling algorithms. In the general case, however, less firm guarantees can be given to a user about the nature of QoS that they can expect to receive – as illustrated in Figure 35.

In certain cases, it is possible to use traffic aggregates for scheduling whilst still achieving hard QoS guarantees on a per-flow basis, and one such example is discussed later. In general, however, such techniques can only provide hard guarantees for a small number of QoS parameters.

Thus, we can see that the type of QoS functionality that we wish to provide has a direct impact upon how easily it can be supported by routers. Broadly speaking, simple QoS services can be supported by simpler scheduler implementations.

More complex QoS services with many parameters to be controlled may require very complex techniques for managing the queues within the routers.

When QoS is used at the network layer, once the traffic reaches the first router, it is scheduled in order to achieve the required service. However, in the wireless world, huge problems could occur in sending the data to the first router.

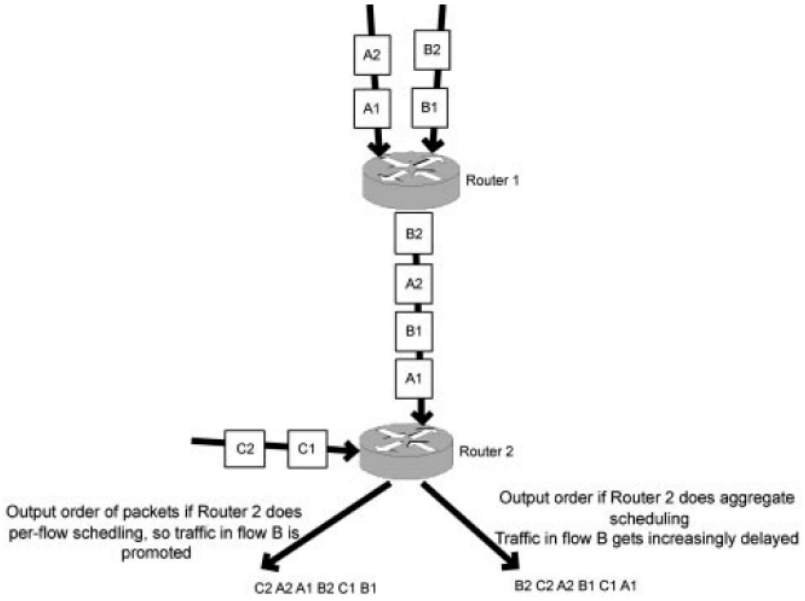

Figure 35: Aggregate scheduling gives less predictable behaviour than per-flow scheduling

Thus, there needs to be a link-layer mechanism that ensures that QoS is controlled across the first link into the Internet. This QoS protocol is linklayer-specific. It is assumed that the IP module understands the mapping between the QoS protocols that it supports and the link layer protocols and QoS classes. For example, the IP module may actually use some form of link-layer reservations for the top-priority prioritisation traffic.

5.6 Signaling Techniques

5.6.1 Prioritization and Reservation

There are two main types of QoS solutions – reservation-based solutions and prioritisation-based solutions. They essentially differ in how the user communicates to the network about their requirements. In reservation based services, a node will signal its request for a particular QoS class prior to data transmission. By providing a description of the data traffic, it is possible for the network to use this information to allocate resources, on either a per-flow or aggregate basis. This enables a large degree of control over the use of the network, and hence can provide a good degree of confidence that the required quality will be achievable.

In contrast, no advance network negotiation takes place with prioritization services. Traffic is simply marked to indicate the required quality class and then sent into the network. This type of system can only ensure that higher priority traffic receives a better quality of service than lower-priority traffic. In most practical implementations, this will be augmented by ‘service level agreements’. These contracts may be thought of as a static signaling mechanism. They may be used to restrict the amount of top-priority traffic transmitted from any particular source, enabling the network provider to make stronger probabilistic assurances of the nature of service that top priority traffic will receive.

5.6.2 Characteristics of Signaling Systems

To enable efficient use of scarce resources whilst also maintaining strong probabilistic service guarantees, it is assumed that, especially in the 3G environment, some reservation signaling will be required for real-time services. The signaling may be carried with the data, which is known as in-band signaling, or it may be out-of-band and thus separate from the data. In-band signaling ensures that the information is always carried to each router that the data visit, which is useful when routes change frequently, as in mobile networks. Out-of-band signaling, as used in telephone networks, is more easily transported to devices not directly involved in data transmission – for example admission control servers. Most importantly, however, is the fact that in-band signaling requires an overhead to be carried in every data packet. A simple in-band signaling system, requesting only real-time service for a specified bandwidth of traffic, could add an approximate 10% overhead to a voice packet.

The signaling may be soft state, in which case, the reservation needs to be explicitly refreshed. This makes it resilient to node failures. Conversely, a hard-state protocol can minimise the amount of signaling. The telephone network uses hard-state signaling – the caller dials only once. With a hardstate signaling protocol, care needs to be taken to correctly remove reservations that are no longer required.

Different models exist in terms of the responsibility for generation of the signaling messages. These models are often coupled with responsibility for payment for use of the network. In a UMTS style of network, the mobile node is responsible for establishing (and paying for) the required Quality of Service through the mobile network domain for both outbound and inbound traffic.

This model does not require that both ends of the communication share the same understanding of QoS signaling. It is a useful solution to providing QoS in a bottleneck wireless network region. The mobile user essentially pays for the privilege of using scarce mobile network resources. However, it is less easy to provide true end-to-end QoS in this situation. Inter-working units need to exist at each domain boundary that mapbetween different QoS signaling and provisioning systems, and this inter-working may break IP security models. This solution typically assumes that the inbound and outbound data paths are symmetric – true in the circuit-switched networks in which this model was developed, but not necessarily true in the IP packet network. Other solutions have one party responsible for establishing the QoS over the entire end-to-end path. The standard Internet models assume that the receiver is usually responsible for QoS establishment, as they receive value from receiving the data. However, these solutions usually require that the data sender also participate in any signaling and they retain ultimate responsibility for any payment – this is seen as a possible mechanism for limiting ‘junk mail’.

5.6.3 Wireless Efficiency

The limited, expensive wireless bandwidths mean that great efforts are required to minimise any signaling overhead carried on the link. This implies the need for hard-state signaling over the wire. This is easily achieved using RSVP (discussed later), which allows the soft-state period to be set on a hop-by-hop basis, although additional functionality is then required to protect the network against hanging reservations – reservations left as a result of incorrect application termination. Further optimisation of signaling attempts to use one signaling message for several purposes. As an example, the link-layer QoS request could be designed to contain enough information (including destination IP address) to enable the wireless access router to establish the network QoS without the need for the mobile to transmit a network layer message. Avoiding this type of protocol coupling/layer merging helps to protect the future flexibility of the network. Similarly, improved efficiency implies the need for wireless application specific information to be passed to

the wireless access router. However, unless wireless specific applications are to be developed, for example using RSVP with wireless extensions, such information would need to be configured into a link-layer driver.

5.6.4 Admission Control

QoS treats some traffic preferentially to others, and this implies the ability to reject traffic. The call admission functionality may exist at various places within the network. These alternatives are illustrated in Figure 36. In some solutions, each router is responsible for their own call admission decisions. Coupled with the Internet resilient routing, this enables a system that has no single point of failure. Each node makes a decision based on its complete knowledge of its current (local) state. However, such a solution does not scale well. The processing overhead of call admission would be significant for core routers, which route many thousands of flows.

Therefore, an alternative solution is that only edge routers process call admission requests. These nodes use their local knowledge of their current state and make some assumptions about the rest of the network that enables them to make a decision on behalf of the core of the network. In particular,

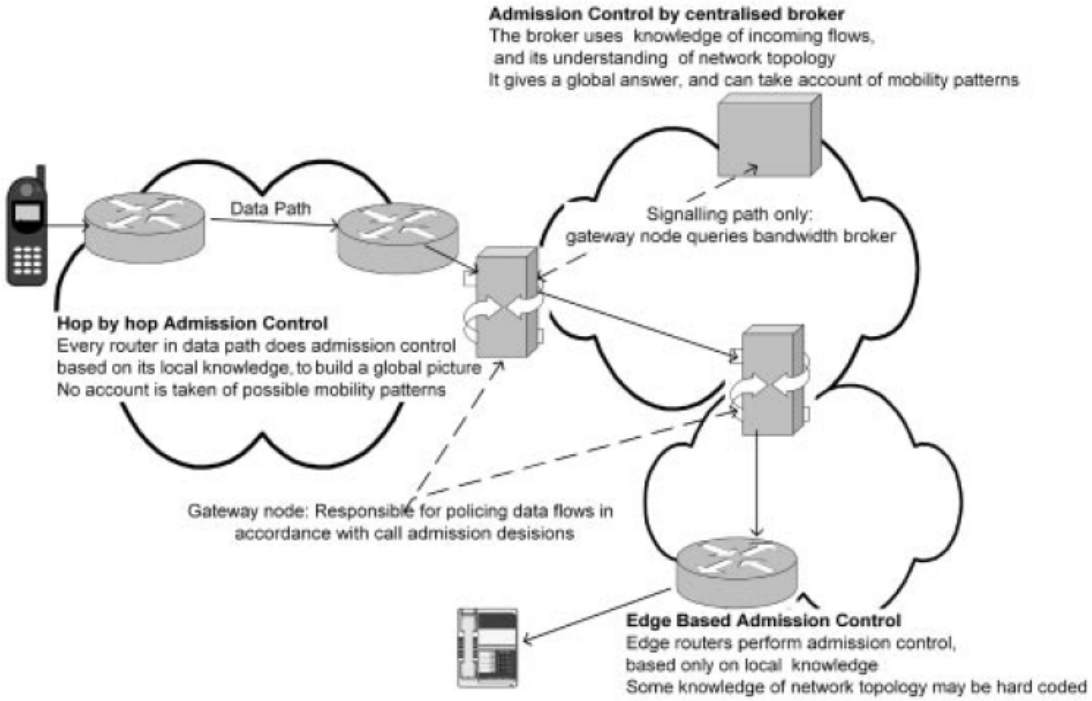

Figure 36: Different locations for the call admission functionality in different subnets

they can assume that no traffic enters the domain without being subjected to the same call admission scheme. The statistical effects of large numbers of flows facilitate the decision making process.

A fully centralised system enables a decision to be based on global as well as local knowledge. An edge router directs the request to the centralised admission control unit. There are a number of benefits of this approach. In addition to avoiding the scalability problems of the hop-by-hop approach, this scheme may enable QoS where routers have no QoS support. It allows the call admission mechanism to be upgraded and replaced easily. Centralised admission is not well suited for schemes with per-flow routing, as then, large amounts of communication would need to exist between every router and the call admission server. In addition, certain types of call admission criteria, in particular delay-based admission, are less well suited to centralised admission schemes. This is because the centralised unit can never know the actual full state

of the network. Similarly, centralised admission schemes are less suited to the mobile environment where the state of the network is likely to change rapidly.

5.6.5 Admission Control Descriptions

Call admission may be based on a number of parameters that describe the traffic. Increasing the number of parameters enables more accurate admission decisions, leading to more efficient network usage. However, such decisions tend to be more complex and require a full analysis of the traffic characteristics of each existing flow. At the other extreme, the information offered could be simply the maximum bandwidth required. Such a minimal approach reduces the amount of information that needs to be signalled across a network. This approach is also more suitable when centralised call admission needs to be supported. This is because a centralised unit can only ever have an approximate understanding of the state of the network. Therefore, to make admission control choices, it needs to use approximations that have been found to be most possible if bandwidth-based admission is used. From the point of view of a network operator, the use of peak bandwidth as the main traffic descriptor also simplifies billing – as the operator can make a bill based on that one parameter that reflects simply how much actual network resources are used. A user can minimise their bill by doing traffic shaping to keep the required peak bandwidth as low as possible.

5.6.6 Traffic Classification and Conditioning

Once the network has accepted that the data can be transmitted, and the data are actually being transmitted, there are a number of functions that need to be provided to ensure that the network is protected against malicious use. As in call admission, these functions may be provided on a hop-by-hop basis, or solely on entry and exit to a network. By using these functions on exit from a network (and terminal), steps can be taken to ensure that transmitted data are within the contract, so that the behaviour through the network is understood. Throughout this section, the term ‘QoS contract’ is used to refer to either the dynamically signalled QoS contract or the static contract described through the service level agreement. The first stage, classification, is to identify the flow to which traffic belongs, through analysis of the packet header. The packet can then be associated with a particular QoS contract. As an example, packets between a particular source–destination pair may be entitled to real-time forwarding provided that a strict bandwidth limit is not exceeded.

Once the stream has been identified, traffic meters measure its temporal properties against the QoS contract. This meter may pass state information to other conditioning functions to trigger specific actions for each packet that is either in- or out-of-profile.

