TECHNISCHE UNIVERSITÄT WIEN

DISSERTATION

Mobility and Quality-of-Service in Global Broadband Communication Networks

Ausgeführt zum Zwecke der Erlangung des akademischen Grades eines Doktors der technischen Wissenschaften unter der Leitung von

o. Univ. Prof. Dr. Harmen R. van As
Institut für Breitbandkommunikation

Eingereicht an der
Technischen Universität Wien
Fakultät für Elektrotechnik und Informationstechnik

Vorgelegt von
Salem Lepaja, Dipl. Ing.
Mat.-Nr. E9726506

Wien, im März 2005

Kurzfassung

Ein wesentlicher Faktor der zukünftigen breitbandigen Telekommunikationsnetze, sowohl in der Mobilfunk- und Festnetztechnologie, wird die Bereitstellung von Dienstleistungsgüte (Quality-of-Service) zur Unterstützung von Echtzeitdiensten sein. Diese Arbeit untersucht drei verschiedene Aspekte der Dienstleistungsgüte in breitbandigen Mobilfunknetzen: Zugangskotrolle (Medium Access Control), reibungsfreies Übergabe-Management (handover) und Signalisierung bezüglich der Dienstleistungsgüte in einer mobilen Internet Umgebung. Bezüglich der Zugangskontrolle werden jene TDMA-basierten Protokolle untersucht die in terrestrischen Funknetzen, Satellitennetzen und lokalen Funknetzen Anwendung finden. Ein neues TDMA-basiertes Zugangskotrollprotokoll für Satellitennetze das Echtzeit und Nichtechtzeit-Dienste effizient unterstützt wird vorgeschlagen und seine Leistungsfähigkeit in Bezug auf Zugangsverzögerung und Durchsatz bewertet und mit einem Referenzprotokoll verglichen. Bezüglich des Übergabemanagements in Mobilfunknetzen wird ein offenes Problem in der Bereitstellung von IP-Diensten zu mobilen Anwendern angesprochen. Das heißt, die Heterogenität der Netze und Technologien stellt für jeden Übergabemechanismus eine Herausforderung dar, um während Bewegungen der Anwender innerhalb und zwischen Netzen eine Kontinuität der Dienste aufrecht zu erhalten. In einem Teil der Arbeit werden zwei MIPv6-basierte Übergabeprotokolle vorgeschlagen und für die Anwendung zur inter-terrestrischen Satellitenverbindung bzw. für Intra-Satellitenverbindungen bewertet. Als dritter Forschungsaspekt werden Architekturen für vermaschte Zugangsnetze in Bezug auf die Erfordernisse der Internet-Betreiber Mobilfunkanwendern dieselben Echtzeitdienste zur Verfügung zustellen wie den Internet-Anwendern im Festnetz betrachtet. Dafür werden neue Rahmenbedingungen für die Bereitstellung einer Ende-zu-Ende Dienstgüte zu Mobilfunkanwender vorgeschlagen. Teilweise vermaschte Zugangsnetze und Kernnetze in der MPLS Technologie werden hier mitbetrachtet. Die resultierende Ende-zu-Ende Netzarchitektur wird untersucht und die Idee eines vermaschten Zugangsnetzes wird ausgearbeitet. Basierend auf diese Rahmenbedingungen wird ein neues Signalisierungsprotokoll zur Bereitstellung von Dienstgüte zu Mobilfunkanwendern für ein teilvermaschtes Zugangsnetz vorgestellt und seine Leistungsfähigkeit bewertet und verglichen anhand von zwei Referenzprotokollen.

Abstract

Quality-of-Service (QoS) provisioning to both fixed and mobile users is an essential issue in future broadband communication networks, aiming to support real-time broadband services. This thesis investigates three different aspects of QoS provisioning to mobile users in global mobile broadband communication networks: Medium Access Control (MAC), seamless handover management, and QoS signaling in a mobile Internet environment. Considering the MAC aspect, protocols based on time division multiple access (TDMA), aimed at terrestrial mobile networks, satellite networks, and wireless local area networks are analyzed. A new TDMA based MAC protocol for broadband satellite networks that efficiently supports real-time and non-real-time services is proposed and its performance in terms of access delay and throughput are evaluated and compared with a reference protocol. Considering handover management in wireless networks a current problem of delivering IP services to mobile users is addressed. That is, the diversity of networks and technologies impose a challenge to any handover mechanism to maintain service continuity while mobile users move within the same mobile network or between networks/systems operated by different operators, which might even be in a different country. In one part of the thesis, two handover protocols based on MIPv6 are proposed and evaluated for application at inter terrestrial-satellite networks and intra-satellite networks, respectively. As a third novelty, architectures for meshed access networks are considered in regard to the requirements of Internet providers to deliver the same real-time broadband services to mobile users as to wired Internet user. Therefore, a new framework for end-to-end QoS provisioning to mobile users applications is proposed, including both partially-meshed access networks and core networks for the "multi protocol label switching" technology. The resulting end-to-end network architecture is investigated and the idea of a meshed access network is elaborated. Based on that framework a new signaling protocol for QoS provisioning to mobile users for partially-meshed access network architecture is introduced and its performance is evaluated compared with two reference protocols.

Acknowledgement

There is a long list of people whom I should thank for the help and support they have given to me to achieve this precious goal. First-of-all, my thanks go to my supervisor Prof. Dr. Harmen R. van As, for the scientific, financial, and moral support he has given to me. I also would like to thank my co-adviser Prof. Dr. Árpad Scholtz for his time for reviewing this thesis and for his kindness and readiness to help me at any time. Many thanks go to my ex-colleagues from the Institute of Broadband Communications, Vienna University of Technology, Kemal Bengi, Hoang Nam Nguyen, Hoang Minh Nguyen, and Arben Lila, for the papers we produced together. I am very grateful to other two of my colleagues Jon Schuringa and Rene Donner for helping me with simulation programs. I would also like to thank my ex-students from University of Prishtina, Astrit, Driton, Idriz and Nysret, for their support from the first day when I came to Vienna and for the time we spent together. Last, but not least I would like to thank my children Agron, Atdhe, Flaka and Ideal and my wife Shpresa for their love and support.

Contents

List of Figures

List of Tables

1 Introduction

During the last decade, we have seen an exponential growth of both Internet and mobile communications. A further rapid growth of these two main communication technologies is expected over the next few years. Furthermore, trends are clearly indicating the integration of mobile communication and Internet technologies. Mobile communication networks are implementing IP technology and IP-based services whereas the Internet is moving towards supporting mobility. In a future communications and information-based society, provisioning of broadband multimedia telecommunication services to mobile and fixed users becomes a very important and essential task. Hence, a crucial and common issue for both Internet and mobile network technologies is Quality-of-Service (QoS) provisioning. QoS means that a network should provide different services to user's applications with an acceptable quality that satisfies communication requirements of each application. QoS requirements have to be satisfied everywhere in the network, that means end-to-end, and for all services that need QoS support. Therefore, QoS provisioning is an essential task of broadband communication networks that needs to be considered regarding to several aspects such as media access Control (MAC), handover management, and QoS signaling in mobile Internet environment. Considering the scarce wireless medium, MAC protocols have an essential role in mobile communication networks. Hence, the design of flexible and efficient Medium Access Contol (MAC) protocols is a crucial starting point in providing QoS in mobile networks. The goal of third and next generation mobile networks is to provide service continuity with acceptable QoS while users move between different networks and systems. Handover might cause QoS degradation or even connection drop, when QoS is under the acceptable limit, due to lack of resources in a new network. Currently, the IP services for mobile users are delivered over a variety of networks and technologies, including Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), satellite networks, and WLAN. However, seamless mobility among these different access networks cannot take place, because mobility management in each of them is handled almost completely by the underlaying network. To overcome this problem, Mobile IPv4 and Mobile IPv6 were developed for handling inter and intra network mobility. Since the Mobile IP (MIP) protocol is not suitable for intra network mobility, new protocols based on MIP are being developed. Hence, handover management based on Mobile IP is an essential mechanism to enable users to communicate continuously while moving within a network or between different networks. However, the existing protocols have to be adapted to the specific requirements of each wireless access network. In the mobile Internet environment, mobile users require the same real-time broadband services as fixed Internet users. These services require both QoS and mobility support. Since existing Internet QoS mechanisms do not consider mobile environments and on the other hand, Mobile IP does not provide QoS, several new solutions addressing QoS provision to mobile users have been proposed. However, none of them considers meshed access network architectures, which are important for communication in local communities in general and for efficient local mobility management in particular. Hence, providing various types of services with different QoS requirements (while considering different mobile communication environments in order to achieve continuous and global communication) is still an open issue that presents a great challenge for researchers and network designers in the next few years. Motivated by these open issues, QoS provisioning to mobile users is investigated in this thesis from different aspects.

1.1 Objectives of the Thesis

The objective of this thesis is to investigate QoS provisioning in global mobile broadband communication networks from different aspects: media access control, seamless mobility management, and QoS signalling in the mobile Internet environment.

1.2 Research Methodology

The research methodology comprises an intensive study of the state-of-the-art of each research discipline and software simulation to evaluate the performance of some new proposals.

1.3 Contributions of the Thesis

The main contributions of the thesis are as follows:

- A novel MAC protocol for mobile satellite networks to accommodate real-time and non real-time applications was designed. The performance of this protocol is evaluated by software simulations and compared with a reference protocol.
- Two handover protocols for interworking between inter terrestrial-satellite networks and intra-satellite network are proposed and their performance is evaluated by software simulations.
- A new framework for end-to-end QoS provisioning to mobile users consisting of partially meshed mobile access network and MPLS core network is proposed and investigated.
- A new signaling protocol for QoS provisioning to mobile users is designed and its performance is evaluated and compared with two reference protocols. Particularly attention is given to partially meshed access networks.
- The thesis also contains an original view concerning the trends of mobile communication networks and their interaction with the Internet. Also some basic concepts are redefined or clarified such as services, applications, and Quality-of-Service (QoS).

1.4 Chapter Overview

This Ph.D. thesis contains seven chapters.

Chapter 1 shows the motivation of research, the objective of the thesis, the research methodology, the contribution of the thesis, and provides an overview of the chapters.

Chapter 2 provides an overview of the wide range of communication networks and serves as a foundation for the following chapters. The chapter first introduces a classification and the basic concepts of communication networks such as: applications, services, Quality-of-Service (QoS), and the OSI reference model. Then concepts of ISDN networks and BISDN/ATM are presented. The main building blocks of the ATM networks and the protocol reference model are covered. Next, the basic elements of the Internet are introduced. Main protocols of the application layer, the transport layer, and the Internet layer of the TCP/IP suite are described. Furthermore, addressing issues of IPv4 and IPv6 as well as transition strategies between IPv4 and IPv6 are covered. This chapter then presents basics of mobile communication networks of the first, second, and third generation. Network architecture, communication protocols and services of GSM, GPRS, and UMTS are covered. In addition, satellite and wireless LAN networks as an important segment of mobile communication systems are discussed.

Chapter 3 presents MAC protocols for wireless communication networks. First, the most common classification of TDMA-based MAC protocols for wireless networks is introduced. Then, the most representative protocols for wireless terrestrial and satellite networks are covered. Next, a new TDMA-based Random-Reservation MAC protocol to support QoS in broadband satellite communication networks is presented with performance evaluations. The chapter concludes with discussion of the two basic medium access mechanisms for IEEE 802.11 WLAN networks: Distributed Coordination Function (DCF) and the Point Coordination Function (PCF).

Chapter 4 covers Mobility Management issues in different mobile communication networks. First, the Mobility Management concept and its components are introduced. Then, the description of the mobility management in 2G-GSM networks and in UMTS networks specified by 3GPP 99 are presented. This chapter then introduces the mobility management in All-IP networks, including MIPv4, MIPv6, and several other protocols as extensions to MIPv6, such as HMIPv6, RegReg6, and Fast Handover. The chapter closes with the discussion of the mobility management in IP based LEO satellite networks. Two innovative handover protocols, inter terrestrial- satellite network and intra-satellite network handover management protocols and their performance are presented.

Chapter 5 provides an overview of the QoS mechanisms in broadband communication networks. First, the QoS mechanisms in the Internet, the Integrated Services architecture, the RSVP protocol, the Differentiated Services architecture and the MPLS mechanisms are presented. Next a brief description of the QoS in UMTS networks is given, explaining UMTS QoS architecture and QoS classes. The chapter concludes with the discussion of IEEE 802.11e standard enhancements to provide QoS in WLANs.

Chapter 6 discusses issues of QoS provisioning in the mobile Internet environment. The chapter begins with the discussion of some of the proposed solutions. Approaches such as Resource Reservation in Advance, Coupling of Micromobility and QoS, and RSVP Interworking with Mobile IP are covered. Next, a new proposed Framework for End-to-end QoS provisioning to mobile users applications is introduced, including partially meshed access networks. The end-to-end network architecture and the idea of meshed access network are elaborated. In addition to this a new signalling protocol for QoS provisioning for partially meshed access network architecture and performance evaluation results are presented.

Chapter 7 provides the conclusion of the presented work in the thesis and outlines further investigations.

2 Broadband Communication Networks

Communication networks are very complex and very expensive systems, which are designed with the aim to fulfill user needs and requirements for communication. The main task of the network is to offer to users different services with acceptable quality in cost-effective manner. User needs today are met with different communication networks, employing a wide variety of technologies and offered services. There are great differences between countries concerning the network technology they use and the services that are provided to users. However, most European countries have a telecommunication infrastructure that contains the following network technology:

- PSTN (Public Switched Telephone Network),
- CSPDN (Circuit Switched Public Data Network),
- PSPDN (Packet Switched Public Data Network),
- N-ISDN (Narrowband Integrated Services Digital Network),
- Broadband-ISDN/Asynchronous Transfer Mode (ATM), with optical fiber infrastructure.
- GSM (Global System for Mobile Communications),
- DECT (Digital European Cordless Telephone),
- Internet,
- WLAN (Wireless Local area Networks),
- Satellite Networks.

In addition to the above listed networks, there are new networks technologies available to the users in the very near future like:

- UMTS (Universal Mobile Telecommunication Networks),
- Broadband LEO Satellite networks,
- Mobile IP technology.

It is obvious, that coexistence of these networks is necessary due to large investments and due to the fact that most of these networks still have a considerable potential for growth in traffic, new subscribers and high revenues. There is no doubt that Internet and mobile communications are the two fastest grown network technologies in the last decade. The IPv4 based Internet technology has been proven as being very successful in internetworking of different networks and making a global communication network. Hence, the Internet became the largest worldwide network providing a wide range of narrowband and broadband services to users. Today Internet services are accessible from everywhere: homes, offices, schools, hospitals, hotels, airports and while we are moving. Although, still in the experimental phase, Internet services are also provided to passengers on planes, trains and buses. However, the ongoing explosive growth of the number of Internet users has exposed insufficiencies in the very successfully deployed worldwide IPv4. The first and main problem to be recognized was IPv4 address exhaustion. The Internet Engineering Task Force (IETF) recognized this problem around 1990 and solicited a solution. This new solution is called Internet Protocol version 6 (IPv6). In addition to almost unlimited address space the designers of IPv6 added other new essential features and enhancements to IPv4, including enhanced support for QoS and embedded support for mobile networks.

One of the driving forces for the wide spread adoption of IPv6 is its use in evolving 3G mobile networks. However, the deployment of IPv6 will be a gradual process lasting many years. In fact, IPv6 deployment is already delaying, first of all due to the lack of end user demand because the most significant obstacle to the success of IPv6 is the transition of existing applications. Parallel to the Internet, mobile communications has seen an exponential growth. In several countries, the number of mobile users exceeds the number of fixed users. In general, the terrestrial mobile communication systems development is grouped into different generations. The first generation (1G) mobile systems are based on analogue network technology and the emphasis was on speech service. The second-generation (2G) mobile communication systems are characterized by the employment of "circuit switched" digital technology. The most successful 2G systems is European GSM, providing data services up to 14.4 kbit/s, in addition to voice services. However, such data rates and the "circuit switched" technology are obstacles for today's Internet services. Hence, the more advanced second and a half generation (2,5G) and third generation (3G) systems were designed. The General Packet Radio Service (GPRS) and other 2,5G mobile communication systems are considered as interim technologies between 2G and 3G systems. GPRS is an extension to GSM but with many enhancements over the GSM system. These enhancements are mainly based on the use of packet switched technology and offering higher data rates than GSM. The 3G mobile systems have been developed to meet further increasing demands for new mobile multimedia services and high-speed data communication in the current environment of the Internet. At present, the European UMTS and other 3G mobile communication systems are just beginning to be deployed, while research on the next generation of mobile communications, the fourth generation (4G) wireless systems, begins to pave the way for the future. Right now, it is hard to say where the third generation ends and the fourth generation starts. However, it is for sure that the final goal for mobile networks evolution, including 3G systems, is IPv6 technology. However, cellular operators are likely to undertake the migration to a full IPv6 solution on Public Land Mobile Networks (PLMN) only beyond third-generation mobile networks.

Other important mobile communication systems are satellite and WLAN networks. Satellite networks are considered a feasible solution to provide broadband as well as narrowband services to users in remote areas, where there is no communication infrastructure, or as complementary networks to terrestrial mobile networks. WLAN technology currently presents a hot topic in the wireless Internet market for providing broadband services to slow mobile users. WLAN will certainly be a key part of future wireless Internet first-of-all due to the high bandwidth-to-cost ratio. It is expected that in the next few years cheap WLAN combined with GPRS will dominate in mobile communications. WLAN will be used by slow mobile users to access broadband Internet services whereas GPRS will be used by fast mobile users for slower data rate services.

In this chapter an overview of the fixed broadband and mobile communication networks will be presented.

2.1 Basic Concepts and Classification of Communication Networks

In the following subsections, some basic concepts and a classification of communication networks will be introduced.

2.1.1 Services and Applications

Services and applications are two fundamental concepts in communication networks that are very often used interchangeably. However, there is a difference between them, as we shall clar-

ify next. A service is what the network offers to the user and what the user pays for, whereas an application is the means of the user to use a service. Actually, the only point of having communication networks is to provide services to the users applications. In fact, users only buy services that add value to their lives and the technology itself that enables service provisioning is less important. This is a concern of the network operators that offer infrastructure to support certain services, whereas service providers use the network infrastructure to offer services to the users. Hence, looking from the network perspective we should use the term services while from user perspective we should use the term applications.

2.1.2 Quality-of-Service

Quality-of-Service (QoS) is an essential issue in communication networks that aim to provide real-time services to user's applications. However, this essential concept has several different definitions. Hence, in order to explain the concept of QoS we will define it from both user and network perspective. Applications require from the network appropriate services that will provide an acceptable quality that satisfies communication requirements. Therefore, from the user perspective QoS presents the quality of the application that a user experiences. From the network perspective QoS are those mechanisms that provide the requested services to the user's applications. These services include provisioning of the resources and appropriate handling of the applications at network nodes. Thus, networks that have the capability to differentiate different application requirements and service them adequately are featured as QoS enabled networks. The service requirements of a real-time application are represented as a set of parameters such as bandwidth, delay, jitter, packet loss, and others, which are recognized as QoS parameters.

2.1.3 OSI Reference Model

Networks communicate with each other by using well-defined procedures called protocols. However, many of the networks were built using proprietary systems implementing different hardware and protocols. As a result, these networks were incompatible and unable to communicate with each other. To alleviate this serious problem for global communication, the International Organization for Standardization (ISO) created a network model that would help vendors create networks that would be compatible and communicate with other networks. This model is known by the name of Open System for Interconnection (OSI), and is documented in ITU Recommendation X.2000. The basic idea of the OSI Reference Model is to break down complex communications processes into smaller and simpler tasks grouped into layers. The OSI reference model is organized in seven independent layers to define all communication functions. The general rules of the OSI Reference Model are:

- OSI defines only the functions of each layer and not the way a certain layer is implemented. Each layer can be implemented in many different ways. A specific layer implementation presents a protocol that belongs to that layer.
- Two layers that lie above each other work independently. Each layer receives a service from the layer immediately below it and provides a service to the layer immediately above it. The lower layer does not care about the content of the received information.
- Each layer communicates directly only with the layers immediately below and above itself and indirectly with its peer layer at the remote end.

The OSI reference model, shown in Figure 2-1, defines the following seven layers.

Layer 7: Application Layer
The application layer is closest to the user and it provides network services only to the user's applications by interfacing between applications and the communication process.

Layer 6: Presentation Layer
The presentation layer ensures that the information that the application layer of one host sends out is readable by the application layer of another host. If necessary, the presentation layer translates between multiple data formats by using a common format.

Layer 5: Session Layer
The session layer was assigned for global synchronization purposes. It establishes, manages, and terminates sessions between two communicating hosts. Part of the synchronization is the ability to determine which information needs to be sent, when, and by whom.

Layer 4: Transport Layer
The transport layer segments data from the sending host into packets and reassembles the packets into a data stream on the receiving host. Furthermore, this layer performs end-to-end data control. The boundary between the transport layer and the session layer can be considered as the boundary between application protocols and network protocols.

Layer 3: Network Layer
The network layer provides connectivity and path selection between two hosts that may be located on geographically separated networks. All the information necessary to route a data packet from the source to destined host is the responsibility of the network layer. Every network node has to analyze and possibly modify the network layer information.

Layer 2: Data Link Layer
The data link layer provides reliable transmission of data across a physical link. The data are combined into frames and then handed to the physical layer. The data link layer information is relevant only between two adjacent network nodes. In general, the data link layer is concerned with physical addressing, network topology, network access, error notification, ordered delivery of frames, and flow control. Furthermore, for particular networks, the data link layer is divided into Logical Link Control (LLC) and Media Access Control (MAC) sublayers.

Layer 1: Physical Layer
The physical layer is responsible for the actual transmission of the data received from data link layer without additional verification. Physical layer specifications define such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, and physical connectors.

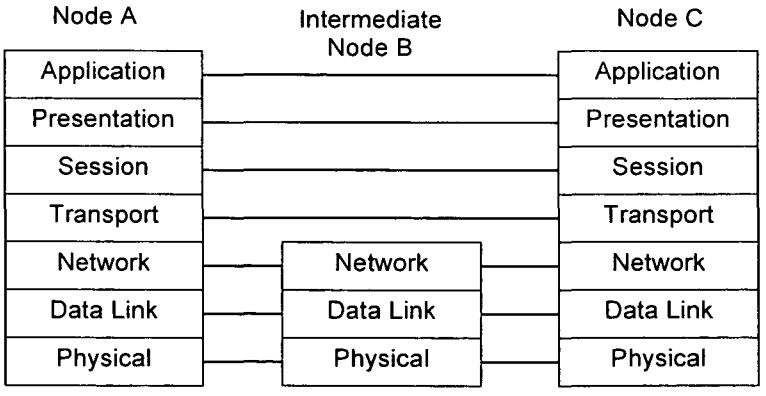


Figure 2-1: OSI Reference Model

Not all seven layers of the OSI reference model need to be implemented in all nodes of the communication path. If a communication process involves more than two network nodes, the intermediate network node needs only to provide the functionality of Layers 1 through 3. As Figure 2-1 shows, network Node-B is equipped only with Layers 1, 2, and 3. Layers 4 through 7 are required at the endpoints of a connection only. Furthermore, protocols used for Layers 1

through 3 on the interface between A and B are not necessarily the same as those used on the interface between B and C.

2.1.4 Classification of the Networks

There are several ways to classify communication networks. The two most common ones are based on the coverage area of the communication environment and on the transmission media that user is connected to the network. Based on the coverage area communication networks are classified into: Local Area Networks (LAN), Metropolitan Area Networks (MAN), and Wide Area Networks (WAN). According to the connecting media, networks are classified into fixed (wired) networks and mobile (wireless) networks. We will use the terms fixed and wired interchangeably as well as the terms mobile and wireless. Note that different wireless networks offer a different scale of mobility to users. Another classification of the networks is based on the bandwidth or bitrate that is provided to network services. Based on this parameter networks are grouped into broadband and narrowband networks. Although there is not an "official" value, networks providing 2 Mbit/s and higher bandwidth values are usually considered as broadband communication networks.

2.1.5 Broadband Networks

Broadband networks are high-speed telecommunication networks intended to provide a wide range of telecommunication services. For the realization of a broadband network several network technologies can be used. The choice of a particular technology depends on different factors such as: the needs for a particular network and for the services that shall be supported, the cost of implementation, and already existing infrastructure owned by network operators. Broadband networks consist of access networks and a core or backbone network. Access networks provide the local connectivity for users, whereas the core network interconnects several access networks with a variety of established access network technologies. Furthermore, broadband technology is applied in both wired and wireless networks. Two main wired broadband backbone networks are Internet and ATM. In Wireless communications UMTS, WLAN, and LEO satellite networks (for example Teledisc), are considered as broadband networks, consisting of access networks and backbone network. In the Internet environment, each of these mobile networks can be considered as an access network connected to the Internet backbone network.

2.2 Broadband Fixed Networks

Broadband Integrated Services Digital Network (BISDN)/Asynchronous Transfer Mode (ATM) and the Internet are two main broadband backbone network technologies. However, the Internet is the largest network providing broadband capabilities, and it is believed that future broadband networks will be based mostly on IP (Internet Protocol) technology. Combination of IP and ATM is also very common, known as IP over ATM model. This architecture consists of an ATM backbone network, which interconnects IP routers. Recently the Internet Engineering Task Force (IETF) has developed a new technology named Multiprotocol Label Switching (MPLS), providing an alternative to the IP over ATM model. MPLS may be operated in a purely IP based network or in an IP over ATM network architecture. The basic principles of the MPLS technology will be introduced in Chapter 5. Broadband backbone networks have to interwork with a variety of established access network technologies. Among broadband access networks, IP based networks are dominating, since many applications are based on IP technology and new applications are also expected to be developed on IP-bases. Thus, the interworking with IP networks is an essential feature for non-IP access networks. Access networks using ATM technology were also planned. However, they were not realized, first-of-all because of economical considerations. In the following subsections first a short overview of narrowband

Integrated Services Digital Network (ISDN), as an evolution step towards BISDN/ATM, will be introduced. Then the basic concepts of BISDN/ATM and Internet will be discussed.

2.2.1 Integrated Services Digital Network - ISDN

In the early 1970s CCITT (International Telegraph and Telephone Consultative Committee) introduced the concept of Integrated Services Digital Network (ISDN). The CCITT, recommendation series I, stated that "an ISDN is a network evolved from the telephony integrated digital network that provides end-to-end digital connectivity to support a wide range of services, including voice and non-voice services, to which users have access by a limited set of standard multipurpose user-network interfaces''. According to the definition, ISDN is seen as a unique network that employs digital technology up to the end user. Furthermore, ISDN provides not only telephony, but will carry different types of traffic and offer to users a wide range of services via one interface or via a limited set of standard user-network interfaces. ISDN is based on the digitized telephone network with 64 kbit/s channel as the fundamental building block. The channel bit rate of 64 kbit/s is derived from the 3.4 kHz voice transmission requirements (8 bit sampling with frequency of 8 kHz). ISDN is intended to provide circuit switched and packet switched connections, but as this network evolved from IDN – Integrated digital telephone network, its characteristics were derived from voice traffic characteristics. The CCITT has defined two standards for physical interfaces to ISDN: the Basic Rate Interface (CCITT ISDN I.430) and the Primary Rate Interface (CCITT ISDN I.431) standards.

The Basic Rate Interface (BRI) provides two 64 kbit/s B channels and one 16 kbit/s signaling D channel. This interface is commonly referred to as 2B+D. The BRI was intended to meet needs of most individual users (residential and small offices). There are two standards defined for Primary Rate Interface (PRI). The PRI used in United States, Canada and Japan is based on 1.544 Mbit/s whereas in Europe on 2.048 Mbit/s. The channel structure for the 1.544 Mbit/s rate is 23 B channel plus one 64 kbit/s D channel (23 B+D), and for the 2.048 Mbit/s rate, 30 B channels plus one 64 kbit/s D channel. The primary rate interface also supports H channels and was intended for higher bandwidth or shared customer devices such as the Private Branch exchange (PBX) and LAN. The B channel of the PRI and BRI is the basic channel to carry user data. Two kinds of connections can be set up over a B channel: circuit switched and packet switched. The D channel serves two purposes: it carries signaling information to control circuit switched calls on associated B channels at the user interface and it may be used for packet-switched or low speed data transmission at times when no signaling information is waiting. H channels are provided for user information at higher bit rates. Two types of H channels are defined: the H0 channel that has a capacity of 384 kbit/s and H1 channels that have capacity of 1536 kbit/s for H11 channels in the USA and 1920 kbit/s for H12 channels in Europe. H channels are combined with appropriate signaling channels D.

2.2.2 Broadband ISDN

User's demands for new broadband services, especially video-based services and the connection of LANs, requiring data rates beyond those that can be delivered by ISDN, resulted in the definition of the Broadband ISDN network. ITU-T recommendation I.121 presents an overview of B-ISDN capabilities. The general definition of the B-ISDN in this recommendation is as follows: "B-ISDN supports switched, semi-permanent and permanent, point-to-point and point-to-multipoint connections and provides on-demand, reserved and permanent services. Connections in B-ISDN support both circuit mode and packet mode services of a mono-and /multimedia and of connectionless or connection-oriented nature and in a bi-directional or unidirectional configuration".

Hence, B-ISDN is conceived as a universal network supporting different kinds of applications and user categories. The first concrete idea of B- ISDN was simply to:

- Add new high-speed channels to the existing channel spectrum.
- Define new broadband user-network interfaces.
- Rely on existing 64 kbit/s ISDN protocols and principles and enhance them when absolutely unavoidable.

B-ISDN thus includes 64 kbit/s ISDN capabilities and in addition, it supports applications requiring bit rates above 1.5 Mbit/s or 2 Mbit/s. So at the early stage of the B-ISDN development, channel bit rates of 32-34 Mbit/s, round 45 Mbit/s and 135-139 Mbit/s were foreseen. According to the ITU-T, Asynchronous Transfer Mode (ATM) technology is considered the ground on which B-ISDN is to be built. Hence, in the next sections a short overview of ATM B-ISDN network will be given.

2.2.3 ATM Network

Asynchronous Transfer Mode (ATM) is a cell based switching and multiplexing technology defined by protocols standardized by the ITU-T, ANSI, ETSI, and the ATM Forum. As specified in the ITU-T, Recommendation I.121, ATM was agreed as the target transfer mode solution for implementing a B-ISDN. The term transfer comprises both transmission and switching aspects, so a transfer mode is a specific way of transmitting and switching information in a network. In ATM, all information to be transferred is packed into fixed-size cells. ATM network is a connection–oriented technique, which combines the advantageous features of both circuit and packet oriented techniques. Because ATM is a connection-oriented technique, a path has to be established between the users before information can be exchanged. This is done by the connection set-up procedure at the start and by the clear-down procedure at the end of communication.

2.2.3.1 ATM Cell

The basic data unit in ATM is the cell. ATM standards define the fixed-size cell with a length of 53 bytes comprised of a 5 bytes header and a 48-bytes payload as shown in Figure 2-2. The payload field is for user data, whereas the header field carries controlling information such as the identification of cells by means of labels. The payload size of 48-bytes is chosen as a compromise between efficiency and delay. Better efficiency occurs at large cell size at the expense of the increase packetization delay. Thus, the ITU-T adopted the fixed length 48-bytes cell payload as a compromise between a long cell sizes for time-insensitive traffic (64 bytes) and smaller cell sizes for time-sensitive traffic (32 bytes).

Two cell formats, shown in Figure 2-2, have been specified, one for the User-Network Interface (UNI) and the other for the Network-Node Interface (NNI). The UNI format is used between the user installation and the first ATM exchange as well as within the users own network. The NNI format is used between the ATM exchanges in the trunk network. All information is switched and multiplexed in an ATM network in these fixed-length cells. The cell header identifies the destination, cell type, and priority. The virtual path identifier (VPI) and Virtual Channel Identifier (VCI) are of local significance only and identify the destination. The Generic Flow Control (GFC) field allows a multiplexer to control the rate of an ATM terminal. The Payload Type (PT) indicates whether the cell contains user data, signaling data, or maintenance information. The Cell Loss Priority (CLP) bit indicates the relative priority of the cell. The cell Header Error Check (HEC) detects and corrects errors in the header. The payload field is passed through the network intact, with no error checking or correction. ATM relies on higher layer protocols to perform error checking and correction on the payload.

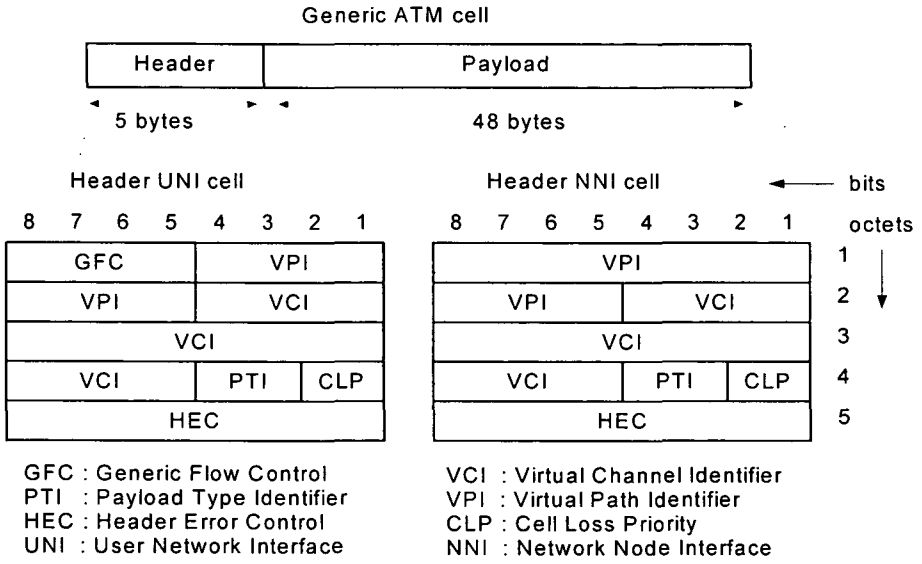


Figure 2-2: ATM Cell Format

2.2.3.2 ATM Networking Concepts

Three major networking concepts in ATM are: Transmission Path (TP), Virtual Path (VP) link, and Virtual Channel (VC) link. A transmission path contains one or more virtual paths, while each virtual path contains one or more virtual channels, as shown in Figure 2-3. Each virtual channel and virtual path is identified by a Virtual Channel Identity (VCI) label and a Virtual Path Identity (VPI) label, respectively. VPIs and VCIs are used to route cells through the network, and they must have unique values on a specific transmission path.

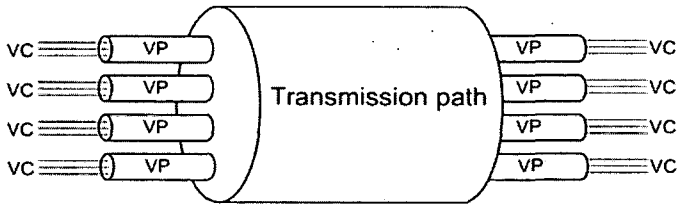


Figure 2-3: Physical Transmission Path, Virtual Paths (VP) and Virtual Channel (VC)

A series of connections of virtual channel links constitutes the virtual channel connection. Devices that perform VC connections are called VC switches because of the analogy with telephone switches. Each VC switching node contains routing translation tables, which provide VCI translation information for every cell entering a switch. The routing information is entered during the connection set-up and remains constant for the duration of a connection. Within a virtual channel link the VCI has a particular value, but it will change from link to link within a virtual channel connection. Virtual path links are also concatenated to form a virtual path connection (VPC) that extends between two VPC endpoints or, in the case of point-to-multipoint arrangements, between more than two VPC endpoints. ATM devices, which connect VPs, are commonly called VP cross-connects, in analogy with the transmission network. Also each cross-connect node contains routing translation tables, which provide VPI translation for each cell going into the cross-connect. However, information about individual virtual channels within the virtual path is not required, as all the virtual channels of that virtual path follow the same route as the virtual path. Figure 2-4, illustrates the concept of virtual path connection and virtual channel connection.

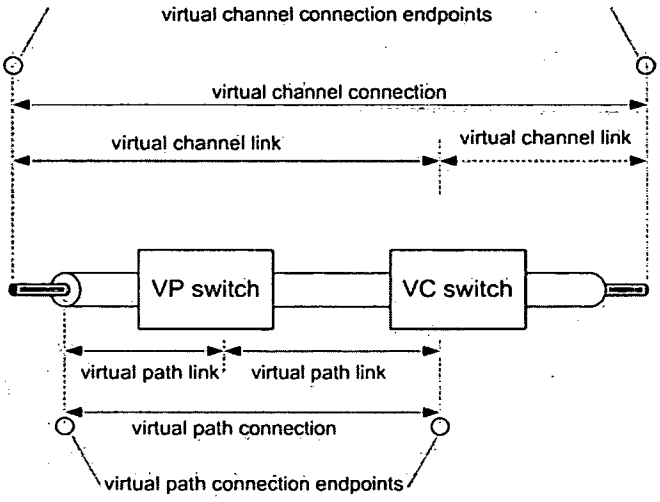


Figure 2-4: Virtual Channel and Virtual Path Connection

Basically, switching can be performed on the transmission path, virtual path, or virtual circuit level. In Figure 2-5 [McD95] an example for an ATM connection with single transmission paths between switches, is illustrated. At the ATM user-network interface, the input device to the Switch 1 provides a service channel over Virtual Channel 6 (VCI 6) of Virtual Path 1 (VP 1). Switch 1 then maps incoming VCI 6 to outgoing VCI 15, and the incoming VP 1 to outgoing VPI 12. Thus, on VPI 12 switch 2 (a VC switch) specifically operates on VCI 15. This channel is then routed fro switch 2 to switch 3 over VPI 16 and VCI 8. Finally, switch 3 translates VPI 16 into VPI 2, and VCI 8 on VP 16 to VCI 11 on VPI 2 at the destination UNI.

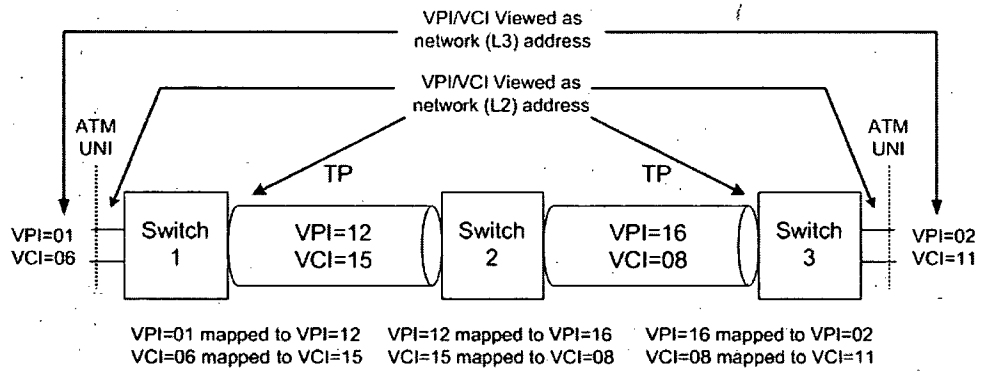


Figure 2-5: VPI and VCI Usage on Link and End-to-End

2.2.3.3 ATM Protocol Reference Model

In a similar way to the familiar OSI 7-layer model, the ATM also has a layered protocol reference model shown in Figure 2-6, which consists of a user plane, a control plane and a management plane. The user plane provides for the transfer of user information and it has a layered structure. All associated mechanisms, like flow control and recovery from errors, are included. The control plane is responsible for the call control and connection control functions. These are all signaling functions, which are necessary to set up, supervise and release a call or connection. The management plane consists of layered layer management and plane management. Layer management performs the management functions related to resources and parameters residing in its protocol entities and it also handles the specific Operation-and-Maintenance (OAM) information flows for each layer. All the management functions that relate to the whole system are located in the management plane, which is responsible for providing coordination between all planes. No layered structure is used within this plane.

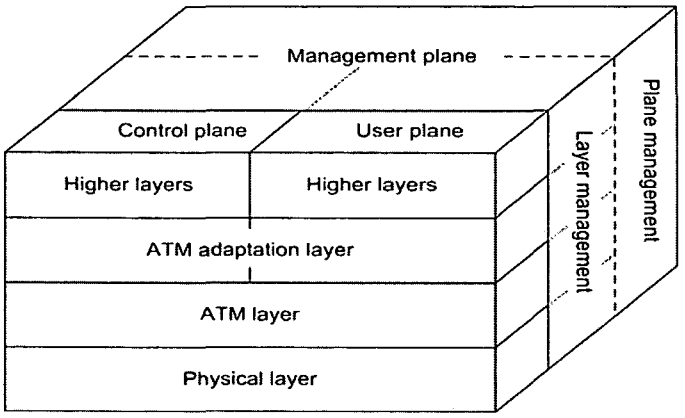


Figure 2-6: ATM Network Protocol Reference Model

2.2.3.4 ATM Services and Applications

ATM is designed for high-performance multimedia networking to support a wide range of services. According to the ITU-T Recommendation I.211, ATM services are grouped into interactive and distributed services. Interactive services comprise conversational, messaging and retrieval services. Conversational services enable the mutual exchange of data, whole documents, pictures, and sounds. Examples of this category of services are videotelephony, videoconferencing, high-volume file transfer, high-resolution image transfer as well as other services. Messaging services include mailbox services for transfer of sound, picture and documents. Retrieval services are used for example, to obtain video films on demand or to access a remote software library. Distribution services can be split into services with user-individual presentation control and without user-individual presentation control. The former category is used for remote education and training, news retrieval, and telesoftware. Examples of the later category are: electronic publishing and TV program distribution with normal and enhanced picture quality. Most of the above mentioned services require wideband networking. Hence, ATM B-ISDN network rates have initially been chosen as 622 Mbit/s and 155 Mbit/s, with the possibility of reaching 2.4 Gbit/s and above. An ATM based 155 Mbit/s UNI would handle 367,000 cells per second in either direction of the interface.

2.2.4 Internet Network

The Internet network is the global interconnected system of computers that provides a wide range of services and information to the users. The current Internet has its roots back in 1969 when the U.S. Defense Advanced Research Project Agency (DARPA) began development of a packet switched network. The first experimental data network named ARPANET was demonstrated in 1972. The ARPANET continued to grow, and in 1983, the introduction of the Transmission Control Protocol/Internet Protocol (TCP/IP) replaced the earlier Interface Message Processor (IMP) protocol. Also in 1983, the ARPANET was split into a military network and a nonmilitary research network that was the origin of the Internet. This was a turning point for the development of the Internet technology. Since then the Internet began to grow and spread with big steps. However, it was not widely acceptable until the World Wide Web (WWW) service appeared that IP networking technology and services would be the global trend and the goal of future communication networks. The WWW has fundamentally changed the Internet and made it what it is today: the world's largest public network offering a wide range of services and global communication to users. Internet applications are developed and used in every segment of our live: education, scientific research, engineering, medicine, arts, entertainment, and others. Today a wide range of Internet services, including multimedia, are accessible from almost everywhere: homes, offices, schools, hospitals, hotels, airports and while we are moving. Although still in the experimental phase, Internet services are also provided to passengers on planes,

trains, and buses. Thus, the Internet is making a strong impact on the way we live, work, and play. In the following subsections some of the most popular protocols of the TCP/IP suite will be presented. The main focus will be on IP protocol, including both versions IPv4 and IPv6, as well as the transition strategies from IPv4 to IPv6.

2.2.4.1 TCP/IP Suite

The Internet network is based on the wide set of protocols called the TCP/IP protocol suite, after the two most important protocols: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were also the first two defined. The function of the TCP/IP suite is the transfer of information from one network device to another. The TCP/IP suite is organized in layered architecture like the OSI model. However, different to the OSI model, TCP/IP has only four layers, as shown in Figure 2-7. In the lower layers, the TCP/IP suite closely maps the OSI reference model, and it supports all standard physical layer and data link layer protocols. The Internet layer corresponds to the OSI network layer. The TCP/IP transport layer corresponds to the OSI transport layer. Session and presentation layers of the OSI model are not considered in TCP/IP as special layers. However, their functions are included in TCP/IP application layer. Protocols of the OSI application layer are more complex and offer more functionality than those of the application layer of TCP/IP.

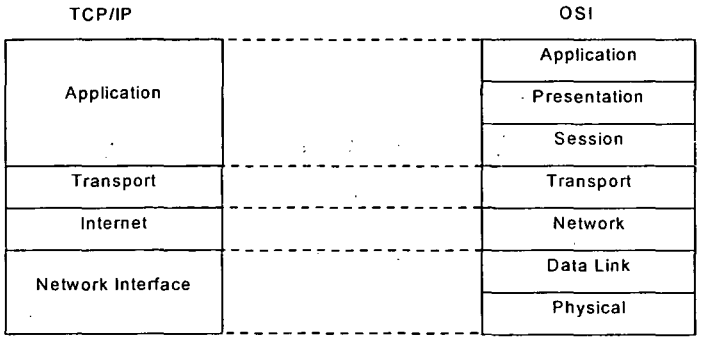


Figure 2-7: Relation TCP/IP - OSI Reference Model

The Internet TCP/IP model was produced as the solution to a practical engineering problem. The OSI model, on the other hand, was a more theoretical approach, and was also produced at an earlier stage in the evolution of networks. Therefore, the OSI model is easier to understand, but the TCP/IP model is the one actually in use. It is helpful to have an understanding of the OSI model before learning TCP/IP, as the same principles apply, but they are easier to understand in the OSI model. There is a very wide range of Internet protocols standardized by the Internet standards body called the Internet Engineering Task Force (IETF). Figure 2-8 illustrates the layered protocol architecture of the Internet.

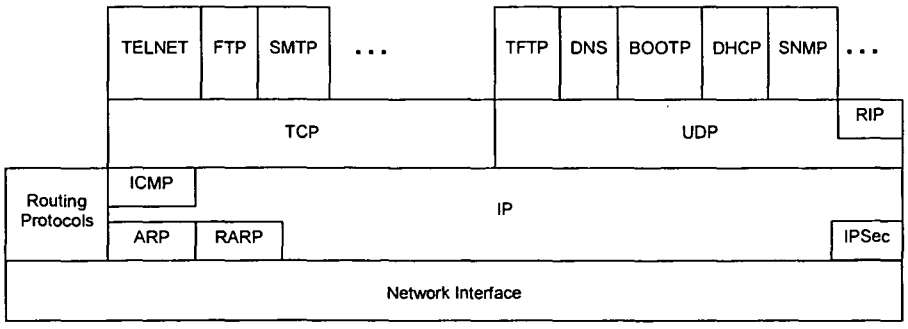


Figure 2-8: TCP/IP Protocol Suite

2.2.4.2 Internet Protocol version 4 – IPv4

The Internet Protocol (IP) is the most important protocol of the TCP/IP suite. IP is a network layer protocol that provides a connectionless packet forwarding service to the transport layer based on the IP address of a packet and IP routing tables. The IP packet forwarding process is also called IP routing. IP routing uses the "longest-prefix match" of the IP address of the packet to routing table entries, for forwarding packets. The current version of the IP protocol is called IPv4 and it is deployed worldwide. IPv4 has proved to be remarkably robust, easy to implement, and interoperable with a wide range of protocols and applications. Though substantially unchanged since it was first specified in the early 1980s, IPv4 has supported the scaling of the Internet to its current global proportions. In the following, the basics of the IPv4 will be presented.

IPv4 packet format

The basic unit of data transfer of the Internet Protocol is the IP packet. The IP packet is divided into two major parts: the header and the data. The header part represents the IP protocol itself. It is 20 octets long and it contains 14 fields. The data part includes the user data as well as higher layer protocols. Figure 2-9 illustrates the IPv4 packet format. The Version field (4 bits) specifies the IP protocol version. The HLEN field (4 bits) specifies the packet header length in units of 32-bit words. The Type of Service field (8 bits) specifies a 3-bit precedence value of 1 to 7, one bit to indicate delay sensitivity, one bit to indicate high throughput, one bit to indicate a request for high reliability, one bit for cost and one unused bit. The Total Length field (16 bits) specifies the total IP packet length for the header and the user data. The Identification field (16 bits) contains an integer that identifies the current packet. The Flag is a 3-bit field in which the two low-order bits control fragmentation – one bit specifying whether the packet can be fragmented, and the second whether the packet is the last fragment in a series of fragmented packets. The Fragment Offset field (13 bits) is used to help piece together IP packet fragments. The Time-To-Live (TTL) field (8 bits) specifies how many seconds the packet can remain in the Internet before it is discarded. Intermediate nodes decrement TTL, and when it reaches zero, the packet is dropped. The Protocol field (8 bits) identifies the higher-level protocol tape (e.g., TCP or UDP). The Header Checksum (16 bits) ensures the integrity of the header fields through a calculation that is easy to implement in software. Source IP address (32 bits) specifies the sending node. Destination IP address (32 bits) specifies the receiving node. The Options field (variable length) allows IP to support various options, such as security. The variable length of the Options field adds to the total size of the IPv4 packet. The Padding field is used for adding extra zeros to ensure that the IP header is always a multiple of 32 bits. The user data is placed in the Data field (variable length, maximum 64 kByte).

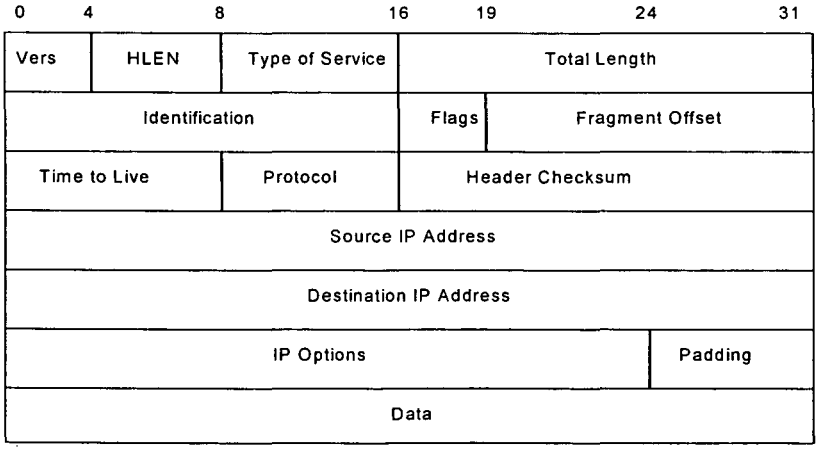


Figure 2-9: IPv4 Packet Format

IPv4 addressing

Addressing is the process of assigning an identifier - an address to each node in the network. A node needs an address in order to be located and communicate with other nodes in the network. In Internet terminology, the node can be a router or a host. Each host connected to the Internet has two addresses: a MAC address and an IP address. The MAC address of a host is a 48-bit data link address, which is burned into the NIC (Network Interface Card) and cannot be changed. The IP addresses are network layer addresses implemented in software and can be changed very easily. The combination of the IP address and the MAC address enables the delivery of packets to their proper destination. There are two addressing schemes used in the Internet: flat addressing and hierarchical addressing. A flat addressing scheme has no structure and it assigns to a host the next available address. The MAC addressing is based on the flat addressing scheme that makes it difficult to locate hosts on other networks. Hierarchical addressing schemes have a specific structure and are not randomly assigned. The IP addressing assignment is a typical hierarchical network-addressing scheme. Hosts are usually grouped in the IP addressing scheme, according to their department, or floor within a building. The hierarchical addressing scheme enables IP packets to traverse an internetwork, along with IP routing to find the destination in an efficient way.

IPv4 address classes and Subnetting- The current Internet uses 32-bit IP addresses as a global network-addressing scheme. The 32-bit IP address is divided into four octets and it is represented in the decimal notation as: XXX.XXX.XXX.XXX, where XXX ranges from 0 to 255 decimal, corresponding to the range of 00000000 to 11111111 binary. There are 2^{32} , or over 4 billion IP addresses.

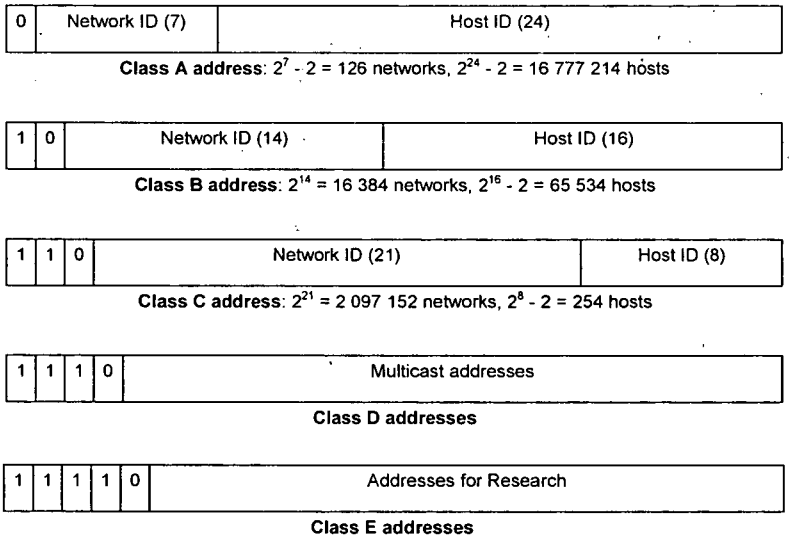


Figure 2-10: IPv4 Address Classes

IP addresses are grouped into five classes: A, B, C, D, and E, as shown in Figure 2-10. The first three classes are only used commercially. Class D is reserved for multicasting whereas class E is reserved for experimental research. Each of the A, B, and C addresses is divided into the network ID portion and host ID portion. The network ID is assigned by ARIN (Internet Assigned Number Authority) whereas the network administrator assigns the host ID. The network ID is used to identify the network whereas the host ID is used to identify the host within that network. The network or host portion of the address cannot be all ones or all zeros. In order to provide extra flexibility for the network administrator, networks are often divided into smaller networks called subnetworks or subnets. Subnet addresses include the Class A, Class B, or Class C network portion, plus a subnet field and a host field. The subnet field and the host field are created from the original host portion for the entire network. To create a subnet address, a network ad-

ministrator borrows bits from the original host portion and designates them as the subnet field. Adding subnets does not change how the outside world sees the network, but within the organization, there is additional network structure. From an addressing point of view subnets are extensions of a network number. The subnet mask is used to determine which part of an IP address is the network field and which part is the host field. Subnet masks use the same format as IP addresses. Default values for subnet mask for addresses of the class A, B, and C are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

2.2.4.3 Internet Protocol version 6 – IPv6

The ongoing explosive growth of the number of Internet users, particularly private users, and their requirements for new broadband Internet services has exposed insufficiencies to the very successfully deployed worldwide IPv4. The first and main problem to be noticed by IETF (around 1990) was IPv4 address exhaustion. To alleviate this problem, various techniques have been introduced including Network Address Translation (NAT) as a mechanism to share a few global addresses among many users. While NAT compensates for the lack of address space, it fails to always meet the requirements of the Internet's end-to-end architecture (security and QoS) and peer-to-peer applications. In addition, residential broadband Internet users require always-contactable global addresses, which are unsupportable with current IP address space and temporary allocation techniques. The current IP address space is also unable to satisfy the requirements of emerging applications such as Internet-enabled personal digital assistants (PDAs), home and small office networks, Internet-connected moving vehicles, integrated IP telephony services, IP wireless services, and distributed gaming. Adding to these insufficiencies the uneven IPv4 address assignment based on address classes a must to IETF for a new IP solution was imposed. This new solution was initially called IP next generation (IPng) and later renamed to Internet Protocol version 6 (IPv6). The IPv6 introduced a 128-bit address space thus providing an almost unlimited number of addresses to meet the emerging requirements and to enable the anticipated growth and development of the Internet for the foreseeable future. In addition to the practicly unlimited address space the designers of IPv6 added other new essential features and enhancements to IPv4, such as:

- Simplified header format for efficient packet handling,
- Hierarchical address architecture for routing efficiency,
- Support for widely deployed routing protocols,
- Autoconfiguration and plug-and-play support,
- Elimination of need for Network Address Translation (NAT),
- Embedded security with mandatory IPSec implementation,
- Enhanced support for QoS,
- Embedded support for mobile networks,
- Increased number of multicast addresses.

In the following subsections, the basics of IPv6 including most of the above mentioned features will be presented. Mobility support of IPv6 will be explained in some more detail in Chapter 4 whereas IP QoS mechanisms will be discussed in Chapter 5.

IPv6 packet format

The IPv6 packet, shown in Figure 2-11, consists of the IPv6 header, a variable number of extension headers, and the data portion of the packet. The header part carries the IPv6 protocol. Extension headers present a new concept in IPv6 and their use is optional. Data part includes transport level PDU (Packet Data Unit).

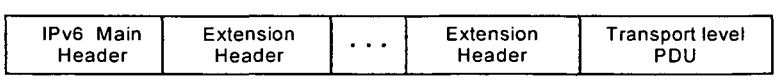


Figure 2-11: IPv6 Packet

The IPv6 main header, illustrated in Figure 2-12, consists of eight fields and it has a fixed size of 40 bytes. The Version is a 4-bit field as in IPv4 but it contains the value 6 for IPv6. The Traffic Class field (8 bits) is similar to the Type of Service field in IPv4. It is used to identify the delivery priority of each packet. The Flow Label is a new 20-bit field in IPv6. It is used by the source to tag packets of a specific flow for additional control of Quality-of-Service by the nodes on the path. The Payload Length field (16 bits) specifies the total length of the data portion of the packet. Therefore, the IPv6 supports payloads up to 65,535 octets long. The Next Header field (8 bits) identifies the type of information following the IPv6 header. This information can be an extension header, or a transport layer packet, such as TCP or UDP packet. The Hop Limit (8 bits) is similar to the TTL field in the IPv4 packet header but simpler to process. It is decremented by one by each node that forwards the packet. The packet is dropped if the Hop Limit is decremented to zero. The Source Address field is similar to the IPv4 Source Address field but it contains 128 bits. The Destination Address field, also 128 bits long, specifies the address of the intended recipient of the packet.

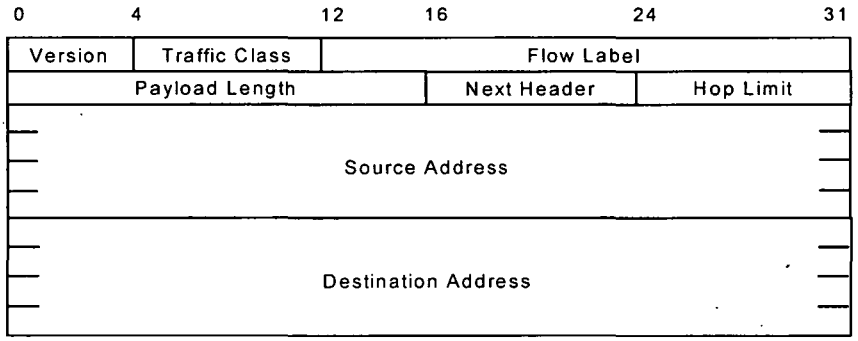


Figure 2-12: IPv6 Main Header

Although the IPv6 header size has increased to 40 octets versus 20 octets in IPv4, the IPv6 header format is simpler compared to the IPv4 header. As shown in Figure 2-12, six of the IPv4 header fields have been removed in IPv6: the Header Length (HL), Identification, Flags, Fragment Offset, Header Checksum, and Padding field. In IPv6 some IPv4 fields have been carried over with modified names, and some new fields have been added to improve efficiency and introduce new features. Also all fields in the IPv6 header are 64-bit aligned, taking advantage of faster processing by the current generation of 64-bit processors.

Extension Header

IPv6 extension headers are optional and provide a powerful means to support security, fragmentation, source routing, network management, and many other functions. If present, extension headers immediately follow the IPv6 header. In all extension headers the first field is the Next Header field, which identifies the value of the next extension header. The final extension header has in the Next Header field the value of a transport layer protocol, such as TCP or UDP.

There are many types of the extension headers. When multiple extension headers are present in a same packet, they should occur in this order:

- The Hop-by-Hop Options Header (value = 0) carries information that must be examined by all the nodes along the delivery path.
- The Routing Header (value = 43) is used by the source node to list all the nodes (IP addresses) the packet needs to traverse on the path to its destination. In other words, this extension header allows the sender to influence the routing of the packet.
- The Fragmentation Header is used by the source to indicate that the packet has been fragmented to fit within the Maximum Transmission Unit (MTU) size. The Fragment Header is used in each fragmented packet. Hence, in IPv6, unlike IP4, the end nodes instead of routers

do packet fragmentation and assembly, which further improves the efficiency of the IPv6 network.

- The Authentication Header (AH) is used in IPsec to provide support for data integrity and authentication by ensuring that a packet is actually coming from the host indicated in its source address. This header has the value = 51.
- The Encapsulating Security Payload (ESP) Header is used in IPsec to provide end-to-end data privacy and confidentiality by encrypting the transport layer header and payload, or the entire IP packet. This header has the value = 50.
- The Destination Options Header (value = 60) follows the ESP header and it is processed only at the final destination. Alternatively, this header can also follow Hop-by-Hop Options header, in which case it is processed at the final destination and also at each visited address specified by a routing header.

In general, with the exception of the Hop-by-Hop Options Header, extension headers are not examined or processed by any node along a packet's delivery path, until the packet reaches the node identified in the destination address field of the IPv6 header. Thus, intermediate nodes only have to investigate the first part of an IP packet. This simplifies processing in comparison with IPv4, where the header length is variable depending on the included options.

IPv6 Addressing Architecture

IPv6 addresses are 128 bits in length, providing approximately 3.4×10^{38} addresses (~340,282,366,920,938,463,374,607,432,768,211,456), enough to allocate about 1030 addresses per person on this planet. Besides the almost unlimited number of IP addresses, the IPv6 addressing scheme has been designed to provide compatibility and interoperability with the existing IPv4 network architecture and to allow the coexistence of IPv6 networks with existing IPv4 networks. The 128-bit IPv6 addresses are represented by eight 16-bit hexadecimal numbers separated by colons (:). The general format of a 128-bit IPv6 address is illustrated in Figure 2-13. The IPv6 network prefix is part of the address that represents the left-most bits that have a fixed value and represent the network identifier. IPv6 addresses are assigned to individual interfaces on nodes, not to the nodes themselves. Hence, the interface ID identifies an individual interface on nodes to which the address is assigned.

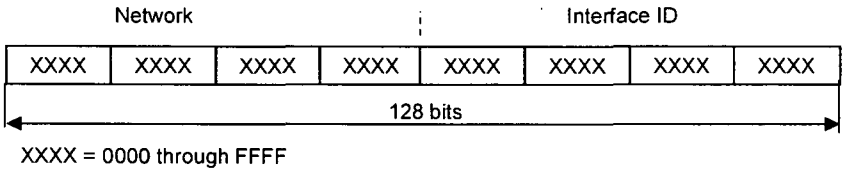


Figure 2-13: General Address Format of IPv6

An example of IPv6 address is the following:

2031:0000:1F1F:0000:0000:0100:11A0:ADDF.

In order to shorten the IPv6 and make them easier to represent, the following conventions are used:

- Leading zeros can be compressed (0000 = 0).
- One or more groups of 16 bits zeros, can be represented by a pair of colons "::", which can only appear once in an address.
- For example: 2001:0:13FF:09FF:0:0:0:0001 = 2001:0:13FF:09FF::1
- The lower four 8 bits can use decimal representation of IPv4 addresses. For example, an IPv4-compatible IPv6 address is 0:0:0:0:0:0.192.168.0.1.

Another important information included in IPv6 address presentation is the /prefix-length variable. The /prefix-length variable is a decimal value that indicates the number of contiguous high-order bits of the address comprising the prefix, which is the network portion of the address. For example, 1080:6809:8086:6502::/64 is an acceptable IPv6 prefix. If the address ends in a double colon, the trailing double colon can be omitted. So, the same address can be written as 1080:6809:8086:6502/64. An IPv6 node, unlike an IPv4 node, allows more than one type of IP address. There are three major types of IPv6 addresses: unicast, anycast, and multicast.

Unicast - An address used to identify a single interface. A packet that is sent to a unicast address is delivered to the interface identified by that address. Based on the reachability of the packets, unicast supports the following main address types: global unicast, site-local unicast, and link-local unicast. A global unicast address is an address that can be reached and identified globally. A global unicast address consists of a global routing prefix, a subnet ID, and an interface ID (Figure 2-14). The current global unicast address allocation uses the range of addresses that start with the binary number 001 (2000::/3), one-eighth of the total IPv6 address space. It is the largest block of assigned addresses. Site-local unicast address can only be reached and identified within a customer site, similar to IPv4 private address 10.0.0.0/8 and 192.168.0.0/16. The site-local unicast address contains a FEC0::/10 prefix, subnet ID, and interface ID (Figure 2-15). Link-local unicast address is an address that can only be reached and identified by nodes attached to the same local link. A link-local unicast address uses a FE80::/ 10 prefix and an interface ID (Figure 2-16). Interface identifiers must be 64 bits long and constructed in the Extended Universal Identifier (EUI)-64 format. The EUI-64 format interface ID is derived from the 48-bit link-layer (MAC) address by inserting the hex number FFFE between the upper three bytes and the lower 3 bytes of the link layer address. For instance, a node with Ethernet interface address 0003B61A2061, combined with network prefix 2001:0001:1EEF:0000/64 provided by router advertisement, will have an IPv6 address:
2001:0001:1EEF:0000:0003:B6FF:FE1A:2061.

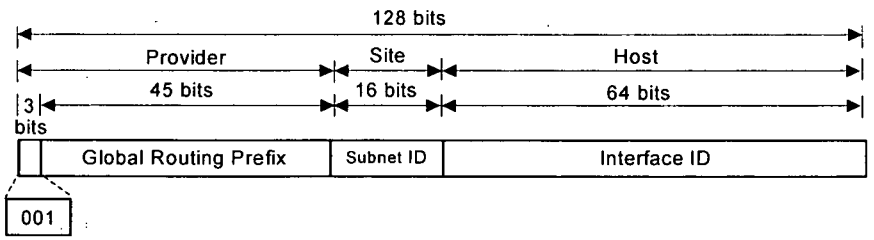


Figure 2-14: Global Unicast Adress Format

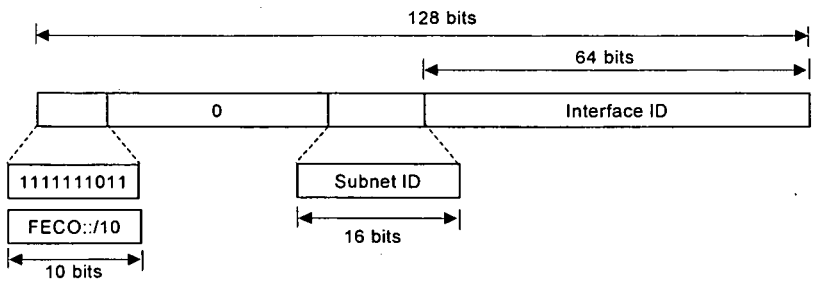


Figure 2-15: Site-Local Unicast Address Format

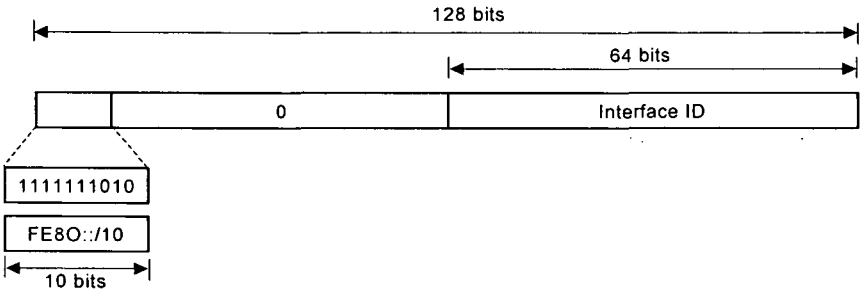


Figure 2-16: Link-Local Unicast Address Format

Anycast - is a global address that is assigned to a set of interfaces belonging to different nodes (Figure 2-17). A packet sent to an anycast address is routed to the nearest interface of the set. The anycast address has the following restrictions:

- An anycast address must not be used as source address of IPv6 packet.
- An anycast address must not be assigned to an IPv6 host. It may be assigned to an IPv6 router.

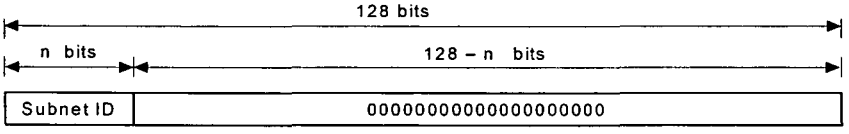


Figure 2-17: Anycast Address Format

Multicast – is the address assigned to a set of interfaces belonging to different nodes. A packet destined to a multicast address is routed to all interfaces identified by that address. The IPv6 multicast address uses the FF00::/8 prefix, 1/256 of the total IPv6 address space (Figure 2-18). There are no broadcast addresses in IPv6, their function being superseded by multicast addresses.

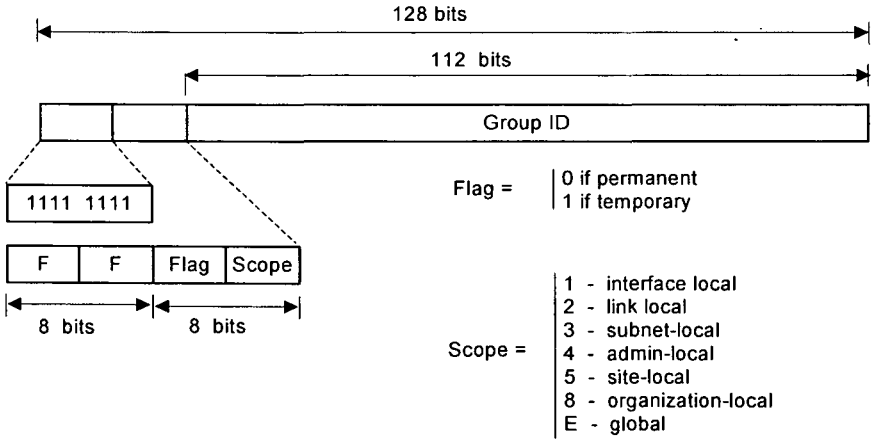


Figure 2-18: Multicast Address Format

Operation of IPv6

For the operation of the IPv6 two processes are essential: neighbor discovery and router discovery. The neighbour discovery enables IPv6 nodes to determine the link-layer address of a neighbor on the same local link, to verify the reachability of a neighbor, and to keep track of neighbor routers. To perform these functions the neighbour discovery process uses IPv6 ICMP (Internet Control Message Protocol) messages and solicited-node multicast addresses. When a node wants to determine the link-layer address of another node on the same local link, a

neighbor solicitation message is sent on the local link, carrying the sender's own link-layer address. After receiving the neighbor solicitation message, the destination node replies by sending a neighbor advertisement message with its own link-layer address on the local link. Having received the neighbor advertisement message the source and destination nodes can communicate. Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on a local link. Nodes use the router discovery process to discover the routers on the local link. To achieve this, the IPv6 router discovery process uses two messages: router advertisement and solicitation. Router advertisements messages are sent out periodically on each configured interface of an IPv6 router, and also in response to router solicitation messages from IPv6 nodes on the link. A router advertisement message contains the following information for nodes: The type of autoconfiguration a node should use (*stateless* or *stateful*), the hop-limit value a node should place in the IPv6 header, the network prefix a node should use to form the unicast address, the lifetime information of the included network prefix, the Maximum Transmission Unit (MTU) size a node should use in sending packets, and whether the originating router should be used as default router. When a host does not have a configured unicast address, it sends a router solicitation message, enabling the host to autoconfigure itself quickly without having to wait for the next scheduled router advertisement message.

Configuration of IPv6 nodes

IPv6 provides a very efficient mechanism for managing the huge number of nodes. This mechanism is named *stateless* autoconfiguration and presents an essential feature of IPv6 that enables serverless autoconfiguration of IPv6 nodes and easy renumbering. Using the *stateless* approach, a host can easily generate an address for itself by combining network's advertised prefix with its own interface identifier. Actually the network prefix information in the router advertisement messages is used as the /64 prefix of the host address. The remaining 64 bits address is constructed in the EUI-64 format, as explained earlier. However, hosts have to perform duplicate address detection. Renumbering of IPv6 nodes is possible through router advertisement messages, which contain both the old and new prefix. A decrease in the lifetime value of the old prefix alerts the nodes to use the new prefix, while still keeping their current connections intact with the old prefix. During this period, nodes have two unicast addresses in use. When the old prefix is no longer usable, the router advertisements will include only the new prefix. In addition to stateless autoconfiguration, IPv6 also supports stateful configuration with DHCPv6 (Dynamic Host Configuration Protocol version 6). In the *stateful* configuration approach, hosts obtain interface addresses and configuration information and parameters from a server. Servers maintain a database that keeps track of which addresses have been assigned to which hosts. *Stateful* configuration may also be used when a host is not able to configure its parameters alone. This may be the case when no routers are found or duplicate addresses are detected. The IPv6 node has an option to solicit an address via a DHCPv6 server.

2.2.4.4 IPv4 – IPv6 Transition

Taking into consideration the successful worldwide deployment of IPv4 technology the transition to IPv6 is a very challenging issue. The challenge is due to the fact that IPv6 has to coexist with IPv4 for a long time and the transition from IPv4 to IPv6 should be as transparent as possible to the end users. Hence, the IETF IPv6 working group has designed several transition strategies for the deployment of IPv6. The most important transition strategies are the following:

- Deploying IPv6 over dual stack backbones,
- Deploying IPv6 over IPv4 tunneling,
- Deploying IPv6 over dedicated data links,
- Deploying IPv6 over MPLS (Multiprotocol Label Switching) backbones.

Dual-stack backbone - This technique requires that all routers in the network maintain both IPv4 and IPv6 protocol stacks. Today, dual-stack routing is the preferred deployment strategy

for network infrastructures with a mixture of IPv4 and IPv6 applications that require both protocols. Applications choose between using IPv4 or IPv6, with the application selecting the correct address based on the type of IP traffic and particular requirements of the communication. However, this strategy has several difficulties. Apart from the obvious need to upgrade all routers in the network, limitations to this approach are that the routers require a dual addressing scheme, require dual management of the IPv4 and IPv6 routing protocols and sufficient memory for both the IPv4 and IPv6 routing tables.

IPv6 over IPv4 tunnelling - Tunneling consists of encapsulating IPv6 traffic within IPv4 packets, to be sent over an IPv4 backbone. This enables isolated IPv6 end systems and routers to communicate through an existing IPv4 infrastructure between them. A variety of tunnel mechanisms are available for deploying IPv6. These mechanisms include IPv6 manually configured tunnels, IPv6 over IPv4 GRE (Generic Routing Encapsulation) tunnels, automatic IPv4 compatible tunnels, automatic 6over4 tunnels, and ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) tunnels. All these tunneling mechanisms require that the endpoints of the tunnel run both IPv4 and IPv6 protocol stacks, that is, endpoints must run in dual-stack mode.

IPv6 over dedicated data links – This transition strategy enables IPv6 domains to communicate by using the same Layer 2 infrastructure used for IPv4, but with IPv6 using for example separate ATM PVCs (Permanent Virtual Circuits).

IPv6 over MPLS (Multi-Protocol Label Switching) backbones - Using MPLS technology (described in Chapter 5), isolated IPv6 domains can communicate with each other over a MPLS IPv4 core network. Because MPLS forwarding is based on labels rather than on the IP header itself, this implementation requires far fewer backbone infrastructure upgrades and less reconfiguration of core routers, providing a very cost-effective way to deploy IPv6.

2.2.4.5 Network Layer Protocols

The TCP/IP protocol suite has two main transport layer protocols: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). These protocols actually provide an interface between the Internet layer below and the application layer above in the TCP/IP suite.

Transmission Control Protocol - Along with IP, TCP represents the most important protocol in the TCP/IP suite. TCP is a connection oriented, reliable protocol documented in IETF RFC 793. TCP works over IP to achieve end-to-end reliable transmission of data across the Internet. It provides adaptive flow control, segmentation of outgoing messages, reassembly of the messages from incoming segments, resends not received data, and supplies a virtual circuit between end-user applications. The main advantage of TCP is that it provides guaranteed delivery of the segments. Figure 2-19 illustrates the TCP format.

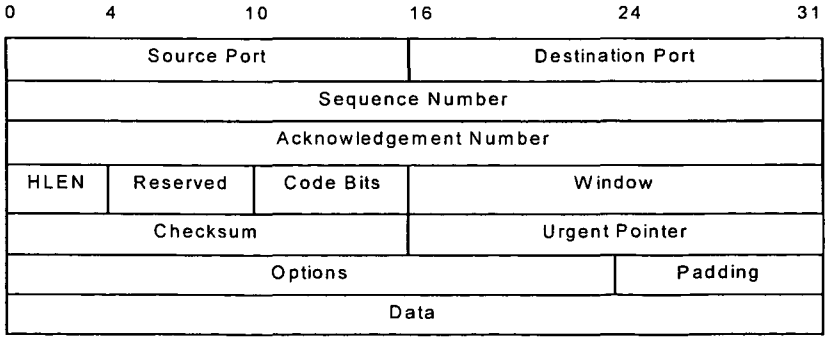


Figure 2-19: TCP Format

The Source Port and the Destination Port indicate the TCP port numbers used to identify a specific application protocol in the source and destination hosts. The Sequence Number field identifies the position of the sender's byte stream in the data field. The Acknowledgment Number

field identifies the number of the next octet to be received. The HLEN field provides the length of the header. The Code Bits field determines the use of the segment contents (e.g., SYN for synchronize sequence numbers and RST for reset connection). The Window field tells the amount of data the application is willing to accept. The checksum is applied across the TCP header and the user data and is used to detect errors. The Urgent Pointer field specifies the position in the data segment where the urgent data begins if the code bits indicate that this segment contains urgent data. The Options and Padding fields are not mandatory. TCP provides reliability by using flow control mechanism with a variable size window (sliding window). The sender starts with a window size equal to that of one TCP/IP segment, usually defined by a Maximum Transmission Unit (MTU) size used by the data link layer below. The IP packets are delivered to the destination host, resulting in a delivered segment, which is acknowledged. The sender then increases the window size to two segments. When this two segments are received they are both acknowledged, and the sender increases the window size to three segments. If a segment is lost the sender detects this by starting a timer whenever a segment is sent. If the timer expires without receiving an acknowledgment, then the segment is present. Upon such a retransmission timeout, the sender resets its window size to one segment and repeats the above process. The described operation is also known in the literature as "slow start" TCP protocol. There are several proposals as refinement of the slow start TCP protocol such as Vegas, Reno, Tahoe, New Tahoe, and Selected Acknowledgement (SACK).

User Datagram Protocol - Is a connectionless transport protocol in the TCP/IP protocol suite that is documented in IETF RFC 768. It is a simple protocol that transports data unreliably between hosts, without acknowledgments, flow control, or guaranteed delivery. UDP does not provide software checking for packet delivery and does not reassemble incoming messages. Error processing and retransmission must be handled by other higher layer protocols. The advantage that UDP provides is speed. Since UDP provides no acknowledgments, less traffic is sent across the network, making the transfer faster. UDP is useful in situations where the reliability mechanisms of TCP are not necessary and when real time data transportation is required. A number of application protocols interface to TCP and UDP as shown in Figure 2-8. Like TCP, the UDP provide the capability for the host to distinguish between application protocols through port numbers. Application software developers have agreed to use the well-known port numbers that are defined in RFC1700.

2.2.4.6 Internet Layer Protocols

Besides IP, there are several other protocols that operate at the Internet layer of the TCP/IP suite, as shown in Figure 2-8. The most important protocols of this layer are routing protocols, which are very often confused with the IP protocol. As a matter of the fact, there is an essential difference between IP and routing protocols. As mentioned earlier, the IP protocol forwards the packets that arrive at the node (router), based on the IP address of a packet and on information contained in the IP routing tables. Whereas routing protocols are used by routers to exchange routing information with other routers of a network in order to build routing tables. The routing table of a router contains the necessary information to forward IP packets to the next router along the way from the source to the destination. If a router receives a packet whose destination address is not in its routing table, it forwards it to the address of another router that most likely does contain information about the destination network in its routing table. The size of the routing tables in the routers is a very important issue as large routing tables consume memory and impact the efficiency of the routing. The hierarchical addressing structure of IPv6, for example, provides an efficient means to reduce the size of routing tables. Routers have the ability to make forwarding decisions regarding the best path for delivery of the packets on the network. Routing decisions are based on some form of least-cost criterion. Each link in a network can be assigned a cost, with a routing objective to find a least-cost route. More typically, the link cost is inversely proportional to the link capacity, proportional to the current load on the link, or may reflect some performance information such as delay, or some combination of parameters. Routing protocols generally exchange information about the network topology, that is, the links that

are connected and their associated costs. Based on the exchanged routing information, routing protocols are grouped into two different classes: Distance-Vector and Link-State.

With the distance vector routing protocols neighbor routers periodically exchange vectors of the distance to every destination in the network. Based on this information a router uses a specific algorithm (such as the Bellman Ford algorithm) to find the shortest path to other routers in the network and updates its routing table. A routing table typically stores very little information about links that are not directly connected to the router running the protocol. For each destination, the router usually stores just a single route table entry, containing very often just the distance from the router to the destination, as well as the next router toward that destination. These protocols have many advantages a key one being simplicity. However, distance vector protocols can suffer from very slow convergence ("counting to infinity" problem). Slow convergence of the distance vector routing protocols is due to the fact that the routing information and the time for it to propagate through the network increases as the network grows. In addition, the neighboring routers can confuse each other by passing "old" information back and forth, incrementing the distance to a destination each time, until the recorded distance exceeds the maximum allowable. An example of the distance vector state routing protocols is RIP (Routing Information Protocol). With the link-state routing protocols, each router maintains a view of the link state topology of the entire network in a link-state database and broadcasts periodically the link state of its outgoing links to all other nodes using a protocol such as flooding. When a router receives this information, it updates its link-state database and it applies a shortest path algorithm (such as the Dijkstra algorithm) to choose its next hop for each destination. Traditional link-state protocols require relatively large bandwidth to maintain a current view of the network state. When the topology of the network changes (due to a link or router failure, or because of addition of a new router or link) this information must be updated at other routers. However, some current link-state protocols do not require all nodes to have identical link-state information. Instead, nodes distribute link-state information only when there has been a significant change. Also, it is not necessary for all routers to receive all link-state information intended for them in order to compute routes. The main advantage of these link-state routing protocols is the reduction of topology update information and the decreased convergence times, whereas a main disadvantage is the increased complexity. An example of the link state routing protocols is the OSPF protocol.

Another classification of the routing protocols is based on the domain or scope that a routing protocol manages. There are two groups of such protocols: Interior Gateway Protocols (IGP) and Exterior Gateway Protocols (EGP). An Interior Gateway Protocol passes routing information between routers within an Autonomous System (AS). An autonomous system is a network connected by homogeneous routers under the control of a single administrative group sharing the same set of policies. Each autonomous system will have its own routing technology, which may well be different for different autonomous systems. Typical examples of IGPs are: Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF). The protocol used to pass routing information between routers in different autonomous systems is referred to as an Exterior Gateway Protocol (EGP). An example of an EGP is the Border Gateway Protocol (BGP). There are other TCP/IP non-routing protocols such as Address Resolution Protocol (ARP), Reverse ARP (RARP), Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), Distance Vector Multicast Routing Protocol (DVMPR), IP security (IPsec) that are considered to belong to Internet layer protocols.

In the following several routing and non-routing protocols will be presented briefly.

Routing Information Protocol (RIP) – Is a distance vector based interior gateway protocol, which runs over UDP. RIP is the most common protocol used to transfer routing information between routers located on the same network, and one of the earliest routing protocols to be

developed. Distances to a destination host are calculated in terms of how many hops a packet must pass through. Whenever a packet passes a router it is considered to have traveled one hop. The maximum number of hops that a packet is allowed to travel is fifteen, otherwise the destination network is considered unreachable. If there are multiple paths to a destination, the router selects the path with the least number of hops. Because hop count is the only routing metric used by RIP, a router does not necessarily select the fastest path to a destination. However, RIP remains very popular. It is still widely implemented, although in the new enhanced versions. The new version of RIP developed for IPv4 is RIPv2, described in RFCs 1723 and 2453. RIP2 is an extension of the RIP intended to expand the amount of useful information carried in the RIP2 messages and to add a measure of security. For IPv6 networks the RIP next generation (RIPng) was designed. RIPng is based on protocols and algorithms used extensively in the IPv4 Internet, with minimum changes as described in RFC 2080 and specified in RFCs 1058 and 1723. RIPng uses IPv6 for transport, including IPv6 prefix distribution, next-hop IPv6 address, and multicast group FF02::9 for RIP updates. The maximum number of hops that an IPv6 packet can travel remains fifteen.