One action that may be triggered by the measurement is traffic shaping. This is the process of delaying packets within a traffic stream to cause it to conform to the traffic profile. A shaper may be used, for example, to smooth out the burstiness of traffic, as traffic that is near constant bit rate can be managed more easily. This process in particular might take place in a terminal. A packet marker might be used to label traffic to ensure that it receives the required QoS treatment through that network domain. Additionally, packet markers might change the marking on a packet if the traffic has broken the agreed contract. This re-marking ensures that the traffic does not damage the QoS of in-contract traffic by ensuring that out-of-contract traffic does not receive the requested QoS. This re-marking also acts as a signal to the receiver that the QoS contract was violated – enabling action to be taken by the end-to-end application. Packet droppers, which simply drop packets, provide another means to handle traffic that has broken the agreed contract.

5.6.7 Mobility Issues

The call admission architecture used has a significant impact on the problems that might be experienced during handover. Therefore some of these issues are examined. Solutions to overcome these problems are in turn affected by the nature of the router and signaling mechanisms used to provide QoS.

A handover occurs when a mobile node changes its point of attachment to the network. This implies that the route taken by data will change. Any QoS that has been established for that data, and particularly any reservation, will therefore be disrupted. To ensure minimal disruption during handover, a number of alternative mechanisms could be used. These are discussed in order of increasing complexity.

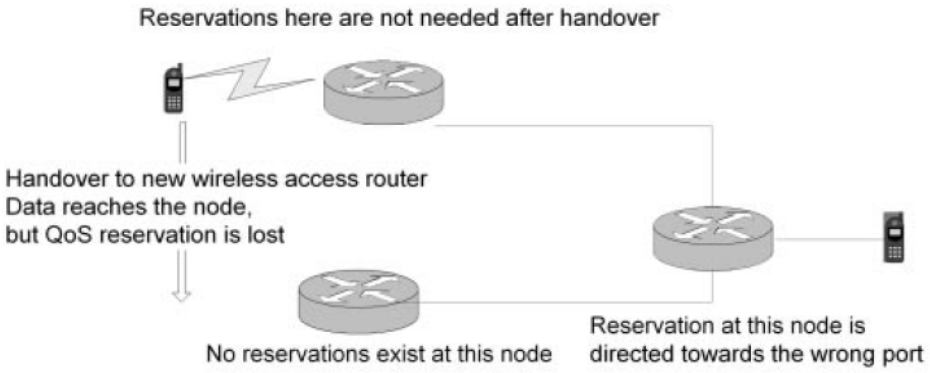

Figure 37: Illustrating how handover can affect reservation based QoS.

For prioritisation QoS, little needs to be done to manage QoS during or after handover, as all class descriptions are relative and assurances are statistical.

The problem is more complex for reservation-based QoS (Figure 37), where some service guarantees have been made. A reservation-based handover is described as seamless if the application or end user cannot identify that a mobility event has taken place. To some extent, this could be managed through careful descriptions of the service classes – for example, by stating that traffic will be delivered within a certain time bound only 90% of the time. Thus, no attempt is made to provide QoS during handover, simply to re-establish the QoS reservation after handover has taken place.

One improvement is that each node simply reserves a portion of its available bandwidth to be used solely for traffic that enters the node as a result of handover. This is known as a 'static guard band'. There needs to be a mechanism to enable nodes to identify the handover traffic, and also the requirements of that traffic. This mechanism needs to be quick, as packets affected will already be in flight. One way to manage this exists if an aggregate, class-based service is provided, and packets carry an explicit QoS class marking in the IP packet header (as is provided, for example, in the aggregate DiffServ approach to QoS). Handover traffic can then be re-marked to the (network internal) handover class associated with the reservation-based service identified by the original class marking. For each reservation class, there exists a guard band for use by this handover marked traffic. Traffic should be remarked into this class by a node that recognises that a route change has occurred; this node will assume that the route change has been caused by handover. This assumes that state information about this reservation is held at any node at which the data path might diverge. Otherwise, there is no way of identifying that a route change has occurred for that particular traffic flow[4]. Thus, if the route were to diverge at any point within the domain (as might occur if a per-host routing mobility management scheme is used), every node within that domain must have per-flow state. This is illustrated in Figure 38. If a tunnel-based mobility management scheme is used, the tunnel

anchor nodes will need per-flow state. Thus, we can see that reservation-based QoS cannot easily be used with the simplest edge admission control schemes. To do so would severely weaken the strength of QoS guarantees that could be made, as the amount of traffic in any one class cannot be limited to any particular node, because paths through the network could change rapidly as a result of mobility after the reservation process has been completed.

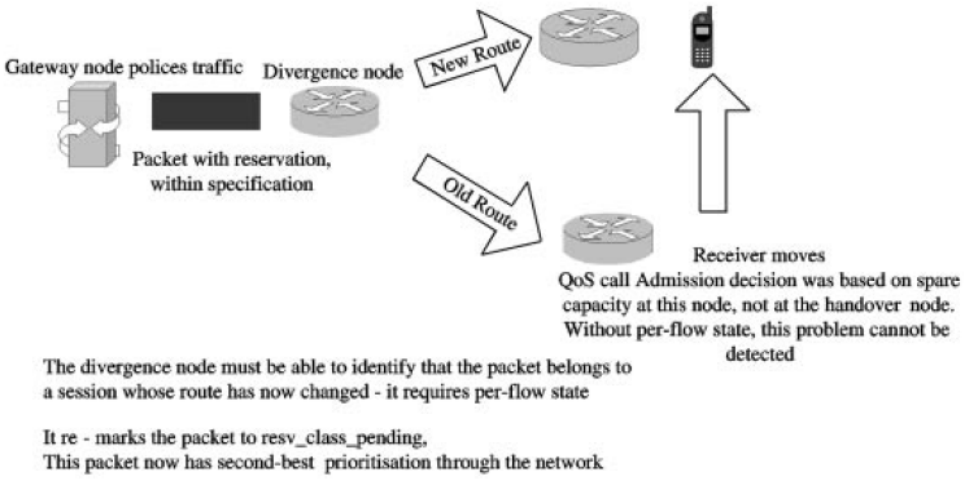

Figure 38: Per-flow state is required at routers if reservation based traffic is to be easily identified during the handover process.

The use of static guard bands means that bandwidth may not be used efficiently, or more complex router schedulers will be needed to enable best-effort traffic to use the guard band when not required by handover traffic. This problem would become worse if a large number of different reservation classes were supported. This system can be improved upon when global information can be used to make the admission control decision – for example, using a centralised network management system – as then the size of this guard band can be adjusted dynamically according to the traffic distribution around the network. Such a node may instruct routers to reserve a larger guard band if the neighbouring cells are all busy, as handover is more likely to occur in this situation. Where nearby cells are empty, very little capacity needs to be allocated for handover traffic. The nature of these policies, their complexity, and the assumptions they make about user mobility are all areas under current research.

Using such procedures, it is possible to design a network such that there is a high probability that, if the new route can support the handover, the handover itself will be seamless. However, it is also possible that, for example, six sessions simultaneously handover, of which five can be supported through reservation once handover is completed, but during handover, all six suffer degradation – the guard band becomes too full. To avoid this situation, either the nodes involved in handover must communicate QoS state, which couples the mobility and QoS protocols, or the admission control must not be based on purely local decisions.

An alternative approach is required for traffic that does not carry a QoS class marking, as is typical for traffic that is processed on a per-flow basis as in Integrated Services. In this situation, each session could make reservations for itself in nearby cells in preparation for likely handover. Thus, the session inserts per-flow state at a number of nodes within the network. (These reservations could be considered a form of dynamic

guard band.) Since many reservations may be needed, although only one will be used, this again could waste bandwidth. Thus, these reservations are 'passive' – the space is used by best-effort traffic until the reservation is made 'active'. Since the mobile node does not, and should not, know the network topology, prereservation is improved by making the base stations responsible for the passive reservations rather than the mobile node. This also reduces the signaling load on the mobile node. Such pre-reservation schemes are difficult, as the route through the network is not usually identified until handover has taken place. Therefore, such schemes couple the mobility management and QoS reservation process. For example, some propose that this passive reservation be made between every probable handover cell and a mobile IP home agent. All traffic in both directions is forced to flow through the home agent – this removes the possibility of any route optimisation. Other approaches propose that the nearby base stations do passive reservations on their wirelink, and that the current base station performs a reservation to each of the nearby base stations. Then, all traffic is forced to go through to the first base station, which then forwards the traffic.

5.6.8 Context Transfer Protocol

When handover occurs, network layer QoS typically needs to be re-established. In a wireless network, the weakest link is often the wireless section. It is most important that the reservation is established here extremely quickly, even if no action is taken to manage the network QoS until after handover is completed. It is assumed that the Layer 2 reservations will be established as part of the handover procedure. However, Layer 3 information is required if the wireless access router is to be able to associate incoming IP packets with the relevant link-layer reservations. We assume here that there is a context transfer protocol that transfers such information between the wireless access routers, as illustrated in Figure 39.

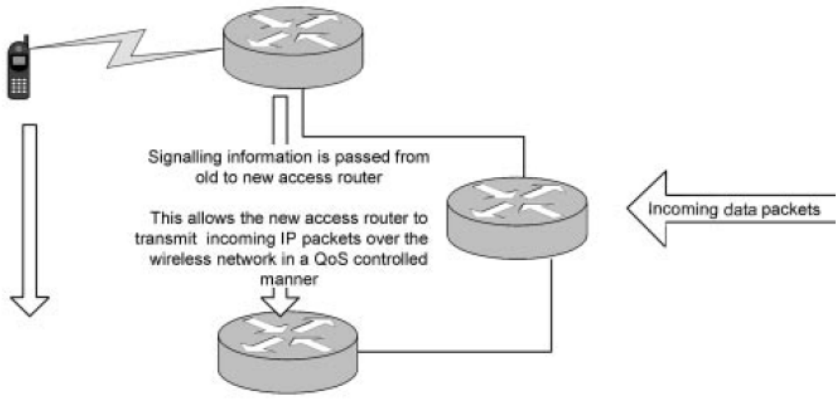

Figure 39: Use of context transfer protocol.

The context transfer protocol does not yet exist. It is being developed by the SEAMOBY working groupwithin the IETF in order to speed up the handover process. The context transfer protocol might include security information or QoS state information.

5.6.9 QoS Management After Handover

Where passive reservations have been used to manage the handover process, there is no need for any further QoS restoration after handover has occurred. Essentially, the call admission process was carried out

in advance of the handover. The other approaches to handover management, however, require that the QoS reservation is formally re-established after handover. Ideally, this process should be confined to the region impacted by mobility and should not involve the mobile node in order to conserve battery power and wireless bandwidth. Later, a discussion of RSVP, a specific QoS signaling mechanism, will show how this can be achieved. When the mobility management mechanism relies on establishing tunnels, it is the responsibility of the tunnel end points (the mobility agent and the wireless access router) to re-establish the QoS. For efficiency and ease of processing, tunnels typically support a large number of flows within the one tunnel, but this would require that the tunnel be established with QoS suitable to support the highest QoS flow, which would usually be wasteful of resources. Otherwise, multiple tunnels need to be established, for example, one for each QoS class. Tunnels also need to be able to correctly route all control messages – so reverse tunnels will be needed in the case of RSVP. Whilst a number of Internet Drafts and RFCs exist addressing the problems of tunnels and QoS, it is clear that this issue presents a large number of practical difficulties, with additional processing requirements and restrictions on network topology.

5.7 Proposed Internet QoS Mechanisms

This section briefly examines the QoS mechanisms that have recently been developed within the IETF. Although these are well advanced, and indeed some implementations have been made, they are still open to development. As usual, attention will be focused on the wireless and mobile implications.

5.7.1 IntServ

The Integrated Services (IntServ) solution provides hard guarantees on the QoS experienced by individual traffic flows. It does this through the use of end-to-end signaling and resource reservation throughout the network. The reservation is regularly refreshed. The IntServ architecture provides three basic levels of service:

- The Guaranteed Service gives hard QoS guarantees with quantified delay and jitter bounds for the traffic. It also guarantees that there will be no packet loss from data buffers, thus ensuring near-lossless transmission. This Service is intended to support real-time traffic.
- The Controlled Load Service makes the network appear to be a lightly loaded best-effort network. This class is aimed at delay-tolerant applications.
- Best Effort (no reservation required).

To achieve this, IntServ requires per-flow state to be maintained throughout the network. It was developed with the assumption that QoS was primarily required for large-scale multicast conferencing applications. This led to the decision to use delay-based admission control. The best-known problem with the IntServ approach is its poor scalability, because per-flow state needs to be maintained in the core network, where thousands of flows may exist simultaneously. Also well known is that reservations need to be regularly refreshed, which consumes valuable resources, especially in bandwidth-scarce environments. Other problems are that the call admission procedures and the routing scheduling schemes are complex and rely heavily on the per-flow state. This is primarily a result of the use of delay-based admission. For example, most IntServ buffers use weighted fair queuing management schemes. The guaranteed service may also lead to inefficient network use, especially within the core network. Whilst many Internet Drafts have been published trying to overcome these problems, the now disbanded IntServ working groupissued a position statement saying that the approach is only suitable for small networks. A further question that has been raised with IntServ is that it provides absolute guarantees and essentially duplicates some of the

functionality already provided in RTP –such as jitter control. Thus, an application that used RTP to provide stream synchronisation would receive jitter control twice if it also wanted packet delay controlled. This is another indication that it is overly complex.

TCP is not the only transport layer service that assumes near-losssless transmission. This assumption also underlies the real-time QoS class definitions. For example, the IntServ guaranteed service assumes that, if a router buffer is not overfilled, the delay can be known and all loss avoided. This is not sufficient in the wireless environment, where there is an (uncontrollable) relationship between transmission delay and loss.

5.7.2 Multi-Protocol Label Switching (MPLS)

MPLS was originally presented as a way of improving the forwarding speed of routers, but it has capabilities that enable an operator to provide service differentiation. It is becoming widely used as a network management or traffic engineering mechanism. It appears particularly suited to carrying IP traffic over fast ATM networks.

The basic principle of MPLS is that routers at the edge of the MPLS domain mark all packets with a fixed-length label that acts as shorthand for the information contained in the IP packet header. This label identifies both the route that the packet needs to take through the MPLS network and the quality of service category of the packet. MPLS packets follow predetermined paths according to traffic engineering and specified QoS levels.

The label is very short (32 bytes). Thus, once within the network, packets can be routed very quickly on the basis solely of the label. This requires significantly less processing than routing based on analysis of an IP packet header.

MPLS can be used to provide a wide range of different service classes, which could include reliable data transport and delay-sensitive transport services. This service is guaranteed not on an end-to-end basis, but only across the particular MPLS domain. This is a prioritisation service, and service level agreements are typically used for admission control.

MPLS has received much favourable press, and is used successfully in certain circumstances to provide some QoS today. Equally, however, it has received unfavourable press. Concerns include the amount of processing that is required to turn IP packets into MPLS packets, scalability, the impact on routing protocol, and finally security. The security concerns primarily apply to the use of MPLS to provide Virtual Private Networks (VPN), and they are twofold.

First, MPLS for VPNs does not, by default, encrypt everything, it is upto human operators to configure the system correctly – and most security problems occur as a result of human error. Second, the humans responsible for the configuration are typically the ISP, not the actual person/company using the network. This highlights the key issue for MPLS – it essentially moves intelligence back into the control of the network operator, breaking away from the end-to-end principle.

In many respects, MPLS for QoS is similar to the DiffServ approach presented below, although, to reduce the scalability problems, it is usually used as a Layer 2 rather than a Layer 3 solution. It provides improved granularity of service at the expense of more complex administration. In itself, it cannot provide end-to-end QoS configurable on a flow-by-flow basis.

5.7.3 DiffServ

The Differentiated Services (DiffServ) architecture aims to provide service differentiation within the backbone networks. It provides a simple QoS, with no signaling mechanism and QoS delivered only to aggregated traffic classes rather than specific flows. Essentially, on entry to a network, packets are placed into a broad service group by the classifier (Figure 40), which reads the DiffServ CodePoint (DSCP) in the IP packet header, the source and destination address, and determines the correct service group. The correct group or class is determined through static service level agreements (for example, packets from the boss are always given the highest priority). The packets are then given a suitable marking – this may involve changing the DSCP. Traffic shaping may then occur, for example to prevent large clumps of data with the same DSCP entering the network. All packets within a specific group receive the same scheduling behaviour. These behaviours can be simple to implement using class-based queuing[6]. Once within the network, routers only have to forward the packets according to these network defined scheduling behaviours, as identified through the DSCP.

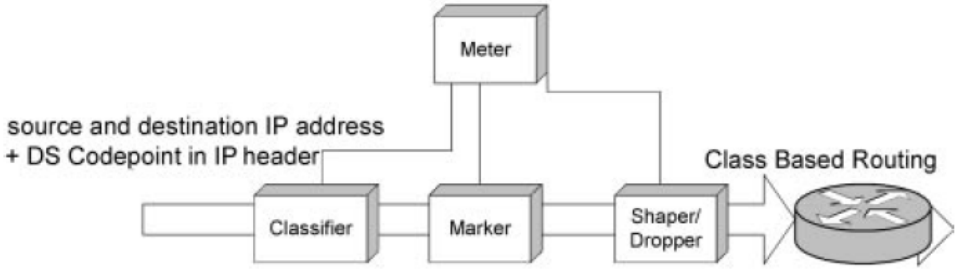

Figure 40: Components in a DiffServ border router

The complex processing (classification, marking, policing to ensure that no class is oversubscribed and traffic shaping) only takes place at the boundaries of each network domain. This may be done individually by the traffic sources, edge nodes, or a centralised bandwidth broker may be involved. This is sufficient to protect the network and guarantee the service for the aggregate class.

A number of different classes have been defined. These include the Expedited Forwarding (EF) class, which aims to provide a low-jitter, low-delay service for traffic. The definition of this class is currently being tightened, primarily to ensure that it can be easily used within the Integrated Services over Specific Link layers (ISSLL) framework described below. Users must operate at a known peak rate, and packets will be discarded if users exceed their peak rate. The Assured Forwarding (AF) classes are intended for delaytolerant applications. Here, the guarantees simply imply that the higher QoS classes will give a better performance (faster delivery, lower loss probability) than the lower classes. These classes have cross-Internet definitions. Finally, network operators are also at liberty to define their own per-hop behaviours – use of these behaviours requires packet re-marking at network boundaries.

This appears to be a good solution to part of the QoS problem as it removes the per-flow state and scheduling that leads to scalability problems within the IntServ architecture. However, it provides only a static QoS configuration, typically through service level agreements, as there is no signaling for the negotiation of QoS. As with MPLS, end-to-end QoS cannot be guaranteed. DiffServ was only ever intended to be a scalable part of an end-to-end QoS solution.

5.7.4 ISSLL

The Integrated Services over Specific Link Layers (ISSLL) working group was initially formed to consider how to provide IntServ over specific link technologies, such as a shared Ethernet cable. One of the key ideas to come from this working group is an approach to provide IntServ QoS by using DiffServ network segments. This solution maintains the IntServ signaling, delaybased admission and the IntServ service definitions. The 'edges' of the network consist of pure IntServ regions. However, the core of the network is a DiffServ region, and all flows are mapped into one of a few DiffServ classes at the boundary – depending upon the implementation, in either the edge or border routers of Figure 41.

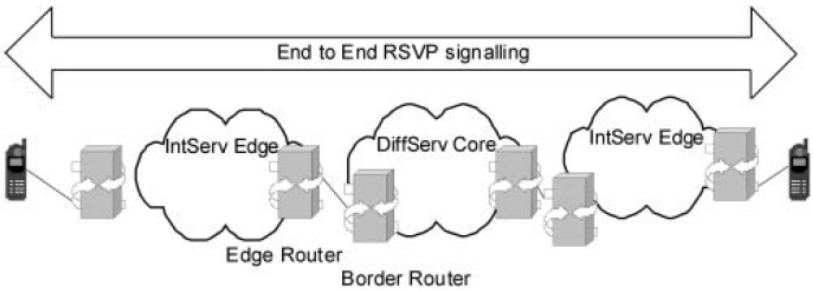

Figure 41: ISSLL architecture

This approach essentially treats the core of the network as a single (logical) IntServ link. This 'link' is created by tunnelling (or IPv6 source routing) the data and signaling messages across the DiffServ Core. This ensures that routing table updates in the core do not lead to changes in the border/edge routers used by traffic. Traffic conditioning may exist both at the edge of the network and at the DiffServ network boundaries.

The advantage of this solution is that it allows hop-by-hop call admission, and flow-based scheduling at the edges of the network, where low traffic densities make this the most practical way to achieve good-quality guarantees.

In the core of the network, the scalable solution of DiffServ scheduling can be used, where hard guarantees on QoS can be made on the basis of more probabilistic judgements. From the above discussion, it can be seen that most QoS architectural solutions may be based around the ISSLL solution, with attention paid to the class definitions. This flexible approach, only standardised in late 2000, should finally enable end-to-end QoS for the Internet. Already, small RSVP/IntServ networks exist, whilst larger network operators are implementing DiffServ core networks.

5.7.5 RSVP

The Resource ReserVation Protocol, RSVP, is a mechanism for signaling QoS across the network. It is a key element of both IntServ and ISSLL approaches described above. Although it is strongly associated with the IntServ architecture, it is a more general QoS signaling protocol. Whilst not widely interpreted by routers within networks, RSVP has been widely implemented on a range of different terminals, including Microsoft Windows.

RSVP is an out-of-band signaling system that operates in a soft-state mode – although the protocol is flexible, and it is possible to operate RSVP in a near-hard-state mode across any section of a network. This is a particularly useful feature in wireless networks, where it is important to minimise the amount of signaling to save both wireless network bandwidth and mobile battery power. RSVP messages are sent end to end,

but carry a flag to enable them to be read and processed by network elements. RSVP assumes that the receiver is responsible for establishing QoS (and, by implication, paying for the level of QoS it receives). It is a two-pass protocol.

This ensures that it can handle asymmetric paths, and it enables the sender to identify the nature of the transmitted traffic to the receiver (so that the receiver can make an informed choice as to the level of QoS requested). Whilst the receiver is typically responsible for the actual reservation, the sender also implicitly acknowledges the suitability of the reservation and so can be held responsible in any case of dispute. The sender initially describes the data and identifies the data path. The receiver then sends a reservation message back along the data path – to achieve this, state is installed throughout the network. Initially, RSVP was designed to operate on a hop-by-hop basis, but the ISSLL community has now considered the use of RSVP across DiffServ domains, where only the edge nodes interpret the RSVP messages.

5.7.6 Details of RSVP Signaling

The main messages are PATH and RESV, which establish a reservation, and PATH_TEAR and RESV_TEAR, which delete a reservation. The PATH message is generated by the sender and propagates through the network to the receiver, gathering information about the network. Each node that processes the message records the session identifier and the address of the previous (RSVP enabled) router. The RESV message, sent by the receiver, actually chooses the required QoS and establishes the reservation. This message is propagated back along the same path though the network via each of the previous router addresses, as stored during the PATH stage. This is needed because, typically, within the Internet, messages that flow in opposite directions between two terminals will follow different paths.

Thus, without this support for reverse routing, control messages from the receiver would not reach the nodes in the data path. PATH_TEAR and RESV_TEAR messages delete the reservation – the PATH_TEAR message is generated by the sender, whereas the RESV_TEAR message is generated by the receiver. This also is propagated using the previous router address mechanism. The process is indicated in Figure 42.

The message contents consist of a number of objects including the session identifier, and the previous (RSVP enabled) hop address. However, most of the message objects, in particular the following, are defined not by RSVP but by the IntServ standards:

- The sender's description of the traffic characteristics (TSPEC).
- The receiver's desired QoS (FlowSpec).
- The network's description of the capability of the Path (ADSPEC).

The traffic description (TSPEC) is supplied by the sender and carried in the PATH message. Since RSVP was developed specifically for multicast applications, this TSPEC is not altered, even if the protocol discovers a network bottleneck.

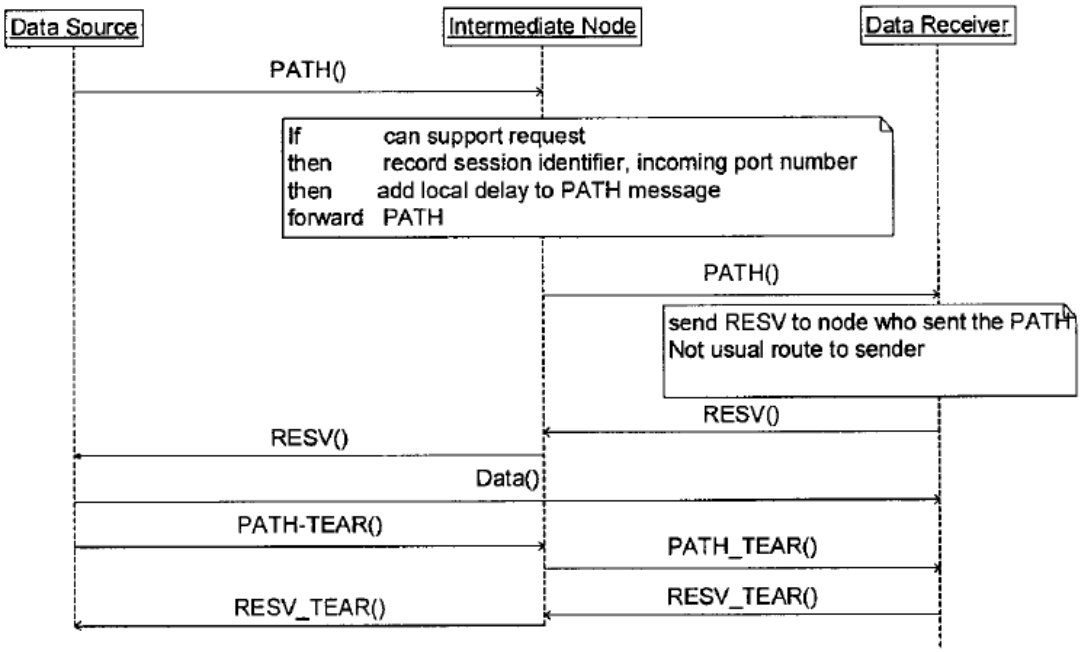

Figure 42: Establishing a uni-directional RSVP reservation

As the PATH message propagates through the network, the network builds the ADSPEC objects. There is an ADSEPC object for each service that the network supports, and it indicates the amount of resources that are available for that type of service. It is up to the receiver to determine the best service for its requirements. The network information contained in the ADSPEC includes:

- If there is a non-IntServ hop.
- The maximum transmission unit (MTU) size.
- The minimum path latency – Zero if no information is available. This is a representation of the expected (distance related) transmission delay.
- The path bandwidth estimate – The amount of bandwidth the receiver could ask for within the service; this bears no relationship to the bandwidth the sender might want.
- Parameters that enable the receiver to calculate routing delay. The receiver uses the PATH information to determine what reservation it should make in a RESV message. This is described in the FlowSpec object.