Interior Gateway Routing Protocol (IGRP) and Enhanced Interior Gateway Routing Protocol (EIGRP) - are two routing protocols that were developed by Cisco Systems, therefore they are considered proprietary routing protocols. IGRP was developed specifically to address problems associated with routing in large multi-vendor networks that were beyond the scope of protocols such as RIP. IGRP is also a distance-vector protocol; however, when determining the best path, it may also take into consideration metrics such as bandwidth, load, delay, and reliability. Network administrators can determine the importance given to any one of these metrics, or, allow IGRP to automatically calculate the optimal path. EIGRP is an advanced version of IGRP. It combines the advantages of link-state protocols with those of distance-vector protocols. Specifically, convergence properties and the operating efficiency of this protocol have improved significantly. It is regarded as an interior gateway protocol but has also been used extensively as exterior gateway protocol for inter domain (autonomous system) routing.

Open Shortest Path First (OSPF) – is a link-state routing protocol. It is defined in several IETF RFCs. The newest version of OSPF developed for IPv4 - OSPFv2 is defined in RFC 2328. OSPF is classified as an Interior Gateway Protocol (IGP). This means it is designed to run internal to a single Autonomous System (AS). Each OSPF router maintains an identical database describing the *autonomous system's* topology. Each individual piece of this database is a particular router's local state. The router distributes its local state throughout the *autonomous system* by flooding. In addition, all OSPF routing protocol exchanges are authenticated. This means that only trusted routers can participate in the *autonomous system's* routing. From the link-state database, a routing table is calculated by constructing a shortest- path tree with itself as root. This shortest-path tree gives the route to each destination in the *autonomous system.* When several equal-cost routes to a destination exist, traffic is distributed equally among them. OSPF quickly detects topological changes in the AS, such as router interface failures, and it quickly calculates new loop-free routes. Compared with RIP, OSPF can provide scalable network support and faster convergence time. OSPF is widely used in large networks such as ISP backbone and enterprise networks. To support IPv6 protocol OSPFv3 version is defined in IETF RFC 2740. The fundamental mechanisms of OSPFv2 remain unchanged. However, some changes have been necessary, either due to changes in protocol semantics between IPv4 and IPv6, or simply to handle the increased address size of IPv6. For example, addressing semantics have been removed from OSPF packets and the basic Link-State Advertisements (LSAs). New LSAs have been created to carry IPv6 addresses and prefixes. Furthermore, authentication has been removed from the OSPF protocol itself, instead relying on IPv6's Authentication Header and Encapsulating Security Payload. However, most packets in OSPF for IPv6 are almost as compact as those in OSPF for IPv4, even with the larger IPv6 addresses.

Border Gateway Protocol (BGP-4) - is an inter- Autonomous System (AS) routing protocol defined in IETF RFC 1771 to work with IPv4. It is the only protocol that is designed to deal with a network of the Internet's size, and the only protocol that can deal well with having multiple connections to unrelated routing domains. The primary function of a BGP system is to exchange network reachability information with other BGP systems. This includes information on the list of *autonomous systems* that the reachability information traverses. This information is sufficient to construct a graph of AS connectivity from which routing loops may be pruned and some policy decisions at the AS level may be enforced. When a BGP router first connects to the network, it exchanges its routing table with all other BGP routers. When the routing table changes, the router also sends the portion of the routing table that has changed. BGP routers do not send regularly scheduled routing updates, and BGP routing updates advertise only the optimal path to a network. BGP uses a single routing metric to determine the best path to a given network. This metric consists of an arbitrary unit number that specifies the degree of preference of a particular link. The value assigned to a link can be based on any number of criteria, including the number of autonomous systems through which the path passes, stability, speed, delay, or cost. In order to support the IPv6 protocol, BGP-4 was extended as defined in RFC 2283. The only three pieces of information carried by BGP-4 that are IPv4 specific are (a) the Next-Hop attribute, expressed as an IPv4 address; (b) Aggregator (contains an IPv4 address), and (c) Network Layer Reachability Information Routes (NLRI), expressed as IPv4 address prefixes. Assuming that any BGP speaker has to have an IPv4 address (which will be used, among other things, in the Aggregator attribute), the only two extensions that have to be added to BGP-4 to support routing for IPv6 are: the ability to associate a particular *network layer* protocol with the next hop information, and the ability to associate a particular *network layer* protocol with NLRI.

Address Resolution Protocol (ARP) – is a method for finding a host's unknown MAC address from its known IP address. To find out the MAC address of a communicating host, the sender host broadcasts an ARP packet containing the Internet address of a communicating host and waits for it (or some other host) to send back its Ethernet address. Each host maintains a cache of address translations (ARP cache), which contains a mapping between each MAC address and its corresponding IP address, to reduce delay and loading. ARP is defined in RFC 826.

Reverse Address Resolution Protocol (RARP) - is the protocol a host uses when it does not know its own IP address. RARP enables a host to request its IP address from the gateway router ARP cache. Assuming that an entry has been set up in the gateway router ARP cache, the RARP server on the router will return the IP address to the host, which can store it for future use. RARP is defined in RFC 2390.

Internet Control Message Protocol (ICMP) - is defined by RFC 950 and it is another major component of the TCP/IP protocol suite. The key ICMP functions are: announce network errors, announce network congestion, assist troubleshooting, and announce timeouts. The ICMP messages are contained within standard IP packets and they are classified as error or informational messages. Error messages can be destination unreachable, packet too big, time exceeded, and parameter problem. The possible informational messages are, Echo Request, Echo Reply, Group Membership Query, Group Membership Report, and Group Membership Reduction. ICMP messages are typically generated in response to errors in IP packets or for diagnostic or routing purposes. For example, if a router receives an IP packet that it cannot deliver, it sends a message back to the sender of the packet. However, hosts cannot count on receiving ICMP packets for any network problems, as ICMP packet delivery is unreliable. Although ICMP messages are contained within standard IP packets, ICMP messages are usually processed as a special case distinguished from normal IP processing, rather than processed as a normal sub-protocol of IP. In particular, ICMP messages should never be generated as a consequence of ICMP message processing, in order to prevent cascades of ICMP messages. The ICMP was revised during the definition of IPv6. The multicast control functions of the IPv4 Group Membership Protocol (IGMP) are now incorporated with the ICMPv6. Every ICMPv6 message is preceded by the IPv6 main header and maybe by one or more IPv6 extension headers. The ICMPv6 header is

identified by a next header value of 58 in the immediately preceding header. ICMPv6 is defined by RFC 2463 and is an integral part of IPv6.

Internet Group Management Protocol (IGMP) - is a multicasting protocol in the TCP/IP suite, defined by the IETF in RFC3376. IP hosts use IGMP to report their host group memberships to any immediately neighboring multicast router. IGMP messages are encapsulated in IP packets, with an IP protocol number 2. IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3. The IGMPv1 allows hosts to join multicast groups but there are no leave-messages. Routers use a time-out based mechanism to discover the groups that are of no interest to the members. The IGMPv2 adds leave-messages to the protocol. This allows group membership termination to be quickly reported to the routing protocol, which is important for high-bandwidth multicast groups and for subnets with often changing group memberships. The IGMPv3 is a major revision of the protocol that adds support for source filtering. This indicates the ability for hosts to specify the list of source hosts from which they want to receive traffic from. Traffic from other hosts is blocked in the routers inside the network. It also allows hosts to block packets that come from sources that send unwanted traffic.

Distance Vector Multicast Routing Protocol (DVMRP) - is a variant protocol of IGMP that provides an efficient mechanism for connectionless message multicast to a group of hosts across an internetwork. DVMRP is an "interior gateway protocol" (IGP) for use within an autonomous system, defined by RFC 1075. DVMRP is not currently developed for use in routing non-multicast packets, so a router that routes both multicast and unicast packets must run two separate routing processes. DVMRP was developed based upon RIP because that implementation was available and simple. However, DVMRP differs from RIP in one very important way. RIP routes and forwards packets to a particular destination. The purpose of DVMRP is to keep track of the return paths to the source of multicast packets. To make the explanation of DVMRP more consistent with RIP, the term destination is used instead of the more proper term source, however, packets are not forwarded to these destinations, but rather, originate from them. DVMRP packets are encapsulated in IP packets, with an IP protocol number of 2 (IGMP). The DVMRP packets use a common protocol header that specifies the IGMP Packet Type as DVMRP, i.e., DVMRP uses the IGMP packets to exchange routing packets.

IP security (IPSec) - is a standard for securing IP communications by encrypting and authentication all IP packets. IPSec is actually a protocol suite consisting of protocols for securing packet flows, and of key exchange protocols used for setting up those secure flows. There are two protocols used for securing packet flows: Encapsulating Security Payload (ESP) for encrypting packet flows, and the rarely used Authentication Header (AH) which provides authentication and message integrity guarantees for such flows, but does not offer confidentiality. Currently only one key exchange protocol is defined, the Internet Key Exchange (IKE) protocol (RFC 2409), which is used to set up a security association in the IPsec protocol suite. IPSec protocols operate at layer 3 of the OSI model, which makes them suitable for protecting UDP-based protocols when used alone. The down side is that compared with transport-layer protocols the IPSec protocols need to deal with reliability and fragmentation issues, which is usually done by TCP. This protocol was intended to provide either portal-to-portal communication security in which security of packet traffic is provided to several hosts (even whole LANs) by a single node, or end-to-end security of packet traffic in which the endpoint hosts do the security processing. It can be used to construct Virtual Private Networks (VPN) in either mode, and this is the dominant use. IPSec protocols are defined by RFCs 2401-2409. They are a mandatory part of IPv6 and an optional part of the IPv4.

2.2.4.7 Application Layer Protocols

Application Layer protocols provide an interface between user applications and Internet services. Most of the Internet services are designed based on the client-server model. This means they have two components: the client part and the server part. The client part is the application

itself located on the local computer that requests a particular service. The server part is the service itself located on a remote server computer that responds to the client's request. A user selects an application based on the type of work he wants to accomplish. A wide set of application layer protocols are available to interface with the Internet. Each application type is associated with its own application protocol. Internet provides a wide range of narrowband and broadband services. The Internet services are out of scope of our discussion. However, we will shortly mention two traditional and most used Internet services: World Wide Web (WWW) and Electronic mail (E-mail). The World Wide Web is the most popular service that made the Internet to be what it is today. The Web is a multimedia client-server based service with millions of pages contained on the computer servers distributed throughout the worldwide Internet. Users access the web pages through applications or client programs called browsers. The two most popular Web browsers are Microsoft Internet Explorer and Netscape Communicator. The appearance and operation of these two client programs is very different, but they both work with the application layer HyperText Transfer Protocol (HTTP). The Web is made up of three standards: (1) The Uniform Resource Locator (URL) specifing how each page of information is given a unique address at which it can be found; (2) the HyperText Transfer Protocol (HTTP) specifing how the browser and server send information to each other; and (3) the HyperText Markup Language (HTML) specifying the method of encoding the information on web pages. Another intensively used Internet service is Electronic Mail or E-mail. The two most popular E-mail client applications are Microsoft Mail and Netscape Mail, which work with the application layer Post Office Protocol (POP). Although there are more application-layer protocol types available, in the following we will briefly describe the most popular ones.

Telnet - is the terminal emulation protocol designed to establish a virtual connection between a client and a server. Telnet allows the client to log in to a remote server and execute commands. Modern Telnet provides many options such as: ability to transfer binary data, support byte macros, emulate graphic terminals, and convey information to support centralized terminal management. However, in environments where security is important, such as on the public Internet, Telnet should not be used, because Telnet sessions are not encrypted. Telnet uses TCP as its transport protocol and is defined in RFC 854, RFC 855. Recently the usage of the Telnet protocol dropped rapidly in favor of a more secure and functional protocol called **Secure Shell Protocol (SSH)**. SSH provides all functionalities present in Telnet with the addition of encryption to prevent sensitive data such as passwords from being intercepted and public key authentication, to ensure that the remote computer is actually the one it claims to be.

File Transfer Protocol (FTP) - is designed to transfer files between hosts and it is defined by IETF RFC 959. FTP uses TCP to create a virtual connection for control information and then creates a separate TCP connection for data transfers. The control connection uses a protocol similar to the Telnet protocol to exchange commands and messages between hosts. FTP control frames are Telnet exchanges and can contain Telnet commands and option negotiation. However, most FTP control frames are simple ASCII text and can be classified as FTP commands or FTP messages. FTP provides user authentication, data encryption and enables a host to list directories of the remote host. However, FTP has extremely high latency from the moment that the request is send until the required data starts to arrive. Sometimes, a long log procedure is required

Trivial File Transfer Protocol (TFTP) - is a very simple protocol to transfer files between hosts on a network, similar to FTP. The TFTP is designed to be small and easy to implement, therefore, lacks most of the features of the FTP. In contrast to FTP, TFTP cannot list directories and does not provide authentication. However, it is often used to transfer small files between hosts on same LANs because it operates faster than FTP in a stable environment. TFTP is defined by RFC 1350 and it has been implemented on top of UDP.

Simple Mail Transfer Protocol (SMTP) - is defined by IETF RFC 821 to transfer electronic mail reliably and efficiently. SMTP uses TCP as its transport protocol and is the de facto stan-

dard for email transmission across the Internet. It is a relatively a simple protocol, where one or more recipients of a message are specified (and in most cases verified to exist) and then the message is transferred.

Post Office Protocol version 3 (POP3) – is designed to retrieve email from a remote mail server to a local client. POP3 and its predecessors (POP1 and POP2) support "offline" mail processing. They allow end users to retrieve email from a mail server when connected, and then to view and manipulate the retrieved messages without the need to stay connected. Clients have an option to leave mail on the server or delete it from the server, and then disconnect. POP3 is the most widely used protocol for mail retrieval. Nearly all individual Internet service providers email accounts are accessed via POP3. This protocol uses TCP as the transport protocol.

Internet Message Access Protocol (IMAP) - is an advanced alternative to POP3 protocol. The current version of IMAP, IMAP version 4 revision 1 (IMAP4rev1) is defined by RFC 3501 and works over TCP. IMAP4 provides several capabilities that are not included in POP3, such as support for both *connected* and *disconnected* modes of operation. When using POP3, clients typically connect to the email server very briefly, only as long as it takes to download any new messages. When using IMAP4, clients often stay connected as long as the user interface is active and download message content on demand. IMAP4 protocol allows simultaneous access by multiple clients to the same mailbox. It provides mechanisms for clients to detect changes made to the mailbox by other, concurrently connected, clients. In contrast, the POP3 protocol assumes the currently connected client is the only client connected to the mailbox. IMAP4 protocol provides the flag mechanism that enables clients to keep track of message state, for example whether or not the message has been read, replied to, or deleted. These *flags* are stored on the server, so multiple clients accessing the same mailbox at different times can detect state changes made by other clients. As a matter of the fact, POP3 also provides flag mechanism but only for local use. IMAP also provides support for accessing multiple mailboxes on the server. IMAP4 clients can create, rename, and/or delete mailboxes (usually presented to the user as folders) on the server, and move messages between mailboxes. IMAP also provides a mechanism for a client to ask the server to search for messages meeting a variety of criteria. This mechanism avoids requiring clients to download every message in the mailbox in order to perform these searches, as would be the case with POP3. Most email clients can be configured to use either POP3 or IMAP to retrieve messages; however, ISP (Internet Service Provider) support for IMAP is not as common.

Hypertext Transfer Protocol (HTTP) - is used to communicate information on the World Wide Web, as well as on internal networks. HTTP is a request/response protocol between clients and servers. An HTTP client sends a request string, such as "GET / HTTP/1.1" to the server. The "GET / HTTP/1.1" string is interpreted by server as a request for the default page of that web server. The server would then respond with a file or error message. An HTTP Header precedes the file sent by the server. The HTTP header is a set of ASCII strings containing information *about* the server and the document being sent. There are several versions of HTTP. The first version, referred to as HTTP/0.9, is followed by the more advanced HTTP/1.0 version, defined by RFC 1945. The latest version HTTP/1.1, defined by RFC 2616, includes more stringent requirements than HTTP/1.0 in order to ensure a reliable implementation of its features. HTTP differs from other TCP-based protocols such as FTP, in that connections are generally torn down once a particular request has been completed. This design makes HTTP ideal for the World Wide Web, where pages regularly link to pages on other servers.

Secure Hypertext Transfer Protocol (HTTPS) - is the secure version of HTTP that provides authentication and encrypted communication. HTTPS, defined in IETF RFC 2660, is designed to coexist with HTTP's messaging model and to be easily integrated with HTTP applications. It provides secure communication mechanisms between an HTTP client-server pair in order to enable commercial transactions for a wide range of applications. Secure HTTP provides symmetric capabilities to both client and server while preserving the transaction model and imple-

mentation characteristics of HTTP. In addition, several cryptographic message format standards may be incorporated into HTTPS clients and servers.

Bootstrap Protocol (BOOTP) - is designed for dynamic configuration of the booting host. BOOTP uses UDP as the transport protocol and originally is defined in IETF RFC 951 as an alternative to RARP. However, BOOTP provides much more configuration information and allows dynamic configuration for entire IP network. Basically, the BOOTP servers assign the IP-address from a pool of addresses to each host with a certain *lease* time. In addition, other configuration information such as: the IP address of the BOOTP server, the local subnet mask, the local time offset, the addresses of default routers, and the addresses of various Internet servers, can also be communicated to a host using BOOTP.

Dynamic Host Configuration Protocol (DHCP) – is an advanced configuration protocol based on BOOTP. The DHCP, also known as DHCPv4, uses UDP as its transport protocol. The latest definition of DHVPv4 is given by RFC 2131. The DHCP (DHCPv4) provides mechanisms to allocate IP addresses quickly and dynamically to hosts on a LAN (Local Area Network). A system administrator assigns a range of IP addresses to DHCP server and each host on the LAN has its TCP/IP software configured to request an IP address automatically from the DHCP server when that host comes on line. The DHCP server chooses an address and allocates it to that host. In addition to the IP address, a DHCP server can provide other information like DNS server addresses, a DNS domain or a gateway IP address, for the convenience of the host. DHCP also uses the concept of a *lease* time. For computers that need a permanent IP address, DHCP supports static addresses. The DHCP was modified for IPv6 networks resulting in the DHCPv6 protocol. DHCPv6 supports the new address architecture and is essential for operating IPv6 infrastructures. DHCPv6 enables DHCP servers to pass IPv6 addresses and other configuration parameters to IPv6 hosts. It offers the capability of the automatic allocation of reusable network addresses and provides additional configuration flexibility.

Simple Network Management Protocol (SNMP) - was developed to manage nodes on an IP network. It enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving change notices from network devices implementing SNMP. There are three versions of SNMP defined: SNMPv1, SNMPv2, and SNMPv3. Versions 1 and 2 have a number of features in common, but SNMPv2 offers enhancements in the performance and adds additional protocol operations. SNMPv3 defined by RFC3411-RFC3418 is the current standard version of SNMP. This version adds security, confidentiality, manager-to-manager communication, and remote configuration capabilities to the previous versions. To solve the incompatible issues among different versions of SNMP, RFC 3584 defines the coexistance strategies. The SNMP runs over UDP.

Domain Name System (DNS) - is a distributed database system used in the Internet for translating names of domains (www.ikn.tuwien.ac.at) to IP addresses (128.131.88.86). Most Internet services rely on DNS to work, because users find it more convenient to use domain names. DNS is a core feature of the Internet, because if DNS fails, web sites cannot be located and email delivery stalls. DNS uses UDP as the transport protocol. It is defined in RFC 1034 and updated by several RFC. The latest one being RFC 2535.

2.3 Mobile Communication Networks

The last 10 years have seen an explosive growth of mobile communication. It is predicted that growth will certainly continue and that in the near future the number of mobile subscribers will be higher than the number of fixed network subscribers. In fact, in several countries, the number of mobile subscribers already exceeds the number of fixed subscribers. Furthermore, it is expected that mobile users will request the same real-time services as fixed Internet users. This

provides hard evidence about the bright future of mobile communications as well as of the challenges that need to be faced in order to meet the mobile user's requirements. In general, the mobile communication systems development is grouped into different generations. The first-generation (1G), such as the Nordic Mobile Telephone (NMT) system and American Mobile Phone System (AMPS), employs analogue network technology. These networks offered basic services for the users and the emphasis was on speech. The second-generation (2G), such as Global System for Mobile Communications (GSM), is characterized by employment of digital technology, providing more efficiency in the network, and more advanced features. Recently introduced General Packet Radio Service (GPRS) and related GSM extensions have been referred to as 2.5G, to provide higher rates for mobile data services. The Universal Mobile Telecommunication Service (UMTS) and other systems belonging to the International Mobile Telecommunication System 2000 (IMT-2000) family, present the third-generation (3G). At present, 3G mobile communication systems are just beginning to be deployed, while research on the next generation of mobile communication systems, the fourth-generation (4G) wireless networks, begins to pave the way for the future. Right now, it is hard to say where the third generation ends and the fourth generation starts. But it is for sure that the final goal for mobile networks evolution is All-IP network. A key role of IP in future mobile communication networks will be the provisioning of efficient and cost-effective interworking between IP based and non-IP overlay networks. However, cellular operators are likely to undertake the migration to a full IP solution on Public Land Mobile Networks (PLMN) only beyond third-generation mobile networks.

Another important segment of mobile communication systems are Satellite and Wireless LAN (WLAN) networks. Satellite networks are considered a feasible solution to provide services for users in remote areas, where there is no communication infrastructure, or as complementary networks to terrestrial mobile networks. On the other hand, WLAN provides broadband services to slow mobile users, and currently present a hot topic in the wireless mobile communication market. The current trend is the unification of at least some of the existing technologies toward IMT-2000 for global mobile communication and envisioned mobile broadband systems for local wireless communication with much higher bandwidth and additional Quality-of-Service features.

In the following subsections an overview of the mobile communication systems will be presented.

2.3.1 Basic Concepts of Mobile Communications

Most mobile communication systems employ cellular concept. Cellular means that the network is divided into a number of geographical coverage areas named cells, as shown in Figure 2-20.

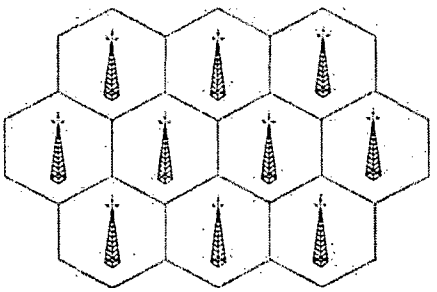


Figure 2-20: Cellular Network

A number of cells constitute Location Area (LA) or routing area (RA), depending on technology, LA for 2G whereas RA for 3G. Within each cell, there is a base station, which comprises the radio transmission and reception equipment. The base station provides the radio communication for those mobile terminals that happen to be within the cell. The connection from the

mobile to the base station is called uplink, whereas the connection from the base station to the mobile is called down link. The coverage area of a given cell depends on a number of factors such as the transmiting power of the base station, the height of the base station antennas, the topology of the landscape, the transmit power of mobile, and the number of expected users in that cell (smaller cells in densely populated areas). The coverage of the cell can range from 100 meters to several kilometers. Basically, a number of specific radio frequencies are allocated to a given cell and those same frequencies are reused in other cells that are sufficiently far away to avoid interference, although not in all systems.

In addition to the frequency reuse, cellular communication enables several key concepts to be employed, such as the following:

- Mobility of the users,
- Mobility management,
- Roaming,
- Paging.

Mobility implies that the users are able to move freely around the network and from one network to another while communicating. This requires that the network has to be kept informed of the approximate location of the user (mobile terminal), to be able to deliver an incoming call to that user in the corresponding cell and to maintain active calls. These tasks are performed by mobility management procedures known as location update and handover. Location update is the process of informing the network about the current location of the mobile user. Handover is the process of handing an active call from one cell to another. Roaming is the ability of mobile stations to access the network at different points of the network of the same or of a different network operator, which might even be in a different country. Paging is used to alert the destined user of the incoming call.

2.3.2 First Generation Mobile Communication Systems

Mobile communication networks started in the late 1970s, with the implementation of a trial network in Chicago in 1978. This network used a technology known as American Mobile Phone System (AMPS), operating in the 800 MHz frequency band. The commercial use of mobile communication networks started also in Chicago in 1983. Besides in North America, AMPS systems have also been deployed in South America, Asia, and Russia. In Europe the first mobile wireless communication system was NMT (Nordic Mobile Telephone) operating in the 450 MHz frequency band, which was deployed in Sweden, Norway, Denmark, and Finland in 1981. Later, a version of NMT was developed to operate in the 900 MHz frequency band, known as system NMT 900. NMT systems have been deployed throughout Europe, Asia, and Australia. In some very remote places NMT systems are still the only available system for mobile communications. The British introduced another technology in 1985, known as the Total Access Communication System (TACS), which operates in the 900 MHz frequency band. TACS is basically a modified version of AMPS. In addition several other national standards evolved and have been deployed throughout the world. All these systems are considered as analog systems and belong to the first-generation (1G) of mobile communication systems. It is important to note that mobile analog systems utilize digital signaling in many parts of their network, including the air interface. The analog reference applies to the method that the information content is transported without involving a codec.

2.3.2.1 Network Architecture

The basic architecture of a 1G network is shown in Figure 2-21. A 1G network is made up of many cell sites that all interconnect to the Mobile Telephone System Office/Mobile Switching

Center (MTSO/MSC). The cell site sends and receives the information to/from the mobile terminal and the MTSO/MSC.

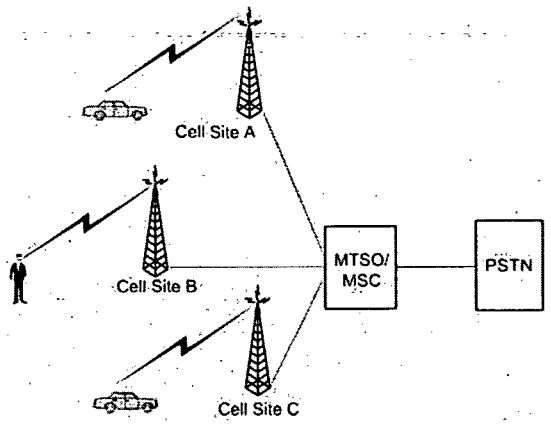


Figure 2-21: General Architecture of the 1G Systems

The mobile communicates to the cell site through the use of full-duplex radio channels. The cell site is connected to the MTSO/MSC either by leased T1/E1 lines or through a microwave system. The MTSO/MSC connects the cell site to the Public Service Telephone Network (PSTN). The MTSO/MSC performs a variety of functions involved with call processing and is effectively the brain of the network. It also maintains the individual subscriber records, the current status of the subscriber, call routing, and billing information. In general, first generation systems have been very successful and many of them are still in service, offering speech service only. However, 1G systems were developed with national scope and have several serious drawbacks such as incompatibility, limited capacity, very little protection against fraud, and they have little to offer in terms of advanced features.

2.3.3 Second Generation Mobile Communication Systems

The second-generation (2G) mobile communication systems are characterized by the employment of digital technology. The use of digital technology has a number of advantages, including increased capacity, greater security, and more advanced features. The fundamental issue with 2G is the utilization of digital radio technology for transporting the information content. Various types of second-generation mobile communication technologies have been developed. The three most successful systems are the European Global System for Mobile Communications (GSM) and two American standards, the Interim Standard 136 (IS-136) TDMA and IS-95 CDMA. The IS-136 is the digital standard based on TDMA technology and is operating in the same frequency band as AMPS. Several operators in the USA currently deploy the IS-136 standard. The CDMA IS-95 system uses a spread spectrum technology that enables multiple users to use the same radio channel at the same time. The CDMA channel utilized is reused in every cell of the mobile network. Many network operators in the United States and Asia have used and still use the IS-95 system. The GSM represents today's most successful digital mobile communication system in the world and is also the foundation of more advanced systems such as GPRS and UMTS. Not to forget is the Japanese Personal Digital Cellular (PDC) 2G system. PDC is confined to the Japanese market, being a proprietary technology developed and installed by NTT DoCoMo. However, the 3G systems in Japan will not be based on PDC but instead an air interface similar to UMTS will be adopted.

2.3.3.1 Global System for Mobile Communications - GSM

Back in the early 1980s, Europe was facing the problem of multiple incompatible analog mobile phone systems. To avoid incompatibility, in 1982, the European Standardization Organization, CEPT (European Conference of Postal and Telecommunications Administrations), established a

Group Special Mobile (GSM). In 1989, the newly created ETSI (European Telecommunication Standard Institute) finalized the specifications and renamed the standard to Global System for Mobile Communications, keeping the acronym GSM. The primary goal of GSM was to develop a pan European mobile phone standard that allows the roaming of users throughout Europe and provides voice services as well as other features and capabilities not possible with analog systems. The first version of the GSM network was deployed in Europe, in 1991, operating in the 900 MHz frequency band (890-915 MHz for the uplinks and 935-960 MHz for downlinks). Other versions comprise GSM at 1800 MHz (1710-1785 MHz uplink, 1805-1880 MHz downlink) also called DCS (Digital Cellular System) 1800, and the GSM system at 1900 MHz (1850-1910 MHz uplink, 1930-1990 MHz downlink) also known as PCS (Personal Communications Service) 1900, mainly deployed in the USA. GSM was very successful thanks to the following features: it offers full international roaming, automatic location services, authentication, encryption on the wireless link, efficient interoperation with ISDN systems, and relative high audio quality. Furthermore, a Short Message Service (SMS) with up to 160 alphanumeric characters and data service at 9.6 kbit/s have been integrated. GSM is deployed in most countries in Europe and also outside Europe.

GSM Network Architecture

The GSM network consists of three subsystems: the Radio SubSystem (RSS), the Network and Switching Subsystem (NSS), and the Operation SubSystem (OSS). Figure 2-22 shows the basic architecture of a GSM network, as specified by ETSI. The RSS and the NSS are connected via the A interface, whereas the connection to the OSS is done via the O interfaces. The A interface is typically based on circuit switched PCM-30 systems, whereas the O interface uses the Signaling System No. 7 (SS7). Each of the subsystems consists of several entities. The Radio Sub System (RSS) consists of the mobile terminal and the Base Station Subsystem (BSS). Mobile terminal in the GSM terminology is called Mobile Station (MS). An MS is composed of two independent parts: the handset itself, known as the Mobile Equipment (ME), and the Subscriber Identity Module (SIM). The ME consists of user independent hardware and software. The SIM is a small card, which is inserted into the ME and contains all user specific information, including the identity of the subscriber, subscriber authentication information, and some subscriber service information. GSM distinguishes between the identity of the subscriber and that of the mobile equipment. An ME is identified via the International Mobile Equipment Identity (IMEI) number, while the subscriber is identified by a International Mobile Subscriber Identity (IMSI) number and a Mobile Subscriber ISDN (MSISDN) number. The described MS architecture enables GSM to support two types of mobility: terminal mobility and personal mobility. Terminal mobility means to use a MS at different access points and in different networks in the case of roaming between different networks. Personal mobility is the capability of the mobile users to obtain network services by using a SIM card with different MSs. Thus, a user can personalize any MS using his SIM. An RSS comprises several BSSs, which perform all functions necessary to maintain radio connections to an MS. Each BSS contains several Base Tranceiver Stations (BTS), a Base Station Controller (BSC) and a Transcoding and Rate Adaptation Unit (TRAU). A BTS comprises all radio equipment necessary for radio transmission, such as antennas, signal processing, and amplifiers. The BTSs, communicates with MSs over the Um air interface. The BSC takes care of all the central functions and control of the radio subsystem. It provides a number of functions related to Radio Resource (RR) management, some functions related to Mobility Management (MM) for the subscriber in the coverage area of the BTSs, and a number of operation and maintenance functions for the overall RSS. All BTSs of a BSS are connected to BSC via an interface known as Abis-interface, which consists of 16 or 64 kbit/s connections. In a GSM network, speech compression is performed in both the MS and the TRAU. The speech from the subscriber is coded at either 13 kbit/s (full rate) or 12.2 kbit/s (enhanced full rate). Since the NSS interfaces with the PSTN network, the function of the TRAU is to convert the coded speech to or from standard 64 kbit/s.

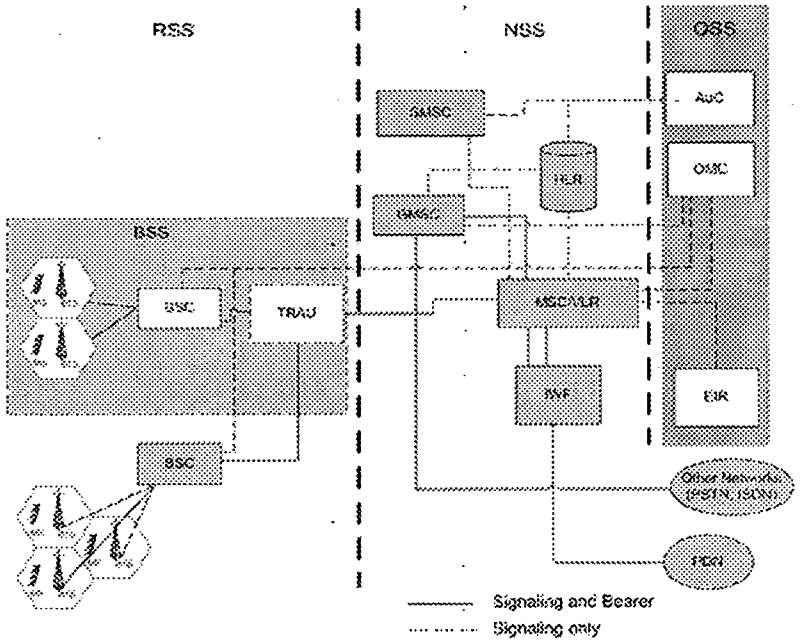


Figure 2-22: GSM Network Architecture

The NSS forms the fixed backbone network of a GSM system and it connects the RSS subsystem with public networks. The NSS comprises functions for the worldwide localization of users, handover, roaming of users between different network operators of different countries, it supports charging and accounting, The NSS consists of the Mobile Switching Center (MSC) switches and databases. MSC are high performance digital switches that control the call set up, call routing, call release, and handover of connections to other MSCs, using signaling system SS7. A MSC is connected to other MSCs and to several BSCs via the A interface, and manages these BSCs. A Gateway MSC (GMSC) is a MSC that has additional connections to other fixed networks, such as PSTN and ISDN. The main task of the GMSC is to query the Home Location Register (HLR) database to determine the location of the mobile user. Connection to Public Data Networks (PDN) is realized through the Interworking Function (IWF) module. The NSS has an additional entity called Short Message Service Center (SMSC), which stores and forwards short text messages sent to and from mobile users. The HLR is the most important database in a GSM system that contains permanent information for each mobile user such as the MSISDN number, subscribed services, authentication key, and current location area. Each subscriber is registered in one HLR The VLR (Visitor Location Register) is a dynamic database associated with each MSC that stores important subscriber specific information for the time a subscriber is in the coverage area of an MSC. If a new MS comes into an area the VLR is responsible for, it copies all relevant information for this user from the HLR. The Operation SubSystem contains all functions necessary for network operation and maintenance. It consists of the following entities: Operation and Maintenance Center (OMC), Authentication Center (AuC), and Equipment Identity Register (EIR). The OMC monitors and controls all network entities. The AUC is associated with HLR and it is concerned with protecting user identity and data transmission. It contains the algorithm for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR. The EIR is a database for all IMEIs and it contains a list of valid IMEIs, malfunctioning devices and a black list of stolen mobiles, for a particular network.

GSM Air Interface

The GSM system implements combination of FDMA and TDMA multiple access scheme at Um, so that multiple carriers or Radio Frequency (RF) channels are used on a time-sharing basis. A given frequency band is divided into 200 kHz frequency bands with a carriers frequency in the middle of the each band, for both uplink and downlink directions. In GSM 900, 124

channels are used for FDMA, DCS 1800 has a maximum of 374, and PCS 1900 has a maximum of 299 channels. A given cell can have multiple RF carriers, depending on the traffic load. In a normally loaded system, typically one to three carriers are allocated, whereas in an area of very high traffic demand as many as six carriers might exists in a cell. Air interface uses a sophisticated hierarchical framing structure consisting of frames, multiframes, superframes, and hyperframes, shown in Figure 2-23.

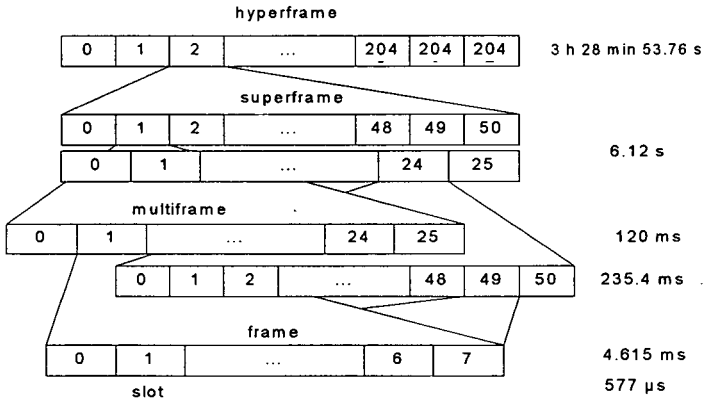


Figure 2-23: Framing Structure of the GSM System

Each RF carrier is divided into eight time slots, numbered 0 to 7, which constitute a frame. Each frame lasts approximately 4.615 ms, so that each time slot lasts about 577 µs. A time slot within a frame represents a physical TDM channel. The same slot is used for uplink and downlink communication but they are shifted for the three slots time. In addition to physical channels, GSM specifies two basic groups of logical channels: Traffic Channels (TCHs) and Control Channels (CCHs). Depending on the number of RF carriers in a given cell, all eight timeslots on a given carrier might be used to carry user traffic, such that a maximum of eight simultaneous users-TCHs can be accommodated. There must be, however, at least one timeslot in a cell allocated for control channel purposes. Thus if only one carrier is in a cell, then there is a maximum of seven TCHs. Traffic and control channels are mapped to physical channels based on the hierarchical framing structure of GSM. Due to space limits, logical channels and the mapping scenarios to physical channels are not presented in this thesis.

GSM Protocol Architecture

In a GSM network, an extensive signaling is required between the mobile station and the network, as well as between the various network elements, far beyond the amount of signaling that fixed networks use. Figure 2-24 shows the layered protocol architecture for signaling in the GSM system.

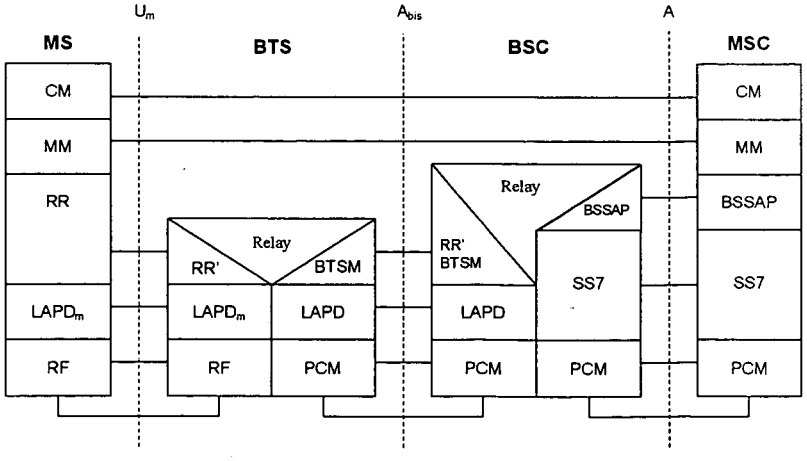


Figure 2-24: Protocol Architecture of the GSM System

The physical layer at the Um interface handles all radio specific functions. Data transmission at the physical layer at the A and A_{bis} interfaces is typically done using PCM leased lines. For layer two signaling, the LAPD (Link Access Protocol for the D channel) protocol has been used at the A_{bis} interface, whereas the $LAPD_m$ protocol has been defined at the Um interface. For signaling between a MSC and a BSC, the signaling system SS7 is used. This protocol is also used to transfer all management information between MSCs, HLR, VLRs, AuC, EIR, and OMC. The network layer consists of three sublayers. The lowest sublayer is the Radio Resource (RR) management. Only a part of this sublayer, RR', is implemented in the BTS, the remainder is implemented in the BSC. The functions of the RR' are supported by the BSC via the BTS Management (BTSM) protocol. The main task of RR is setup, maintenance, and release of radio channels. Mobility Management (MM) contains functions for registration, authentication, identification, location updating, and the provision of a Temporary Mobile Subscriber Identity (TMSI) that replaces the IMSI in order to hide the real identity of an MS user over the air interface. The Call Management (CM) layer contains three entities: Call Control (CC), Short Message Service (SMS), and Supplementary Service (SS). SMS allows for message transfer. The SS offers supplementary services such as user identification, call redirection, or forwarding of ongoing calls. The CC provides a point-to-point connection between two terminals and is used from higher layers for call establishment; call clearing and change of call parameters. The BSS Application Part (BSSAP) protocol is used for communication between the MSC and the BSC, and also between the MSC and the MS. Since the MSC communicates separately with both the BSC and the MS, the BSSAP is divided into two parts the BSS Management Application Part (BSSMAP) and the Direct Transfer Application Part (DTAP). The BSSMAP contains those messages that either originated from the BSS or need to be acted upon by the BSS. The DTAP contains those messages that are passed transparently through the BSS from the MSC to the MS or vice versa.

GSM Services

GSM has been design for voice services and these services still are the main use of GSM, although there has been a great increase in uses of the SMS. In addition GSM offers a circuit-switched symmetric data service up to 9.6 kbit/s between the network and the MS. At the time GSM systems were deploying 9.6 kbit/s was more than sufficient for existing data services. In recent years, a new coding scheme has been approved that takes this data rate to 14.4 kbit/s. However, in the todays Internet, such data rates are considered very slow to provide high-speed access to Internet services such as e-mail and the World Wide Web (WWW). Also, the use of circuit-switched connections is not an efficient way of carrying the bursty traffic of these types of services. Hence, several solutions, as upgrades to GSM, known as 2.5G and 3G technologies were proposed to provide high mobile data rates to satisfy user needs.

2.3.4 The 2.5 Generation Mobile Communication Systems

The second and a half generation or 2.5G mobile communication systems are considered as interim technologies between 2G and 3G systems. The 2.5G systems have many enhancements over the 2G systems. These enhancements are mainly based on the use of packet switched technology and on offering higher data rates than the existing 14.4 kbit/s of 2G systems. There are several systems referred to as 2.5G, such as HSCSD (High Speed Circuit Switched Data), GPRS (General Packet Radio System), EDGE (Enhanced Data Rates for GSM Evolution), and CDMA 2000 phase 1. The HSCSD is a circuit switched technology that uses the same 200 kHz channel and eight-timeslot frame structure as used in GSM. HCSD provides higher data rates by using multiple timeslots. If four timeslots are used, with 14.4 kbit/s each, data rates of up to 57.6 kbit/s are provided. The GPRS, in contrast to HCSD, is a packet switched technology which offers higher data rates. Like in HCSD, higher data rates are achieved by using multiple timeslots in the GSM eight-timeslot frame. Theoretically, it can support data rates of up to 170 kbit/s. GPRS is the foundation for the 3G UMTS system and will be presented in more detail in

the following subsections. The EDGE system aims to increase data rates offered by the GSM and GPRS system. EDGE also uses the same 200 kHz channel and eight-timeslot frame structure as used in GSM and GPRS. Higher data rates are based on new modulation scheme applied in the air interface. Instead of Gaussian Minimum Shift Keying (GMSK) scheme used in GSM, EDGE uses the 8 Phase Shift Keying (8 – PSK). When this modulation technique is combined with a new channel coding and multiple timeslot use, data rates up to 384 kbit/s can be achieved. The CDMA2000 (phase 1) is a step-stone to 3G CDMA2000. It is fully backward compatible with the IS-95 system and is meant to upgrade it from a voice system to a high data rate packet network. It also supports all of the IS-95 existing services such as voice, SMS, and circuit switched data.

2.3.4.1 General Packet Radio Service - GPRS

The GPRS system can be considered as an extension to the GSM system aiming to provide efficient packet-switched services at higher data rates for typical Internet applications. The biggest advantage of GPRS over GSM is the employment of packet-switching technology. GPRS provides packet data channels on the air interface as well as a packet data switching and transport network. This means that a given user consumes network resources only when receiving or sending data. This is a very important feature that enables efficient use of the scarce radio resources. Furthermore, GPRS offers the possibility to use asymmetric connections when required and thus the network resources are utilized even better. Although GPRS does not offer the high bit rate services envisioned for 3G, it is an important step in that direction. The initial UMTS system reuses a great deal of GPRS functionality, as we shall see in the next section. Therefore, understanding of GPRS is a good foundation to understand UMTS.

GPRS Network Architecture

The GPRS network architecture is an extension of the GSM architectures with several new network elements and a number of new interfaces, as shown in Figure 2-25.

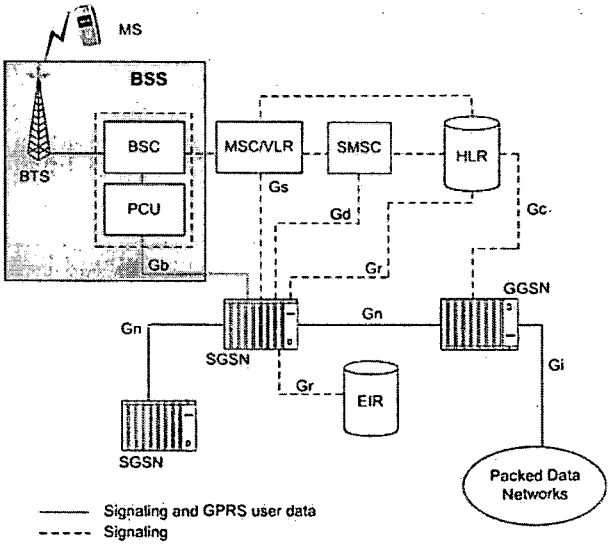


Figure 2-25: GPRS System Architecture

In particular, the GPRS architecture introduces two new network nodes, which are called Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN). The SGSN interfaces between the GPRS backbone and the radio access network and is analogous to the MSC/VLR in the circuit switched domain. The SGSN performs a number of functions such as the delivery of data packets from and to the mobile stations within its service area, mobility management, logical link management, security, charging, and access control. The service area of an SGSN is divided into Routing Areas (RA), which are analogous to Location Areas (LA) in

the circuit-switched domain. When a GPRS MS moves from one RA to another, it performs a routing area update. The SGSN may serve multiple BSCs, whereas a given BSC interfaces with only one SGSN. The interface between the SGSN and the BSC is the Gb interface, which is used to pass control information as well as user data traffic to or from the SGSN. The direct logical interface is also used between an MS and an SGSN for signaling and for packet data transfer, even though the interfaces pass physically through the BSS. A SGSN is connected to a MSC via the Gs interface. This is an optional SS7 based interface. The purpose of the Gs interface is to enable coordination between an MSC/VLR and a SGSN for those subscribers that support both voice services controlled by the MSC/VLR and packet data services controlled by the SGSN. The SGSN interfaces to a HLR via the Gr interface. This is an SS7 based interface, which is used by the SGSN to provide the location update to the HLR for GPRS subscribers and to retrieve GPRS-related subscription information for any GPRS subscriber that is located in the service area of the SGSN. A SGSN may interface with other SGSNs on the network via the Gn interface. This allows the SGSNs to exchange user profiles when a mobile station moves from one SGSN area to another as well as the tunneling of packets from an old SGSN to a new SGSN. Across the Gf interface, the SGSN may query the EIR for the IMEI of a mobile station trying to register with the network. The SGSN interfaces with a Short Message Service Center (SMSC) via the Gd interface, which is an SS7-based interface. This interface enables the GPRS subscriber to send and receive short messages over the GPRS air interface and GPRS network. The Gateway GPRS Support Node (GGSN) provides the interface towards the external IP and X.25 networks as well as to other GPRS networks. The GGSN performs several functions such as routing, address and protocol conversion, authentication, and charging. It converts the GPRS packets coming from the SGSN into the appropriate Packet Data Protocol (PDP) format for IP or X.25 networks and sends them out on the corresponding packet data network. In the other direction, addresses of incoming data packets are converted to the GSM address of the destination user. The readdressed packets are sent to the responsible SGSN. A given SGSN may interface with one or more GGSNs and may route its packets over different GGSNs to reach different packet data networks. The interface between an SGSN and GGSN is IP based interface named the Gn interface. In general, all GSNs are connected via an IP-based GPRS backbone network. A GGSN may also optionally use the Gc interface to an HLR when a GGSN needs to determine the SGSN currently serving a subscriber. From the external IP network's point of view, the GGSN is seen as an ordinary IP router owning all IP addresses of the mobile stations served by the GPRS network. The GGSN is connected to external networks via the Gi interface. An additional new network element in the GPRS architecture is the Packet Control Unit (PCU). In fact, the PCU is a logical network element that is responsible for a number of GPRS-related functions such as the air-interface access control, packet scheduling on the air interface, and packet assembly and re-assembly.

GPRS Air Interface

GPRS uses the same frequency bands and the same TDMA/FDMA structure at the air interface as GSM. An MS can access more than one time slot, hence higher bit rates are available to the user. Furthermore, GPRS enables that for a given 200 kHz carrier some of the eight timeslots at a given instant carry GSM traffic while some are carrying GPRS data. In addition, GPRS enables on demand allocation of resources, thus a given timeslot may be used for standard voice traffic and subsequently for GPRS data traffic, depending on the traffic type demands. On top of the physical channels a number of new logical channels, named Packet Data Channels (PDCH), and their mapping onto physical channels have been defined. Packet Data Channels are grouped, like in GSM, into two categories: traffic channels and control channels. Traffic channels known as Packet Data Traffic Channels (PDTCH) are used for the transfer of actual user data over the air interface. One mobile station can use up to eight PDTCHs simultaneously. All PDTCH are unidirectional, either uplink or downlink. GPRS also defines a large number of control channels that are used for signaling, broadcast of general system information, synchronization, channel assignment, and paging.

GPRS User Terminals

The user terminal is equipped with the GPRS protocol stack and is the means of connecting the user to the GPRS network. Three classes of user terminals have been defined in the GPRS system: A, B and C.

- Class-A terminals are able to support circuit switched and packet switched services simultaneously and independently of each other.
- Class-B terminals handle one service at the time circuit switched or packet switched but have the possibility for automatic switching between the two services.
- Class-C terminals must be manually set to either circuit switched service or packet switched service. When the terminal is attached to the circuit switched service than it is unreachable for the packet-switched service and vice versa.

GPRS Protocol Architecture

There are two protocol planes introduced in GPRS: the transmission plane and the signaling plane. The transmission plane consists of protocols for user data transmission and its associated control procedures like flow control, error detection, and error correction. The signaling plane comprises protocols that control and support the transmission of the user information. Figure 2-26 shows the protocol architecture of the transmission plane for GPRS.

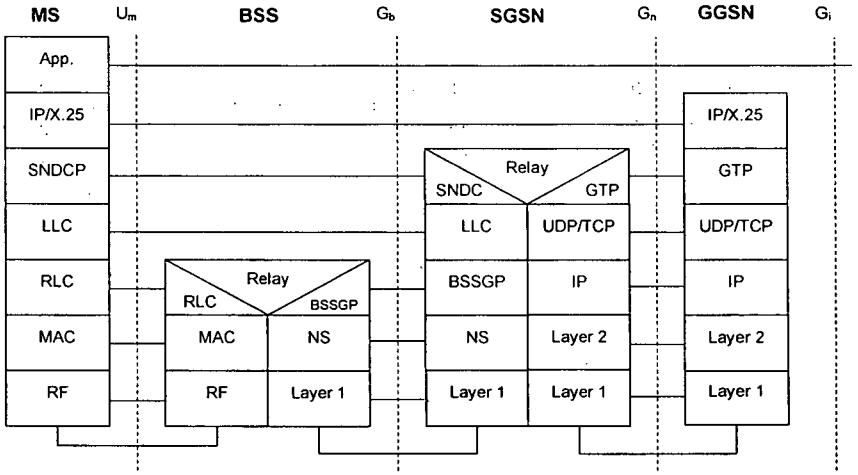


Figure 2-26: GPRS Protocol Architecture of the Transmission Plane

All data within the GPRS backbone is transferred using the GPRS Tunneling Protocol (GTP). The GTP utilizes either TCP or UDP transport protocols, depending on whether a reliable transmission is needed (for X.25 packets) or not (for IP packets). The IP protocol is used as a network protocol for the GPRS backbone. In order to support the different characteristics of the underlying networks, the SubNetwork Dependent Convergence Protocol (SNDCP) is used between a SGSN and the MS. SNDCP also provides data compression and header compression to improve channel efficiency. The Logical Link Control (LLC) protocol operates across the Um and the Gb interfaces, providing a highly reliable logical link for packet transfer between MS and SGSN. Its functionality is based on the well-known LAPD (HDLC) protocol and includes ciphering, flow control, sequence control, detection of transmission errors, and retransmission (ARQ). Any data between the MS and SGSN is sent in Logical Link Protocol Data Units (LL-PDUs). Below the LLC there is the Base Station Subsystem GPRS Protocol (BSSGP), which is used to convey routing and QoS related information between the BSS and SGSN. The underlying Network Service (NS) protocol is based on the Frame Relay protocol. At the BSS, a relay function relays LL-PDUs from the Gb interface to the Um interface. Similarly, at the SGSN, a relay function relays PDP- PDUs (Packet Data Protocol - Protocol Data Units) between the Gb interface and the Gn interface. The RLC/MAC protocol layer, located in the BSS (PCU), pro-

vides services for the transfer of LLC PDUs using a shared medium between multiple MSs and the network. The function of RLC includes segmentation and reassembling of LLC PDUs. The MAC protocol realizes the different logical channels needed to share the common transmission medium by several MSs. It allows one MS to use several physical channels in parallel, but also the multiplexing of several MSs over one physical channel. The physical layer between MS and BSS is divided into two sublayers: the Physical Link Layer (PLL) and the Physical RF Layer (PRFL). The PLL provides a number of physical channels to the RLC/MAC layer. Its tasks include channel coding, Forward Error Correction (FEC), interleaving, monitoring of radio link signal quality, and power control procedures. The lowest level on the Um interface, the PRFL, performs the transmission and reception of modulated waveforms on the carrier frequencies.

The protocol architecture of the signaling plane consists of protocols for control and support of the functions of the transmission plane, such as GPRS attach and detach, control of routing paths, and allocation of network resources. Attach is the procedure that the MS performs to inform the GPRS network, specifically the SGSN, that the MS is available for packet traffic. Detach is the procedure of disconnection of the MS from the GPRS network. Figure 2-27 shows the signaling plane from the MS to the SGSN. At the lower layers, it is identical to the transmission plane. However, at the higher layers, the GPRS Mobility Management and Session Management (GMM/SM) protocol (instead of the SNDCP) is defined. This protocol supports mobility management, session management, and security functions.

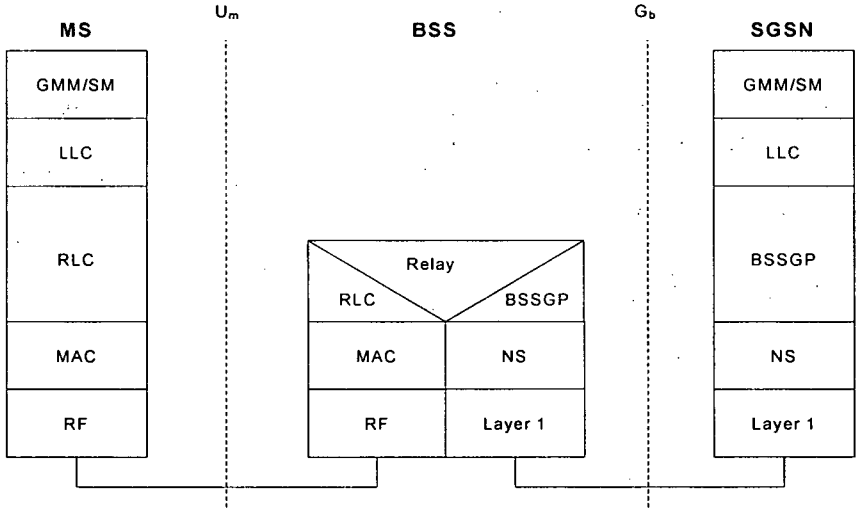


Figure 2-27: Protocol Architecture of the GPRS Signalling Plane

GPRS Services

GPRS has been designed to provide packet data services at higher speeds than those available with standard GSM circuit-switched data services. In theory, GPRS could provide speeds of up to 170 kbit/s, though such speeds are never achieved in real networks. In fact, the practical maximum is actually a little over 100 kbit/s, with speeds of about 40 kbit/s or 53 kbit/s being more realistic. However, such speeds are much higher than the 9.6 kbit/s provided by GSM. From the service point of view, GPRS starts a development path where more and more traditional circuit switched services are converted to be used over GPRS because those services were originally more suitable for packet switched connections. GPRS has an important role to play in bringing evolved messaging services to the market. In general, GPRS supports the following packet based services: interactive services, web browsing, email with file attachments, file transfer, transactions, m-commerce applications, and instant messaging. All these services can be used parallel to conventional services. GPRS also supports a QoS concept, by allowing users to specify a QoS profile. Because GPRS is a packet-switched technology, network providers could support charging on volume and not connection time as it is done for circuit-switched services.

2.3.5 Third Generation Mobile Communication Systems

The third generation (3G) mobile systems have been developed to meet increasing demands for high-speed data communication in the current environment of the Internet and mobile multimedia services. The need for third generation mobile communication technology was recognized as far back as the 1980s. The ITU (International Telecommunication Union) was heavily involved and the work within the ITU was originally known as Future Public Land Mobile Telecommunication Systems (FPLMTS), later renamed to International Mobile Telecommunication 2000 (IMT-2000). The IMT-2000 effort within the ITU has resulted in a number of specifications, which address areas such as: global standardization, worldwide roaming capability, multimedia services and terminals, and high-speed data rates. To address the technical solutions, the ITU has solicited technical proposals for air interface from interested standard bodies and organizations, to meet the requirements laid down for IMT-2000. As a response a number of technical solutions were submitted for air interface technologies, including both TDMA and CDMA (with both FDD and TDD modes) technologies. From several of the IMT-2000 proposed technologies the WCDMA and CDMA2000 were the most successful ones, as the vast majority of wireless operators are planning to utilize one of these two technologies.

The 3G system in Europe is known under the name UMTS (Universal Mobile Telecommunication Services). In early 1988, ETSI decided to select WCDMA using FDD as its UMTS radio technology. The GSM/GPRS core network was selected for the development of the UMTS core network technology. In Japan, a WCDMA solution was also proposed, with both TDD and FDD modes. In Korea, two different types of CDMAs were proposed - one similar to the European and Japanese proposals, and one similar to a CDMA proposal being considered in North America - CDMA2000. The CDMA2000 is an evolution of IS-95 CDMA. The system architecture of a CDMA2000 network is a logical extension of the IS-95 CDMA network with the fundamental difference being the introduction of packet data services. Furthermore, it is expected that CDMA2000 will be able to interoperate with WCDMA. Since a number of standardization groups were working on very similar technologies, for unification of the efforts, two common project groups were created: the Third Generation Partnership Project (3GPP) and the Third Generation Partnership Project 2 (3GPP-2). The 3GPP was created in the beginning of 1988, with the aim to produce open specifications for the 3G/UMTS system, by the following six regional standards bodies:

- ETSI (European Telecommunication Standard Institute) – Europe,
- ARIB (Association of Radio Industries and Business) – Japan,
- CWTS (China Wireless Telecommunication Standard group) – China,
- T1 (Standardization Committee T1 – Telecommunications) – US,
- Telecommunication Technology Association (TTA) – Korea,
- Telecommunication Technology Committee (TTC) - Japan.

The 3GPP2 was founded, almost one year later, at the initiative of the American Standard Institute (ANSI) and it involved the following regional standards bodies: TIA (Telecommunication Industry Association)/USA, ARIB, TTC, TTA, and CWTS. The 3GPP2 has the task to create specifications for the CDMA2000 system.

In the following section an overview of the 3GPP UMTS mobile system will be presented.

2.3.5.1 Universal Mobile Telecommunication Services – UMTS

The 3GPP specifications for UMTS are known by the common name of 3GPP Releases. The first release of specifications from 3GPP is known as 3GPP Release 1999. In 3GPP R99 the major changes were targeted at the radio access network, including a totally new wideband air interface. At the core network the aim was to minimize changes and utilize the existing GSM/GPRS network elements and functionalities as much as possible. The next Release named

3GPP Release 4 (3GPP R4) focuses on changes to the architecture of the core network circuit switched domain. The main changes are related to the separation of user data flows and their control mechanisms. The next step of the 3GPP in the UMTS evolution is the introduction of 3GPP Release 5 (3GPP R5). The 3GPP R5 aims to introduce a UMTS where the transport network utilizes IP networking as much as possible. IP and overlaying protocols will be used in network control too and also the user data flows are expected to be mainly IP based. The 3GPP R4/R5 will also start to utilize the possibility for new radio access technologies derived from GSM. The Enhanced Data for GSM Evolution (EDGE) will be specified to create the GSM/EDGE Radio Access Network (GERAN) as an alternative to building a UMTS mobile network. A further step of 3GPP specifications is Release 6, which focuses on specifications for the Internet Multimedia System (IMS).

3GPP Release 1999 Network Architecture

Like in most mobile communication networks, the network architecture of UMTS can be split into two main parts: the Radio Access Network (RAN) and the Core Network (CN), as shown in Figure 2-28. The radio access network of UMTS is known as UTRAN (UMTS Terrestrial Radio Access Network). The UMTS user device is called User Equipment (UE) and it contains two separate parts: the Mobile Equipment (ME) and the UMTS Subscriber Identity Module (USIM). The ME is the radio terminal used for radio communications and the USIM is a smart card that holds subscriber specific data, plus security keys. It is similar to the SIM in GSM. The UE connects to UTRAN via the Uu air interface. This is an open interface, which in UMTS is physically realized with WCDMA technology. The UMTS 3GPP Release 1999 uses the basic core network architecture defined for GSM/GPRS, with some enhancements. In most vendor implementations, many of the network elements are being upgraded to simultaneously support GSM/GPRS and UMTS radio access networks. Such network elements include the MSC/VLR, the HLR, the SGSN, and the GGSN. Though the names of the elements are the same as in GSM/GPRS, their functionality is not. Furthermore, the UMTS specifications also include the support for a hard handover from UMTS to GSM and vice-versa.

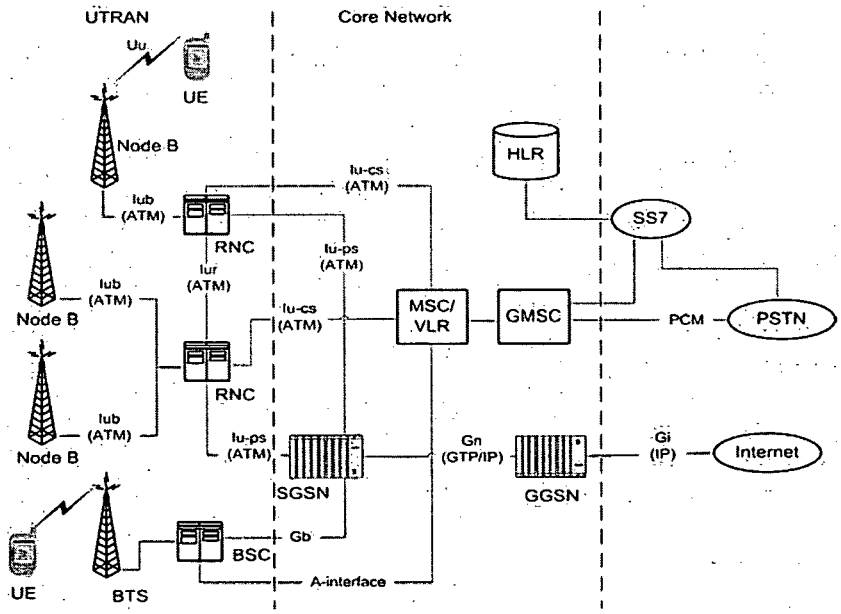


Figure 2-28: 3GPP Release 99 Network Architecture

In the UMTS 3GPP Release 99, like in GSM/GPRS, the traffic will be both circuit switched and packet switched. In order to satisfy requirements of both traffic types the CN is functionally divided into two domains, Circuit Switched (CS) domain and Packet Switched (PS) domain. The CN CS domain is evolved from GSM and is responsible for circuit switched traffic man-

agement. The CS domain has two basic network elements: the MSC/VLR and GMSC. The PS domain is evolved from GPRS and this can be seen from the inherited interface names always starting with G and having another letter indicating which interface is in question. The PS domain has also two mobile network specific elements, SGSN and GGSN and is responsible for packet switched traffic management. Since the most considerable new development of UMTS is related to the radio access network, a short overview of UTRAN will be presented in the next subsection.

UTRAN Architecture

The UMTS Radio Access Network (UTRAN) consists of Radio Network Subsystems (RNS). Each RNS contains a set of base stations and one Radio Network Controller (RNC). The UTRAN architecture is shown in Figure 2-28 as it applies to the first release of UMTS specification 3GPP Release 1999. In 3GPP specifications, the base station is known as Node-B. The main task of a Node-B is to establish the physical implementation of the Uu air interface and the implementation of the Iub interface towards the RNC by utilizing the protocol stacks specified for these interfaces. The Iub is a fully standardized open interface, which means that a network operator could acquire Node-Bs from one vendor and RNCs from another vendor. A Node-B is connected to a single Radio Network Controller. The RNC controls the radio resources of the Node-Bs that are connected to it and is analogous to the GSM Base Station Controller (BSC). RNCs are also connected to each other through an open interface named Iur. The primary purpose of this interface is to support inter-RNC mobility and soft handover between Node-Bs connected to different RNCs. The Iur interface carries both signaling and traffic information. The UTRAN is connected to the core network via the open interface named Iu. The Iu interface, has two different components: the Iu-Cs interface and Iu-Ps interface. The Iu-Cs interface connects a RNC to a single MSC/VLR and supports circuit-switched services. The Iu-Ps interface connects a RNC to an SGSN and supports packet-switched services. In 3GPP Release 1999, all of the interfaces within UTRAN, as well as the interfaces between UTRAN and the core network, use ATM as the transport mechanism.

UMTS Air Interface

UMTS air interface is implemented with Direct-Sequence Wideband CDMA (DS-WCDMA) technology. There are two versions of the air interfaces based on DS-WCDMA. One version uses FDD and the other uses TDD mode. A DS-WCDMA technology means that user data is spread over a much wider bandwidth through multiplication of each bit of data by a sequence of pseudo-random bits called chip code. The bit rate of the chip code (chip rate) in WCDMA is 3.84×10^6 chips/second. This value is constant for all WCDMA variants used in 3G networks. For simplicity, the name WCDMA is used as a synonym of DS-WCDMA. In the WCDMA FDD option paired 5 MHz carriers are used in the uplink and downlink. For uplink frequencies of 1920-1980 MHz are used, whereas for downlink 2110-2170 MHz. Thus, for FDD mode the separation of 190 MHz exists between uplink and downlink. The FDD solution is expected to see the greatest deployment – particularly in Europe and the Americas. The TDD variant of the WCDMA uses a frequency band located in both sides of the WCDMA-FDD uplink. The lower frequency band offered for the TDD variant is 20 MHz and the higher one is 15 MHz. Thus, a number of frequencies have been defined, including 1900 MHz to 1920 MHz, and 2010 MHz to 2050 MHz. Of course, the given carrier is used in both the uplink and the downlink so that no separation exists. The TDD is expected to see deployment primarily in Asia. In the following text, we will focus only on the FDD option (referred as WCDMA). The WCDMA contains a frame structure, which is divided into 15 slots, each of length 2/3 ms and thus the frame length is 10 ms, as shown in Figure 2-29. Based on this, one WCDMA frame is able to handle 38400 Chips. Hence, one slot in the WCDMA frame contains 2560 Chips (38400 Chips / 15 slots). Unlike GSM, WCDMA does not contain any hierarchical frame structure. Instead, WCDMA frames are numbered by an SFN (System Frame Number). An SFN is used for the internal syn-

chronization of UTRAN and the timing of information transmission. An important capability of WCDMA is that user data rates do not need to be fixed. In fact, within a frame the user data rate is fixed but the user data rate can change from frame to frame, this means that WCDMA can offer bandwidth on demand.

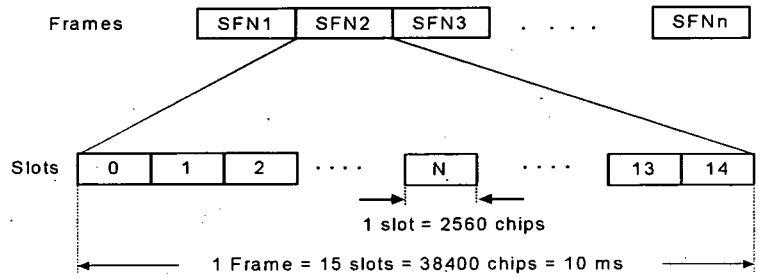


Figure 2-29: Frame Structure of the WCDMA

WCDMA Radio Channels

Many different channel types exist in WCDMA, which use a 10-ms frame structure. The content of each frame and of the each slot is dependent upon the type of channel in question. The WCDMA uses a three-layer logical hierarchy channel organization, shown in Figure 2-30. There are physical channels, transport channels and logical channels. The physical channels form the physical existence of the Uu interface between the UE and Node-B. A physical channel is what carries the actual data or control information over the air interface. A number of different physical channels are used in the uplink, with a given type of channel selected according to what the UE is attempting to do, such as simply requesting access to the network, sending a single burst of data, or sending a stream of data. A number of physical channels exist only for the correct operation of the physical layer. Information from upper layers is passed to the physical layer through a number of transport channels. These transport channels are mapped to a number of physical channels on the air interface, and the physical element that does the mapping is the Node-B. In general, two types of transport channels exist: the common transport channels and dedicated transport channels.

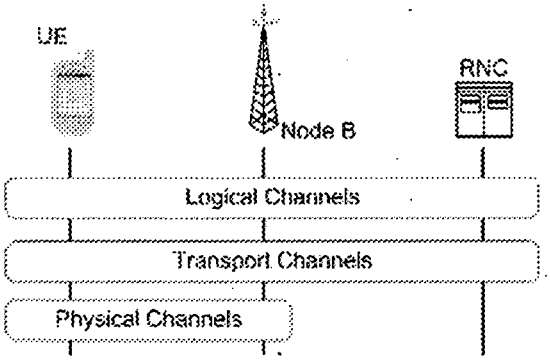


Figure 2-30: WCDMA Channel Types and their Location in UTRAN

Logical channels contain user data and information related to different tasks that the network and the terminal should perform in different moments of time. The logical channels are mapped to transport channels. While transport channels relate largely to the manner in which the information is transmitted, logical channels are characterized by what type of data is transported over them. Basically, two groups of logical channels exist: Control channels and traffic channels. Control channels are used to transmit control information, whereas traffic channels are used to transmit user data. There are four kinds of control channels and two kinds of traffic channels.

3GPP Release 4 Network Architecture

3GPP Release 4 introduces significant changes to the circuit switched domain of the core network architecture. The main changes are related to the separation of user data flows and their control mechanisms for the Core Network (CN) Circuit Switched (CS) domain. Figure 2-31 shows the basic network architecture for 3GPP Release 4. The MSC in the CN CS domain evolves into the MSC server and the Media Gateway (MGW). The MSC server contains all the mobility management and call control logic that would be contained in a standard MSC. The MGW contains the mechanisms to perform the actual switching and network interworking functions. It also performs circuit packet conversions in the case of VoIP calls. The MGW is controlled by the MSC server and can be placed remotely from the MSC server. One MSC server may control numerous MGWs, this means that the CN CS domain is scalable. Control signaling for circuit-switched calls occurs between the RNC and the MSC server, whereas, the media path for circuit-switched calls is between the RNC and the MGW. Typically, an MGW will take calls from the RNC and routes those calls towards their destinations over a packet backbone. In many cases, that packet backbone will be IP-based. At the remote end another MGW, controlled by a Gateway MSC server (GMSC server), is needed to handover calls to another network, such as the PSTN. This MGW will convert the packetized voice to standard PCM for delivery to the PSTN. It is only at this point that transcoding needs to take place. This results in significant bandwidth savings on the backbone network. In the CN PS domain, the packet data traffic from the RNC is passed to the SGSN and from the SGSN to the GGSN over an IP backbone. Many of the protocols used within the core network are packet-based, using either IP or ATM. Given that data and voice can both use IP transport within the core network, a single IP backbone can be constructed to support both types of services. This will result in capital savings in comparison to having separate packet and circuit switched backbone networks. The UMTS 3GPP Release 4 network interfaces with traditional networks via media gateways whereas with standard SS7 networks through the SS7 gateway (SS7 GW).

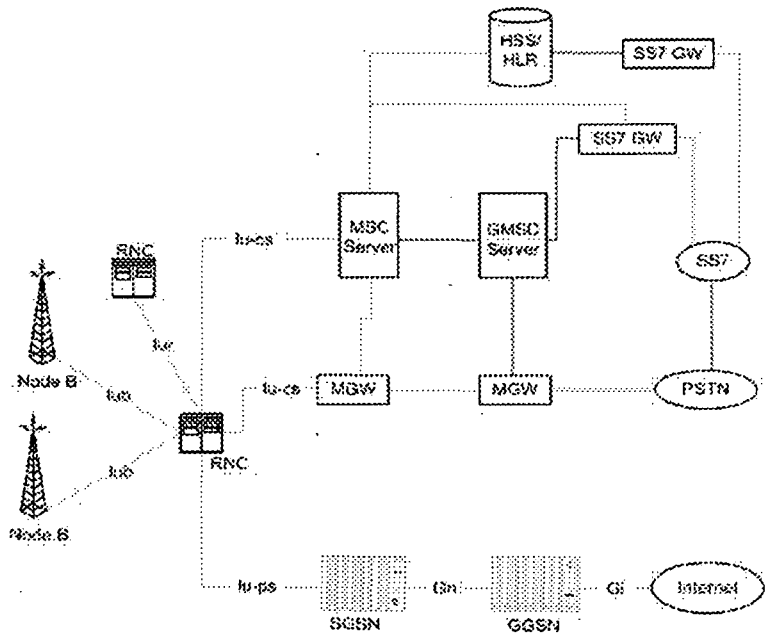


Figure 2-31: 3GPP Release 4 Network Architecture

From the Communication Management (CM) point of view, the main issue is how to implement the connection between the UE and MSC server, between the MSC server and MGW, and with which control protocol. There are several alternatives, but one of the most attractive protocols to implement call control protocols is the IP based Session Initiation Protocol (SIP). It is natural that when the traffic transport is IP based, that traffic control should also be IP based.

3GPP Release 5 All-IP Network Architecture

The IP-based technology has proved to be very successful in internetworking different networks and making a global communication network. The final goal is an all-IP global network from end-to-end, meaning IP up to the user. In this all-IP world, IP is run over all kinds of access networks – wireless or fixed - as well as core networks and Intranets, offering to users IP connectivity any time and anywhere. Namely, all-IP network technology includes: Integration of mobile communications and the Internet, packet transport using IP protocols, IP-based call control protocols; IP client enabled terminals; and IP-capable radio access networks. The 3GPP Release 5 aims to introduce all-IP multimedia network architecture to the UMTS network, as shown in Figure 2-32. This step in the UMTS evolution includes essential changes in the call model. Both voice and data calls are handled in the same manner all the way from the user terminal to the destination.

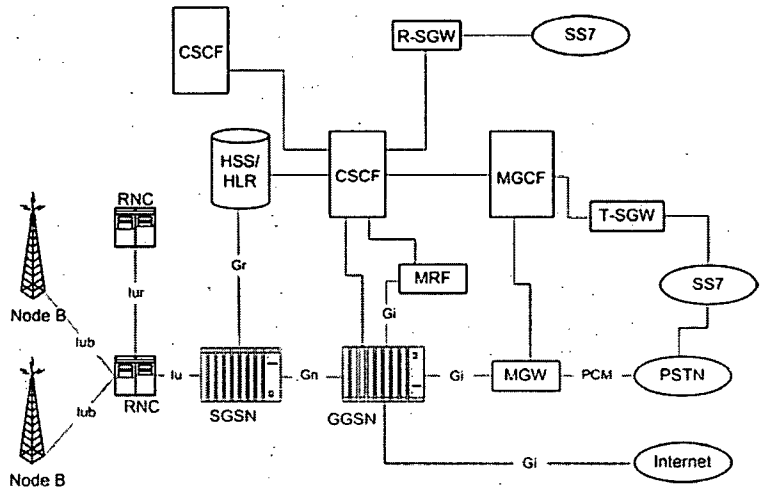


Figure 2-32: 3GPP Release 5 Network Architecture

As can be seen in Figure 2-32, there is only a single Iu interface that can carry voice and data traffic, as well as other media. Within the core network, the SGSN and GGSN are enhanced versions of the same nodes used in GPRS and UMTS Release 1999 and Release 4. The difference is that these nodes, in addition to data services, now support services that have traditionally been circuit-switched such as voice. Consequently, appropriate QoS capabilities need to be supported either within the SGSN and GGSN or in the routers immediately connected to them. The MGW in the 3GPP release 5 is connected to GGSN and has the same functions as the equivalent MGW within the 3GPP Release 4 architecture. It performs interworking with external networks at the media path level. The Transport Signaling Gateway (T-SGW) and the Roaming Signaling Gateway (R-SGW) are SS7 Gateways. The T-SGW provides SS7 interworking with standard external networks such as the PSTN. The R-SGW provides signaling interworking with legacy mobile networks that use standard SS7 signaling. It should be noted that the Release 5 all-IP architecture is an enhancement to an existing Release 1999 or Release 4 network. It is effectively the addition of a new domain to the core network – the IP Multimedia (IM) domain. The IM domain consists of the Multimedia Resource Function (MRF), the CSCF (Call State Control Function), and the Media Gateway Control Function (MGCF). The MRF is a conference bridging function used to support features such as multi-party calling and meet me conference service. The CSCF manages the establishment, maintenance, and release of multimedia sessions to and from the UE. The MGCF controls the MGW and also communicates with the CSCF. The new IM domain uses the services of the PS domain for transport purposes. All IM traffic is packet based and is transported using PS-domain nodes such as the SGSN and GGSN, and interfaces that belong to the PS domain. The IM domain is based on the Session Initiation Protocol (SIP). The IM architecture enables voice and data calls to be carried over IP all the way from UE to the destination. This convergence of voice and data enables a number of new ad-

vanced services. Moreover, the use of SIP means that a great deal of service control can be placed in the UE rather than the network, making it easier for the subscriber to customize services to meet his particular needs. An important aspect of the all-IP architecture is the fact that the user equipment is greatly enhanced as significant logic is placed within the UE. In conclusion, the UMTS network implemented according to the 3GPP R5 specifications will be an end-to-end packet switched cellular network using IP as the transport protocol instead of SS7.

UMTS Protocols

There are three major areas concerning the protocol architecture in the UMTS network: Air interface protocol architecture, UTRAN protocol architecture, and core network protocol architecture. Other key design criteria applied in the UMTS protocol architecture model are the separation of user data from control signaling. All protocols used for user data transfer belong to the User Plane and those used for control purposes belong to the Control Plane.

WCDMA Air Interface Protocol Architecture

The air-interface protocol architecture is organized in a layered model as shown in Figure 2-33. At the lowest level is the physical layer that controls the physical media through which both control signaling and user data traffic is transferred. The purpose of the physical layer is to provide upper layers with a set of WCDMA transport channels. The physical layer maps the flows from transport channels to physical channels and vice-versa. In fact, the WCDMA physical channels exist at physical layer and are used for transmission across the RF interface.

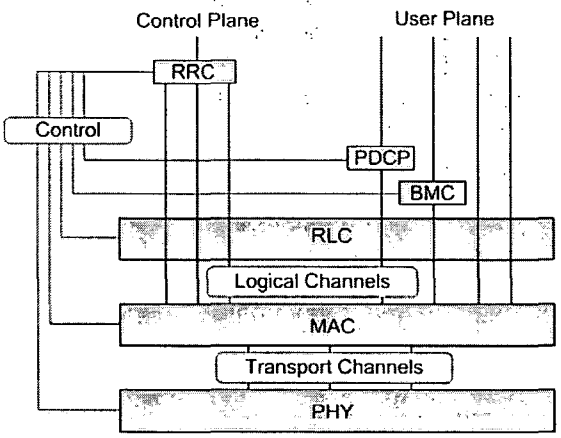


Figure 2-33: WCDMA Air Interface Protocol Architecture

Higher layers that want to transmit information across the RF interface pass information to the physical layer through the MAC layer. MAC provides its services as a set of logical channels, by mapping these to transport channels and vice versa. MAC has the overall responsibility of controlling the communication over the WCDMA transport channels provided by the physical layer. It shares the capacity of the transport channels among the number of users. Above the MAC layer there is the Radio Link Control (RLC) layer, which provides several services to upper layers. The RLC protocol runs both in the RNC and the UE and it performs the usual link layer functionality over the WCDMA radio interface. RLC is active both in the control plane and the user plane simultaneously and it provides data link services for both circuit switched and packet switched connections. One of the protocols above the RLC layer is the Packet Data Convergence Protocol (PDCP), which is similar to the SNDCP of GPRS. Its main objective is to enable the lower layers (RLC, MAC, and the physical layer) to be common regardless of the type or structure of the user data. The PDCP enables the UMTS radio interface to carry IP data packets. Another protocol the Broadcast/Multicast Control (BMC) has been defined for message broadcast and multicast. The main task of this protocol is the broadcast of user messages across

the cell. One of the most important components depicted in Figure 2-33 is the Radio Resource Control (RRC) protocol. The RRC can be considered the overall manager of the air interface and is responsible for the management of the radio resources. The RRC has control interfaces with all other protocol entities on both the UE and the UTRAN side so that a request from a user or from the network can be analyzed and radio resources can be allocated as appropriate.

UTRAN Protocol Architecture

The UTRAN protocol architecture is also organized in layers and planes. Figure 2-34 depicts the generic protocol architecture for the terrestrial interfaces used in UTRAN, namely the Iu-CS, Iu-PS, Iur, and Iub Interfaces.