This message must be forwarded to each router in the data path using the reverse route installed during the PATH set upstage. Within the ISSLL architecture, the DiffServ region must append a DiffServ class object to the message that tells the sender (or previous node) which DiffServ class to use.

5.7.7 Use of RSVP in a Mobile Environment

In the section on QoS management after handover, a need was identified for a process that repairs the reservation after handover, whilst minimising the signaling and processing load on both the network and mobile terminal. Where the mobility is managed through manipulation of the routing tables (as in the per-host forwarding mobility management schemes), the RSVP local path repair mechanism is an example of a suitable process. As in the case of handover markings, this assumes that the divergence/convergence nodes

hold per-flow state. When a node detects a change in the set of outgoing interfaces for a destination, RSVP can update the path state and send PATH refresh messages for all sessions to that destination. The delay between detecting a path change and sending a path change message is configurable and should be adjusted to give the mobility management mechanisms a chance to build the path. Once the new path message reaches a node that recognises that the message is a result of local path change, it should send a RESV message immediately – thus, the end nodes need not know that the path has changed. Essentially, local path repair is using the detection of a routing change rather than a timer to initiate the soft state refresh messages. It enables quick re-establishment of QoS.

There are a couple of potential problems with using this in the mobile environment. The first is that the mobile node is always either the divergence or convergence node, and so, using straight RSVP local path repair, this mobile node would have signaling and processing requirements placed upon it. Where the context transfer protocol is used, this situation can be avoided (Figure 43). Figure 43 also indicates that the old reservation is explicitly removed in this process. This is not part of the standard RSVP implementation, which relies on unnecessary reservations being removed through the soft-state management.

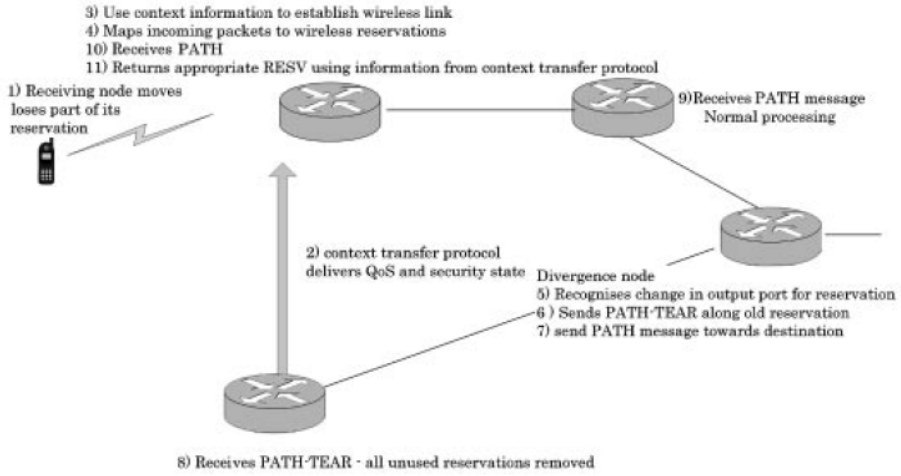

Figure 43: Context Transfer Protocol and RSVP

However, in bandwidth-restricted networks (mobility and wireless networks), this process may not be sufficient. RSVP may be operated in near-hard-state mode to minimise the amount of Signaling that is needed within the network. This could then result in 'hanging reservations' being left after a mobility event. Such hanging reservations could also be left if a session is incorrectly terminated. Thus, if RSVP is used in near-hard state mode through the network, additional mechanisms need to be in place to protect the network. An example of how to achieve this could be to use data traffic as an implicit reservation refresh indicator. The approach described above essentially fixes the reservation after the handover has taken place – which leaves the problem of what happens to data whilst the reservation is being repaired. Other approaches to the handover problem in RSVP have also been devised, essentially using the active and passive reservation approach previously outlined. These ensure that a reservation is in place as soon as handover occurs – although with the penalty of additional complexity and scalability problems.

5.8 IPv6 Quality of service

The behavior defined for the Differentiated Services field in both IPv4 and IPv6 is the same, so an understanding of DiffServ for IPv4 should carry over to DiffServ for IPv6. In both protocols, the Differentiated Services field is defined for the six bits following the version in the IP header. RFC 2474, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," spells out how DiffServ works for both protocols.

The following are some other RFCs of interest for DiffServ.

RFC 2963 "A Rate Adaptive Shaper for Differentiated Services"

RFC 2998 "A Framework for Integrated Services Operation over Diffserv Networks"

RFC 3086 "Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification"

RFC 3260 "New Terminology and Clarifications for Diffserv"

RFC 3290 "An Informal Management Model for Diffserv Routers"

RFC 2430 "A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)"

RFC 2474 "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers"

RFC 2475 "An Architecture for Differentiated Service"

RFC 2638 "A Two-bit Differentiated Services Architecture for the Internet"

RFC 2983 "Differentiated Services and Tunnels" Closely related to the issue of differentiated services is the use of flows in IPv6, as will be seen in the next section.

5.8.1 IPv6 Flows

The Flow Label field in the IPv6 header was originally designed as a 28-bit field (see notes in RFC 1809), reduced to 24-bits by 1995, and ultimately to 20 bits, as defined in RFC 2460. RFC 2460 states the following.

The 20-bit Flow Label field in the IPv6 header may be used by a source to label sequences of packets for which it requests special handling by the IPv6 routers, such as non-default quality of service or "real-time"service. Hosts or routers that do not support the functions of the Flow Label field shall set the field to zero when originating a packet, pass the field unchanged when forwarding a packet, and ignore the field when receiving a packet.

In an appendix to RFC 2460, a *flow* is defined as "a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers." That "special handling" might be specified by a resource reservation protocol or by some data within the flow packet headers such as a hop-by-hop option. As to the specifics of the implementation of flows, however, RFC 2460 is silent other than to specify the characteristics of the value of the flow header field.

Packets that don't belong to flows must have the flow header set to zero.

Each flow is assigned in a random or pseudo-random manner and (in combination with source address) is uniquely identifiable.

The flow label is assigned by the source of the flow.

Packets that belong to the same flow must all originate from the same source address, must be addressed to the same destination, and must be sent with the same value in the flow label header field. Flows are traditionally also identified by the transport layer protocol in use, as with TCP.

As of 1998, the flow label was considered an experimental portion of the IPv6 specification; five years after, the IETF had not yet published the IPv6 flow label specification as a proposed standard RFC. Although still officially a work-in-progress as of mid-2003, publication of an RFC titled “IPv6 Flow Label Specification” may already have occurred by the time this volume is published.

The definition of a flow, meanwhile, has changed.

A flow could consist of all packets in a specific transport connection or a media stream. However, a flow is not necessarily 1:1 mapped to a transport connection.

One change from RFC 2460 is that flows can be specified without reference to the destination address or transport layer protocol type. These values may not always be available in the IPv6 header, particularly if the packet is fragmented or encrypted.

The flow label may not be changed from the value assigned by the sender, unlike the DiffServ value, which may be modified to reflect the appropriate behaviour aggregate for a particular router or network as it traverses the Internet. Routers that don’t offer flow-related handling are required to ignore the flow label and treat the packet as any other.

IPv6 nodes that use flow labelling should assign separate flows for different and unrelated transport layer connections as well as for different and unrelated application layer data streams. Thus, a multi-user host with multiple telnet sessions from different users to the same remote host should assign a separate flow to each of those sessions.

5.8.2 Explicit Congestion Notification in IPv6

Quality of Service specifications are largely intended to address the problem of how to guarantee a particular level of service for a particular set of packets. For example, an ISP may want to offer its customers a level of service that uses only their premium, high-performance networks. To achieve that level of service, the ISP would need to be able to differentiate packets coming from subscribers to that service and assign those packets to a behaviour aggregate for which the routing policy is to always route on the most expensive link.

Network congestion can occur on any link as a result of high-demand conditions or router malfunctions, and in most cases nodes sending packets that encounter congestion are only able to detect the condition as a result of some timer—usually in the transport or application layer protocols—timing out. Explicit Congestion Notification was first proposed as an experiment for the transport layer inRFC2481, “A Proposal to Add Explicit Congestion Notification (ECN) to IP,” in 1999, and quickly moved to the standards track in 2001 when it was published as RFC 3168, “The Addition of Explicit Congestion Notification (ECN) to IP.”

Using ECN and a Congestion Manager implementation, nodes are able to negotiate the use of ECN. The ECN field in the IPv6 (and IPv4 header, as well), consists of the two bits after the Differentiated Services field. Unlike in earlier proposals, the two bits are used together as *codepoints* rather than as separate flag bits. The four different values possible for these two bits—00, 01, 10, and 11—indicate whether the end-nodes

(sender and destination) are using an ECN-Capable Transport as well as whether there is congestion at the sender (though not so much congestion that would cause the node to have dropped the packet).

These are the four codepoints and their uses.

00 When a node is not using ECN, it puts zeroes in the ECN field.

01/10 These two codepoints are treated in the same way and are also called ECT(0) (for the value 01) and ECT(1) (for the value 10). These values are set by the sender to indicate that ECN is supported at both ends of the transmission.

11 Routers that are just beginning to experience congestion, or that are experiencing mild congestion, can signal their state by setting the codepoint to 11 in outgoing packets.

The following current RFCs provide more information about Explicit Congestion Notification and congestion control in general.

RFC 2481 "A Proposal to Add Explicit Congestion Notification (ECN) to IP"

RFC 2914 "Congestion Control Principles"

RFC 3124 "The Congestion Manager"

RFC 3168 "The Addition of Explicit Congestion Notification (ECN) to IP"

RFC 2884 "Performance Evaluation of Explicit Congestion Notification (ECN) in IP Networks"

5.9 Summary

This section has looked at some of the mechanisms that have been proposed to enable the Internet to provide real-time QoS services. After reading this section, the reader may feel that there is no complete solution for this problem that will work in a fixed, let alone mobile, environment. IntServ is too complex and non-scalable, MPLS and DiffServ do not provide full end - to - end QoS solutions, and ISSLL is a framework for a solution, not a solution in itself, and relies on RSVP, which in turn needs some fixes to work well in a mobile environment. However, many of the required elements are present, and solutions exist for many of the potential problems. The following section therefore looks at one way in which a solution can be created. Within all this, however, it is worth remembering that both DiffServ forwarding behaviours and RSVP are being modified within the IETF, to reflect how people actually use them.

Quality of Service, IPv6 Flows, and Explicit Congestion Notification are all related to the quest for better service over an Internet in which, by definition, all packets are supposed to be treated equally. As we've seen in this chapter, Quality of Service is designed to offer consumers of Internet connectivity options for guaranteed levels of service, while IPv6 flows and Explicit Congestion Notification are designed to provide improved routing and connectivity for any nodes on the Internet.

6 HIP Host Identity Protocol

6.1 Introduction

During the research study of Secricom Task 6.1 we found interesting protocol which is balanced between IPv4 and IPv6. Task 4.3 will be the place to try this protocol for development of new solution in PTT services. The comparing of pure IPv6 and HIP give us chance to developed new efficient secure communication application. D6.2 will be more focused to security and cryptography, Security and dependability are, then, crucially important aspects of communications and networks that need very much more exposure, as well as considerably more investment by enterprise owners. The Host Identity Protocol (HIP) offers the dual prospects of more secure and more dependable communications through the separation of identity and location, as well as a number of related potential benefits. Although the first HIP draft was submitted in 1999 at the IETF, HIP remained unknown to a wider audience until recently.

HIP is developed to address these issues in an integrated approach that fits well within the TCP/IP architecture. The original ideas on the separating of host identity and location in the Internet date back to Saltzer in “RFC 1498 On the Naming and Binding of Network Destinations”. However, only recent advances in public key cryptography and new requirements of portable terminals have made the actual design and implementation possible. It is true that HIP is only one of many proposals developed recently in the IETF in the area of security and mobility. Compared with other proposals that often solve only a small part of the problem, HIP integrates host mobility and multihoming in a simple and elegant way.

The Host Identity Protocol uses a wide range of cryptographic mechanisms to secure the Host Identity (HI) namespace, to securely establish a protected channel, to defend against Denial of-Service attacks, and to protect the mechanisms that, among other features, enable mobility and multihoming. This chapter introduces some basics that are necessary to understand the design and rationale of the security mechanisms employed by HIP. After stating some goals for secure communication protocol, we will discuss various attacks that aim at undermining these goals. In the following, we introduce some basic cryptographic techniques that serve as building blocks for security and key-exchange protocols.

6.2 Internet namespace

Namespace in the Internet allows to uniquely identify an entity such as a host or a service. At the moment two namespaces for hosts are globally deployed in the Internet: IP addresses and DNS names. The IP addresses also serve as host locators in the Internet as we will describe in the following sections. DNS names provide hierarchical human-friendly host names. DNS names can be location independent (such as from .net domain) or limited to a certain geographical area (such as .fi for Finland). The DNS namespace has several limitations.

Updating the current IP address in DNS can be too slow to support mobility. Furthermore, most hosts do not even have modification access to the DNS servers they are using. The basic DNS service is not secure and can be easily spoofed. DNSSEC offers an improvement in security, but is still not universally used. Many DNS names are bound to a specific organization or country. For example, if a user changes employer or school, the host DNS name suffix will almost certainly change to reflect the new administrative location.

Such updates can last for many hours due to caching of DNS information. To make things worse, some applications such as Internet Explorer ignore DNS Time-to-Live information and can cache DNS entries longer than their lifetime.

Current namespaces have three shortcomings. First, changing the host address is not directly possible without breaking transport layer connections. Second, authentication of the host is not supported; spoofing of a source IP address is a common problem in the Internet. Third, privacy-preserving communication is not provided.

6.3 Methods of identifying a host

In HIP, a pair of self-generated public and private keys provides the Host Identity. The length of the public key can be 512, 1024 or 2048 bytes and is generated with the RSA algorithm by default. Most HIP implementations also support the DSA algorithm as it was the default before. Generation of new keys is a relatively time-consuming operation and occurs only infrequently, e.g. when the old keys have been compromised. Current Unix HIP implementation store public and private keys in the file system at /etc/hip directory.

In this chapter, we assume that a single identity per host is sufficient. In reality, often several identities are needed to protect the privacy of the user. Using the public key as a host identifier in packets and the application interface is inconvenient due to large and variable size. A typical Maximum Transmission Unit of 534 bytes would not even fit the shortest public key. For this reason, and to maintain compatibility with existing applications using the Berkeley socket interface, two additional forms of host identity are introduced as shown in Figure 44.

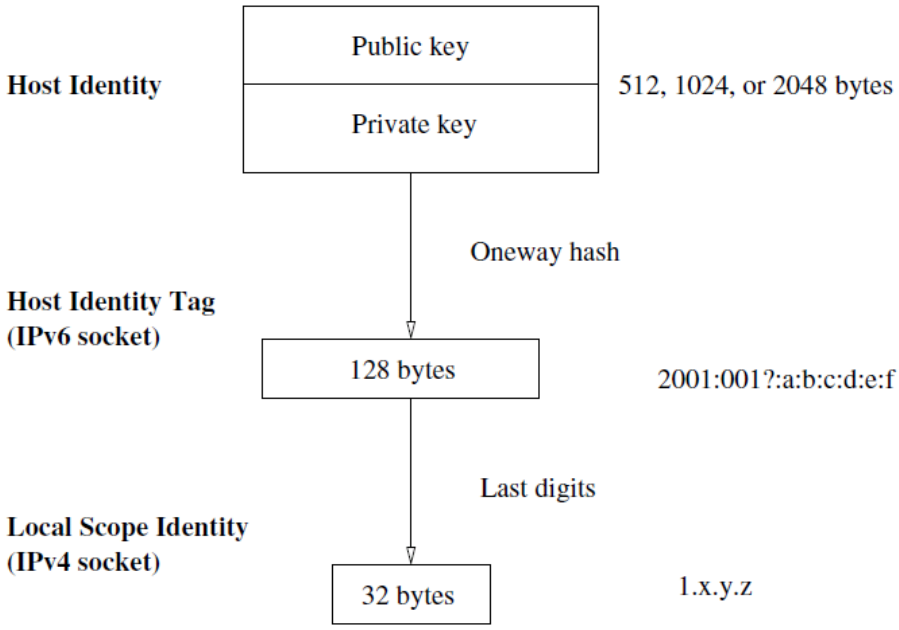

Figure 44: Methods of identifying a host

The Host Identity Tag (HIT) is a 128-byte hash of the public key. HIT has deliberately the same length as an IPv6 address and can be used instead of it by applications. The hash is one-way, it is not possible to restore the original public key from it. HITs are statistically unique given their sufficient length. The probability of a collision when two different public keys map to the same HIT is negligible. HITs have a prefix 2001:0010::/28 that enables to distinguish them from currently allocated IPv6 addresses. Having fixed-length identifiers gives an additional benefit of protocol independence from the cryptographic algorithm used to generate public−private keys.

The Local-Scope Identifier (LSI) is a 32-bit identifier that can be constructed taking the last bytes of the HIT. LSIs have shorter lengths than HITs and the probability of their collisions is significant. Therefore, LSIs have only local meaning and cannot be assumed to be globally unique. The LSI have the same length as IPv4 addresses and can be used by the legacy IPv4-only applications in the socket interface. LSIs have a prefix 1. to distinguish them from publicly allocated IPv4 addresses.

Each HIP implementation is required to support multiple HIs. One HI should be reserved for anonymous communication. Initiators are expected to utilize anonymous communication more often than Responders.

6.4 Overlay Routable Cryptographic Hash Identifiers

IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHIDs) reserves a part of the IPv6 address space to serve as identifiers in the socket APIs. Internet Assigned Numbers Authority (IANA) allocated a prefix for ORCHIDs. ORCHIDs appear as IPv6 addresses but are not routable at the IP layer, although are expected to be routable at the overlay layer on top of IP. Applications can transparently use ORCHIDs in place of regular IPv6 addresses. ORCHIDs can contain, for example, HIP HITs or Temporary Mobile Identifiers for the Mobile IP Privacy Extensions.

6.5 The purpose of an IPv6 prefix

The main goal of introducing a special format for ORCHIDs is to prevent confusion with regular IPv6 addresses. Naturally, an application can use a subset of IPv6 addresses in place of identifiers. That, however, can cause leaking of non-routable addresses to unaware applications for example through referrals. In addition, different applications can select different prefixes for identifiers that can potentially prevent interoperability in the Internet. ORCHIDs are meant to be used as identifiers in the legacy application APIs. Newly developed applications are expected to use “native” API utilizing identifiers such as a public key in the interface instead of 128-bit ORCHIDs. However, in the near future it is unreasonable to expect that all applications and host OS are updated to support the new model. Instead, ORCHIDs offer a possibility to experiment with new network architectures in a reasonable way. ORCHIDs have the following properties. They are generated using a hash function that provides secure binding to the input parameters and statistical uniqueness. ORCHIDs are compatible with an IPv6 global unicast address format.

6.6 The role of IPsec

By default, HIP data packets are carried using IPsec utilizing the Encapsulated Security Payload (ESP) transport mode. The HIP control messages essentially provide a session key exchange between two hosts. While it would have been possible also to use other key exchange protocols, such as IKE or IKEv2, the new HIP architecture was created to be friendly with middleboxes. Middleboxes, such as firewalls, are able to examine the process of HIP key negotiation.

The ESP transport mode spans from an end host to another end host encrypting IP packet payload. Packets are multiplexed using the Secure Parameter Index (SPI) value to identify a Security Association (SA) between two hosts. An SA is established between HITs of two end points; only a single SA between a pair of HITs is supported. As the SA is bound to HITs, not IP addresses, the active set of IP addresses at the SA end point can change dynamically. The SA is identified using the SPI in ESP packets that are mapped to HITs at the end point. This property is sometimes called the HIT compression. There is no need to transmit HITs in data packets, which reduces the packet size. In summary, there is no HIP-specific data packet format defined, but the standard IPsec ESP mode is used. While the use of IPsec is preferable in all cases to enhance the security level, it is not always feasible e.g. for busy web servers or lightweight devices.

Furthermore, encryption could be also implemented on the upper layer such as SSH or TLS. Therefore, a different transport mode than IPsec might be needed in HIP in some cases. While some activities on developing lightweight HIP are ongoing, there is not yet a standardized solution.

6.7 Related IETF activities

Figure 45 shows the position of HIP with regard to other relevant proposals in the IETF. The figure shows relevant groups in the areas of Internet architecture, security, mobility, and multihoming. Most proposed protocols are placed in one or two areas and thus require combination with other protocols to achieve all desired properties. Complexity of such combinations can result in poor performance and implementation errors. HIP, on the other hand, provides secure mobility and multihoming with a simple and architecturally sound approach. In this section, we present a brief overview of IETF Working Groups (WG)relevant to IP.Mobility for IPv4 (mip4) and Mobility for IPv6 (mip6) Working Groups continue to develop the Mobile IP protocol based on the use of Home Agent for providing a stable IP address to a mobile host. The WGs document the existing deployment experience and examine interoperability issues between the implementations. The current goals of WGs include adoption of IKEv2 for establishing IPsec Security Associations, dual-stack support and reducing the configuration burden per mobile node. Switching of the Home Agent and bootstrapping a mobile node after powering on, as well as firewall traversal and location privacy, are also within the scope.

The IKEv2 Mobility and Multihoming Protocol (MOBIKE) WG concluded in 2006 after publishing protocol specifications in RFC 4555. The MOBIKE protocol enables the IP addresses of IPsec tunnel mode Security Associations to change and can be used for mobile VPN or site multihoming. The MOBIKE protocol removes the need to create new Security Associations, which reduces the computation overhead and can save the user from entering codes from a token card.

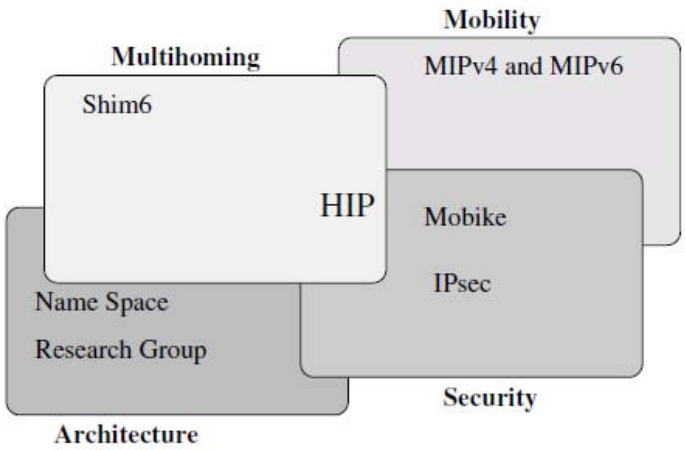

Figure 45: HIP relation to other IETF activities

The Site Multihoming in IPv6 (multi6) WG documented the ways that multihoming is currently implemented in IPv4 networks and evaluated several approaches for advanced multihoming. The security threats and impact on transport protocols were covered during the evaluation. The work continued in anotherWG Site Multihoming by IPv6 Intermediation (shim6) focusing on specifications of one selected

approach. This WG uses the approach of inserting a shim layer between the IP and the transport layers that hides effects of changes in the set of available addresses. The applications are using one active address that enables referrals. Shim6 relies on cryptographically generated IPv6 addresses to solve the address ownership problem. The shim6 host can benefit from multihoming properties even when its peer host does not support shim6 extensions.

The current IPsec and IKE protocols provide strong security guarantees but require the use of pre-existing credentials that can be validated. Better-Than-Nothing Security (btns)WG specifies extensions to the IPsec architecture and IKE to support unauthenticated Security Associations. The use of self-signed certificates and self-generated public keys with BTNS would enable simpler and faster deployment of IPsec. The WG also studies how to use IPsec to secure upper-layer protocols. As an example, if a user accesses a sensitive web site over IPsec, there must be some indicator in the browser confirming that the traffic is protected by IPsec.

The WG Mobility for IP: Performance, Signaling and Handoff Optimization (mipshop) develops Hierarchical Mobile IPv6 (HMIPv6, RFC 4140) and Fast Handovers for Mobile IPv6 (FMIPv6, RFC 4068) to reduce the delay and packet loss for a mobile host. The goal of the group is to advance the specifications from an experimental to the standard-track status. The group also develops on optimization of return ratability test in terms of security and performance by using Cryptographically Generated Addresses and Credit-based Authorization. Other WGs possibly related to HIP include Mobile Nodes and Multiple Interfaces in IPv6 (Monami6), Network Mobility (nemo), and Network-based Localized Mobility Management (netlmm).