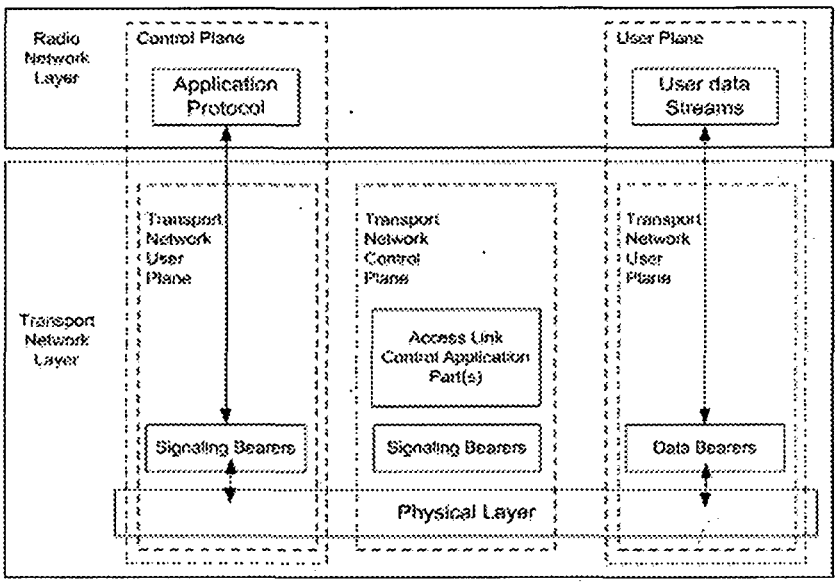


Figure 2-34: UTRAN Generic Protocol Architecture

The layering principle distinguishes between two major parts of the protocol stack. All the lower layer protocols together compose what is called the transport network layer of UTRAN. The other set of protocols on top of the transport network layer is called the radio network layer. The transport network layer represents the transport technology that the various interfaces use. In the case of 3GPP release 1999, the transport network layer represents an ATM – based transport. The radio network layer represents the application information to be carried – either user data or control information. Figure 2-34 also distinguishes three planes – the control plane, the user plane, and the transport-network control plane. The control plane is used for UTRAN related control signaling. It includes the application protocol used on the interface in question. The control plane is responsible for the establishment of the bearers that transport the user data. The user bearers established by the application protocol are generic bearers and are independent of the transport technology being used. The user plane is what carries the actual user data. This data could for example be data packets being sent or received by the UE as part of a data session. Each data stream carried in the user plane will have its own framing structure. Another vertical plane in the UTRAN protocol architecture is the transport network control plane, which contains functionality that is specific to the transport technology being used and is not visible to the radio network layer. It involves the use of an Access Link Control Application Part (ALCAP). This is a generic term that describes a protocol or set of protocols used to set up a transport bearer. The ALCAP to be used is dependent on the user plane transport technology. By applying the appropriate protocols for each interface into the presented generic model, the protocol architecture for each interface Iu-CS, Iu-PS, Iur, and Iub is obtained. A good overview related to the protocol architecture at each interface is given in [Smi02] [Kaa01].

Core Network Protocol Architecture

The 3GPP R99 protocol architecture within CN is derived from that of the GSM/GPRS system. In the following text, only the protocol architecture for the CN PS domain will be presented. Figure 2-35 shows the protocol stack of the User Plane, whereas the Control Plane protocol stack is shown in Figure 2-36.

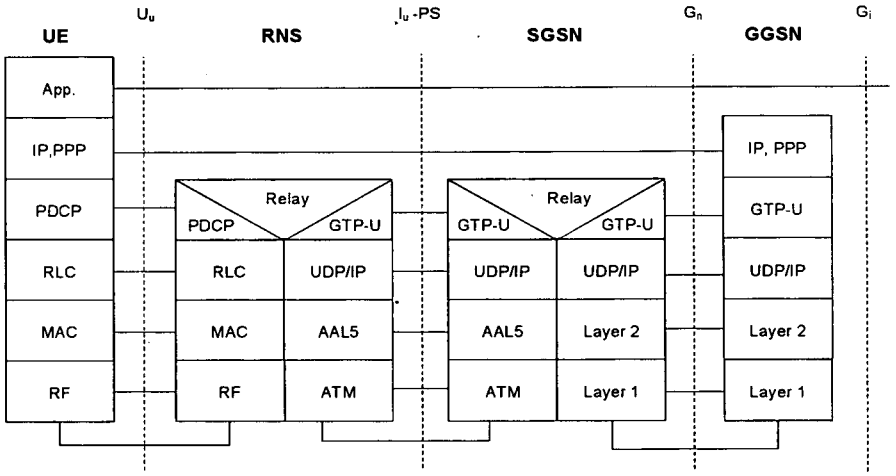


Figure 2-35: UMTS User Plane Protocol Stack

As can be seen from the Figure 2-35 and Figure 2-36.b, the GPRS Tunneling Protocol (GTP) evolved in two protocols: GTP-U for the User Plane and GTP-C for the Control Plane. GTP-U is a transport network protocol supporting user plane data transfer in the UMTS CN PS domain. GTP-U extends from GGSN across the Iu-Ps interface to the UTRAN side. This termination of GTP-U communication at the RNC, instead of the SGSN, differs from the GPRS specifications. Tunnels between GTP-U endpoints are established by control plane protocols: GTP-C at the Gn interface and RANAP (Radio Access Network Application Part) at the Iu-PS interface. GTP-C is a control plane protocol specifying tunnel management and control procedures in order to allow SGSN and GGSN to provide user data packet transfer. It is located in SGSN and GGSN. In the SGSN, the GTP-C protocol interworks with GTP-U protocol at the Gn side. In the GGSN, the GTP-C interworks with the GTP-U located at the Gn interface and with the external network interworking function at the Gi interface.

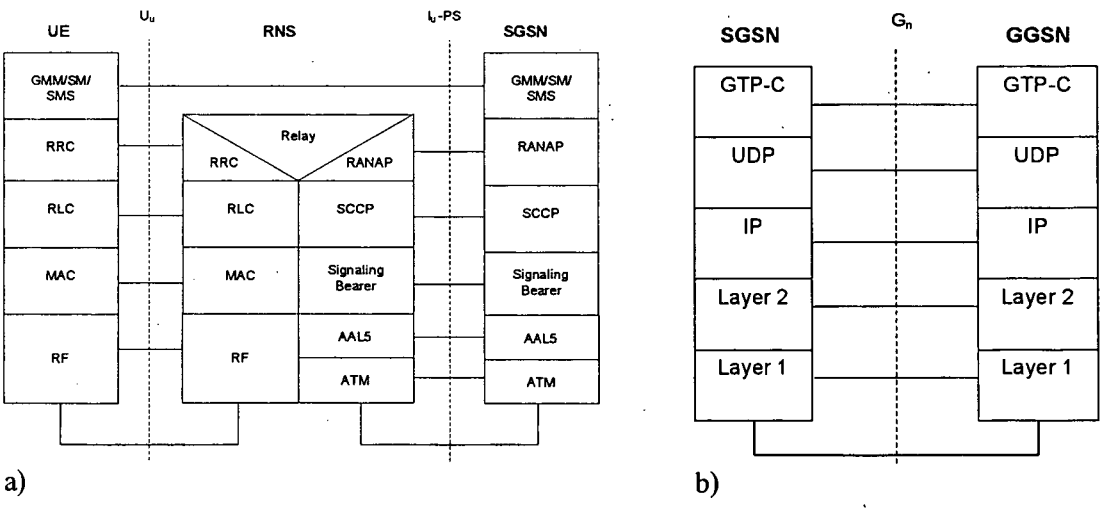


Figure 2-36: a) UMTS Control Plane UE to SGSN; b) Control Plane SGSN to GGSN

The RANAP protocol controls the resources in the Iu interface. The RANAP protocol resides in the RNC and SGSN and it is located on top of the Iu signaling transport layer. In the 3GPP R99, the transport layer in the Iu interface is comprised of a SS7 protocol stack over ATM or IP over ATM. The SS7 stack consists of several protocol layers but the top most protocol is always the Signaling Connection Control Part (SCCP) protocol. This protocol supports both connection-oriented and connection less services.

UMTS Services

The UMTS system has been designed for high-speed multimedia packet data and voice services. To achieve this task, UMTS supports high bit rate connections for both circuit switched and packet switched connections. Table 2-1 shows the bit rates offered, depending on the communication environment. However, the indicated bit rates should be understood as target values.

Table 2-1: UMTS Bit Rates

Circuit switched	Packet switched	Coverage area
144 kbit/s	144 kbit/s (peak)	Basic coverage, rural/suburban, fast moving vehicle
384 kbit/s	384 kbit/s	Extended coverage, urban, moving vehicle, outdoor
2 Mbit/s	2 Mbit/s (peak)	Hot spot areas, urban, center, walking speeds, indoor

The UMTS network will be used for a variety of packet switched data services as well as for speech, which at least in 3GPP Release 1999 and 3GPP Release 4, is a circuit switched service. In the initial phase of UMTS deployment, speech service may well remain the most widely used service in the UMTS, hence speech quality in UMTS needs to be comparable to that in fixed telephony networks and certainly no worse than that experienced in 2G wireless networks. From the user's perspective, 3G/UMTS is first of all a network of services and not of technology. In fact, users only buy services that add value to their lives and the technology itself that enables service provisioning is less important. This is the network operator's concern. Figure 2-37, gives an overview of the UMTS services based on a Siemens [SIE 01] end user survey, indicating the contribution of each specific service to overall UMTS services.

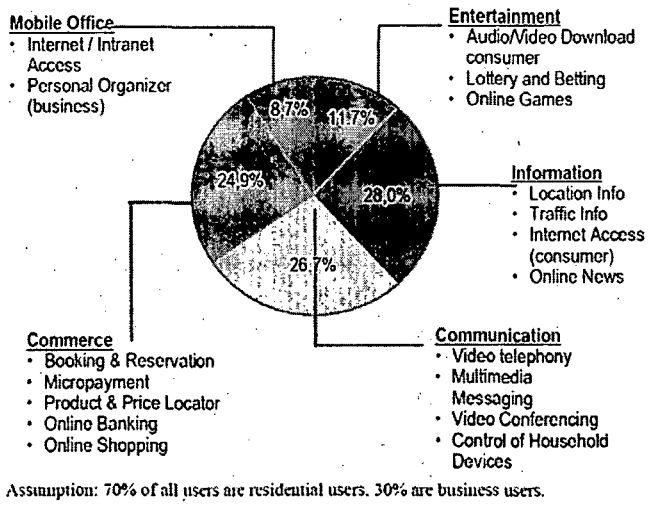


Figure 2-37: UMTS Services

Many of these complex services will take time to develop. Hence, services will be implemented slowly throughout 2005 in developed countries, while many countries in the developing world will use 3G services only later in the decade. It is necessary to stress that UMTS services have certain QoS requirements in terms of throughput, delay, jitter, and error-free delivery, all of which are derived from human perceptions and expectations. Therefore, UMTS contains mechanisms to satisfy these QoS requirements end-to-end. Furthermore, QoS is one of the most important issues in UMTS and it will be presented in Chapter 5.

2.3.6 Satellite Communication Systems

In future communications and the information-based society, provisioning of broadband multimedia telecommunication services to users, independently of time and location becomes a very important and essential task. Using communication satellites is one of the feasible solutions to carry out this task as satellites can provide wide coverage and can supply services to remote areas where there is no terrestrial infrastructure. In addition, satellite systems are able to provide applications that terrestrial systems cannot do. Point-to-multipoint communications, for example, can easily be done by satellite systems, which is very hard to realize in terrestrial networks. Currently, many satellite systems are in the design or development phase. Several orbital options have been considered for future mobile satellite systems: Low Earth Orbit (LEO) satellites in the range of altitudes from 500 to 2000 km, Medium Earth Orbit (MEO) satellites at altitudes about 10.000 km and Geostationary (GEO) satellites at altitudes about 36.000 km. Both transparent and layer-2 switching satellites are proposed for both GEO and mobile satellite networks, which are seen as two competitive systems. The trend for communication satellites is to support global mobile broadband multimedia communications. As GEO satellites are not ideal for this task, due to large round trip delay, satellites using lower orbits are expected to fulfill this task. It is worth to stress that the basic purpose of satellites for mobile communications is not the replacement of existing mobile phone networks, but their extension into areas without coverage.

In the following subsections a short overview of satellite communication systems will be presented, including a new proposal for a satellite IP Network Architecture for global network connection, employing both GEO and LEO systems.

2.3.6.1 Background

The year 1960 marked the beginning of satellite communications, when the first communication satellite ECHO was launched. ECHO was basically a mirror in the sky enabling communication by reflecting signals. The first commercial GEO Communication satellite INTELSAT 1, also known as "Early Bird", was launched in 1965, offering 240 duplex telephone channels or alternatively a single TV channel. INTELSAT 2 followed in 1967, whereas INTELSAT 3 in 1969 offering 1.200 telephone channels. Satellite communications were considered particularly important for ships at sea. Therefore, three MARISAT satellites were launched in 1976, which offered worldwide maritime communication. The first mobile satellite telephone system, INMARSAT-A, was launched in 1982. INMARSAT-C followed, in 1988, as the first satellite system offering mobile phone and data services. The year 1988 finally marked the beginning of a new era of satellite data communication with the introduction of global satellite systems, Iridium system, for small and truly portable mobile satellite phones. The current number of the launched GEO and LEO satellite systems, and those planned to be installed in the next few years show the huge growth of satellite communication systems.

2.3.6.2 Basic Concepts of Satellite Communication Systems

A satellite revolves around the earth in an orbit that forms an orbital plane, which passes through the center of gravity of the earth or the geocenter. A satellite revolves in either a circular or an elliptical path, which can be accurately described mathematically. Hence, it is possible to calculate the position of a satellite at any given time. Some of the specific characteristics of a satellite orbit are: Height, speed or period, angle of inclination, and angle of elevation. The orbit height is the most crucial parameter, which determines the number of satellites and number of orbits needed for a certain satellite communication system. In a circular orbit, the height is the distance of the satellite from the earth. However, in geometrical calculations, the height is really the distance between the centre of the earth and the satellite. In other words, the distance includes the radius of the earth, which is generally considered to be about 6,370 km. The closer the satellite is to earth, the stronger the effect of the earth's gravitational pull. Hence, in low orbits, the satellite must rotate faster to avoid falling back to earth. The farther the satellite is

from the earth, the lower its orbital speed. The time it takes for a satellite to complete one orbit is called the revolution or synodic period.

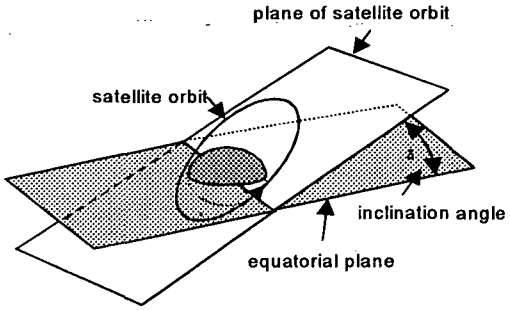


Figure 2-38: Angle of Inclination of a Satellite Orbit

The angle of inclination, shown in Figure 2-38 is the angle between the equatorial plane and the satellite orbit plane as the satellite enters the northern hemisphere. When the angle of inclination is 0° or 180°, the satellite will be directly above the equator. When the angle of inclination is 90°, the satellite will pass over both the north and south poles once during each rotation around the Earth. Orbits with a 0° inclination are called equatorial, while orbits with inclination 90° are referred to as polar. The angle of elevation of a satellite is that angle that appears between the line from the earth station's antenna to the satellite and the line between the earth's station antenna and the earth's horizon, as shown in Figure 2-39. If the angle of elevation is too small, the signals between the earth station and the satellite have to pass through much more of the earth's atmosphere. Because of the very low powers used and high absorption of the earth's atmosphere, it is desirable to minimize the amount of time that the signal spends in the atmosphere. Five degrees is regarded generally as minimum practical angle of elevation ε_{min} for good satellite performance. Another important parameter of communication satellites is the coverage area on the earth, called footprint. The footprint is that part of the surface of the earth where a satellite can be seen under a certain elevation angle ε greater than a given minimum elevation angle. By the use of multibeam antennas the footprints can be divided into smaller cells, the so-called spotbeams and each one corresponding to a beam of the satellite antenna. Use of multiple spotbeams can increase system capacity (due to the higher frequency reuse possibility, concentrated transmission power) and reduce antenna size of user terminals and required transmission power.

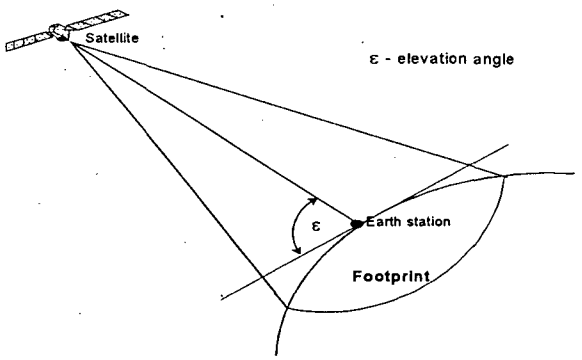


Figure 2-39: Angel of Elevation and Footprint

2.3.6.3 Classification of Satellites Based on Orbit Height

Satellites are usually classified according to the type of orbit they are in. As shown in Figure 2-40, three basic types of satellites can be identified according to orbit height: Geostationary or Geosynchronous Earth Orbit (GEO) satellites, Medium Earth Orbit (MEO) satellites, and Low Earth Orbit (LEO) satellites. GEO satellites, as their name implies, rotate around the earth in exact synchronism with the earth's rotation. For this reason, it appears to be in a fixed or geosynchronous/geostationary orbit. This corresponds to the 24 hours orbit period at 36,000 km

altitude. The rather long distance from the earth's surface results in a large Round Trip Delay (RTD). This is the time it takes for a signal to travel up to a satellite and back down to a receiver station) of 250-280 ms. Due to the high orbit altitude, GEO satellites have a very large servicing area of almost 1/3 of the Earth's surface, from about 75° south to 75° north latitude. The combination of the fixed position along with the very large servicing area provides near-global coverage with a minimum of three satellites in orbit. A large round trip delay is a main drawback of GEO satellites for real time communication services. Besides this, the high altitude requires high power transmission both at satellites and at the earth stations. Thus, larger receiving user terminals are needed. Therefore, GEO satellites cannot be used with small mobile phones. However, these satellites are very useful, especially for broadcasting services and are the most used communication satellites today.

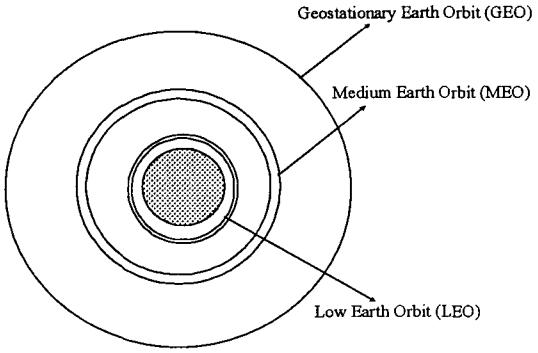


Figure 2-40: Satellite Orbits

MEO satellites rotate around the earth at an altitude of around 10,000 km. Thus, they have different angular velocities compared to the earth and do not have a fixed position in reference to the user on the earth. Their orbit period measures about six hours, while the maximum time during which a MEO satellite is above the local horizon for an observer on the earth is on the order of a few hours. The typical round trip delay for MEO satellites is 70-80 ms. A global communications system using MEO orbits requires several satellites in two to three orbital planes to achieve global coverage, because shorter distance results in smaller footprints. Shorter distance to the earth, in comparison to GEO satellites, means that smaller and lighter receiving terminals can be used. There have not been many communication satellites of this type. The U.S. Navistar Global Positioning System (GPS) is a typical example of an MEO system.

LEO satellites rotate in orbits at a height of 500-2000 km above the surface of the earth. The typical round trip delay of LEO satellites are 5-5 ms. Like for MEO, LEO satellites do not have a fixed position over the earth, and move in reference to the ground. The maximum time during which a satellite in the LEO orbit is above the local horizon for an observer on earth is up to 20 min, while there are long periods during which the satellite is out of view. In order to increase accessibility and make global coverage possible, more than one satellite and multiple orbital planes are required. For instance, the Iridium system utilizes 66 satellites (plus six in-orbit spares) in six orbital planes at an orbital height of 780 km with an orbital period of 100 min and 28 s. Due to their smaller distance from the earth surface, LEO satellite systems can provide communication services with very good end-to-end delays. They have also lower power consumption requirements for both the mobile terminal and satellite. Hence, LEO systems can be used for small mobile phones. In most LEO satellite constellations, the coverage area is partitioned into multiple spot beams. Future broadband LEO satellite communication systems will increasingly rely on Inter-Satellite Links (ISL). There are two types of inter-satellite links: intra-orbital satellite links and inter-orbital satellite links. Table 2-2 shows the constellation parameters for LEO satellite systems employing ISLs [Wer01]. In the emerging era of the IMT-2000 LEO satellite communication networks are expected to coexist with terrestrial networks. LEO satellite networks will be able to support end-to-end connections in the near future and thus they will play both complementary and competitive roles compared to fixed telecommunication net-

works as well as cellular networks, and may partially substitute for fixed networks in sparsely populated areas where fixed telephone services are unavailable.

Table 2-2: LEO Satellite Systems

Satellite System	Iridium	Teledisc	M-Star
Orbit altitude	780 km	1375 km	1350 km
Orbit period	100 min	114 min	113 min
Number of satellites	66	28	72
Number of orbits	6	12	12
Inclination	86.4 °	84.7 °	47 °
Intra-orbit ISLs per satellite	2	up to 4	2
Inter-orbit ISLs per satellite	up to 2	up to 4	2/4

2.3.6.4 Architecture of the Satellite Networks

Figure 2-41, shows the typical network architecture for satellite communication systems supporting global mobile communications [Sch00].

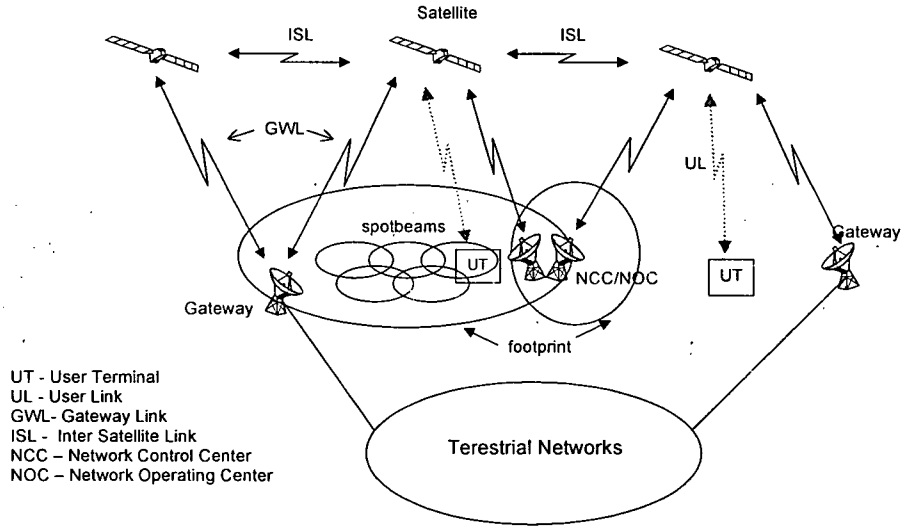


Figure 2-41: Satellite Communication System

A satellite communication system is divided generally into a space and a ground segment [Dao00]. The ground segment consists of User Terminals (UT), Gateway Earth Stations (GES), and the Network Control Center and/or Network Operations Center (NCC/NOC). User terminals (which may be fixed, transportable, or mobile) provide access to the satellite network and perform similar functions in both GEO and LEO satellite systems. However, because of the large distance from the user to the GEO satellite, user terminals need a high gain antenna, causing difficulties for providing handheld terminals. Gateway earth stations are the boundary of the satellite network and they provide connectivity to the different external networks. In the gateways, management and call control functions, and external routing are also implemented. The NCC and/or an NOC are generally involved in network control, management, maintenance, and administrative operations. The space segment includes satellites with all the encountered payload functionalities, depending upon satellite type, relaying, On-Board Processing (OBP) or onboard routing capable. In general, more processing power on board of a satellite increases its complexity, but offers better integration with the ground segment. In addition to the space and the ground segment, there is a third segment of the satellite system, namely the air interface and satellite links. The air interface is primarily involved in physical layer issues, layer-2 functions such as medium access control, and some layer-3 functions such as call control, radio resource management, and mobility management. Mobile users communicate with the satellite via a Mobile User Link (MUL), whereas gateways communicate with the satellite via the Gateway Link

(GWL). Additionally, satellites might have the capability to communicate directly with each other via Inter-Satellite Links (ISL). This facilitates direct communication between users within different footprints without using gateways or other networks on earth, thus reducing latency. Some satellites might have special antennas to create smaller cells using spot beams.

2.3.6.5 Frequency Bands

There are several frequency bands used in satellite communications between the ground and the space segment, shown in Figure 2-42 [Lut00].

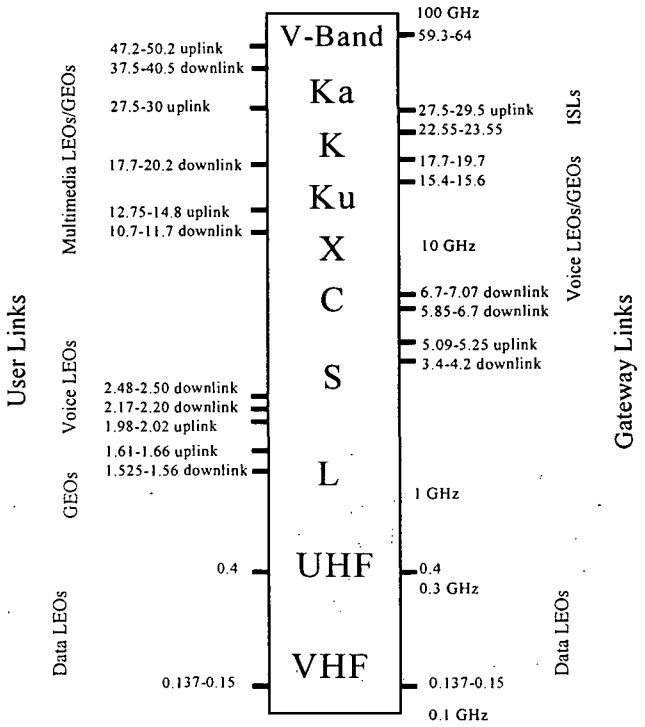


Figure 2-42: Frequency Bands for Satellite Communication

The C-band, Ku-band, and Ka-band are considered as being the basic frequency bands in satellite communications. Actually, the C-band and the Ku-band are currently the two most common frequency spectra used in satellite communications. The C-band occupies the 4 - 8 GHz frequency spectra. These relatively low frequencies result in larger wavelengths, subsequently larger satellite antennas are required to receive the required minimal signal strength. Therefore, the minimum size of an average C-band antenna is approximately 2 - 3 m in diameter. The Ku-band occupies the 11 - 17 GHz frequency spectra. These relatively high frequency transmission results in smaller antennas required to gather the required signal strength. Ku-band antennas can be as small as 50 cm in diameter. The Ka-band occupies the 20 - 30 GHz spectra. These very high frequencies used in satellite transmission result in very small receiving antennas. The Ka-band has also wider frequency spectra available than the Ku-band, but is also more rain attenuated. In addition to the three above mentioned frequency bands, satellite systems employing inter-satellite links use the V-band and K-band.

2.3.6.6 Next-Generation Broadband Satellite Networks

Recently, the interest in broadband satellite multimedia systems and in provisioning Internet access to any areas and any users (fixed or mobile) has grown rapidly. Several factors are fueling the growing interest in Internet provisioning over satellite. Many areas still are not covered by wireless cellular infrastructures due to high costs (rough terrain or low-density user population) or due to geographic locations (aeronautical and maritime area). Thus, providing mobile

Internet access via broadband satellite networks is considered a feasible solution for users located in areas where there are neither terrestrial infrastructures nor mobile networks. The next-generation satellite communication systems are expected to implement this task and to offer Internet services with global coverage. Both, stationary (GEO) and mobile (LEO, MEO) satellite systems are proposed for the future global information infrastructure. Relaying satellites are being replaced by on-board processing satellites, thereby becoming a layer-2 switch or even an IP router. To reuse the frequency better, multi-beam antennas focusing on a smaller footprint are employed. Most of the GEO satellite systems do not employ Intersatellite Links (ISLs). Besides the long propagation delay, another cited drawback of the GEO satellites is that south and north Polar Regions cannot be covered because of the low elevation angle above the latitude of 75 degrees. In contrary to GEO satellites, LEO satellites have smaller coverage areas, due to relatively low altitudes. However, a high number of LEO satellites forming a satellite constellation are needed for global coverage. In addition, LEOs provide a much higher elevation at the Polar Regions and, thus a better coverage. LEO satellites are connected by intra and inter-satellite links, which require on-board routing as well. The constellation mobility combined with inter-satellite links creates a very complex dynamic communication network in the sky. This raises additional problems, mobility management, and routing being the most challenging ones.

In future satellite communication, seamless interworking or integration of satellite networks with fixed or mobile terrestrial networks have to be enabled. For efficient internetworking with the terrestrial Internet, satellite networks must provide complex interworking units placed at the Gateway Earth Station (GES). The implemented interworking functions should include address mapping, protocol conversions and QoS mapping. Two broadband transport technologies, ATM and IP, are proposed for future broadband satellite architectures. Using ATM technology generally means IP over ATM networking. In the case when we want to provide mobile Internet over satellite-ATM networks, the mobile IP protocol must interwork with particular satellite-ATM mobility management protocols, resulting in more complex interworking. In the case of satellite IP network, with IP routers implemented on-board, the first advantage is that the satellite network can integrate seamlessly with the terrestrial Internet. Furthermore, IP-based protocols are easily implemented and compatible with most of the terrestrial networks i.e., seamless internetwork mobility management. Another advantage is the IP QoS support without any required interworking with terrestrial IP QoS mechanisms. Multicast application provision is also well supported by using an IP on-board router [Woo01]. Due to the high efficiency and flexibility of using satellite IP networks for providing Internet services, in the next section we will focus on satellite networks, which employ IP-layer on-board routers, mainly in terms of network architecture.

Satellite IP Network Architecture

Satellite IP network architecture is a part of the global communication network architecture, which comprises the Internet network, multi access networks and remote networks. We assume that IPv6 is the main communication protocol of the Internet. We consider different access networks such as terrestrial mobile and fixed, IP or non-IP-based, and satellite IP networks. IP-based access networks are connected to the Internet through access routers supporting the mobile IPv6 protocol. For the access networks that lack IP mobility functions, an IWU is needed to connect to the Internet, where a protocol conversion and other interworking functions have to be implemented. Assuming only a satellite network environment, remote networks (fixed or mobile) are directly connected to satellite networks through access router. Depending upon the remote network technology, IP or non-IP-based, an IWU may be needed to interwork with satellite IP networks. For remote network users, a satellite network provides access to global Internet services and to another remote network. In the latter case, the satellite network is in fact used as a transport network. In the presented global network architecture, our focus is on the satellite network component. We propose two satellite networks, one based on GEO satellites and the other one based on a LEO constellation. The network architectures described relate primarily to

the IP network layer aspects of system implementation and in particular to the provision of Internet services.

Our proposed GEO satellite network architecture, shown in Figure 2-43, is organized around GEO satellites, equipped with On-Board Processing (OBP) and IPv6 routing with multi-beam antennas and without ISLs. Satellites have multi-attachment points to the Internet through gateways. Depending on traffic demands in the service areas, we assume one gateway for one or several beams. On-board processing and a large number of spot beams are needed to provide better coverage and to reduce the power consumption on-board and particularly at user terminals. Each beam is considered as a sub-network, with own address prefix, therefore fixed users located in each beam service area would have a particular network prefix address. We suppose that this also applies for the case of mobile users, because when a user moves from beam to beam, the movement is detected as a change of IPv6 address. On-board routing functions in a single GEO satellite case consists of one-hop packet forwarding from one beam to one or more beams in order to provide unicast and multicast connections to users.

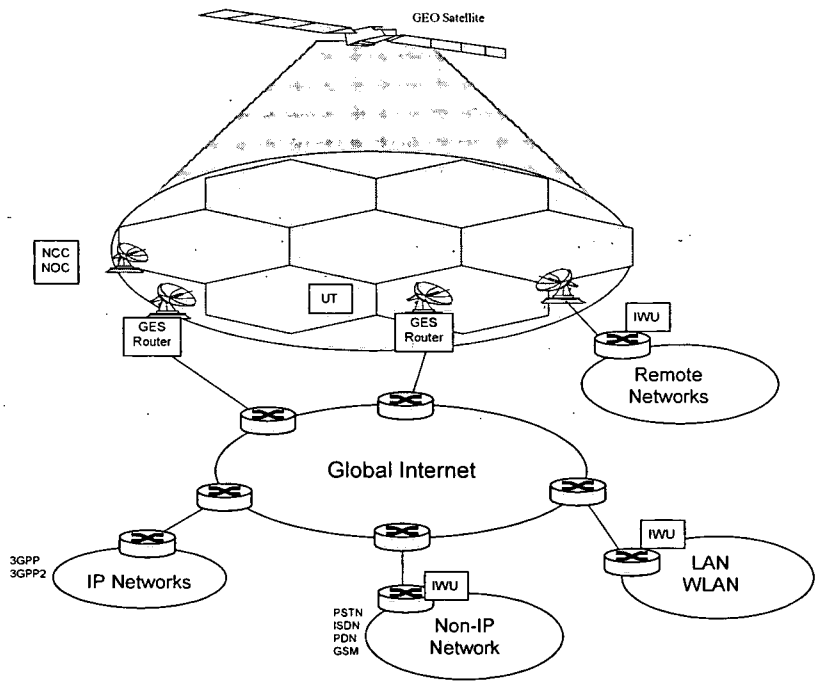


Figure 2-43: GEO Satellite IP Architecture and Global Network Interconnection

The proposed LEO satellite access network, shown in Figure 2-44 comprises a number of LEO satellites with ISLs and spotbeam antennas. The mobile IPv6 protocol, enhanced to support QoS, paging and handover, is employed on-board. The LEO constellation is organized as an autonomous system with multiple points of attachment to the Internet network through a number of GESs, whereby gateways are interconnected through fast Internet. The employment of ISLs reduces the number of gateways, which is much smaller than the number of satellites. Gateways also play the role of both border gateway router to the Internet and home network router for the particular service area. It can be implemented such that each gateway manages a sub-domain, addressed by a particular sub-prefix address. A gateway is also a DNS and knows all the IP addresses of the terminals in its serving area. For addressing issues, we distinguish different user categories including satellite and non-satellite users. The former category indicates such users, who subscribe to satellite network providers. The latter category indicates those users, who roam within the satellite domain and require Internet services.

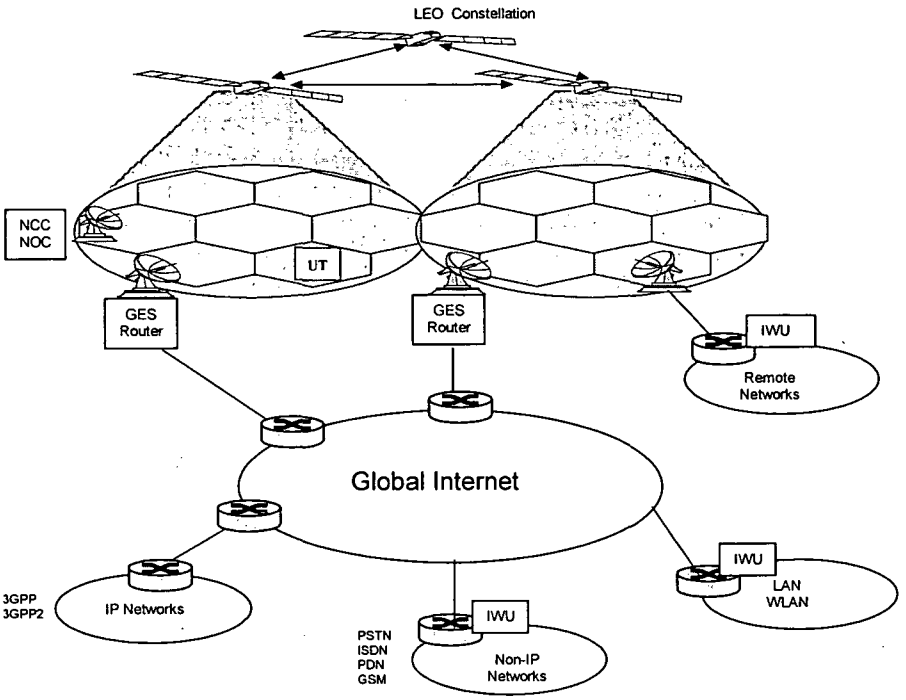


Figure 2-44: LEO Constellation IP Architecture and Global Network Interconnection

Within the technical challenges, IP routing in mobile satellite networks is considered a complex issue because the terrestrial Internet routing cannot be used straightforward for on-board routing. IP routing issues over a satellite constellation are widely described in the literature [Woo01] [Nar98] [Ngu02]. Researchers have common points of view when considering satellite networks as *autonomous systems*, that routing can be implemented at two levels: internal and external. External routing is realized by the Border Gateway Protocol (BGP). Whereas for internal routing, in a constellation with on-board routers, different routing strategies considering QoS, costs, and other issues can be applied.

Services

Future broadband satellite communication systems will be able to offer a wide range of services, similar to those offered by terrestrial systems. Owing to the unique properties of satellite communications, the provision of certain services will be much easier and will serve a considerably wider group of interested users. Broadband satellite networks are expected to provide services to customers in areas where deployment of terrestrial networks is very expensive. The most frequently named services for real-time and non real-time applications are: Access to the Internet and WWW pages, electronic transfer of documents, electronic mail, message transmission, data distribution, television to home, television on demand, radio on demand, radio for global service area, distribution of music programs, books on demand, local publishing and printing of documents, switched broadcasting services, interactive television, high-definition television, video and audio conferences, bank services, electronic transactions, electronic shops, tele-medical services, remote teaching, satellite news gathering, library services, access to data bases as well as positioning and localization services based on the Global Positioning Systems (GPS).

The characteristics of several broadband satellite systems, which are expected to provide the above-mentioned services, are listed in the Table 2-3 [Jam01].

Table 2-3: Broadband Satellite Systems

System	Orbit	On-board Technology	Access Scheme	Number of satellites	Coverage	Planning year of operation
Astrolink [Ast]	GEO	ATM-based	MF-TDMA	9	Global	In operation
Cyberstar [Cyb]	GEO	Packet switching	MF-TDMA CDMA	3	Multiregional	In operation
EuroSkyway [Eus]	GEO	Packet switching	MF-TDMA	5	Europe	2005
SkyBridge [Sky]	LEO	N/A	CDMA	80	Global	In operation
Spaceway [Spa]	GEO	ATM-based	MF-TDMA	8	Global	2004
Teledesic [Tel]	LEO	Packet switching	MF-TDMA	288	Global	2005

2.3.7 Wireless Local Area Networks

Wireless Local Area Network (WLAN) is a flexible wireless data communication system implemented as an extension to or as an alternative for a wired LAN within a small area. Wireless LANs were first introduced in 1997 and originally have been designed for deployment in the corporate communication environment. Recently, more and more new applications are currently developed for the residential environment as well as for the public environment. As a result, WLANs are being adopted at mass scale in the home, Small Office Home Office (SOHO) environments, within the enterprises, and public networks to allow end-users the easiest possible access to the Internet and corporate resources using existing laptops and PDAs. The global WLAN market today is one of the fastest growing markets in the wireless Internet at an annual average rate of 40-50% year over year. Various research firms predict an estimated 15-20 million public users and 37,000 WLAN public hotspots in Europe by 2006 while by 2007 worldwide WLAN users are expected to exceed 147 million. Public hot spots refer to WLANs deployed in hotels, airports, cafes, university campuses, apartment complexes, supermarkets and other common locations to allow visitors temporary broadband network access from their laptops and hand-held devices. With the massive growth, WLANs are experiencing at this time, many industry experts are also predicting that voice over WLAN and streaming video will be the next killer applications for WLANs. Another opinion is that ubiquitous broadband wireless Internet access itself presents the killer application. Today, WLANs can provide data connectivity at up to 11 Mbit/s per access point; in one year access speeds of up to 54 Mbit/s will be common and looking beyond two years this data rate is expected to reach 100 Mbit/s, providing data throughput many times the speed of today's wireless networks. WLAN technology will certainly be key part of future networks first-of-all due to the high bandwidth-to-cost ratio.

2.3.7.1 WLAN Features

In the following text, the main features of wireless LAN networks will be introduced.

- **Broadband services provision** - WLANs have a unique capability for providing wideband services within a small and dense area to low mobility and fixed users.
- **Complementing 3G/2.5G technologies** - As WLANs offer limited coverage and mobility they cannot be positioned as competitors of truly mobile data systems such as GPRS and UMTS, but rather complement them.
- **License free spectrum** - WLANs use free radio spectrum in the 2.4 GHz ISM (Industrial Scientific and Medical) band and in the 5 GHz UNII (Unlicensed National Information Infrastructure) band.

- **Reduced costs** - While the initial investment required for WLAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower, particularly in dynamic environments requiring frequent moves and changes.
- **Scalability and flexibility** - Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific communication environments. Configurations are easily changed and range from ad-hoc networks suitable for a small number of users to full infrastructure networks of thousands of users enabling roaming over a broad area.
- **Installation simplicity** - Installing a WLAN is relatively easy and eliminates the need to pull cabling through walls and ceilings.
- **Transmission technologies** – WLANs basically use radio transmission in the GHz licence-free band, but also infrared light can be used.
- **Security** - Due to radio transmission interference between different WLAN systems communicating on same frequency and with other high-tech equipments is very likely. To prevent eavesdropping, security protocols such as AAA (Authentication Authorization Accounting) based and IEEE 802.1x are developed or currently developing for WLAN environment.
- **Power consumption** - User equipments communicating via WLAN are usually wireless devices running on battery power. Hence, power-saving modes and power management functions have already gained considerable attention.

2.3.7.2 WLAN Applications

Early adopters of WLAN technology are universities, hospitals, warehouses, older office facilities, and airports. The following list describes some of the many applications made possible through wireless LANs:

- Students at universities and training sites at corporations use wireless connectivity to facilitate access to lectures, information, and information exchanges.
- Doctors and nurses in hospitals are more expeditive because laptops or notebook computers with wireless LAN capability deliver patient information instantly.
- Network managers installing networked computers in older buildings find that wireless LANs is a cost-effective network infrastructure solution avoiding rewiring buildings.
- Warehouse workers use wireless LANs to exchange information with central databases and increase their productivity.
- Senior executives in conference rooms make quicker decisions because they have real-time information on their laptops.

2.3.7.3 WLAN Architecture

WLANs can be set up in two different basic system architectures: infrastructure networks and ad-hoc (on demand) networks. A typical infra-structured WLAN system comprises three basic components: the User Terminal, the Access Point (AP), and the Access Controller/Router as illustrated in the Figure 2-45.

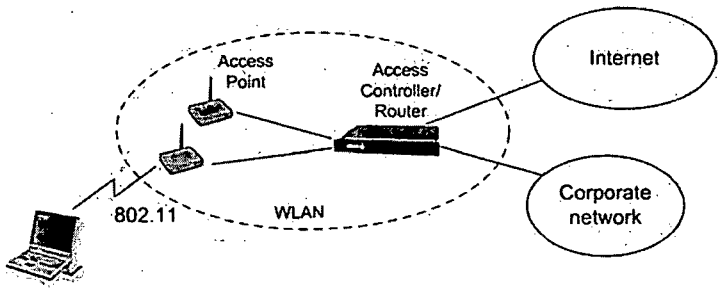


Figure 2-45: WLAN Architecture

User Terminal - Is any device that holds a standard WLAN card and that is able to communicate with other WLAN enabled devices. The WLAN card provides access mechanisms to the wireless medium and radio contact to the AP. User terminals are also called stations (STA). Currently the most common deployed user terminal is the laptop computer.

Access Point (AP) – An AP in WLAN is comparable to a base station for the mobile wireless network. It connects user terminals to a wired network and serves as the wireless equivalent of a LAN hub. An access point typically has an Ethernet port for connection to the wired network, and a WLAN card for wireless communication. A single access point can support a small group of users and covers an area of about 30 to 100 m radius, depending on the environment. A WLAN usually comprises more APs that have some area of overlap enabling roaming of the users from one AP to the next seamlessly.

WLAN Access Controller/Router - Provides the connectivity for the user terminal with the rest of the network (corporate network, Internet). It plays a vital role during the authentication and authorization of the user. The second possible WLAN architecture, the ad-hoc network, is a simple configuration offering peer-to-peer connectivity to a set of user terminals, equipped with WLAN cards. Any time when two or more laptops or PDAs are within range of each other, they can set up an independent ad-hoc network without an access point to meet the instantaneous communication needs. These on demand networks typically require no administration or pre-configuration.

2.3.7.4 WLAN Technologies

WLAN encompasses several technologies. In the following sections a short overview of the existing and forthcoming WLANs will be given. We will focus on 802.11 WLAN and particularly on 802.11b WLAN, as the most widely deployed standard today.

IEEE 802.11 WLANs

The IEEE 802.11 standard (IEEE, 1997) and its supplement standard 802.11x, specify the most popular family of WLANs today. Like other 802.x LAN standards, IEEE 802 defines the Medium Access Control (MAC) sublayer and Physical Layer adapted to the special requirements of WLANs. The Logical Link Control (LLC) sublayer, above the MAC sublayer, is specified in the IEEE 802.2 standard. The IEEE 802.11 architecture provides a transparent interface to the higher layers. User stations may move, roam through an 802.11 WLAN and still appear as stationary to IEEE 802.2 LLC sublayer and above. Hence, applications should not notice any difference apart from the lower bandwidth and perhaps higher access time. Figure 2-46 shows the protocol architecture of the most common scenario: an end-to-end connection between a laptop and web server via IEEE 802.11 WLAN, IEEE 802.3 Ethernet, access router and Internet.

The LLC sublayer covers the difference of the MAC sublayers needed for the different transmission media. The basic tasks of the MAC sublayer comprise medium access, fragmentation of user data, and encryption. IEEE 802.11 supports three different physical layers: Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), and infrared light. DSSS generates a redundant bit pattern, called a chip code, for each bit to be transmitted. Even if one or more bits in the chip are damaged during the transmission, the original data can be recovered without retransmission using the chip and statistical techniques. To an unintended receiver, transmitted data appears as low-power wideband noise and is ignored by most narrowband receivers. FHSS uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. To an unintended receiver, FHSS appears to be short-duration impulse noise. Infrared lights are electromagnetic waves at around 900 nm wavelengths. The main disadvantages of infrared light, for use for WLANs, are low bandwidth and requirement for line of sight. Hence, most wireless LAN systems use radio waves.

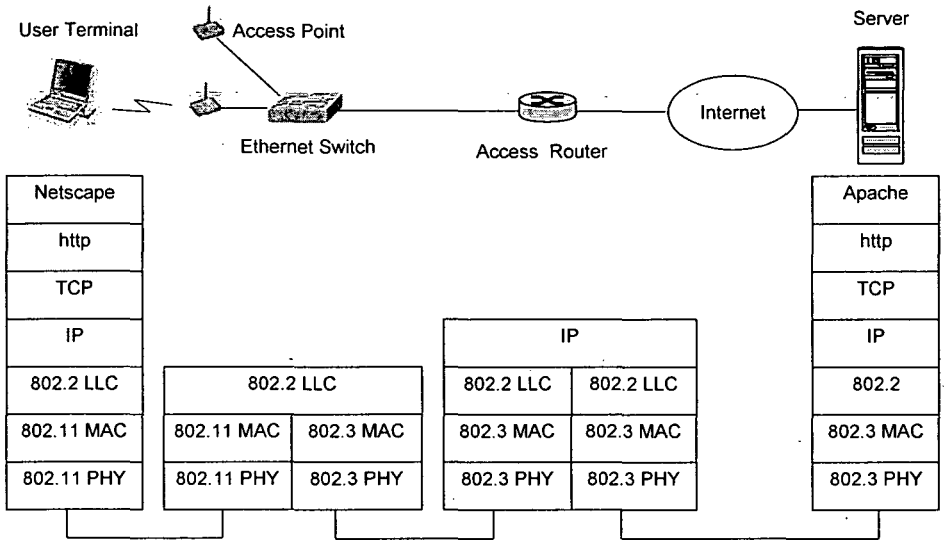


Figure 2-46: IEEE 802.11 Protocol Architecture and Bridging with 802.3 Ethernet

The 802.11 WLAN is a typical infrastructure based network, but it also supports ad-hoc network structure. Hence the IEEE 802.11 standard defines two network operation modes: the Point Coordination Functional (PCF) and the Distributed Coordination Functional (DCF). The PCF mode uses a centralized approach in which a network Access Points (AP) controls all traffic in the network, including traffic between wireless users in the network. The DCF mode supports direct communication between wireless users, thus it fits the needs of ad-hoc networking. Figure 2-47 shows the components of an infrastructured WLAN network as specified by IEEE 802.11 standard. Several stations (STAi) are connected to access points. The stations and the access points, which are within the same radio coverage area, form a Basic Service Set (BSS). In order to extend the coverage area, two or more adjoining BSS can be connected via distribution system to form a single network called Extended Service Set (ESS). Furthermore, the WLAN is connected through APs or a distribution system to the fixed network (LANs or Internet). A station establishes connection to the AP through a basic service called association. Though no handover mechanism is specified in the standard, the standard introduces a service called reassociation, which is related to the roaming from one BSS to another.

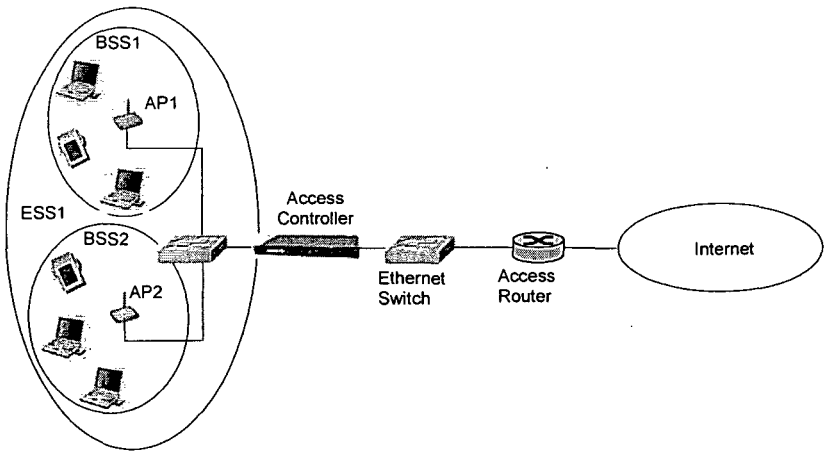


Figure 2-47: Infrastructured WLAN

IEEE 802.11b – Is the most widely deployed physical layer standard today for WLANs. The IEEE approved 802.11b standard in 1999 to add two higher data rates, 5.5 and 11 Mbit/s, to the 802.11 basic standard. However, the maximum data rates of 11 Mbit/s are often not achievable and the maximum user throughput will be approximately half of this. Environment surroundings, distance from the AP, and bandwidth sharing with other users lower throughput. Gener-

ally, when the signal to the mobile terminal weakens, transmissions are automatically rate-shifted from 11 Mbit/s down to 5.5 Mbit/s, 2 Mbit/s, or 1 Mbit/s. The IEEE 802.11b standard provides a transmission range of about 30 to 100 meters and operates in the 2.4-GHz ISM band using DSSS. Laws to govern operations of the allocated ISM band differ from one country to another. In Europe there are 13 channels, with center frequencies located in 5 MHz interval (2412 MHz - 2472 MHz), for IEEE 802.11b use. The channels are overlapping and the receiver adjacent channel rejection demand is 35 dB, which needs 30 MHz gap between the neighboring channels. This means that there are to be five channels between, in order to avoid interference caused by neighboring access points. Hence, a maximum three access points can be put in the same place, as there are only three available channels for transmission. Lucent Technologies, Intersil Corp, Cisco and Symbol are some of the major companies that support the IEE 802.11b standard. The Wireless Ethernet Compatibility Alliance (WiFi) certifies the interoperability between IEEE 802.11b products from different vendors.

IEEE 802.11a - Is a physical layer standard for WLANs in the 5 GHz UNII radio band, which is free for the end users. This standard uses the same MAC (Media Access Control) layer as IEEE 802.11b but an entirely different encoding scheme, called OFDM (Orthogonal Frequency-Division Multiplexing), which departs from the traditional spread-spectrum technology. OFDM utilizes multiple sub-carriers; i.e., the information signal is divided into multiple lower-speed sub-signals that the system transmits simultaneously at different frequencies in parallel. The orthogonal nature of OFDM allows to theoretically avoid interference. IEEE 802.11a is designed to have a transmission range of 30 up to100 meters, to support 54 Mbit/s, but maximum user data throughput will be approximately half of this. It specifies eight available radio channels (available radio spectrum in some countries would permit the use of 12 channels), in much less crowded frequency band. Hence, the QoS will be much better than with 802.11b. Standard completed in 1999, products are available now but not widely deployed.

IEEE 802.11g – Is also a physical layer standard for WLANs to provide data rates of 54 Mbit/s in the same 2.4 GHz frequencies as IEEE 802.11b. The IEEE 802.11g standard uses Orthogonal Frequency-Division Multiplexing (OFDM) modulation but also is backward compatible with IEEE 802.11b. The IEEE 802.11g is still in development and like IEEE 802.11b specifies three available radio channels. Because most customer WLANs available today operate at 2.4 GHz, the introduction of IEEE 802.11g standard will create spectrum overcrowding, interference and scalability issues, which need to be considered.

IEEE 802.11d – This standard is supplementary to the IEEE 802.11 MAC layer. As IEEE 802.11 standards cannot legally operate in some countries, the purpose of IEEE 802.11d is to add features and restrictions to allow IEEE 802.11 WLANs to operate within the rules of these countries, and to promote their worldwide use.

IEEE802.11e – Is also supplementary to the IEEE 802.11 MAC layer to provide QoS support for multimedia applications in WLAN. It will apply to IEEE 802.11 physical standards a, b and g. The purpose is to provide classes of service with managed levels of QoS for data, voice and video applications. This standard will be analyzed in some more details in the Chapter 5

IEEE 802.11h – Is another supplementary standard to the MAC layer to comply with European regulations for 5 GHz WLANs. Based on European radio regulations requirements for the 5 GHz band products, it introduces Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS). TPC limits the transmitted power to the minimum needed to reach the furthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.

IEEE 802.11f – It specifies an Inter-Access Point Protocol (IAPP), which provides the necessary capabilities to achieve multi-vendor Access Point interoperability across a Distribution System supporting IEEE 802.11 Wireless LAN Links.

2.3.7.5 HomeRF

HomeRF is one of the first WLAN technologies. As the name suggests, this technology was developed from the beginning to bring wireless networking to the consumer in his home using RF (Radio Frequency). HomeRF products operate in the globally available 2.4 GHz ISM radio band using FHSS. First generation HomeRF products have peak data rates of 1.6 Mbit/s and cover homes and small offices with a 50-meter typical indoors range. The HomeRF consortium developed the second-generation HomeRF/2, on the same frequency as HomeRF to support a data peak transfer rate of 10 Mbit/s. Second generation HomeRF products were supposed to be on the market by mid 2001. Third-generation HomeRF devices are planned to be even faster (20 Mbit/s) and were supposed to be on the market in the first half of 2003. HomeRF is fully backward compatible. Cayman Systems, Compaq, Intel, and Proxim are some companies that work with HomeRF, though Intel recently announced strong support for IEEE 802.11b.

2.3.7.6 HiperLAN/2

High Performance Radio Local Area Network type 2, is an ETSI (European Telecommunications Standards Institute) project called BRAN (Broadband Radio Access Networks), developing a new generation of standards, which will support both asynchronous data and time critical services (e.g., packetized voice and video) that are bounded by specific time delays to achieve an acceptable quality of service. The HiperLAN/2 Global Forum was launched in September 1999 and was supported by six founding members: Bosch, Dell, Ericsson, Nokia, Telia and Texas Instruments. HiperLAN/2 provides a flexible platform for a variety of businesses and home multimedia applications that uses the unlicensed 5 GHz UNII (Unlicensed National Information Infrastructure) radio band. It supports a set of bit rates up to 54 Mbit/s (actual throughput around 40 Mbit/s) and a transmission range of 30 up to 100 meters. HiperLAN2 standard, like 802.11a, uses the Orthogonal Frequency Division Multiplexing radio technology, and almost identical physical layer. However, HiperLAN2 uses ATM like MAC layer. Standards for Hiperlan/2 wireless LAN network propose two architecture modes: a Centralized Mode (CM) and a Direct Mode (DM). In the centralized mode, mobile hosts communicate with Access Points (AP) over the air interface as defined by the HiperLAN/2 standard. The user of mobile terminal can move around freely in HiperLAN/2 network, which ensures that the user gets the best possible transmission performance. In the direct mode, there are direct radio links between mobile hosts, which resembles the nature of ad hoc networking. However, access points control the communication between mobile hosts. Hence, any two HiperLAN/2 mobile hosts cannot communicate on an ad hoc basis without being in the rich of an access point. The ad-hoc mode of operation of HiperLAN/2 is still in its infant stage of the development, thus the enhancements are expected.

2.3.7.7 Bluetooth

Bluetooth technology is a forthcoming Wireless Personal Area Networking (WPAN) technology that has gained significant industry support and will coexist with most wireless LAN solutions. Bluetooth was born in 1994 at Ericsson mobile communication as a low cost and low power wireless connection for cable replacement to offer point-to-point links. In February 1998 five companies, Nokia, Ericsson, IBM, Toshiba and Intel, formed the Bluetooth SIG (Special Interest Group) to support WLAN applications in the next generation Bluetooth technology. The idea that resulted in Bluetooth was to make a wireless PAN (Personal Area Network) with a transmission range up to 10 meters. This type of network is needed in order to connect different small devices in close proximity without expensive wiring or the need for an infrastructure. Hence, Bluetooth presents most suitable technology for ad-hoc networking. Bluetooth units within range of each other can set up an ad-hoc connection. Two or more (up to eight) units that share a channel for communicating with each other can form what is called a piconet, with slotted communication controlled by a master. The unit that initiated the connection assumes the role of a master, unlike a cellular system wherein the base station always acts as master. A slave

unit may take over the role of a master, but there can be only one master in any piconet. When there are more than eight devices, Bluetooth requires that multiple piconets be formed. These piconets can be connected together into a scatternet if one of the slaves agrees to relay data between two of the masters. This suggests that the slave should have separate time slots in each piconet to reduce latencies for data transmissions. It may even be necessary to form scatternets for the PAN that is associated with a single person. It is almost guaranteed that scatternets will be required for the interaction of multiple PANs. Today, Bluetooth technology is embedded in a wide range of devices and can provide links between mobile phones, mobile computers and other portable handheld devices and connectivity to the Internet. Bluetooth communication occurs in the unlicensed ISM radio band at 2.4 GHz. The transceiver utilizes frequency hopping to reduce interference and fading. The communication channel can support both data (asynchronous) and voice (synchronous) communications with a total bandwidth of 720 kbit/s.

2.4 Review

This chapter presented an overview of the wide range of communication networks as a basis for next chapters. First, the basic concepts of communication networks such as: applications, services, Quality-of-Service (QoS), OSI Reference model, network classification, and broadband networks, were introduced. Then the concept of ISDN network and BISDN/ATM was presented. The main building blocks of the ATM network, protocol reference model, and ATM services, were covered. Next, the basic elements of the Internet were presented. The main protocols of the application layer, the transport layer, and the Internet layer of the TCP/IP suite were described. Also addressing issues of IPv4, IPv6 and transition strategies IPv4-IPv6 were covered. This chapter then presented the mobile communication networks of the first, second and third generation. The network architecture, communication protocols and services of the GSM, GPRS, and UMTS were covered. Also Satellite and Wireless LAN networks as an important segment of mobile communication systems were described. In addition, a new proposal for a satellite IP Network Architecture for global network connection, employing both GEO and LEO systems, was presented.

3 MAC Protocols for Wireless Communication Networks

For particular networks, the Data Link Layer (DLC) of the OSI reference model is divided into Logical Link Control (LLC) and Media Access Control (MAC) sublayers. As the name implies, Media Access Control (MAC) protocols belong to the MAC sublayer of the OSI reference model. MAC protocols control access to a shared transmission media among distributed stations, defining how and when stations gain access to medium and transmit packets. The distribution of the stations depends on the type of the communication network and their topology. Hence, MAC protocols depend on the type and topology of the network as well as on the type of stations. Standard organizations and companies have developed or adopted a wide range of MAC protocols for various types of network environments such as LANs, WLANs, cellular mobile networks, wireless ATM (WATM), and satellite networks, with different user requirements. A survey and analysis of MAC protocols for high-speed LANs and MANs is given in [As94]. A survey of MAC protocols for wireless ATM networks is given in [San97]. A survey and analysis of MAC protocols for satellite communications is described in [Pey95]. In general, MAC protocols that are designed for LAN and WAN fixed networks do not meet the requirements of wireless communication environment. Furthermore, a MAC protocol designed for one type of the wireless network usually is not suitable for other types of wireless network. With respect to the type of station, the generated traffic type is a very important factor that influences the design or selection of a MAC protocol for a wireless network, as MAC protocols that are suitable for some applications often do not meet the requirements for other applications. In the Internet communication environment all commonly used high-level protocols such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Trivial File Transfer Protocol (TFTP), Transmission Control/Internet Protocol (TCP/IP) and Asynchronous Transfer Mode (ATM) use one or more low-level MAC protocols, and the performance of these protocols and the whole network depends on MAC protocol performances.

General goals of MAC Protocol designers are:

- To ensure fair sharing of the transmission channel,
- To support different traffic types and priorities in order to satisfy QoS requirements,
- To obtain high throughput and network utilization together with low and bounded delays and packet drops with respect to traffic type,
- To be simple, robust, reliable, and easy to implement.

MAC protocols are deployed in conjunction with basic multiplexing techniques such as FDM (Frequency Division Multiplex), TDM (Time Division Multiplex), and CDM (Code Division Multiplex). In the context of the MAC sublayer these techniques are named FDMA (Frequency Division Multiple Access), TDMA (Time Division Multiple Access), and CDMA (Code Division Multiple Access) respectively. Therefore, MAC protocols can be based on FDMA, TDMA or CDMA.

- FDMA-based MAC schemes typically are used in a rather fixed fashion, i.e., a certain frequency, or frequency-hopping pattern is assigned to a station for longer period-of-time. In the case of frequency hopping the sender and receiver have to agree on a hopping pattern for the

receiver to tune to the right frequency. However, as an alternative to a fixed frequency assignment, frequencies can be assigned dynamically, on demand, as stations require them. Early MAC protocols for satellite networks were FDMA based.

- TDMA-based MAC schemes are much more flexible and efficient in comparison to FDMA based MAC, as time can be allocated on demand and in a distributed fashion. The receiver can stay at the same frequency the whole time. Listening to many channels separated in time at the same frequency is simple, but listening to the different frequencies at the same time is very difficult. There are many different MAC protocols for wireless networks based on TDMA.
- CDMA-based MAC schemes assign certain codes to stations to allow the separation of different users in code space and to enable access to a shared medium without interference. CDMA based MAC protocols are used in, for example, UMTS networks and military satellite networks.

The focus of this chapter is on TDMA-based MAC protocols for different wireless communication networks. We will first present the most common classification of TDMA-based MAC protocols for wireless networks. Then the basic and most representative protocols for wireless terrestrial and satellite networks will be briefly described. In addition we introduce and evaluate a new TDMA based Random-Reservation MAC protocol to support QoS in satellite communications. The chapter will be concluded with a review of MAC protocols for IEEE 802.11 WLAN networks.

3.1 TDMA Based MAC Protocols Classification

In general, MAC protocols differ in the way that stations coordinate their transmission and resolve collisions. TDMA-based MAC protocols for wireless communication networks can be classified as:

- Fixed access protocols,
- Random access protocols,
- Reservation-based protocols,
- Polling protocols,
- Combined protocols.

Protocols of the first two classes are simpler than protocols of the other three classes, because later protocols require an extra processing either at base station or at the mobile stations. Protocols of the third class use fixed access and random access techniques. Protocols of the fourth class require a central controlling station. As their name implies, protocols of fifth class are combination of protocols of first four classes and almost all advanced MAC protocols to support multimedia applications belong to this class of MAC protocols.

Fixed access or fixed assignment protocols are the simplest MAC protocols based on TDMA. In these protocols a proportion of the total channel capacity (bit rate) is exclusively allocated to each station in a fixed pattern and is independent of the station's activities. This results in a fixed-channel bit rate and is the standard solution for a wireless phone system in which the base station can assign the fixed pattern. In general, fixed access protocols guarantee successful transmission and are most appropriate for streaming traffic. They provide the best QoS performance in that worst case delay can be determined, which is essential for real-time applications, and it provides high throughput when the traffic load is high. However, because channel assignment is tightly controlled and is not adaptable to traffic changes, the air interface is poorly exploited when stations are not active, as active stations cannot use the idle stations' share of channel capacity.

With **random access**, or **contention protocols** stations access transmission medium randomly and compete for channel capacity every time they have a packet to transmit. Each station makes its own decision about when to access the channel, and there is no coordination among the stations. Random access protocols are very simple to implement and can serve a large number of stations with a low average data rate and a high peak rate. Thus, they provide low latency when the traffic is light and are suitable for bursty traffic. However, since there is no coordination among active stations collisions may occur and successful transmissions are not guaranteed. Furthermore, contention protocols exhibit an inherent instability: as the load on the network increases, a saturation point is reached beyond which throughput drops rapidly while latency increases.

Reservation-based protocols, also known as **DAMA** (Demand Assignment Multiple Access) protocols, are designed to have the advantages of both random access and fixed access. The aim of reservation protocols is to avoid collisions by reserving a portion of the channel capacity such that only one station can access channel at a time. Reservation protocols typically have a reservation period and packet transmission period. During the reservation period, stations can reserve future slots in the transmission period, and the transmission period can then be accessed without collision or split into transmission periods with or without collision.

Reservation protocols are a very broad class of MAC protocols, which can be classified as:

- Implicit reservation protocols.
- Explicit reservation protocols.

With **implicit reservation protocols**, stations initially transmit a packet randomly. Successful transmission of the first packet is a reservation of channel capacity for transmissions of the rest of the packets.

With **explicit reservation protocols**, a control channel needs to be set aside for reservation requests. Access to this channel is another multiple access protocol. Stations wishing to transmit packets first will reserve a portion of the channel capacity by sending reservation request. Successful transmission of reservation request results in successful reservation of requested capacity of the channel.

Explicit reservation protocols are contention free as far as user data packets are concerned, whereas reservation request is either contention oriented or contention free. Based on the type of reservation request, explicit reservation protocols can further be divided into two groups:

- Reservation by contention,
- Reservation without contention.

With **reservation by contention,** transmission of reservation request is performed by random access. The stations contend during a reservation period, and those who succeed in making reservations transmit without contention.

With **reservation without contention**, each station is assigned its own control channel for its reservation request. Thus, there is no collision of reservation requests.

In general, reservation protocols cause higher delays under a light load but allow higher throughput under a heavy traffic load. They derive their efficiency from the fact that reservation periods are shorter than transmission periods by several orders of magnitude. The minimum delay incurred by a message, excluding message transmission time, is more than twice the channel propagation time. This is an important consideration for satellite channels.

Polling-based protocols are strictly central-controlled schemes, which need a central station like the base station of a mobile phone network or AP in WLAN, to determine which mobile

station currently has the right to transmit. The central station can poll the mobile stations randomly, according to station priority, or in round-robin fashion, in which each mobile station is polled sequentially in the order in which it is placed in the polling list.

Combined protocols or hybrid protocols, utilize various MAC protocols by taking their advantage depending upon the traffic type and instantaneous traffic loads. To accommodate different traffic types and multimedia applications, channel capacity is partitioned into several sections, each operating under its own protocol. Borders between sections can be fixed or movable. Depending upon traffic loads appropriate combined protocol switches from one mode to another mode adapting to the actual state of the channel. Combined protocols are considered best suitable for meeting objectives for multiservice environments.

An additional important feature of the MAC protocols is the **coordination strategy**. Two control strategies are applied: centralized and distributed. In centralized coordination, a single station schedules the transmission time for all other stations. Each station has to synchronize with the central station and wait for the scheduled time in order to transmit its own packets. In distributed coordination, each station executes the same algorithm to schedule transmission of packets randomly or via reservation. Each individual station makes a decision on when it can transmit and maintains the scheduling synchronization in order to avoid collisions. The robustness inherent in a distributed control mechanism for dealing with station failure and network reconfiguration makes this approach more attractive than central coordination.

3.2 Basic MAC Protocols for Terrestrial Wireless Networks

In the following subsections, a brief explanation of some of the basic MAC protocols for wireless networks will be given.

3.2.1 Aloha

Aloha [Abr70] is the first MAC protocol developed for wireless networks. It was invented at the University of Hawaii in the 1970s and was used in the ALOHANET packet radio network for wireless connection of several stations. Aloha is a distributed random access protocol without coordination among the stations. Each station can access the medium at any time and transmit data packets. After transmission, the station listens for an amount of time equal to the maximum possible round-trip propagation delay on the network for the acknowledgment. If there is no acknowledgement, the station assumes that a collision has occurred. Collisions occur when two or more stations access the medium at the same time. When a collision occurs, the station retransmits the packet after a randomized delay. This randomized delay is crucial to the protocol stability and thus to the throughput versus delay performance of all contention oriented protocols. If the collision repeats, the station gives up the transmission. Aloha works well for light loads and does not require any complicated access mechanisms. However, the maximum throughput, assuming Poisson arrival of the packets, is only 18 percent.

3.2.2 Slotted Aloha

To improve efficiency of Aloha protocol, Slotted Aloha (S-Aloha) [Rob75] was developed. S-Aloha is a modification of Aloha, in which time on the channel is organized into slots with equal size. Stations can start to transmit their packets only at the beginning of each time slot. Hence, a mechanism is needed to synchronize all stations, but still, access is not coordinated. In the event of a collision, each station will be involved in the collision resolution process in which retransmission time is determined at some random time in the future in order to reduce the possibility of another collision. Obviously, the packet retransmission backoff time will have an effect on the delay associated with a successful packet delivery. If the backoff time is too short,

the probability of a repeated collision is high. If the backoff time is too long, it will cause unnecessary delays and possibly a waste of channel capacity. Under the assumptions of Poisson arrival of packets, the introduction of slots raises the maximum channel throughput to 36 per cent. Both Aloha principles are used in many networks that implement distributed access to a medium. They work perfectly under a light load but cannot give any hard transmission guarantees, such as maximum delay before accessing the medium or minimum throughput. Hence, they are used in combination with other protocols, as will be shown in later subsections.

3.2.3 Carrier Sense Multiple Access

Carrier Sense Multiple Access (CSMA) is a random access protocol that works by sensing the carrier before accessing the medium and deferring transmission when the channel is sensed to be busy. This decreases the probability of collisions and presents a better alternative to the Aloha protocol. CSMA takes advantage of one of the key properties of a broadcast channel with short propagation delay namely that the propagation delay between stations is insignificant compared to packet transmission time. When a station starts to transmit a packet, all the other stations know almost immediately, and they will not transmit anything until the active station is done. Several versions of CSMA exist: non-persistent, 1-persistent, and p-persistent. In non-persistent CSMA, stations wishing to transmit sense the carrier and start sending packets immediately if the medium is idle. If the medium is busy, the station pauses for a random amount of time before sensing the medium again. In 1-persistent, CSMA systems stations sense the medium and access the medium as soon as it becomes idle. In p-persistent, CSMA systems stations also sense the medium and as soon as the medium is idle, transmit with a probability of p, or defer transmission to the next slot with the probability 1-p. However, carrier sensing does not prevent collision. CSMA is widely used in both wired LANs and WLANs. CSMA with Collision Avoidance (CSMA/CA), for example, is one of the access schemes used in WLANs following the standard IEEE 802.11. Here sensing the carrier is combined with a backoff scheme in case of a busy medium to achieve some fairness among competing stations. However, CSMA/CA cannot solve the so-called "hidden station problem." This problem occurs when one mobile station can receive two others, but those mobile stations cannot receive each other. If those two stations access the channel and sense it to be idle, they may start transmission of a packet and cause a collision at the receiving station. To avoid hidden station problem, an enhancement to CSMA/CA called RTS/CTS mechanism or MACA protocol, has been developed. RTS/CTS mechanism will be described in the Subsection 3.4.1.3

3.2.4 Packet Reservation Multiple Access

Packet Reservation Multiple Access (PRMA) [Goo89] is an implicit reservation protocol for integrating voice and data over short-range radio channels. The PRMA is closely related to the Reservation Aloha (R-Aloha) protocol [Cro73], in that it merges characteristics of S-Aloha and fixed-assignment TDMA protocols. R-Aloha is a typical protocol for satellite networks and it will be described in Subsection 3.3.1.2. PRMA is distinguished from R-Aloha by its response to network congestion and by its short round trip transmission time. PRMA is designed for star network topology with dispersed stations and a central base station. All stations use a single channel to transmit information packets to the base station. The upstream channel is divided into slots, which are grouped into repetitive sequence of frames. After each time slot, the base station transmits a short acknowledgement packet, which indicates each slot as reserved or available. The short propagation time allows stations to learn quickly the results of transmission attempts. In many cases, an acknowledgment message for the current time slot can arrive at the stations before the beginning of the next time slot, or at most, one slot later. All stations, which have received this information will then update their frame reservation registers, which contain one bit for each slot in the frame, by setting a bit to "0" or to "1" when the corresponding slot is available or reserved, respectively. In addition, the base station schedules the downstream traf-

fic, avoiding contention. In PRMA, stations are grouped into voice and data stations. Voice stations generate voice or periodic information packets, whereas data stations generate random information packets. The voice stations in PRMA use speech activity detectors to obtain a bandwidth efficiency improvement over fixed assignment TDMA protocol. The basic principle of PRMA is to occupy a time slot only during speech talkspurts and release the channel during silent periods. When a talkspurt begins, the voice station uses Aloha protocol to contend with other stations for an available slot. When it successfully transmits a speech packet, it reserves that slot in future frames and there are no subsequent collision with packets from other stations. At the end of the talkspurt, the station releases its reservation by leaving the reserved slot empty and the base station sets the slot to available and all stations can contend for this slot in the future frames. If the voice station does not successfully transmit the first packet, it retransmits the packet with a certain probability in subsequent available slots. The voice packets are discarded if they remain in the station beyond a certain time limit. The number of dropped packets affects the quality of the received speech. A data station transmits random information packets in available time slots. When a random packet is successfully transmitted, in contrast to voice stations, the data station does not obtain a time slot reservation. Instead, the data station has to contend for an available slot for each packet it sends. In the event of a collision, packets are retransmitted usually with lower probability than periodic packets. The random information may experience long delays due to network congestion but no packet loss as the periodic information. PRMA also has the possibility of using the "capture effect" due to near/far phenomenon when two or more stations transmit packets in the same time slot. The capture effect is the ability of the receiver to receive the strongest packet while all other overlapping packets appear as noise. Capture could lead to substantial performance improvements, as in the absence of capture, all contending packets require retransmission. PRMA protocol has been studied extensively [Hon94], and several enhancements were proposed. Enhanced PRMA protocols, such as Centralized-PRMA [Bia97] and Integrated-PRMA [Won92], improve channel efficiency and provide some service fairness for data sources. However, these protocols suffer variable packet access delay, and QoS with bounded delay cannot be guaranteed. In [Ben02] a modified PRMA protocol for LEO satellite networks to support real-time applications, named PRMA with hindering states (RMA-HS), is proposed. Due to long trip delay in comparison to terrestrial mobile systems, here a station may attempt transmissions also while it is waiting for the outcome of a previous attempt. If that attempt has been unsuccessful, a faster access is achieved. Otherwise, further attempts are useless and may hinder the accesses of other stations.

3.3 MAC Protocols for Satellite Networks

In the last decade there has been a tremendous growth in interest among researchers and manufacturers in GEO and LEO satellite networks for providing broadband, as well as narrowband, services to end users. Since the satellite radio-spectrum resource is scarce and very expensive, Medium Access Control (MAC) protocols play a crucial role in satellite communication networks. Hence, a wide range of MAC protocols have been standardized or proposed for satellite networks. All three multi-access technologies (FDMA, TDMA, and CDMA), are used in designing MAC protocols for satellite networks.

- FDMA-based MAC protocols are first protocols to be used in early multiple access schemes for satellite communication.
- TDMA-based satellite MAC protocols are more efficient than FDMA based protocols. In addition, the TDMA protocols are very flexible and promise to fulfill QoS-requirements in future high-speed broadband satellite networks. Hence, in the following subsections, we focus our discussion on TDMA based MAC protocols for satellite networks.
- CDMA-based MAC protocols are by far the least efficient and have been used mainly for military systems.

3.3.1 TDMA Based MAC Protocols for Satellite Networks

The design of a medium access control protocols for a satellite network is determined by two main factors: the nature of the link and the nature of the users. These two factors are also related to each other, as time delay and time jitter requirements of real-time applications depend on Round Trip Delay (RTD). Considering the nature of the link, the most important thing to note is that the bit length of the link for LEO satellites is relatively large, whereas for GEO satellites are very large. Despite the great difference in RTD between LEO and GEO satellites, an immediate implication of the long bit length is that carrier sense techniques will not work on either of these satellite networks. The other determining factor is the nature of the users. In general, it is best to assume that there will be a variety of traffic types generated by different real-time and non-real-time applications. For example, some of the stations may generate real-time traffic with stringent delay requirements, while other stations may generate short bursty traffic with modest throughput requirements but a need for a short delay time (e.g., transactions). Some other stations may generate long streams of traffic that require high throughput, but they may be able to tolerate moderate delays prior to the start of a transmission (e.g., file transfers). Fulfilling all of these requirements is a challenging issue, so there is a wide spectrum of TDMA-based MAC protocols for satellite networks and most of them are based on combinations of the advantages of the individual protocols. In general, in TDMA based MAC protocols for satellite networks, time on the channel is organized in the form of a repetitive sequence of frames, each of which is divided into a number of slots. Furthermore, a certain slot or part of it can be divided in mini-slots, depending upon the protocol type. The allocation of the time slots in most of the satellite MAC protocols is a distributed function carried out by the earth stations. For efficiency goals, it is important that the duration of a frame must be greater than the RTD of the satellite link. This criterion is considered almost in all existing MAC protocols for satellite networks. An interesting property that satellites share with broadband local networks is that a station on earth receives its own transmissions. Thus, a station knows at list a *round trip delay* time after it has ceased transmitting, whether its transmission was successful or suffered collision. This property is exploited almost by all MAC protocols for satellite networks. TDMA based MAC protocols for satellite networks obey the general classification given in the Subsection 3.1.

In satellite networks, there are two TDMA-based fixed-assignment multiple access protocols:

- B-TDMA (Basic TDMA)
- G-TDMA (Generalized TDMA)

Considering the random access class of protocols, S-Aloha is also used in satellite communication networks, as a part of combined protocols for the reservation of the communication channels. Due to long *round trip delay* of satellite links, CSMA is not used in satellite networks.

The best-known protocol from implicit reservation group of protocols is the Reservation Aloha. From the group of protocols with explicit reservation, A-Reservation (Aloha Reservation) and PDAMA (Packet-Demand Assignment Multiple Access) are typical protocols for reservation by contention. In A-Reservation, the reservation process is very simple, whereas in PDAMA, it is more complicated. However, in both protocols S-Aloha is used for reservation request. The following protocols can be classified into the group of reservation without contention: FPODA (Fixed Priority-Oriented Demand Assignment), BBM (Basic Bit-Map Protocol)), BRAP (Broadcast Recognition with Alternating Priorities), BRAM (Broadcast Recognition Access Method), and MSAP (Mini-Slotted Alternating Priorities). Another MAC protocol that can be classified as explicit reservation protocol is PODA (Priority-Oriented Demand Assignment), in which either contention based or contention free reservation request is used. In a satellite communication environment, the most suitable protocols for meeting requirements of multimedia applications are combined protocols. Some of the protocols that can be classified as combined protocols are listed below:

- RRR (Round Robin Reservation),
- SCS (Satellite-Controlled Scheme),
- FODA-TDMA (FIFO Ordered Demand Assignment-TDMA),
- IFFO (Interleaved Frame Flush-Out),
- RUC (Reservation Upon Collision),
- SRUC (Split-channel Reservation Upon Collision),
- ARRA (Announced Retransmission Random Access),
- SRMA (Scheduled Retransmission Random Access),
- RA/DAMA (Random DAMA),
- CFDAMA (Combined Free/DAMA),
- FBA/DAMA (Fixed Bandwidth Allocation/DAMA),
- ARP (Anticipated Reservation Protocol),
- RRAA (Random-Reservation Adaptive Assignmen)t,
- GRAP (Generalized Retransmission Announcement Protocol).

Figure 3-1 shows the classification of the TDMA based MAC protocols for satellite networks. In the following subsections a brief explanation of some of the basic MAC protocols for satellite networks is given.

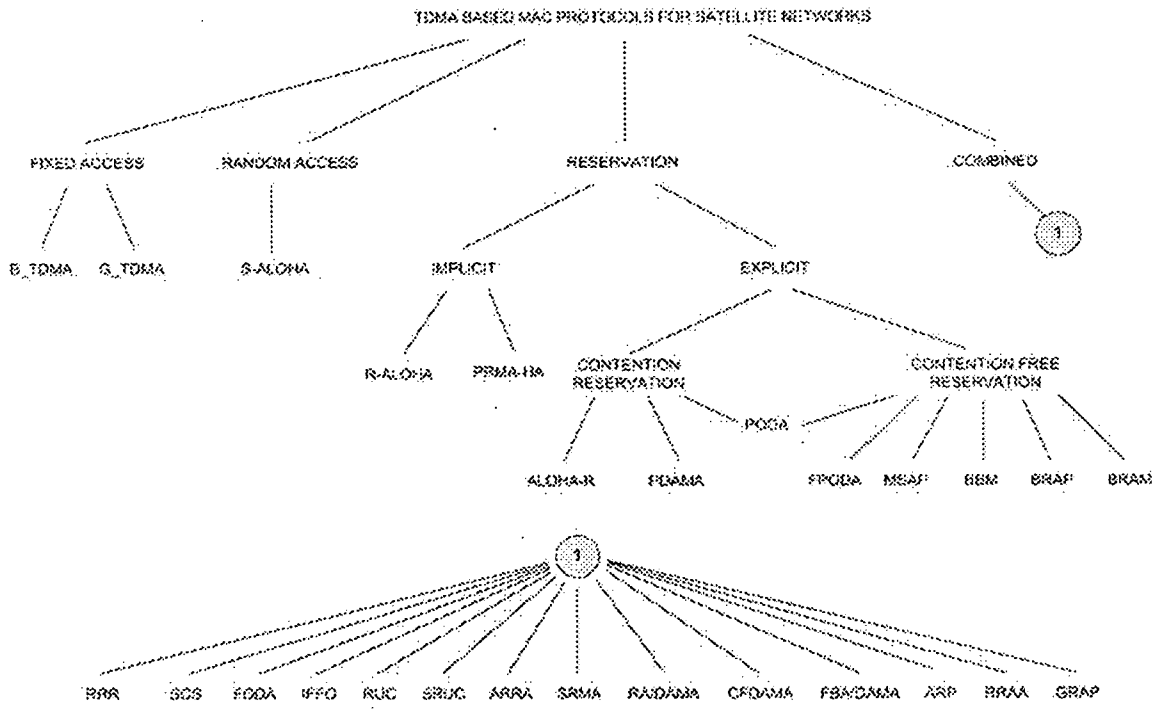


Figure 3-1: TDMA based MAC protocols for satellite networks

3.3.1.1 Basic TDMA and Generalized TDMA

In basic TDMA (B-TDMA) fixed assignment protocol, the time is divided into equal time slots. Each station is allocated equal portions of channel capacity. This is done by dedicating each slot position across the sequence of frames to a particular station. Individual stations take turns using the uplink channel and may put a burst of data in the assigned time slot. The satellite repeats all incoming transmissions, which are broadcast to all stations. All stations must know which time slot to use for transmissions, and which time slot to use for reception. Hence, the satellite also periodically transmits the reference burst, and all stations must synchronize with the reception of the burst. The major disadvantage of the B-TDMA is the requirement that each station must have a fixed allocation of channel time, whether or not it has to transmit. Generalized TDMA (G-TDMA) increases the efficiency by allocating more slots (channel capacity) per frame to

stations that generate more traffic, provided that this is known in advance. This is done by increasing the number of slots per frame, such that they can be proportionally divided among stations. Slots can be allocated continuously or uniformly spaced over each frame.

3.3.1.2 Reservation Aloha

Reservation Aloha (R-Aloha) [Cro73] is a distributed protocol with implicit reservation that merges the characteristics of S-Aloha and fixed-assignment TDMA protocols. Transmission time is divided into slots of equal size, which are further organized into repeated sequences of equal size frames. In general, there are fewer slots per frame than there are stations. R-Aloha is the simplest reservation protocol. A station wishing to transmit one or more packets of data monitors the slots in the current frame. Any slot that is empty or contains a collision is available for the next frame. Stations initially access available slots randomly using S-Aloha. Successful transmission in a slot serves as a reservation for the corresponding slot in the next frame. By repeated use of that slot position, a station can transmit a long stream of data. This protocol supports a dynamic mixture of stream and bursty traffic. If the average message length is long, R-Aloha behaves like a fixed-assignment TDMA scheme. If most of the traffic is bursty, the protocol performs as S-Aloha. In fact, performance could be even worse than S-Aloha if most messages are one slot in length, because after a slot is used, it will remain empty for the next frame as stations cannot realize that it is free. Performance can be improved by including an end-of-use flag in the last packet of the message.

3.3.1.3 Round-Robin Reservation

The Round-Robin Reservation (RRR) protocol [Bin75] is a distributed reservation protocol based in the fixed TDMA assignment. This protocol requires a fixed number of stations less than or equal to the number of time slots in a frame. Each station owns a particular slot position and the owner may use its slot to transmit continuously. If there are any extra slots, these are contended for by all stations using S-Aloha. If the owner station has no data to send, its slot will become empty and available for other stations to use. Stations contend for these unused slots also by S-Aloha. The owner gets its slot back simply by using it. If the transmission is successful, the owner continues to use it. If the collision occurs, then other stations defer and the owner reclaims the slot in the next frame. There are three types of slots available for use in this protocol: fixed assignment slots, slots in excess of fixed-assignment slots, and fixed assignment slots that were unused in the previous frame. An enhancement to the basic RRR protocol is proposed. In the header of each packet that a station sends, it is required to include the length of its own queue of packets. Each station has to keep information about the global queue, which is the sum of the individual queues. A round-robin algorithm is used to allocate available slots to queued packets. By broadcasting its queue length, a station is explicitly reserving future slots. A station that uses its own slot implicitly reserves it for the next frame. Thus, this protocol uses both explicit and implicit reservation. RRR protocol performs better than R-Aloha for stream-dominated traffic, since each station is guaranteed one slot of channel capacity. This protocol allows the combination of fixed bit rate traffic and best-effort traffic. However, for a large number of stations, it can lead to a large delay because of the required number of slots per frame.

3.3.1.4 Aloha Reservation

Aloha Reservation (Aloha-R) [Rob73] is a distributed reservation protocol that uses exclusively explicit reservations. A frame is divided into equal-length slots, one of which is further divided into minislots. The minislots, acquired via S-Aloha, function as a common queue for all stations. The data slots are used on a reservation basis and are conflict-free. The number of slots is adapted to the current load. A station wishing to transmit sends a request packet in a minislot specifying the number of slots desired, up to a maximum number. If the reservation is successful, the station then determines which future slots it has acquired and transmits in them. To do this, each station is required to maintain a global queue that holds the information on the num-

ber of outstanding reservations. When each frame is received, the station adds to the global queue the sum of all successful reservations (including its own) and subtracts the number of slots containing data. When a reservation is successful, the station determines by the FIFO discipline when it owns reservation begins and sends its data. Performance analysis of this protocol [Sta94] shows that it is a significant improvement to S-Aloha. However, for lengthy streams, Aloha-R requires a user to contend for slots repeatedly, which results in significant delivery delay variance if there is much traffic. Setting the maximum reservation size high enough to allow complete stream transmission can alleviate this but causes long delays in beginning transmission to other traffic.

3.3.1.5 Fixed Priority-Oriented Demand Assignment

Fixed Priority-Oriented Demand Assignment (FPODA) is a centralized reservation protocol used in the Universe Network [Wat84]. This network ties together six local networks scattered around the United Kingdom with a data rate of 1 Mbit/s. A frame length is 130 ms and each frame begins with six minislots, one dedicated to each of the six stations. A minislot is 100 bytes in length, and may be used by its station to transmit data or a reservation request. FPODA is one of the simplest centralized reservation protocols. One of the six stations acts as a master and allocates time on the channel based on reservation requests (including its own). The master splits the remainder of the frame (after the six minislots) into one to six variable-length slots, with each slot assigned to a particular station. A station sends a reservation to request a particular service with a choice of priority, normal, and bulk. Priority requests are always served first on the FIFO bases. If there is any time remaining in the frame, it is divided among normal requests proportional to the throughput estimates (bytes per frame) provided by the stations. In turn, if there is any time remaining after that, it is divided equally among all stations with bulk requests. FPODA is an effective protocol when a small, fixed number of stations share the channel capacity.

3.3.1.6 Satellite-Controlled Scheme

The Satellite Controlled Scheme (SCS) is a centralized reservation protocol that employs the satellite rather than an Earth station to make reservations [Sud83]. It is designed to support a mixture of stream and bursty traffic. Each frame consists of a reservation subframe, an unreserved subframe, and a reserved subframe. The frame starts with the reservation subframe, which consists of a set of reservation minislots. The reservation subframe is followed by the unreserved subframe, which consists of data slots (intended for bursty traffic) that station contends for using S-Aloha. Finally follows the reservation subframe of data slots that may be reserved for stream traffic. To acquire slots in the reserved subframe, a station contends for a minislot in the reservation subframe using S-Aloha to transmit a reservation. A reservation consists of the Earth station identifier. If a reservation is successfully received at the satellite and if at least one slot is free in the reserved subframe, the satellite immediately sends an acknowledgment in the same minislot. The acknowledgment consists of a slot position within the reserved subframe, and upon receipt of the acknowledgment, the Earth station can then use the reserved slot in each succeeding frame until it transmits an end-of-message flag. This signals the satellite to release the slot for future use. An important timing constraint is related to the length of the unreserved subframe. This subframe must be longer than the RTD in order for earth stations to know whether or not its reservation was successful before the beginning of the reserved subframe in the same frame. This results in more efficient use of reserved slots.

3.3.1.7 Split Reservation Upon Collision

The Split Reservation upon Collision (SRUC) [Bor78] protocol combines S-Aloha and reservation protocols and switches from one to the other according to the state of the channel. In SRUC, the frame is divided into L slots. Each slot is subdivided into one data subslot and several minislots (control subslots). A data subslot is used to transmit fixed size data packets. The

minislots are used to transmit control information. The number of minislots for each slot is [N/L], where N is the number of stations and [x] is the smallest integer not less than x. SRUC divides the stations into a number of groups. The size of the control subslot becomes smaller, because each of them serves only some of the stations. The data subslot can be in a random or reserved mode. A station in random mode can continuously transmit packets in data subslots using S-Aloha protocol and transmit control information in its minislots, and access to minislots is collision-free. The control information contains information on outstanding packets (including unconfirmed packets) the station has at that time. When a collision is detected and control information is received, the data subslot switches to reservation mode. In the reservation mode, a station with packets to transmit sends control information in one of its own minislots to reserve data subslots. All stations receive this information. Hence, there is one global queue of reservations with FIFO priority, and the number of data subslots reserved is calculated on the basis of the information contained in a control information minislot. The number of data subslots in a minislot includes the number of outstanding packets yet to be confirmed. Therefore, this number should be decremented by the number of packets successfully received. The data subslot remains in the reserved mode until the global queue is empty (until all collided packets have been successfully transmitted). Thus, the previously contended stations do not mix with new ones. Hence, the SRUC protocol is always stable since all colliding packets are retransmitted in the reserved mode.

In the following tables the main characteristics for each group of the TDMA based MAC protocols for satellite networks are given..

Table 3-1 : Fixed Access Protocols

Protocol	Throughput	Mean delay	Coordination
B-TDMA	0.8	medium-high	distributed
G-TDMA	0.85	medium-high	distributed

Table 3-2: Random Access Protocols

Protocol	Throughput	Mean delay	Coordination
S-Aloha	0.36	low	distributed

Table 3-3: Implicit Reservation Protocols

Protocol	Throughput	Mean delay	Coordination
R-Aloha	0.75	medium	distributed
PRMA-HS	medium	medium	distributed

Table 3-4: Implicit Reservation Protocols

Protocol	Throughput	Mean delay	Coordination
Aloha-R	0.6	medium	distributed
PDAMA	medium-high	medium	centralized

Table 3-5: Explicit Reservation Protocols

Protocol	Throughput	Mean delay	Coordination
PODA	medium-high	med	distributed
FPODA	medium	medium-high	centralized
MSAP	high	medium	distributed
BBM	high	low	distributed
BRAP	high	medium	distributed
BRAM	medium	medium	distributed

Table 3-6: Combined Protocols

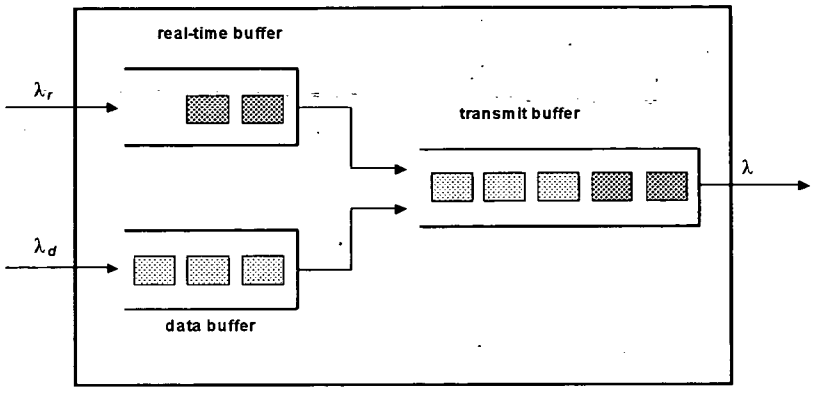
Protocol	Throughput	Mean delay	Coordination
RRR	medium-high	medium	distributed
SCS	medium-high	medium	centralized
IFFO	medium-high	medium	distributed
RUC	high	medium	distributed
SRUC	high	low-medium	distributed
ARRA	med	low	distributed
SRMA	high	low	distributed
FODA	medium-high	medium	centralized
ARP	medium-high	medium	centralized
RA/DAMA	medium-high	low-medium	centralized
CFDAMA	medium-high	medium	centralized
FBA/DAMA	medium-high	low-medium	centralized
RRAA	medium-high	medium	centralized
GRAP	high	low	centralized

3.3.2 A Random-Reservation MAC Protocol for Satellite Networks

Since sharing the limited satellite radio spectrum resource is essential, the design of flexible and efficient Medium Access Control (MAC) protocols is a key element in providing QoS in satellite communication networks. In this subsection, a new random reservation TDMA based MAC protocol [Lep01] for satellite networks, efficiently supporting real-time services, is presented. This protocol represents a combination of the so-called Extended ARRA (E-ARRA) [Ray85] [Kor00] and the Aloha-R protocols. It can be classified into the combined class of MAC protocols, while it can also be viewed as a broadcast protocol with distributed control. We have combined the above-mentioned protocols to accommodate two types of traffic with different requirements and priorities. In principle, the frame structure of the basic E-ARRA scheme, in which a potentional retransmission slot is announced in case of data packets collision in a frame-by-frame manner, is used for the proposed protocol. The characteristic feature of the proposed access protocol is the switching from random access mode to reservation mode depending on the traffic class, like non real-time or real-time applications, as well as implicitly the current state of available network bandwidth, like low or high-traffic loads. In general, data traffic is transmitted using the E-ARRA protocol in which new arrivals are separated from retransmitted messages to avoid excessive collisions. For higher priority traffic (real-time traffic), the protocol is switched to the Aloha-R mode, whereas the non real-time traffic is still accommodated by the Extended ARRA scheme. The proposed protocol is, in principle, capable of working in both LEO and GEO satellite environments, even though E-ARRA was originally designed for GEO satellites. The protocol performance is analyzed by discrete-event simulations.

3.3.2.1 Access Protocol Description

The considered system architecture consists of network stations, each maintaining a real-time buffer for storing real-time messages and a data buffer in which the non real-time traffic (data messages) is placed. Furthermore, the real-time traffic is given priority over data traffic in the transmit buffer. Each station first checks its real-time buffer and then the data buffer, as illustrated in Figure 3-2.



$\lambda_r = r\lambda$; λ – mean arrival rate, r – real time traffic fraction

Figure 3-2: Transmit Buffer Prioritization

The proposed media access protocol can functionally be divided into the non- real-time traffic and the real-time traffic transmission part. The underlying transmission frame structure is shown in Figure 3-3. In this frame structure, the E-ARRA protocol, which is used for data transmission and an Aloha-R based protocol, applied for real-time transmission, are appropriately incorporated.

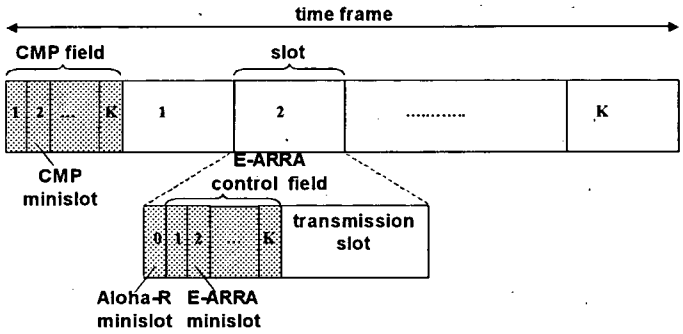


Figure 3-3: Frame Structure of the Proposed Protocol

The time frame consists of K slots and a so-called CMP (Common Mini-Pool) field, also divided into K CMP minislots. Furthermore, each slot consists of a transmission slot, an Aloha-R minislot, and an E-ARRA control field made up of K E-ARRA minislots. In a transmission slot, both real-time and data packets may be transmitted. Note that the CMP field and the E-ARRA control field are assigned for retransmission announcements in case of the data transmission protocol, while the Aloha-R minislot obviously is dedicated to reservation requests for the real-time transmission protocol. Of course, the lengths of the control minislots are much smaller than those of the transmission slots. The meaning of control fields and the detailed description of the proposed protocol (differentiated between the individual parts) are described in the following sections.

3.3.2.2 Data Transmission

The protocol used for the transmission of data traffic is based on the E-ARRA scheme. E-ARRA is generally suitable for satellite links with long round-trip propagation delays. Figure 3-4 shows the algorithm of the MAC protocol for non real-time data transmission. The protocol works as follows. Stations monitor transmission on both transmission slots and minislots and are able to of storing feedback information for one frame. When a source station has a data packet to transmit, in the next frame, it randomly selects one of the free slots according to a status table $A_{1\times K}$ (Table 2, in the flow diagram shown in Figure 3-4), which captures all the free slots out of K slots for the next frame) maintained at each station. Then, the station also randomly chooses one of K retransmission announcement minislots (E-ARRA minislots) of the selected free slot. In the selected minislot the station sends out an E-ARRA control packet in

order to indicate the slot (according to the minislot number within the E-ARRA control field) where the corresponding data packet will be retransmitted in case of a data packet collision in the first attempt. This control packet transmission is followed by the corresponding data packet transmission in the selected transmission slot. Then the station waits for round trip delay for the feedback.

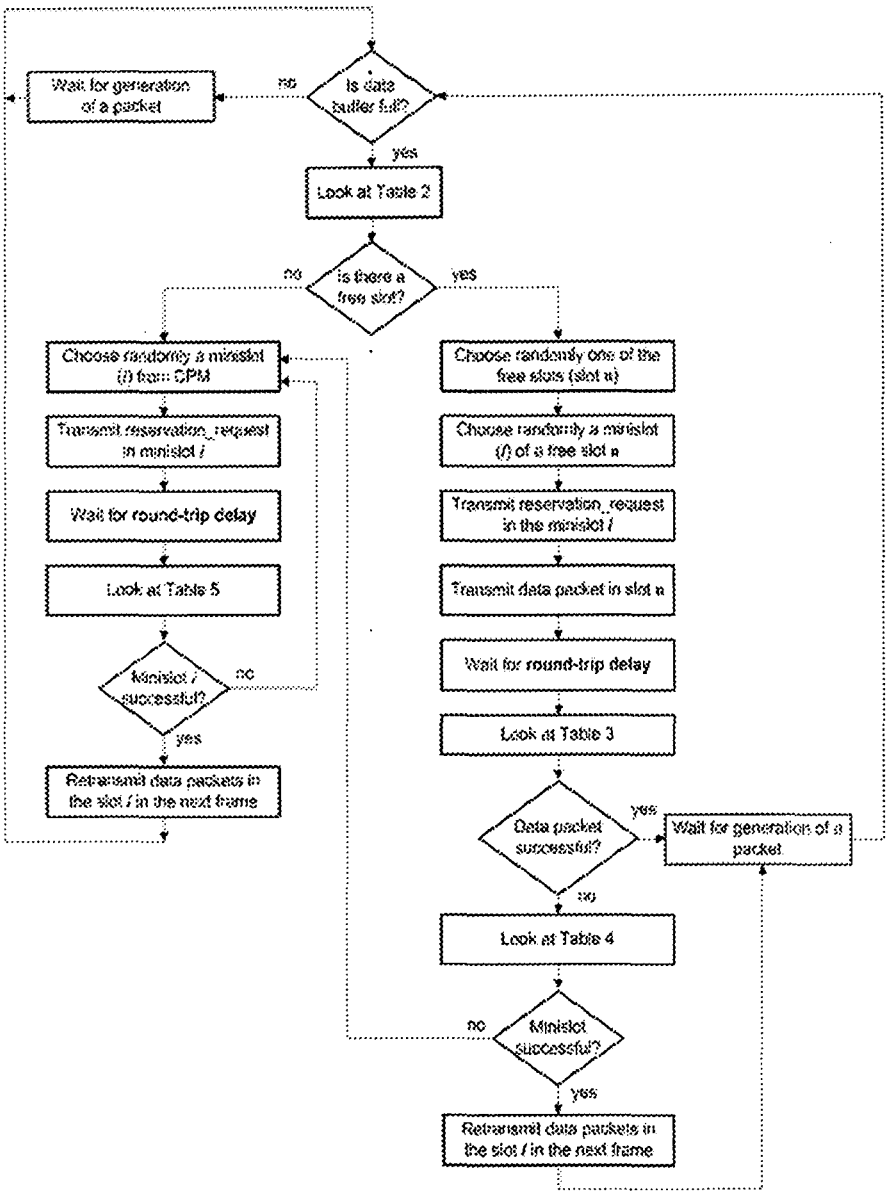


Figure 3-4: Algorithm of the non real-time traffic MAC protocol

Having received the feedback, the station updates the status table of the data packets (Table 3). If the transmission was successful, station waits for generation of a new packet. If the transmission of the data packet failed, station checks the status table of the E-ARRA minislots (Table 4). If the transmission was successful, station transmits the data packet in the reserved transmission slot of the next frame. When both the data packet and the corresponding E-ARRA control packet collide, or when there is no free slot in the next frame, station selects randmomly one of the CMP minislots and transmits the reservation request. After waiting for round trip delay, station updates the status table of the CMP minislots (Table 5). If the transmission is successful, station transmits data packet in the reserved slot of the upcoming frame. Station transmits a CMP control packet repeatedly until it successfully reserves a slot according to the position of

this control packet within the CMP field. In this way, retransmissions are efficiently separated from new transmissions avoiding excessive packet collisions. Note that the status information regarding the following frame is broadcast by the individual stations via satellite, thereby allowing that each station may calculate the set $A_{1\times K}$ in a distributed manner before the next frame begins.

3.3.2.3 Real-Time Transmission

The transmission of real-time messages (shown in Figure 3-5) is done similarly to in the Aloha-R scheme, i.e., a certain slot within the frame is reserved first by sending out an Aloha-R control packet in the Aloha-R minislot before all the real-time packets derived from the same real-time message may be successively transmitted in the same slots frame-by-frame.

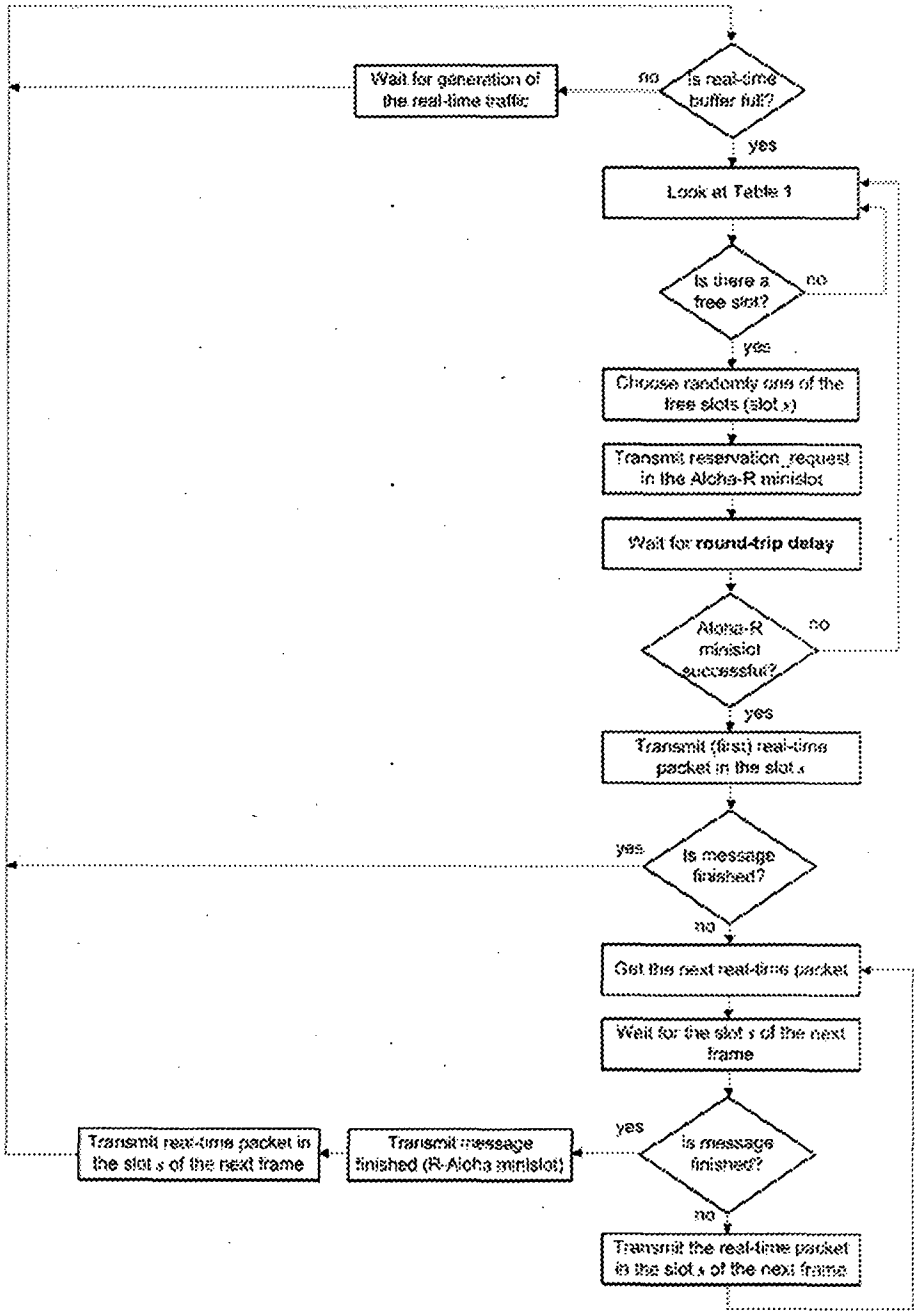


Figure 3-5: Algorithm of the real-time traffic MAC protocol

The Aloha-R minislot has to be chosen such that it belongs to a free slot according to a set $R_{1\times K}$ (Table 1 in the flow diagram shown in Figure 3-5) keeping track of the reservation status (only according to Aloha-R) of the K transmission slots. Moreover, the set associated with the data transmission protocol, i.e., $A_{1\times K}$, represents the intersection of set $R_{1\times K}$ and a set $A^*_{1\times K}$ (indicating the retransmission reservation status of all K slots only according to E-ARRA, i.e., due to data traffic). As a result, the reservation of slots for real-time transmission has higher priority than the reservation of retransmission slots for non real-time traffic. Note that the first real-time packet of a real-time message is transmitted after having waited for a round-trip propagation delay to detect whether the corresponding R-Aloha control packet has been transmitted successfully (without having experienced collisions with other stations with a real-time message to transmit). Along with the transmission of the last real-time packet of a real-time message, again an R-Aloha control packet is sent in order to inform all the other stations about the release of the corresponding slot from the next frame on. Thus, for each real-time message to be transmitted, at least two R-Aloha control packets have to be sent, namely, for the head-of-line and tail-of-line packets.

3.3.2.4 Performance Evaluation

In order to evaluate the behaviour of the protocol a performance study is carried out by means of discrete-event simulation. We have taken the network throughput, the mean packet access delay and the mean real-time session connection set-up time as performance measures. The mean packet access delay is defined as the amount of time elapsed since a packet (acquired from a message) has reached the first place of the transmit queue until the packet has been successfully transmitted by the source station. The connection set-up time is the time needed for a successful slot reservation, i.e., the time until the first real-time packet corresponding to a real-time session is allowed to be transmitted. Concerning the traffic pattern, we assume a homogeneous load derived from a Poisson process with mean arrival rate λ. We assume the message lengths for both real-time and data traffic to be exponentially distributed with mean value $l = 5$ slots. Further note that the arrival rate of the real-time traffic is given by $\lambda_r = r\cdot\lambda$, where r (set to 0.2) denotes the fraction of the overall station traffic represented by real-time traffic. The buffer size is assumed infinite.

Comparison with the Extended ARRA Protocol

To demonstrate the major benefits of our proposed media access protocol, we have compared its performance with the E-ARRA scheme using prioritization of real-time traffic at the transmit buffer. Figure 3-6 shows the results in terms of the packet access delays/network throughput characteristics for M = 50 stations, a Round Trip Delay (RTD) of 10 frames, a slot duration of 1 kbit, and different numbers of slots K per frame. Concerning the mean packet access delay for the real-time traffic (left-hand side), it can be clearly observed that the new protocol highly outperforms the E-ARRA scheme for different numbers of slots K. In addition, it may be stated that the higher K is, the larger is the delay difference (about 75 slots for K = 8) since a larger number of slots could be reserved for real-time transmission in a frame when K is increased. Conversely, when K is decreased, the probability of finding a free slot before the reservation procedure is reduced, resulting in a smaller performance gap between the protocols. In terms of the delays for the data traffic case, one can see that our protocol does not lead to significant degradations compared to the E-ARRA case. Thus, we achieve a rather beneficial access delay balance between real-time and data traffic, whereas the throughput remains almost the same. Note that due to the fact that the transmit buffer prioritization has no impact on the packet access delays, the corresponding curves belonging to the E-ARRA case are almost identical.

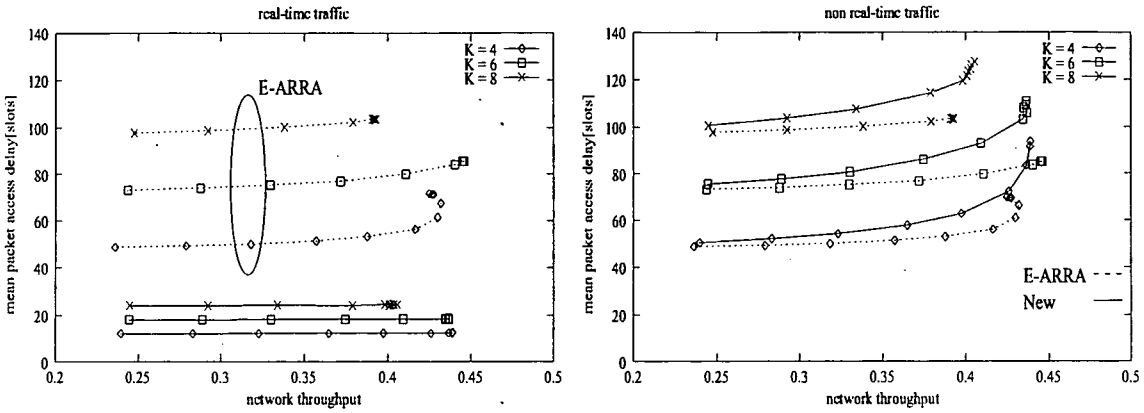


Figure 3-6: Packet access delay/throughput for different values of *K*.

In Figure 3-7 the protocols' dependence on the round trip propagation delay (given in frames, a frame contains K = 6 slots) is illustrated. For GEO satellite networks, the *round trip delay* is about 250 (240-270) ms, whereas for LEO satellites about 15 (10-20) ms. It is noticeable that higher *round trip delays* (corresponding to GEO satellite networks) significantly degrade the performance of both schemes. Again, our protocol exhibits superior real-time performance. Furthermore, in terms of data transmission performance, the degradation is still kept to a satisfactory amount.

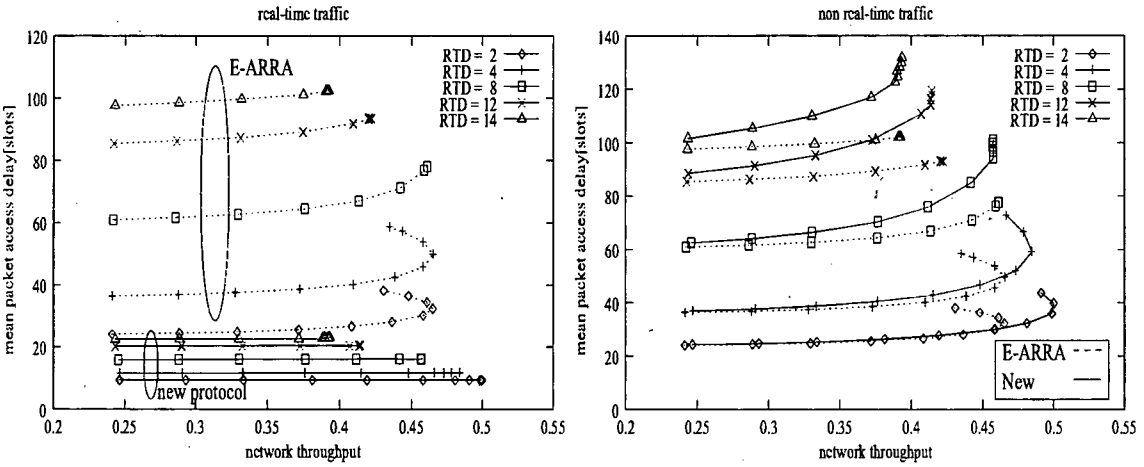


Figure 3-7: Packet access delay/throughput for different round-trip delays.

In general simulation results show that the proposed protocol highly outperforms the E-ARRA scheme considering delay- throughput behaviour for real-time traffic. Thus, the QoS requirements in terms of multimedia traffic may be fulfilled by this novel protocol in an efficient way.

Case Study

Figure 3-8, shows the connection set-up time for real-time traffic versus throughput for different Round Trip Delay (RTD) values, expressed in frames with K = 6. From the plots it can be seen that as RTD increases the mean connection set-up increases while the throughput drops. For example for RTD = 2 frames = 10 ms (1 frame = 5 ms, 1 slot = 0.83 ms), which corresponds to LEO satellite case, the mean connection set-up time is 23 slots (19 ms). For RTD = 14 frames = 70 ms, which corresponds to MEO satellites, the mean connection set-up time is 100 slots (83 ms). This is obvious, since the greater the distance to a satellite needs longer connection set-up time. From the plots the impact of frame length on connection set-up time can also be analyzed. For the case of the LEO satellite we assume RTD = 10 ms and consider the RTD = 2 frames and

RTD = 14 frames curves. For the RTD = 2 frames (1 frame = 5 ms) the connection set–up time of 19 ms (23 slots) is obtained corresponding to the channel bit rate of 1.2 Mbit/s, whereas link-capacity is 7.2 Mbit/s. For the RTD = 14 frames case (1 frame = 0.7 ms), the connection set-up amounts to 12 ms (100 slots), where the corresponding values for channel bit rate and link capacity are 8.4 Mbit/s and 50 Mb/s respectively. A similar case study has been carried out for GEO satellites. If we assume RTD = 240 ms, from the RTD = 2 frames (1 frame = 120 ms) curve, the connection set-up time amounts to 460 ms (channel bit rate 50 kbit/s, link capacity 300 kbit/s), whereas for RTD = 14 frames (1 frame = 17 ms), the connection set-up time is 285 ms (channel bit rate 350 kbit/s, link capacity 2.1 Mbit/s). Obviously, shorter frames result in better transmission delay than longer frames. This leads to the conclusion that the number of frames and their durations are very important system parameters in MAC protocols for satellite networks, especially for real-time traffic transmission. In practice the frame length lies in the range 0.75 - 20 ms [Pey95], which is the case for LEO satellites when RTD = 14 frames (frame length 0.7 ms) and GEO satellites RTD = 14 frames (frame length is 17 ms). The decrease in throughput as the RTD increases (number of frames increases) can be explained as a result of the signalling overhead and is primarily due to the fact that the indication of real-time session termination needs a longer time period (with higher numbers of frames), in which the slots still remain reserved and thus unused.

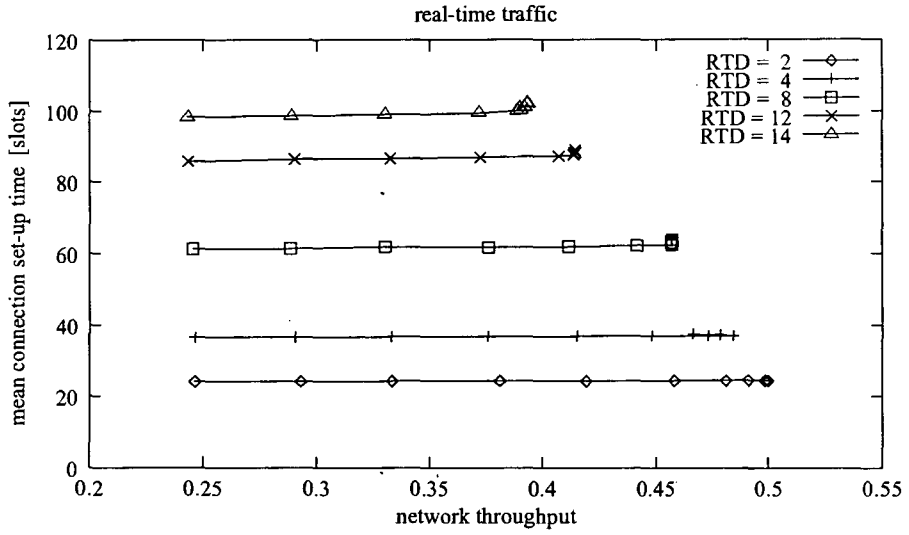


Figure 3-8: Connection set-up delay/throughput for different round-trip delays.

3.4 MAC Protocols for IEEE 802.11 WLAN Networks

The IEEE 802.11 WLAN standard defines the MAC sublayer and the Physical Layer (PHY) of the OSI (Open System Interconnection) network reference model, adapted to the special requirements of WLANs. The most important functions of a wireless MAC sublayer include controlling medium access, maintaining QoS, and providing security. In this section, the basic MAC mechanisms for WLAN will be presented, whereas MAC protocols to support QoS in WLANs will be explained in the Chapter 5. The IEEE 802.11 MAC sublayer has two different medium access mechanisms: the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF). The DCF is the basic access mechanism of IEEE 802.11 and its implementation is mandatory in all stations of a WLAN. However, the DCF does not support time-bounded services. The DCF can be used both in ad-hoc and infrastructure network. The PCF uses a central-controlled polling method, which needs a Point Coordinator (PC) controller at the Access Point (AP) to determine which STA currently has the right to transmit. Hence, the PCF is only used in infrastructure network configurations and is built on top of the DCF. However, unlike the DCF, an implementation of the PCF is optional and it aims to provide a time-bounded

service to different applications. Therefore, the PCF has higher priority than the DCF, and it starts transmissions after a PCF Interframe Space (PIFS) time interval, which is shorter in duration than a DIFS (DCF Interframe Space). In the following subsections, the most important characteristics of the DCF and PCF mechanisms will be presented in some more detail.

3.4.1 Distributed Coordination Function

The basic and mandatory 802.11 MAC protocol, the Distributed Coordination Function (DCF), as its name implies, is a distribution medium access mechanism that uses the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme. The basic idea of CSMA/CA is that stations listen to the medium before transmission (CSMA component) and if the medium is busy, stations perform a backoff procedure to minimize possible collisions (CA component). In order to further minimize collisions a refinement of the CSMA/CA method may be used under various circumstances. The refinement consists of introducing two short control frames: Request-To-Send (RTS) and Clear-To-Send (CTS), which the source and destination STA exchange after determining that the medium is idle prior to data transmission. RTS/CTS can be considered as means for medium reservation. In the following the basic CSMA/CA, backoff procedure, fragmentation, and RTS/CTS mechanism are described

3.4.1.1 Basic Access Mechanism and Backoff Procedure

According to CSMA/CA, each station (STA) before attempting to transmit first checks whether the medium is idle. If the medium has been sensed as being idle for a minimum duration called the DCF Interframe Space (DIFS), which is 34 μs for 802.11a, whereas 50 μs for 802.11b, a STA can access the medium immediately and begin to transmits MAC Service Data Units (MSDUs) or a MAC frame of arbitrary length (up to 2304 bytes). If the medium is busy, the STA shall defer until the end of the current transmission. When the current transmission is over and the medium is sensed idle again, the STA has to wait for the duration of DIFS and then enters a contention phase (starting a backoff procedure) with other stations trying to access the medium. In the contention phase the STA chooses a random backoff time within a Contention Window (CW). This additional waiting time is measured in multiple slots. Slot time is derived from the medium propagation delay, transmission delay, and other PHY dependent parameters. Slot_time for 802.11b is 20 μs whereas for 802.11a it is 9 μs. If the backoff waiting time is over and the medium is still idle, the STA can access the medium immediately and initiate the transmission. The basic CSMA/CA mechanism is shown in Figure 3-9

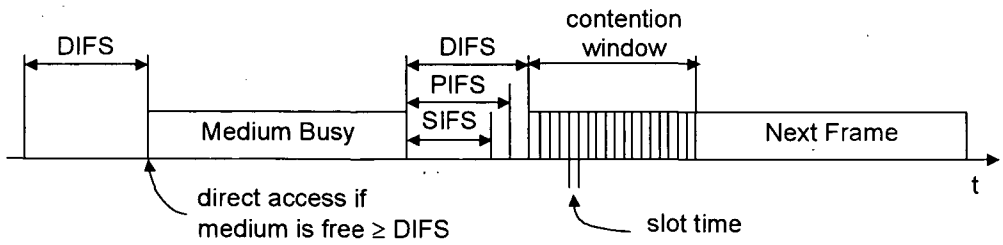


Figure 3-9: Basic Access Method

The random backoff time is computed as follows:

$$\text{Backoff Time} = \text{Random}() * \text{SlotTime} \qquad (3\text{-}1)$$

Here, Random() is a pseudorandom integer drawn from a uniform distribution over the interval [0,CW]. CW is an integer within the range of values $CWmin \leq CW \leq CWmax$, depending on the PHY characteristics. For a given PHY the Cwmin and Cwmax are fixed values. This means that in DCF all stations and traffic classes have the same priority to access the wireless medium, so different delay and bandwidth requirements of applications are not supported. For 802.11b

WLAN the bounded values of CW are: CWmin = 31 and CWmax = 1203. The CW parameter starts from the initial value of CWmin. If the transmission is not successful, a collision is considered to have occurred. To reduce the probability of collision, the contention window is doubled until a prededefined maximum value.CWmax is reached. Once it reaches CWmax, the CW shall remain at the value of CWmax until the transmission is successful or discarded. To improve the channel utilization, after each successful transmission, the contention window is reset to a predefined CWmin.

By selecting a different random backoff time for different stations, the backoff procedure reduces the possibility of collision. To begin the backoff procedure, a STA shall set its Backoff Timer to a random backoff time using Equation (3-1). During each slot of backoff time a STA uses the carrier-sense mechanism to detect the medium. If the medium is determined to be idle for the duration of a particular backoff slot, then the backoff timer decrements the backoff time for one slot time. If the medium is determined to be busy during a backoff slot, then the backoff procedure is suspended. In order to resume the backoff procedure, the medium shall be determined to be idle for the duration of a DIFS. As soon as the backoff timer expires, the station can begin to transmit. Another point is that stations do not select a new random backoff time, but continue to count down the time of the deferred backoff in progress after sensing a channel as being idle again. In this manner, stations that deferred from channel access because their random backoff time was larger than the backoff time of other stations are given a higher priority when they resume the transmission attempt. To determine the state of the medium physical and virtual carrier-sense functions are used. The medium is considered idle only when both functions indicate an idle medium, otherwise; the medium is considered busy. A physical carrier-sense mechanism is provided by the PHY according to the individual PHY specifications. A virtual carrier-sense mechanism is provided by the MAC sublayer. This mechanism is referred to as the Network Allocation Vector (NAV). The NAV maintains a prediction of the state of the medium based on duration information that is carried in data frames. Each STA maintains a local NAV. Unlike wired networks (using CSMA/CD), in a wireless environment collision detection is impossible, as stations cannot hear their own transmission due to the significant difference between transmitted and received power levels. Hence, a positive acknowledgement is used to notify the sender that the transmitted frame has been successfully received. The transmission of the acknowledgement is initiated after SIFS (Shortest Interframe Space) time interval (16 μs for 802.11a) following the end of the reception of the previous frame. Since the SIFS is smaller than the DIFS, the receiving station does not need to sense the medium before transmitting an acknowledgement. If the acknowledgement is not received, the sender assumes that the transmitted frame was lost and schedules a retransmission and then enters the backoff process again.

3.4.1.2 Fragmentation of MAC Frames

It is well known that, due to channel characteristics, wireless links have much higher bit error rates than wired links, resulting in a higher rate of the erroneous MAC frames. Hence, to increase the reliability of MAC frame transmission, the IEEE 802.11 standard specifies a fragmentation mechanism. Fragmentation divides large MSDUs into several smaller data frames or fragments, which can then be transmitted sequentially as individually acknowledged data frames. Fragmentation is accomplished at the transmitter and should be transparent for a user. At each receiver data fragments should be recombined into a single MSDU. Since an error in a large frame wastes more bandwidth and transmission time than an error in a shorter frame, fragmentation may also increase the efficiency. However, the obvious drawback to the fragmentation process is the increased overhead due to multiple ACKs. To minimize this drawback an optimization parameter named fragmentation-threshold is specified to control the usage of fragmentation. This means that only when the MAC frame size is larger than this threshold, will the frame be partitioned into several smaller frames. It is also important to note that only MAC frames with a unicast receiver address are to be fragmented. Broadcast/multicast frames are not

to be fragmented, even if their length exceeds the fragmentation-threshold. Transmission of a fragmented MAC frame is shown in the Figure 3-10.

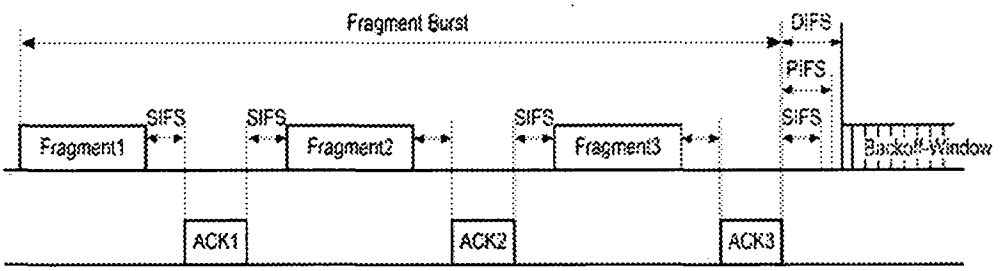


Figure 3-10: Transmission of Multiple fragments using SIFS

The following is a description of a MAC frame transmission using fragmentation. A source STA sends the fragments in order and they are individually acknowledged by the destination STA. This process of sending multiple fragments is defined as a fragment burst. The source STA sends the first fragment of the burst after a waiting time of DIFS and a random backoff time, if the medium was initially busy. Having transmitted the first fragment the STA shall release the channel and immediately monitor the channel for an acknowledgment. If the receiver of the data transmission receives Fragment1, it acknowledges it with an ACK1 message after waiting for SIFS. Having received the ACK1, to transmit the next fragment (Fragment2) the STA has to wait only for SIFS, which is shorter than DIFS. Hence, transmission of the fragmented MAC is not interrupted by new transmissions. The STA shall continue to send the subsequent fragments in the same manner until either all fragments of a single MAC frame have been sent or an acknowledgment is not received. If the transmission of the fragment burst is interrupted because the source STA does not receive an acknowledgment frame, the STA shall resume transmission and try to retransmit the failed fragment after contending for the channel again. After the destination STA acknowledges the last fragment of the particular MAC frame, all stations can compete for the medium again after having waited for DIFS.

3.4.1.3 RTS/CTS Mechanism

As CSMA/CA cannot detect hidden stations, the so-called hidden station problem is also inherited by WLANs. Thus, if a hidden terminal transmits at the same time as another sender, a collision might occur at the receiver. To alleviate the hidden station problem, the IEEE 802.11 standard defines an optional Request-to-Send/Clear-to-Send (RTS/CTS) mechanism known also as the MACA protocol. The RTS/CTS mechanism consists of introducing two short control frames, RTS (Request-to-Send) and CTS (Clear-to-Send), which the source and destination STA exchange after determining that the medium is idle prior to data transmission. These frames contain the name of a sender and a receiver as well as a duration/ID field to define the period-of-time needed to transmit the next data frame and the corresponding ACK frame for a particular sender. Actually, the RTS/CTS mechanism reserves the medium for one sender exclusively. The RTS/CTS mechanism is illustrated in the Figure 3-11.

The MACA protocol works as follows. The source STA sends a short RTS frame (20 bytes) after waiting for DIFS. Every station receiving this RTS now has to update its Network Allocation Vector (NAV) timer, in accordance with the duration filed information, and will not start any transmissions during this time-period. The local NAV at each station specifies the earliest point in time at which the particular station can try to access the medium again. When the destination STA receives the RTS, it answers with a CTS frame after waiting for SIFS. All STAs receiving this CTS frame have to update their NAV, according to the duration field of CTS frame, which is the same as the duration field of the RTS frame, and will also not start any transmissions. Note that the set of receiving STAs need not be the same as the set of STAs re-

ceiving the RTS packet. When the source STA receives the CTS, it starts transmitting its frame after waiting for SIFS, being sure that the channel has been reserved for it during the entire frame transmission duration. Finally, the frame arrives at the destination STA, which after waiting for SIFS sends an acknowledgment frame that completes the transmission of a data frame. To transmit a new frame a STA has to repeat the same procedure again.

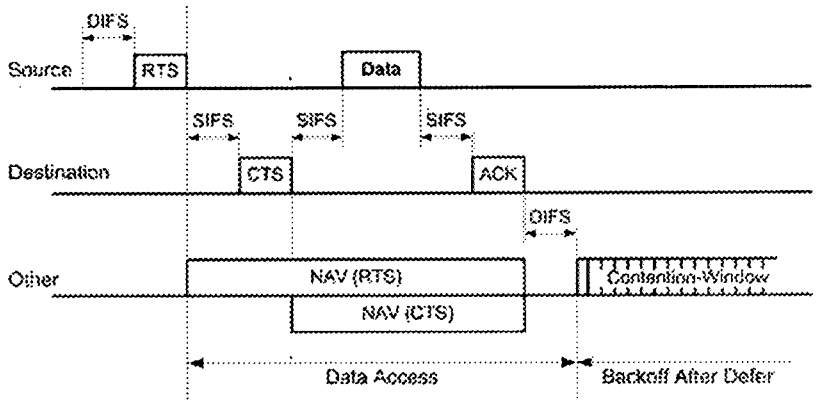


Figure 3-11: RTS/CTS /Data/ACK and NAV Setting

It is obvious that within the RTS/CTS mechanism a collision can only occur at the beginning when the RTS is sent. Note that a collision of the small RTS frames (20 bytes) is less severe and probable than a collision of much larger MAC frames (2304 bytes). Furthermore, with fragmentation of MAC frames, multiple ACKs are transmitted, whereas with RTS/CTS the MSDU can be efficiently transmitted in a single data frame. However, RTS/CTS results in overhead causing wasted of bandwidth and higher delays. This overhead of sending RTS/CTS frames becomes considerable when data frame sizes are small. Therefore, an RTS threshold is needed to determine when to enable or disable the optional RTS/CTS mechanism. Even though the mechanism is optional, every 802.11 station has to implement it in order to know how to handle the reception of a RTS/CTS control frame. It also should be noted that the RTS/CTS mechanism cannot be used for MPDUs with broadcast and multicast addresses because there are multiple destinations for the RTS, and thus potentially multiple concurrent senders of the CTS in response.

3.4.1.4 RTS/CTS with Fragmentation

The IEEE 802.11 standard has also defined the usage of the RTS/CTS mechanism in combination with fragmentation, as illustrated in Figure 3-12.

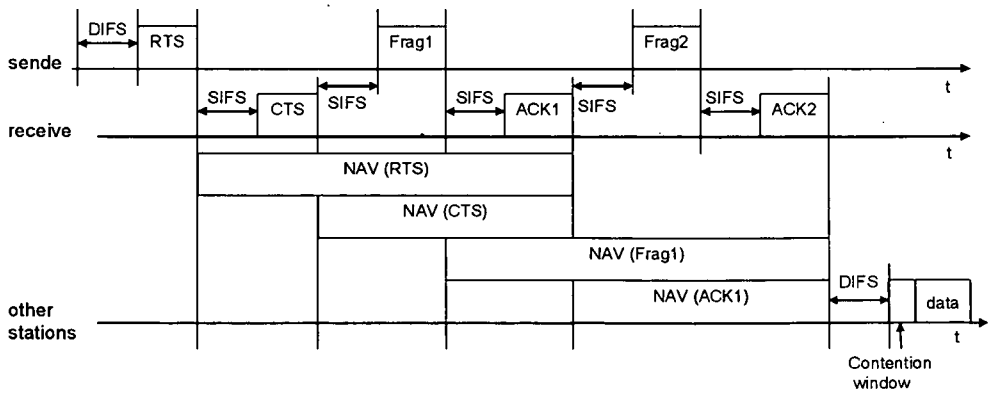


Figure 3-12: RTS/CTS with Fragmented MSDU

The new aspect of this fragmentation scheme is that the duration/ID field is included in each data fragment and acknowledgment frame (ACK), in addition to the RTS/CTS frames. The duration/ID field in RTS/CTS frames defines the duration of the first fragment (Frag1) and corre-

sponding acknowledgment (ACK1). Hence, this duration information is used to update the NAV to indicate busy until the end of ACK1. The duration/ID field in the MAC frame and acknowledgment frames gives the total duration of the next fragment and acknowledgment. Hence, both Frag1 and ACK1 shall contain duration information to update the NAV to indicate busy until the end of ACK2. This shall continue until the last fragment, which shall have duration of one ACK time plus one SIFS time. The corresponding ACK of the last fragment shall have its duration/ID field set to zero. In this fragmentation scenario each fragment and ACK frame acts as a virtual RTS and CTS; therefore the RTS/CTS frames are generated only at the beginning of the MAC frame transmission.

3.4.2 Point Coordination Function

In order to provide time-bounded services to real-time applications such as voice and video, the IEEE 802.11 standard defined an optional Point Coordination Function (PCF) medium access mechanism. As its name implies, the PCF uses a central-controlled polling method, which requires a Point Coordinator (PC) to determine which STA currently has the right to transmit. The Point Coordinator operates at the Access Point (AP), restricting the implementation of the PCF mechanism only to infrastructure network configurations. Actually, the PCF is built on top of the DCF and they coexist. Thus, the PCF and the DCF can operate within the same BSS concurrently in a coordinated way. All STAs inherently obey the medium access rules of the PCF, because these rules are based on the DCF.

3.4.2.1 PCF Access Procedure

If PCF is supported within a BSS, the access time is organized into repeated periods, called superframes. Each superframe consists of a Contention Free Period (CFP) where PCF is used and a Contention Period (CP) where DCF is used. A typical sequence of alternating CFP and CP during a superframe is shown in Figure 3-13. Each CFP or superframe begins with a beacon frame, which is a management frame that maintains the synchronization of the local timers in the stations and delivers protocol related parameters. The PC generates beacon frames at regular beacon frame intervals, thus every station knows when the next beacon frame will arrive. This time is called Target Beacon Transition Time (TBTT) and is announced in every beacon frame. At TBTT, a PC schedules the beacon frame as the next frame to be transmitted.

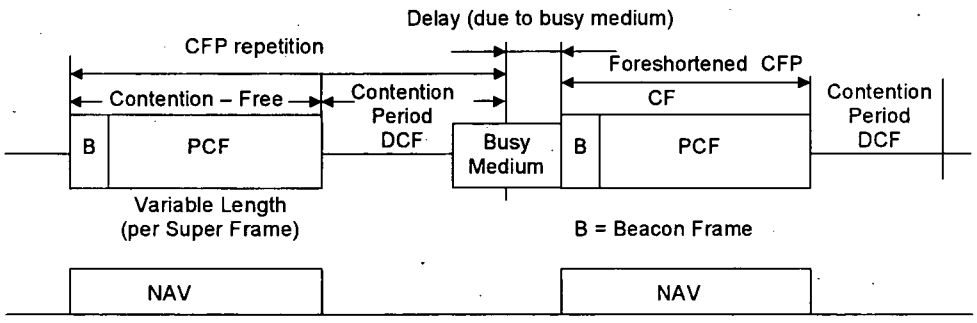


Figure 3-13: CFP/CP Alternation

The beacon frame can be transmitted when the medium has been determined to be idle for at least the PIFS (PCF Interframe Space) interval, which is shorter than the DIFS interval and longer than the SIFS interval. Depending on whether the wireless medium is idle or busy at TBTT, a delay of the beacon frame may occur. This delay may cause serious problems in transmission of time-bounded MSDUs that have to be delivered in CFP, because CFP is also generated at a defined repetition rate called the Contention-Free Repetition Rate (CFPRate), which has to be synchronized with the beacon interval. The PC controls the length of the CFP, with maximum possible duration specified by the value of the CFPMaxDuration parameter.

However, the PC may terminate any CFP at or before the CFPMaxDuration, based on the available traffic and size of the polling list. Since the transmission of any beacon frame may be delayed due to a medium busy condition at the nominal beacon frame transmission time (TBTT), a CFP may be foreshortened by the amount of the delay. In the case of a busy medium due to DCF traffic, the beacon frame shall be delayed for the time required to complete the current DCF frame exchange. It is mandatory that a superframe include a CP of a minimum length that allows at least the transmission of one MSDU under the DCF access method.

3.4.2.2 Frame Transmission

Frame transmissions under the PCF typically consist of frames alternately sent from the AP to stations and from stations to the AP within a BSS. During the CFP, the ordering of these transmissions and the STA allowed to transmit frames to the PC are controlled by the PC. Figure 3-14 depicts a frame transmission during a typical CFP, where a PC and several STAs are shown on the same line. At the nominal beginning of each CFP, the PC first senses the medium. When the medium is determined to be idle for one PIFS interval, the PC starts a CFP by broadcasting a beacon frame. Since the PIFS is smaller than DIFS, the STAs using the DCF access method will not be able to interrupt the transmission of the stations using the PCF access method. For the 802.11a, PIFS is 25 μs, whereas for 802.11b it is 30 μs. All STAs in the BSS, except the STA with the PC, set their NAVs to the CFPMaxDuration value at each TBTT at which a CFP is scheduled to start. This avoids most contention by preventing STAs from taking control of the medium during the CFP. After the beacon frame, the PC shall wait for at least one SIFS interval, which is shorter than PIFS, and then poll stations by sending one of the following frames: a CF-Poll frame, a Data+CF-Poll frame (data frame piggybacked with a CF-Poll), a Data+ACK frame (data frame piggybacked with an ACK for the previous transmission), or Data+ACK+Poll (data frame piggybacked with an ACK and CF-Poll). Piggybacking improves the channel utilization significantly in the PCF. The PC polls stations cyclically in the order in which they are placed in the polling list. Priority-based polling mechanisms can also be used if different QoS levels are requested by different polled stations.

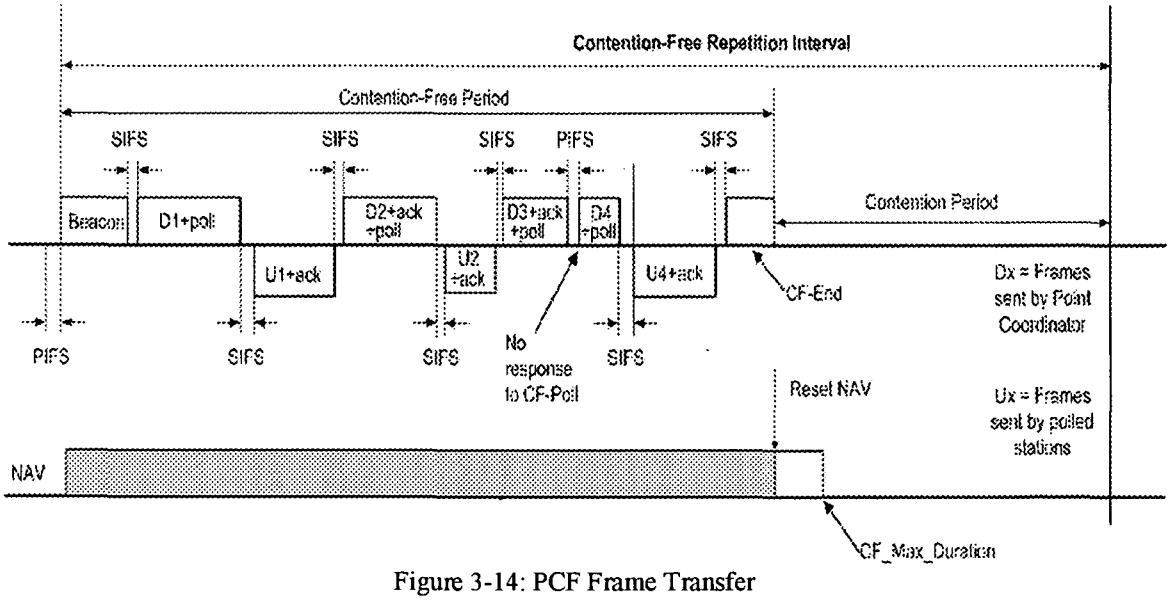


Figure 3-14: PCF Frame Transfer

The receiving PCF station, after waiting for one SIFS interval, may transmit only one data frame and may "piggyback" the acknowledgment of a frame received from the PC. If the data frame is not in turn acknowledged, the PCF STA shall not retransmit the frame unless the PC polls it again or decides to retransmit during the CP period. However, a PC may retransmit an unacknowledged frame during the CFP period after a PIFS time. PCF STAs and the PC do not use RTS/CTS in the CFP. If the polled station does not respond to the PC's poll within the SIFS

period, the PC waits until PIFS and polls the next station. This is the only case when packet transmissions are not separated by SIFS during the CFP. The PC continues to poll other stations until the CFP expires. The PC shall send a CF-Poll message to at least one STA during each CFP when there are entries in the polling list. When time remains in the CFP, all CF frames have been delivered, and all STAs on the polling list have been polled, the PC may generate one or more CF-Polls to any STAs on the polling list or send data/management frames to any STAs. A specific control frame CF-End or CF-End+ACK is transmitted by the PC as the last frame within the CFP to indicate the end of the CFP. A STA that receives either of these frames shall reset its NAV. Note that if there is no traffic buffered and no polls sent at the PC, a CF-End frame shall be transmitted immediately after the initial beacon. This means that the PC can terminate the CFP at any time by transmitting a CF-End frame. The operating characteristics of the PCF are such that all STAs are able to operate properly in overlapping BSS in which a PC is operating, and, if associated with a point-coordinated BSS, are able to receive all frames sent under PCF control. In general, a STA may transmit a pending frame when it is operating under the DCF access method, either in the absence of a PC, or, in the CP of the PCF access method, when the STA determines that the medium is idle for greater than or equal to the DIFS period.

3.4.2.3 QoS Limitations with PCF

PCF aims at supporting real-time applications such as voice and video. However, there are several problems with the PCF that impose serious limitations to support targeted and new real-time applications. The unpredictable beacon delay and unknown transmission durations of the polled stations are the most common problems. First, the time the beacon frame is sent after the announced TBTT, delays the transmission of time-bounded MSDUs that have to be delivered in CFP. From the legacy 802.11 standard, stations can start their transmissions even if the MSDU delivery cannot finish before the upcoming TBTT. This may severely affect the QoS as this causes unpredictable time delays in each CFP. In 802.11a, beacon frame delays of around 4.9 ms are possible in the worst case. Further on, a hidden station that misses a couple of the previous beacon frames or receives non at all has no knowledge about the TBTT and obviously does not stop its operation based on DCF. It is likely that it transmits interfering frames during CFP. Secondly, a station that has been polled is allowed to send a single frame (possibly fragmented) of arbitrary length, up to the maximum of 2304 bytes. Thus the unknown transmission time of polled stations may also introduce delays in CFP since the duration of the MSDU delivery that happens after polling can change and is not under the control of the PC. This destroys any attempt to provide QoS to other stations that are polled during the rest of the CFP. These problems with the PCF have led to the design of the new 802.11e standard supplement to support QoS. The mechanisms defined in 802.11e for QoS provisioning in a WLAN environment will be described in the Chapter 5.

3.5 Review

This chapter has described the MAC protocols for Wireless Communication Networks. First, the most common classification of TDMA based MAC protocols for wireless networks was presented. Then the discussion moved to the most representative protocols for wireless terrestrial and satellite networks. Next, a new TDMA based Random-Reservation MAC protocol to support QoS in LEO and GEO satellite communication networks was proposed and its performance was evaluated. The chapter concluded with a discussion of the two basic medium access mechanisms for IEEE 802.11 WLAN networks: the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF).

4 Mobility Management

Mobility management enables telecommunication networks to deliver telecommunication services to mobile users and to maintain connections as the user is moving to a new service area. Hence, mobility management is considered as one of the most important issues for wireless mobile communications. In this chapter first the concept of the mobility management and its components will be given. Then the most important mobility management issues in the second-generation GSM networks and the third-generation UMTS networks will be presented. Particular attention is given to Mobile IPv4 and Mobile IPv6, to mobile IPv6 extension protocols, and to mobility management issues in the IP based satellite networks. In addition, we introduce and evaluate two innovative handover protocols: inter terrestrial-satellite network and intra-satellite network handover management protocols.

4.1 Mobility Management Components

Mobility management contains two distinct but related components: location management and handover management [Aky99]. Location management is concerned with how to locate a mobile node, track its movement, and update the location information, whereas handover management is concerned with how to keep an active connection alive while the mobile station moves within the same mobile network or between networks operated by different operators. Roaming is the capability that makes it possible for the user to access the network at different points of the network of the same or of a different network operator, which might even be in a different country. Thus roaming presents another key service provided by mobility management.

4.1.1 Location Management

The location management process enables the network to track and locate the mobile user for delivering incoming calls. It handles information concerning the original cell of the mobile user, the cell where he/she is currently located, and the routes towards the current location. Location management encounters two phases: location update and call delivery, as shown in Figure 4-1.

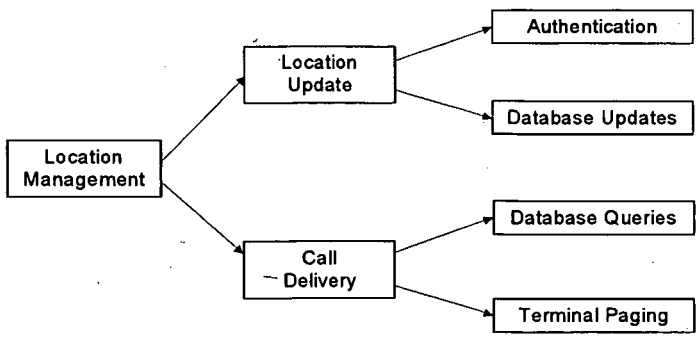


Figure 4-1: Location Management Functions

During the location updates, the mobile user notifies the network of its new access point, allowing the network to authenticate the user and revise the user's location profile. For call delivery, the network is queried for the user location and the user profile. Finally, paging is used to determine the location of the destined mobile user and to alert him of an incoming call. Since location management deals with database and signalling issues, many of the issues are not protocol dependent and can be applied to various mobile and fixed networks, depending on the requirements.

4.1.2 Handover Management

The process of changing the attachment point to the network while the mobile user is moving is known as handover. The task of handover management is to maintain a user's connection and communication during the handover process. The basic concept of handover is simple: when the mobile user moves from the coverage area of one cell to another, a new connection with the target cell has to be set up and the connection with the old cell is released. However, the handover management process is quite complicated task. Unlike the location management protocols, handover protocols relay on routing and resource management protocols. The handover procedure involves three phases: initiation, decision, and execution (Figure 4-2).

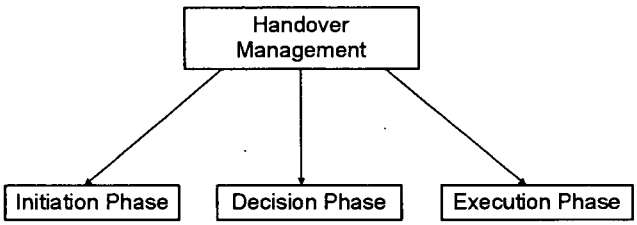


Figure 4-2: Handover Management Functions

Initiation phase: The objective of this phase is to identify the need for a handover and subsequently initiate it. Either the mobile station or the mobile network may initiate handover. There are many reasons why a handover procedure may be initiated. The basic reason is the degradation of the radio link quality between a mobile station and its attachment point to the network. The radio link quality may vary drastically due to the fading and signal path loss, resulting from the cell environment and user mobility. However, a handover can also be initiated for network management and maintenance reasons, for example due to traffic load.

Decision phase: In this phase, measurements on neighbouring radio transmitters and eventual network policy information are first analysed. Then the best target cell (access router) that the mobile station should be associated with is identified, taken into account the aforementioned measurements and available resources. The execution phase is finally triggered to perform the corresponding handover.

Execution phase: This phase includes the establishment of a new connection and the release of the old connection. The order of connection establishment and release procedure depends on the type of the handover.

4.1.2.1 Handover Types

There are several handover types and strategies available, summarized as follows:

- **Backward handover**: Is referred to as the case when the MS initializes the handover to a new access point. Handover signalling is exchanged through the old connection. The MS continues to maintain the current radio connection while the handover is in process and switches over to a new access point after radio resources have been reserved and all entities

involved are prepared for the handover. Backward handover is considered as the standard type of handover.

- **Forward handover**: Is referred to as the case when a MS suddenly loses its current connection and arrives at a new access point, which has to initiate and control the handover from then on. Loss of the connection could be due to interference or a fast moving station.
- **Network Controlled Handover (NCHO):** The surrounding BSs measure the quality of the radio links from MS, and the network initiates the handover process when handover criteria are met. Link quality comprises signal level and bit error rate.
- **Mobile Controlled Handover (MCHO)**: The MS continuously monitors the quality of the links of the surrounding BSs and initiates the handover if handover criteria are met.
- **Network Controlled Mobile Assisted Handover (MAHO)**: The MS measures the quality of the links from the surrounding BSs and sends this information to the network. Based on this information the network makes the decision to initiate handover.
- **Mobile Controlled Network Assisted Handover (NAHO)**: The network measures the quality of the current link and sends it to MS. Based on this report and on own measurements the MS desides whether to initiate a handover process or not.
- **Soft handover**: A new target radio link is established while the current link is maintained. Hence, a MS has connection to the old and to the new access point at the same time. This means, during a soft handover the MS communicates simultaneously with the old and the new access point.
- **Hard handover:** The current radio link is released before the new link is established between the MS and the access point
- **Signal diversity**: Combination of the hard and the soft handover. A signal link to the new access point is established, while old signal and traffic links are still in use.
- **Predictive handover:** In the mobile IP terminology the predictive handover refers to the case when handover is initiated via the current access router. The predictive handover procedure can set up the new access router for the handover before the handover actually occurs, thus the handover latency can be reduced.
- **Reactive handover**: Is initiated through the new access router.
- **Smooth handover**: A handover operation that minimizes packet loss during the time that the mobile host is establishing its link to the new access router.
- **Fast handover**: A handover procedure that minimizes packet delays during the time that the mobile host is establishing connection to the new access router.
- **Seamless handover**: A handover procedure that comprises a smooth and fast handover.
- **Bicasting or IP diversity** – Refers to the process of duplicating packets and sending them to the mobile host at both its previous and new access router.

4.1.2.2 Handover Scenarios

In wireless mobile networks different handover scenarios might occur. Some of them are summarized as follows:

- **Intra-cell handover**: Occurs when the user moves within the cell and experiences signal strength deterioration below a certain threshold. The user's connection is transferred to new radio channels of appropriate strength at the same base station.
- **Inter-cell handover**: Happens when the user moves into an adjacent cell and the station's connection must be transferred to a new base station.
- **Intra-access network handover**: Is the handover between two access points belonging to the same access network.
- **Inter-access network handover**: Is the handover to a new access point, which is in a different access network.
- **Intra-frequency handover**: If the new carrier, to which mobile terminal is accessed after the handover is the same as the original carrier then there is an intra-frequency handover.

- **Inter-frequency handover**: If the new carrier to which the mobile terminal is accessed to after the handover is different from the original carrier then there is an inter-frequency handover.
- **Horizontal and vertical handover**: Are said to happen if the old and the new access point use the same or different wireless technology, respectively. In horizontal handover coverage area and data rates remain the same, whereas in vertical handover bandwidth adaptation is also required. Horizontal handover is used in intra-system mobility, whereas vertical handover in inter-system mobility.

Some of the above mentioned handover types and strategies are applicable only to a certain wireless mobile network. However, the general principles of handover apply to all cellular systems.

4.1.3 Roaming

Roaming is usually identified with the possibility of the mobile user to access the mobile network of another operator when the user moves into the service area of that operator. This possibility depends on an agreement between the two network operators: the home network operator and the visiting network operator, provided that both networks are based on same technology. The goal of third and next generation networks is to provide service continuity while users move between different networks and systems, i.e., different network operators and different network technologies. We will name this kind of roaming continuous roaming, meaning that ongoing communication/service will not be interrupted when the user moves to the area covered by other network operator with the same or a different network technology. For continuous roaming, in addition to the needed agreement between network operators, handover plays a crucial role. If network operators use the same network technology than inter operator handover is needed. If network technologies are different than we talk about inter-system handover. The final goal is global roaming, which requires integration and interoperation of mobility management processes of each independent network. Mobile IP is the most widely accepted protocol to integrate mobility management functions of different access networks.

4.2 Mobility Management in 2G - GSM Networks

Mobility management in second-generation (2G) cellular networks is supported by two international standards: the Electronic/Telecommunications Industry Associations Interim Standard 41 (EIA/TIA IS-41) mostly used in the United States for the AMPS and IS-54/IS-136 networks, and the GSM Mobile Application Part (MAP) for GSM 900, DCS-1800, and PCS-1900. There are a lot of similarities between the two standards. In both cases the call processing and location management functions are based on Signal System 7 (SS7). In the following part of this section the general principles of the mobility management in 2G networks will be presented. As it is well known the 2G networks are organized in cells, shown in Figure 4-3 [Zah02], with the Mobile Switching Centre (MSC) responsible for a specific geographical area. Location management is based on location databases: the Home Location Register (HLR) and the Visitor Location Register (VLR). The two main components of the location management in 2G networks are location update and paging. Since mobile stations have a very limited power capacity, their batteries must be spared. An ideal solution would be that the MS transmits nothing except when actively connected to the network (active mode). However, to allow the network to efficiently forward the incoming packets, a MS must periodically transmit a beacon packet to inform the network of its current location in both active and standby mode, resulting in power consumption. It is well known that there is a trade-off between the costs of location update and paging. If the mobile station updates its location whenever it crosses a cell boundary, the network can maintain its precise location, thus obviating the need for paging. However, if the call arrival rate is low, the network wastes its resources by processing frequent update of information, and the

mobile station wastes its power transmitting the update signal. On the other hand, if the mobile station does not perform location update frequently, a large coverage area has to be paged when a call arrives, which wastes radio bandwidth. Thus, the central problem of location management is to devise algorithms that minimize the overall cost of location update and paging. There are different location update schemes the basic ones being time-based, movement-based and distance-based [Bar95]. In the time-based update scheme, an MS updates its location periodically at a constant time interval T (e.g., T = 1 hour). This scheme does not require the MS to record or process location information during the time between updates. For implementation, the timer threshold can be programmed into the MS by a hardware or software. In the movement-based update scheme, each MS counts the number of boundary crossings between cells during its movements. Location update is performed when this number exceeds a predefined number referred to as the movement threshold M (e.g., M = 3). This scheme allows the dynamic selection of movement threshold on a per-user basis. For implementation the MS only needs a counter to count the number of cell boundary crossings In the distance-based update scheme, each MS tracks the distance it has moved (in number of cells) since the last update and transmits an update signal whenever the distance exceeds a predefined value referred to as the distance threshold. For implementation, the MS requires some knowledge of cell topology.

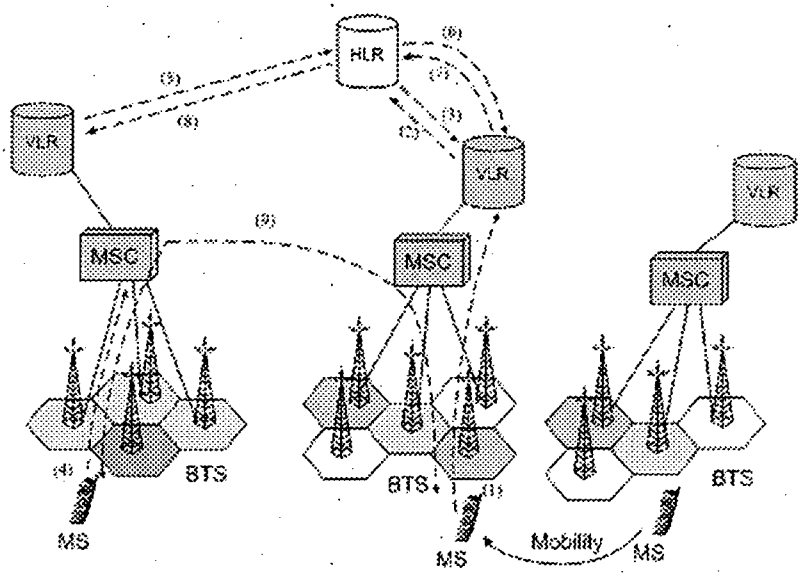


Figure 4-3: Mobility Management in a 2G Network

Considerin the handover management, when a mobile station changes base station, it may move to a cell that corresponds to a new serving VLR. In that case, it has to update the information stored in the HLR. Therefore, the station initiates an update message (1), which via the base station and MSC is forwarded to the current associated VLR. The VLR checks its local data. If the station's identification number is already stored there, no further action takes place, since the station has not changed location area. Otherwise, the station's identification number is stored locally and a new update message is forwarded to the HLR (2). The HLR in turn authenticates the station and replies with a positive registration acknowledgment to the new VLR (3). Additionally, the HLR may send a registration cancellation message to the old VLR, or a time-based mechanism may automatically update the VLR database and remove out-of-data entries. Whenever a new connection is initiated (4) the VLR will check its local data for the called numbers. If both calling and called parties are in the same servicing area, the call is directly routed to the station. Otherwise, the VLR of the calling station initiates a location request to the HLR (5). The HLR confirms that the station is located in this area and sends a route request message (6). This message is forwarded via the VLR to the serving MSC, which allocates a Temporary Local Directory Number (TLDN) for the specific station. The TLDN is returned to the HLR (7) and forwarded to the calling VLR (8). Using SS7, a path between the MSCs is established (9), and a

paging or alerting message is sent to the called mobile station. If the station changes VLR while connections are established, all the steps have to be repeated, increasing the signalling overhead, especially when the station is far away from the HLR. Second-generation systems, such as GSM, use the hard handover procedure, meaning that the mobile station keeps the connection to only one base station at a time, breaking the connection to the former base station immediately before making a new connection to the target base station. In GSM, always the network makes a handover decision and it is based on BSS criteria (received signal level, channel quality, distance between MS and BTS) and on network operation criteria (e.g. current traffic load of the cell).

4.3 Mobility Management in 3G - UMTS Networks

In this section, we will present Mobility Management (MM) issues in UMTS networks specified by 3GPP Release 1999. In general, the MM task in UMTS 3GPP 99 networks covers the management of UE locations and addressing issues of the mobile users and their terminals. In the specifications, the security aspects are also considered as part of mobility management. However, we will restrict our discussion only on the main functions of mobility management: location management and handover. The MM functions in UMTS separately cover the Circuit Switched (CS) and Packet Switched (PS) Core Network (CN) domains. In the CN CS domain, the serving MSC/VLR and the GMSC are responsible for circuit switched connection management activities, MM related issues like location update, paging and security activities. In the CN PS domain the SGSN is mainly responsible for MM related issues such as routing area update, location registration, packet paging and controlling the security mechanism related to the packet communication. Further on, the mobility management entity is divided between the RNC and the SGSN. This means that every cell change the subscriber does in UTRAN is not necessary visible to the CN domain, but the RNC handles these situation.

4.3.1 Location Management in UMTS Networks

In general, Location Management (LM) in 3G mobile networks needs a kind of logical hierarchy for its functioning [Hei01]. Hence, UMTS contains basically four-level logical definitions: Location Area (LA), Routing Area (RA), UTRAN Registration Area (URA), and Cell, as shown in Figure 4-4.

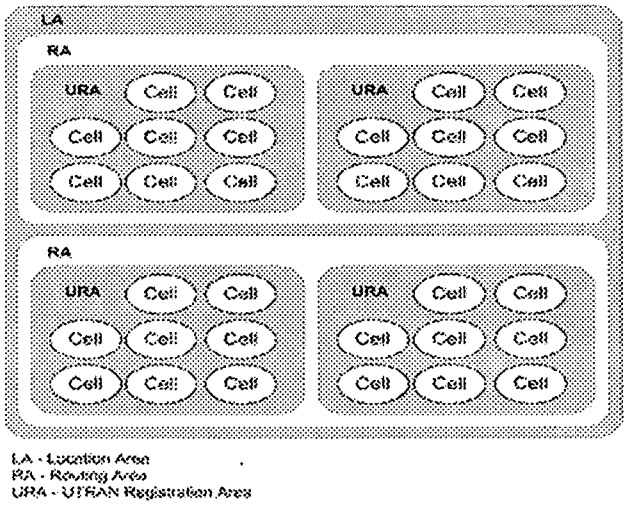


Figure 4-4: UMTS Location Management Coverage Area

In the CN CS domain the Location Area (LA) is the area where the UE may move without performing the location update procedure. The LA consists of cells; the minimum is one cell and

the maximum is all the cells under one VLR. In the location update procedure the location of the UE is updated in the VLR with LA accuracy. The VLR pages the desired UE from the location area in which it has performed the latest location update. It should be noted that one RNC may have several location areas or one location area may cover several RNCs. The PS CN domain, similar to the CN CS domain, has its own location registration based on Routing Area (RA). RA is like LA. This means, it is the area, where the UE may move without performing the RA update). The RA can be considered also as a subset of the location area LA: one LA may have several RAs within it but not vice versa. In addition one RA cannot belong to two location areas. Because the UTRAN is involved in MM, it contains local mobility registration, a UTRAN Registration Area (URA). Furthermore, mobility management in UMTS networks can be characterized with a state model, for both circuit and packet switched connections. In the following text, the abbreviation MM refers to the circuit switched mobility management, whereas PMM (Packet Mobility Management) refers to the packet switched mobility management.

For the circuit switched connections a UE, from the MM point of view, may have three states, MM-detached, MM-idle and MM-connected. These MM states indicate how accurate the terminal location is known compared to the logical structure presented in Figure 4-4. In the MM-detached state the network is not aware of the UE (mobile user) at all. This is the MM state when the terminal is switched off. In the MM-idle state the network knows the location of the UE with the accuracy of a LA. In the MM-connected state the network knows the location of the terminal with the accuracy of a cell. For the packet switched connections the PMM states are the same, but the situation is different in terms of PMM procedures and the triggers that allow moving from one state to another are different. In the PMM-detached state the network does not have any valid routing information available for the packet switched connection. When the PMM state is PMM-connected the data can be transferred between the terminal and the network: the SGSN knows the valid routing information for packet transfer with the accuracy of the routing address of the actual serving RNC. In the PMM-idle state the location is known with the accuracy of a routing area identity. In this state, the paging procedure is needed in order to reach the terminal.

4.3.2 Handover Management in UMTS Networks

In the UMTS network, there are two basic handover types: hard handover and soft handover.

Hard handover can be further divided into intra-frequency and inter-frequency handover, illustrated in Figure 4-4 and Figure 4-5, where the adjacent Node-Bs may transmit with the same frequencies or with the different frequency, respectively.

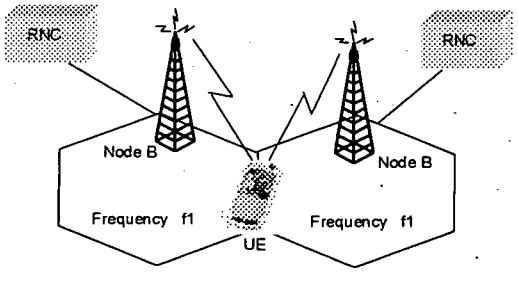


Figure 4-5: Intra-Frequency Hard Handover

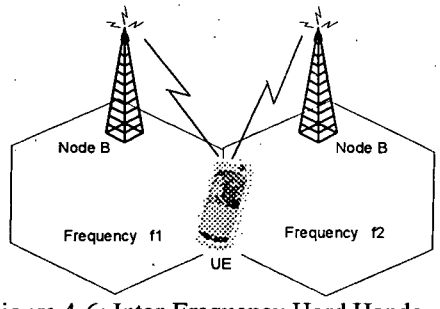


Figure 4-6: Inter-Frequency Hard Handover

Inter-frequency handover also may happen in hierarchical cell structure networks between separate cell layers, for instance, between macro cells and micro cells, which use different carrier frequencies within the same coverage area. Furthermore, inter-frequency handover may occur

between two different radio access networks, for instance, between GSM and UMTS, as shown in Figure 4-7. In this context, it can also be called inter-system handover.

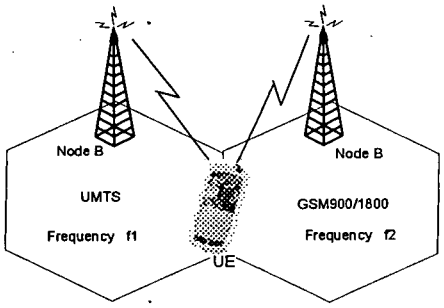


Figure 4-7: Inter-System Handover

Soft-handover is further divided into: soft and softer handover, illustrated in Figure 4-8 and Figure 4-9, respectively.

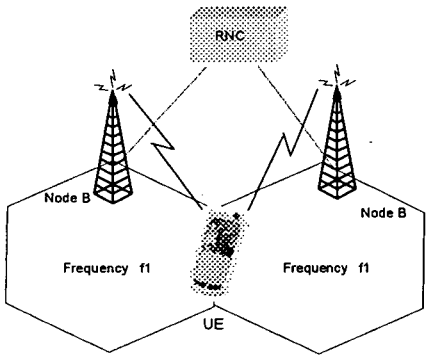


Figure 4-8: Soft Handover

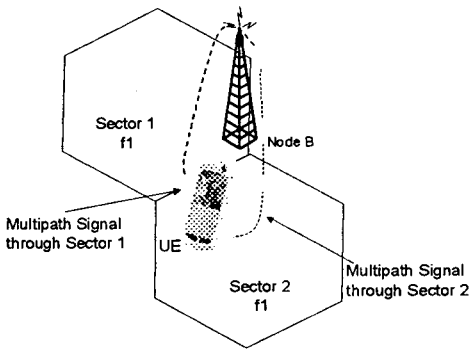


Figure 4-9: Softer Handover

Soft handover occurs when UE passes between two adjacent cells corresponding to different Node_Bs. Communications between UE and Node_B occurs simultaneously through two channels, one to each cell, as illustrated in Figure 4-8. In the Down Link (DL), the UE receives the same signals from both Node_Bs but with different codes. In the Up Link (UL), both Node_Bs receive the same signal from UE, and route it to the RNC for combining. Node_Bs involved in the handover may or may not belong to the same RNC. However, the RNC involved in the soft handover must coordinate the execution of the soft handover over the Iur interface. Soft handover is an intra-frequency handover, i.e., the source and target cells have the same frequency. In the UMTS system, the majority of handovers are intra-frequency soft handovers. Softer handover is actually a variation of soft handover. Softer handover happens when a UE passes between the overlapped coverage area of two adjacent sectors of a Node_B, as illustrate in the Figure 4-8. During softer handover, the UE communicates simultaneously with Node_B through two channels (using two different DL codes) corresponding one to each sector. Maximally three codes may be used, each corresponding to three different sectors. In the UL Node_B receives the UE's signal in each sector and routes them to the same receiver. Softer handovers occur more rarely than soft handovers. While softer handover may occur at maximum 16% of links, soft handover may occur at about 20- 40% of the links.