6.8 HIP multicast

The HIP architecture is designed for host-to-host communication, also known as unicast. However, certain applications, such as Internet TV, involve data transmission from one source to multiple destinations. Some applications, such as multi-party video conferencing, involve transmission from several sources to several destinations. Such scenarios are most efficiently handled using multicast data transmission, where the source transmits a single copy of data and routers or hosts in the network multiply packets as needed for delivery to downstream recipients.

Multicast can be implemented on the networking layer as native IP multicast, or as an application service on the overlay network. The network multicast is more efficient than the application multicast, because it can achieve “one link - one packet” principle, whereas application multicast can still transmit multiple copies of the same packet over a link. The Internet Indirection Infrastructure (i3) is one possible system for implementing application layer multicast. Application multicast is easily deployable while several issues hindered deployment of IP multicast. One issue is lack of access control in the native IPv4 multicast model known as Any Source Multicast (ASM). Any host can join the multicast tree as a receiver by informing its router. A more restrictive version of multicast called Source Specific Multicast (SSM) limits who can transmit to the multicast tree; a complete access control for receivers is still missing.

In standard HIP, a single public−private key pair identifies a single host. Some researchers perceive HIP multicast as using a public key to identify a group of hosts. Therefore, the group must generate and share a private key between members of the group. In this section, we focus on the case where each host has own public−private key pair and is willing to join an IP multicast tree.

6.9 Challenges for IP multicast

Mobility of hosts participating in multicast is a largely unsolved problem. Particularly, if the multicast source changes the IP address, the whole multicast tree needs to be reconstructed. Although some solutions to the mobility problem based on bi-directional tunnelling are proposed, fundamentally the host identity is coupled with the current IP address. Furthermore, current multicast solutions do not allow construction of native dualstack IPv4/v6 multicast trees and do not support multihoming.

Two common approaches for multicast receiver mobility are Bidirectional Tunneling and Remote Subscription. With Bidirectional Tunneling, the receiver subscribes to the multicast stream via its home agent located in the user´s home network. When the user moves to a foreign network, it creates a tunnel to the home agent that relays the user´s multicast Signaling and stream data. Therefore, the user can move between networks without affecting the multicast tree. With Remote Subscription, the user asks the local multicast router in a visiting network to join the multicast tree. The old branch of the multicast tree from the previous user´s network location eventually times out and the data starts arriving to the new user´s location.

Few solutions exist to the mobility of the multicast sender. In SSM, the entire multicast tree is constructed using the IP address of the source as the root. If the sender moves, the entire tree needs to be rebuilt using the new IP address as the root. During the rebuilding process the multicast stream is interrupted and listeners do not receive any data. Bi-directional tunnelling can be applied to avoid the tree reconstruction for the mobile multicast sender.

Some solutions to provide authentication to multicast receivers were proposed, including Multicast Control Protocol (MCOP). However, MCOP is only able to authenticate the subnetwork where the user is located, not the host of the user. Therefore, other hosts from the same subnetwork can receive the multicast stream without authentication.

The last problem with native IP multicast is the difficulty of constructing a multicast tree combining IPv4 and IPv6 hosts. Although several solutions for IP version interoperability do exist, they are aimed at unicast communication and do not yet support construction of dual-stack multicast trees. A host that wants to join a multicast tree with a source located in a different IP version network is unable to create a valid join message. The receiver is unable to join the multicast tree even if the source has the same IP version but there is a transit network on the path to the source that has a different IP version.

7. Best practice of IPv6 use in safety services

7.1 Introduction

Among projects dealing with IPv6 in safety services we have to mention project U2010, where was IPv6 used in various scenarios. As example we can mention fire service solution., where was mobility based on IPv6. Short description of this solution:

7.2. U2010 and IPv6 used in Fire in tunnel scenario

The communication vehicle used in the fire services prototype is organised as a full network roaming between different networks (Wifi, UMTS and Satellite). The next picture illustrates the network configuration of the vehicle:

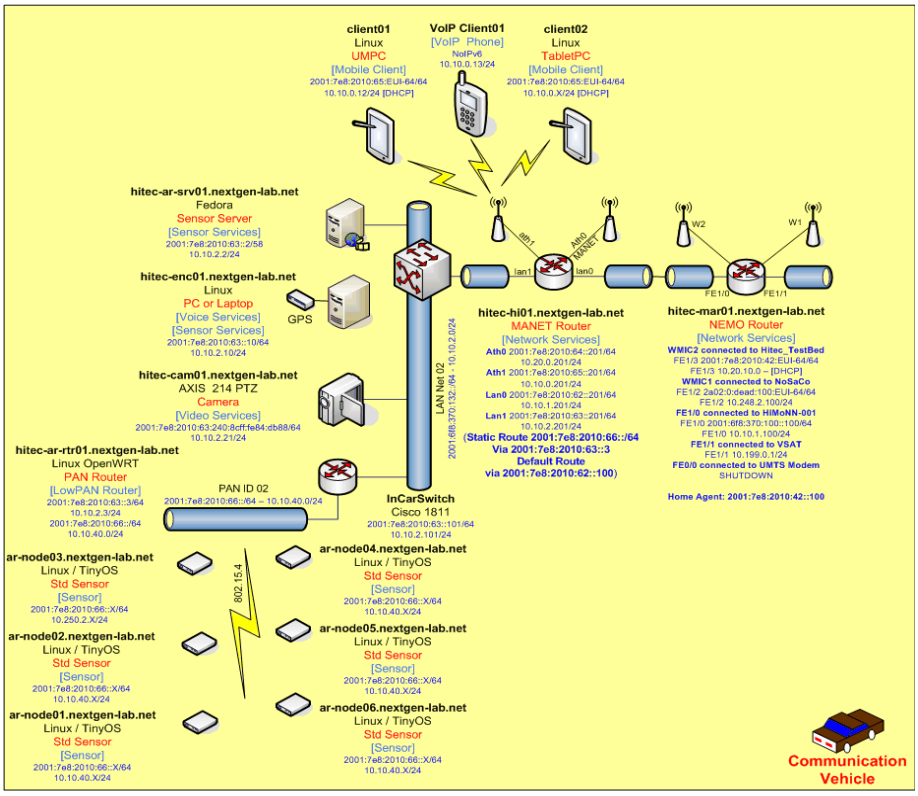

Figure 45: Vehicle network – U2010

There exists an IETF standard to provide mobility features for IP. Whereas it was optional in an IPv4 stack implementation, it becomes mandatory for the stack to support it with the new version of the Internet protocol, IPv6. With Mobile IP it is possible to assign a single and well defined IP address from within its home network to a device, wherever this device is located in the world. This means that such a device can be reached by it's correspondent node using this known address as soon as it connects somewhere to the global network, and that connections that have been established do not break when the device changes its point of attachment. It must be noted that no user intervention is necessary for this to work. As soon as the device connects to the a network, it registers it's current point of attachment (the current care-of address) at its home agent, which will take then the charge of forwarding the data destined to this device from it's home network to its current location.

7.3 U2010 and IPv6 used in Sensor Network Monitoring

Another work of U2010 was done for sensor monitoring based on ZigBee technology interworking with IPv6. Here we can mention this part of solution.

With the rising market demand for computing and ubiquitous network access, wireless local area networks (WLANs) become very popular. To convey information over relatively short distances, several wireless technologies and wireless personal area networks (WPANs) such previously described ZigBee platform is proposed and being extensively discussed. Unlike WLANs, connections effected via WPANs involve little or no infrastructure. To get availability of sensor network the interconnection gateway to wider network is needed. Such wide network model is presented on Figure 46.

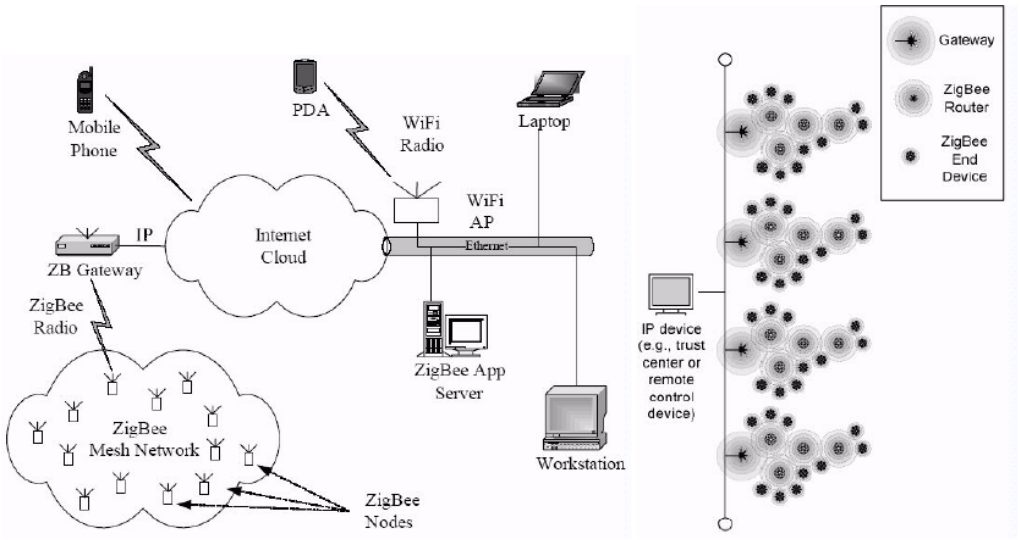

Figure 46: ZigBee network with interconnection to TCP-IP based network using gateway

With gateways the ZigBee mesh network can be reached via widespread internet network and it allows using of general software (web browser) and hardware (Wifi PDA) to connect mesh network. This feature allows small, power-efficient, and inexpensive solutions to be implemented for a wide range of devices. IEEE approved the standard for the low-rate WPAN (LR-WPAN) as 802.15.4 in 2003. Especially designed for low data rate wireless connectivity devices with limited battery consumption, 802.15.4 defines the physical layer (PHY) and medium access control (MAC) sublayer specifications typically operating in the radius of 10m and more. The maximum raw data rate is 250 kb/s to satisfy a set of simple needs such as consumer electronics, home automation, industrial controls, and sensor applications. The specification is focused on low complexity, low cost, low power consumption, and low data rate wireless connectivity among inexpensive devices. For the same LR-WPAN purpose and based on 802.15.4, the most popular upper layer protocol, ZigBee, was developed by the ZigBee Alliance in 2004. The ZigBee protocol standard contains the specifications of the network layer (NWK) and application layer (APL). Inside the APL, functions are defined separately as the application support sub-layer (APS), the ZigBee device objects (ZDO), the ZigBee device profile (ZDP), the application framework (AF), and ZigBee security services. The comparisons of ISO OSI, TCP/IP, and ZigBee/802.15.4 are shown in Figure 47.

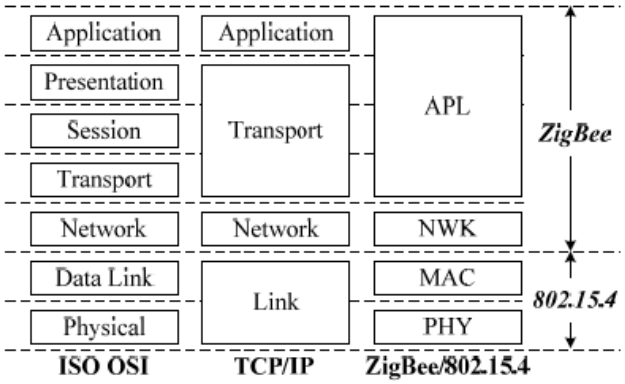

Figure 47: Protocol stacks overview

Since the TCP/IP has become the dominant protocol in the Internet due to its widespread use and reliability, and also the 802.3 ethernet is networking standard, the demand for internetworking between ZigBee/802.15.4 and TCP/IP/802.3 is inevitable. However, the design of ZigBee/802.15.4 is incompatible with the TCP/IP network. An internetworking architecture has to be designed to overcome this problem. Proposed design is dedicated to IPv6.

The straight forward method to make IPv6 work over ZigBee is to put the IPv6 stack on the top of ZigBee NWK layer. All the ZigBee nodes are assigned with an IPv6 address. At Gateway B, if a packet is received from the 802.3 network, it will be encapsulated into ZigBee NWK and forwarded to the 802.15.4 network . On the other hand, when a packet is transmitted from Node C to Host A, Gateway B will decapsulate the packet and use the IPv6 payload inside to continue the transmission (Figure 48). Because the data communication in ZigBee/802.15.4 is asynchronous message-passing, only UDP can be used with IPv6 in this scenario. The key issue of IPv6 over ZigBee is the packet size problem. According to the 802.15.4 specification, the maximum PHY service data unit is 127 bytes. In a data frame, after reducing the 23 bytes MAC header, 2 bytes frame check sequence (FCS), and 8 bytes NWK header, there are only 94 bytes left for the IPv6 packet. If the security mechanism (such as AES-CCM-128) is enabled, only 81 bytes will be left. This is quite tight for an IPv6 packet, which has 40 bytes basic header and even more extension headers. Also, the ZigBee/802.15.4 does not support packet fragmentation. It can not handle the 1280 bytes minimum transfer unit required by IPv6.