Concerning soft and softer handovers, the multipath signal propagation is utilized for better call quality. This means, the transmitted signal propagates in many different ways from the transmitter to the receiver. There are two terms describing the handling of the multipath components. These are microdiversity and macrodiversity. Microdiversity refers to the case where the propa-

gating multipath components of the same signal are received from one cell, and in the case of sectored Node_B, the outcome from different sectors, are combined in the Node_B by using the so-called RAKE receiver. In the case of the soft handover the UE may use cells belonging to different Node_Bs or even different RNCs. Macrodiversity functionality is used in the RNC to combine signals from different cells. However, the way of combining the signals is quite different from the microdiversity case at the Node_B because there is no RAKE receiver at the RNC. In addition to better call quality, multipath propagation contributes to better capacity preservation in the radio network by decreasing radio interference. Actually, in the UMTS system the transmit power of the UE and Node_Bs should be relatively small in order not to block the other users. This decreases the radio interference and gives more space to other transmissions. Despite the fact that soft and softer handovers consume radio access capacity (UE uses more than one radio link connection in the Uu interface), the added capacity gained from the interference reduction is bigger and the overall system capacity is actually increased.

In general, the following handover types, illustrated in Figure 4-10, are supported by UMTS.

- Intra-Node_B handover: Handover from one sector to other within a Node_B,
- Inter-Node_B, Intra-RNC handover: Handover between different Node_Bs of the same RNCs,
- Inter-RNC handover: Handover between RNCs within the same RANs,
- Inter-MSC handover: Handover between two MSC,
- Inter-system handover: Handover between GSM and UMTS networks.

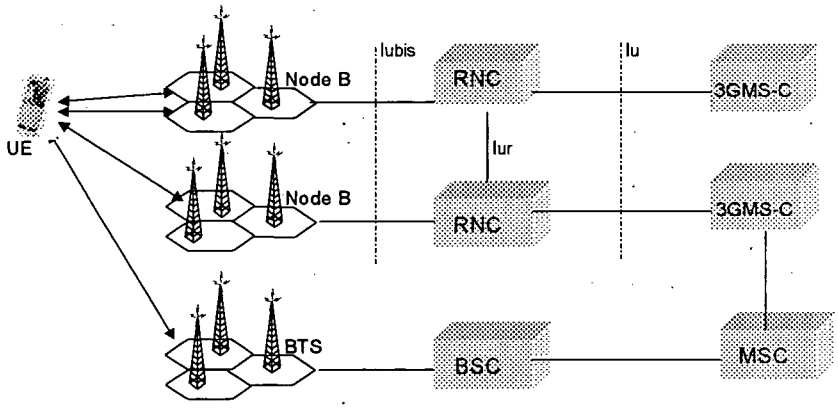


Figure 4-10: Types of Handovers in UMTS Networks

4.3.3 Handover Criteria and Measurements

Regardless of the type of handover, there are different reasons why the handover should be executed. The handover execution criteria depend mainly upon the handover strategy used in the system. However, most criteria behind the handover activating are based on: the signal quality, user mobility, traffic distribution, and bandwidth. For the handover purposes, during the connection the UE continuously measures the signal strength on the DL concerning the surrounding cells, and reports the results to the RNC. Node_B also carries out measurements on UL. According to the 3GPP, the UE measurements may be grouped into different categories depending on what the UE should measure. On the downlink, the following measurements are carried out: intra-frequency measurements, inter-frequency measurements, and inter-system measurements. On the uplink, the measurements of traffic volume are carried out. Measurements of QoS parameters are done both on uplink and downlink. However, the type of needed measurements depends on handover type, for instance, inter-frequency and inter-system measurements are made only when requested by RNC. Handover decision is based on the measurements reported by the UE and the Node-B as well as the criteria set by the handover algorithm. In UMTS networks, the final decision about the handover is always made by the RNC, because the RNC has

the information of the system overall load as well as other necessary information needed for handover execution. However, the decision is mobile assisted. The mobile measures radio resource quantities, informs the radio network controller about the availability of the radio access, and the controller decides about handovers.

4.3.4 Inter-System Handover

An inter-system handover is always a type of inter-frequency handover, since different frequencies are used in different systems. Intersystem handover for UMTS plays an essential role in the evolution process of 2G and 3G mobile systems. On one side, UMTS/UTRAN needs to interoperate seamlessly with the family of IMT 2000 networks and co-exist for some time with all types of deployment scenarios. However, complete interoperability will not necessarily occur at the introduction of UMTS, but will follow a gradual process. On the other side, it is likely that the patchy UMTS coverage will be supported by GSM/GPRS, both nationally and internationally, for many years. Hence, the inter-system UMTS and GSM handover will be very important to complement the coverage areas of each other in order to ensure continuity of services. For this reason, it will be particularly important that UMTS terminals are also capable of using the existing GSM networks. This will allow the UMTS users to roam to more ubiquitous GSM networks where there is no UMTS coverage. The inter-system handover will enable that a call or data session is continued on the new network without the users having to re-establish the session. Ideally, users should not notice this network changeover but in many cases handover from UMTS to GSM will cause a noticeable degradation. The inter-system handover can also be used to control the load between GSM and UMTS systems, when the coverage area of the two systems overlaps with each other. Other inter-system handover reasons might be the service requested by the UE and user's subscription profile. The main problem is that the 2G networks will not be capable of supporting the data rates required by the product or service in use. This should not be noticeable for voice but will be significant for large bandwidth services such as live video. For this reason, it is important to note that the handover process can degrade the product performance gracefully. An example is a videophone call. A 2G network will not be able to handle both the voice and the video components of the call because of the large data rates required. In this case, on handover from 3G to 2G, it would be desirable for the voice component to continue and the video component to be dropped. The video component would be re-instated when the call is handed back to the 3G networks. In practice, this may prove difficult in the early years of UMTS and some other means of managing the handover of this type of product will need to be determined.

4.4 Mobility Management in All-IP Networks

The increasing usage of portable devices, such as laptops and Personal Digital Assistants (PDAs), has recently led to a growing demand for access to the Internet and corporate intranets independent of technology and point of attachment. A further ongoing evolution is the provision to mobile user's wireless access to Internet so that they can maintain connectivity while moving. Hence, mobility management is one of the main issues of the next generation mobile networks, to support worldwide roaming and mobile Internet service provisioning. Currently the IP services for wireless mobile users are delivered over a variety of networks and technologies, including GSM, GPRS, satellite, and WLAN. However, none of these solutions can be considered really universal because each is targeted on a specific set of services and applications, and therefore has different characteristics in terms of geographical coverage and QoS parameters. Furthermore, it is expected that the same geographical region will be covered by several wireless overlay networks, so it will be up to the user to decide when to switch from one wireless access network to another based on availability or cost/performance considerations. For example, when in the office, the mobile user will access the Internet through the local 10 Mbit/s WLAN, even if satellite, or GSM coverage is available. In such a complex environment, the first step is to gain

connectivity at the physical layer, by using either multimode or adaptive terminals. For example, terminals equipped with commercial WLAN (e.g., IEEE 802.11b), cellular (e.g., GSM and GPRS), or satellite network interface cards may be introduced. However, the main drawback of the above solutions is that mobility management is handled almost completely by the underlying network. Therefore, seamless mobility among overlay networks cannot take place; any user roaming to a new wireless domain is typically assigned a new identity (i.e., a new IP address), and any previously active communication session is lost. To overcome this problem, innovative protocols, mobile IPv4 [Per02, Per96] and mobile IPv6 [Joh00], for handling inter-domain user mobility at the IP layer are developed by the Internet Engineering Task Force (IETF). In particular, it will be possible to deploy a common IP backbone to interconnect heterogeneous wireless IP networks, and to rely on mobile IP protocols to manage user mobility among them. This will allow any mobile user, equipped with a multimode handset or laptop PC, to transparently roam among wireless domains, being constantly reachable at the same address.

In the following sections, the basic principles of MIPv4, MIPv6, and some other protocols as extensions to MIPv6, such as HMIPv6, RegReg6, and Fast Handover will be presented.

4.4.1 Mobile IPv4

The Mobile IPv4 components include Mobile Node (MN), Correspondent Node (CN), Home Agent (HA), Foreign Agent (FA), and the Access Router (AR), as shown in Figure 4-11. A MN is a node that can change its point of attachment to the Internet, whereas a CN is a node communicating with the MN. A home agent is a router in the MN's home network, handling the mobility of the MN. A foreign agent is a router handling the mobility of the MN in the visited network. Access router is the MN's default router. In IP terminology the MN can be a user terminal or a router. As we will consider only the mobility of the user terminal, in this thesis we will refer to the MN as Mobile Host (MH). The mobile IPv4 protocol enables a MH to communicate with CH, after changing its point of attachment to the Internet from one IP subnet to another without changing its IP address. Without this feature, the MH would not be able to maintain transport and higher layer protocol sessions, which depend on a static IP address. This problem is solved by assigning two IP addresses to a MH: a permanent IP address, which is called IP home address, and a temporary IP address, named Care-of-Address (CoA), which is assigned each time the mobile host is visiting a new foreign subnet. The home address is used for transport and higher layer sessions whereas the CoA is needed to route packets correctly to the actual point of attachment. In this way, the impact of host mobility is reflected only in the internet layer and is kept transparent to transport and higher layer protocols.

Protocol Description

A mobile host attached to its home network operates like any fixed host, using a home address. When MH enters a new subnet and acquires a new CoA, it has to register it to the home agent, by sending registration request known as Binding Update (BU) messages. A BU message contains the association made between the home address and the current CoA of an MH and an association lifetime. Note that the CoA may be assigned to an interface of a mobile host itself, and this is called the Collocated CoA (CCoA), or is the address of the FA. Once the HA receives the BU, either from the MH (when CCoA is used) or from the FA, it updates the corresponding entries in its routing table and approves the request by sending a registration reply back to the MH. From now on the HA intercepts all packets addressed to the MH, encapsulate them using an outer IP header with the destination address set to the registered CoA, and tunnels them using regular IP forwarding to the mobile node's current location. Packets from the MH are sent to the CH through the Internet as usual. The IPv4 suffers from several drawbacks. First of all, the path a packet takes on its route to a MH is obviously not optimal. The packet needs to first reach the HA, and only then is it tunnelled to the final destination a phenomenon known as triangular routing. A set of routing optimization extensions has been proposed to alleviate triangular routing. This is achieved by providing a means for the corresponding hosts to cache

gular routing. This is achieved by providing a means for the corresponding hosts to cache the binding information of the mobile host and tunnel the packets directly to their CoAs. Another important issue is associated with the requirement that a MH has to use its home address as the source address in the packet header. When MH is in a visiting network, this address is topologically incorrect, which may cause the packet to be dropped at any point in a network that implements ingress filtering or firewalls. In solving this problem, a reverse tunnelling option has to be used, at the expense of yet another overhead routing path: an outgoing packet is encapsulated and tunnelled by the FA or mobile host to the HA.

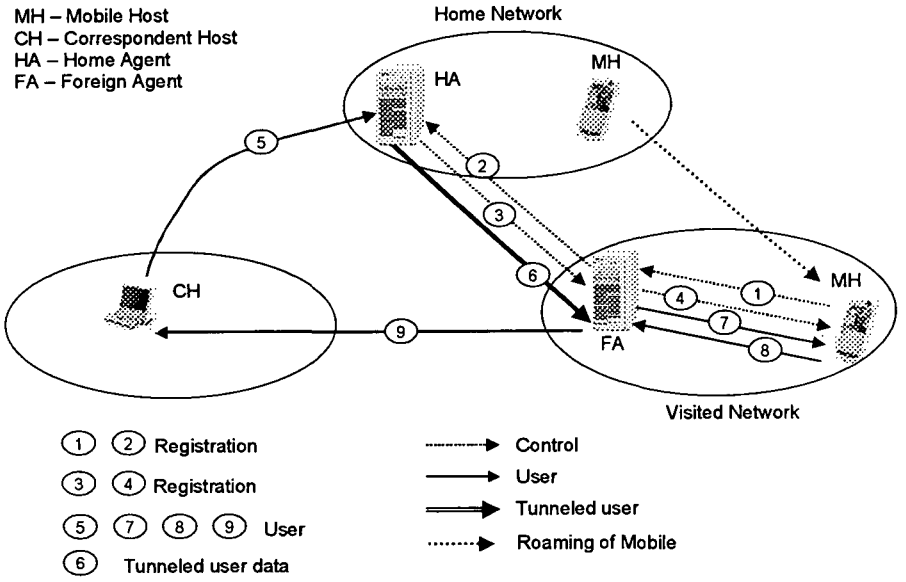


Figure 4-11: Mobile IPv4

4.4.2 Mobile IPv6

MIPv6 is considered as a basic protocol for handling mobility management in the future mobile Internet. It provides an efficient approach for handling mobility based on inherited features from IPv6 such as autoconfiguration, neighbour discovery, and destination option. Mobility support in IPv6 is a built-in feature, as a fundamental difference to IPv4, implemented as an integral part of the underlying IP layer by using destination options: binding update, binding acknowledgment, binding request, and home address. While the basic principles and concepts of HA, home address, and CoA are retained from IPv4, the neighbor discovery feature of IPv6 allows a mobile host to operate without explicit support of an FA. The basic structure of MIPv6 is illustrated in Figure 4-12.

Protocol Description

A mobile host detects that it has moved to a new subnet by analyzing the *router advertisement* periodically sent by the Local Access Router (LAR). Having entered a new subnet, the MH uses neighbour discovery and autoconfiguration to form a new care-of address. In the next step the MH has to register its new CoA with the HA and the CH, by sending Binding Update (BU) messages. The HA and the CH update the corresponding entries and confirm the receipt of the BUs by sending a Binding Acknowledgment (BA) messages to the MH. Thereafter, packets of new calls are intercepted by the HA and then tunnelled to the MH's registered CoA by using IPv6 encapsulation (IPv6 within IPv6 tunnelling), whereas packets belonging to active sessions are sent directly to CoA. It is also worth to mention that the HA may also send a binding request to the MH to get the MH's current binding information if the latest BU expires. The MH then

responds to the binding request with its new BU and waits for a BA from the HA. Packets from the MH are sent to the CH through the Internet as usual.

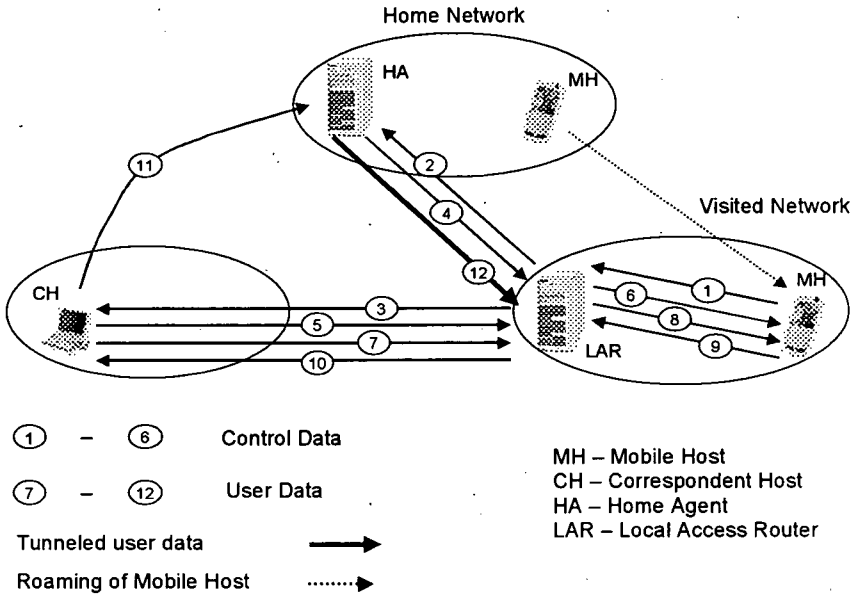


Figure 4-12: Mobile IPv6

When a CH wants to communicate with a MH, it first looks for an entry with the MH's home address in its binding cache. If such an entry is found, the packets can be sent directly to the care-of address. Otherwise, packets will be sent to the home address and then be encapsulated by the HA and tunnelled to the CoA of the MH. The MH can easily determine whether packets from a CH reach it via the HA by triangle routing, since such packets are encapsulated and tunnelled from the HA's address. If packets are received via the HA, the MH understands that the CH has no binding update information and sends a BU to its CH. Having received and processed the BU, the CH will send all subsequent packets directly to the MH's CoA. When MH is a sender, in order to operate in a network environment with ingress filtering, the MH will set the source address of its packets to its CoA, whereas the home address is carried in the destination option. The network layer in the CH receiving these packets will replace the source address with the address found in the home address destination option. Hence, the TCP sessions and upper layers will not be affected by the fact that the MH is using a temporary address and there is no need for reverse tunnelling. Another issue related to mobile IP is smooth handover. When the MH changes its point of attachment and forms a new care-of address, some packets are still likely to arrive to its previous care-of address before the new binding is processed by its HA and CHs. These packets are potentially lost. To prevent this, the MH can send a BU to its previous Access Router (AR) and ask for packet forwarding to the new CoA. In this case, the previous AR would function as a temporary home agent for the MH. While MIPv6 effectively eliminates many of the shortcomings of MIPv4, both these protocols are oriented toward wide-area network mobility management, or macromobility. Every time a host moves beyond the limits of link layer connectivity, a binding update message needs to propagate all the way to the host's HA and CHs. When the host moves within a relatively small geographic area, or performs micromobility, remotely located with respect to its home network, this may lead to large handover signalling latency and overhead. Enhancing the IPv4 and particularly IPv6 mobility management protocols with scalable capabilities that reduce latency, packet loss, and signalling overhead due to micromobility handovers has resulted in several protocol designs, such as hierarchical mobile IPv6 [Cas01], mobile IPv6 regional registration [Mal01], fast handover [Koo03], cellular IP [Cam99], and HAWAII [Ram99]. The relevant protocols for this thesis will be explained in the following sections.

4.4.3 Hierarchical Mobile IPv6

Hierarchical Mobile IPv6 (HMIPv6) [Cas01] is an extension to Mobile IPv6 with the task to reduce handover latency and the amount of signalling due to intra-domain handovers, especially in the cases when the Mobile Host (MH) is located far away from its Home Agent (HA) and Correspondent Hosts (CH).

Protocol Description

In HMIPv6, a network operator's domain is organized in a hierarchical structure consisting of Access Routers (AR) at the lowest level, HMIPv6-aware routers above them and one or more Mobility Anchor Points (MAPs). The basic HMIPv6 network architecture is illustrated in Figure 4-13.

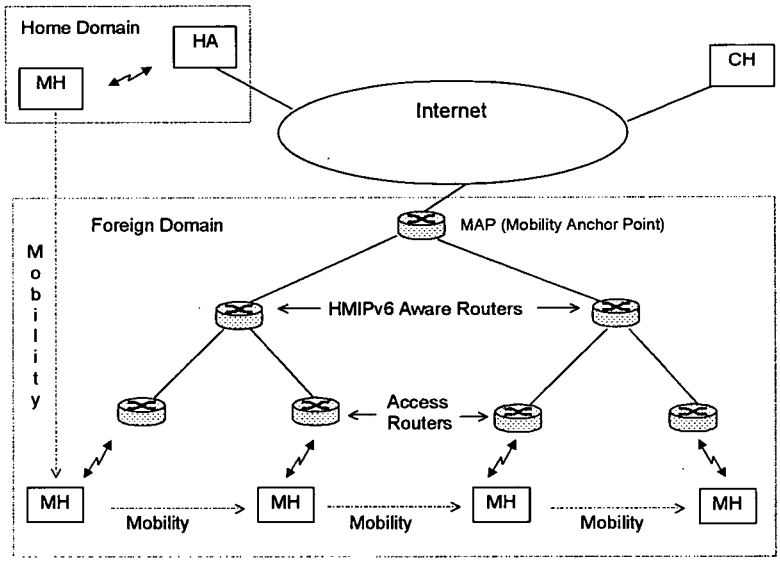


Figure 4-13: Hierarchical Mobile IPv6

MAP is a router located in the visited domain at any level in the hierarchy, which serves as a local home agent for MHs registered with it. By serving as a local home agent, the MAP allows localization of the mobility signaling to the visited domain. This results in faster handovers and consequently, in reduced packet loss. Upon entering a new HMIPv6 domain, the MH forms two new care-of addresses: a Regional Care-of Address (RCoA) and an On-link Care-of Address (LCoA). The LCoA is formed using stateless autoconfiguration based on the network prefix advertised by its new AR and its own network interface identifier, as defined in IPv6. The way of forming an RCoA is determined by the MAP's mode of operation, Basic or Extended.

Basic mode

In this mode of operation the RCoA is auto-configured from the MAP's prefix in the router advertisement MAP option. After forming the RCoA, a Binding Update (BU) is sent to the MAP with the LCoA as the source address, and the RCoA as a home address destination option. Upon reception of a BU, a MAP performs Duplicate Address Detection (DAD) on its subnet. If the RCoA formed by the MH is found to be unique, the MAP stores the RCoA–LCoA binding in its binding cache, and replies with a Binding Acknowledgment (BA) indicating a successful operation. Thereafter, the MAP intercepts all packets addressed to the RCoA of the registered MH and tunnels them to the corresponding LCoA. The MH updates the HA and the CHs with the RCoA as soon as the binding acknowledge is received from the MAP. These BUs contain the MH's home address in the home address destination option, and the RCoA as the source address. If ingress filtering is applied in the visited network, the MH may not use its RCoA as the source address. In this case, the LCoA is used as a source address and the RCoA is specified in

an Alternate Care-of Address sub-option. It is required that the lifetime for Binding Updates sent to the HA/CHs must be shorter than the lifetime of the registration with the MAP. After this initial update process has been performed, when the MH changes its point of attachment inside the visited domain and forms a new LCoA, it only needs to register this new address with its MAP. The Basic mode is completely transparent to all other entities like HA or CH.

Extended mode

In the extended mode the RCoA will be the IP address advertised in the MAP option, which is assigned to one of the MAP's interfaces. Having obtained both LCoA and RCoA addresses, the MH performs local registration by sending a BU to its MAP. This BU contains the LCoA as the source address and the MH's home address in the home address destination option. Because the MH uses the MAP's address as an RCoA, there is no need to perform DAD for the RCoA. The MAP stores the LCoA – home address bindings for the MHs, and sends a BA to the MH. After receiving the BA from the MAP, the MH updates its HA/CHs. Since the MH uses one of the MAP's addresses as RCoA, it must not set the RCoA as the source address of its packets. Instead, the LCoA will be the source address; the home address will be in the home address destination option and the RCoA in an alternate Care-of Address suboption. Packets encapsulated and tunneled by the HA will be de-capsulated by the MAP and then encapsulated again and send to the LCoA.

4.4.4 Mobile IPv6 Regional Registration

Mobile IPv6 Regional Registration (RegReg6) [Mal01], just like HMIPv6, is an extension to Mobile IPv6 with the goal to reduce the binding update signalling latency and signalling load outside the visited domain due to intra-domain handovers of the mobile host.

Protocol Description

Similar to HMIPv6, a RegReg6 network domain is organized in a hierarchy of regional-aware routers, as illustrated in Figure 4-14. On the top router of the hierarchy is a Gateway Mobility Agent (GMA). Besides the topmost GMA, other GMAs may also exist in the domain on lower levels. Upon entering a foreign domain, the Mobile Host (MH) attaches to an Access Router (AR) and forms a new care-of address, which is referred to as a Local Care-of Address (LCoA). In addition to this address, GMAs advertise their IP addresses, which the MHs can use as a Regional Care-of Address (RCoA). The MH chooses one of these addresses and sends a regional binding update to register itself for regional services in the domain. The regional-aware access router is the first router that receives the regional binding update. This AR updates its regional binding cache with an entry that binds the home address and LCoA of the MH. Then it encapsulates the binding update message and forwards it to the next Regional Router (RR) upwards in the hierarchy. This router also creates an entry in its regional binding cache binding the home address of the MH with the source address found in the encapsulating header, which is the address of the previous router below. Then it encapsulates the binding update again and sends it further upwards in the hierarchy. In this way, the binding update propagates hop-by-hop upwards in the hierarchy, and each router creates an entry for the MH in its binding cache. Non-regional-aware routers may also be located in the hierarchy between regional-aware ones and can interoperate with regional-aware routers without any restriction. The binding update finally arrives at the router containing the GMA, which controls the address that was selected as an RCoA by the MH. When this last router is also updated successfully, an ordinary binding acknowledgement message is sent to the MH back through the hierarchy. As soon as the BA is received, the MH can update its HA and CHs with its RCoA. Packets tunnelled to the RCoA by these nodes will be received by the GMA. The GMA de-capsulates the packets and determines the destination address of the original header, which is the home address of the registered MH. Then it looks for a corresponding entry in its Regional Binding Cache, which reveals the care-of

address belonging to the home address. This CoA is the address of a router located one level below the GMA in the hierarchy. Finally, the GMA encapsulates the packet to this CoA. The next router and all the routers below follow exactly the same procedure: de-capsulate the packet, find the next CoA for the home address, encapsulate the packet again to that CoA. Thus, the packets propagate hop-by-hop downwards the hierarchy, until they reach the MH at its current location.

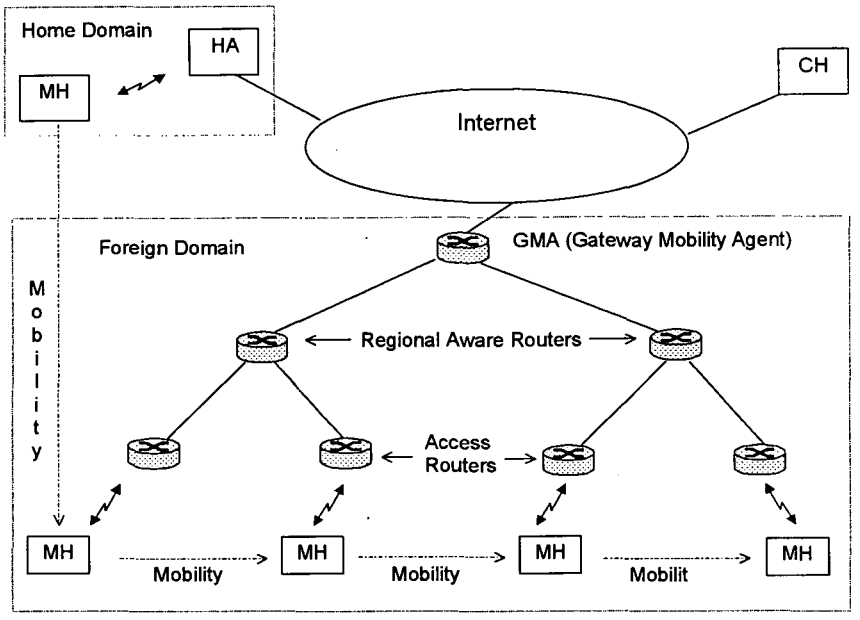


Figure 4-14: Mobile IPv6 Regional Registration

When the MH changes its point of attachment in the visited domain and attaches to a new access router, it forms its new LCoA and it sends a regional binding update to the visited domain routers. It appends a "Previous Access Router" sub-option in its BU, which is an option defined by RegReg6 to identify the MH's previous access router with its IP address. All regional routers in the domain maintain a list of their descendant routers. Therefore, when the regional BU is propagating upwards in the hierarchy, each RR can decide whether the previous AR is among its descendants. The router, which is the ancestor of the previous AR, is the crossover router. The domain hierarchy above the crossover router will not be involved in updates due to the handover. In the case when the MH enters a new domain the regional binding update propagates up to the GMA, which will play the crossover router's role. The RegReg6 is an optional extension to Mobile IPv6, i.e., the visitor MHs are not mandated to use its features, which gives the protocol great flexibility. There is also a Regional Registration version for MIPv4 described in [Gus02].

4.4.5 Fast Handover

Handover latency resulting from standard Mobile IPv6 handover procedures could be greater than what is acceptable for real-time traffic. Hence, several protocols have been proposed, as extension to Mobile IP that seeks to reduce the handover latency at Layer 3 (L3). Low latency handover protocol or Fast Handover [Koo03] designed for Mobile IPv6 relies on the existence of certain Layer 2 (L2) triggers. An L2-trigger is information based on the link layer protocol, in order to begin the L3-handover before the L2-handover ends. Either the MH (for mobile controlled handovers) or the AR (for network controlled handover) needs to receive an indication (this trigger) that the handover is imminent for the fast handover protocol to work. The main L2 triggers used for fast handover are the following:

- **Link Up**: Indicates that a MH has established a new link with the new AR.
- **Link Down**: Indicates that the MH has terminated connection with the current AR.

- **Source trigger:** Sufficiently before L2-handover starts, indicates that the MH starts an L2-handover.
- **Target trigger:** Sufficiently before L2-handover finishes, indicates that the MH finished an L2-handover.

Each L2-trigger is sent to a certain entity (e.g., the MH, the AR), and it contains information relevant to handover. A L2-trigger, for instance, contains information on the MH L2-connection and on the link layer identification (e.g., the link layer address) of the different entities. When an AR receives an L2-trigger, it must be capable of matching the entity identification to an IP address. For example, when it receives access point identification, it must know to which subnet this access point belongs. For this, the neighbouring ARs have to exchange information to discover each other. The information exchanged can be a network prefix or a list of the access points operating in an AR subnet. There are three phases in the Fast Handover protocol operation: handover initiation, tunnel establishment, and packet forwarding.

Handover Initiation

The MH or the current AR (when the L3-handover is controlled by the network) receives a L2-trigger indicating that the MH is about to perform a L2-handover. If the MH receives the L2-trigger, it must initiate the handover by requesting its AR (i.e., current AR) to assist in handover by sending a message (Router Solicitation for a Proxy-RtSolPr). The RtSolPr message allows a MH to request the IP address, link-layer address as well as network-prefix of the new AR's interface to which the MH may attach. In respond to this message the current AR sends a message (Proxy Router Advertisement-PrRtAdv), which provides the link-layer address, and network prefix information about the new AR. In the network-initiated handover, the current AR sends a message without receiving a message from MH, and provides the parameters (i.e., link-layer address and IP address of the new AR) necessary for the MH to send packets as well as the network prefix for the MH to formulate a prospective new care-of-address. The current AR sends a valid IPv6 address for the new subnet also to the new AR for validation. Having received this, the new AR controls if the address is unique in its subnet and sends the validation result to the current AR. If the address is valid, the current AR forwards the authorization (to use this address in the new subnet) to the MH. Then when the MH establishes the connection with the new AR, it can immediately use the new care-of address as the source address and send a binding update to the home agent and the correspondent nodes.

Tunnel Establishment and Packet Forwarding

A bi-directional tunnel is established from the L2-triggers between the two access routers for the following purpose. Since the MH cannot use the new CoA until it completes the binding update with its HA and the CH, it is allowed to use the previous CoA until it establishes itself as a Mobile IPv6 end-point. For this purpose, the new AR tunnels packets sent with the previous CoA as source IP address to the previous AR. Until the CH establishes a binding cache entry for new CoA, the CHs continue to send packets to the previous CoA, which need to be forwarded to the MH. The previous AR tunnels these packets to the new AR, which then forwards them to the MH. Since it is desirable to deliver these packets independent of the new CoA configuration, the previous AR tunnels the packets to the new AR instead of to the new CoA. However, the tunnel establishment and packet forwarding on the tunnel to the MH begins when previous AR receives a Fast Binding Update (FBU) message from the MH. The MH sends a FBU to the previous AR after it receives a PrRtAdv message. If the MH moves quite fast from the new AR to another AR (new AR') before completing its Layer-3 handover and performing binding updates to its correspondents, the three party handover takes place. This means that when the MH moves before configuring a new CoA on the new AR, the previous AR would still be considered its default router when MH attaches to the new AR'. Hence, the MH should send a FBU to the previous AR to set up a tunnel between the previous AR and the new AR'. This FBU may be in addition to the FBU it sends to the new AR. The result is that the MH should be able to receive

packets arriving at the previous CoA or new CoA through potentially different tunnels. If the MH returns to the previous AR without completing the Mobile IPv6 updates, it must send an FBU with lifetime set to zero so that the previous AR can disable any outgoing tunnels.

4.5 Mobility Management in IP Based LEO Satellite Networks

Mobility management in satellite networks strongly depends on the type of satellite network: GEO, MEO, and LEO, as discussed in Chapter 2. In general, due to the fixed position of the GEO satellites, location management in GEO networks may be considered to be similar to 2G networks. On the other hand, due to large coverage area provided by GEO satellites, handover in these networks is not a common issue. Contrary to GEO satellites, in MEO and particularly in LEO satellite networks, due to small coverage area and fast satellite movement, mobility management is a very important and challenging issue. Hence, this section discusses the basic issues of mobility management in LEO satellite networks. In addition, we introduce and evaluate the performance of two innovative handover protocols: an inter terrestrial-satellite network and an intra-satellite network handover management protocol.

4.5.1 Location Management in LEO Satellite Networks

Location management procedures for LEO satellite networks are also based on the LA concept (Location Area). However, LEO satellite network environment brings more challenging problems due to movement of the satellite footprints. Hence, location update mechanisms for mobile terrestrial networks [Aky99] cannot be applied straightforward in LEO satellite networks. For example, an LA cannot be associated with the coverage area of a satellite because of the very fast movement of a LEO satellite. Thus, location management techniques for terrestrial mobile networks have been modified and new LA definitions for satellite networks have been proposed. In [Mis97] LA is defined using (gateway, spotbeam) pairs, where Mobile Terminal (MT) must perform a location update whenever it looses the current satellite broadcast. This method reduces paging load, but it results in excessive signalling because of frequent location updates due to the very fast movement of spotbeams. Another approach for LA designations is proposed in [Lut98]. This approach is based on the geographical position of the user, where the MT obtains its geographical location information via the Global Positioning System (GPS) and then notifies the network of its current geographical position. A location update is performed when the MT's travelling distance exceeds a predefined value. This method causes a variable location update load and requires a large paging area consisting of all Fixed Earth Stations (FES) and satellites that have access to the MT's geographical position. A hierarchical database strategy for LEO satellite networks has been described in [Mcn00]. This location management technique uses a LA concept with the (Satellite, FES)-pair in order to reduce the paging load. By providing the Intermediate Location Register (ILR) in the three-level database hierarchy (HLR, ILR, and VLR), the proposed location registration procedure reduces the amount of long-distance signalling messages transmitted from the VLRs to the HLR. The placement of the ILR within the satellite systems depends on the geographical location of the gateways as well as the local availability of the terrestrial mobile networks.

4.5.2 Handover Management in LEO Satellite Networks

To ensure that ongoing calls are not disrupted as a result of satellite movement, calls should be handed off to new spotbeams, satellites, or mobile terrestrial networks. Hence, in LEO satellite networks the following handover scenarios are encountered: Inter-network handover, inter-satellite handover, and intra-satellite handover. In addition, another form of handover occurs as a result of the change in the connectivity pattern of the network. This type of handover is re-

ferred to as link handover. In the following, we will describe shortly the above-mentioned handover scenarios.

- **Inter-network handover** - This handover refers to the case when the ongoing connection is transferred from a terrestrial mobile network to a mobile satellite network and vice versa.
- **Inter-satellite handover** – Occurs when an ongoing call is transferred between two satellites. This results in the change of the connection route as the new satellite is involved in the route between two end terminals. The connection route can be changed by augmenting the existing route or rerouting the connection completely. Route augmentation is implemented simply by extending the original route connection with a hop to the next satellite. However, the resulting route is not optimal. Complete rerouting achieves optimal routes at the expense of signalling overhead. Another approach is *partial connection rerouting*, which consists on replacing and rerouting only the part of the connection that has been modified.
- **Intra-satellite handover** - If a handover occurs between two spotbeams served by the same satellite, it is referred as intra-satellite or spotbeam handover. Intra-satellite handovers occur frequently due to small size of the spotbeams. While inter satellite handover typically happens every 10 min, spotbeam handover occurs every 38 s. As spotbeam handover occurs on the same satellite, the ability to maintain on going connections or not depends on the satellite resources and the traffic load on the specific spotbeam. If no ground-satellite channels were available in the new spotbeam, the frequent handovers would cause blocking of ongoing calls. No rerouting is required for the spotbeam handover.
- **Link handover** – This type of handover occurs when the topology of the LEO satellite network changes due to inter-satellite links that are temporarily turned off. There are two cases when satellites switch off their links to other satellites in the neighbour orbits. The first case is when satellites move over the polar areas and the second case is due to the change in distance and viewing angle between satellites in contra rotating neighbour orbits. Any connection is subject to rerouting if it is passing through a link that will be turned off before the connection is over. If the number of connections that need to be rerouted due to link handover is large, the resulting rerouting attempts cause signalling overhead in the network and some of the ongoing calls might be blocked.

In the following sections we will introduce two innovative handover management protocols for inter terrestrial-satellite mobile networks [Ngu01a] and intra-satellite mobile network [Ngu01b], refering to the Figure 4-15.

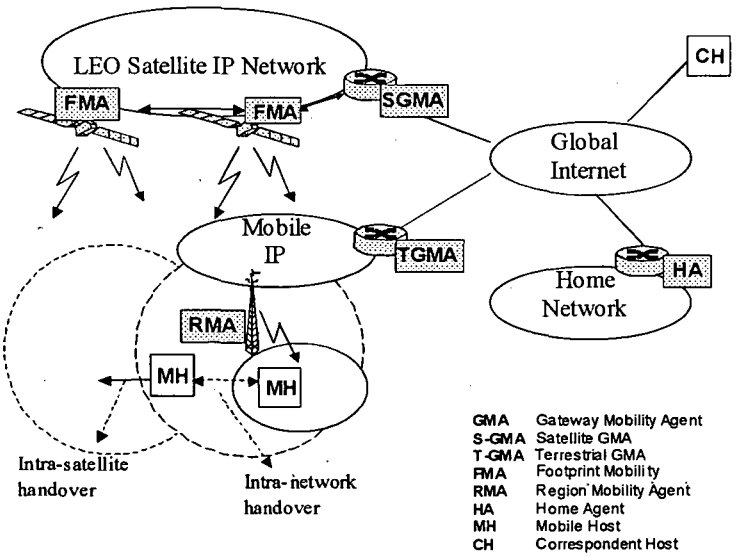


Figure 4-15: Handover Scenarios in LEO Satellite IP-based Networks

For inter-network mobility management, the basic mobile IPv6 protocol is used, whereas for intra-network, the mobile IPv6 protocol enhanced with a hierarchical mobility agent management scheme is applied. Mobility management functions are carried out in the gateways and satellites. To perform these functions, each gateway and the corresponding satellite cache all the required information for the particular service area. Both the satellite and terrestrial networks have hierarchical mobility agent structures where routers with Gateway Mobility Agents (SGMA and TGMA) are considered as ingress points, viewed from outside the networks. The lower mobility agent level is called the Footprint Mobility Agent (FMA) and the Region Mobility Agent (RMA) for the satellite and terrestrial networks, respectively. Within each network, the regional binding update occurs when mobile users change their access points. Only when a mobile user moves to another network, they need to send a binding update to the HA and the CH.

4.5.2.1 Inter-Terrestrial-LEO Satellite Network Handover Protocol

Generally, we can classify inter-network mobility into the following scenarios:

- Inter-network mobility between a home network and a foreign network.
- Inter-network mobility between two foreign networks.

In the inter-network mobility between a home network and a foreign network, where either the current Access Router (AR) or the new AR belongs to the home network, the current GMA can decide immediately if the mobile user has roaming rights in the new network based on either its contract or its home address. After that, the handover initiation message is forwarded to the new gateway router to ask for a handover. The MH will obtain a new regional CoA from the GMA and a Local CoA (LCoA) from the FMA/RMA. Thereafter, the binding update is sent to its HA and CH. In the inter-network mobility between two foreign networks, where both the current AR and the new AR belong to two different foreign networks, the new gateway router would need to exchange authentication messages with the home network after receiving the forwarded handover initiation message from the current gateway router. The long network-layer handover latency could occur especially when home to foreign network distance is large. To reduce the handover latency, a possible solution could be that the new gateway accepts the handover initiation, assigns a new CoA to the MH, provides all necessary functions like smooth handover, performs the binding update and then does the authentication process later to decide whether the connection is further accepted or not.

Protocol Description

The handover signalling message flow from the terrestrial network to the satellite network is described in Figure 4-16. The message flow is derived based on the handover management scenario shown in Figure 4-15. The handover procedure is implemented in the following three phases:

- **Initiation**: The MH detects the degrading of current link parameters and measures the new link parameters (here at the multi-mode terminal). The initiation can also be triggered based on the QoS of the ongoing connection, or pricing. The handover initiation message, which could include information of the user requests such as QoS requirements, is sent to the current access point and then forwarded to the current gateway - TGMA. The current gateway will send the request to the nearest gateway - SGMA of the new network to ask for handover permission.
- **Decision**: The new gateway, subject to the availability of network resources and the user's QoS requirements, accepts or rejects the handover request. If the new network accepts the handover request, the new network link-layer information is sent to the MH, which is switched to the new connection to access the new network with the new radio characteristics. The new gateway might also inform the user (MH) whether the new network could guarantee

the required QoS or not. If not, the user might have to re-negotiate QoS of the ongoing connection.

- **Execution**: The MH forms a new CoA based on the Router Advertisement of the new access router, broadcasted in a beacon signal. The MH sends an IP connection request to the new access router and then receives its reply for continuing the connection. The QoS requirements of the ongoing connection could be re-negotiated during the control process. A binding update message is sent to the HA and the CH through the new GMA. In the mean time, the old signaling and traffic links are only dropped after receiving the Handover_complete message, i.e., signalling diversity is used for the inter-network handover. A forwarding request is sent from the new gateway to the old gateway and then to the old access routers to ask for forwarding all packets destined to the previous CoA of the MH.

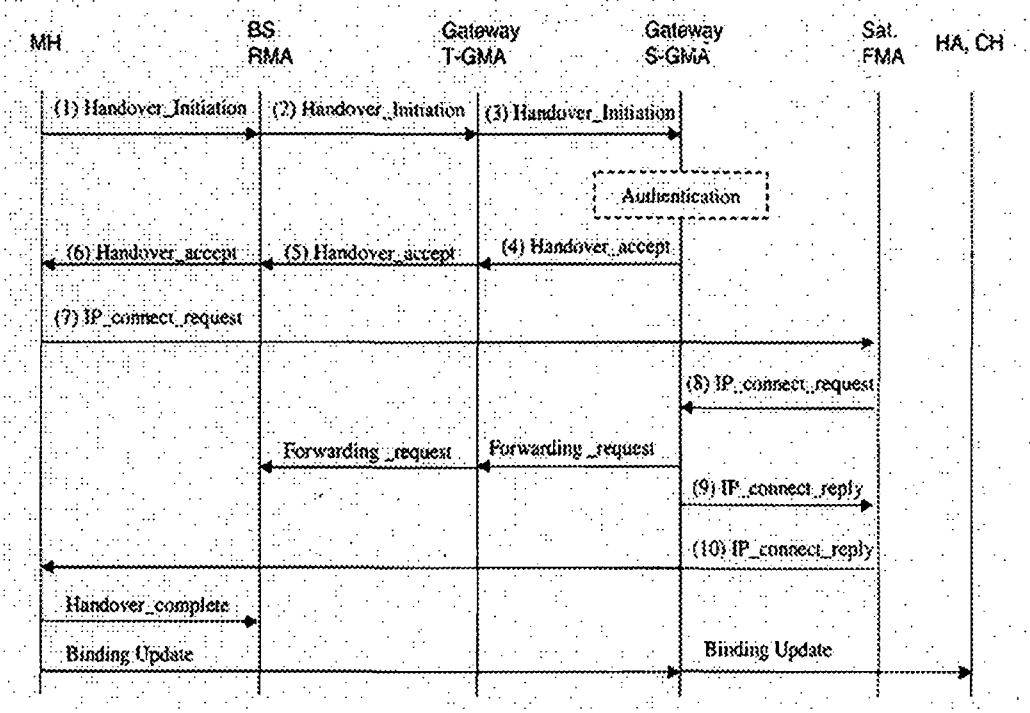


Figure 4-16: Terrestrial-to-Satellite Handover Signaling Flow

Performance evaluation

The handover metrics consists of the handover delay (Ho-Delay), handover dropping probability and the number of forwarding packets. The handover delay consists of decision delay and execution delay. The decision delay is the time difference between sending the handover initiation message and receiving the handover accept message. The execution delay is the time needed for a successful access to the new access router (the new mobility agent) and the execution of the ongoing IP connection. The maximum handover delay can be calculated by using Equation (4-1), whereby the individual delay components are calculated by using Equations (4-2) and (4-3):

$$Ho\_Delay = decision\_delay + execution\_delay, \tag{4-1}$$

$$decision\_delay = \sum_{i=1}^{6} PT_i + \sum_{i=1}^{6} P_i + T_{aut}, \tag{4-2}$$

$$execution\_delay = T_{RA} + \sum_{i=7}^{10} PT_i + \sum_{i=7}^{10} P_i, \tag{4-3}$$

PT_i: Message propagation and transmission delay,
P_i: Message processing delay, i: message index,
T_{aut}: Authentication time,
T_{RA}: Beacon period of broadcast router advertisement in the new network.

Handover dropping can be considered to occur mostly in the case of a handover from the terrestrial boundary cell to the satellite footprint because the MT might have no new radio access before leaving the terrestrial coverage area [Mcn00]. The handover dropping probability depends on the value of the decision-delay and the residency time of the MH in the terrestrial boundary cell. It depends on the moving speed of the MH and the terrestrial cell size. A detailed calculation of handover dropping probability is given in [Mcn00]. To reduce the number of lost packets, the forwarding process between the old and new gateway is essential [Koo00]. The number of forwarded packets depends on the execution delay, binding update delay, and connection rate. It also depends on how forwarding is implemented, i.e., in the GMA only or both in the GMA and the RMA (FMA). We propose that for non real-time traffic, forwarding should be executed by both the GMA and the RMA (FMA) to minimize the number lost packets, which can cause wrong feedback to the sender (CH). For real-time services, forwarding only at the GMA might be enough because if forwarding is also implemented in the RMA (FMA), the forwarding packets could experience a longer delay than other coming packets that should be discarded. We have measured the number of forwarding packets for the inter-network handover from the terrestrial to the satellite network (Figure 4-17) and vice versa (Figure 4-17) by means of software simulations. The following parameters are chosen. Delays between the HA (CH) and the gateways are assumed to be 10 ms. The delay between gateways is taken 10 ms. A constant delay of 10 ms is assumed between the TGMA and the RMA, and a variable delay between the SGMA and the FMA. Note that HA, CH, TGMA, RMA, and SGMA are on the ground, whereas FMA on the satellite. Transmission rates of links are very high. Thus, the effects of transmission delay are neglected. Without loosing the generality, the CH generates packets according to a Poisson process and an on-off model. For both distributions, we have taken the same value for the average number of the generated packets. With the Poisson process, mean packet arrival time is 4 ms. By using the on-off model, on-time and off-time periods are exponentially distributed with mean durations 3 s and 0.5 s respectively. During on-time period, packets are generated according to exponential distribution with the mean packet inter-arrival time of 4 ms.

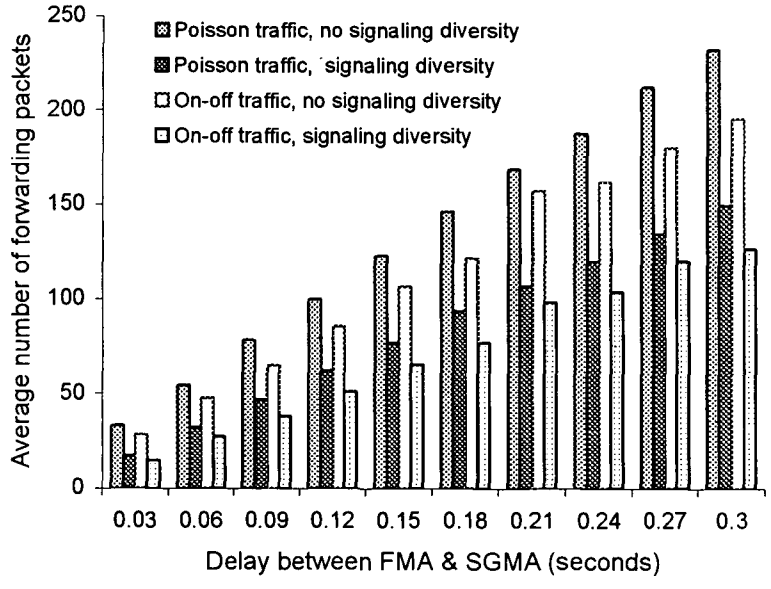


Figure 4-17: Forwarding Packets in Terrestrial-Satellite Handover

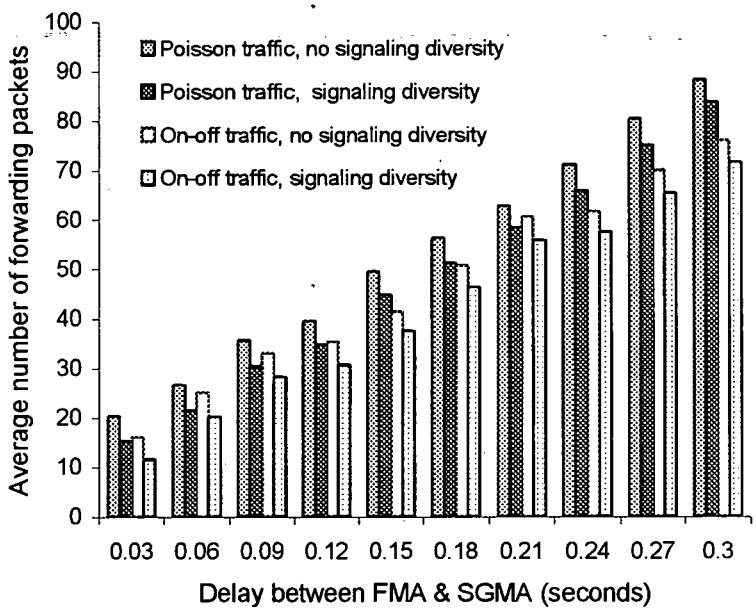


Figure 4-18: Forwarding Packets in Satellite-Terrestrial Handover

The results show that signalling diversity is necessary to reduce the number of forwarding packets. Due to the long latency in satellite networks, the handover from the terrestrial to the satellite network causes more packets to be destined to the terrestrial routers than in the case of handover from satellite network to terrestrial network, before the CH is updated with a new CoA of the MH. This is due to longer latency of the binding update message. In the case of the handover from the satellite to the terrestrial network and an increasing delay between the SGMA and the FMA, more packets are still in the satellite networks after handover finishes, causing more packets to be forwarded. Packet generation according to Poisson process results in more packets needed to be forwarded than in the case packet generation according to the on-off model. The reason is that by using on-off model, packets are generated in burst mode i.e., when handover occurs, there might be fewer packets to be sent.

4.5.2.2 Intra LEO-Satellite-Network Handover Protocol

Intra-network handover in the LEO satellite IP-based networks consists of intra-satellite and inter-satellite handovers. The intra-satellite or spotbeam-handover is in fact a handover execution at the link-layer only. In this section, we investigate the inter-satellite handover in the IP layer. To realize the handover procedure, two possible inter-satellite handover schemes are proposed: proactive and reactive handover.

- **Proactive handover** - The network, i.e., the current satellite predicts the handover and asks the new satellite for resource reservation and a new CoA allocation before the handover actually occurs.
- **Reactive handover** - No preparation for a handover is performed in advance. The resource reservation and CoA assignment are done after the MH has issued a handover request.

The proactive inter-satellite handover scheme is more complicated than the reactive scheme because it requires more network resources and a high computation load. However, the proactive handover scheme is more appropriate for LEO satellite networks because the handover can be predicted and the positions of satellites are also known in advance. We propose that the selected scheme should depend on service types, e.g., for real-time applications proactive handover is more suitable, whereas reactive handover can be used in the case of non real-time appli-

cations. Subject to traffic type and resource availability, the network decides which scheme should be applied.

Protocol Description

In the following, we will describe the proactive handover procedure shown in Figure 4-19. In order to have a better insight into the differences between the two-handover schemes, the reactive handover procedure is also shown in Figure 4-20.

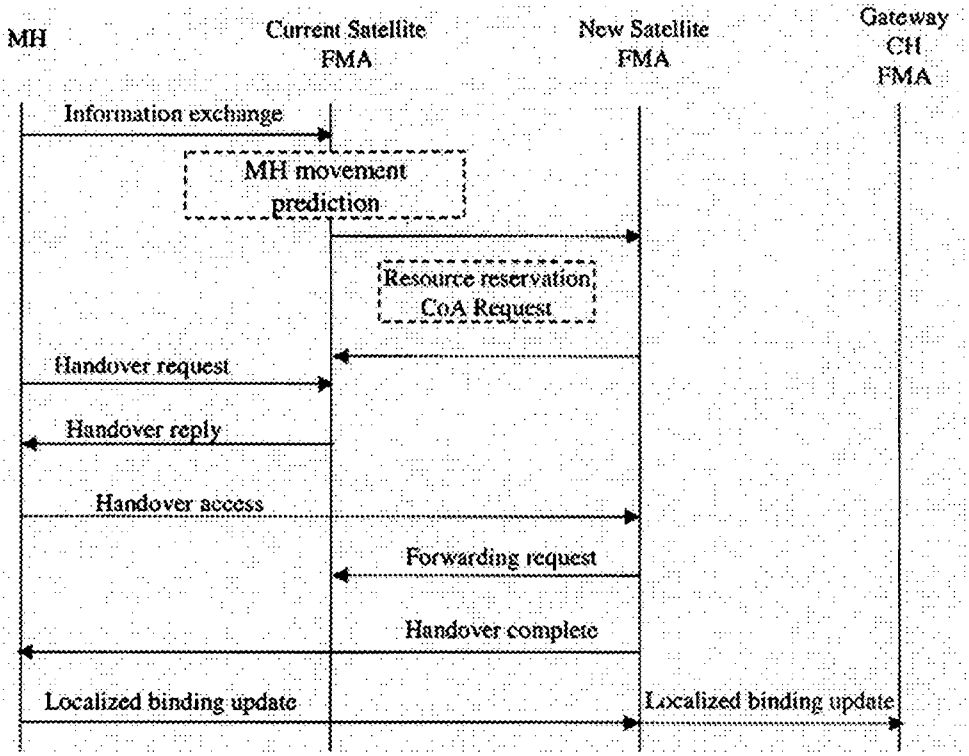


Figure 4-19: Proactive Inter-Satellite Handover Procedure

The inter-satellite proactive handover procedure includes three phases: handover prediction, initiation, and handover execution:

- **Handover prediction**: The MH and the current satellite exchange information relevant to location update. Based on the information provided by the MH, the current satellite can anticipate the MH's cell-location. The satellite needs to determine if the MH is moving within its subnet or to a new one (whether the IP layer handover is taking place). If the IP layer handover is predicted, then the current satellite prepares the handover in advance by requesting resource reservation in the new satellite (link layer and IP layer resources). Subject to availability of resources, the new satellite reserves the requested resources and informs the current satellite.
- **Handover initiation**: Based on the link quality measurement, the mobile host detects that an inter-satellite handover has to occur. It initiates the handover by sending a handover request to the current satellite. The current satellite sends a handover reply message to the MH with the embedded information about the link parameters and the new CoA.
- **Handover execution**: The MH sends a handover access message to the new satellite. Because a CoA is already assigned to the MH, the message could be a request for a connection set up between the mobile host and the new satellite. The new satellite replies with a handover complete message. Having completed the handover, the MH sends a localized binding message according to the connection scenarios. A forwarding process will be carried out to

forward all packets, destined to the MH, to the new satellite aiming to provide a smooth handover [Koo00].

The reactive handover scheme differs from the proactive scheme in terms of handover initiation and execution phases. In this scenario, no resource reservation is performed in advance like in the proactive scheme. A mobile user will initiate a handover request to the new satellite based on the access link quality measured in the terminal.

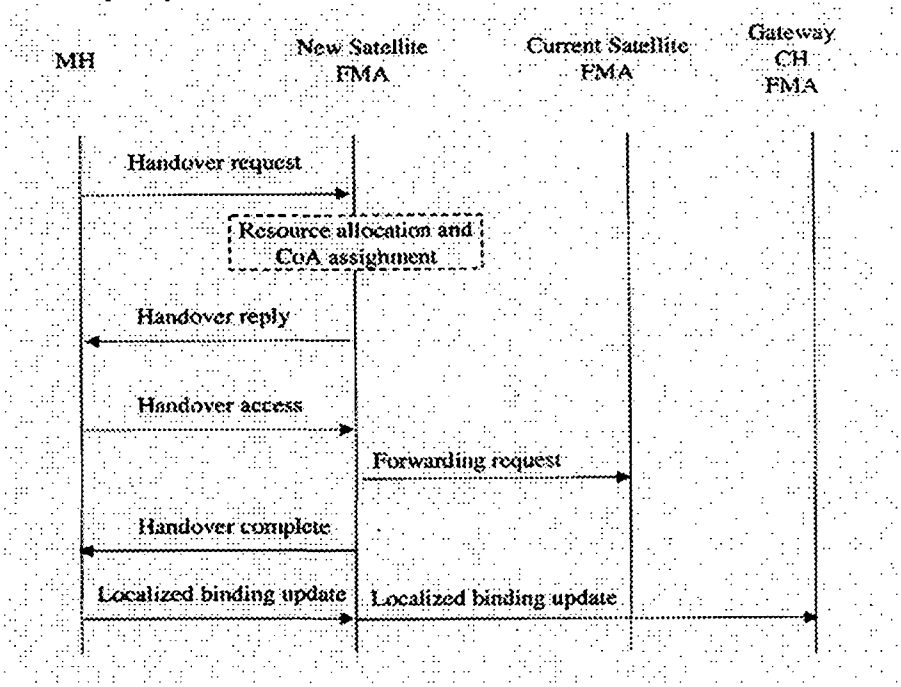


Figure 4-20: Reactive Inter-Satellite Handover Procedure

When the user recognizes that a handover is necessary, it sends the Handover Request message to the new satellite to ask for the handover process. The new satellite then checks if the requested resources are available and if there are free resources it allocates a new CoA to the user. After that, the Handover Reply message is sent to the user, which contains information for the handover process such as a new CoA and link parameters. The user applies the obtained information to perform the handover execution phase as described above.

Performance evaluation

We evaluate quantitatively the binding delay and the number of forwarded packets of inter-satellite IP handovers for a particular constellation, a given traffic and simulation scenarios. The considered satellite constellation has 84 satellites distributed into six orbits. The satellite period is 110 minutes. Each satellite has four ISLs, including two intra-orbital ISLs and two inter-orbital ISLs, which are switched off when the satellite latitude exceeds 75 degrees. We periodically update the topology information and routing table while taking into account the utilization of links. Because the full information of a real global traffic density is not available, we assume that homogeneous traffic is applied. For satellites covering polar areas, we assume that the loaded traffic is very small, about 1% of non-polar area satellites. A satellite is loaded with background Poisson traffic, destined to other satellites. The background traffic load factor to each satellite is defined as follows:

$$Load\_factor = \frac{Total\_mean\_traffic\_load}{Total\_ISL\_capacity} \qquad (4\text{-}4)$$

We observed 1000 connections between random user pairs. For each connection, packets are generated deterministically with a packet size of 512 bytes and a connection rate of 320 kbit/s.

The users are initiated by connecting to randomly selected satellites. We have measured the binding delay and the number of forwarding packets for each handover of the connections under studied network load traffic of two scenarios: light background traffic with very small load factor of 0.05 and medium background traffic with a load factor of 0.3. In general, as shown in Figure 4-21 to Figure 4-24, after an inter-satellite handover, many packets need to be forwarded from a current to a new satellite. The constellation equipped with cross-seam ISLs reduces both the binding delay and the number of forwarded packets. When background traffic load increases, binding delay is increased because the binding packets have to wait in queue longer. That results in higher number of forwarding packets.

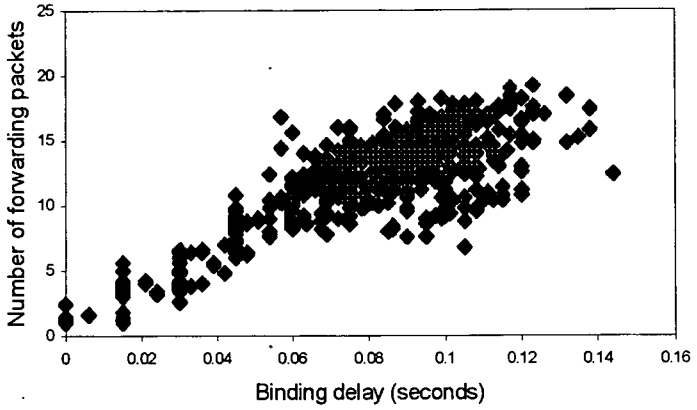


Figure 4-21: Number of Forwarding Packets: Constellation with Seam ISLs, light background traffic

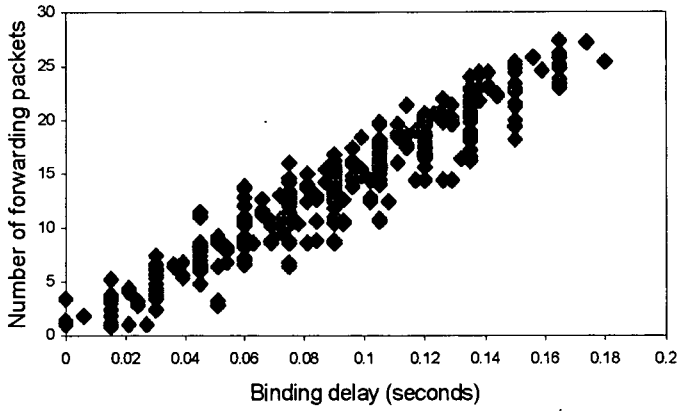


Figure 4-22: Number of Forwarding Packets: Constellation without Seam-ISLs, light background traffic

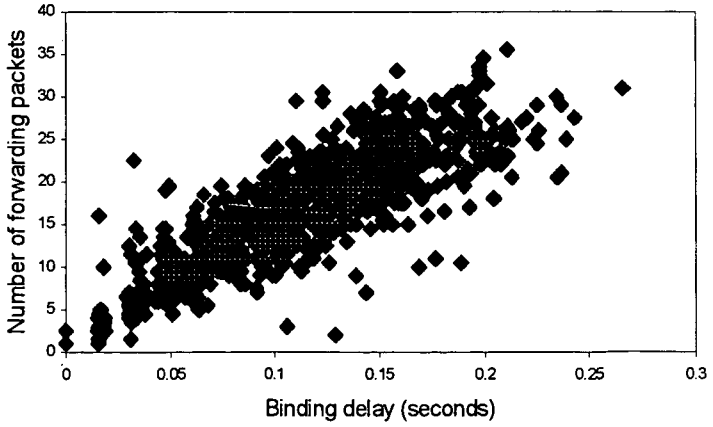


Figure 4-23: Number of Forwarding Packets: Constellation with Seam-ISLs, medium background traffic

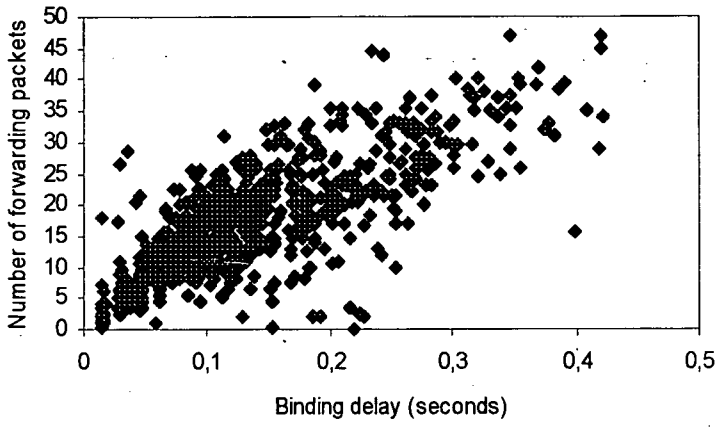


Figure 4-24: Number of Forwarding Packets: Constellation without Seam-ISLs, medium background traffic

4.6 Review

This chapter began with the definition of the Mobility Management concept and its components. Next, the handover types and handover scenarios were classified. The presentation then moved on to the description of the mobility management in 2G-GSM networks. Next location and handover management in UMTS networks specified by 3GPP 99, including inter-system handover, were presented. This chapter then explained the mobility management in All-IP networks. MIPv4 and several other protocols as extensions to MIPv6, such as HMIPv6, RegReg6, and Fast Handover were clarified. The chapter closed with the discussion of the mobility management in IP based LEO satellite networks. Two innovative handover protocols: inter-terrestrial satellite network and intra-satellite network handover-management protocols were introduced and their performance was evaluated.

5 Quality-of-Service in Broadband Communication Networks

Broadband networks aim to accommodate a wide range of applications with different Quality-of-Service (QoS) requirements. In addition, broadband communication networks have to interwork with a variety of established network technologies, each with its own performance characteristics. QoS makes sense only when it is provided end-to-end while each network has its own QoS mechanisms. Therefore, providing QoS to different users' applications in this heterogeneous environment is an essential task of broadband communication networks and presents a great challenge to network designers as well as to network operators and service providers. The two main fixed broadband communication networks, ATM and the Internet were designed with different approaches to QoS issues. Designers of ATM were concerned with QoS provisioning from the beginning and developed appropriate QoS mechanisms for ATM networks. In contrast to ATM, the Internet was designed to provide only best-effort service, handling all applications in the same way. Hence, QoS mechanisms had to be developed additionally in order to satisfy the requirements of new real-time applications. Broadband wireless communication networks such as UMTS and WLAN also have different approaches to QoS issues. The 3GPP originally specified mechanisms for QoS support of services offered by UMTS for user applications. In contrast to UMTS, IEEE 802.11 WLAN was initially designed to offer only best-effort services. Thereof, the existing standard is supplemented with a IEEE 802.11e standard to provide QoS for wide range of multimedia and non-multimedia real-time applications. In this chapter QoS issues and mechanisms for Internet, UMTS, and WLAN will be discussed.

5.1 Quality-of-Service in Internet

Today's Internet treats all applications in the same way, known as best-effort service. New IP based applications and particularly real-time broadband applications have requirements that cannot be met with the best-effort service. Hence, in order to differentiate services offered to different applications, IETF has developed Quality-of-Service (QoS) architectures and mechanisms such as Integrated Services (IntServ), Resource Reservation Protocol (RSVP), Differentiated Services (DiffServ), and Multi Protocol Label Switching (MPLS).

In the following subsections, an overview of the architecture and main features of these Internet QoS techniques will be discussed.

5.1.1 Integrated Services Architecture

Integrated Services (IntServ) [RFC1633] is an extension to the Internet architecture to provide Quality-of-Service (QoS) to real-time applications that demand more from the network than best-effort service offers. The IntServ architecture is based on resource reservation for each flow. This requires a resource reservation protocol to set up flow-specific states in the routers along the flow path, which represents a fundamental change to today's Internet service model. Today's Internet architecture was founded on the concept that all flow-related state should be in the end systems. The Integrated Services Working Group proposed two new service models for

real-time applications: guaranteed service [RFC212] and controlled-load service [RFC211]. Guaranteed service is for applications requiring a fixed delay bound. Controlled-load service is for applications requiring reliable and enhanced best-effort service. Integrated services are implemented in four components: the admission control process, the classifier, the packet schedule, and the resource reservation signaling protocol. Admission control, classification, and scheduling are part of the traffic control tools of the network element. Admission control is the process of deciding whether a newly arriving traffic flow can be granted the requested QoS without impacting earlier guarantees. This process must be performed by each element of the network in order to determine whether there are enough resources to accept the service request. The admission-control decision criteria depend on the requested service model. The classifier classifies each incoming packet according to their QoS request. The choice of a class may be based upon the contents of the existing packet headers or some additional classification information added to each packet. All packets in the same class receive the same treatment but different routers along the path may classify the same packet differently. The packet scheduler will then schedule the packet according to its class, in order to meet its QoS requirements. Resource reservation signaling is needed because applications requesting guaranteed or controlled-load service must reserve resources before transmitting their data. The Resource Reservation Protocol (RSVP) [RFC2205] is designed for this purpose. Integrated Services provide reliable end-to-end QoS to traffic flows, provided no path change or network failures occur during the life of the flow. However, the per-flow reservation does not scale well to the huge number of flows in the core Internet. Hence, due to its lack of scalability IntServ architecture is recommended for access networks and corporate networks where the number of flows is much lower. In the following subsections, IntServ models and RSVP will be described.

5.1.1.1 Guaranteed Service

The purpose of guaranteed service is to provide guaranteed bandwidth and strict bounded end-to-end queuing delays for all datagrams of the conforming flows. Guaranteed service controls only the maximal queuing delay. By combining the parameters from the various service elements in a path, an application can accurately estimate, a priori, what queuing delay guaranteed service will guarantee for specified flows. This service model is intended for applications that require a firm guarantee that a datagram will arrive no later than a certain time after transmission.

Service Invocation

Applications invoke guaranteed service by specifying the traffic parameters (TSpec) and the desired service (RSpec) to the network element.

TSpec describes traffic sources and it includes the following parameters:

- The bucket rate r, measured in bytes/sec, denotes the rate at which tokens arrive at the bucket.
- The depth of the token bucket b, measured in bytes.
- The peak rate p, measured in bytes per second, denotes the rate at which packets will be sent,
- The minimum policed unit m, is measured in bytes. Any IP datagram that is less than size m is counted, when tested for conformance to the TSpec, as being of size m.
- The maximum datagram size M that will be sent by the flow conforming to the TSpec, measured in bytes.

Guaranteed service uses the Token-Bucket-Tspec defined in [RFC2215] to describe a data flow's traffic parameters. The description above is of that parameter. Given the description of a flow, a network element (a router, a subnet, etc) computes various parameters describing how the service element will handle the flow's data. The service requirements (RSpec) are described with two parameters: a rate R and a slack term S. The R is the service rate or bandwidth requirements measured in bytes/second and must be greater than or equal to r. The slack term S is

the difference between the desired delay and the delay obtained by using a reservation level R and it must be nonnegative. The slack term can be used by the network element to compute a lower level of resource for the specified flow. The use of guaranteed service in conjunction with the RSVP resource reservation setup-protocol is specified in [RFC2210]. This document gives the format of RSVP Flowspec, Sender-Tspec, and Adspec objects needed to support applications desiring guaranteed service and gives information about how RSVP processes those objects.

Delay Calculation

Based on the Tspec and Rspec, the worse case end-to-end queuing delay for a flow can be calculated. A simple approach is to use the fluid model. The fluid model at service rate R essentially yields the service that would be provided by a dedicated wire of bandwidth R between the source and the receiver. Since guaranteed service delivers specific delay bounds to the flows, it has to be based on both a model of source behavior and a model of how the network elements handle the flow's data. The models are shown in Figure 5-1.

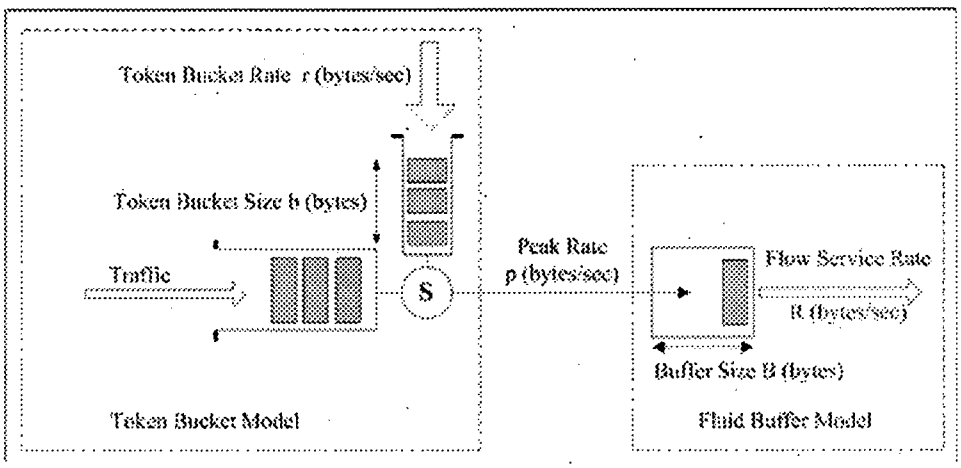


Figure 5-1: Guaranteed Service Model

The model on the left is a token bucket for the source. The model on the right is the "fluid buffer model" of a link in a router. The bandwidth (or service rate) R and the buffer size B are the resources that a router must allocate for guaranteed flows. Actually, the flow's level of service is characterized at each network element by resources R and B. The bandwidth R, in fact, represents only the share of the link's bandwidth the flow is entitled to and B represents the buffer space in the network element that the flow may consume. The model operates as follows. The source releases fluid at an average rate r (rate of generated tokens) but it is possible for the source to produce (occasionally) fluid faster than rate r. This excess is stored at the source and released at rate r. If the source has not transmitted anything for some time, tokens keep accumulating up to a limit, b. As long as there are tokens available, any fluid that arrives at the source can be released instantaneously. The rate at which fluid can be transmitted is p. The fluid flow from the source arrives at the network element, which serves it at rate R. The buffer B is needed because the transmission rate p may be much greater than R. The definition of guaranteed service relies on the result that the fluid delay of a flow conforming to the token bucket and being served by a line with bandwidth R is bounded by b/R (given that $r \leq R$). This value is obtained by assuming that p is infinite (that is, the fluid is instantaneously transferred from the source to the buffer), and by assuming that there are b tokens available. Under these assumptions the buffer at the network element would be filled up with b units of fluid and the largest delay experienced would be the b/ R. However, real network elements do not implement guaranteed service exactly according to the fluid model, so two error terms, C and D, have been introduced to represent how the actual implementation of the guaranteed service deviates from the fluid

model. The error term C is rate-dependent and represents the delay a datagram in the flow experience due to the rate parameter and datagram length (packetization delay at nodes). The error term D is rate-independent, per-element error term and represents the worst-case non-rate-based transit time variation through the service element. It is generally determined or set at configuration time. The error term D is measured in units of microseconds.

Incorporating these parameters, the adjusted delay is:

$$\text{Delay} = b/R + C/R + D \qquad (5\text{-}1)$$

Equation (5-1) shows that the queuing delay is primarily a function of two parameters: the token bucket (in particular, the bucket size b) and the data rate (R) the application requests. These two values are completely under the application's control, meaning that guaranteed service gives applications considerable control over their delay. Furthermore, if the delay is larger than expected, the application can modify its token bucket and data rate in predictable ways to achieve a lower delay. In order to determine specific end-to-end delay bounds, guaranteed service relies on the behaviour of each network element in the path starting from the source. The delay bounds are computed along the path of the flow according to Equation (5-1). The end to-end sums of C and D on a path from the sender to the receiver are C_{tot} and D_{tot}, respectively. These parameters are computed locally by each network element in the path and then added to the total. The unit of C_{tot} is the byte, whereas D_{tot} is measured in microseconds. C_{tot} and D_{tot} are used by the endpoints to compute the end-to-end delay bounds achievable on the path. Incorporating the C_{tot} and D_{tot} error terms and packet lengths, the end-to-end worst-case queuing delay can be calculated as follows:

$$Qdelay_{end2end} = (b - M)(p - R)/R(p - r) + (M + C_{tot})/R + D_{tot} \quad (p > R \geq r) \qquad (5\text{-}2)$$

$$Qdelay_{end2end} = (M + C_{tot})/R + D_{tot} \quad (\text{case } R \geq p \geq r) \qquad (5\text{-}3)$$

It is important to note that the queuing delay determined by guaranteed service is only a component of the total delay. The other components of end-to-end delay are the propagation delay, shaping delay, and other processing delays inside the hosts. These delays are considered as a fixed component of the total delay. Hence, to estimate the total end-to-end delay a datagram will experience, the fixed delay must be computed and added to the guaranteed queueing delay.

Policing and reshaping

To ensure conformance to the TSpec, guaranteed service traffic must be policed at the network access points. The usual policy enforcement is to treat nonconforming packets as best-effort datagrams at all subsequent routers on the traffic flow path and marked accordingly if such a facility is available. In addition to policing of traffic flows at the edge of the network, guaranteed service also requires reshaping of traffic to the token bucket of the reserved TSpec at certain points on the distribution tree (within network). Any packets failing the reshaping are treated as best-effort at all subsequent routers. Reshaping must be applied at any points where it is possible for a data flow to exceed the reserved TSpec, even when all senders associated with the data flow conform to their individual TSpecs.

5.1.1.2 Controlled-Load Service

Controlled-load service is intended for a certain class of real-time applications that can adapt somewhat to network conditions, but which tend to perform badly on loaded networks. This service model attempts to create "unloaded" (not heavily loaded or congested) network conditions for such applications, but does not provide service guarantees in terms of delay bounds and bandwidth. Hence, the controlled-load service does not accept or make use of specific target values for control parameters such as delay or loss like the guaranteed service model. In fact, the

controlled-load service model lies somewhere between best-effort service and guaranteed service through appropriate admission control. For this reason, it is often referred as better than best-effort service. So the end-to-end behavior provided to an application by network elements closely approximates the behavior visible to applications receiving best-effort service "under unloaded conditions" from the same network elements.

In requesting the controlled-load service, assuming the network is functioning correctly, applications may expect that [RFC2211]:

- The network will successfully deliver a very high percentage of transmitted packets.
- The transit delay experienced by a very high percentage of the delivered packets will not greatly exceed the minimum transmit delay experienced by any successfully delivered packet.

Quality-of-Service disruption in a delivery under controlled-load service is related to the burst time. It is defined as the time required for the flow's maximum size data burst to be transmitted at the flow's requested transmission rate, where the burst size and rate are given by the flow's TSpec, as described below. Quality-of-Service disruption occurs for a short duration when a flow receiving controlled-load service experiences [RFC2211]:

- Little or no average packet queueing delay over all timescales significantly larger than the "burst time".
- Little or no congestion loss over all timescales significantly larger than the "burst time" defined above.

Events of shorter duration are viewed as statistical effects, which may occur in normal operation. Events of longer duration are indicative of failure to allocate adequate capacity to the controlled-load flow.

Service Invocation

Applications invoke controlled-load service by specifying the data flow's desired traffic parameters (TSpec) to the network element. This TSpec takes the form of a token bucket specification plus a peak rate (p), a minimum policed unit (m) and a maximum packet size (M). The token bucket specification includes a bucket rate r and a bucket depth, b. The rate r is measured in bytes of IP datagrams per second. The bucket depth b is measured in bytes. The peak rate p is measured in bytes of IP datagrams per second and it may always be ignored by a controlled-load service. It uses the Token-Bucket-Tspec defined in Reference [RFC2215] to describe a data flow's traffic parameters. The use of controlled-load service in conjunction with the RSVP resource reservation setup-protocol is specified in reference [RFC2210]. This document gives the format of RSVP Flowspec, Sender-Tspec, and Adspec objects needed to support applications desiring controlled-load service and gives information about how RSVP processes those objects.

Service Implementation

Each network element accepting a request for controlled-load service must ensure that adequate bandwidth and packet processing resources are available to handle the requested level of traffic specified in the TSpec of the requestor. This must be accomplished through admission control. The admission control algorithm for deciding whether a flow can be accepted is left as a local matter and may be implementation specific. One possible implementation of controlled-load service in a network element is shown in Figure 5-2. All packet streams flow through the packet classifier. This determines which packets are eligible for controlled-load service and which are not. At the exit of the packet classifier, there is a token bucket. The token bucket mechanism, described in [Par94], is used to determine which of the packets of the flow identified by the

packet classifier are eligible to receive the controlled-load service. This process is known as the conformance of the flow. Controlled-load service modules provide QoS control for traffic conforming to the TSpec given at setup time. In the implementation shown in Figure 5-2 there are two queues with different priorities. The upper queue has higher priority and is used for controlled-load service; this means that packets that conform to the token bucket are put in this higher priority queue. An admission control algorithm is used to limit the amount of traffic placed into this queue. This algorithm may be based either on the specified characteristics of the high-priority flows (using information provided by the TSpecs), or on the measured characteristics of the existing high-priority flows and the TSpec of the new request.

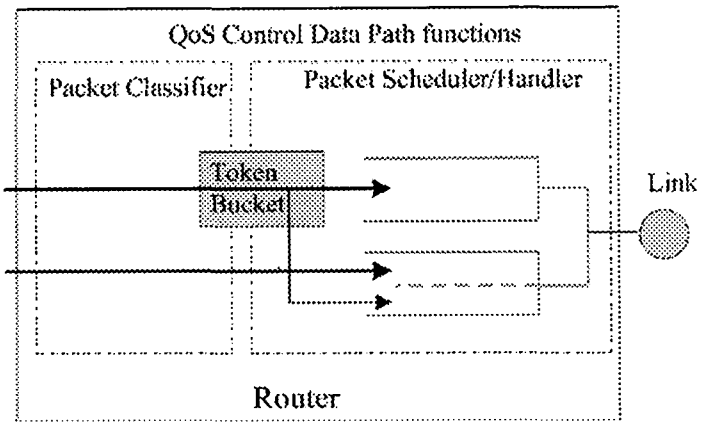


Figure 5-2: Controlled Load Service

The lower queue is shared between packets, which do not conform to the token bucket for the flow and packets that receive only best-effort service. There are different views on how to treat the non-conforming controlled-load service traffic. According to the [RFC211], the excess traffic (non-conforming traffic) from controlled-load service should be treated as best-effort traffic. As shown in Figure 5-2 the excess traffic is queued into the best-effort queue. However, this non-conforming traffic should not adversely affect the normal best-effort service. For example, it should not cause significant degradation of normal best-effort service. Hence, some mechanisms are needed to handle excess traffic to ensure that it does not disturb the best-effort traffic. Such mechanisms could be weighted fair queuing or class-based queuing, for instance.

5.1.1.3 Resource Reservation Protocol - RSVP

The Integrated Services (IntServ) models described in the previous sections require some information to be communicated between the hosts and the network elements to reserve network resources for QoS provisioning. For this purpose IETF, has developed an independent signalling protocol for reserving of resources called the Resource ReSerVation Protocol - RSVP [RFC2205]. RSVP signalling is used to configure the QoS flow handling mechanism in RSVP-capable routers along the path of the traffic. However, this is not the only possibility. Some other protocols have been designed for this purpose as well. RSVP is independent of Integrated Services, but it is mostly associated with IntServ and is very often considered part of the IntServ architecture. The architecture of RSVP was influenced in part by the requirements to support large multicast groups, like multicast-video-conferencing applications, for example. RSVP is a receiver-oriented protocol. Receivers are responsible for deciding which resources will be reserved and for requesting the reservation of resources for unicast or multicast flows. Furthermore, RSVP is a simplex protocol. For each flow direction, resources are reserved independently. It is important to note that each RSVP operation only applies to packets of a particular session. RSVP identifies a communication session by a combination of destination address, transport layer protocol type, and destination port number. RSVP is independent from the applied routing protocol, and it is designed to operate with current, as well as future unicast and multicast routing protocols. The decision to select the path for reservation is done by routing

protocols. The RSVP protocol simply consults the forwarding table and sends the RSVP message accordingly. However, for efficient use of network resources, coordination between routing decisions and resource reservation is needed so that the choice of the route can depend on the quality of the requested service (QoS routing). Great efforts are now being given in research to use RSVP as a signalling protocol in large MPLS core networks. Hence, RSVP protocol is extended to a TE-RSVP protocol to include traffic-engineering aspects. With traffic engineering extensions, an explicit route object can be carried in the RSVP message to specify the entire path over which the reservation should be made.