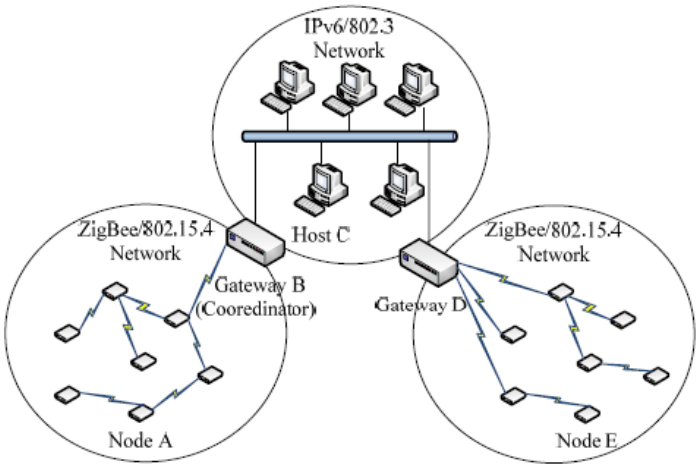

Figure 48: Network diagram

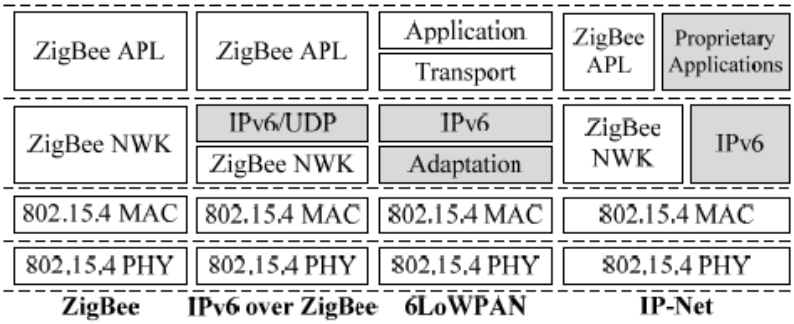

Figure 49: Approaches of protocol stacks

Transmission of IPv6 Packets over IEEE 802.15.4 networks can be done by an adaptation layer above the 802.15.4 MAC to support the IPv6 data packet (Figure 49, designed by 6loWPAN group). The adaptation layer is used to handle the packet fragmentation so that an IPv6 packet can be separated into many 802.15.4 frames for transmitting. The working group lists lots of problems in current development in. Besides, it throws the ZigBee stack away. Without ZigBee NWK, all the routing structures, address assignment, and data forwarding must be redesigned.

Another approach is IP-Net designed by the Helicomm Inc. and used in their product, IPLink, which is developed with the Silicon Laboratories Inc. As presented in Fig. 3b, it is a dual stack approach. Both the 6LoWPAN design and ZigBee stack are working on the same 802.15.4 MAC. Although it endows a node with both IPv6 and ZigBee functions, only one of them can be used at the same time. Thus, it is not an internetworking solution. Also, it has all the problems that 6LoWPAN has.

The only internetworking mechanism is NAT-PT solution. Example of network is presended on fig. 3a. When the network initiates, Host C must register its IPv6 address (IPC) to pre-assigned Gateway B (IPv6 address: IPB; ZigBee address: ZB). B will help C to get its ZigBee address (ZC). Node A must register its ZigBee address (ZA) to B, too. If A wants to communicate with C, it sends out the packet to ZC. B will translate the packet into IPv6 format with "Destination IP address = IPC" and "Source IP address = IPB". In the reverse path, for communicating from C to A, A will send the packet to IPB with a data payload which contains "Destination ZigBee address =ZC" and "Source ZigBee address = ZA". After B receives thepacket, it decapsulates the packet, looks for the payload, and translates it to 802.15.4 format. Users must pre-configure their hosts with fixed gateway address. The NAT-PT like design also breaksmany end-to-end features such as information security. Service discovery, one of the most important functions in ZigBee network, is unsolved. Also, the mechanism can not perform cross regions transmission, such as the communication between A and E. Because all the mechanisms above are not proper to integrate ZigBee/802.15.4 and IPv6/802.3 networks together, we design a novel overlay mechanism for the internetworking.

For further readings or design aim your attentions to internetworking mechanism comprising such desing criteria:

- Each ZigBee node should be assigned with a global unicast IPv6 address.
- Each IPv6 host which may communicate with ZigBee node should obtain a ZigBee address.
- Service discovery should be propagated to different network domain.

• Broadcast data in ZigBee network should be transferred to proper IPv6 hosts.

• Data packet transformations in the gateways should be as simple as possible and should not break the end-to-end model above the transport layer.

7.4 Mobile Emergency Room and IPv6-based Video System for Emergency Care Support

On October 19, 2005, Nara Institute of Science and Technology (NAIST) and City of Ikoma Fire Headquarters in Nara Prefecture conducted public trial of “Mobile ER”, a video system to support emergency care activities.

This system uses wearable computers (sets of a small PC, a camera and a display), as well as a server and wireless communication device mounted on an ambulance to send visual images of patients and accident scenes to fire headquarters and emergency medical centers. CDMA2000 1x EV-DO, a 3G communication technology, and IEEE802.11b/g, a wireless LAN technology, are used to provide communication infrastructure, while IPv6, Mobile IPv6 and IPv6NEMO are used as protocols (Figure 50).

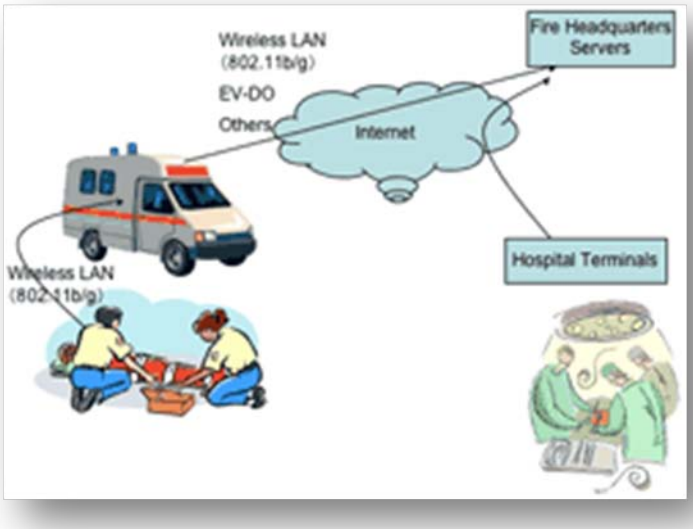

Figure 50: Mobile ER simple architecture

The public trial this time was only about sending images using a head-mount display and a camera worn by rescue personnel. But future plans include transmitting information from various devices such as magnetocardiograph and GPS. The system can incorporate communication infrastructure technology such as WiMAX and iBurst, for more realtime and high-quality images and video. With ambulances equipped with such information system, emergency care doctors can give appropriate instructions and prepare for care given to patients after they arrive at the hospitals even when the patients are still at the accident scene, improving the quality of medical care.

At present, communication from doctors at the hospital to rescue personnel is conducted by conversation over cellular phone. Future challenges include integrating the voice communication to Internet, move to broadband wireless, connect vital information gathering devices (such as magnetocardiograph), and correction and extraction of images.

Reasons IPv6 is used in this experiment are as follows:

- Mobile IPv6 and Network Mobility technology will be available on IPv6 only
- ISO (International Organization for Standardization) consensus is to use IPv6 for automobile network connectivity (TC204WG16)
- IPv6 enables flexible switching among multiple network interfaces (such as wireless LAN, cellular communication, and PHS).
- Privacy can be kept at protocol level using IPsec

Advantages of using such Internet standard technology are lower device purchase cost as all devices necessary for implementation can be off-the-shelf components, with no need to design dedicated devices or protocols. Existing PCs and network devices can be utilized also. Application software is the only thing that has to be developed. The system is scalable in that only part of it needs to be replaced to support future technological innovations.

This trial is a solution for emergency medicine, as well as a field trial of basic technology for connecting mobile devices to networks. In other words, there are several challenges in securing connectivity from a closed and mobile space of automobile to network. As for infrastructure, WiMAX, iBurst and other broadband wireless infrastructure will be available in the future, but implementation of mobility features as protocols will be necessary to conduct communication over it. These necessary components are defined in IPv6, and this trial attempted to run these components in reality. There have been some trials using IPv4, but this is perhaps the first case with IPv6. We should keep an eye on this as the next generation mobile communication technology.

7.5 Nextel Direct Connect Services

7.5.1 Direct Connect

Dedicated to quick, to-the-point conversations, Direct Connect gives possibility of instant, nationwide, one-to-one communication with other Nextel Direct Connect user.

Key Features:

- Instant and Nationwide. Allows connect in under a second with other Nextel Direct Connect user on the national push-to-talk network .
- Send Call Alerts function. Allows send a repeating alert to another user. All alerts will repeat until they're acknowledged or time out.
- Send text with Call Alerts function. In Sprint phone with Nextel Direct Connect, user can send or receive a free, pre-set text with Call Alert.

7.5.2 Group Services

Enable group push-to-talk communication options to fit users needs and group size. The three primary Nextel's group services:

- **Group Connect:** Allows set up groups of up to 20 other users, dynamically on phone, and connect instantly with others anywhere on Sprint's nationwide push-to-talk network. Groups can be created and stored directly on phone. With a Sprint phone, user can also set up and manage push-to-talk groups online via Sprint Mobile Sync (software to store and manage up to 5,000 contacts).

- **TeamDC:** User can create groups of up to 34 other users online. Then, any group member can initiate calls to that group and participate in calls initiated by other group members. Available only on dedicated Sprint phones. Allows user or someone else in user's group to take the floor if either of user has higher talking priority than the current speaker. The group owner, can set "high", "medium" or "low" priority for yourself or others in his group. Once a TeamDC group list is set up, each member of the group will be notified on their phone and can choose to either accept or decline the invitation. Only the group owner can make any changes or updates to the group, but all group members will receive those changes on their phones. All TeamDC groups are automatically stored on the Sprint network and can be accessed from user's phone or online via Sprint Mobile Sync. Up to 40 TeamDC groups can be saved in phone's contact list.
- **Talkgroup:** For implementations that need instant, large group communication for dispatch and collaboration, Talkgroup lets user the word out to 200 people at once. All users must be within the same local market and in the same fleet. Available only on Nextel or PowerSource phones. Dedicateed for large security, dispatch and industrial teams, Talkgroup is a group push-to-talk service that allows pre-defined groups to participate in ongoing communications, but all Talkgroup members must be located within the same local calling area. Each Talkgroup can consist of up to 200 users, although as with any group service, call quality may be reduced as group size increases. Users can belong to up to 250 groups (25 can be stored on a phone). Users can monitor only one Talkgroup at a time. Similar to tuning into a radio station, users select which Talkgroup to monitor and press "join", which allow them to hear conversations pertinent to only that Talkgroup. Talkgroup Scan is available on select phones, this feature allows users to simultaneously monitor communications on up to four Talkgroups. Members of a Talkgroup can identify who is speaking on a Talkgroup call.

7.5.3 Direct Talk

Maintain short-range (range up to six miles) contact with Direct Talk, the all-digital off-network push-to-talk service that works between compatible phones. During emergency situations or network outages, or when user is in a remote area, Direct Talk provides a reliable back-up communications tool. User can choose from 10 channels and 15 codes to keep his entire team in touch for short-range communication. In addition to the U.S. and U.S. territories, Direct Talk is legally approved and capable for use in Canada, Mexico, Peru, Brazil, Argentina, Columbia, Venezuela, and the Philippines.

7.5.4 International Direct Connect

International Direct Connect allows user to quickly reach any subscriber, even if he in different country. Eligible countries (out of USA): Canada, Mexico, Argentina, Brazil, Chile and Peru. International Direct Connect provides the same speed as local connections .

7.5.5 Summary

There is chance to analyzed outputs from various projects and take the best practice on IPv6 solution in safety services.