RSVP Messages

There are several RSVP messages: Path, Resv, PathErr, ResvErr PathTear, RevTear, and ResvConf, shown in Figure 5-2 associated with the direction of the flow. Each RSVP message consists of a common header and a variable number of objects. The most important RSVP messages are the Path and Resv, which are used to create path state and reservation state, respectively. The RSVP error messages, PathErr and ResvErr signal errors to the sender of the message. PathErr is sent upstream to the sender that created the error; whereas ResvErr is sent to the receiver if the reservation is rejected at any router along the upstream path. PathTear and ResvTear are used to immediately remove the path or reservation state, respectively. PathTear is sent downstream, whereas ResvTear is sent upstream. The reservation confirmation message ResvConf is sent to the receiver to acknowledge the reservation request if it has asked for confirmation of the Resv message.

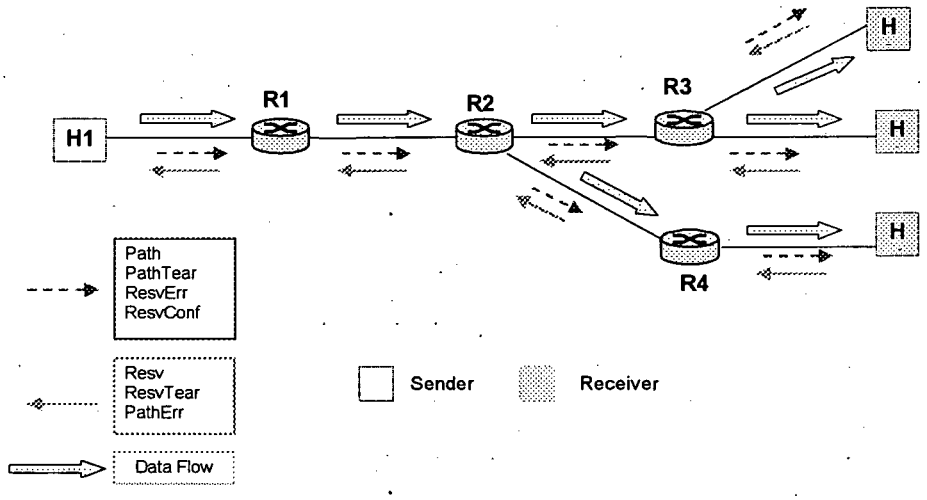


Figure 5-3: RSVP Principles

Path Message

The Path message is sent by the sender to the receiver along the path of the data packets, and it is used for several tasks. First, it provides receivers with information about the characteristics of the sender traffic. Second, it is used to set up the path state at the routers along the path from the sender to the receiver. Path states are used by Resv messages for reverse path. Third, Path messages are used (optionally) to provide the characteristics of the path to receivers. The Path message contains, among other objects, the Sender Template, Sender TSpec, Previous Hop (PHOP), Session and the Adspec. The Sender Template identifies the sender of the flow. It contains the IP address of the sender and optionally the sender port (in the IPv6 the flow label may be used instead). The Sender TSpec describes the traffic characteristics of the flow that the sender will generate. It can be used for deciding how much of the resources should be reserved and as part of the input to the admission control system. The PHOP identifies the previous hop, which has sent this Path message, whereas the Session object identifies the destination of the flow. The

Adspec is an optional object that is used to advertise to receivers the characteristics of the end-to-end communications path, so that they can make appropriate reservation request in order to achieve their desired end-to-end QoS. The sending host, or the firs router in the path, originates the Adspec. Each RSVP router processes Path messages to create the path state for each sender. It also periodically scans the path states to create new Path messages and to forward them to the receivers.

Resv Message

Receivers initiate reservation by replying to Path messages with Resv messages The Resv messages are sent from the receiver to the sender along the reverse path of the Path messages hop-by-hop to request resources (e.g., bandwidth) from routers on the path. Resv messages are used by routers to create and maintain the reservation state. A Resv message contains, among other objects, the Flowspec and Filterspec, which are referred to together as a flow descriptor. The Flowspec object contains two sets of numeric parameters: a Traffic Specification (TSpec) and a Request Specification (RSpec). The TSpec describes the traffic characteristics of the data flow and it contains the specific values of the parameters that make up the traffic characteristics. The RSpec defines the desired QoS, and it contains the specific values of the parameters of the service being requested. The Filterspec object defines a subset of packets to receive the desired QoS defined in the RSpec. The FilterSpec serves for packet discrimination. Based either on the flow label (in an IPv6 packet) or the combination of source address and source port (in an IPv4 packet), a substream of packets is selected to which the service is applied.

RSVP Features

The RSVP protocol contains many features among which soft state, local repair, and merging are the most important. RSVP uses soft states to manage the reservation in routers and hosts. Soft state means that established path states and Resv states are timed out after certain time. Hence, soft states are periodically refreshed by Path and Resv messages. Local repair provides fast adaptation to routing changes. Merge functionality is used to merge reservation requests that share parts of the transmission path, resulting in efficient usage of bandwidth. Merging takes place at the outgoing interface of the RSVP router by merging Resv messages from different next hops that arrive at the same interface and that can be satisfied by a single reservation. Associated with each reservation made at a router's outgoing interface is a Filterspec and effective Flowspec, obtained from the merging process. The effective Flowspec is passed to the traffic control module within the router, which applies both admission control and policy control, to determine whether or not the reservation can be accepted. The amount of merging possible is determined by reservation style, which is carried within each Resv message. Reservation style determines how multiple requests are merged and which resource requests are forwarded to the upstream node. In addition, the reservation requests that are transmitted towards a common previous hop are also merged. The router calculates the Filterspec and Flowspec of Resv messages to be sent to the previous hops upstream by applying style-dependent merging of stored reservation state. Thus, the amount of signalling in forwarding reservation requests from all next hops to the previous hops is reduced. So far, three reservation styles are defined: Fixed Filter (FF), Wildcard Filter (WF), and Shared Explicit (SE).

- **Fixed Filter (FF) Style** - With FF style, only reservation requests that specify the same sender merge. Hence, the Filterspec of each FF reservation installed at an interface consists of a single sender only. The effective Flowspec of the reservation installed is the maximum of all FF reservation requests received on that interface for that particular sender. For each sender, the Flowspec of the FF Resv message forwarded to the previous hop is the maximum Flowspec of all reservations installed in the router for that sender.

- **Wildcard Filter (WF) Style** - This style is the opposite of the FF style. The Filterspec of each WF reservation installed at an interface is "wildcard" and matches any sender from upstream. The effective Flowspec installed is the maximum from all WF reservation requests received on that particular interface. The Flowspec of each WF Resv message forwarded to a previous hop upstream is the maximum Flowspec of all WF reservations installed in the router. Actually, all reservations for the same interface and all reservations towards the same previous hops are merged, respectively.

- **Shared Explicit (SE) Style** – This style is somewhat a combination of the two previously described styles. The Filterspec of each SE reservation installed at an interface contains a specific set of senders from upstream and is obtained by taking the union of the individual Filterspecs from each SE reservation request received on that interface. The effective Flowspec installed is the maximum from all SE reservation requests received on that particular interface. The Filterspec of an SE Resv message forwarded to a previous hop is the union of all senders whose previous hop is via that interface and who are contained in the Filterspec of at least one SE reservation in the router. The Flowspec of this SE Resv message is given by the maximum Flowspec of all SE reservations, whose Filterspecs contain at least one sender whose previous hop is via that interface.

It should be noted that the merging applies only to packets of the same Session and can only occur between messages with the same reservation style. Filter styles are mutually exclusive and a Session's filter style is determined by the first arriving RESV message. Shared reservation styles (WF and SE) are designed for conferencing applications in which it is unlikely that all senders transmit simultaneously. In audio conferencing, for example, only one or two people can typically speak at the same time. In these cases, the WF or SE reservation request for, perhaps twice the bandwidth of one sender should be sufficient to allow an amount of overbooking.

5.1.2 Differentiated Services

Differentiated Services (DiffServ or DS for short) is an alternative service-architecture to Integrated Services, for providing QoS on the Internet. The DiffServ architecture aims to be scalable and simple. Scalability is achieved by aggregating traffic flows into a relatively small number of traffic classes named forwarding classes, or behaviour aggregates. Simplicity is achieved by locating the sophisticated QoS handling mechanisms in border routers of the DS network, whereas core routers only forward traffic based on forwarding classes, rather than individual flows. Differentiated Services architecture is significantly different from Integrated Services architecture. The main difference is that Differentiated Services allocate resources to traffic aggregates by provisioning, whereas the Integrated Services architecture allocates resources to individual flows through reservation. Hence, the amount of state information in differentiated services is proportional to the number of classes, rather than the number of flows. This results in better scalability and easier implementation of the DiffServ, than IntServ architecture.

5.1.2.1 Basic Concepts of Differentiated Services

Differentiated services are based on several specific concepts, which will be explained in the following subsections.

Per-Hop-Behaviour

Per-Hop Behaviour (PHB) is defined as "the externally observable forwarding treatment applied at differentiated services nodes to a particular forwarding class or behaviour aggregate." The PHB is actually the means by which a node allocates resources to a forwarding class. It should be noted that DiffServs define forwarding treatments and not services. Services and forwarding treatments are not the same, but are closely related. However, different levels of services can be

created by allocating resources hop-by-hop to forwarding classes and controlling the amount of traffic for these classes. It is also important to stress that DiffServs provide resource assurance but not absolute bandwidth guarantees nor delay bounds for individual flows. There are currently two standard per-hop-behaviours: Expedited Forwarding (EF) and Assured Forwarding (AF), which will be presented later. For a particular PHB, a variety of implementation mechanisms may be used to achieve the same desired forwarding treatment.

Differentiated Services Codepoint

The DiffServ standard redefined the existing IP TOS (Type of Service) octet, shown in Figure 5-4, in the IPv4 header and the Traffic Class octet in the IPv6 header to indicate a forwarding treatment. The IP TOS octet consists of a 3-bit precedence field, a 3-bit type of service field, and two unused bits that must be zero. The precedence bits are used to indicate the priorities for traffic. The letters in type of service field indicate the following: D – delay, T – throughput, R – reliability. Applications can set these bits to value 1 to request low-delay, high throughput, or low-loss-rate service. Value 0 indicates normal values for delay, throughput, and reliability.

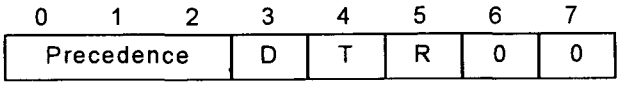


Figure 5-4: IPv4 TOS Field

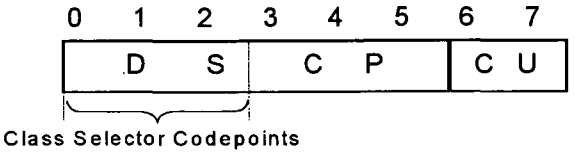


Figure 5-5: Differentiated Services Field

The redefined octet in DiffServ standard is called DS field. This field, as shown in Figure 5-5, is divided into two parts: a 6-bit portion called Differentiated Services Codepoint (DSCP) and a 2-bit currently unused portion. A specific value in the DSCP part is used to indicate the PHB. The relationship between the 6-bit DSCP value and PHBs implemented in a node is configurable. All packets with the same DSCP value are classified in a particular behaviour aggregate, and they receive the same forwarding treatment. A PHB is selected at a node by a mapping of the DS codepoint value in a received packet, as described in [RFC2474]. Standardized PHBs (AF and EF) have recommended codepoints. In order to maintain partial backward compatibility with known current use of the IP precedence field, a set of codepoints is specified, which are mapped to a standard set of minimum behaviours that are compatible with current common practice. This set of codepoints is reffered to as Class Selector Codepoints. (Note that the IP Precedence field is 3 bits). There are eight class selector codepoints supported by DS nodes. The basic PHB is called the default PHB, which is defined for backward compatibility with the current best-effort forwarding treatments or behaviour of IP. The default PHB indicates that, subject to resource constraints dictated by the network administration, packets are forwarded at every opportunity, when there are no service requests from other forwarding class. The codepoint, which selects the default PHB, is B'000000'. Other codepoints may be mapped to this PHB also, and an unrecognized codepoint may select this PHB as a default way of handling it. The default PHB is compatible with the way packets with that TOS byte value are treated today. The PHBs selected by the other seven codepoints must meet certain requirements.

Service Level Agreement

DiffServ is based on the existence of a Service Level Agreement (SLA), which is a service contract between a customer to receive differentiated services and its Internet service provider

(ISP). An SLA specifies the forwarding service a customer should receive and the amount of traffic allowed in each forwarding class. A service level agreement can be either static or dynamic. Static SLAs are negotiated on a monthly or yearly basis, whereas for dynamic SLAs, customers must use a signaling protocol to request services on demand. SLAs also exist between two adjacent DS network domains. An SLA may include traffic conditioning rules, which constitute a Traffic Conditioning Agreement (TCA) in its whole or in part. Traffic conditioning rules and TCA will be explained in the next sub-section.

Traffic classification and conditioning functions

The key components within a differentiated services boundary node are traffic classification and conditioning functions. These functions perform mapping of packets of the arrived traffic streams to one of the supported aggregate behaviors and must ensure that the traffic conforms to the SLA for the specific customer. Traffic classification and conditioning are implemented by several entities of the DS node, shown in the Figure 5-6. The first entity is a packet classifier, which selects packets in a traffic stream based on the content of some portion of the packet header according to defined rules. Diffserv defines two types of classifiers: the Behavior Aggregate (BA) and the Multi-Field (MF) classifiers. BA classifiers select packets based on the DS codepoint only. For a BA classifier, the DSCP is essentially an index into the Per-Hop Behavior table. This type of classifier is generally used when the DSCP has been set before the packet reaches classification. The advantage of BA classification is that it is simple (1 byte field) and there are only a limited number of states, which have to be maintained by the router or interface. The MF classifier selects packets based on the value of a combination of one or more header fields such as source address, destination address, DS field, protocol ID, source port, destination port numbers, and other information like incoming interface. One advantage of this type of classification is that packets from flows arriving on the same interface, but which are covered by separate SLAs, may be identified and distinguished. A disadvantage is that state information is potentially very large.

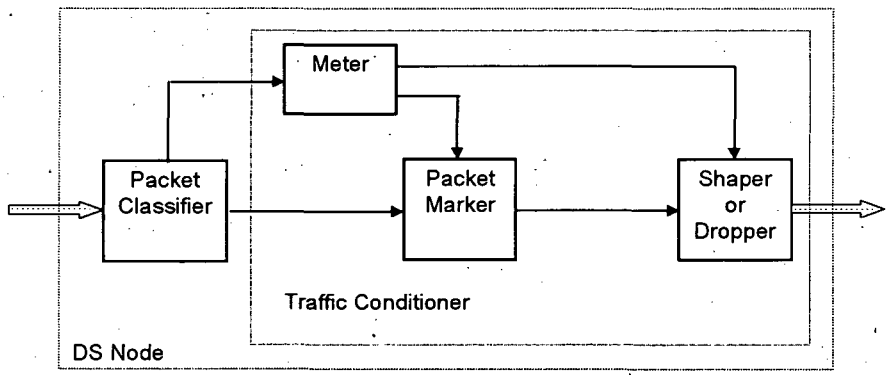


Figure 5-6: Nodal Architecture of Differentiated Services

A number of logical entities grouped together, as shown in Figure 5-6, constitute a traffic conditioner. A traffic conditioner, as its name implies, performs traffic conditioning functions and may contain meters, markers, droppers, and shapers. Traffic conditioning functions are performed to enforce rules specified in a Traffic Conditioning Agreement (TCA). A TCA specifies classifier rules and any corresponding traffic profiles, as well as metering, marking, discarding and shaping rules, which are to apply to the traffic streams selected by the classifier. A TCA encompasses all of the traffic conditioning rules explicitly specified within a SLA, along with all of the rules implicit in the relevant service requirements and/or in a DS domain's service provisioning policy. The service provisioning policy defines how traffic conditioners are configured on DS boundary nodes and how traffic streams are mapped to DS forwarding classes to achieve a range of services. Traffic conditioners are typically deployed in DS boundary nodes only. However, they can also exist in hosts and in interior DS nodes. In a particular node in a

DS network domain, a traffic conditioner may not contain all four elements, and sometimes none of them. The functions of each element of a traffic conditioner are as follows. The meter measures the traffic streams from the classifier and compares them with the customers' traffic profile specified in a TCA. A traffic profile specifies some of the properties of the flow, which is to receive a certain level of service. A meter passes state information to other conditioning functions to trigger a particular action for each packet. When packets are within the profile, they will be allowed to enter the network. If the customer sends more packets than allowed, actions will be taken to ensure that traffic flow is fully consistent with the traffic profile.

- A marker sets the DS field of a packet to a particular DSCP value, adding the marked packet to a particular DS forwarding class. The marker may be configured to mark all packets that are passed to a single codepoint, or it may be configured to mark a packet to one of a set of codepoints used to select a PHB, according to the state of a meter. The nonconformant packets may also be marked with a special DSCP. When the marker changes the codepoint in a packet, it is said to have re-marked the packet. Origin hosts can also mark DS fields of individual packets to indicate the desired service or have them marked by the access router based on MF classification.
- A sharper ensures that a particular traffic stream conforms exactly to the parameters given by a particular traffic profile. In order to bring the traffic stream into compliance with a traffic profile, shapers may delay some or all of the packets in a traffic stream.
- A dropper discards some or all of the packets in a traffic stream in accordance with the state of a corresponding meter enforcing a traffic profile, in order to bring the stream into compliance with a traffic profile. This process is known as policing the stream.

5.1.2.2 Assured Forwarding

Assured Forwarding (AF) is a Per-Hop Behaviour group standardized by IETF. The purpose of AF forwarding treatment is to enable service providers to offer different levels of forwarding assurances for IP packets received from a customer domain and possibly different delays and jitters. However, the last two quality metrics are not the primary focus of AF, as there are no timing requirement goals associated with the forwarding of AF packets. AF standard defines four forwarding classes and three-drop precedences within each forwarding class. Each forwarding class in each DS node is allocated a minimum amount of forwarding resources (buffers and bandwidth) and these resources must be configurable. Customers subscribe to the service built with AF forwarding class and their packets will be assigned into one or more of these AF classes, marked with appropriate AF DSCPs by the customer or the provider DS domain. A DS node must implement all four AF classes. Packets belonging to different AF classes must be forwarded independently of one another. A DS node must not aggregate AF classes together. Any DS node must accept all three-drop precedences. For the three levels of drop precedence, a node must implement at least two different levels of drop probability. If the DS node implements only two levels of drop probability, then the two higher drop precedence values are mapped into the precedence codepoint that yields the highest drop probability, and the lowest drop precedence value is mapped into the precedence codepoint that yields the lowest drop probability. Within an AF class, a DS must forward a packet in accordance with the drop precedence of the packet. Packets with lower drop precedence are forwarded with higher probability than packets with higher drop precedence. In general, a DS node may reorder packets of different AF classes but must not reorder packets of the same application flow (microflow) when they belong to the same AF class regardless of their drop precedence. Thus, the boundary nodes should avoid splitting traffic from the same application flow into different AF classes since it will lead to packet reordering within a microflow. The traffic conditioning applied to AF traffic entering a DS domain must not cause reordering of packets of the same microflow. The recommended codepoints for AF are given in Table 5-1. The first 3 bits of the DS field encode the AF class number (2, 3, 4, and 5), whereas last three bits encode the drop precedence (0, 2, and 4). The numerical ordering of the DS byte (AF class number) implies an ordering of the service delivered. Likewise, the ordering of the drop precedence implies an ordering of dropping prob-

ability. The higher-level service has the lowest dropping probability. For example, if codepoint(x) < codepoint(y), then class(y) has at least as many forwarding resources allocated to it as class(x). For drop precedence: if codepoint(p) < codepoint(q), then the dropping probability of packets within an AF class with drop precedence p must be at least as small as the dropping probability of packets marked with drop precedence q.

Table 5-1: DS Byte Codepoints for AF

	AF 1	AF 2	AF 3	AF
Low drop preference	b'010000'	b'011000'	b'100000'	b'101000'
Medium drop preference	b'010010'	b'011010'	b'100010'	b'101010'
High drop preference	b'010100'	b'011100'	b'100100'	b'101100'

In a DS node, the level of forwarding assurance that an IP packet receives depends on the amount of resources allocated to the AF class to which that packet belongs, the amount of traffic admitted into the AF class, and in case of congestion, the drop precedence of the packet. By combining these parameters, the AF PHB group could be used to construct different services. AF PHB can be used, for instance, to construct the so-called Olympic service, which consists of three service classes: bronze, silver, and gold. Packets are assigned to these three service classes such that packets belonging to the gold class experience lighter loads than the packets assigned to the silver class. The bronze, silver, and gold services would be mapped to the AF1, AF2, and AF3 forwarding classes, with different bandwidth allocation. Similarly, 3 drop precedences may be mapped to AF drop precedence levels 1, 2, or 3. Another possibility is to use AF PHB group to create simple services based on drop precedence, such as the Expected Bandwidth Service, as described in the RIO scheme [Cla98]. The AF standard also specifies certain properties for the implementation of the drop mechanism, including Random Early Discard (RED) [Cla98].

5.1.2.3 Expedited Forwarding (EF)

Expedited Forwarding (EF) is another standardized PHB in differentiated services architecture. The EF PHB is defined as "a forwarding treatment for a particular traffic aggregate where the departure rate of the aggregate's packets from any DS node must equal or exceed a configurable rate." The EF traffic should receive this rate independent of the intensity of any other traffic attempting to transit the node. The purpose of EF forwarding treatment is to build a low loss, low latency, low jitter, assured bandwidth, and end-to-end service through DS domains. This service is experienced by endpoints like a "virtual leased line" service and has also been described as premium service. Constructing such a service is carried out in the following two steps: First, nodes should be configured so that the aggregate has a defined minimum departure rate independent of the intensity of other traffic at the node. Second, the arrived aggregate traffic should be conditioned such that its arrival rate at any node is always less than that node's configured minimum departure rate. The EF PHB provides the first step, whereas the network boundary traffic conditioners provide the second step. The key idea of the DS PHB, in order to provide the service with the characteristics listed above, is that for the EF aggregate flow, the queues must be kept consistently low by adjusting arrival and departure aggregate rates properly. It is also implicitly assumed that the EF traffic can preempt other traffic within a certain limit. Codepoint 101110 is recommended for the EF PHB. A Diffserv boundary node can remark the EF PHB packets with a new DSCP only if the new DSCP satisfies the EF PHB requirements. Packets marked for EF PHBs must not be demoted or promoted to another PHB by a DS core node. Several types of queue scheduling mechanisms may be used to implement the EF forwarding treatment. A simple approach is a priority queue scheme. The queue for the EF traffic must be the highest priority queue in the system. However, a rate policer, such as a token bucket associated with each priority queue, should also limit the total amount of the EF traffic entering the DS node, so that other traffic will not starve. Another possibility for implementing EF is to use a variant of Waited Fair Queuing (WFQ) and configure the weights in such a way that the EF traffic has relative priority. It is also possible to use a single queue in a group of

queues serviced by a weighted round robin scheduler where the share of the output bandwidth assigned to the EF queue is equal to the configured rate. Another way to implement EF is by a Class Based Queuing (CBQ) scheduler that gives the EF queue priority up to the configured rate. All of these mechanisms can implement the basic EF PHB properties, but different implementation choices result in different properties of the same service, such as jitter as seen by individual microflows.

5.1.3 Multi-Protocol Label Switching

Multi-Protocol Label Switching (MPLS) is a method of forwarding packets at a high speed. It combines the key features of both Layer-2 and Layer-3 technologies. Many of the MPLS components are similar to traffic engineering and Quality-of-Service (QoS) techniques employed in ATM. Some other components of the MPLS are simply extensions of already existing technologies, such as the extensions added to existing routing protocols. An additional benefit to MPLS is that upgrades can be done easily, because the forwarding and control components are separate. The forwarding component is responsible for transporting a packet based on a routing table. The control component is responsible for the construction and maintenance of the routing table, as well as working with the control components of other nodes to exchange routing information. MPLS is protocol-independent, so it is applicable to any network layer protocol other than IP or directly over data-link layer. That is why it is called multi-protocol. Furthermore, MPLS is not application controlled and it resides only on routers. All of these components combined enable MPLS to function at a higher degree of performance and intelligence than current technologies. Label switching was initially driven by the need for seamless IP/ATM integration and to simplify IP forwarding. However, rapidly changing technologies have made these considerations less important. Instead, traffic engineering and QoS provisioning have emerged as the key applications and promoted MPLS as an important new technology for the Internet. Traffic engineering refers to the process of optimizing the utilization of network resources through balanced distribution of traffic across the network. Traffic-engineered networks can guarantee bandwidth for various flows, which is a necessary condition for QoS. In today's Internet, traffic engineering is difficult to achieve, as IP routing is destination based and has no possibility of adjusting traffic loads to available network resources. Therefore, traffic tends to distribute unevenly across the network, resulting in some links being heavily congested and others remaining lightly loaded. This results in a poor utilization of the rather expensive network resources. In the following subsections, the main concepts and elements of the MPLS will be explained, whereas in the Chapter 6, the use of the MPLS to provide QoS is presented.

5.1.3.1 MPLS Basic Concepts

Several concepts and MPLS network elements are inherited from well-known technologies, but there are also several specific concepts used in MPLS, which will be presented briefly.

Forwarding Equivalence Class (FEC)

Forwarding Equivalence Class (FEC) is a set of IP packets, which are forwarded over the same path, with the same forwarding treatment. When a packet enters the network, the ingress router assigns it to a particular FEC. For determining the assignment, the ingress router may use different information it has about the packet, even if that information is not carried in the network layer header. For example, the port on which a packet arrives can be used for FEC assignments. However, an FEC usually includes packets whose destination addresses match a particular IP network prefix or packets that belong to a particular application between a source and destination computer, or packets that go out on the same egress node. This flexibility in forming FECs is one of the important benefits that MPLS brings to routing. In general, the considerations that determine how a packet is assigned to an FEC can be very complicated, but they have no impact

on the routers that merely forward MPLS packets. FECs are usually created based on information learned through an IGP, such as OSPF.

Label

A label is a short, fixed length, locally significant identifier that is used to identify an FEC. The label is put on a particular packet and represents the Forwarding Equivalence Class to which that packet is assigned. A label provides the information needed to forward a packet. It does not encode any information from the packet header (like an IP address), but rather a numerical value agreed upon by two MPLS routers on how to identify an FEC and to signify a connection along a path. It can be viewed simply as an index in the forwarding table. Thus, the forwarding process becomes very straightforward: It involves a direct lookup to find the outgoing interface and the label for the next hop. MPLS allows more than one label to be encoded in a packet. This is referred to as a label stack, since the labels are organized in a "last-in, first-out" mode. As the packet traverses the network, only the label at the top of the label stack is processed. An unlabeled packet can be thought of as a packet whose label stack is empty.

Shim Header

MPLS label values are carried in an MPLS-specific Shim Header or in an L2 header such as an ATM header. A shim header is placed by the ingress router between layers 2 and 3 of the OSI model. It is shown in Figure 5-7. Although the shim header is neither a part of layer 2 nor layer 3, it provides a means to relate both layer-2 and layer-3 information. The Shim Header consists of 32 bits divided into four parts. Twenty bits are used to encode the label value. The next 3-bit field is reserved for experimental use. Currently, this field is being considered for QoS implementations to set drop priorities for packets like in Differentiated Services. The S bit is used to indicate if a label stack is present. If the label is at the bottom of the stack or if there is only one label present, the S bit will have a value of zero. The eight bits for Time-To-Live (TTL) are used to signify the number of MPLS nodes that a packet has traversed to reach its destination. The value is copied from the IP packet header and copied back to the IP packet header when the packet leaves the MPLS network.

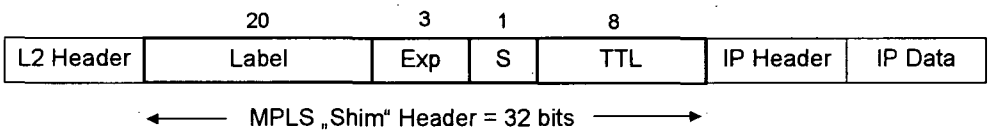


Figure 5-7: The MPLS Format and Shim Header

5.1.3.2 MPLS Network

An MPLS network, like other core networks, can be considered as built up by edge and core routers, as shown in Figure 5-8. Edge routers in MPLS terminology are called Label Edge Routers (LERs), whereas core routers are called Label Switch Routers (LSRs).

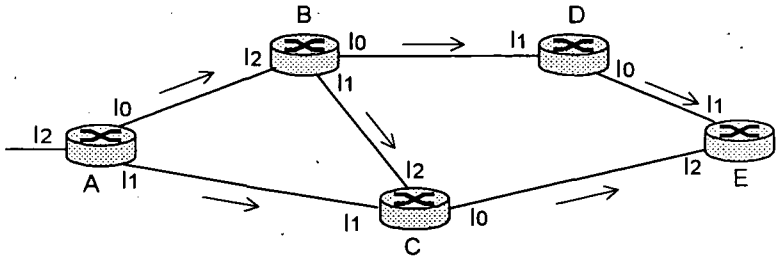


Figure 5-8: MPLS Network

When IP traffic enters the MPLS network, the ingress Label Edge Router analyses the network layer header of each packet and classifies packets into particular Forward Equivalence Classes (FEC). Based on the particular FEC to which a packet is assigned, the ingress LER adds a shim header (Label is a part of the shim header) to each packet and forwards packets to the next hop LSRs. To accomplish these functions, LER uses a forwarding table called FEC-to-NHLFE Map (FTN). The NHLFE (Next-Hop Label Forwarding Entry) is the entry to which the FEC points. Table 5-2 shows one example of the LER's FTN, referencing the Figure 5-8.

Table 5-2: FTN at Ingress LER A

Dstination / IP	Port Nr.	FEC	Label	Exit Interface	Instruction
128.131.88.1	80	F1	80	I0	Push
128.131.88.1	443	F2	17	I1	Push
128.131.88.1	25	F3	12	I0	Push

As one can see from Table 5-2, LER A classifies the incoming packets into three different Forwarding Equivalence Classes: F1, F2, and F3, based on the Destination IP address and Port number. Associated instruction is to Push labels. Packets belonging to FEC F1 and FEC F3 are labeled with labels 80 and 12, respectively, and forwarded to LSR B through interface I0. Packets assigned to class F2 are labeled with a label 17 and forwarded to LSR C, through interface I1. The label is used as an index into a forwarding table called the Label Information Base (LIB), which typically specifies mappings of incoming labels to outgoing labels and interfaces. The entry in the LIB that the incoming label points to is also called the Next-Hop Label Forwarding Entry, like in FTN table. Based on the LIB table, the LSR replaces the incoming label with the outgoing label and forwards the packet to the interface specified in the corresponding NHLFE. Table 5-3 and Table 5-4 show the LIB tables for LSR B and LSR C, referencing the Figure 5-8. Packets belonging to FEC F1 will arrive at Router B on interface I2 with a label of 80. They will be referenced against NHLFESs of the LIB for forwarding. Based on the LIB table, packets with a label value of 80 arriving on interface I2 will have the label swapped for a label with a value of 45 and will be switched out through interface I0. In this case, the instruction is to swap. Packets belonging to FEC F3 will arrive at Router B on interface I2, but with a label of 12, which will be changed to a value of 68 and the packet forwarded out interface I1. Packets assigned to FEC F2 will arrive at Router C on interface I1 with Label value of 17, which based on LIB of LSR C, will be changed to a value of 36 and then packets will be forwarded out to interface I0. In all cases, the instruction is to swap.

Table 5-3: Label Information Base of LSR B

Interface In	Label In	Label Out	Interface Out	FEC	Instruction
I2	80	45	I0	F1	Swap
I2	12	68	I1	F3	Swap

Table 5-4: Label Information Base of LSR C

Interface In	Label In	Label Out	Interface Out	FEC	Instruction
I1	17	36	I0	F2	Swap
I2	68	92	I0	F3	Swap

It is important to note that the labels and MPLS forwarding tables are router specific. In the described example, all three Tables are consistent and should be analyzed together. At the egress of the network, the egress LER removes the shim header and forwards the packet to an IP network. The most important feature of the described MPLS forwarding technique is that analysis of the IP packet header needs to be done only by ingress LER when a packet enters the MPLS network. Once a packet has been assigned to an FEC, forwarding of the packet is based only on the swapping of the labels. This simple technique results in fast and efficient packet forwarding.

This is in contrast to the hop-by-hop used in traditional routing. Furthermore, having classified traffic, ingress LERs can place only the highest priority traffic on the most expensive paths, while allowing the routine traffic to take other paths.

5.1.3.3 Label Switched Path and Label Distribution

The Label Switched Path (LSP) is the path through one or more routers that packets, assigned to a particular FEC, traverse through an MPLS network to reach their destinations. Each LSP is unidirectional, and therefore, return traffic must use a separate LSP. In general, label-switched path setup can be control-driven or data-driven. In a data-driven mode, the LSP set up is triggered by the presence of a specific flow, which causes the LSPs setup on demand while the data packets are arriving. In a control-driven mode, the LSP setup is triggered by control traffic, such as explicit signaling request, to establish a LSP or routing updates. The MPLS standards use the control-driven mode. The LSPs set up by label distribution protocols before forwarding packets. A label distribution protocol is a set of procedures by which two LSRs inform each other of the label/FEC bindings they have made and learn each other's MPLS capabilities. Specific label distribution protocols will be discussed later. In MPLS, a pair of LSRs, which use a label distribution protocol to exchange label/FEC-binding information, are known as "label distribution peers" with respect to the binding information they exchange. If A and B are "label distribution peers", they may agree that when A transmits a packet to B, A will label the packet with an arbitrary label value L if and only if the packet is a member of a particular FEC F. This means they agree to a binding between label L and FEC F for packets moving from A to B. As result of such an agreement, L becomes an outgoing label for LSR A representing FEC F, and L becomes an incoming label for LSR B representing the same FEC F. The decision to bind a particular label L to a particular FEC F is always made by the downstream LSR with respect to the flow of the traffic. The downstream LSR then informs the upstream LSR of the binding. Thus label bindings are distributed in the "downstream to upstream" direction, opposite to the data flow direction. Furthermore, the downstream LSR B must make sure that the binding from label to FEC is one-to-one. That is, an LSR B may bind label L1 to FEC F and distribute that binding to the upstream label distribution peer LSR A. LSR B may also bind label L2 to FEC F, and distribute that binding to another upstream label distribution peer LSR C. Binding of the same label L to two different FECs can be performed only under specific conditions [RFC 3031]. Therefore it is better to avoid it. There are two different methods of triggering label distribution: down-stream unsolicited and down-stream on demand. With the down-stream unsolicited label distribution method, an LSR distributes bindings to its neighbor LSRs that have not explicitly requested them. On the other hand, the downstream-on-demand method allows an LSR to explicitly request, a label binding for particular FEC from its next hop. Both of these label distribution methods may be used in the same network at the same time. However, the upstream LSR and the downstream LSR must agree on which technique to use. Furthermore, the set up of the LSPs can be done in one of two ways: Independent LSP control or Ordered LSP control. In Independent LSP control, each LSR makes an independent decision to bind a label to a particular FEC and to distribute that binding to its label distribution peers. In Ordered LSP control, an LSR only binds a label to a particular FEC if it has already received a label binding for that FEC from its next hop for that FEC or if it is the egress LSR for that FEC. If neither of these conditions is satisfied, the LSR must wait until a label from the downstream LSR is received before binding the FEC and passing corresponding labels to upstream LSRs. Either the ingress or the egress router is responsible for initiating the LSP setup (distributing labels). Ordered control and Independent control are fully interoperable. Since the two methods interwork, a given LSR need support of one or the other. Generally, the choice of Independent versus Ordered control does not appear to have any effect on the label distribution mechanisms, which need to be defined. Ordered control has the advantages of better traffic engineering and tighter network control, but its disadvantages are that convergence time is slower and the label controller (typically egress router) is the single point of failure.

5.1.3.4 Route Selection

Route selection refers to the method used by an LSR to determine the next hop for the LSP that it tries to establish. MPLS supports two route selection methods: hop-by-hop routing, and explicit routing. Hop-by-hop routing allows each node to independently choose the next hop to set up an LSP. This method is based on IP routing information, and it is the usual method used today in existing IP networks. In explicit routing, a single LSR, generally the ingress or the egress of the LSP, specifies the LSRs in the LSP. There are two modes of the explicit routing: "strictly" explicit routing (when a single LSR specifies the entire LSP) and "loosely" explicit routing (when a single LSR specifies only some of the LSP). The sequence of LSRs followed by an explicitly routed LSP may be chosen by configuration or may be selected dynamically by a single node that initiates explicit routing. Hence, explicitly routed LSPs provide the possibility of overriding the routes established by IP routing. This may be done as a matter of policy or to support traffic engineering to route traffic around congested links and optimize resource utilization across the network, for example. In conventional forwarding, this requires the packet to carry an encoding of its route (source routing) along with it,. Instead, in MPLS, a label can be used to represent the explicit route, so that the identity of the explicit route need not be carried with the packet. In general, routing algorithms designed to achieve certain specified objectives, are used to compute routes for the LSPs. Such routing algorithms are often referred to as constraint-based routing.

5.1.3.5 Label Distribution Protocols

Label distributions protocols are essentially the signalling protocols used to build and maintain the label-switching table at each LSR in an MPLS network. A number of different label distribution protocols are being standardized. For example, a new protocol has been defined for the explicit purpose of distributing labels, named LDP (Label Distribution Protocol). In addition to LDP, some existing routing protocols, such as Border Gateway Protocol (BGP), have been modified to carry information for labels along with routing information. The LDP and BGP protocols establish the Label Switch Path (LSPs) but do not support traffic engineering and meet QoS needs of applications, as traffic could be routed to "hot" traffic spots, causing congestion. To overcome this problem, MPLS signalling protocols were established to create explicit LSPs to enable better traffic engineering and support QoS applications. The two best-known protocols to support such functions are Constraint Route Label Distribution Protocol (CR-LDP) and Resource Reservation Setup Protocol-Traffic Engineering (RSVP-TE). In addition, the Open Shortest Path First (OSPF) routing protocol has undergone modifications to handle traffic engineering (OSPF-TE), but it is not currently widely used.

In the following, a short description of the LDP, CR-LDP, and RSVP-TE protocols will be given.

Label Distribution Protocol

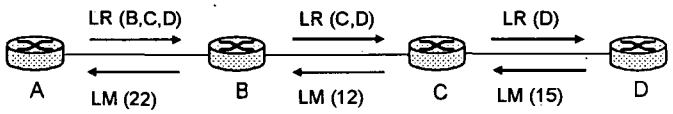
The Label Distribution Protocol (LDP) Specification Internet Draft [And01] defines LDB as "the set of procedures and messages by which LSRs establish LSPs through a network by mapping network-layer routing information directly to data-link layer switched paths." The MPLS workgroup standardized the Label Distribution Protocol (LDP), which was the first protocol specifically designed for label distribution. Standardized LDP is based on hop-by-hop routing. LDB supports both downstream unsolicited and downstream on demand label distribution. Also, LSPs can be set up either independently or in order from egress LSR to ingress LSR along the path. Another important feature of LDB is that when labels are bounded, they stay bounded until there is a command to tear down the LSP. An LSR exchanges the following messages with its peer:

- Discovery message to announce and maintain its presence in MPLS network.

- Session messages for establishing, maintaining, or ending sessions to its peer.
- Advertisement messages for creating, modifying, or deleting label bindings to FECs.
- Notification messages for distributing advisory information and error information.

Constraint-Based Routing Label Distribution Protocol

The Constraint-Based Routing Label Distribution Protocol (CR-LDP) is an extension of the LDP for carrying explicit routes and resource reservations to support traffic engineering. CR-LDP allows resources to be reserved for explicit routes (point-to-point LSP) by defining the adequate traffic and service parameters to characterize the LSP. In CR-LDP, the explicit route is also referred to as a constraint-based route, or CR-LSP. CR-LDP creates explicit routes, using both strictly and loosely explicit routing, providing maximum flexibility in building a specific path through a network. An ingress router initiates the setup of an explicit LSP by sending a Label request message specifying the list of nodes along the explicit route. An LSP ID, a unique identifier within an MPLS network, identifies each CR-LSP. An LSP ID is composed of the ingress LSR Router ID and a locally unique CR-LSP ID to that LSR. Figure 5-9 shows an example of a downstream allocation of labels in setting up an explicit route with CR-LDP. The ingress router, LER A, initiates the setup of LSP from LER A to LER D. LER A indicates that the LSP should follow an explicit route starting from LSR B. It then sends a Label Request message to LSR B with an explicit route (B, C, D). Having received this message, LSR B modifies the explicit route and forwards it to LSR C with an explicit route (C, D). LSR C receives this message and after modifying the explicit route to D, forwards it to egress LER D. Having received the Label Request message from LSR C, LSR D determines that it is the egress of the LSP. It sends a Label Mapping message back to LSR C with allocated label 15 for the LSP. LSR C uses the LSP ID in the Label Mapping message to match the original Label Request message. It then sends a Label Mapping message to LSR B with label 12. LSR C also updates the ILM table with the incoming label 12 pointing to outgoing label 15. Having received the Label Mapping message from LSR C, LSR B performs similar procedures to LSR C. It sends a Label Mapping message to LER A with label 22 and also updates the ILM table with incoming label 15 and outgoing label 22.



A, B, C, D – Label Switch Routers
LR Label Request
LM Label Map

Figure 5-9:CR-LDP Example

RSVP-TE

RSVP-TE or Extensions to RSVP for LSP Tunnels is another method of establishing an explicit LSP that meets QoS requirements in MPLS. As its name implies, RSVP-TE is an extension of the RSVP to perform label distribution and support explicit routing. Figure 5-10 shows an example of the allocation of labels in creating an explicit LSP with RSVP_TE. The ingress router LER A first creates a Path message and adds to it a LABEL_REQUEST Object (LRO), which indicates that a label binding for this path is requested. In addition, LSR A needs to specify the route in an EXPLICIT_ROUTE Object (ERO) and to add it to the Path message. LER A may also add other objects to the Path message. For example, a RECORD_ROUTE Object (RRO) may be used to request notification from the network about changes in the actual router or to detect loops in the route.

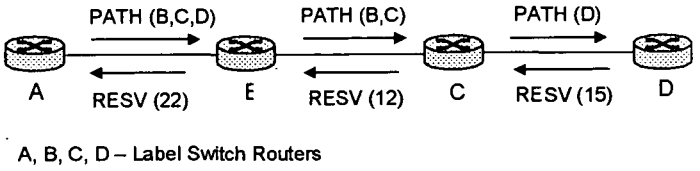


Figure 5-10: RSVP-TE Example

Once the Path message is constructed, LER A sends it to the next hop as indicated by the ERO. If no ERO is present, then the hop-by-hop routing provides the next hop. Having received the Path message, intermediate node LSR B modifies the ERO and forwards it to the next hop LSR C. The LSR C also modifies the ERO and sends it to the next hop, which is the egress router LER D. LER D allocates a new label, includes it in a LABEL Object (LO), and inserts it into the Resv message. LER D then sends the Resv message back to the sender, according to the RSVP protocol rules (following the path state created by the Path message, in reverse order). When the intermediate node LSR C receives a Resv message, it retrieves the label in the LO and uses it as the outgoing label for the LSP. It also allocates a new label and places that label in the corresponding LO of the Resv message, which it sends upstream to the previous hop. LSR C then updates the label-switching table with this new pair of labels. The previous hop router is LSR B, which performs the same functions as LSR C, of course using a new label, and forwards the Resv message to the ingress node LER A. When the Resv message arrives at the ingress node LER A, an LSP is established. A Resv message also includes RECORD_ROUTE Object (RRO).

5.2 Quality-of-Service in UMTS

The 3GPP has specified mechanisms for QoS support of the services offered by UMTS to the users. In general, the services are considered end-to-end (from TE to another TE), and each service has its specific QoS requirements. Hence, QoS requirements have to be provided everywhere in the network, that is end-to-end and for all services that need QoS support. The various parts of the network contribute to fulfilling the QoS requirements of the services in different way. The 3GPP specifications define the QoS architecture and QoS classes only for UMTS networks. Thus, in the following subsections, an overview of both QoS architecture and QoS classes for UMTS will be presented.

5.2.1 UMTS QoS Architecture

QoS support in UMTS matters only for packet switched domain, as the circuit switched systems generally have built-in QoS support. In UMTS, the end-to-end QoS for the packet domain is provided through Bearer Services (BS), which has to be established between UMTS modules from the source to the destination of a service. Bearer services can be defined as mechanisms that offer a set of services, which provide the capability for information transfer between the end- points of the bearer. Since the UMTS network architecture contains many system levels with their own QoS properties, the QoS is handled on many different levels, taking into account the special characteristics related to each particular level. Hence, UMTS standards propose a layered architecture of bearer services, as shown in Figure 5-11.

Each bearer service specifies all aspects to enable the provision of a negotiated QoS. These aspects are, among others, the control signalling, user plane transport, and QoS management functionality. According to the well-known rule of layered architectures, a bearer service on a specific layer offers its individual services, using services provided by the layers below.

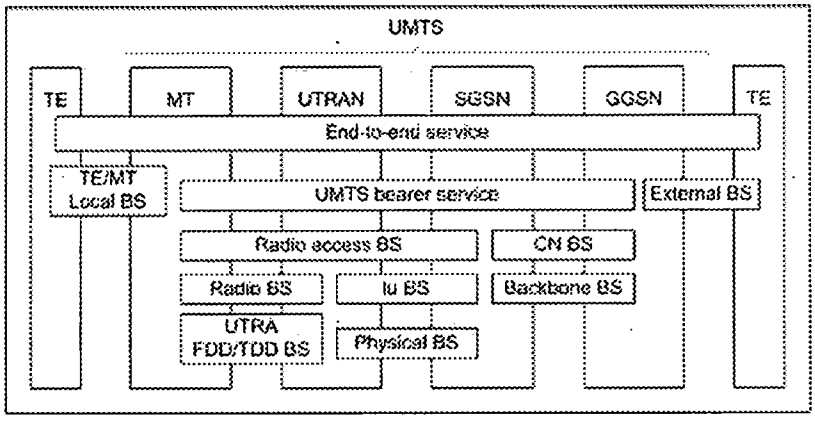


Figure 5-11:UMTS QoS/Bearer Architecture

5.2.1.1 The End-to-End Service

Following the layered architecture shown in Figure 5-11, the end-to-end service sets the QoS requirements. These requirements will then be mapped to the next level, which in turn performs QoS mapping for the next level and, so on. As a result, the UMTS network forms a connection through itself, fulfilling the original QoS requirements. However, the end-to-end service may be conveyed over several networks, not only UMTS. This means that on its way from one TE to another, the traffic must pass different bearer services of one or more networks. Actually, the end-to-end service used by the TE will be realized using a TE/MT local bearer service, a UMTS bearer service, and an external bearer service. The chosen TE/MT local bearer service contains the mechanisms (QoS-capable application-programming interface- API) to handle QoS between TE and MT. This bearer service is outside the scope of the UMTS network and will not be discussed further at this point. UMTS bearer service contains mechanisms to allocate QoS inside a UMTS network from MT to CN. It is actually the UMTS bearer service that provides the UMTS QoS, which is specified by the 3GPP, and it will be discussed shortly in the next subsection. Since the UMTS network attaches itself to external networks, the end-user QoS requirements from the other networks must be met, too. Particularly UMTS QoS mechanisms must interact with QoS mechanisms used in the Internet. This is taken care of by the external bearer service. The external BS deals with the interoperability and interworking aspects with external IP bearers, for example, and provides the appropriate functionality to support it. It is logically situated in the GGSN, which is the gateway of UMTS to external networks. The QoS mechanisms outside the UMTS network are not in the scope of 3GPP specifications.

5.2.1.2 UMTS Bearer Service

The UMTS QoS model is effective only within the UMTS bearer service and is designed to be independent of external QoS mechanisms. Within the UMTS network, the QoS handling is different between UTRAN and CN, since these are two different environments requiring their own mechanisms and protocols. Therefore, the UMTS bearer service consists of two parts: the Radio Access Bearer (RAB) service and the Core Network Bearer service. In a wireless network, the bottleneck is likely close to a radio network. Thus, the QoS must first overcome problems of this part of the network. This is handled by RAB service, which is responsible for the confidential transport of signaling and user data between MT and SGSN with the QoS adequate to the negotiated UMTS bearer service. RAB experiences more changes as a function of time and UE's movement, and this sets different challenges for QoS. Hence, the RAB is based on the characteristics of the radio interface and is maintained for a moving MT. The radio access bearer service is realized by a radio bearer service and an Iu-bearer service. The role of the radio bearer service is to cover all of the aspects of the radio interface transport. This bearer service

uses the UTRA FDD/TDD. The Iu-Bearer Service, together with the physical bearer service, provides the transport between UTRAN and CN. Iu-Bearer services for packet traffic shall support different physical bearer services for a variety of QoS. Within the UMTS packet core network, the core network bearer service connects the UMTS SGSN with the GGSN. The role of this service is to efficiently control and utilize the backbone network, in order to provide the negotiated UMTS bearer service. The UMTS packet core network shall support different backbone bearer services for a variety of QoS. The core-network bearer service uses a generic backbone network service. The backbone network service covers the Layer1/Layer2 functionality and is selected according to operator's choice in order to fulfill the QoS requirements of the core network bearer service. In order to have actual end-to-end QoS support, mapping is needed to ensure QoS interworking between existing defined schemes and the UMTS QoS model. Fortunately, mapping is needed only on boundary elements, like MT and GGSN. Hence, the RAN and CN's other components do not have to understand external QoS mechanisms and consequently, do not have to be upgraded frequently. Specifically, on the uplink the MT should be able to represent the external QoS requirements in a form suitable to the UMTS QoS model, while GGSN translates internal UMTS QoS parameters to the external network. MT and GGSN mapping roles are reversed on the downlink.

QoS Management Functions in the Network

The QoS management aspect of a bearer service is responsible for establishing, modifying and maintaining a UMTS bearer service with a specific QoS. The QoS management functions allocated to the UMTS entities indicate the requirement for the specific entity to enforce the QoS commitments negotiated for the UMTS bearer service. Furthermore, the QoS management functions of all UMTS entities together have to ensure the provision of the negotiated service between the end points of the UMTS bearer service.

5.2.2 UMTS QoS Classes and Service Attributes

3GPP specifications concerning QoS in UMTS define the following four QoS classes: Conversational, Streaming, Interactive, and Background. The main distinguishing factor among the UMTS QoS classes is length of transfer delay.

5.2.2.1 Conversational Class

Conversational class is characterized by low transfer delay, low jitter, and low error tolerance. It preserves time relation between information entities of the traffic stream, and it does not involve buffering. Traffic is generally symmetrical and has a guaranteed bit rate from the network. This class is meant for real-time traffic, which is highly delay-sensitive. A typical conversational application is voice or telephony speech. In addition to voice, Internet and multimedia have brought a number of new applications, which require conversational class, like voice over IP and video conferencing, for example. Video conferencing has similar delay requirements for voice, but it is less error-tolerant and generally requires relatively higher data rates than voice. Conversational class is the only QoS class in which the required QoS characteristics (low delay and preserve time relation) for conversational applications are strictly given by human perception. Therefore, the limit on acceptable transfer delay is very strict, as failure to provide low enough transfer delay will result in unacceptable quality. It is important to note that even if the user has a QoS conversational class in use at the UMTS bearer service level, on the end-to-end service level the user may still experience low quality problems if the external bearer service and the other end of the connection are not able to guarantee QoS. For example, the UE capabilities form a QoS profile, which may limit the UMTS bearer service that can be provided.

5.2.2.2 Streaming Class

Streaming class is characterized by a high tolerance for delay jitter, no requirements on low transfer delay, and low error tolerance. However, the delay variation of the end-to-end flow must be limited to preserve the needed time relation between information entities within a flow. In addition, the receiving application in the user equipment is allowed to buffer data for time alignment so that it can be played to the user in a synchronized manner. Hence, the highest acceptable delay variation over the transmission media is given by the capability of the time alignment function of the application. Acceptable delay variation is thus much greater than the delay variation given by the limits on human perception. Actually, streaming class service is asymmetric (one-way service) in nature using low to high bit rates, with guaranteed bit rate from the network. Typical applications are streaming audio and video, like video and music downloaded from the network, for example.

5.2.2.3 Interactive Class

Interactive class is characterized by low tolerance for errors but with a larger tolerance for delays than conversational class. Jitter is not a major impediment to interactive class applications, provided that the overall delay does not become excessive. Interactive class may require low or high data rates from the network, depending on the application in question, but it has no guaranteed bit rate. The data rate is significant only in one direction at a time. Traffic is generally asymmetric, and its buffering is allowed at the receiving application. Interactive class is meant for end-to-end services, which typically consist of a request response pattern of the end-user and that are not sensitive to delays. The user sends a request, whereas the network responds when there are free resources for responding. Responsiveness is ensured by separating interactive and background applications and by assigning higher priority to interactive applications than to background ones in terms of resource allocation. At the message destination, there is an entity expecting the message within a certain time interval. Therefore, one of the key attributes is round trip delay time. In addition to the request response pattern, another fundamental QoS characteristic is that the content of the payload must be preserved with a very low bit error rate. This is achieved by means of channel coding and retransmission. Typical interactive applications are: Web browsing, Telnet, FTP, data base retrieval, server access, message chatting, interactive email, and gaming.

5.2.2.4 Background Class

Background class is the most delay insensitive QoS class in UMTS. Background applications require error-free delivery but have no guaranteed bit rate from the network. Traffic is asymmetrical and the receiving application is allowed to buffer data. Furthermore, background class traffic has lower priority in scheduling than interactive class traffic, so background applications use transmission resources only when interactive applications do not need them. This is a very important issue in the wireless environment where the bandwidth is low compared to fixed networks. The fundamental QoS characteristics for traffic in the background class are that the destination is not expecting the data within a certain time and payload content must be preserved. The background class is mainly intended for background delivery of E-mails, background file downloading, SMS, and reception of measurement/performance records traffic.

5.2.2.5 Service Attributes

Ongoing work within 3GPP defines the QoS service attributes that characterize the classes at the UMTS bearer service, RAB service as well as at the other bearers. The following tables, Table 5-5 and Table 5-6, list the defined UMTS bearer service and RAB service attributes and their value ranges for all four QoS classes, respectively. This information originates from the 3GPP standardization documents TS 23.107 and TS 23.207. UMTS bearer service attributes describe the service provided by the UMTS network to the user of the UMTS bearer service and

their values reflect the capability of the UMTS network. RAB service attributes values reflect the capability of UTRAN.

Table 5-5: UMTS Bearer Service Attributes

Traffic class	Conversational class	Streaming class	Interactive class	Background class
Maximum bit rate [kbit/s]	< 2000	< 2000	< 2048 – over-head	< 2048 – over-head
Delivery order	Yes/No	Yes/No	Yes/No	Yes/No
Maximum SDU size [octets]	< 1500	< 1500	< 1500	< 1500
Delivery of erroneous SDUs	Yes/No	Yes/No	Yes/No	Yes/No
Residual BER	$5*10^{-2}$,10^{-2},10^{-3}, 10^{-4}	$5*10^{-2}$,10^{-2},10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$4*10^{-3}$,10^{-5},$6*10^{-5}$	$4*10^{-3}$,10^{-5},$6*10^{-5}$
SDU error ratio	10^{-2},10^{-3},10^{-2}, 10^{-5}	10^{-2},10^{-3},10^{-4}, 10^{-5}	10^{-3},10^{-4},10^{-5}	10^{-3},10^{-4},10^{-5}
Transfer delay [ms]	100 - maximum value	500 - maximum value		
Guaranteed bit rate [kbit/s]	< 2000	< 2000		
Traffic handling priority			1,2,3	
Allocation/Retention priority	1,2,3	1,2,3	1,2,3	1,2,3

Table 5-6: Radio Access Bearer Service Attributes

Traffic class	Conversational class	Streaming class	Interactive class	Background class
Maximum bit rate [kbit/s]	< 2000	< 2000	< 2000 – overhead	< 2000 – over-head
Delivery order	Yes/No	Yes/No	Yes/No	Yes/No
Maximum SDU size [octets]	< 1500	< 1500	< 1500	< 1500
Delivery of erroneous SDUs	Yes/No	Yes/No	Yes/No	Yes/No
Residual BER	$5*10^{-2}$,10^{-2},10^{-3}, 10^{-4}	$5*10^{-2}$,10^{-2},10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$4*10^{-3}$,10^{-5}, $6*10^{-8}$	$4*10^{-3}$,10^{-5}, $6*10^{-3}$
SDU error ratio	10^{-2},10^{-3},10^{-2}, 10^{-8}	10^{-2},10^{-3},10^{-4}, 10^{-5}	10^{-3},10^{-4},10^{-5}	10^{-3},10^{-4}, 10^{-5}
Transfer delay [ms]	80 - maximum value	500 - maximum value		
Guaranteed bit rate [kbit/s]	< 2000	< 2000		
Traffic handling prior-ity			1,2,3	1,2,3
Allocation/Retention priority	1,2,3	1,2,3	1,2,3	1,2,3

5.3 Quality-of-Service in WLAN IEEE 802.11

IEEE 802.11 WLAN was originally designed for best-effort services. However, the demands of WLAN customers for real-time applications such as video, audio, voice over IP, and other multimedia applications, are increasing. Those applications require Quality-of-Service (QoS) support in terms of guaranteed bandwidth, delay, jitter, and error rate. Guaranteeing those QoS requirements in IEEE 802.11 WLAN is a very challenging issue, first-of-all, due to physical (PHY) layer characteristics. Wireless links have high error rate, which is more than three orders of magnitude larger than that of wired LAN (802.3), causing bursts of frame loss, packet reordering, large packet delay and jitter. To handle QoS traffic in a manner comparable to other IEEE 802 LANs, despite the enormous differences in characteristics of the underlying media, the IEEE 802.11 QoS facility incorporates functionality that is not traditional for MAC sublayers. The DCF media access mechanism of IEEE 802.11, discussed in Chapter 3 does not support QoS, whereas PCF access method has serious limitations. Therefore, to support applications with QoS requirements over IEEE 802.11 WLAN, the IEEE 802.11 Task Group E is currently working on IEEE 802.11 standard supplement called IEEE 802.11e. The main concern the Group E has is the enhancement of the original 802.11 MAC for QoS provision. The IEEE 802.11e aims to enhance the ability of all of the physical layers IEEE 802.11b, IEEE 802.11a, and IEEE 802.11g to deliver real-time multimedia in addition to data packets.

In the following subsections, the basic concepts and media access methods for supporting QoS in WLANs will be presented.

5.3.1 IEEE 802.11e Basic Concepts

In order to support QoS in 802.11 WLAN, the IEEE 802.11e standard has defined a new function called HCF (Hybrid Coordination Function). The HCF combines contention-based and controlled-based access methods in a single medium access protocol and enhances them with QoS mechanisms and frame subtypes. The HCF contention-based medium access method is usually recognized as EDCF (Enhanced Distributed Coordination Function). Note that EDCF is part of the HCF and is not a separate coordination function. As the rules of operation for channel access are similar to that of DCF, the term EDCF is used. The HCF controlled channel access mechanism is based on polling and operates concurrently with EDCF. The HCF is a mandatory function and shall be implemented in all QoS Stations (QSTAs), but it also supports best-effort STAs. In IEEE 802.11e, QSTA indicates an enhanced station (STA) that operates under IEEE 802.11e. All STAs and QSTAs inherently obey the medium access rules of the HCF, because these rules are based on the DCF. Thus, HCF is upwardly compatible with the DCF and may optionally contain the PCF(Point Coordination Function). The HCF implementation requires a centralized controller called Hybrid Coordinator (HC) in each QBSS (QoS Basic Service Set). Hybrid Coordinator is a type of PC (Point Coordinator) but operates under rules that are different from the PC of the PCF, although it may optionally implement the functionality of a PC when HCF contains PCF. An HC will typically reside within an 802.11e AP (Access Point), also denoted QAP (QoS Access Point). Hybrid Coordinator implements the frame exchange sequences and MSDU handling rules defined by the HCF. The HC also performs bandwidth management including the allocation of Transmission Opportunities (TXOPs) to QSTAs. A QBSS is a BSS that supports LAN applications with Quality-of-Service (QoS) requirements, while Transmission Opportunities (TXOP) are intervals of time in which a particular QSTA has the right to initiate transmissions onto the wireless medium. The TXOP is defined by a starting time and a maximum duration. If an HC is operating in a QBSS, the access time is organized into superframes with a contention free period (CFP) and a contention period (CP), which alternate over time continuously, similar to the PCF medium access mechanism. The EDCF is used in the CP only, while the HCF controlled channel access emchanism is used in both CP and CFP intervals. During the CP, each TXOP begins either when the medium is determined to be available under the EDCF rules (EDCF-TXOP), or when the QSTA receives a special polling

frame (polled-TXOP) from the HC. The duration of an EDCF-TXOP is limited by a QBSS-wide TXOP limit distributed in beacon frames, while the duration of a polled-TXOP is specified in the frame header of a special QoS (+)CF-Poll frame. During the CFP interval, the starting time and duration of TXOP is also specified by the HC, again using QoS CF-Poll frame. The MAC entity at each QSTA makes local decisions regarding which MPDUs (MAC Protocol Data Units) can be transmitted during each TXOP interval.

5.3.1.1 Enhanced DCF

Enhanced DCF (EDCF) is the contention-based medium access method for the IEE 802.11e standard. The aim of the EDCF is to enhance current DCF access mechanisms of IEEE 802.11 to support service differentiation. The QoS support is realized with the introduction of traffic categories (TCs), priorities at QSTAs, and Access Categories (AC). In order to support different TCs, up to eight priorities are defined at each QSTA. AC are media access mechanisms that provide support for those different priorities at the stations. Each QSTA has four ACs, thus one or more stations' priorities are assigned or mapped to one adequate AC. A QSTA accesses the medium based on the AC of the frame that is to be transmitted. At the HC, there is only one access mechanism and consequently only one access category even though there might be multiple queues. Each AC is an enhanced variant of the DCF. It contends for TXOPs using two ECDF channel access parameters: Contention Window (CW) and Arbitration Interframe Space (AIFS). Different priorities are provisioned by assigning different values of these parameters to different access categories. Assigning a short CW to a high priority AC ensures that in most cases, high-priority AC is able to transmit ahead of a low-priority one. This is done by setting the contention window limits CWmin[AC] and CWmax[AC], from which the contention window CW[AC] is computed, to different values for different ACs. For further differentiation, different ACs use different IFSs (Inter Frame Spaces). Instead of using a DIFS, a new kind of interframe space called Arbitration Interframe Space (AIFS) is used in EDCF. The AIFS is a DIFS and can be enlarged individually for each AC. Smaller AIFS are assigned to higher priority ACs. Priority over DCF stations is provided by setting CWmin[TC] < 15 (in case of 802.11a PHY) and AIFS = DIFS. An illustration of the EDCF timing relationship is shown in Figure 5-12. In EDCF, the access procedure is similar to DCF. If the medium is sensed to be idle, a transmission can begin immediately. Otherwise, the QSTAs defer until the end of current transmission on the wireless medium. After deferral, the QSTA waits for a period of AIFS(AC) and then starts the backoff procedure. The backoff interval here is calculated by using a random number drawn from the interval [1, CW(AC) +1]. Each backoff timer sets its counter to this random number. After any unsuccessful transmission attempt, a new CW is calculated with the help of another ECDF parameter, the persistence factor PF[AC], and another uniformly distributed backoff time calculated out of this new enlarged CW to reduce the probability of a new collision. Whereas in legacy IEEE 802.11 CW is always doubled after any unsuccessful transmission (equivalent to PF = 2), IEEE 802.11e uses the PF to increase the CW different for each TC:

$$newCW\,[AC] >= ((oldCW[AC]+1)*PF)-1$$

Each Access Category (AC) within the station behaves like a virtual station. It contends to access the medium and starts its backoff time independently after sensing the medium idle for at least AIFS. If the backoff counters of two or more parallel ACs in one station reach zero at the same time, a scheduler inside the station avoids the virtual collision by granting the TXOP to the highest priority Access Category (AC), while the lowest priority colliding ACs behave as if there is an external collision on the wireless medium. Since EDCF can only solve the problem of internal collisions for high-priority ACs, there is still the possibility that external collisions between stations will occur.

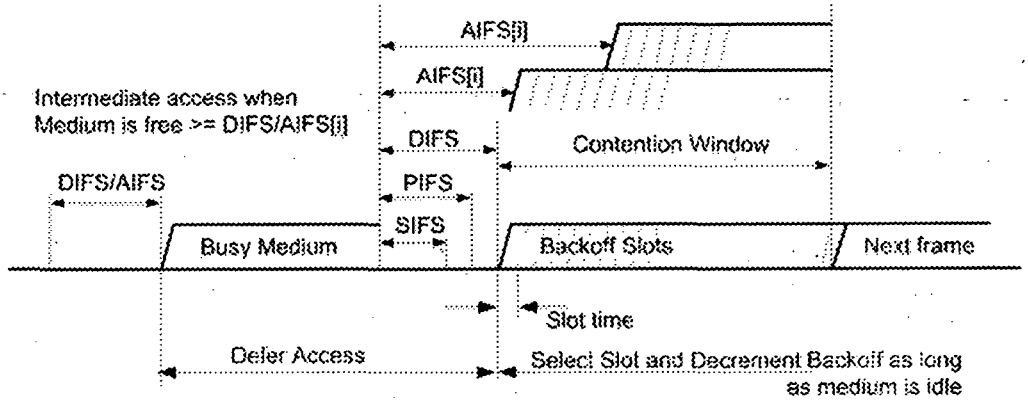


Figure 5-12: EDCF Timing Relationship for Different Priorities

An example of the implementation of priorities and the AC is shown in Figure 5-13, which illustrates a mapping from priorities to access categories.

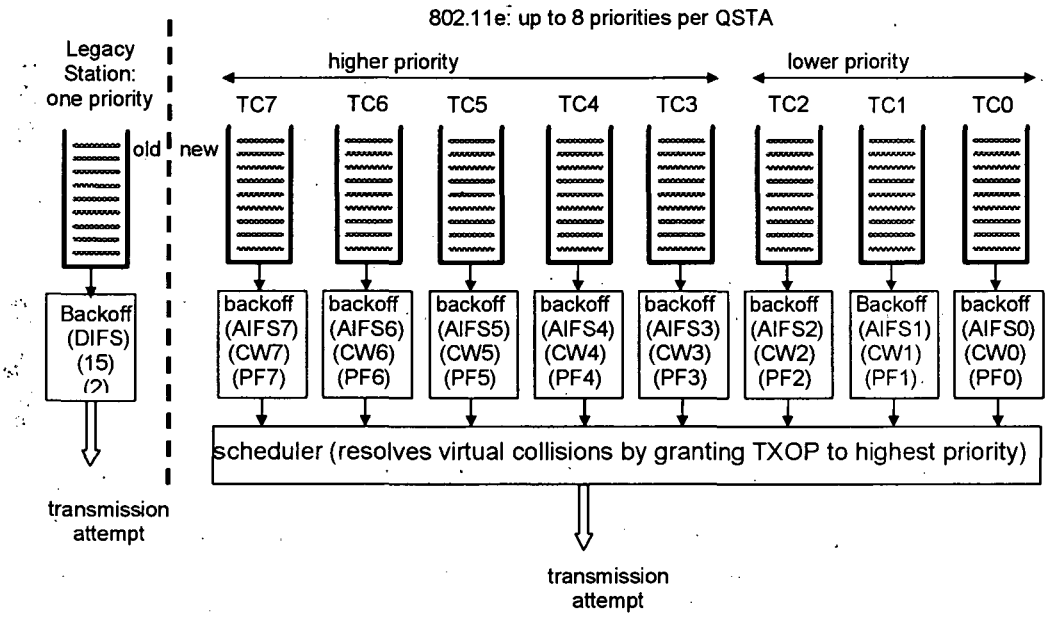


Figure 5-13: Enhanced DCF with Eight Priorities vs Legacy DCF

To enhance the performance and achieve better medium utilization, packet bursting called Contention Free Burst (CFB) can be used in IEEE 802.11e, meaning that once a station has gained access to the medium, it can be allowed to send more than one frame without contending for the medium again. A QSTA can initiate a CFB after either receiving a QoS (+)CF-Poll frame in a CP or on winning an EDCF contention. A CFB exists during a TXOP and a station is allowed to send as many frames as it wishes, as long as the total access time does not exceed a certain limit, the TxOpLimit. To ensure that no other station interrupts the packet bursting, a shorter IFS (SIFS) than usual is used between packets. If a collision occurs, the packet bursting is terminated.

5.3.1.2 HCF Controlled Channel Access Mechanism

The HCF controlled channel access mechanism is based on a polling scheme controlled by HC (Hybrid Coordinator) located at QAP of the QBSS. Hybrid Coordinator is a type of PC (Point Coordinator) but operates under rules that are different from those of a PC in the PCF. The most

important difference is that HC operates during both the CP and CFP periods. The HC has higher medium access priority than QSTAs. This allows it to transfer traffic from itself and to allocate transmission opportunities (TXOPs) to QSTAs. HC traffic delivery and TXOP allocation may be scheduled during both the CFP and CP, to meet the QoS requirements of particular TCs. The HC gains control of the wireless medium as needed to send QoS traffic to QSTAs and QoS (+)CF-Polls to QSTAs by waiting for a shorter time between transmissions than the stations using the EDCF or DCF access procedures The QoS CF-Poll from the HC can be sent after a PIFS idle period without any backoff. To give the HC priority over the EDCF, AIFS must be longer than PIFS, which are shorter than DIFS. Therefore, the HC can issue polled TXOPs in the CFP and CP intervals using its prioritized medium access.

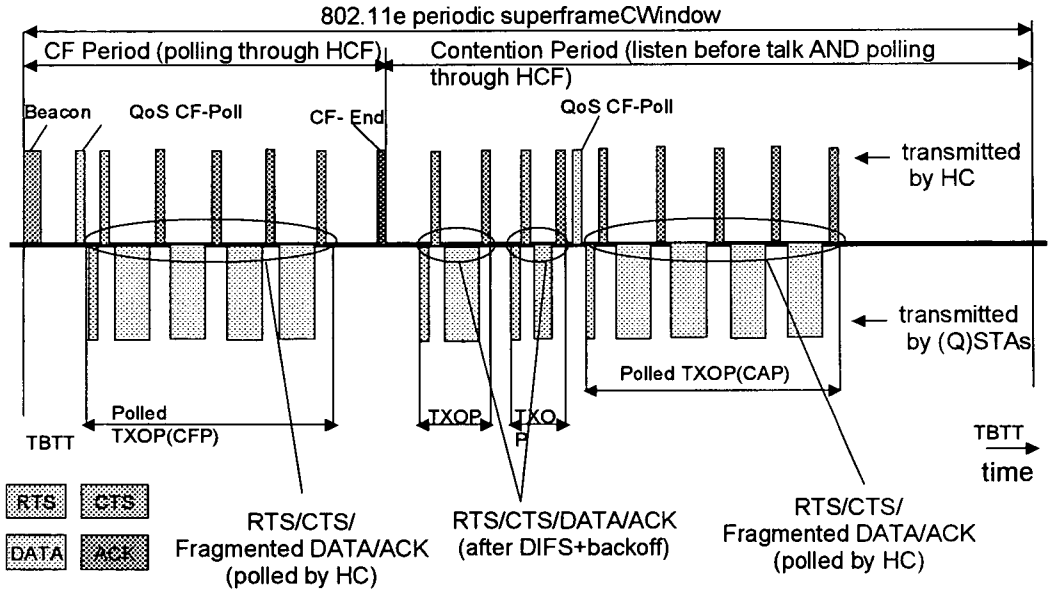


Figure 5-14: A Typical 802.11e Superframe

During the CFP, QSTAs will not attempt to get medium access on their own. Therefore, only the HC can grant TXOPs by sending QoS CF-Poll frames. Moreover, the HC provides improved protection for the CFP using a virtual carrier sensing mechanism, which solves the problem of unpredictable beacon delay. In the original 802.11 standard, this protection solely depends on having all the stations in the BSS set their NAVs to the value of the maximum duration of CFP at TBTT (Target Beacon Transmission Time). The CFP ends after the time announced in the beacon frame or by a CF-End frame sent from the HC. For controlled channel access during the CP period, several intervals named Controlled Access Periods (CAP) are defined. During each CAP interval, short bursts of CFB frames are transmitted using polling-based controlled channel access mechanisms, while during the remainder of the CP, all frames are transmitted using the EDCF contention-based rules. The HCF protects the transmissions during each CAP using the virtual carrier sense mechanism. Transmission protection during each CAP is also based on the virtual carrier sensing mechanism. Figure 5-14 illustrates an example of a typical 802.11e superframe. While in a controlled channel acces mechanism, polled-TXOP is used to determine which station can send traffic and how long, the HC sends a frame of QoS Data+CF-Poll+CF-Ack, "piggybacking" an MPDU with the ACK to the QoS data. So, the QSTA's initial TXOP limit is extended by this piggybacked frame of an additional CF-Poll.

5.4 Review

This chapter covered the QoS mechanisms in communication networks. First, the concept and needs of QoS were discussed. Next, a brief description of QoS architecture for ATM networks was presented, covering Traffic parameters, QoS parameters, and ATM service categories. The presentation then moved to QoS mechanisms in the Internet. Integrated Services architecture, RSVP protocol, Differentiates services architecture, and MPLS mechanisms were explained. Then, the QoS in UMTS networks was presented. In this section, UMTS QoS architecture and QoS classes were covered. The chapter concluded with a discussion of IEEE 802.11e standard enhancements to provide QoS in WLAN. Enhanced DCF and HCF Controlled Channel Access mechanisms were explained.

6 QoS Provisioning in Mobile Internet

During the last decade, we have seen an exponential growth in the Internet and mobile communications. A further rapid growth of these two main communication technologies, particularly towards real-time multimedia service provisioning, is expected in the next few years. Furthermore, it is expected that mobile users will request the same real-time services as fixed Internet users. It is obvious that, in a mobile Internet environment, these services require both mobility and QoS support. The MIPv4 and MIPv6 protocols provide transparency of host mobility to transport and higher layer protocols but do not provide QoS. On the other hand, the Internet QoS techniques of IntServ/RSVP, DiffServ, and MPLS do not consider mobile environments. To date several solutions addressing QoS provision to mobile hosts have been proposed. In this chapter, we propose a new framework for end-to-end QoS provisioning for mobile users' applications. In order to meet the requirements of mobile users' real-time applications, we also propose a new protocol for QoS provisioning and evaluate it for partially meshed access network architecture. In the planned network technologies of the present and near future, terrestrial wireless networks such as WLANs, GSM, and UMTS have a strict hierarchical topology, whereas satellite systems such as Iridium and Teledisc are typical cases of a partially meshed topology of access points. However, we propose a partially meshed topology for terrestrial wireless networks as well, which we think is beneficial for local communities' communication in general and for local mobility management in particular. The following sections first present an overview of the proposed solutions for QoS provisioning to mobile users, such as Resource Reservation in Advance, Coupling of Micro Mobility and QoS, and RSVP and Mobile IPv6 Interworking, and then present our proposed framework and signalling protocol for end-to-end QoS provisioning.

6.1 Resource Reservation in Advance

In order to provide Quality-of-Service for mobile hosts' applications, resource reservation is needed. An ideal resource reservation, to guarantee QoS to applications, would be the advance reservation of resources at the cells that the mobile host may possibly visit during the lifetime of the connection. There have been many proposals to perform prior reservations, which can be classified into two groups: Admission Control Priority, and Explicit Advanced Reservation. These strategies can also be used together, as admission control strategies are transparent to explicit advanced reservations mechanisms, except when a request is rejected.

6.1.1 Admission Control Priority

In general, in telecommunication networks a higher priority is given to ongoing calls than to new call requests. This rule holds for mobile networks as well, implying that network should give higher priority to a handover connection request than to new connection requests. Admission control priority based mechanisms rely on this rule to provide priorities on the admission control to handover requests without significantly affecting new connection requests. The main idea of these admission control strategies is to reserve resources in each cell that has to deal with future handover requests. The key issue here is to effectively calculate the amount of bandwidth to be reserved based on the effective bandwidth [EM93] of all active connections in a cell and the effective bandwidth of a new connection request.

6.1.2 Explicit Advance Reservation

To accommodate both mobile hosts that can tolerate variations in QoS and those that want mobility independent service guarantees in the same network, admission control mechanisms are not enough. To obtain good service guarantees in a mobile environment, the mobile host needs to make resource reservations at all the cells it may visit during the lifetime of the connection. This strategy is known in the literature as explicit advance reservations. The challenge for these schemes is how to predict the mobile host's movement so that advance reservation may be done only in some of the potential new cells. If predictions are not available, resource reservation has to be performed in all neighboring cells, which results in a waste of resources. There are a number of different protocols for advanced reservation in the literature. A well-known protocol of this group is the Mobile RSVP (MRSVP) [Tal01], which allows a mobile host to make advance reservation along the data flow paths to and from the cells it may visit during the lifetime of the connection. According to the MRSVP reservation model, a mobile host can make an advance reservation from a set of cells called Mobility Specification (MSPEC). Ideally, MSPEC should be the set of cells the mobile host would visit during the ongoing sessions. A mobile host acquires its MSPEC either from its mobility profile or from the network when it initiates a reservation. For efficient use of resources active and passive reservations are defined in MRSVP, illustrated in Figure 6-1.

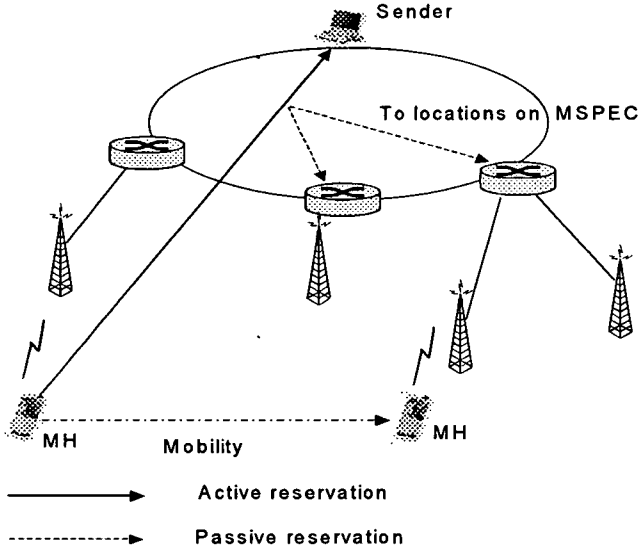


Figure 6-1: MRSVP Advanced Reservation

A mobile sender makes an active reservation from its current cell or a passive reservation from the other cells in its MSPEC. Similarly, a mobile receiver makes an active reservation to its current cell and passive reservation to the other cells in its MSPEC. For better utilization of the resources (links), bandwidth of passive reservations may be used from other mobile users requiring weaker QoS guarantees or best-effort services, whereas active reservations belong only to the mobile user itself. However, when a passive reservation becomes active the QoS may be affected. It should be also noted that an active - passive reservation model results in a very complex and expensive protocol. Mobile RSVP introduces three service classes to which a mobile user may subscribe:

- Mobility Independent Guarantees (MIG) in which a mobile user will receive guaranteed service.
- Mobility Independent Predictive (MIP) in which the service received is predictive.
- Mobility Dependent Predictive (MDP) in which the service is predictive with high probability.

6.2 Coupling of Micro Mobility and QoS

In a mobile environment, there is a need for fast re-establishment of QoS paths every time a mobile host changes its Access Router (AR). In order to improve the behaviour of reservation-based QoS, as defined in the Integrated Services architecture, in a dynamic micro-mobile environment, the QoS and micro-mobility mechanisms can be coupled to ensure that reservations are made as soon as possible when handover occurs. The reservations are made along the data path using a QoS signalling protocol, the most widely adopted of which is RSVP.

There are three levels of coupling Micro Mobility and QoS mechanisms:

- Decoupled,
- Loosly coupled,
- Closely coupled.

6.2.1 Decoupled Concept

In the decoupled scenario, the QoS and micro-mobility mechanisms operate independently of each other and the QoS implementation is not dependent on a particular mobility mechanism. When handover occurs, the Mobile Host (MH) changes the AR and the path to and from the MH changes as well. Changes in network topology are handled by the soft-state nature of the reservations. However, due to handover the QoS for traffic flows will be degraded until a new reservation is installed via refreshed messages of the RSVP between the router where the old route and new route intersects to the new AR. This router is referred to as a crossover router, a concept used in some micro-mobility schemes, and is illustrated in the Figure 6-2.

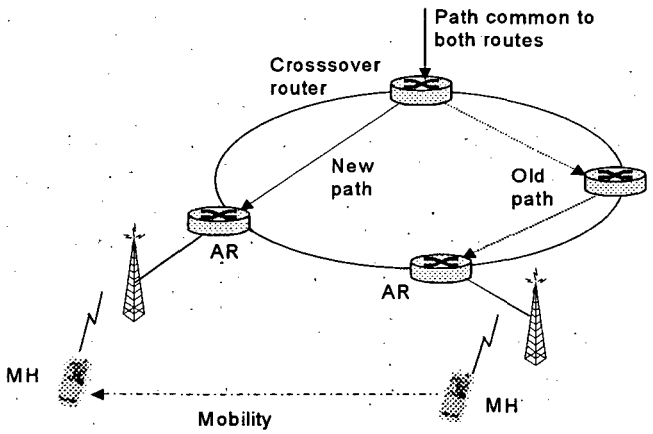


Figure 6-2: Crossover Router, New path, and Old path

6.2.2 Loosely Coupled Concept

The loosely coupled approach uses handover events to trigger the generation of RSVP messages that distribute the QoS information along new paths across the network. The RSVP messages can be triggered as soon as the new routing information has been updated in the routers. This mechanism is the Local Path Repair option, and is outlined in the RSVP specification [Bzb97]. It has the effect of minimizing the disruption to the application's traffic streams because there is a potentially shorter delay between handover and reservation set up. It also avoids the problem of trying to install a reservation across the network before the routing update information has been propagated. The latency for installing the reservation can also be reduced by localising the installation to the area of the network affected by the change in topology (the path between the crossover router and the new AR). The part of the network affected by the topology change can

have reservations installed across it almost immediately, instead of having to wait for the update to travel end-to-end or for the CH to generate a refresh message for reservations to the MH. In the case where the QoS must be re-negotiated, however, end-to-end signalling is required. The old reservation should be explicitly removed, freeing up unused resources immediately. However, the loosely coupled approach requires additional complexity within the intermediate network nodes to support the interception and generation of RSVP messages when the router is acting as the crossover router. Another disadvantage is that bursts of RSVP signalling messages are generated after handover to install multiple reservations, which is not then case in the decoupled scenario.

6.2.3 Closely Coupled Concept

The closely coupled approach uses the same signalling mechanism to propagate both the mobility and QoS information, either as an extension to the QoS/MM signalling protocol or via a unique QoS-routing protocol. This approach minimizes the disruption to traffic streams after handover by ensuring that the reservation is established as soon as possible after handover. However, instead of having to wait for an acknowledgement that the route to the MH is established in the network, as with the loosely coupled approach, the QoS requirements for traffic flows travelling to the MH can be updated at same time as the routing information. This avoids the problem of making a reservation before valid routing information to the MH has propagated across the network, and also provides a means to make multiple reservations using one signalling message. This reduces the bursts of QoS signalling traffic sent across the network that occur with the loosely coupled approach. In addition, the reservation along the old path can also be removed explicitly.

6.3 RSVP and Mobile IPv6 Interworking

Interworking of Mobile IP and RSVP protocols is another approach for QoS provisioning to mobile users. Several schemes have been proposed based on this approach such as that of Chi[99], Fan[98], and [She01a]. In Chi[99] and Fan[98] a combined scheme of RSVP and Mobile IPv6 is given, whereas in [She01], an interworking schem of RSVP and mobile IPv6 named Flow Transparency (FT) scheme is proposed. In the following we will present shortly the basic features of these schemes.

6.3.1 A combined scheme of RSVP and Mobile IPv6

The basic feature of the combined cheme is that flow identification (source and destination addresses) is based on the Mobile Host's (MHs) Care of Address (CoA). Each time that the MH changes the CoA during a session, an end-to-end RSVP signalling between the MH and the CH is needed. This results in wastege of resources, signalling overhead and high QoS signalling delay during handover. The QoS signalling delay from the time packets using the new CoA are released into the network until the time the QoS handling mechanisms are configured along the new path is one round trip delay when the MH is a sender and one and a half round trip delay when the MH is a receiver.

6.3.2 Flow Transparency Scheme

To alleviate the above-mentioned problems the Flow Transparency (FT) scheme has been proposed. The FT is an advanced interoperation scheme between the Mobile IPv6 and RSVP protocols to provide seamless QoS handover by avoiding an end-to-end resource reservation renegotiation process. The idea of the flow transparency concept (Figure 6-3) is to keep host mobility transparent to the network layer flow-handling mechanism, as in the Mobile IP concept, which

keeps host mobility transparent to the transport layer protocols. This is achieved by keeping the flow identity (source/destination addresses) constant, regardless of the change of the MH's CoA. However, this has an impact on both the RSVP and Mobile IPv6 protocols. In order to keep the flow identity constant, Path and Resv messages use MH's home address to identify the flow. When the MH is a sender, the MH's home address will be written in the Sender Template field of the Path message. Furthermore, the Filterspec field of the respective Resv message will carry the MH's home address. When the MH is a receiver, the flow destination will be identified with the MH's home address, written in the Session Object field of the RSVP messages. Certain modifications are also required in RSVP routers (depending on MIPv6 modifications) such as where the packet classifier should read the home address of the data packets.

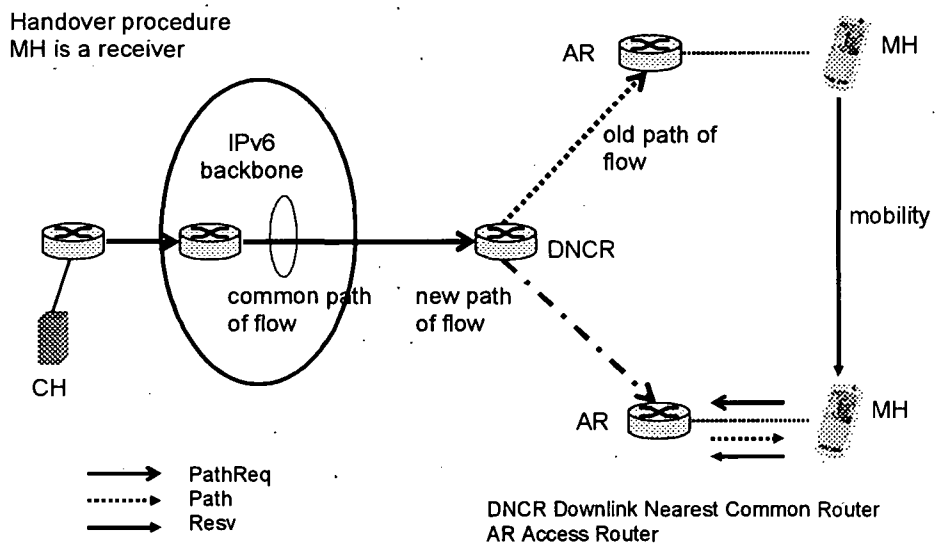


Figure 6-3: Flow Transparency

When the MH is a sender, in Mobile IPv6, the CoA is used for the source address of the packets, whereas the MH's home address is carried in the destination option header. When the MH is a receiver, the MH's CoA is used as a destination address, whereas the MH's home address is carried in the routing header. Considering the flow transparency concept and the MH as a sender, modifications are needed in MIPv6 for correct classification of packets in routers. The following solutions have been proposed:

- The home address of the MH is used as the source address, whereas the CoA is in the Destination Option Header.
- The CoA of the MH remains in the source address field, whereas the home address is in the Hop-by-Hop Option Header.
- A new header option called the Flow Transparent Route Alert Option is carried in the Hop-by-Hop Option Header, whereas the MH's CoA and home address remain as they are in MIPv6.

The first two solutions require the modification of MIPv6's basic properties. The third solution can be considered an extension of the MIPv6 features, because only a Route Alert Option field needs to be added. When the MH is a receiver its home address is also hidden from intermediate routers. However, due to the flow label parameter in MIPv6, the flow handling mechanism can process packets according to the flow source and flow label without examining the packet's flow destination.

6.3.2.1 Handover Procedure

For fast QoS signalling renegotiation due to handover, the merge and local repair features of RSVP at the Nearest Common Router (NCR), the first common router on the old and new paths of the flow, are exploited. For simplicity, explanations of handover procedures when the MH is a sender and when the MH is a receiver are presented separately.

Mobile host as a sender

After the MH acquires a new CoA, it first sends a Binding Update (BU) message to the CH and the HA as usual. Immediately thereafter the MH sends a Path message with the same flow address as before the handover but with a different CoA and previous hop address. If a router observes that the Path message has the same flow address but both the CoA and the previous hop addresses are different from the ones already stored in the path state, it will identify itself as an Uplink NCR (UNCR). The UNCR immediately replies with a Resv message to reserve resources along the newly added path to the MH (local repair due to sender mobility). In the common uplink flow path (from UNCR to CH), the previously reserved resources will be used. Since the Path message traverses a shorter distance than the BU message, a QoS configuration of routers in the newly added path is achieved before packets with the new CoA are issued in the network, resulting in seamless handover.

Mobile host as a receiver

When the mobile host acts as a receiver, handover operation proceeds differently. After changing the CoA, the receiver sends a BU to the CH and the HA. Because it cannot issue the Resv message before it receives the Path message, and instead of waiting for a Path message from the CH, the MH informs the Downlink NCR (DNCR) of its mobility to trigger the Path message from the DNCR. For this task, an additional RSVP message named PathReq is needed. The PathReq_message will carry mobility information in the Mobility Object (MO), which contains the home address and the current CoA of the MH. The home address will be used as the flow destination, whereas CoA will be used as the destination address of the subsequent Path message sent by the DNCR. The MO can also be piggybacked on a Path message sent by the MH itself if the MH acts as both sender and receiver. Upon receiving a PathReq message or a Path message with a MO sent from the MH, the RSVP router decides whether it is the DNCR by comparing the home address in the MO with the related information in the path state for the flow destinated to the MH. If the router identifies itself as a DNCR then it sends a Path message to the MH's new CoA (local repair due to receiver mobility) for the flow indicated by the destination.

6.4 A Framework for End-to-End QoS Provisioning

In this section, a new framework for end-to-end QoS provisioning to mobile users applications is presented, considering heterogeneous access networks, fixed and mobile. In order to meet the requirements of mobile users' real-time applications, a new signalling protocol for QoS provisioning is also proposed and evaluated.

6.4.1 Network Architecture

The proposed network architecture for end-to-end QoS provisioning to mobile users, shown in Figure 6-4, consists of IPv6 based access and core networks.

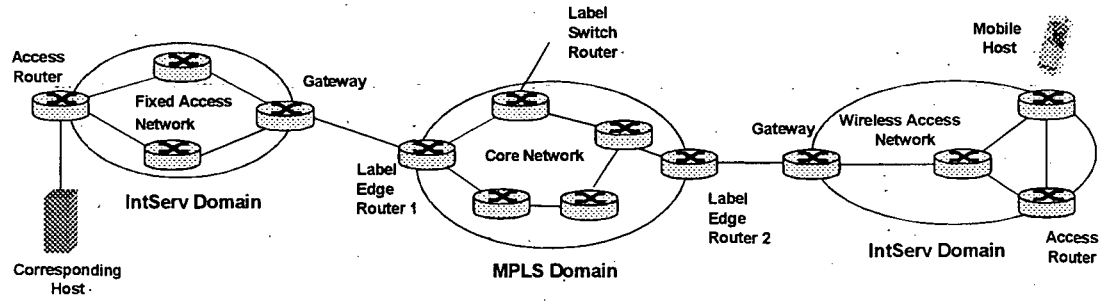


Figure 6-4: Architecture for End-to-End QoS Provisioning

The access network consists of MIPv6 and RSVP capable access and intermediate routers connected in a hierarchical structure, with partially meshed access routers at the lowest level. Each router is responsible for one or two wireless subnetworks. These wireless subnetworks, from the point of view of mobility, may be organized into three groups:

- Wireless LANs (WLANs) for local areas,
- Cellular for wide areas, and
- Satellite for worldwide coverage.

We will assume that in a WLAN environment, mobile hosts are connected to access routers via an access point; that in cellular networks mobile hosts are connected via base stations or directly to access routers, which also have base station functionalities; and that in satellite subnetworks each satellite is considered an access router, to which the mobile hosts have direct connection. In the planned network technologies of the present and near future, satellite systems such as Iridium and Teledisc are typical cases with partially meshed topology, whereas terrestrial wireless networks such as WLANs, GSM, and UMTS have a strict hierarchical topology of access points. Hence, we propose a partially meshed topology for the terrestrial wireless networks, which in our opinion is particularly important and beneficial for local communities. The idea of meshed access networks is to make the networking of local communities more efficient. By this we basically mean, on the one hand, an easier communication within a neighbourhood, more robust networks against remote failures and to avoid payments to remote agencies for local communication and, on the other hand, that mobility management functions are more efficient. Motivated neighbors, for example, will install higher speed WLAN equipment for high-speed sharing. Hence, local email, local web pages, local multimedia communication, and local telephone calls will not be under the necessary control of remote charging administrations. Existing mobile networks and the Internet as it is today are very reliant on the correct operation of distant network elements. In general, one or more core networks may be between two or more access networks. In our model, we have assumed only a single core network that consists of edge and core routers. For QoS provisioning in the access network we apply the IntServ/RSVP model. The core network is assumed as a pure MPLS domain, i.e., MPLS is used to set up paths (Label Switched Paths) and to support QoS models to provide service differentiation [Hor02]. We also assume that RSVP signaling messages travel end-to-end between CH and MH to support RSVP/IntServ reservations outside the MPLS network domain and are tunneled across the MPLS domain. According, to the RSVP protocol, admission control functions for requested access network resources are performed at the routers, hop-by-hop, along the path from the receiver to the sender in the IntServ domain. For the MPLS domain, admission control is performed at the ingress Label Edge Router (LER). Furthermore, at the LER of the MPLS domain, service mapping between service classes of IntServ and MPLS is performed. A proposal for a possible scenario for service mapping from IntServ classes to MPLS service classes is given in the Table 6-1.

Table 6-1: An example for service mapping from IntServ to MPLS

IntServ Service	MPLS EXP Field	MPLS Service Class
GS	111	MGS
CL1	110	MCL1
CL2	101	MCL2
CL3	100	MCL3
CL4	011	MCL4
CL5	010	MCL5
CL6	001	MCL6
BE	000	BE

In the proposed model, all three QoS classes for IntServ are included: the Guaranteed Service (GS) class with the highest priority, the Control-Load Service (CL) with the lower priority, and the Best Effort (BE) service with lowest priority. Furthermore, control-load service is divided into six subclasses, from CL1 to CL6, with different priorities, based on the traffic parameter (TSpec) values of the applications. Hence, different applications can invoke different subclasses of the control-load service. Based on the Experimental (Exp) bits on the MPLS shim header, up to eight MPLS service classes can be defined to match the defined IntServ QoS classes. These are: MGS (MPLS Guaranteed Service) for the guaranteed service class, six MCL (MPLS Controlled-Load service) classes, from MCL1 to MCL6, and the best-effort service class can be extended to include service classes under the DiffServ architecture.

6.4.2 Protocol Description

In order to provide fast handover QoS signalling while avoiding end-to-end signaling due to local mobility handover, a new protocol is proposed. The main feature of this scheme is that it requests resource reservation only in the newly added path (due to handover) of the ongoing connection, whereas in the common flow path the previously reserved resources are used. Actually, the proposed protocol consists of two parts. The first part is related to signaling messages for new connections; the second part is related to signaling messages when handover occurs. For simplicity, we will only consider the communication between a single Mobile Host (MH) in a wireless IntServ access network and a single Correspondent Host (CH) in a fixed IntServ access network.

6.4.2.1 Signaling Message Flow for New Connections

In Figure 6-4, we will consider only the case when MH is a receiver while the CH is a sender. The case when the MH is a sender and the CH is a receiver is identical, except that the MH and CH have to swap roles. The following message sequences illustrate the process by which an application obtains resource reservations for end-to-end QoS provision:

1) The QoS process on the sending host CH generates and sends to the MH the RSVP Path message that describes the traffic offered by the application.
2) At the Label Edge Router 1 (LER 1), the Path message is subjected to standard RSVP processing and the path state is installed in the router. In addition, the LER 1 has already an established LSP that terminates at egress LER 2. The Path message it is then encapsulated into the LSP and transmitted to LER 2. When the Path message reaches LER 2, it is decapsulated and sent through the access network to the mobile host.
3) When the Path message reaches the MH, a Resv-message indicating the offered traffic of the sending application of a certain IntServ service type is generated. Then, the Resv message is carried back to the MPLS network domain and the sending host.

4). At the LER 2 and at any RSVP capable node in the path, the Resv message may be rejected if resources on the downstream interface are insufficient to carry the requested traffic. If it is not rejected, it will be transmitted via a tunnel through the MPLS network to LER 1.
5) Having arrived at LER 1, the Resv message triggers admission control processing. The LER 1 compares the resources requested in the RSVP/IntServ request to the resources available in the already established LSP to the LER2 at the corresponding MPLS service level.
6) If the LER 1 approves the request, the Resv message is sent upstream through the network domain to which the CH is attached. Any RSVP node in this network domain may reject the reservation request due to inadequate resources or policy. If the request is not rejected, the Resv message will arrive at the sending host, CH.
7) At the CH, the QoS process interprets receipt of the Resv message as indication that the specified traffic flow has been admitted for the specified IntServ service type.

6.4.2.2 Signaling Message Flow when Handover Occurs

In this section, we present a new protocol for QoS provisioning for mobile users when handover occurs. The proposed protocol is based on the Flow Transparency (FT) Mobile IP and RSVP interworking scheme and can be considered as its compliment for meshed access network topologies. The basic idea of the proposal is to use the previous Access Router (AR) as a Nearest Common Router (NCR) for the old and the new added flow paths. We have added two new RSVP messages: PathState_discovery and PathState_reply, to optimize the use of already reserved resources. As far as MIPv6 is concerned, for address mismatch avoidance, we propose the solution c) given in Section 6.1.3.1, which is just an extension to MIPv6 and not a modification as required by other proposals. For the proposed framework for end-to-end QoS provisioning, the proposed protocol may be viewed as a "Micro Mobile QoS", which improves handover QoS performances within a domain consisting of wireless and fixed access networks. In the following paragraphs, we will explain handover procedures, first presenting the cases when the MH is a sender, then when the MH is a receiver, and then when MH is a both sender and a receiver.

Mobile host as a sender

The initial procedure of the protocol is the same as in the flow transparency concept. When handover occurs the MH acquires a new CoA and immediately sends a BU (Binding Update) to the CH and HA. Thereafter, the MH sends a Path message with the same flow address as before the handover but with a different CoA and previous hop address. When the access RSVP router receives the Path message it checks first if it is the Uplink NCR (UNCR), by the standard procedure of the flow transparency concept. The following two cases may occur: either the new access router is a UNCR or it is not.

1) If the new access router identifies itself as an Uplink NCR (UNCR), the UNCR immediately replies with a Resv message to reserve resources along the newly added path to the MH and also sends a PathTear message to the old MH's CoA to trigger the release of the old reserved resources. In the common uplink flow path (from UNCR to CH), the previously reserved resources will be used.
2) If the new access router is not a UNCR, as shown in Figure 6-5, then the router sends a PathState_discovery message to all adjacent routers. PathState_discovery contains the flow identification information. All routers that receive this message with reply with the PathState_reply message for the indicated flow, which besides other necessary information contains a one-bit flag to indicate whether the router has already a related path state. The following two cases may occur:

2.a) If two or more adjacent routers have a path state then the access router selects one of them for the next hop router, based on the routing table, and forwards the Path message. Upon receiving the Path message, the selected router will respond with a Resv message to-

wards the MH's new CoA to reserve resources and will also send a PathTear message to the old MH's CoA to trigger the release of the old reserved resources.

2.b) If none of the adjacent routers has a path state then the access router selects the next hop router, based on the routing table, and sends the Path message to that router. The selected router will forward the Path message to the next hop router. The next hop router will check for being a UNCR. If it is, it will reply with a Path message towards MH CoA, if it is not, it will forward the Path message to the next hop router. This procedure is repeated until the Path message reaches the UNCR. In the worst case, it reaches the CH. When UNCR is reached, it responds with Resv message to reserve resources along the new added path.

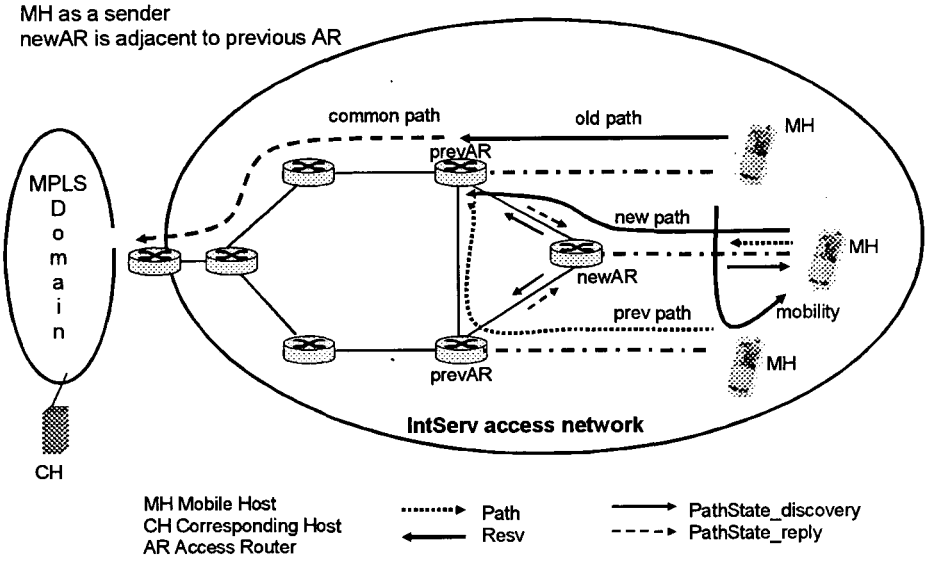


Figure 6-5: Handover Procedure: Mobile Host as a Sender

Mobile host as a receiver

When the mobile host acts only as a receiver, as in the flow transparency concept, the mobility object (containing the mobility information) is carried in the PathReq_message. When the access RSVP router receives the PathReq message from MH, it checks first if it is the DNCR, by comparing the MH's home address with the existing one in the path state information. The following two cases may occur: either the new access router is a DNCR or it is not.

1) If the new access router is a DNCR, then the protocol procedures are the same as in the flow transparency concept. Having received the PathReq message the DNCR will immediately trigger and send appropriate Path message to the MH's new CoA for the flow indicated by home address in the Mobility Object (MO). After receiving the Path message, the MH can issue the Resv message to ask for resource reservation along the newly added path to the MH.
2) If the new access router is not a DNCR, then the router sends a PathState_discovery message to all adjacent routers where PathState-discovery contains the flow address. All routers that receive this message reply with the PathState_reply message for the indicated flow, which besides other necessary information contains a one-bit flag to indicate whether the router already has a related path state.

2.a) If two or more adjacent routers have a path state then the access router selects the next hop router, based on the routing table, and forwards the PathReq_message. This case illustrates Figure 6-6. Upon receiving the PathReq-message, the selected router will respond with a Path message towards the MH's new CoA and will also send a PathTear message to the old MH's CoA to trigger the release of the old reserved resources. After receiving the Path message the MH sends Resv message to reserve resources along the new path.

2.b) If none of the adjacent routers has a path state then the access router selects the next hop router, based on the routing table, and sends the PathReq-message to that router. The selected router will forward the PathReq-message to the next hop router. Each next hop router will check for being a DNCR. If it is, it will reply with a Path message to the MH's new CoA; if it is not, it will forward the PathReq-message to the next hop router and the procedure repeates until the PathReq message reaches the DNCR.

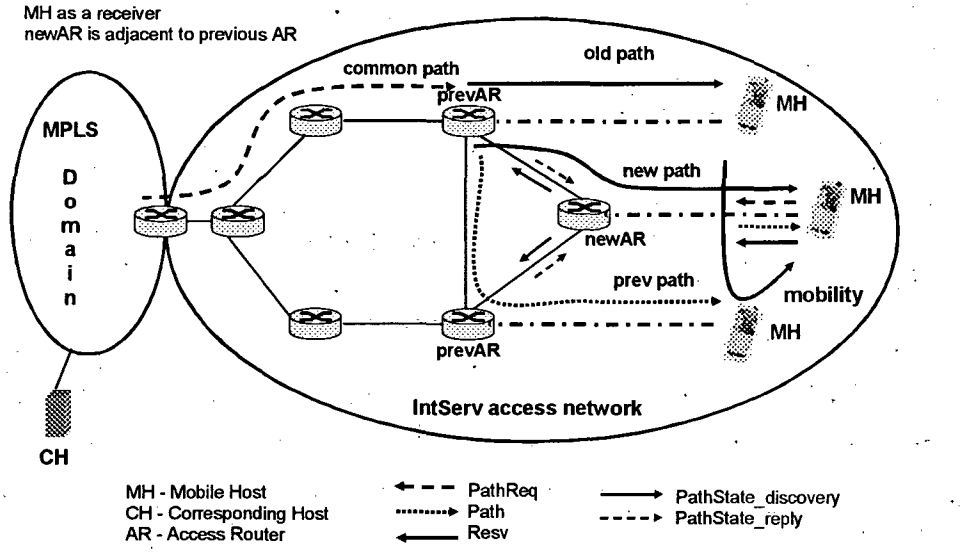


Figure 6-6: Handover Procedure: Mobile Host as a Receiver

Figure 6-7 shows the flow diagram of the signalling messages when the mobile host is a receiver and the previous access router is an adjacent router.

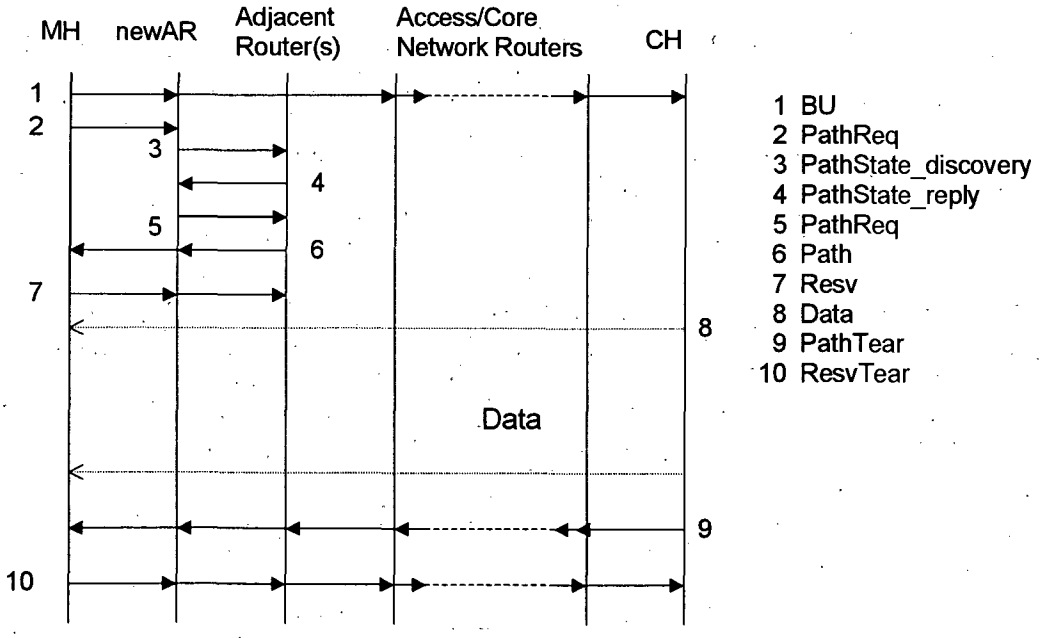


Figure 6-7: Signaling Messages Diagram: Mobile Host as a Receiver

Mobile host as both sender and receiver

This case can be considered as a combination of the above cases, with some minor differences. The main difference is that the mobility object is piggybacked onto the Path message sent from the MH to the CH. The new access router will first check the uplink, then the downlink direction.

Uplink direction

When the new access router receives the Path message from the MH, it checks first if it is the UNCR. This results in the following two cases:

1) If the new access router is a UNCR then the protocol procedures are the same as in the case when mobile host is a sender, case (1).
2) If the new access router is not a UNCR then the procedure proceeds as in the case when mobile host is a sender, case (2).

Downlink direction

After processing the mobility information for the uplink direction, the new access router will proceed to compare the same mobility information, piggybacked onto the Path message, with the path state for the downlink direction. The protocol procedures are identical to the case when the mobile host acts only as a receiver, except that the name of the message is Path instead of PathReq.

6.4.3 Simulation and Performance Evaluation

To evaluate the performances of the proposed protocol when handover occurs, we have used discrete event network simulator IKNsim, developed at the Institute of Broadband Communications (formerly named Institute of Communication Networks) of Vienna University of Technology.

6.4.3.1 Simulation Environment

The simulation environment includes the following elements: network topology, traffic, congestion state in the network, protocols, and mobility scenario.

Network topology

In order to investigate the impact of the meshed network concept, we have simulated different network topologies referred as Topology 1 to Topology 5. The basic topology of the simulated network is hierarchical with the lowest level of routers being meshed. Referring to Topology 1 (Figure 6-8) nodes 1 to 8 are Access Routers (AR) and we assume that each router is responsible for one subnetwork, i.e., there are eight wireless subnetworks. Nodes 9 to 14 are intermediate routers in the access network, whereas node 15 is the Gateway (GW) to the core network. In the core network, only the Correspondent Host (CH) and the Home Agent (HA) are shown, (nodes 16 and 17, respectively). In all simulated topologies, there are four types of links with different delays and capacities. The wireless a-links are used to interconnect mobile hosts with the access routers and they are assigned a constant delay of 1 ms and a constant bit rate of 2 Mbit/s. The b-links between the access routers have a delay of 2 ms. All other links in the access network, the c-links, have a delay of 5 ms. The d-links in the core network have a delay of 30 ms.

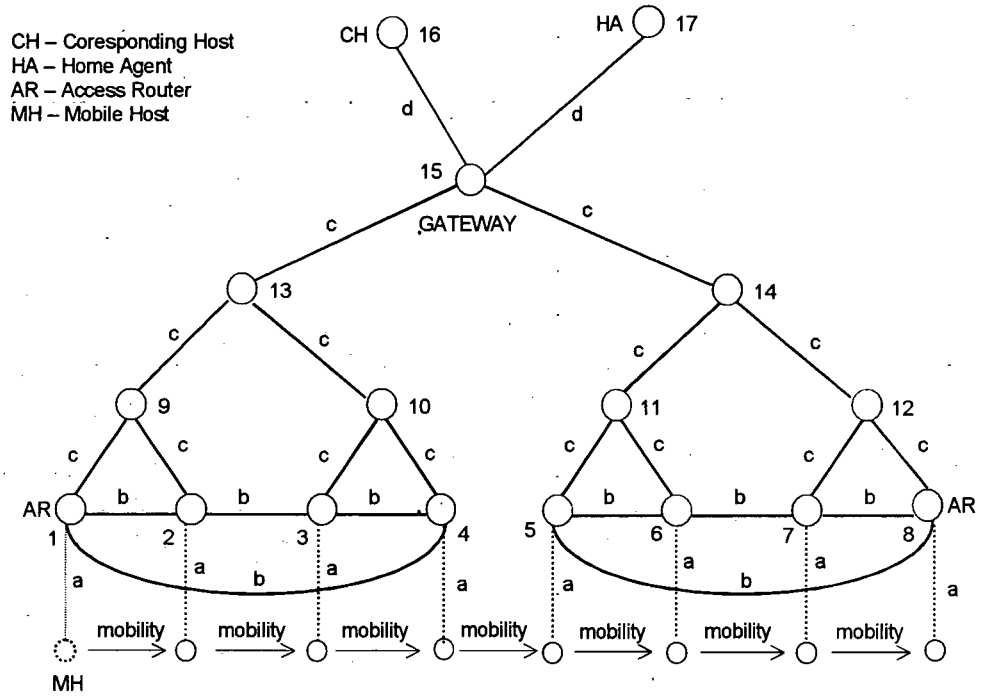


Figure 6-8: Network Topology 1

Traffic

Two types of traffic are simulated: real-time traffic transmitted from the Corresponding Host (CH) to the Mobile Host (MH) and background traffic. Traffic from the CH to the MH is a 500 kbit/s Poisson flow with constant packet size 500 bytes. Therefore, a bandwidth of 500 kbit/s is reserved from the CH to MH. According to the MIPv6 principles, the first packets are intercepted by the Home Agent (HA), whereas packets sent later are directly transmitted to the mobile host. Background traffic consists of n x (k x 64 kbit/s) streams transmitted from the CH to the access routers (one stream per access router), where n is the number of access routers, whereas k = 1, 2, 3, 4, ... is a parameter for the traffic load. The background traffic is also generated according to a Poisson distribution with a constant packet size of 80 bytes.

Congestion

By assigning different bit rates to the links and by generating different background traffic loads, we have simulated three network congestion scenarios: access network congestion, core network congestion, and no-congestion.

- The access network congestion is modelled by assigning a bit rate of 2 Mbit/s to the links in the access network, 10 Mbit/s to the links in the core network and by generating the adequate amount of traffic load for each topology to cause congestion in the access network.
- The core network congestion is modelled by assigning a bit rate of 2 Mbit/s to the d-links in the core network and a bit rate of 10 Mbit/s to the b-links and c-links in the access network. Again, for each topology the traffic load is generated adequately to cause congestion in the core network.
- In the no-congestion scenario, we assumed that there is no congestion at all by assigning a bit rate of 10 Mbit/s to all the links (except wireless a-links, which have a constant bit rate of 2 Mbit/s in all scenarios). The total traffic load (background and traffic from CH to MH) in this scenario amounts to n x (6 x 64 kbit/s) + 500 kbit/s, and will not cause congestion to the links of 10 Mbit/s bit rate.

Protocols

In order to demonstrate some of the features of the proposed protocol, we have also simulated two existing similar protocols, those of [Chi99] and [She01a] presented in Section 6.1.3. All three protocols are simulated for the case that the MH is a receiver. The simulation results of the protocols given in these sections are denoted as "proposed protocol", "FT protocol", and "conventional protocol", respectively. Figure 6-9 shows the block diagram of all three simulated protocols.

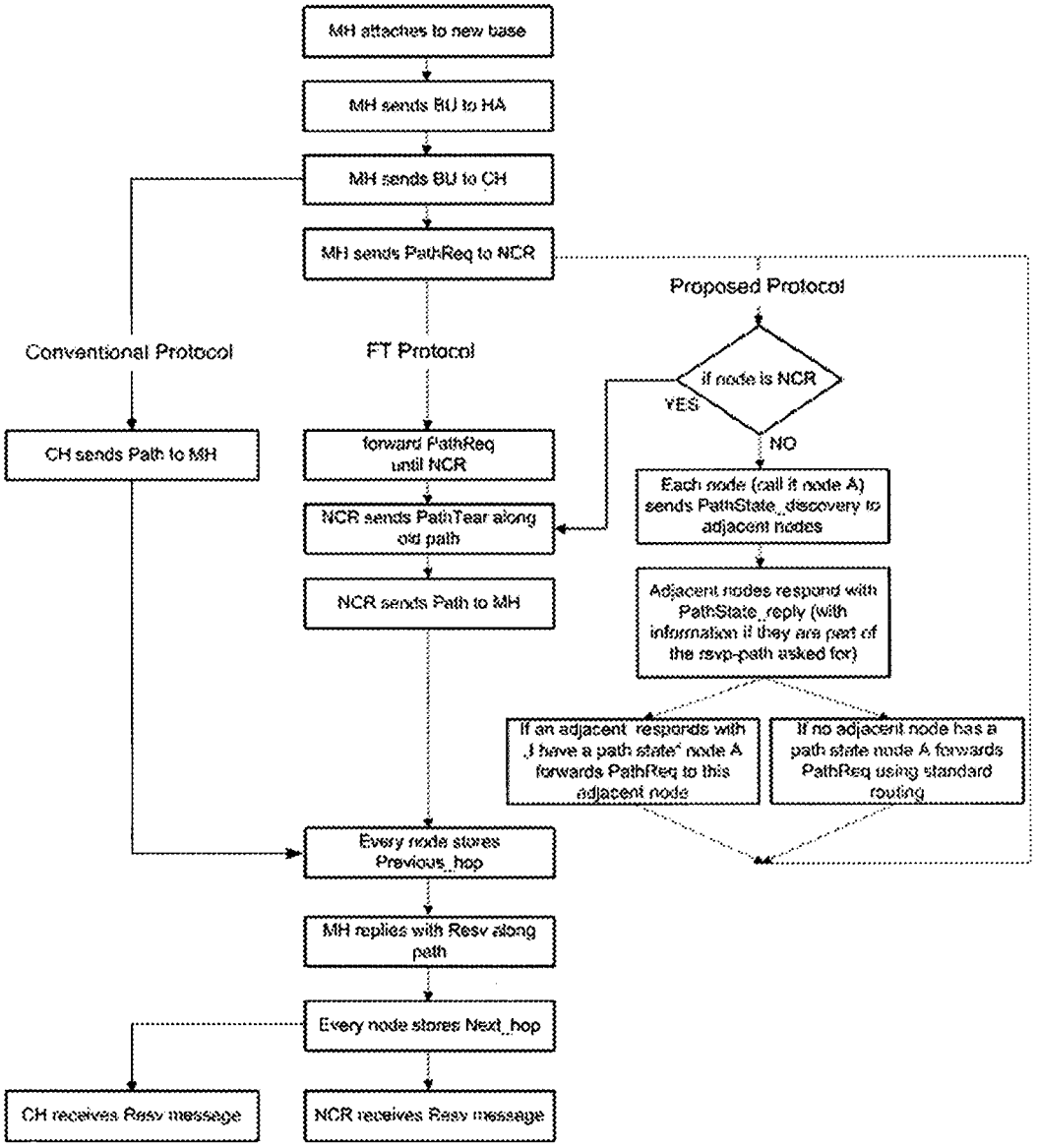


Figure 6-9: Block diagram of the Proposed, Conventional and FT Protocols

Mobility

Two mobility scenarios are simulated considering one MH in the network.

- In the first scenario, referred as mobility scenario 1, we assume that MH is moving in the pattern 1-2-3-4-5 ... n (n is the number of subnetworks or access routers), which is typical for example when a MH is moving along a highway in cellular networks or along a corridor in case of WLAN networks.
- In the second mobility scenario, referred as mobility scenario 2, we assumed the mobility pattern where mobile host moves to the new subnetwork and then goes back again to the previous subnetwork. For Topology 1, for example, the mobility pattern for mobility scenario

vious subnetwork. For Topology 1, for example, the mobility pattern for mobility scenario two is: 1-2-3-2-1-4-5-6-7-8.

In both mobility scenarios, handover occurs every 10 seconds, meaning that the MH stays in each subnetwork for 10 seconds. We have considered only IP level handover, which takes place when the MH crosses two cells that belong to different subnetworks.

6.4.3.2 Performance Evaluation

The RSVP signalling delay and the maximum allowed delay for QoS provisioning have been taken as performance metrics for the simulated protocols.

- RSVP signalling delay is defined as the amount of time elapsed since a MH acquires a new CoA until resources in the new added path are reserved.
- Maximum allowed delay for QoS provisioning is defined as the time from the instant when the Binding Update (BU) is sent to the CH until the first packet with the new CoA arrives at the NCR (Nearest Common Router).

In the following subsections, we will first analyse and compare the proposed protocol and the conventional protocol, then the proposed protocol and the FT protocol. Then a further analyses of the proposed protocol related to meshed access network topologies will be discussed.

Comparison of the proposed protocol and the conventional protocol

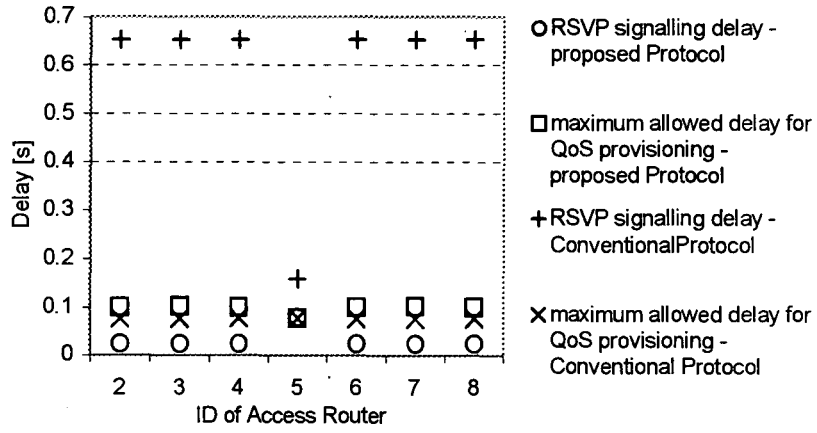
Figure 6-10 shows the simulation results for the proposed protocol and the conventional protocol for Topology 1, for the three congestion scenarios assuming mobility scenario 1 (mobility pattern 1-2-3-4-5-6-7-8).

- For the access network congestion, the background traffic of 8 x (7 x 64 kbit/s) = 3.584 kbit/s (8 is the number of subnetworks or access routers) was generated. This means that 2 Mbit/s link between nodes 15 and 13, as well as 2 Mbit/s link between nodes 15 and 14 are loaded with 1.792 kbit/s each. Adding to the background traffic, the 500 kbit/s real-time traffic transmitted from CH to MH, the total traffic load on each of the above-mentioned links would be 2.292 kbit/s, which causes congestion in the access network.
- For core network congestion, the 2 Mbit/s link between CH and gateway is loaded with 8 x (4 x 64 kbit/s) = 2.048 kbit/s. Again adding the 500 kbit/s traffic load from CH to MH, the total traffic load on the core network link will be 2.548 kbit/s, which causes congestion in the core network.
- For the no-congestion scenario, we have generated traffic load of 8 x (6 x 64 kbit/s) + 500 kbit/s = 4.596 kbit/s, which does not cause congestion on the links with a bit rate of 10 Mbit/s.

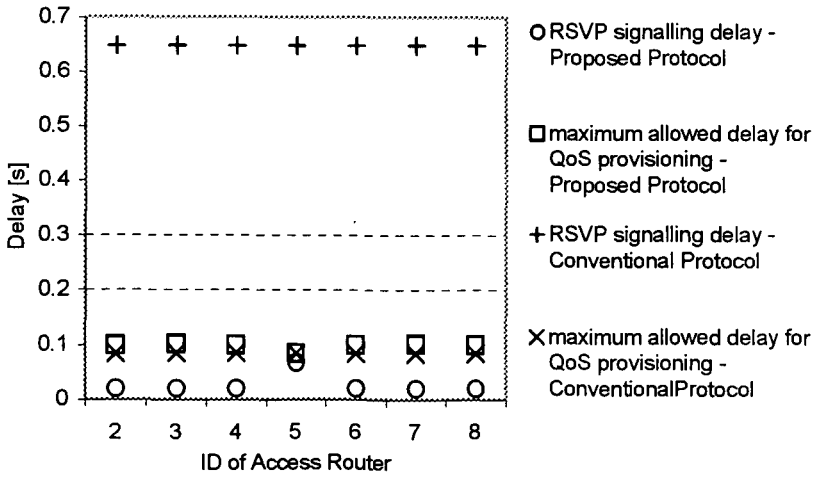
Figure 6-10a shows for the access network congestion scenario that the handover RSVP signalling delay in the proposed protocol is much smaller for all handover instants. This can be explained by the fact that in the conventional protocol the handover Path message is always issued by the CH after it receives the Binding Update (BU) from the MH, while in proposed protocol, the handover Path message is issued by the Nearest Common Router (NCR) after it gets the request message called PathReq from the MH. Since the PathReq traverses a shorter distance than BU and there is no congestion in the reverse direction of the packet flow Path message in the proposed protocol is issued faster and traverses shorter distance than in the conventional protocol. Similarly, the handover Resv message traverses a shorter distance with in proposed protocol. However, the main reason for the huge difference in the RSVP signaling delay between two protocols lays in the fact that in conventional protocol, during each handover the Path message has to go through all links between CH and MH, including the most congested links between the gateway and nodes 13 or 14. On the other hand, in the proposed protocol the

Path messages are always issued by the previous access router except in the case of the handover from subnetwork 4 to subnetwork 5 (where there is no direct link in between). At this handover instant, the Path message is issued by the gateway (node 15), which serves as NCR, and it has the longest delay since the maximum number of links are involved in the signalling path. From the plot, it can also be noticed that the RSVP signaling delay for the conventional protocol in case of handover from subnetwork 4 to subnetwork 5 is relatively small in comparison to the other handover instants. An explanation is that the link that connects nodes 15 and 14 is not yet congested, since traffic from CH to MH is still transmitted to the old care of address along the link that connects nodes 15 and 13.

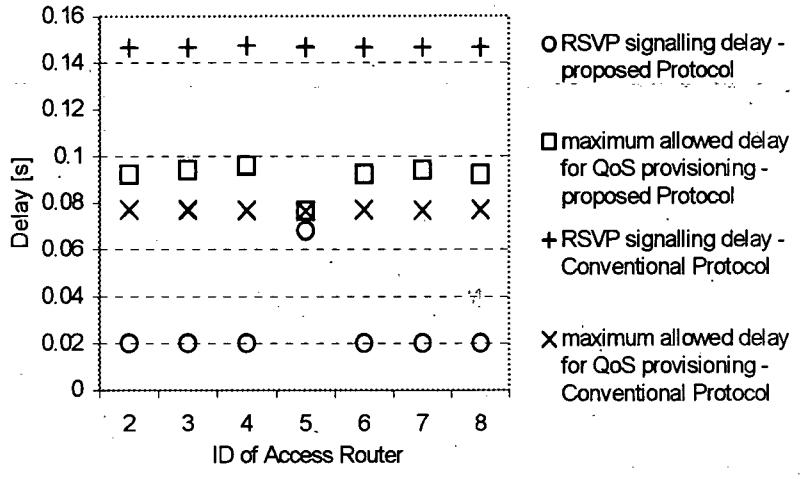
Figure 6-10a also shows that, for the proposed protocol the RSVP signalling time span is relatively smaller than the maximum allowed delay for QoS provisioning at all handover instants, except during the handover from subnetwork 4 to subnetwork 5. This means that during all handover instants, the proposed protocol ensures QoS provisioning for all packets that use the new CoA, because resource reservation in the new flow path is established before the packet transmission starts along the new path. In the case of handover from subnetwork 4 to subnetwork 5, RSVP signalling delay and the maximum allowed delay are almost equal. An explanation is that in this case the Nearest Common Router is node 15 (gateway), resulting in shorter maximum allow delays in comparison to the other handover instants, because only the uncongested link between CH and NCR is involved, whereas the RSVP delay is longer in comparison to the other handover instants. With the conventional protocol, the RSVP signalling delay is much longer than the maximum allowed delay. Therefore, packets that use new CoA will lack QoS until the BU is processed in the CH and before QoS for the new path is ensured.



a) Access network congestion in Topology 1



b) Core network congestion in Topology 1



c) No-congestion in Topology 1

Figure 6-10: Proposed and Conventional Protocol, Topology 1, Mobility Scenario 1

For the core congestion scenario, Figure 6-10b shows that handover RSVP signalling delay is significantly reduced in the proposed protocol for all handover instants. An explanation is that during each handover the Path message has to go through all links between CH and MH, including the most congested link, which in this scenario is the link between CH and gateway. On the other hand, in the proposed protocol, none of the Path messages (issued by previous access router or gateway) needs to go through congested link between CH and gateway. Furthermore, as it can be seen from Figure 6-10b the RSVP signaling delay for the proposed protocol is relatively smaller than maximum allowed delay for all handover instants, ensuring QoS for the new path. This is obvious, since RSVP signaling messages have to pass through the uncongested links between access routers, while traffic has to pass all links from CH to access router including the congested link between CH and the gateway. For the handover from subnetwork 4 to subnetwork 5, RSVP signaling delay for the proposed protocol is higher than for other handover instants, because in this case the gateway serves as NCR. For the conventional protocol, similar to access congestion case, RSVP signaling delay is much longer than maximum allowed delay. This means that QoS is not ensured for the packets, which are issued with the new CoA before RSVP signaling reserves the new path.

Simulation results for no congestion scenario, Figure 6-10c, show that the absolute difference between RSVP signaling delays at all handover instants of the two protocols is far smaller than that of the scenarios with traffic congestion. However, the relative reduction of signaling delay obtained by proposed protocol is still very high, ranging from 53% to 87 %. Similar to congestion scenarios, the RSVP signaling delay in the no congestion scenario for the proposed protocol is relatively smaller than maximum allowed delay for all handover instants, ensuring QoS. For conventional protocol the RSVP signaling delay is relatively longer than maximum allowed delay. However, in this case the difference between RSVP signaling delay and the maximum allowed delay is much smaller than in congestion scenarios, which results in smaller number of packets that lack QoS until the BU is processed in the CH and before QoS for the new path is ensured.

As can be seen from this performance evaluation, BU was not specifically measured. It is the part of the maximum allowed delay for QoS provisioning and it is the same for all protocols. The maximum allowed delay can be estimated from Equation (6.1), which is an extension of Equation (4) [She01]:

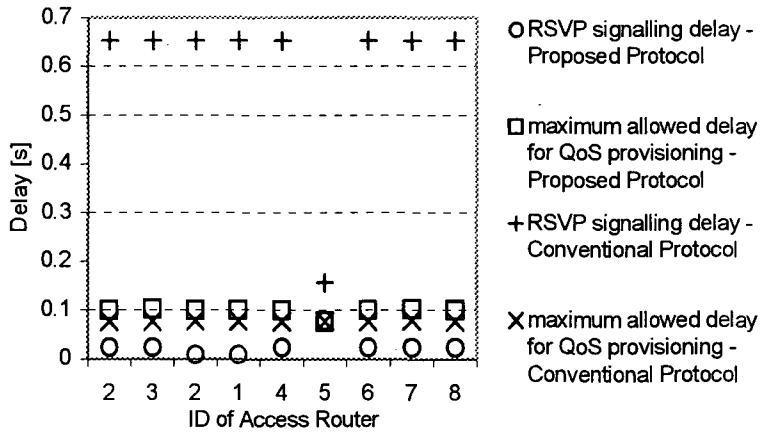
$$d_{\max-allowed} = \sum_{i=1}^{m} d_i + \sum_{j=1}^{n} \frac{s_{pkt}}{bwr_i} + \sum_{k=1}^{s} d_k. \qquad (6.1)$$

First part of Equation (6.1) presents the binding update delay, the second part the transmission delay, and the third part the propagation delay. Here m is the number of links from MH to CH, d_i is the delay of the i-th link, n is the number of congested links along the real-time traffic path, s_{pkt} is the size of the packets, b_{wrj} is the reserved bandwidth for the traffic in link j, s is the total number of links along the path from CH to NCR and d_k is the delay of the k-th link. Given a packet size of 500 bytes and a reserved bandwidth of 500 kbit/s, the approximate maximum allowed delay for the proposed protocol is as follows:

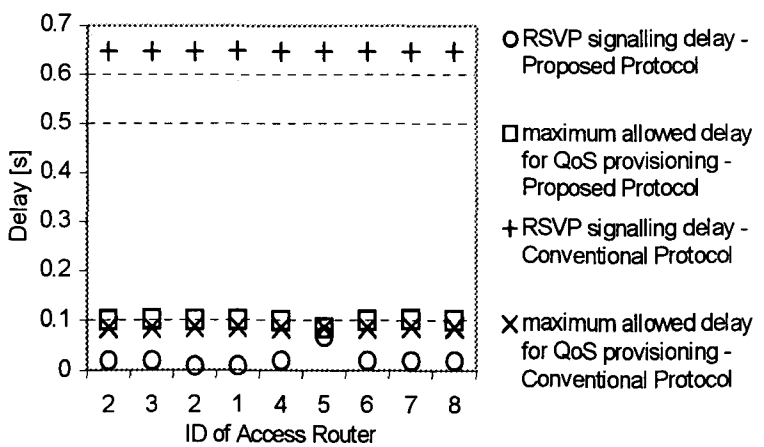
- For no congestion case in the range 76 ms to 93 ms,
- For access network congestion in the range 76 ms to 101 ms,
- For core network congestion in the range 84 ms to 101 ms.

This matches with the simulation results given in Figure 6-10. Note that for the no congestion scenario the second part of Equation (6.1) is zero because there are no congested links. Also for access congestion scenario, in case of the handover from subnetwork 4 to subnetwork 5 there are no congested links involved. For all other cases of the handover for access network congestion, only the link from gateway to node 13 or 14 is congested. For core congestion scenario is always involved only the congested link between CH and gateway. From Figure 6-10, we can also notice that the RSVP signalling delay and maximum allowed delay distribution of the proposed protocol and the conventional protocol is symmetric, at handover instant from subnetwork 4 to subnetwork 5. This is simply due to the symmetry of the network topology itself.

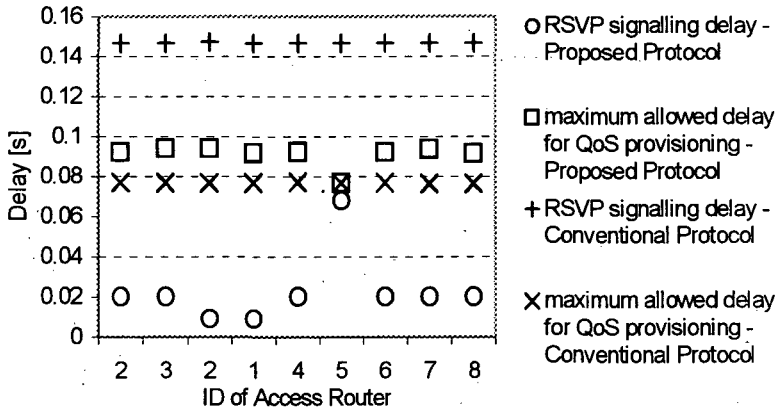
Figure 6-11 shows the simulation results for the proposed protocol and the conventional protocol for Topology 1, assuming mobility scenario 2 (mobility pattern 1-2-3-2-1-4-5-6-7-8). Traffic load is same as in the case of mobility scenario 1.



a) Access network congestion in Topology 1



b) Core network congestion in Topology 1



c) No congestion in Topology 1

Figure 6-11: Proposed and Conventional Protocol, Topology 1, Mobility Scenario 2.

From the plots, one sees that with proposed protocol, for all three congestion scenarios, the results differ from that of mobility scenario 1 mainly on RSVP signalling delay at handover instants from subnetwork 3 back to subnetwork 2 and from subnetwork 2 to subnetwork 1. The relative reduction of RSVP signaling delay obtained in proposed protocol by applying mobility scenario 2 is 62% for the access network congestion scenario, while for core congestion and no congestion is about 54 %. An explanation is that the reserved path between access routers already exists and the delay is only due to the path-state discovery procedure applied in our protocol (PathState_discovery and PathStat_reply messages). As expected, mobility scenario 2 has no impact on RSVP signaling delays for conventional protocol since links between access routers are not involved in signaling path. Therefore, with mobility scenarion 2 differences between RSVP signalling delays for the proposed protocol and the conventional protocol are more pronounced at handover instants when MH moves back to previous subnetwork.

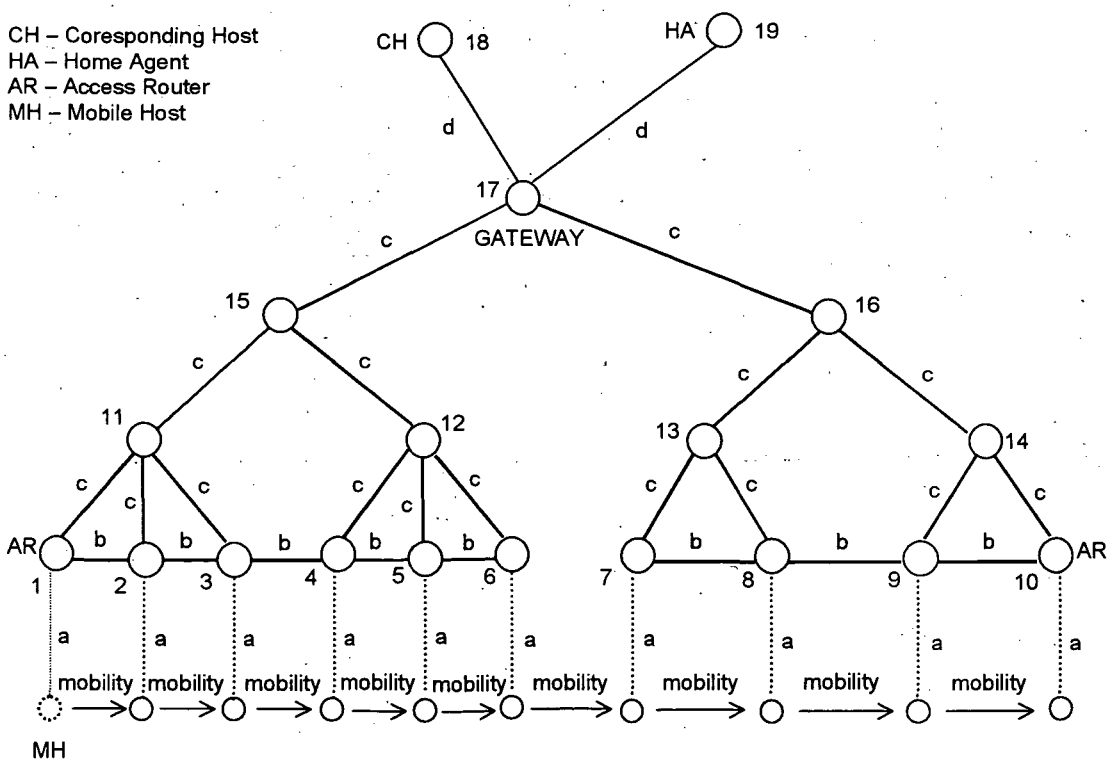
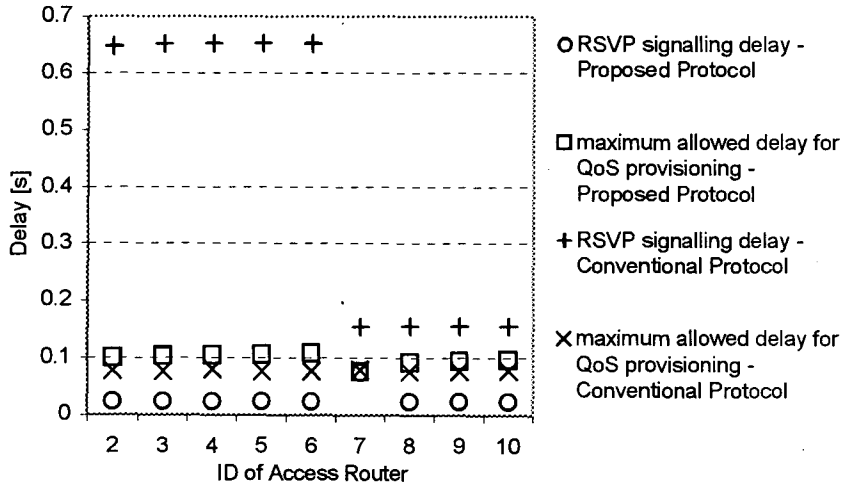


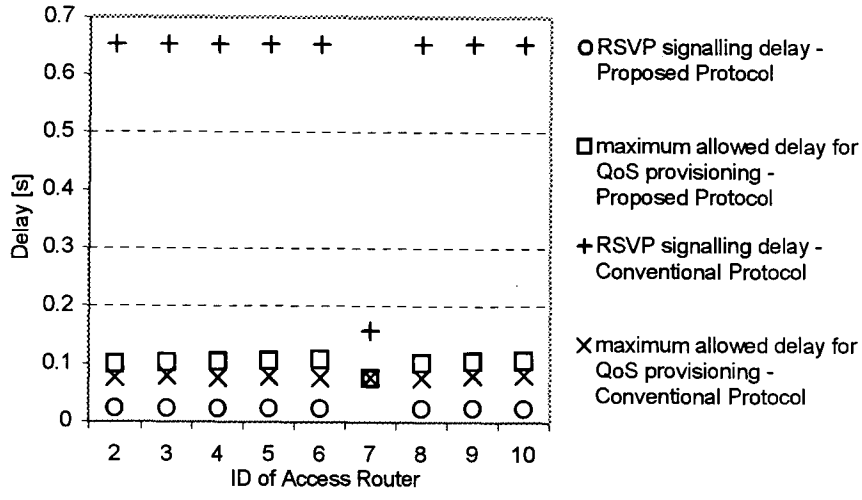
Figure 6-12: Network Topology 2

Figure 6-12 shows the simulated Topology 2, which contains ten access routers (subnetworks) that are divided into two groups. Six access routers of the first group form a meshed network and four access routers of the second group form another meshed network. Therefore, different to Topology 1, Topology 2 is not symmetric. Similar to Topology 1, three congestion scenarios in combination with two mobility scenarios are simulated for Topology 2.

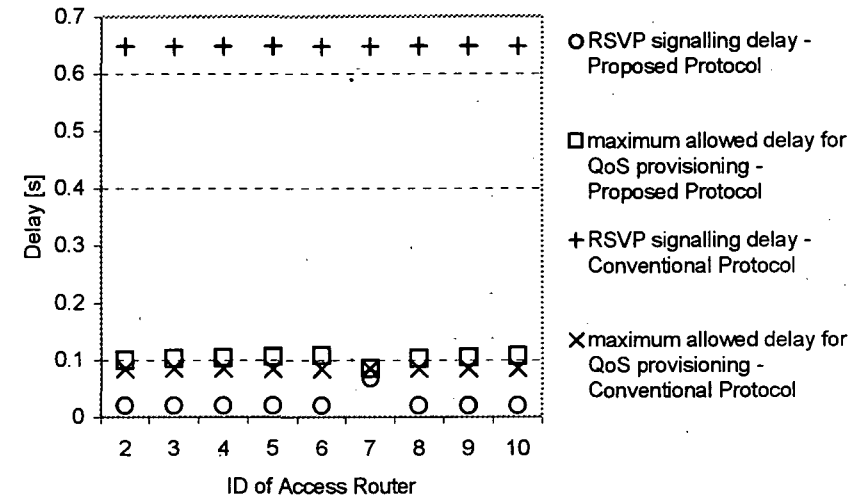
- For access network congestion, we have simulated two scenarios: congestion only on the left part of the access network and congestion on both left and right part of the access network. For access congestion only on the left part of the access network the background traffic of 10 x (5 x 64 kbit/s) = 3.200 kbit/s was generated. Therefore, the 2 Mbit/s link between nodes 17 (gateway) and node 15 is loaded with 6 x (5 x 64 kbit/s) + 500 kbit/s = 2.420 kbit/s, which causes congestion, while the 2 Mbit/s link between gateway and node 16 is loaded with 4 x (5 x 64 kbit/s) + 500 kbit/s = 1.780 kbit/s, which cannot cause congestion. Simulation results for access congestion scenarios are shown in Figure 6-13a and Figure 6-13b, respectively.



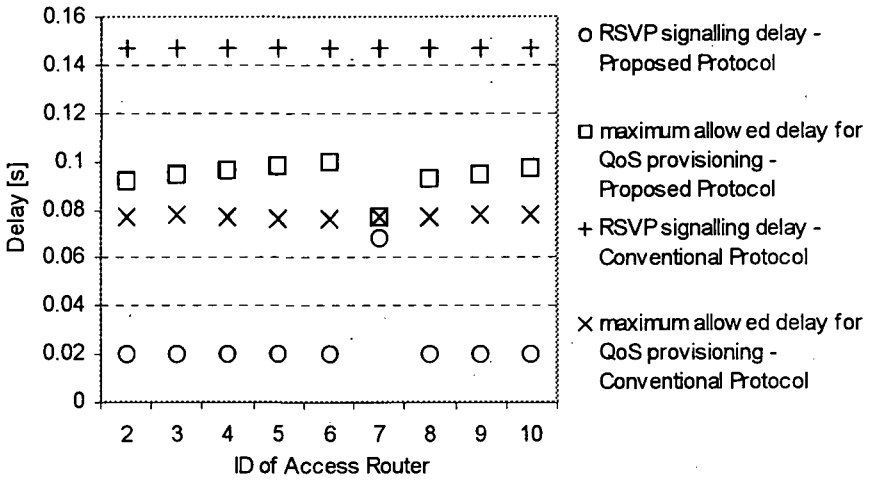
a) Access network congestion on the left side of Topology 2



b) Access network congestion on both sides of Topology 2



c) Core network congestion in Topology 2



d) No congestion in Topology 2

Figure 6-13: Proposed and Conventional Protocol, Topology 2, Mobility Scenario 1

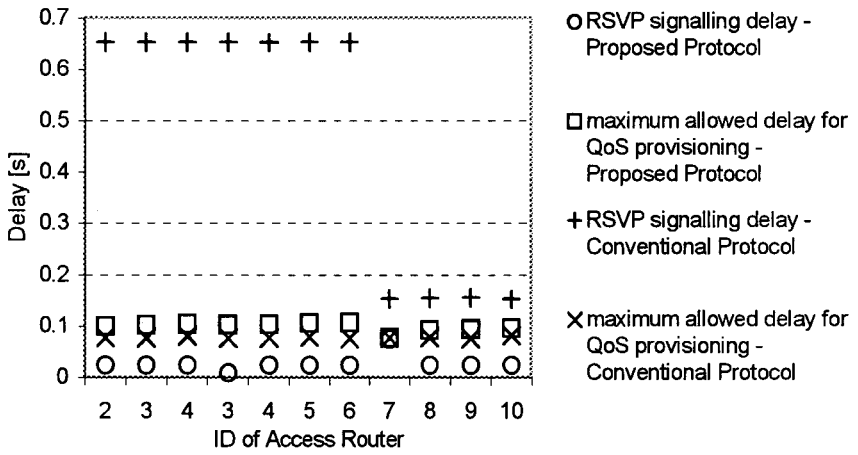
From the plot shown in Figure 6-13a it can be seen that asymmetric network topology has no impact on RSVP signalling delay for the proposed protocol. An explanation is that in the proposed protocol access routers are used as NCR, with an exeption at handover instant from subnetwork 6 to subnetwork 7, when gateway serves as NCR. For the conventional protocol it can be noticed that RSVP signalling delay at handover instants on the congested left part of the network are much higher than on the uncongested right side of the network. Considering maximum allowed delay for the proposed protocol, the impact of the asymmetric topology is that maximum allowed delays are longer on the left part of the network because traffic has to go through congested link between gateway and node 13. An addition delay is due to greater number of the access routers that traffic has to go through to reach the MH at subnetworks 5 and 6. The RSVP signalling delay for the proposed protocol at all handover instants is larger than maximum allowed delays, ensuring QoS provision at all handover instants. For the conventional protocol, similar to Topology 1, the RSVP signalling delay is larger than maximum allowed delay at all handover instants. However, this difference is much smaller for the uncongested part of the network, which results in smaller number of packets that lack QoS until the BU is processed in the CH and before QoS for the new path is ensured.

- For the second scenario of the access congestion of the asymmetric Topology 2, simulation results presented in the Figure 6-13b show that RSVP signalling delay and maximum allowed delay for both protocols are similar to access congestion scenario in Topology 1. Therefore all the discussions presented for Topology 1, also apply here.

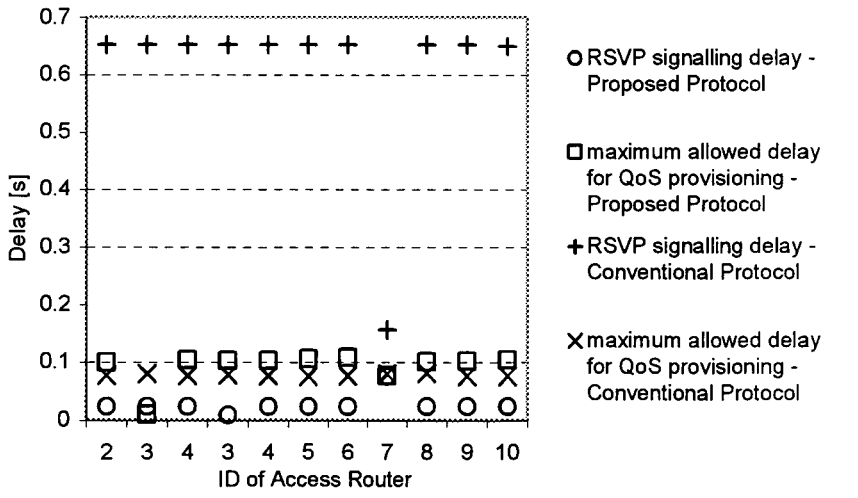
- For the core network congestion, the 2 Mbit/s link between CH and gateway is loaded with 10 x (3 x 64 kbit/s) + 500 kbit/s = 2.420 kbit/s, which causes congestion in the core network. From the simulation results shown in Figure 6-13c, one sees that asymmetric topology has no additional impact to those discussed for Topology 1, on the RSVP signalling delay neither on maximum allowed delay. Therefore, the simulation results are similar to Topology 1 for the case of core congestion. An explanation is that in the core congestion scenario the congested link between CH and gateway has the main impact on RSVP signalling delay for conventional protocol and maximum allowed delay for both protocols.

- For the no-congestion scenario, we have generated traffic load of 10 x (6 x 64 kbit/s) + 500 kbit/s = 4.340 kbit/s, which does not cause congestion on the links with 10 Mbit/s bandwidth. Simulation results presented in Figure 6-13d show that as long as there is no congestion on the links, asymmetric topology has no additional effect, besides those already discussed for the Topology 1 with no congestion scenario.

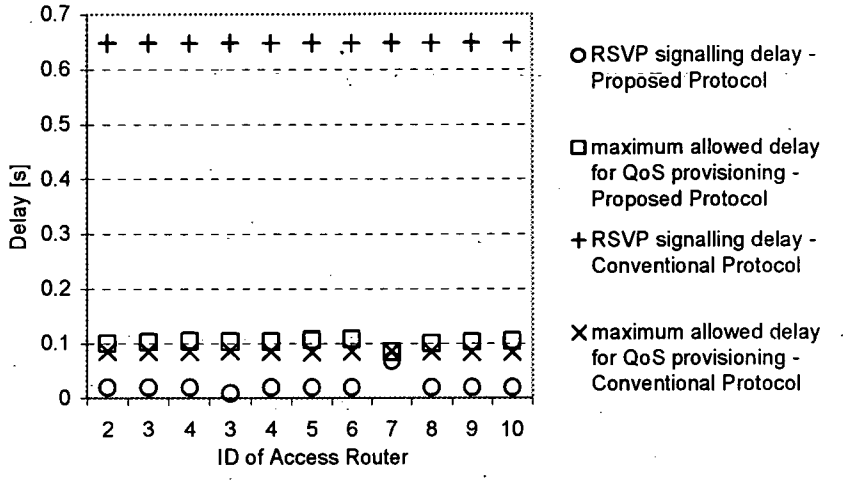
Topology 2 was also simulated assuming mobility scenario 2 (1-2-3-4-3-4-5-6-7-8-9-10) and the same congestion scenarios as with mobility 1. Simulation results are shown in Figure 6-14.



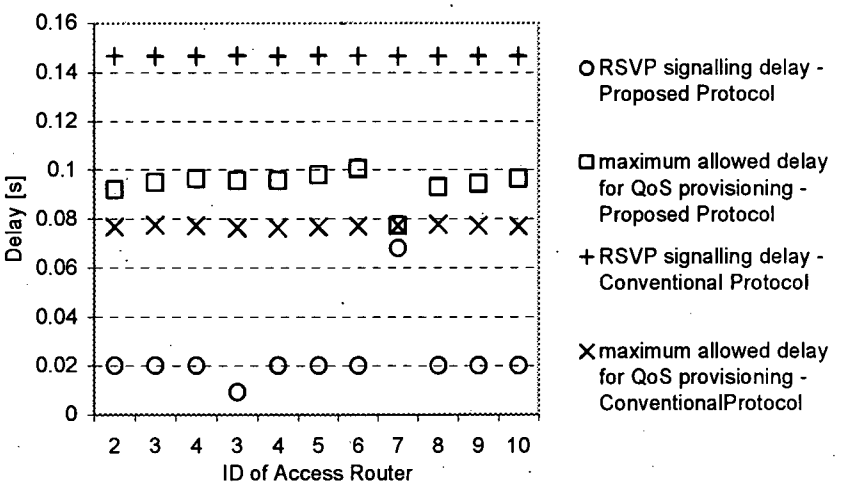
a) Access network congestion on the left side of the Topology 2



b) Access network congestion on both sides of the Topology 2



c) Core network congestion in Topology 2



d) No congestion in Topology 2

Figure 6-14: Proposed and Conventional Protocol, Topology 2, Mobility Scenario 2

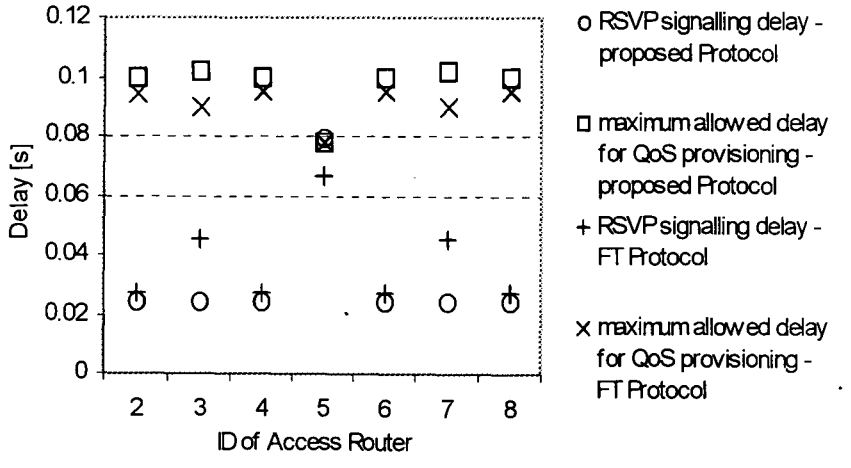
From the plots in Figure 6-14, it can be seen that with proposed protocol, for all three congestion scenarios, the results differ from that of mobility scenario 1 mainly on RSVP signalling delay at handover instants from subnetwork 4 back to subnetwork 3. The relative reduction of RSVP signaling delay obtained in proposed protocol by applying mobility scenario 2 is 62% for the access network congestion scenarios, while for core congestion and no congestion is about 50 %. An explanation is that the reserved path between access routers already exists and the delay is only due to path state discovery procedure applied in our protocol (PathState_discovery and PathState_reply messages). Therefore, the impact of the mobility scenario 2 with Topology 2 is similar to the impact of the mobility scenario 2 with the Topology 1, for both protocols and for all congestion scenarios.

Comparison of the proposed protocol and the FT protocol

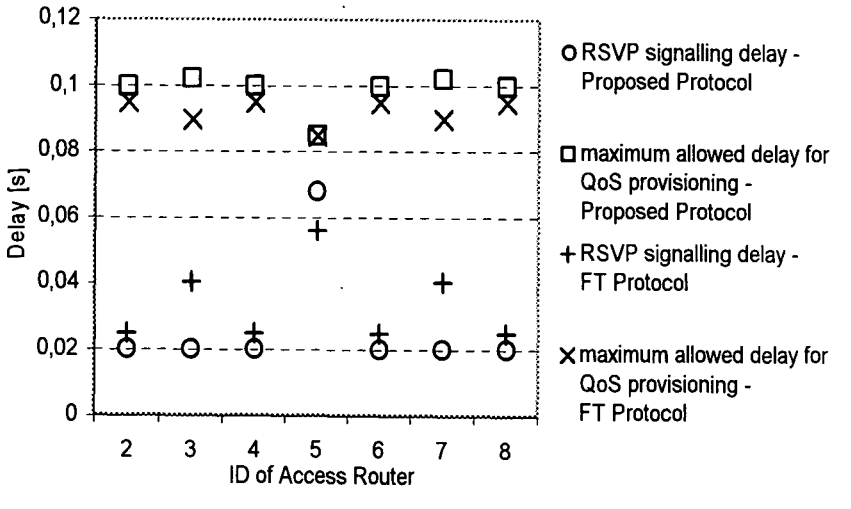
As it was mentioned in the paragraph 6.4.2.2, the proposed protocol is based on an existing Flow Transparency (FT) Mobile IP and RSVP interworking scheme and can be considered as its compliment for meshed access network topologies. Therefore, in this subsection we will com-

pare the proposed protocol and FT protocol, applying the simulation environment as in the case when we compared proposed protocol and conventional protocol. The simulation results for the proposed protocol and the FT protocol for Topology 1 (Figure 6-8), assuming mobility scenario 1 and all three congestion conditions, are shown in Figure 6-15.

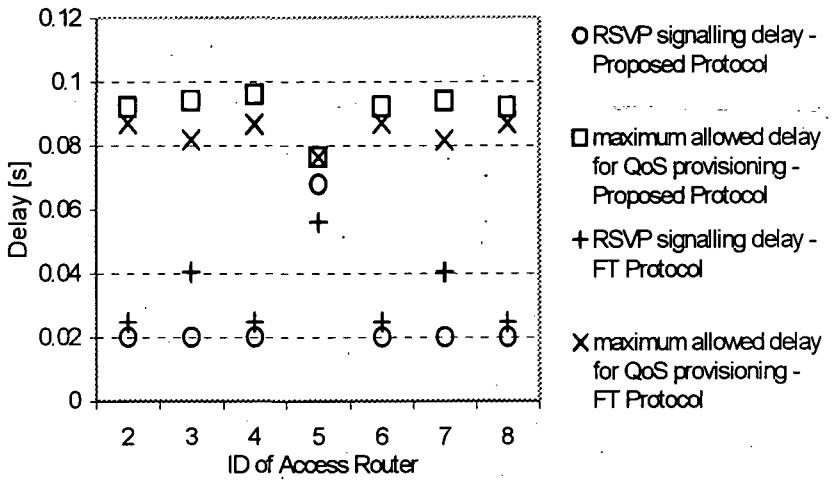
For the case of access network congestion, Figure 6-15a shows that the proposed protocol results in lower RSVP delays at all handover instants except during the handover from subnetwork 4 to subnetwork 5 (where there is no direct link between access routers 4 and 5). The relative reduction of the RSVP signalling delays is 11% when routers 9, 10, 11 and 12 serve as Nearest Common Router (NCR), whereas 46% when routers 13 and 14 serve as NCR for the FT protocol. An explanation is that at all these handover instants in the case of the proposed protocol previous access routers serve as NCR, whereas for FT protocol routers that serve as NCR belong to different levels of the network hierarchy, resulting in longer RSVP signalling delays. At handover instant from subnetwork 4 to subnetwork 5 signalling delay for the proposed protocol is increased by 16 %, because in this case the NCR for both protocols is node 15 (gateway) and the path state discovery procedure applied in our protocol (PathState_discovery and PathStat_reply messages) results in longer RSVP signalling delays in comparison to the FT scheme.



a) Access network congestion in Topology 1



b) Core network congestion in Topology 1



c) No congestion in Topology 1

Figure 6-15: Proposed and FT Protocol, Topology 1, Mobility Scenario 1

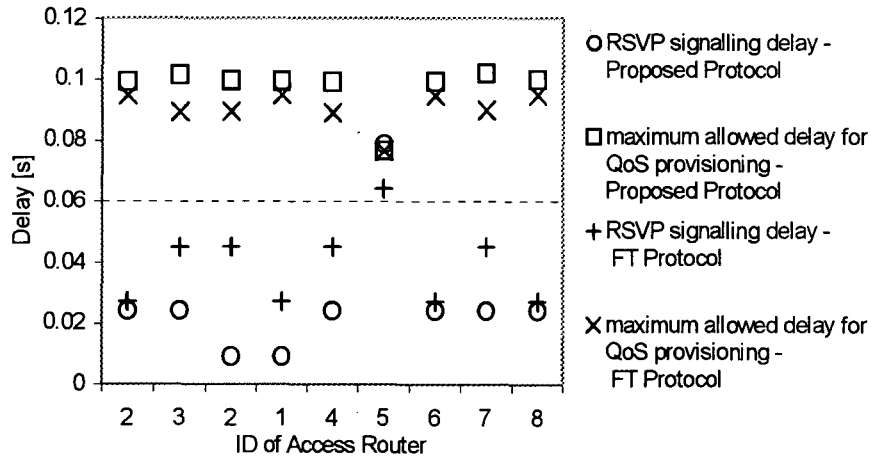
Furthermore, from the simulation results it can be seen that for both protocols the RSVP signalling delay is relatively smaller than the maximum allowed delay for QoS provisioning at all handover instants, exept during the handover from subnetwork 4 to subnetwork 5. Therefore, the resource reservation in the new flow path is settled before the packet transmission starts along the new path. This means that during all handover instants, both protocols ensure QoS provisioning for all packets that use the new CoA. At the handover instant from subnetwork 4 to subnetwork 5, RSVP signalling delay and maximum allowed delay are almost equal, for both protocols. An explanation is that in this case the gateway is the NCR, resulting in longer RSVP delays in comparison to the other handover instants, and the maximum allowed delay also is much shorter than in other handover instants, because only the uncongested link between CH and NCR is involved. The plot also shows that the maximum allowed delay for QoS provisioning is longer in the case of the proposed protocol, because the NCR is located closer to the MH than in the case of FT protocol. The handover from subnetwork 4 to 5 is an exception, where the values are equal because in this case gateway serves as NCR for both protocols.

For the core congestion scenario, simulation results are shown in the Figure 6-15b. Similar to the access congestion scenario, the proposed protocol results in the reduction of the RSVP signaling delays at all handover instants except at handover from subnetwork 4 to subnetwork 5. The relative reduction is 18.5% when nodes 9, 10, 11, and 12 serve as NCR, whereas 50% at handover instants when nodes 13 and 14 serve as NCR for the FT protocol. At handover instant from subnetwork 4 to subnetwork 5 signalling delay for the proposed protocol is increased by 16,7%. Explanation for the difference in signalling delays between two protocols is same as in the case of access congestion scenario. Furthermore, the RSVP signalling delays for FT protocol, similar to proposed protocol, is much shorter than maximum allowed delay at all handover instants, ensuring QoS for real-time traffic transmitted from CH to MH. The RSVP signalling delay for FT protocol has the highest value at handover instant when the gateway serves as NCR. Similar to access congestion case, the maximum allowed delay is longer for the proposed protocol than for FT protocol, except for the handover from subnetwork 4 to 5, where the values are equal.

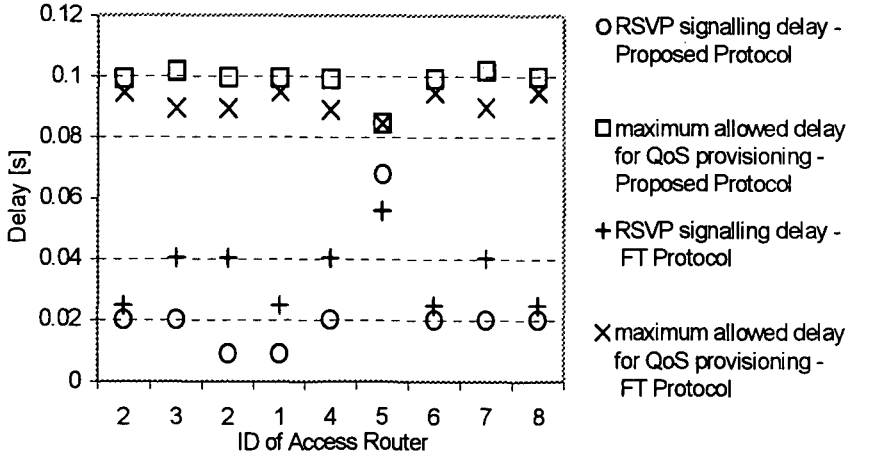
Figure 6-15c shows the simulation results for the no congestion case. Similar to congestion cases, the RSVP signaling delays for the proposed protocol is shorter than for FT protocol, exept at handover instants from subnetwork 4 to subnetwork 5 (when there is no link in between). Explanation for the difference in signalling delays between two protocols is same as in the case of access congestion scenario. The relative reduction of the RSVP signaling delays are similar to congestion scenario, since RSVP signaling messages for both protocols do not pass through the core network at any handover instant. Furthermore, the RSVP signaling delays are

smaller than maximum allowed delays at all handover instants for both protocols. The maximum allowed delays are smaller than in congested scenarios, because transmission delay is negligible since there are no congested links involved. From Figure 6-15, one sees that the RSVP signalling delay distribution of the proposed protocol and the FT protocol is symmetric, around the value when gateway serves as Nearest Common Router, due to the symmetry of the network topology.

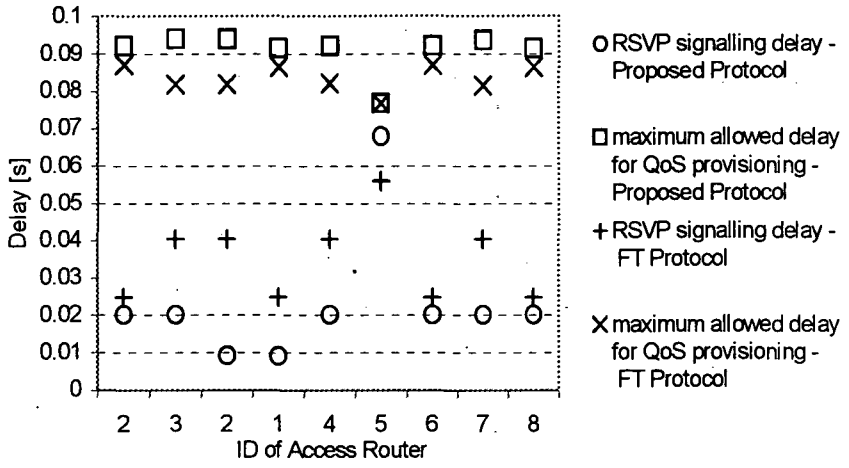
We have also simulated the FT protocol assuming mobility scenario 2 (mobility pattern 1-2-3-2-1-4-5-6-7-8). Figure 6-16 shows the simulation results for the FT protocol and the proposed protocol for Topology 1, with the same traffic load as in the case of mobility scenario 1. From the plots it can be seen that mobility scenario 2 results in reduction of signalling delay with proposed protocol at handover instants from subnetwork 3 back to to subnetwork 2 and from subnetwork 2 to subnetwork 1, for all three congestion scenarios. The relative reduction of RSVP signaling delay obtained in proposed protocol by applying mobility scenario 2 ranges from 66% (handover from subnetwork 2 to subnetwork 1) to 76% (handover from subnetwork 3 to subnetwork 2) for access network congestion scenario, while for core congestion and no congestion ranges from 63% to 77%. An explanation is that in the case of proposed protocol the reserved path between access routers already exists and the delay is only due to path state discovery procedure applied in our protocol (PathState_discovery and PathState_reply messages). For the FT protocol the signalling path during the handover from subnetwork 3 to subnetwork 2 involves more links than in the case of handover from subnetwork 2 to subnetwork 1, resulting in longer signalling delays. To conclude, when MH moves back to the previous subnetwork (where there is direct link in between) with the proposed protocol the path reservation is provided very fast.



a) Access network congestion in Topology 1



b) Core network congestion in Topology 1



c) No congestion in Topology 1

Figure 6-16: Proposed Protocol and FT Protocol, Topology 1, Mobility Scenario 2

Aditional analyses of the proposed protocol

In order to show some additional features of the proposed protocol and of the meshed access network topologies, we have farther investigated the impact of meshed access network to RSVP signaling delays as well as the impact of the proposed protocol on traffic distribution over the links of the access network for different network topologies and different number of MHs. Therefore, in addition to Toplogy 1 (Figure 6-8), where access routers are meshed we have also simulated the Topology 3 shown in Figure 6-17, where access routers are not meshed.