8. Abbreviations

ACK	Acknowledgment packet
ACL	Access Control List
ADSL	Asynchronous Digital Subscriber Line
AES	Advanced Encryption Standard
AH	Authentication Header
API	Application Programming Interface
AR	Access Router
ARP	Address Resolution Protocol
ASM	Any Source Multicast
BE	Base Exchange
BEET	Bound End-to-End Tunnel
BOS	Bootstrap packet
BSD	Berkeley Software Distribution
CA	Certificate Authority
CBA	Credit-Based Authorization
CBC	Cipher Block Chaining
CPU	Central Processing Unit
CRL	Certificate Revocation List
CS	Cryptographic Session
DCCP	Datagram Congestion Control Protocol
DH	Diffie–Hellman
DHCP	Dynamic Host Configuration Protocol
DHT	Distributed Hash Table
DNSSEC	Domain Name System with Security
DoS	Denial-of-Service
DR	Designated Router
DSA	Digital Signature Algorithm
ED	Endpoint Descriptor
ESP	Encapsulated Security Payload
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GNU	GNU is not UNIX
GPL	General Public License
GPRS	General Packet Radio Service
GRUU	Globally Routable UA URI
GSM	Global System for Mobile communications
GUI	Graphical User Interface

HCVP	Hash Chain Value Parameter
Hi3	Host Identity Indirection Infrastructure
HIP	Host Identity Protocol
HIPD	HIP Daemon
HIPL	HIP for Linux
HISM	Host Identity Specific Multicast
HIT	Host Identity Tag
HMAC	Hash Message Authentication Code
HMIP	Hierarchical Mobile IP
HTTP	Hyper Text Transfer Protocol
i3	Internet Indirection Infrastructure
IANA	Internet Assigned Numbers Authority
ICE I	nteractive Connectivity Establishment
ICMP	Internet Control Message Protocol
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IHC	Interactive Hash Chain
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IPv6	Internet Protocol version 6
IRTF	Internet Research Task Force
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LHIP	Lightweight HIP
LRVS	Local Rendezvous Server
LSI	Local Scope Identifier
MAC	Message Authentication Code
MIME	Multipurpose Internet Mail Extensions
MIP	Mobile IP
MITM	Man-In-The-Middle
MKI	Master Key Identifier
MLD	Multicast Listener Discovery
MOBIKE	Mobile Key Exchange
MODP	More Modular Exponential
MR	Mobile Router
MTU	Maximum Transmission Unit
NACK	Negative Acknowledgment
NAT	Network Address Translator

NEMO	Network Mobility
NIC	Network Interface Card
OCALA	Overlay Convergence Architecture for Legacy Applications
ORCHID	Overlay Routable Cryptographic Hash Identifier
OS	Operating System
P2P	Peer-to-Peer
PACK	Pre-Acknowledgment
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PIDF	Presence Information Data Format
PISA	P2P Internet Sharing Architecture
POSIX	Portable Operating System Interface
PSIG	Pre-Signature Packet
PSP	Pre-Signature Parameter
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
RFID	Radio-Frequency Identification
PKI	Public Key Infrastructure
ROC	Rollover Counter
RPC	Remote Procedure Call
RR	Resource Record for DNS
RSA	Rivest–Shamir–Adleman algorithm
RTO	Retransmission Timeout
RTP	Real-time Transmission Protocol
RTT	Round-Trip Time
RVA	Rendezvous agent
RVS	Rendezvous server
SA	Security Association
SACK	Selective Acknowledgment
SAD	Security Association Database
SCTP	Stream Control Transmission Protocol
SD	Service Discovery
SDP	Service Discovery Protocol
SHA	Secure Hash Algorithm
SIGMA	Signature and MAC
SIM	Subscriber Identity Module
SIMA	Simultaneous Multi Access
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SPD	Security Parameter Database

SPI	Security Parameter Index
SRTP	Secure Real-time Transmission Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SSM	Source Specific Multicast
SSO	Single Sign-On
SSRC	Synchronization Source
STUN	Simple Traversal of UDP through NATs
SYN	Synchronization packet for TCP
TCP	Transmission Control Protocol
TESLA	Timed Efficient Stream Loss-tolerant Authentication
TLS	Transport Layer Security
TLV	Type-Length-Value
TRIG	Trigger packet
TTL	Time to Live
UA	User Agent
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
URI	Universal Resource Identifier
UUID	Universally Unique Identifier
VIGMP	Version-Independent Group Management Protocol
VM	Virtual Machine
VMM	Virtual Machine Monitor
VoWLAN	Voice over WLAN
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WIMP	Weak Identifier Multihoming Protocol
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XFRM	Linux IPsec Transforms
XML	Extensible Markup Language

9. REFERENCES

6NET, D2.2.4: Final IPv4 to IPv6 Transition Cookbook for Organisational/ISP (NREN) and Backbone Networks, Version:1.0, Project Number: IST-2001-32603, CEC Deliverable Number 32603/UOS/DS/2.2.4/A1, February 4, 2005.

Cisco Systems, Internet Protocol (IP) Multicast Technology Overview and White Papers, Cisco Systems, San Jose, CA.

J. Davies, Understanding IPv6, Microsoft Press, 2002.

Desmeules, Cisco Self-Study: Implementing IPv6 Networks (IPV6), Pearson Education, May 2003.

M. Goncalves, K. Niles, IPv6 Networks, McGraw-Hill Osborne, 1998.

S.Goswami, Internet Protocols: Advances, Technologies, and Applications, Kluwer Academic Publishers, May 2003.

B. Graham, TCP/IP Addressing: Designing and Optimizing Your IP Addressing Scheme, 2nd ed., Morgan Kaufmann, 2000.

S. Hagen, IPv6 Essentials, O.Reilly, 2002.

C. Huitema, IPv6 the New Internet Protocol, 2nd ed., Prentice-Hall, 1997.

IPv6Forum, IPv6Vendors TestVoice,Wireless and Firewalls onMoonv6, http://www.

ipv6forum.com/modules.php?op¼modload&name¼News&file¼article&sid¼15&mode¼ thread&order¼0&thold¼0, November 15, 2004.

IPv6 Portal, http://www.ipv6tf.org/meet/faqs.php.

J. Itojun Hagino, IPv6 Network Programming, Butterworth-Heinemann, 2004.

H. K. Lee, Understanding IPv6, Springer-Verlag, New York, 2005.

P. Loshin, IPv6: Theory, Protocol, and Practice, 2nd ed., Elsevier Science & Technology Books, 2003.

M.A. Miller, Implementing IPv6: Migrating to the Next Generation Internet Protocol, Wiley, 1997.

M. Miller, P. E. Miller, Implementing IP V6: Supporting the Next Generation Internet Protocols, 2nd ed., Hungry Minds, 2000.

D. Minoli, VoIP over IPv6, Elsevier, 2006.

J. J. Amoss, D. Minoli, Handbook of IPv4 to IPv6 Transition Methodologies for Institutional and Corporate Networks, TF-ARBCH, New York, 2008.

Microsoft Corporation, MSDN Library, Internet Protocol, http://msdn.microsoft.com, 2004.

N. R. Murphy, D. Malone, IPv6 Network Administration, O.Reilly&Associates,2005.

RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden, December 1998.

RFC 2893, Transition Mechanisms for IPv6 Hosts and Routers, R. Gilligan, E. Nordmark, August 2000.

RFC 3022, Traditional IP Network Address Translator (TraditionalNAT), P. Srisuresh, K. Egevang, January 2001.

RFC 3306, Unicast-Prefix-Based IPv6 Multicast.

RFC 4038, Application Aspects of IPv6 Transition, M-K. Shin, Ed., Y-G. Hong, J. Hagino, P. Savola, E.M. Castro, March 2005.

H. S. Soliman, Mobile IPv6, Pearson Education, 2004.

D. Teare, C. Paquet, CCNP Self-Study: Advanced IPAddressing, Cisco Press, June 11, 2004.

J. D. Wegner, IP Addressing and Subnetting, Including IPv6, Elsevier Science & Technology Books, 1999.

RFC 2205 Resource ReSerVation Protocol (RSVP); Version 1 Functional Specification, Braden R ., September 1997.

Metz C, IP QOS: traveling in first class on the Internet, IEEE Internet Computing, Vol. 3, No. 2, March–April 1999.

RFC 2208 Resource ReSerVation Protocol (RSVP); Version 1 Applicability Statement Some Guidelines on Deployment, Mankin A, et al., 1997.

RFC 2746 RSVP Operation Over IP Tunnels, Terzis A, Krawczyk J, Wroclawski J, Zhang L, January 2000.

Pajares A, Berie´r N, Wolf L, Steinmetz R, An Approach to Support Mobile QoS in an Integrated Services Packet Network with Mobile Hosts, Technical report DCS-TR-337, Rutgers University, 1997.

Talukdar A, Badrinath B, Acharya A, MRSVP: A Resource Reservation Protocol for an Integrated Services Packet Network with Mobile Hosts. In Proceedings of ACTS Mobile Summit98, June 1998.

Fankhauser G, Hadjiefthymiades S, Nikaein N, Stacey L, RSVP Support for Mobile IP version 6 in Wireless Environments, draft-fhns-rsvp-support-inmipv6-00.txt, Internet-Draft, November 1998.

RFC 2212 Specification of Guaranteed Quality of Service, Shenker S,Partridge C, Guerin R, September 1997.

Shengming Jiang, Tsang DHK, Bo Li An enhanced distributed call admission control for wireless systems, Proceedings of 3rd IEEE Symposium on Computers and Communications, 1998, IEEE Computing Society, pp. 695–699.

Mahadevan I, Sivalingam KM, An experimental architecture for providing QoS guarentees in mobile networks using RSVP, Proceedings of the Ninth International Symposium on Personal, Indoor, and Mobile Radio Communications 1998, IEEE, Vol. 1, pp. 50–54.

Terzis A, et al., A simple QoS Signaling protocol for mobile hosts in the integrated services Internet. Proceedings of INFOCOM99: Conference on Computer Communications, March 1999, IEEE.

Mahadevan I, Sivalingam KM, Quality of Service architectures for wireless networks: IntServ and DiffServ models, Proceedings of the 1999 International Symposium on Parallel Architecture, Algorithms and Networks, IEEE Computing Society, pp. 420–425.

RFC 3002 Overview of 2000 IAB Wireless Internetworking Workshop, Mitzel D, December 2000.

Tanenbaum A, Computer Networks, Prentice-Hall, Englewood Cliffs, NJ, ISBN 0-13-394248.

RFC 2581 TCP Congestion Control, Allman M, April 1999.

RFC 2757 Long Thin Networks, Montenegro G et al., 2000.

U2010, D4.4.1 Report of concept of Sensor Monitoring System via IPv6_technology, Project no. 035003 - Ubiquitous IP-centric Government & Enterprise Next Generation Networks Vision 2010

U2010, D4.3.2 Prototype of Fire Service Solution, Project no. 035003 - Ubiquitous IP-centric Government & Enterprise Next Generation Networks Vision 2010

Real-Time Multi-user Transcoding for Push to Talk Over Cellular; Stephane Coulumbe

A Study on Session Setup for Group Communications in Push-to-talk over Cellular Using Rich Presence; Lan Wang, Daqing Gu

Push-to-talk over Cellular (PoC); Architecture; PoC Release 2.0

IMS Basics, Standards Update and Future Challenges in Face of Converged Internet/Telecommunications; Thomas Magedanz, Niklas Blum

Motorola Push-To-Talk over Cellular Consortium Phase 2 Specifications and Documentation; UE Provisioning V2.0.7 (2004-06)Asdas

Motorola Push-To-Talk over Cellular Consortium Phase 2 Specifications and Documentation; UE Provisioning V2.0.7 (2004-06)

IMS Basics, Standards Update and Future Challenges in Face of Converged Internet/Telecommunications; Thomas Magedanz, Niklas Blum

Critical Issues for QoS Management and Provisioning in The IP Multimedia Subsystems; Richard Good, Fabricio Carvalho de Gouveia, Shengyao Chen, Neco Ventura, Thomas Magedanz

Performance Measurment, Evaluation and Analysis of Push-to-Talk in 3G Networks; Wei-Peng Chen, Steven Licking, Takashi Ohno, Satoshi Okuyama, Takeo Hamada

Performance Measurment, Evaluation and Analysis of Push-to-Talk in 3G Networks; Wei-Peng Chen, Steven Licking, Takashi Ohno, Satoshi Okuyama, Takeo Hamada

Performance Measurment, Evaluation and Analysis of Push-to-Talk in 3G Networks; Wei-Peng Chen, Steven Licking, Takashi Ohno, Satoshi Okuyama, Takeo Hamada

Performance Measurment, Evaluation and Analysis of Push-to-Talk in 3G Networks; Wei-Peng Chen, Steven Licking, Takashi Ohno, Satoshi Okuyama, Takeo Hamada

Performance Measurment, Evaluation and Analysis of Push-to-Talk in 3G Networks; Wei-Peng Chen, Steven Licking, Takashi Ohno, Satoshi Okuyama, Takeo Hamada

Performance Measurment, Evaluation and Analysis of Push-to-Talk in 3G Networks; Wei-Peng Chen, Steven Licking, Takashi Ohno, Satoshi Okuyama, Takeo Hamada

Cisco advertising material

Global IPv6 Submit in China 12 April 2007

www.ipv6style.jp

Nortel advertising material

Nextel advertising material

10. Annex 1 Run Out Of IPv4 Report

Annex_1_Run out_of_ IPv4_ report

11. Annex 2 IPv6 READY Test Specification Management

Because of size of the document we added this annex as independent file. Click on the icon to open the whole document.

Annex_2_IPv6_READY_Test_Specficatior