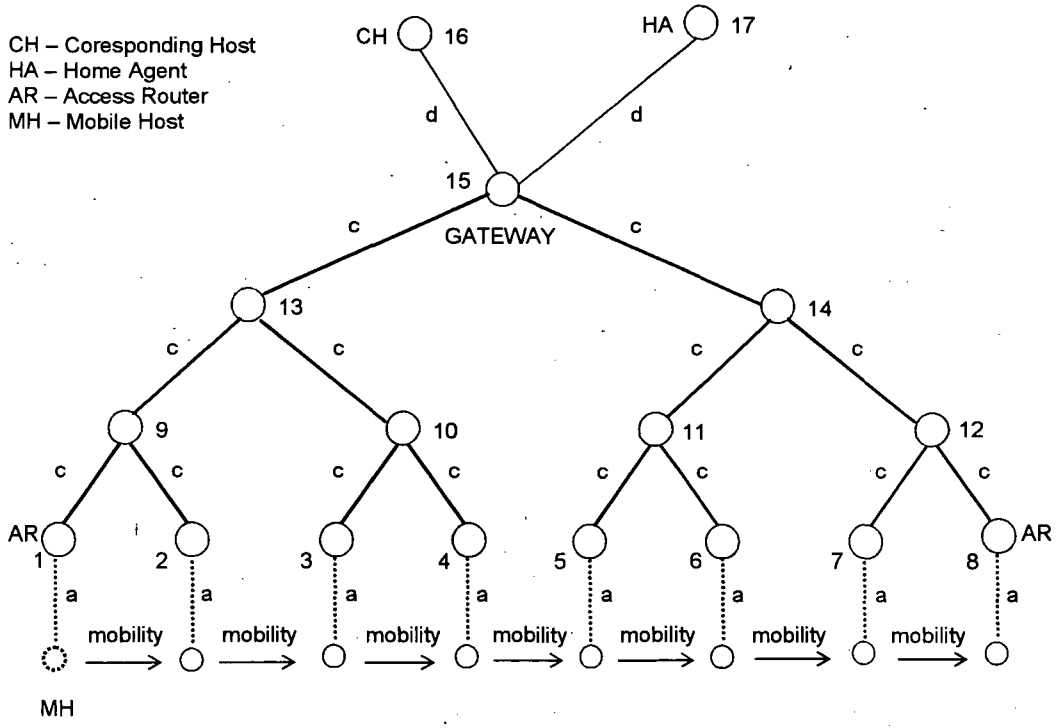
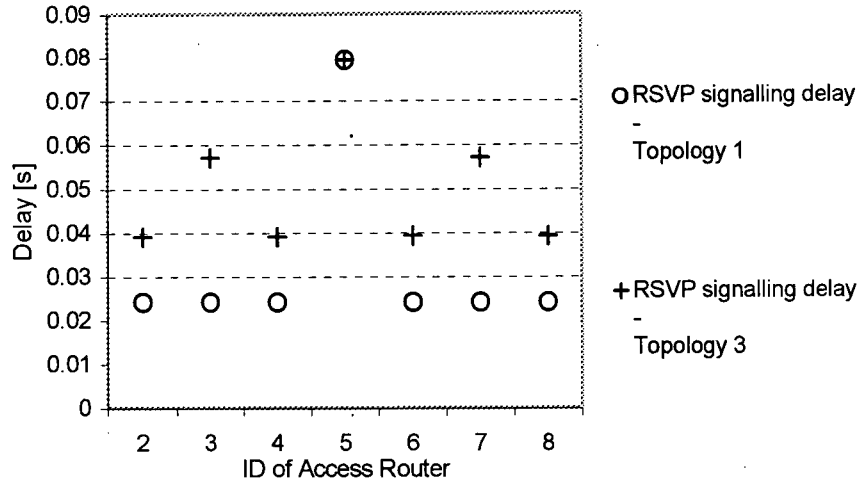
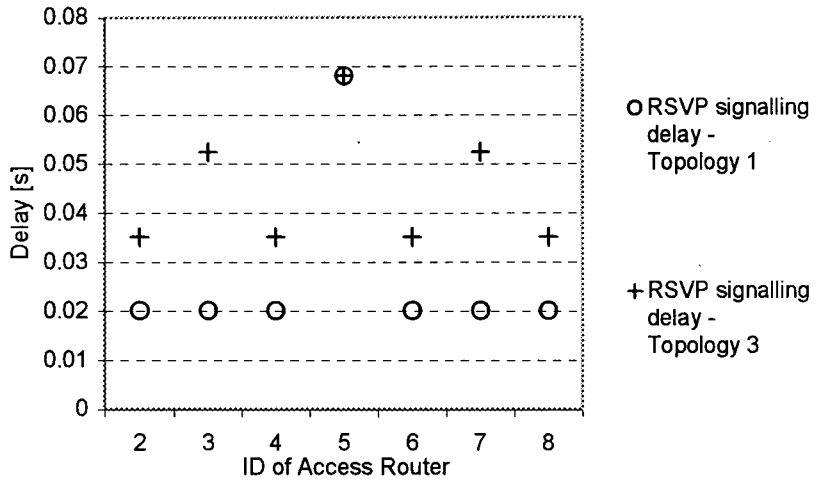


Figure 6-17: Network Topology 3

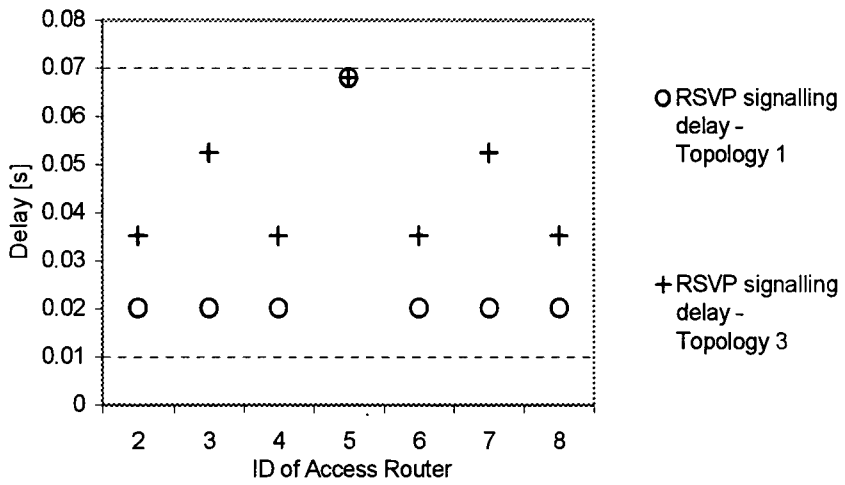
Topology 3 is simulated assuming the same traffic load and congestion conditions, as for Topology 1. Simulation results for both topologies, Topology 1 and Topology 3 are shown in Figure 6-18.



a) Access network congestion



b) Core network congestion

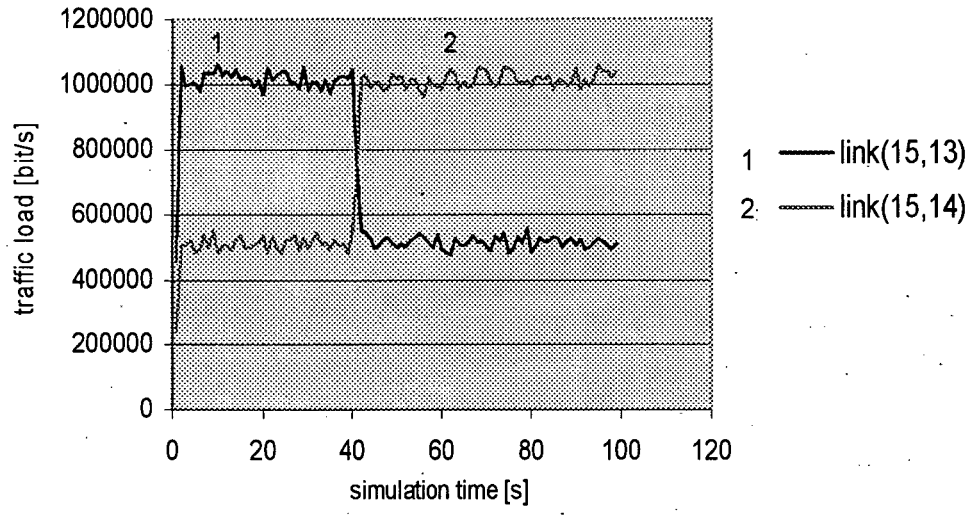


c) No congestion

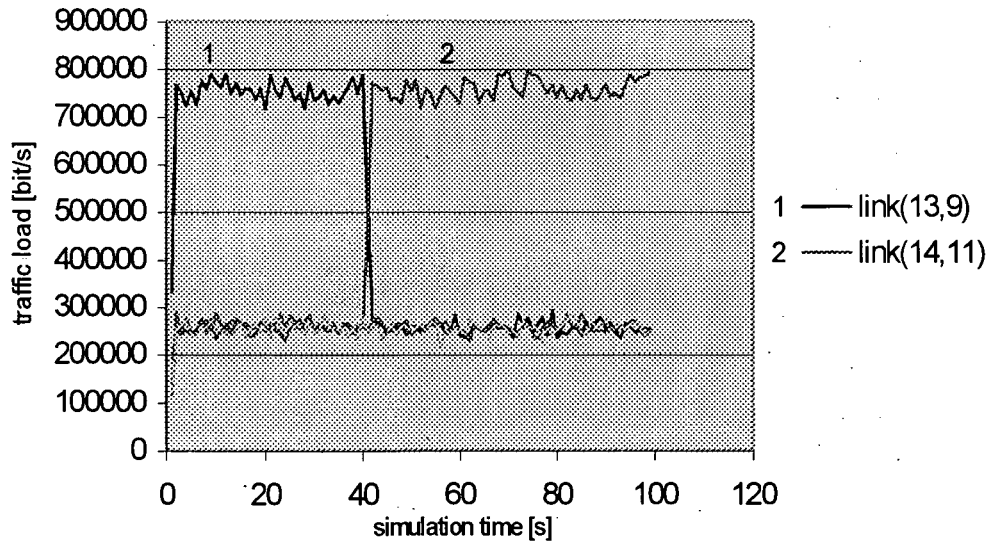
Figure 6-18: RSVP signaling delay for Topology 1 and Topology 3, proposed protocol

As it can be seen from the Figure 6-18, RSVP signaling delays for Topology 1 with meshed access routers is shorter than for unmeshed Topology 3, at all handover instants, except during the handover from subnetwork 4 to subnetwork 5, where these values are equal. An explanation is that for Topology 1, access routers serve as NCR, whereas for Topology 3, access routers belong to different levels of network hierarchy, resulting in longer RSVP delays. For the handover from subnetwork 4 to subnetwork 5 the gateway serves as NCR for both topologies. The reduction of the RSVP delays for Topology 1 ranges from 38% to 57% for access congestion scenario, whereas for core congestion and no congestion scenario from 42% to 57%. The values for core congestion and no congestion are equal because the core congestion has no impact on RSVP signaling delays for the proposed protocol, since non of the RSVP signaling messages needs to go through the core network during the handover. Conclusion is that the proposed protocol shows better performances when access routers are meshed

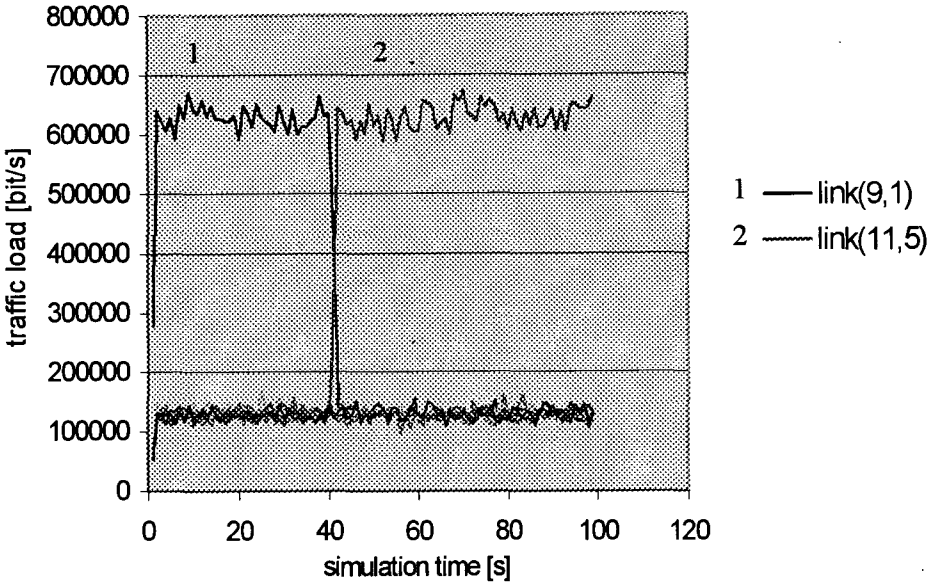
Figure 6-19 shows the traffic distribution on different links of the Topology 1, assuming background traffic load of 8 x (2 x 64 kbit/s) and 500 kbit/s real-time traffic load from CH to MH. Initially MH is located in the subnetwork 1, and then it moves along the subnetworks 1-2-3-4-5-6-7-8, at time intervals of 10 s. Curves on the upper part of the Figure 6-19a, 6-19b, and 6-19c, show the total traffic, whereas curves on the buttom show the background traffic.



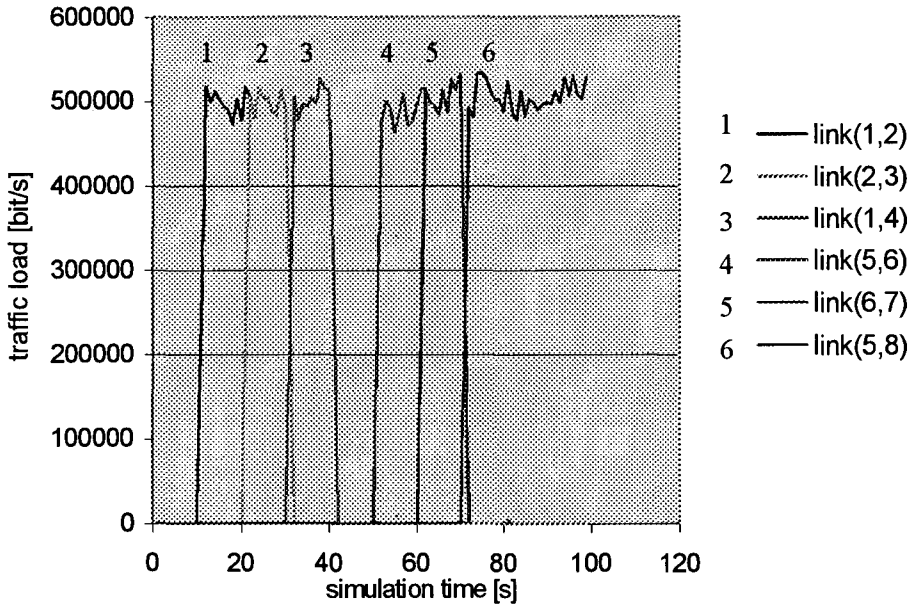
a) Traffic load on links between gateway and routers on the third level



b) Traffic load on links between routers of the second and third level



c) Traffic load on links between access routers and routers on second level



d) Traffic load on links between access routers

Figure 6-19: Traffic load distribution in Topology 1

As it can be seen from the Figure 6-19a, 6-19b and 6-19c traffic always flows along the reserved path 15-13-9-1, as long the MH moves within the subnetworks on the left of the Figure 6-8 with access routers meshed. When MH moves from subnetwork 4 to subnetwork 5 (at time instant of 40 s), then traffic flows along the reserved path 15-14-11-5, as long as MH moves within the subnetworks on the right side of the Figure 6-8, with access routers meshed. For example total traffic load on the link between nodes 9 and 1 is 500 kbit/s + 128 kbit/s = 628 kbit/s. The 500 kbit/s due to traffic from CH to MH and 128 kbit/s is the background traffic destinated to access router 1. Along all other links flows only background traffic. When MH moves from subnetwork 4 to subnetwork 5 then link 11-5 is loaded with 628 kbit/s, whereas along all other links flows only background traffic. This shows the specific characteristic of the proposed protocol that traffic load on the links that connect initial access router of the MH to Nearest Common Router (NCR) and other routers on the network hierarchy until to the gateway remains constant

as long as MH moves between access routers that form a meshed access network. This feature gives the possibility to control the distribution of the traffic load on the access network. Therefore, dimensioning of the network is more accurate when number of home mobile users for each access routers is known. For example in WLAN environment the number of potential mobile users for each access points is a priory planed, hence the traffic load on the links in access networks can also be estimated.

Figure 6-19d shows the traffic load on the links between access routers. This is a 500 kbit/s real-time traffic load transmitted from CH to MH. The plot shows that when MH moves from subnetwork 3 to subnetwork 4, traffic is carried along the direct link between access router 1 and access router 4. This is the case described in the paragraph 1.4.2.2, when mobile host is a receiver and two or more adjacent routers have a path state then the access router selects the next hop router, based on the routing table, and forwards the PathReq_message. In our example both access router 3 and the access router 1 have the path state. The access router 4 has selected access router 1 to forward the PathReq message. Access router 1 replays with Path message. Having received the Path message from access router 1, the access router 4 sends the Resv message to reserve the bandwidth. Similarly, when MH moves from subnetwork 7 to subnetwork 8, the access router 8 has selected the access router 5 to forward PathReq and having received the Path message reserves the bandwidth between access routers 5 and 8.

Topology 1 was extended to Topology 4, which contains two MHs, two CHs and two HAs, as shown in Figure 6-20. The MH1 is initially located in subnetwork 1 and it moves in the following pattern: 1-2-3-4-5-6-7-8, whereas the MH2 is initially located in the subnetwork 8 and it moves in the pattern 8-7-6-5-4-3-2-1. In addition to the background traffic load of 8 x (2 x 64 kbit/s) transmitted to each access router, CH1 transmits 500 kbit/s real-time traffic to MH1, whereas CH2 transmits 250 kbit/s real-time traffic to MH2.

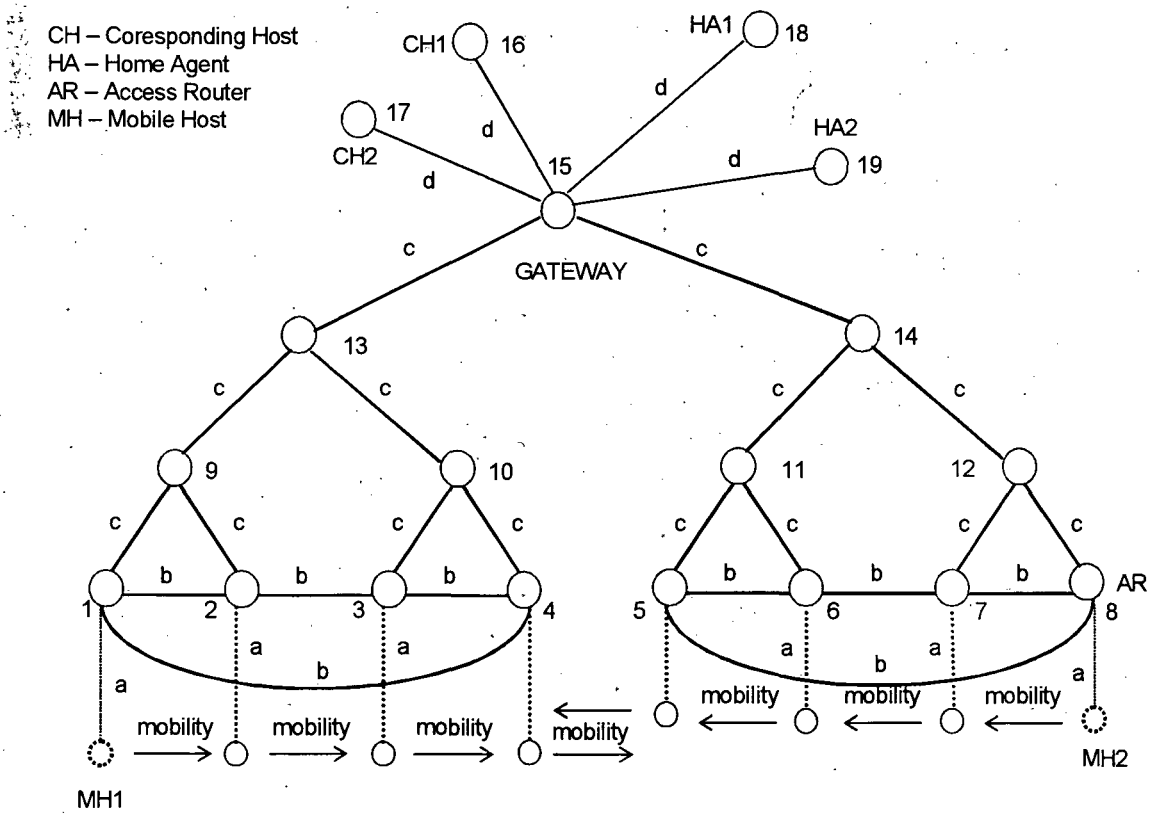
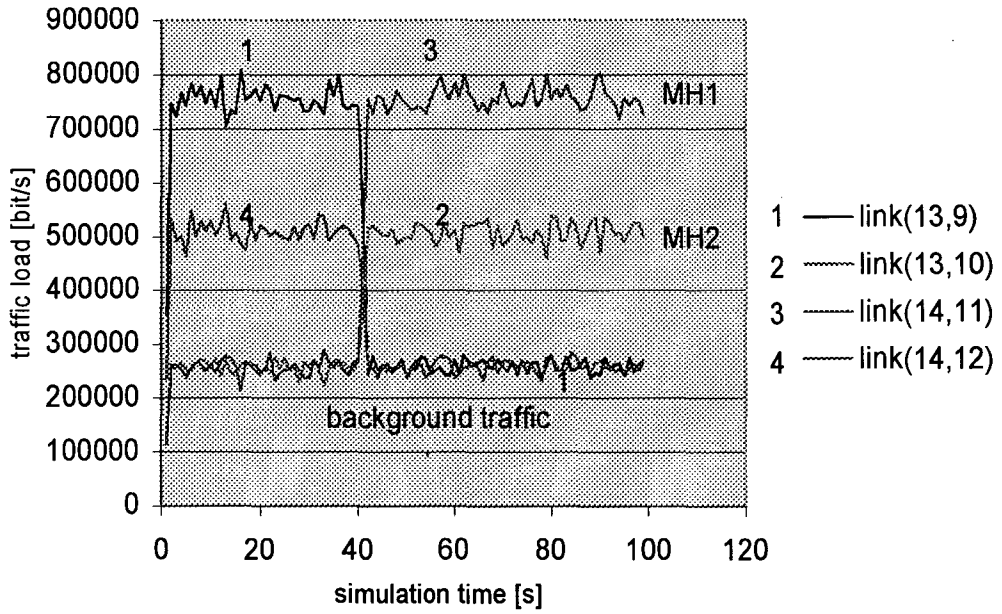
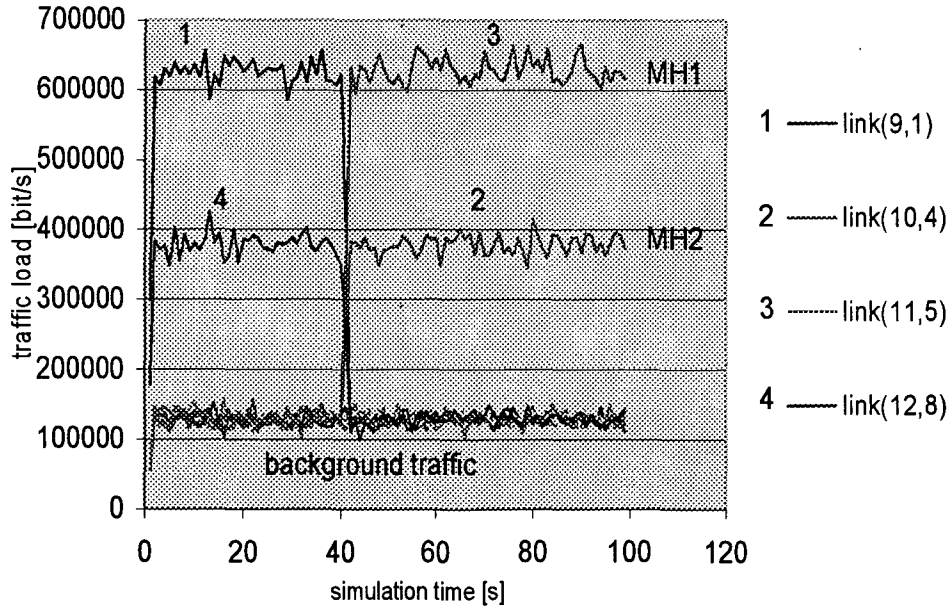


Figure 6-20: Network Topology 4

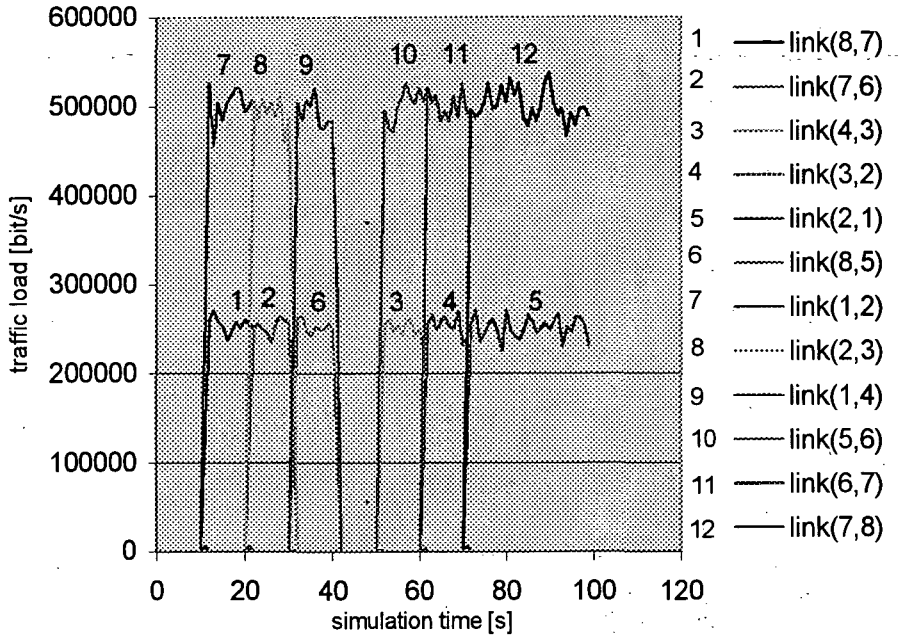
The traffic distribution on different links of the Topology 4 is shown in Figure 6-21. Curves on the upper part of the Figure 6-21a and Figure 6-21b show the traffic from CH1 to MH1 and the background traffic, curves in the middle show the traffic from CH2 to MH2 and the background traffic, whereas curves on the button show the background traffic. From these plots, we can notice again that traffic load on the links remains constant as long as MHs move within subnetworks with meshed access routers. If we consider for example traffic load on links between routers on the third level (routers 13 and 14) and second level (routers 9, 10, 11, and 12) in Figure 6-21a, it can be seen that traffic load on the link between nodes 13 and 9 is 2 x 128 kbit/s + 500 kbit/s = 756 kbit/s. The 500 kbit/s is the traffic from CH1 to MH1 and 2 x 128 kbit/s is the background traffic destined to access router 1 and 2. Similarly link between 14 and 12 is loaded with 2 x 128 kbit/s + 250 kbit/s = 506 kbit/s. The 250 kbit/s is the traffic from CH2 to MH2, whereas 2 x 128 kbit/s is the background traffic destined to access routers 8 and 7.



a) Traffic load on links between routers of the second and third level



b) Traffic load on links between access routers and routers on the second level



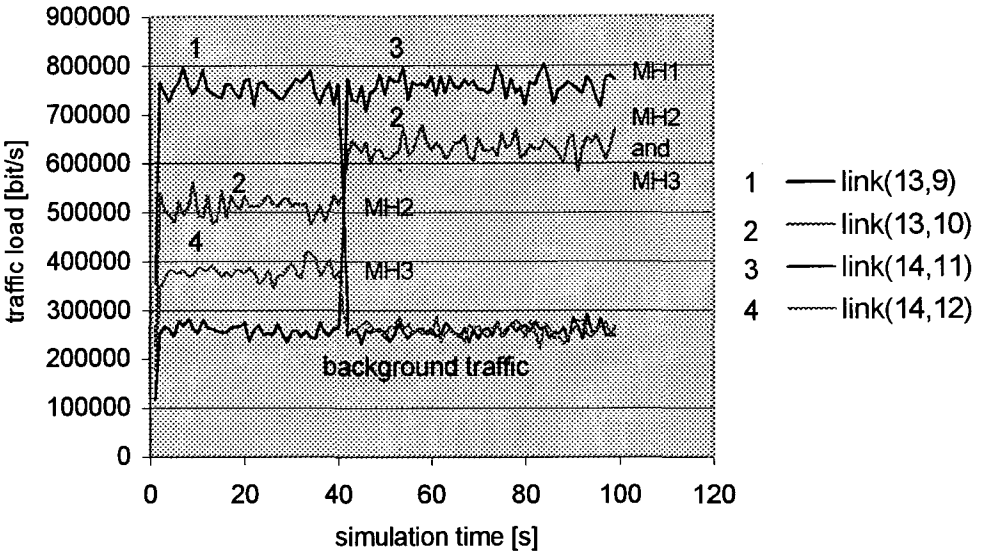
c) Traffic load on links between access routers

Figure 6-21: Traffic load distribution for Topology 4

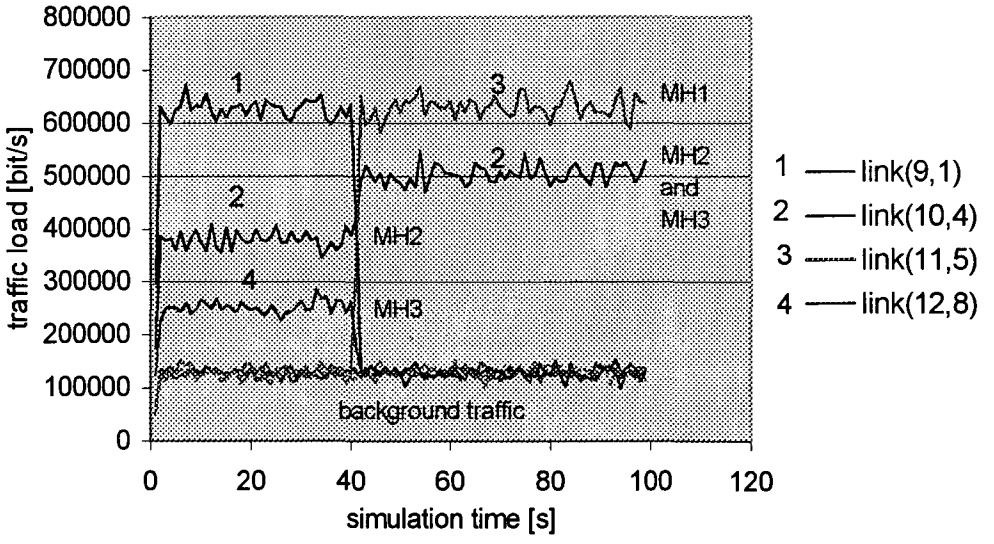
At time instant 40 s MH1 moves from subnetwork 4 to subnetwork 5, whereas MH2 moves from subnetwork 5 to subnetwork 4. In this case, the link between nodes 14 and 11 is loaded with 500 kbit/s + 256 kbit/s = 756 kbit/s. The 500 kbit/s is the traffic transmitted from CH1 to MH1, whereas 256 kbit/s is the background traffic destinated to access routers 5 and 6. The link between nodes 13 and 10 is now loaded with 250 kbit/s + 256 kbit/s = 506 kbit/s. The 250 kbit/s is the traffic transmitted from CH2 to MH2, whereas 256 kbit/s is the background traffic destinated to access routers 3 and 4. Along all other links only flows background traffic. Traffic loads between access routers (routers 1 to 8) are shown in Figure 6-21c. Curves on the upper part present 500 kbit/s real-time traffic transmitted from CH1 to MH1, whereas 250 kbit/s curves present real-time traffic transmitted from CH2 to MH2. As it can be seen from the figure, the traffic load transmitted to CH2 is half as much and it flows in the opposite direction, starting from the access router 8.

Topology 4 can be further extended with more CHs and MHs. Curves in Figure 6-22 show the traffic loads on the links of the access network assuming three MHs and three CHs. The MH1 is initially located in subnetwork 1 and it moves along the subnetworks 1-2-3-4-5-6-7-8. The MH2 is initially located in subnetwork 4 and it moves along subnetworks 4-3-2-1-2-3-4-5. The MH3 is initially located in subnetwork 8 and it moves along subnetworks 8-7-6-5-4-3-2-1. In addition to the background traffic load of 8 x (2 x 64 kbit/s) transmitted to each access router, the CH1 transmitts traffic of 500 kbit/s to the MH1, the CH2 transmits 250 kbit/s to the MH2, and the CH3 transmitts 125 kbit/s to the MH3. The lowest curves on Figure 6-22a and Figure 6-22b show the background traffic, whereas other graphs show the total traffic on the links of the access network. For example, Figure 6-22b shows that link between nodes 9 and 1 is loaded with 500 kbit/s + 128 kbit/s = 628 kbit/s. The 500 kbit/s is the real-time traffic transmitted from CH1 to MH1, 128 kbit/s is the background traffic destined to access router1. Link between nodes 10 and 4 is loaded with 250 kbit/s + 128 kbit/s = 378 kbit/s. The 250 kbit/s is the real-time traffic transmitted from CH2 to MH2. Link between nodes 12 and 8 is loaded with 125 kbit/s + 128 kbit/s = 253 kbit/s. The 125 kbit/s is the real-time traffic transmitted from the CH3 to MH3. At time instant of 40 s, MH1 moves from subnetwork 4 to subnetwork 5, MH2 moves from subnetwork 1 to subnetwork 2, whereas MH3 moves from subnetwork 5 to subnetwork 4. Therefore, link between nodes 11 and 5 is loaded with 500 kbit/s real-time traffic transmitted from

CH1 to MH1 and the 128 kbit/s background traffic. The link between nodes 10 and 4 is now loaded with 250 kbit/s + 125 kbit/s + 128 kbit/s = 503 kbit/s. The 250 kbit/s is the real-time traffic transmitted from CH2 to MH2, 125 kbit/s is the real-time traffic transmitted from CH3 to MH3, and 128 kbit/s is the background traffic. This means that traffic destined to MH2 and MH3 is transmitted via link between nodes 10 and 4, because both MH2 and MH3 initially access the network via access router 4. The MH2 was located initially at the subnetwork 4 and remained within the subnetworks with meshed access routers, whereas MH3 moved from subnetwork 5 to subnetwork 4. This confirms the previous conclusion that traffic load on the links remains constant as long as MHs move within a certain group of subnetworks with meshed access routers. Therefore, if the MHs are distributed uniformly over subnetworks, the traffic load on the links is expected to be constant independently how MHs move.



a) Traffic load on links between routers of the second and third level



b) Traffic load on links between access routers and routers on the second level

Figure 6-22: Traffic distribution in Topology 4 with 3 MHs and 3 CHs

In its most complex form, a meshed access network could work like a peer-to-peer network, where access routers both send their own traffic and forward traffic on for other access routers. In its simplest form, shown in Figure 6-23, access routers are connected in a ring. In the WLAN environment, for example, instead of moving traffic from a MH to a wireless Access Point (AP) to a wired network, such a mesh network moves traffic from AP to AP, depending on availability, and then eventually onto a wired network, and vice versa. Therefore, using this topology, a network manager might only have to connect one of every four or five APs to the fixed network. In our example, for the network topology shown in Figure 6-23, the MH is initially located in subnetwork 1, and then moves along subnetworks 1-2-3-4-5-6-7-8 after staying 10 s in each of them.

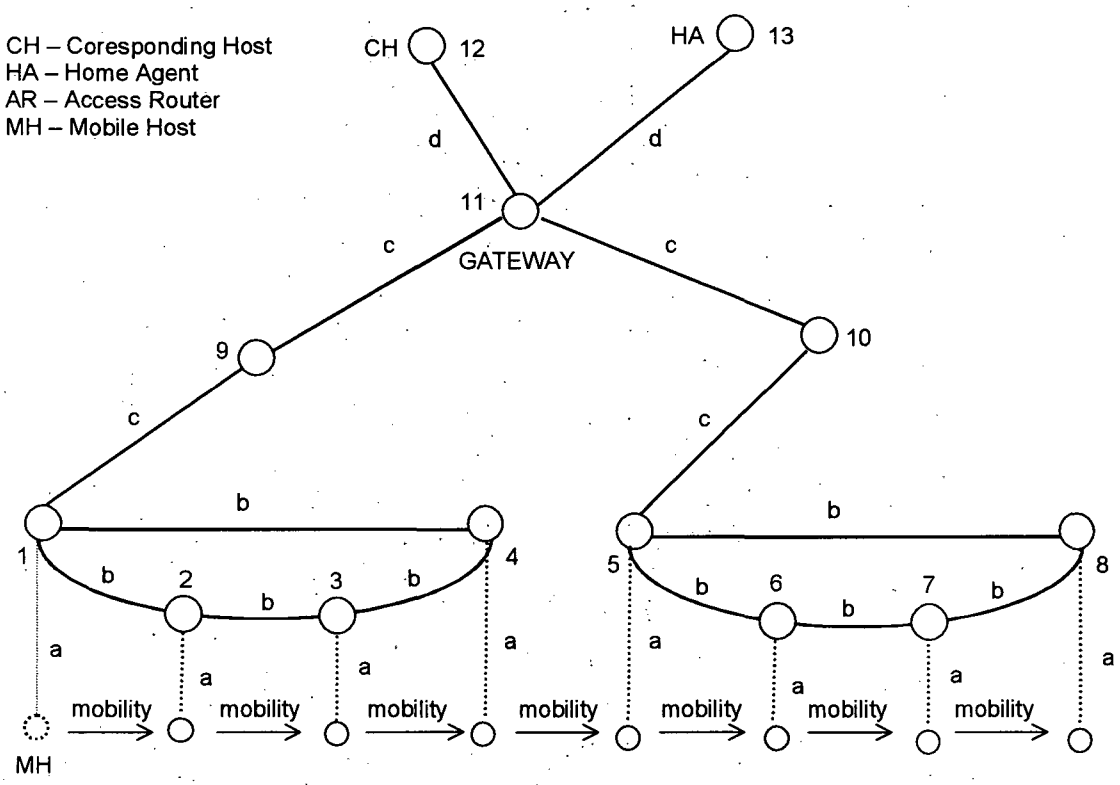
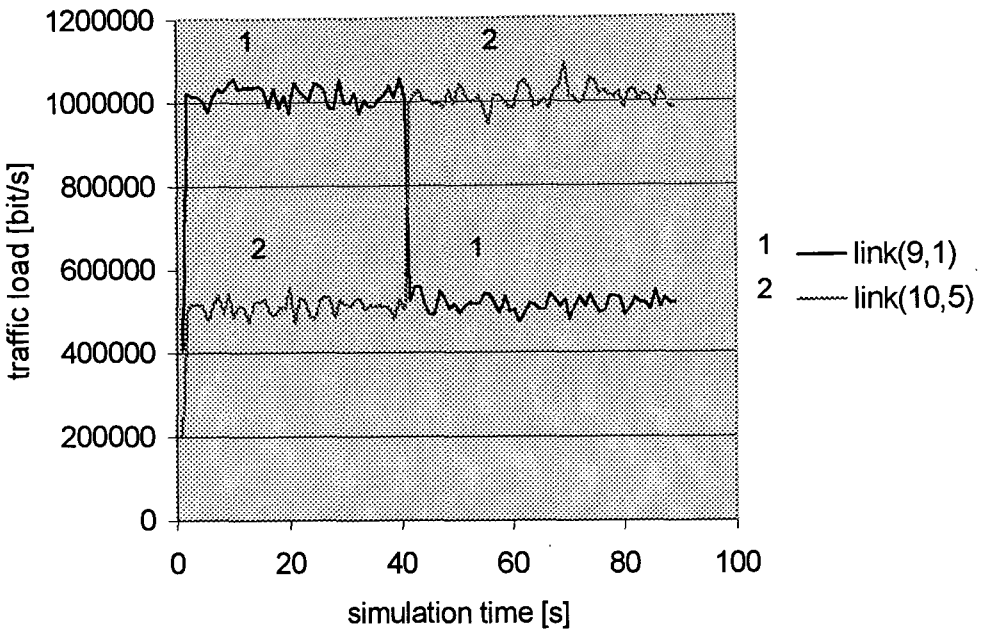
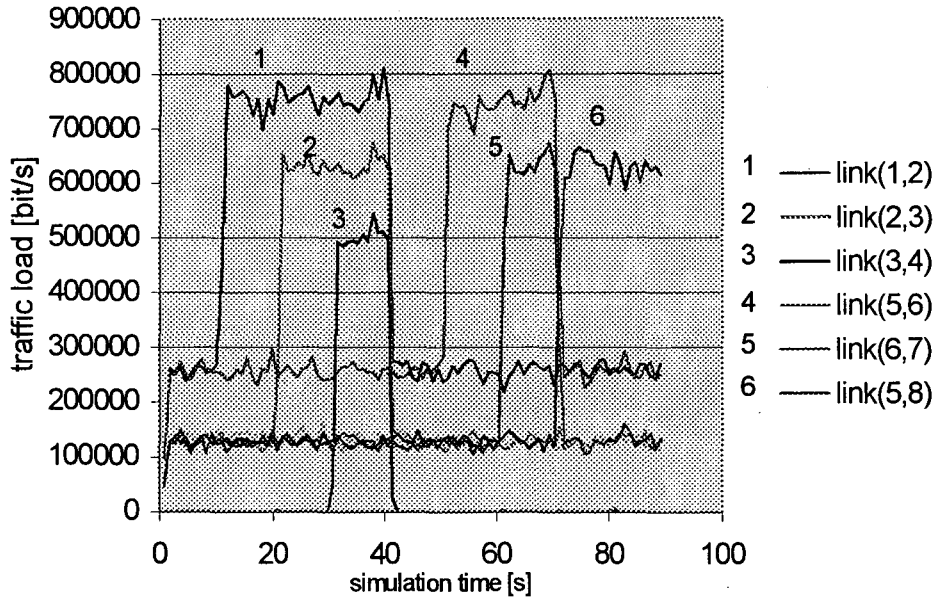


Figure 6-23: Network Topology 5

Assuming a traffic load of 8 x (2 x 64 kbit/s) + 500 kbit/s = 1524 kbit/s, Figure 6-24 shows the traffic load distribution on the different links of the access network of Topology 5. Curves on the upper part of Figure 6-24 show the total traffic, whereas curves at the buttom part show the background traffic. Analysing the plot in Figure 6-24b, one may observe that the total traffic load on the link between access routers 1 and 2 is 500 kbit/s + (2 x 128 kbit/s) = 756 kbit/s. The 500 kbit/s is the real-time traffic transmitted from CH1 to MH1, whereas 2 x 128 kbit/s is the background traffic destined to access routers 2 and 3. The background traffic destined to access router 4 is transmitted via direct link between access routers 1 and 4. The traffic load on the link between access routers 2 and 3 is 500 kbit/s + 128 kbit/s = 628 kbit/s. Whereas, the link between access routers 3 and 4 is loaded only with 500 kbit/s real-time traffic transmitted from CH to MH, since the background traffic is transmitted via the link between access routers 1 and 4. Therefore, the most loaded link, as it is expected, is the link between access routers 1 and 2, since it has to carry the traffic transmitted from CH to MH and the background traffic destined to access routers 2 and 3.



a) Traffic load on links between routers of the second level and access routers



b) Traffic load on links between access routers

Figure 6-24: Traffic distribution for Topology 5

When MH moves within the subnetworks on the right part of Topology 5, the most loaded link is the one between access routers 5 and 6, since it has to carry 500 kbit/s real-time traffic transmitted from CH to MH and 2 x 128 kbit/s background traffic. Link between access routers 6 and 7 is loaded with 500 kbit/s + 128 kbit/s. At the handover from subnetwork 7 to subnetwork 8, both the background traffic destined for access router 8 and the real-time traffic destined to CH, are transmitted via link 5-8.

To conclude, the traffic load on the links between access routers may change as MH moves between subnetworks. However, since access routers are relatively close to each other, capacity provision on the links between access routers should not be a problem.

6.5 Review

This chapter discussed the issues of QoS provisioning in a mobile Internet environment. The chapter began with discussion of the state of the art in QoS provisioning in mobile communication environments. Approaches such as Resource Reservation in Advance, Coupling of Micro-mobility and QoS, and RSVP Interworking with Mobile IP, were covered. Next, the discussion moved to a new proposed Framework for end-to-end QoS provisioning for mobile users' applications. End-to-end network architecture was presented and the reasoning behind proposing a meshed access network was elaborated. In addition, a new signalling protocol for QoS provisioning for partially meshed access network architecture was proposed and evaluated.

7 Conclusions

In this thesis, QoS provisioning in global mobile broadband communication networks is investigated from the aspects of media access control, seamless handover management and QoS signalling in mobile Internet. There is no doubt that Internet and mobile communications are the two fastest evolving network technologies in the last decade. The IPv4 based Internet technology has been proven as being very successful in internetworking of different networks and creating a global communication network. Hence, the Internet became the largest worldwide network providing a wide range of narrowband and broadband services to users. Today Internet services are accessible from everywhere: homes, offices, schools, hospitals, hotels, airports and while we are moving. Although still in the experimental phase, Internet services are also provided to passengers on planes, trains and buses. Further dynamic growth of the number of Internet users and many new IP-based applications are expected in the future. The final goal is an all-IP global end-to-end network. However, the ongoing explosive growth of the number of Internet users has exposed insufficiencies of Internet Protocol version 4 (IPv4). The first and main problem to be recognized was IPv4 address exhaustion. The Internet Engineering Task Force (IETF) recognized this problem around 1990 and solicited a solution. This new solution was Internet Protocol version 6 (IPv6). In addition to the huge address space the designers of IPv6 added other new essential features and enhancements to IPv4, including enhanced support for QoS and embedded support for mobile networks. Hence, one of the driving forces for the widespread adoption of IPv6 is its use in evolving 3G or UMTS mobile networks. However, the deployment of IPv6 is a gradual process lasting many years. In fact IPv6 deployment is already delaying, first-of-all due to lack of end user demand as the most significant obstacle to the success of IPv6 is the transition of applications. Parallel to Internet, mobile communications has seen an unpredicted growth. In general, the terrestrial mobile communication systems development is grouped into different generations. The first-generation (1G) mobile systems are based on analogue network technology and the emphasis was on speech service. The second-generation (2G) mobile communication systems are characterized by employment of "circuit switched" digital technology. The most successful 2G system no doubt is European GSM, providing data services up to 14.4 kbit/s, in addition to voice services. However, for today's Internet such data rates are to low. Hence, new more advanced second and a half generation (2.5G) and third-generation (3G) systems were designed. The GPRS and other 2.5G mobile communication systems are considered as interim technologies between 2G and 3G systems. The 2.5G systems have many enhancements over the 2G systems. These enhancements are mainly based on the use of packet switching technology and offering higher data rates than the existing 2G systems. The 3G mobile systems have been developed to meet further increasing demands for new mobile multimedia services and high-speed data communication in the current environment of the Internet. At present, the European UMTS and other 3G mobile communication systems are just beginning to be deployed, while research on the next generation of mobile communications, the fourth-generation (4G) wireless systems, begins to pave the way for the future. Right now it is hard to say where the third-generation ends and the fourth-generation starts. However, it is for sure that the final goal for mobile networks evolution, including 3G systems, is IP technology. However, cellular operators are likely to undertake the migration to a full IP solution on Public Land Mobile Networks (PLMN) only beyond third-generation mobile networks.

Other important mobile communication systems are satellite and WLAN networks. Satellite networks are considered a feasible solution to provide broadband as well as narrowband services to users in remote areas, where there is no communication infrastructure, due to high costs (rough terrain or low-density population) or due to geographic location (aeronautical and maritime area). Satellite systems can be used also as complementary networks to terrestrial mobile networks. WLAN technology currently presents a hot topic in the wireless Internet market for providing broadband services to slow mobile users. WLAN will certainly be a key part of the future wireless Internet first-of-all due to the high bandwidth-to-cost ratio. In my opinion there is no doubt that UMTS is going to happen, first-of-all because of large investments. However, the already delayed UMTS will be further delayed until it is economically acceptable for users. For the next few years, the cheap WLAN combined with GPRS will fulfill user needs and most users are expected to use broadband Internet services through WLAN.

Considering the scarce wireless medium, MAC protocols have an essential role in mobile communication networks. Hence, the design of flexible and efficient Medium Access Control (MAC) protocols is a crucial starting point in providing QoS in wireless networks. Hereby, TDMA-based MAC protocols for terrestrial mobile networks, satellite networks, and WLAN are analysed in this thesis. A new TDMA-based MAC protocol for broadband satellite networks efficiently supporting real-time and non-real time services is proposed and its performance in terms of access delay and throughput are evaluated compared with a reference protocol. Simulation results (Figure 3-6) show that the proposed access scheme leads to significant performance improvements for real-time traffic while performance degradations for non real-time traffic are kept to acceptable values. It is noticeable (Figure 3-7) that higher round-trip delays (corresponding to GEO satellite networks) significantly degrade the performance of both protocols. Again, our protocol exhibits superior real-time performance. Furthermore, in terms of data transmission performance, the degradation is still kept to a satisfactory amount. Thus, QoS requirements in terms of delay of multimedia traffic may be fulfilled by this novel protocol in an efficient way.

The goal of third and next generation mobile networks is to provide service continuity while users move between different networks and systems. Currently the IP services for mobile users are delivered over a variety of networks and technologies, including GSM, GPRS, satellite, and WLAN. However, seamless mobility among these different access networks cannot take place, because mobility management in each of them is handled almost completely by the underlaying network. To overcome this problem Mobile IPv4 and IPv6, for handling inter and intra network mobility were developed. Hence, handover management based on Mobile IP is an essential mechanism to enable users to communicate continuously while moving within the same network or between different mobile networks. Therefore, two handover protocols, based on MIPv6, for inter terrestrial-satellite network and intra-satellite networks are proposed and evaluated in this thesis. Simulation results show that signaling diversity is necessary to reduce the number of forwarded packets from the terrestrial to the satellite network (Figure 4-17) as well as from the satellite to the terrestrial network (Figure 4-18). For the inter-satellite handover results show (Figure 4-21 to Figure 4-24) that after handover, many packets need to be forwarded from the current to a new satellite. The constellation equipped with the cross-seam ISLs (Figure 4-21 and Figure 4-23) reduces both the binding delay and the number of forwarded packets.

Quality-of-Service (QoS) is an essential issue in communication networks that aim to provide real-time services to user's applications. QoS requirements have to be provided everywhere in the network, that is end-to-end, and for all services that need QoS support. Hence, broadband networks such as Internet, UMTS, and WLAN have developed and are still developing QoS mechanisms, to accommodate real-time services. In mobile Internet environment mobile users require the same real-time broadband services as fixed Internet users. These services require both QoS and mobility support. Since existing Internet QoS mechanisms do not consider mobile environments, and on the other hand, Mobile IP does not provide QoS, several new solutions addressing QoS provision to mobile users have been proposed. However, none of them considers meshed access network architectures. Hereby, a new framework for end-to-end QoS provi-

sioning to mobile users applications is proposed in this thesis, including semi-meshed access networks. In addition, a new signalling protocol for QoS provisioning to mobile users for meshed access network architecture is proposed and and its performance is evaluated compared with two reference protocols. The RSVP signalling delay and the maximum allowed delay for QoS provisioning have been taken as performance metrics for different network topologies under different traffic congestion conditions and user mobility scenarios.

Simulations results (Figure 6-10 to Figure 6-14) show that proposed protocol, highly outperform conventional protocol for both symmetric (Figure 6-8) and asymmetric (Figure 6-12) network topology, under all traffic congestion conditions and mobility scenarios. Differences are particularly distinguished for access and core network congestion with mobility scenario 2. Furthermore, the allowed maximum delay for the proposed protocol is greater than RSVP signalling delay at all handover instants, ensuring QoS provisioning, whereas in the case of the conventional protocol it is the other way round. Comparing the proposed protocol and FT protocol, simulation results (Figure 6-15 and Figure 6-16) show that both protocols ensure QoS provisioning at all handover instants. However, the proposed protocol has better performances at all handover instants except during the handover from subnetwork 4 to subnetwork 5 (where there is no direct link between access routers 4 and 5). The differences in favour of the proposed protocol are more pronounced with mobility scenario 2.

A very important and a specific characteristic of the proposed protocol is that traffic load on the links that connect initial access router of the MHs to Nearest Common Router (NCR) and other routers on the network hierarchy until to the gateway remains constant as long as a MH moves between access routers that form a meshed access network (Figure 6-19, Figure 6-20, and Figure 6-22). This feature gives the possibility to control the distribution of the traffic load on the access network. Therefore, dimensioning of the network is more accurate when number of home mobile users for each access routers is known. Furthermore, the proposed protocol is appropriate for the simplest form of meshed topologies (Figure 6-23) where only one of a group of access routers is connected to a wired network. In the WLAN environment, for example, instead of moving traffic from a MH to a wireless Access Point (AP) to a wired network, such a meshed network moves traffic from AP to AP, depending on availability, and then eventually onto a wired network, and vice versa. Therefore, using this topology, a network manager might only have to connect one of every four or five APs to the fixed network. Therefore, in my view, partially meshed topologies for the access points are very beneficial for local communities communication and it is a topic for further investigations in the future.

In general, it is expected that future global telecommunication networks will be multiservice networks that provide legacy and emerging services across different IPv6 based access networks connected to the IPv6/MPLS backbone Internet, running over a high-capacity optical infrastructure. For large mobile and fixed access networks MPLS technology in combination with MIPv6 is a new possibly the most optimal solution. However, for small networks, RSVP remains the most reliable protocol for QoS provisioning. Hence, another future topic for investigation will be oriented on applying MPLS in mobile access networks with a partially meshed topology of access points.

References

[Abr70] N. Abramson, "The ALOHA System – Another Alternative for Computer Communications," Proceedings, Fall Joint Computer Conference, 1970.

[Aky99] I.F. Akyildiz, J. McNair, J.S.M. Ho, H. Uzunalioglu, W. Wang, "Mobility Management for Next Generation Wireless Systems" Proceedings of IEEE, Vol. 87, No. 8, Aug. 1999, pp. 1347-1384.

[ARIN] ARIN American IPv6 registration services, http://www.arin.net/ipv6/ipv6-regserv.html

[As94] H. R. van As, "The Evolution towards Terabit/s LANs and MANs," Computer Networks and ISDN Design, vol. 26, 1994, pp. 603-56.

[Awd98] D. Awduche et al., "Requirements for Traffic Engineering over MPLS," Internet draft, draft-ietf-mpls-traffic-eng.00.txt, Oct. 1998.

[Bar95] A. Bar-Noy, I. Kessler, M. Sidi, "Mobile Users: To Update or Not to Update?," ACM/Baltzer J. Wireless Networks, Vol. 1, No. 2, July 1995, pp. 175-195.

[Ben02] G. Benelli, R. Fantacci, G. Giambene, C. Ortolani, "Performance Analysis of a PRMA Protocol Suitable for Voice and Data Transmissions in Low Earth Orbit Mobile Satellite Systems," IEEE Transactions on Wireless Communications, Vol. 1, No. 1, Jan. 2002, pp. 156-168.

[Ber00] Y. Bernet at al., "A Framework for Integrated Services Operation over DiffServ Networks", NWG RFC 2998, November 2000.

[Ber98] Y. Bernet et al., "A Framework for Differentiated Services," Internet draft, draft-ietf-diffserv-framework-00.txt, May 1998.

[Bia97] G. Bianchi, F. Borgonovo, L. Fratta, L. Musumeci, M. Zorzi, "C-PRAMA: A Centralized Packet Reservation Multiple Access for Local Wireless Communications," *IEEE Trans. on Veh. Technol.*, vol. 46, No.2, May 1997, pp. 422-436.

[Bi01] Q. Bi, G.L. Zysman, H. Menkes, "Wireless mobile communications at the start of the 21st century," IEEE Communications Magazine, Vol. 39, No. 1, January 2001, pp. 110-116.

[Bin75] R. Binder, "A dynamic packet switching system for satellite broadcast channels," Proc. ICC, 1975.

[Bor78] F. Borgonovo, L. A. Fratta, "SRUC: A technique for packet transmission on multiple access channels," *Proc. ICCC*, Kyoto, Japan, 1978, pp. 601–607.

[Cam99] A. Campbell, J. Gomez, C-Y. Wan, S. Kim, Z. Turanyi, A. Valko, "Cellular IP," Internet Draft, draft-ietf-mobileip-cellularip-00, Work in Progress, Dec. 1999.

[Cas98a] C. Castelluccia, "A Hierarchical Mobile IPv6 Proposal", INRIA technical report TR-0226, 1998.

[Cas98b] C. Castelluccia, "A Hierarchical Mobility Management Scheme for IPv6," Proc. of the third IEEE Symposium on Computers and Communications, 1998 (ISCC '98), Athens, Greece, June 1998, pp. 305-309.

[Cas01] C. Castelluccia, K. Malki, H. Soliman, L. Bellier, "Hierarchical MIPv6 mobility management", draft-ietf-mobileip-hmipv6-05.txt, July 2001.

[Chi02] F. M. Chiussi, D. A. Khotimsky, S. Krishnan, "Mobility Management in Third-Generation All-IP Networks," IEEE Communications Magazine, Vol. 40, No. 9, September 2002, pp. 124-135.

[Chi99a] P. Chitre, F. Yenenoglu, "Next Generation Satellite Networks: Architectures and Implementations," IEEE Comm. Magazine, Vol. 37, No. 3, March 1999, pp. 30-36.

[Chi99b] G. Chiruvolu, A. Agrawal, M. Vandenhoute "Mobility and QoS support for IPv6-based real-time wireless Internet traffic", 1999 IEEE International Conference on Communications (ICC'99) Vancouver, BC, Canada, June 1999, Vol. 1, pp.334-8.

[Cisco] Cisco IOS Learning Services, "The ABCs of IP version 6," www.cisco.com/go/abc.

[Col00] F. Di Cola, P. Chan, R. Sheriff, Y. Hu, "Handover with QoS Support in Multi-segment Broadband Networks," Proceedings of the European Workshop on Mobile and Personal Satellite Communications 2000, London, UK, September 2000, pp. 92-101.

[Com97] G. Comparetto, R. Ramirez, "Trends in Mobile Satellite Technology," IEEE Computer, Vol. 30, No. 2, February 1997, pp. 44-52.

[Cra98] E. Crawley et al., "A Framework for QoS-based Routing in the Internet," RFC 2386, Aug. 1998.

[Cro73] W.R. Crowther et al., "A system for broadcast communication: Reservation ALOHA," Proceedings of the Sixth Hawaii International System Science Conference, January 1973.

[Eis96] M. Eischenschmid, H. J. Vogel, M. Werner, "Handover Signalling in LEO/MEO Satellite Systems," Proc. of the International Conference on Personal Mobile and Spread Spectrum Communications, (ICPMSC 96), Hong Kong, December 1996, pp. 117-120

[Elh96] A. El Hoiydi, R. Finean, "Location Management for the Satellite-Universal Mobile Telecommunication System," Proc. of the International Conf. on Universal Personal Communication (ICUPC), 1996, Cambridge, MA, USA, Vol. 2, pp. 739-744

[EUI-64] "Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority", March 1997. http://standards.ieee.org/regauth/oui/tutorials/EUI64.html

[Goo89] D. J. Goodman, R.A. Valenzuela, K.T. Gayliard, B. Ramamurthi, "Packet Reservation Access for Local Wireless Communications," IEEE Transactions on Communications, Vol. 37, No. 8, August 1989, pp. 885-890.

[Gun96] A. Guntsch, "Mobility Management in an Integrated GSM and Satellite PCN," Proc. of the IEEE Vehicular Technology Conference, VTC'96, Atlanta, GA, USA, April 1996, Vol. 3, pp. 1830-1834.

[Gus02] E. Gustafsson, A. Jonsson, C. Perkins, "Mobile IP Regional Registration," Internet draft, draft-ietf-mobileip-reg-tunnel-06.txt, Mar. 2002, work in progress.

[Hon94] Honghui Qi, "Packet Reservation Multiple Access Protocol for Cellular Systems," PhD. thesis, University of South Australia, August 1994.

[Hor02] Horlait, N. Rouhana, "Differentiated Services and Integrates services Use of MPLS", http://www-rp.lip6.fr/~eh/Files/mpls.pdf

[IANA] The Internet Assigned Numbers Authority (IANA) http://www.iana.org

[Ier02] A. Iera, A. Molinaro, "Designing the Interworking of Terrestrial and Satellite IP-Based Networks," IEEE Communication Magazine, Vol. 40, No. 2, February 2002, pp. 136-144.

[IXI04] White Paper "Internet Protocol version 6 (IPv6) Conformance and Performance Testing," IXIA, 2004.

[Jam01] A. Jamalipour, "Broadband Satellite Networks - The Global IT Bridge", Proceedings of the IEEE, Vol. 89, No. 1, January 2001, pp. 88-104.

[Job00] K. Jobmann, ''Mobilfunk und Intelligente Netze", Universität Hannover, Institut für Allgemeine Nachritentechnik Kommunikationsnetze, 2000.

[Joh00] D. Johnson, C. Perkins, "Mobility Support in IPv6," IETF Internet draft <draft-ietf-mobileip-ipv6-12.txt>, April 2000.

[Kaa01] H. Kaaranen, A. Ahtiainen, L. Laitinen, S. Naghian, V. Niemi, ''UMTS Networks," John Wiley & Sons, LTD 2001 (ISBN 0471 48654 X).

[Ker93] A. Kershenbaum, "Telecommunications Network Design Algorithms," *McGraw-Hill*, Inc, 1993.

[Kim01] J. Kim, A. Jamalipour, "Traffic Management and QoS Provisioning in Future Wireless IP Networks," IEEE Personal Communications, Vol. 8 No. 5, October 2001, pp. 46-55

[Kle00] L. Kleinrock, "On Some Principles of Nomadic Computing and Multi-Access

Communications", IEEE Comm. Magazine, Vol. 38, No. 7, July 2000, pp. 46-50.

[Koo03] R. Koodli, editor, "Fast Handovers for Mobile IPv6," Internet Draft <draft-ietf-mobileip-fast-mipv6-06.txt>, March 2003.

[Koo00] R. Koodli, "A Framework for Smooth Handovers with Mobile IPv6," IETF Internet Draft <draft-koodli-mobileip-smoothv6-00.txt>, July 2000.

[Kor00] H. Koraitim, S. Tahme, "Performance Analysis of Multiple Access Protocol for Multimedia Satellite Networks," IEEE Journal on Selected Areas in Communications, Vol. 18, No. 9, 2000, pp.1751-1763.

[Lad00] L. Ladid "IPv6 – The new generation Internet," Ericsson Review, No. 1, 2000, pp. 6-13.

[Leo01] M. Leo, M. Luglio, "Inter-segment Handover Between Terrestrial and Satellite Segments: Analysis and Performance Evaluation Through Simulation," IEEE Transactions on Vehicular Technology, Vol. 50, No. 3, May 2001, pp. 750-766.

[Lep01] S. Lepaja, K. Bengi, "A Random-Reservation Medium Access Protocol For Satellite Networks To Accommodate Real-Time Traffic," IEEE 53rd Vehicular Technology Conference (VTC 2001 Spring), Rhodes, Greece, vol. 2, pp. 861-865.

[Lep02] S. Lepaja, R. Fleck, R. Donner, N. Hoang, "QoS Provisioning to Mobile Internet Users," Proceedings of the ECUMN 2002, April 2002, Colmar, France, pp. 230-237.

[Lep03] S. Lepaja, A. Lila, N. Kryvinskaja, M. Hoang, "A Framework for End-to-End QoS Provisioning in Mobile Internet Environment," Proceedings of the WCMN 2003, Sept 2003, Singapore, pp. 86-89.

[Lin02] A Lindgren, A. Almquist, O.Schellen, "Evaluation of Quality-of-Service Schemes for IEEE802.11 Wireless LANs," University of Technology, Sweden.

[Lut00] E. Lutz, M. Werner and A. Jahn, "Satellite Systems for Personal and Broadband Communication," Springer Verlag 2002.

[Lut98] E. Lutz, "Issues in Satellite Personal Communication Systems," ACM Journal of Wireless Networks, Vol. 4, No. 2, February 1998, pp. 109-124.

[Mal01] J.T. Malinen, F. Le, C.E. Perkins, "Mobile IPv6 Regional Registrations," IETF Internet Draft |<draft-malinen-mobileip-regreg6-01.txt>, July 2001

[Man02] S. Mangold1, S Choi, P. May, O. Klein, G. Hiertz, L. Stibor, " IEEE 802.11e Wireless LAN for Quality-of-Service," Proc. of European Wireless (EW2002), Florence, Italy, February 2002.

[Mar98] G. Maral, J. Restrepo, E. del Re, R. Fantacci, G. Giambene, "Performance Analysis for a Guaranteed Handover Service in an LEO Constellation with a "Satellite-Fixed Cell" System", IEEE Transactions on Vehicular Technology, Vol. 47, No. 4, November 1998, pp. 1200-1214.

[McD95] David E. McDysan, Darren L.Spohn, "ATM, theory and Application," McGraw-Hill, Inc, 1995 (ISBN 0-07-060362-6).

[Mcn00a] J. McNair, "Location Registration and Paging in Mobile Satellite Systems", Proc. of the Fifth IEEE Symposium on Computers and Communications, 2000 (ISCC '00), Antibes, France, July 2000, pp. 232-237

[Mcn00b] J. MacNair, I.F. Akyildiz, M. Bender, "An Inter-system Handoff Technique for The IMT-2000 System," Proc. of the IEEE Conference of Computer and Communications Societies (INFOCOM '00), Tel-Aviv, Israel, March 2000, Vol. 1, pp. 208-216.

[Mou02] M.N. Moustafa, I. Habib, M. Naghshineh, Th. J. Watson, M. Guizani, "QoS-Enabled Broadband Mobile Access to Wireline Networks," IEEE Communications Magazine, Vol. 40, No. 4, April 2002, pp. 50-56.

[Nar98] P. Narvaez, A. Clerget, W. Dabbous, "Internet Routing over LEO Satellite Constellations," Third ACM/IEEE International Workshop on Satellite-based Information Services (WOSBIS '98), Dallas, TX, USA, October 1998, pp. 89-95.

[Ngu01a] H.N. Nguyen, S. Lepaja, H. R. van As, "Mobile Internet Provisioning in Satellite-IP Networks: Mobility Management, Interworking and Integration with Terrestrial

Networks," Proc. of the 19th AIAA International Communications Satellite Systems Conference, Toulouse, France, April 2001, pp. 235-245.

[Ngu01b] H.N. Nguyen, S. Lepaja, J. Schuringa, H. R. van As, "Handover Management in Low Earth Orbit Satellite IP Networks," Proc. of the IEEE Global Telecommunications Conference, 2001 (GLOBECOM '01), Saint Antonio, TX, USA, November 2001, Vol. 4, pp. 2730-2734

[Ngu02] H.N. Nguyen, Routing and QoS in Broadband Low Earth Orbit Satellite Networks", Ph.D. Dissertation, Institute for Communication Networks, Vienna University of Technology, 2002.

[Ni02] Q. Ni, L. Romdhani, Th. Turletti, I. Aad, "QoS Issues and Enhancements for IEEE 802.11 Wireless LAN," Institute National de Recherche en Informatique et en Automatique, N° 4612, November 2002, France.

[Pat00] G. Patel and S. Dennett, "The 3GPP and 3GPP2 Movements Toward an all-IP Mobile Network," IEEE Personal Communications, Vol. 7, No. 4, August 2000, pp. 62-64.

[Pav86] C. Pavey, R. Rice, E. Cummins, "A Performance Evaluation of the PDAMA Satellite Access Protocol," Proc. INFOCOM'86, Bal Harbour, FL, USA, April 1986, pp. 580-586.

[Per97] C. Perkins, "Mobile IP," IEEE Communications Magazine, Vol. 35, No. 5, May 1997, pp. 84–99.

[Per02] C.Perkins, et all., " Fast Handovers for Mobile IPv6", draft-ietf-mobileip-fast-mipv6-04.txt, 2002.

[Pey95] H. Peyravi, "Multiple Access Control Protocols for the Mars Regional Network: A Survey and Assessments," Tech. rep., Dept. of Math and Comp. Sci., Kent State Univ., Sept. 1995.

[Pey99] H. Peyravi, "Medium Access Control Performance in Satellite Communications", IEEE Communications Magazine, Vol. 37, No. 3, March, pp. 62-71.

[Ram99]. R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, L. Salgarelli, "IP Micro-Mobility Support using HAWAII," Internet Draft, draft-ietf-mobileip-hawaii-00, Work in Progress, June 1999.

[Ray85] D. Raychaudhuri, "Announced Retransmission Random Access Protocol," IEEE Transactions on Communications, Vol. 33, No. 11, Nov. 1985, pp. 1183-1190.

[Ric95] M. Richharia, "Satellite Communication Systems," McGraw-Hill, Inc. publisher, 1995, ISBN 0-07-052374-6.

[Rob73] L. G. Roberts, "Dynamic Allocation of Satellite Capacity through Packet Reservation," *Proc. Nat'l. Comp. Conf.*, AFIPS NCC73, vol. 42, June 1973, pp. 711–16.

[Rob75] L. Roberts, "ALOHA Packet System With and Without Slots and Capture," Computer Communications Review, April 1975.

[Ros98] E. Rosen, A. Viswanathan, R. Callon, "Multiprotocol Label Switching Architecture," Internet draft, draft-ietf-mpls-arch-01.txt, Mar. 1998.

[San97] J. Sanchez, R. Martines, M. W. Marcellin, "A Survey of MAC Protocols for Wireless ATM," *IEEE Network*, Vol. 11, No. 6, Nov. 1997, pp. 52–62.

[Sch00] J.H. Schiller, "Mobile Communications," Pearson Education Limited, London 2000, ISBN 0 201 39836 2.

[Ser97] M. Sexton, A. Reid, "Broadband Networking - ATM, SDH and SONET," Artech House 1997.

[She01a] Shen et al, "An interoperation framework for using RSVP in Mobile IPv6 Networks", IETF Internet draft <draft-s1hen-rsvp-mobileipv6-interoip-00.txt>, July 2001.

[She01b] Q. Shen, A. Lo, W. Seah, "Performance Evaluation of Flow Transparent Mobile IPv6 and RSVP Integration", July 2001.

[SIE 01] „UMTS," White Paper, Siemens AG 2001

[Smi02] C. Smith, D. Collins, "3G Wireless Networks", McGraw-Hill, 2002, ISBN 0-07-13681-5.

[Sol01] H. Soliman *et al.*, "Hierarchical MIPv6 Mobility Management," IETF draft, draft-ietf-mobileip-hmipv6-05.txt, July 2001.

[Sot02] S.I. Maniatis, E.G. Nikolouzou, I.S. Venieris, "QoS Issues in the Converged 3G Wireless and Wired Networks," IEEE Communications Magazine, Vol. 40, No. 8, August 2002, pp. 44-53.

[Sud83] T. Suda, H. Miyahara, T. Hasegawa, "Performance Evaluation of an Integrated Access Scheme in a Satellite Communication Channel," IEEE Journal on Selected Areas in Communications, Vol. 1, No. 1, Jan. 1983, pp. 153-164.

[Sta94] W. Stalling, "Data and Computer Communications," Third Edition, Prentice Hall, 1994.

[Sta99] W. Stalling, "ISDN and Broadband ISDN with Frame Relay and ATM", Fourth Edition, Prentice Hall 1999.

[Tal01] A. K. Talukdar, B.R. Badrinath, A. Acharya, "MRSVP: A Resource Reservation Protocol for an Integrated Services Network with Mobile Hosts", Wireless Networks, Vol. 7, No. 1, Jan/Feb. 2001, pp. 5-19.

[Tat04] M. Tatipamula, P. Grossetete, H. Esaki, "IPv6 Integration and Coexistance Strategies for Next-Generation Networks," IEEE Communications Magazine, Vol. 42, No. 1, Jan. 2004, pp. 88-96.

[UMT02] UMTS Forum, "Evolution to 3G/UMTS Services," White Paper No. 1 (August 2002).

[Uzu97] H. Uzunalioglu, 'Managing Connection Handover in Satellite Networks", Proc. of the IEEE Global Telecommunications Conference, 1997 (GLOBECOM '97), Phoenix, AZ, USA, November 1997, Vol. 3, pp. 1606-1610.

[Uzu98] H. Uzunalioglu, "Probabilistic Routing Protocol for Low Earth Orbit Satellite", Proc. of the IEEE International Conference on Communication 1998 (ICC'98), Atlanta, GA, USA, June 1998, Vol. 1, pp. 89-93.

[Zah02] Th.B. Zahariadis, K.G. Vaxevanakis, Ch.P. Tsantilas, N.A. Zervos, "Global Roaming in Next-Generation Networks", IEEE Communications Magazine, Vol. 40, No. 2, February 2002, pp. 145-151.

[Wat84] A. Waters, C. Adams, "The satellite transmission protocol of Universe project," Proc. SIGCOMM Symp. Commun. Architectures and Protocols, June 1984.

[Wer95] M. Werner, A. Jahn, E. Lutz and A. Botscher, "Analysis of System Parameters for LEO/ICO Satellite Communication Networks", IEEE Journal on Selected Areas in Communications, Vol. 13, No. 3, February 1995, pp. 371-381.

[Won92] W. C. Wong, D. J. Goodman, "A Packet Reservation Multiple Access Protocol for Integrated Speech and Data Transmission," IEEE Proceedings – I, Vol. 139, No. 6. Dec. 1992

[Woo01] L. Wood, A. Clerget, I. Andrikopoulos, G. Pavlou, W. Dabbous, "IP Routing Issues in Satellite Constellation Networks", International Journal of Satellite Communication, John Wiley & Son, Vol. 19, No. 1, January 2001, pp. 69-92.

[Wis00] D. R. Wisely, "The Challenges of an All-IP Fixed and Mobile Telecommunication Networks", Proc. of the Personal Indoor Mobile Radio Communications 2000 (PIRMC '00), London, UK, September 2000, Vol. 1, pp. 13-18.

[RFC3220] Ch.Perkins "IP Mobility Support for IPv4", RFC 3220, 2002.

[RFC2002] Ch.Perkins "IP Mobility Support", RFC 2002, 1996.

[RFC2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.

[RFC2215] S. Shenker, J. Wroclawski, "General Characterization Parameters for Integrated Service Network Elements", RFC 2215, September 1997.

[RFC2205] R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin, "Resource ReSerVation Protocol (RSVP) Version 1 Functional Specification", IETF RFC 2205, proposed standard, September 1997.

[RFC211] J. Wroclawski, "Specification of the Controlled-Load Network Element Service," RFC 2211, Sept. 1997.

[RFC212] S. Shenker, C. Partridge, R. Guerin, "Specification of Guaranteed Quality of Service," RFC 2212, Sept. 1997.
[RFC2210] J. Wroclawski, "The use of RSVP with IETF Integrated Services", RFC 2210, September 1997.
[RFC1633] R. Braden, D. Clark, S. Shenker, "Integrated Services in the Internet Architecture: an Overview," Internet RFC 1633, June 1994.
[RFC792] J. Postel, "Internet Control Message Protocol", RFC 792, September 1981.
[RFC1058] C. Hedrick, "Routing Information Protocol", RFC 1058, June 1988.
[RFC1771] Y. Rekhter, T.J. Watson, T. Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995.
[RFC 080] G. Malkin, R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.
[RFC2740] R. Coltun, D. Ferguson, J. Moy, "OSPF for IPv6", RFC 2740, December 1999.
[RFC2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.
[RFC2474] K. Nichols, S. Blake, F. Baker, D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.
[RFC2131] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
[RFC2460] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2406, December 1998.
[RFC2461] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.
[RFC2462] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.
[RFC2463] A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.
[CCITT] CCITT ISDN I.430 standard
[CCITT] CCITT ISDN I.431 standard
[I.121] ITU-T, "Recommendation I.121, Broadband Aspects of ISDN," 1991
[I.211] ITU-T, "Recommendation I.211, B-ISDN General Network Aspects," 1991
[I.321] ITU-T, "Recommendation I.321, B-ISDN Protocol Reference Model and Its Application," 1991
[I.413] ITU-T, "Recommendation I.413, B-ISDN User Network Interface," 1991
[3GPP] www.3GPP.org
[3GPP2] www.3GPP2.org

Abbreviations

1G	First Generation
2G	Second Generation
2,5G	Second and half Generation
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
4G	Fourth Generation
AAL	ATM Adaptation Layer
ACK	Acknowledgement
AMPS	Ameican Mobile Phone System
AP	Access Point
AR	Access Router
ARRA	Announced Retransmission Random Access
ARP	Address Resolution Protocol
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BGP	Border Gateway Protocol
B-ISDN	Broadband Integrated Service Digital Network
BS	Base Station
BSC	Base Station Controller
CAC	Connection Admission Control
CBR	Constant Bit Rate
CDMA	Code Division Multiplex Access
CDV	Cell Delay Variation
CDVT	CDV Tolerance
CH	Correspondent Host
CLP	Cell Loss Priority
CLR	Cell Loss Ratio
CoA	Care-of-Address
CSCF	Call State Control Function
CSMA	Carrier Sense Multiple Access
CSPDN	Circuit Switched Public Data Network
DAMA	Demand Assignment Multiple Access
DCF	Distributed Coordination Function
DECT	Digital European Cordless Telephone
DiffServ	Differentiated Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DS	Differentiated Service
DSSS	Direct Sequence Spread Spectrum

EDCF	Enhanced Distributed Coordination Function
EDGE	Enhanced Data Rate for GSM Evolution
ETSI	European Telecommunication Standard Institute
EUI	Extended Universal Identifier
FA	Foreign Agent
F-CoA	Footprint CoA
FDMA	Frequency Division Multiplex Access
FEC	Forward Error Correction
FEC	Forward Equivalence Class
FES	Fixed Earth Station
FHSS	Frequency Hopping Spread Spectrum
FMA	Footprint Mobility Agent
FPLMTN	Future Public Land Mobile Telecommunication System
FT	Flow Transparency
FTP	File Transfer Protocol
GEO	Geostationary Earth Orbit
GERAN	FSM/EDGE Radio Access Network
GES	Gateway Earth Station
GFC	Generic Flow Control
GFR	Guaranted Frame Rate
GGSN	Gateway GPRS Supporting Node
GMA	Gateway Mobility Agent
GPRS	General Packet Radio System
GSM	Global System for Mobile Communication
HA	Home Agent
HCF	Hybrid Coordination Function
HDLC	High Level Data Link Control Protocol
HLR	Home Location Register
HSCSD	High Speed Ciorcuit Switched Data
HTTP	HyperText Transfer Protocol
ID	Identifier
IGRP	Interior Gateway Routing Protocol
IETF	Internet Engineering Task Force
IMT-2000	International Mobile Telecommunications 2000
ISO	International Standards Organization
IntServ	Integrated Service
IP	Internet Protocol
Ipv4	IP version 4
Ipv6	IP version 6
ISDN	Integrated Service Digital Network
ISL	Inter-Satellite Link
ITU	International Telecommunication Union
IWF	InterWorking Function
IWU	InterWorking Unit

LA	Location Area
LAN	Local Area Network
LAPD	Link Access Protocol for the D Channel
LDB	Label Distribution Protocol
LEO	Low Earth Orbit
LLC	Logical Link Control
LSP	Label Switched Path
MAC	Media Access Control
MAHO	Mobile Assisted Handover
MBS	Maximum Burst Size
MCHO	Mobile Controlled Handover
MEO	Medium Earth Orbit
MF-TDMA	Multi-Frequency TDMA
MH	Mobile Host
MIP	Mobile Internet Protocol
MO	Mobility Object
MPLS	Multi Protocol Label Switching
MSC	Mobile Switching Center
MT	Mobile Terminal
NAHO	Network Assisted Handover
NAT	Network Address Translation
NCC	Network Control Center
NCHO	Network Controlled Handover
NCR	Nearest Common Router
NMT	Nordic Mobile Telephone
NNI	Network-Network Interface
NOC	Network Operation Center
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PC	Personal Computer
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PHB	Per-Hop Behaviour
PHY	Physical layer
PLMN	Public Land Mobile Network
PSTN	Public SwitchedTelephone Network
QoS	Quality of Service
RAN	Radio Access Network
RFC	Request For Comment
RIP	Routing Information Protocol
RMA	Region Mobility Agent
RR	Resource Reservation
RRM	Radio Resource Management
RSVP	Resource Reservation Protocol

SCR	Sustainable Cell Rate
SDH	Synchronous Digital Hierarchy
SGMA	Satellite GMA
SGSN	Serving GPRS Supporting Node
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLS	Service Level Specification
SS7	Signaling System No. 7
TCP	Transmission Control Protocol
TDMA	Time Division Multiplex Access
TFTP	Trivial File Transfer Protocol
TGMA	Terresstrial GMA
TOS	Type Of Service
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
UNI	User Network Interface
UPC	Usage Parameter Control
UT	User Terminal
VBR	Variable Bit Rate
VC	Virtual Circuit
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VLR	Visitor Location Register
VPC	Virtual Path Connection
VPI	Virtual Path Identifier
WAN	Wide Area Network
WCDMA	Wideband CDMA
WLAN	Wireless LAN

List of Publications

[Lep01] S. Lepaja, K.Bengi, "A Random-Reservation Medium Access Protocol For Satellite Networks To Accommodate Real-Time Traffic," IEEE 53rd Vehicular Technology Conference (VTC 2001 Spring), Rhodes, Greece, vol.2, pp. 861-865.

[Ngu01a] H. N. Nguyen, S. Lepaja and H: R. van As, "Mobile Internet Provisioning in Satellite-IP Networks: Mobility Management, Interworking and Integration with Terrestrial Networks", Proc. of the 19th AIAA International Communications Satellite Systems Conference, Toulouse, France, April 2001, pp. 235-245.

[Ngu01b] H. N. Nguyen, S. Lepaja, J. Schuringa and H. R. van As, "Handover management in low earth orbit satellite IP networks", Proc. of the IEEE Global Telecommunications Conference, 2001 (GLOBECOM '01), Saint Antonio, CA, USA, November 2001, vol. 4, pp. 2730-2734.

[Lep02a] S. Lepaja, R. Fleck, and N. Hoang, "QoS Provisioning in to Mobile Internet Environment", In the Proceedings of the European Wireless 2002 (EW2002), February 2002, Florence, Italy, pp. 536-540.

[Lep02b] S. Lepaja, R. Fleck, R. Donner and N. Hoang, "QoS Provisioning to Mobile Internet Users", In the Proceedings of the European Conference on Universal Multiservice Networks (ECUMN2002), April 2002, Colmar, France, pp. 230-237.

[Lep03] S. Lepaja, A. Lila, N. Kryvinskaja and M. Hoang, "A Framework for End-to-End QoS Provisioning in Mobile Internet Environment," In the Proceedings of the Mobile Wireless Communication Networks 2003 (MWCN2003), Sept 2003, Singapore, pp. 86-89.

[Kry03] N. Kryvinskaja, S. Lepaja, and M. Hoang, "Service and Personal Mobility in Next Generation Networks," In the Proceedings of the MWCN 2003, Sept 2003, Singapore, pp. 116-119.