European University Studies

Thi-Thanh-Mai Hoang

Computer Networks, the Internet and Next Generation Networks

A Protocol-based and Architecture-based Perspective

PETER LANG

European University Studies

Europäische Hochschulschriften
Publications Universitaires Européennes

Series XLI
Computer Science

Reihe XLI Série XLI
Informatik
Informatique

Vol./Bd. 46

PETER LANG
Frankfurt am Main · Berlin · Bern · Bruxelles · New York · Oxford · Wien

Thi-Thanh-Mai Hoang

Computer Networks, the Internet and Next Generation Networks

A Protocol-based and Architecture-based Perspective

PETER LANG
Internationaler Verlag der Wissenschaften

Bibliographic Information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the internet at http://dnb.d-nb.de.

ISSN 0930-7311
ISBN 978-3-631-62156-1 (Print)
ISBN 978-3-653-01750-2 (E-Book)
DOI 10.3726/978-3-653-01750-2

© Peter Lang GmbH
Internationaler Verlag der Wissenschaften
Frankfurt am Main 2012
All rights reserved.

All parts of this publication are protected by copyright. Any utilisation outside the strict limits of the copyright law, without the permission of the publisher, is forbidden and liable to prosecution. This applies in particular to reproductions, translations, microfilming, and storage and processing in electronic retrieval systems.

www.peterlang.de

Contents

1. Introduction

1.1 What is The Specific Feature of this Book?

The subject used for designing and developing computer networks is very complex, involving many mechanisms, different protocols, architectures and technologies. To deal with this complexity, authors of many computer network books used layers to describe the computer networks. Examples are OSI/ISO model with 7 layers and TCP/IP model with 5 layers. With a layered architecture, readers, such as students or computer specialists, learn about concepts and protocols in one layer as a part of this complex system, while seeing a big picture of how it all fits together [Kur-2001]. At each layer, the authors described the protocols, their mechanisms and architectures. Because a protocol can be used in several layers and a protocol mechanism can be used in distinct protocols at several layers and at numerous architectures, describing the fundamental protocols and protocol mechanisms before addressing the layered architecture will reduce the protocol complexity, and providing the readers a good overview about the protocol design through knocking the existing protocol mechanisms together.

Unlike the other computer network books, this book starts with a chapter about fundamental protocol mechanisms. Based on these protocol mechanisms, the layered architecture or the Internet protocol suite as a “bottom-up” principle and the Next Generation Network are then described. Thus, each protocol or protocol mechanism is only illustrated one time and the readers then have a depth overview, in which layer and in which protocol or architecture a given protocol mechanism can be used.

1.2 What are the Contributions of this Book?

The main contributions of this script are described in the following. We first provide a rather self-contained survey of techniques including mechanisms, architectures, protocols and services to control the traffic and to ensure the QoS for data and multimedia applications. Evaluation and analysis of these techniques in respect of layers, communication types, application and of QoS achievement are shown.

We then present a depth overview about the Internet protocol suite in respect of the layered architecture and on the basic of the mechanisms and protocols illustrated in the previous section. At each layer, selected protocols and technologies with used mechanisms are discussed. Finally, the next generation

network architecture, its fundamental mechanisms and the IMS (IP Multimedia Subsystem) are described.

The outline of this script is described as follows. Chapter 2 gives background information about computer networks and their design. Section 2.1 provides a brief description of the basis reference models for communication systems. The Multimedia Networking, Next Generation Networking and Mobile Networking as important drivers for the future of fixed-mobile convergence are presented in section 2.2. Consequences for network planning and the network planning considerations are discussed in section 2.3 and 2.4 respectively.

Chapter 3 provides a rather self-contained survey of techniques including architectures, mechanisms, protocols and services for controlling the traffic and guaranteeing QoS at several layers in multi-service computer networks. It starts with the mechanisms for detecting and correcting the packet level and bit level errors. Following it, section 3.2 represents the multiple access control mechanisms and protocols that allow sharing a single broadcast medium among competition users. Section 3.3 introduces the traffic access control mechanisms allowing the filtering of source traffic flows at the network entry and at the specific points within the network. Section 3.4 investigates packet scheduling mechanisms. Mechanisms for congestion control and avoidance at the transport layer and Internet layer are presented in section 3.5 and 3.6 respectively. Section 3.6 describes fundamental mechanisms for unicast and multicast routing and the Internet routing protocols. QoS routing is also investigated. The mechanisms and protocols for admission control and Internet signaling are illustrated in section 3.8 and 3.9. Section 3.10 summarizes the architectures and technologies developed for guarantee the QoS in Internet. Mobility support for both IPv4 and IPv6 are discussed in section 3.11. Section 3.12 gives a brief background on the new transport protocols developed for support end-to-end multimedia communications. Finally, Virtual Private Network (VPN) including MPLS VPNs and multicast VPNs is described in section 3.13. A summary of all protocol mechanisms discussed in chapter 3 is shown in section 3.14.

Chapter 4 represents a depth overview about the Internet protocol suite on the basic of the protocol mechanisms discussed in the chapter 4. The main goal of this chapter is to introduce the students how to design and develop new protocols on the basic of existing protocol mechanisms. It begins with a short introduction to the TCP/IP reference model covering 5 layers (physical, data link, network, transport and application) and its basic terminologies. The physical layer and its major protocol mechanisms are summarized section 4.2. Main services and selected protocols for the data link layer are discussed in section 4.3. Following this, the network layer services and protocols are illustrated in section 4.4. Transport layer services and transport layer protocols

are described in section 4.5. Chapter 4 ends with the application layer services and protocols.

Chapter 5 gives a survey about the next generation networks covering architectures, functions and the IP Multimedia Subsystem (IMS). The fundamental mechanisms illustrated in chapter 3 are also used in this chapter as a basic for describing the architectures, functions and IMS. Finally, conclusion and outlook are given in chapter 6.

2. Fundamentals of Computer Networks, the Internet and Next Generation Networks

Before embarking on an investigation of traffic management and quality of service (QoS) control together with their analysis and design, this chapter starts with a brief description of the basis reference models used for describing the communication systems. It then gives a selection of important applications driving the future of the Internet and the Next Generation Networks toward fixed mobile convergence. Finally, consequences and a review of significant aspects in the computer network planning.

2.1 Network Reference Models

Computer networks do not remain fixed at any single point of time. They must evolve to accommodate changes in the underlying technologies upon which they are based and changes in the service requirements placed on them by applications. Designing a network to meet these requirements is no small task. In order to help deal with this complexity, the OSI (Open Systems Connection) reference model and the TCP/IP reference model have been developed. These reference models define a common network architecture that guides the design and implementation of networks.

2.1.1 OSI Reference Model

The OSI reference model developed by the ISO (International Organization for Standardization) provides a fundamental theoretical model for partitioning the network functionality into seven layers, where the functionality assigned to a given layer is implemented in a set of protocols. Each layer offers certain services to the higher layers, shielding these layers from details of how the offered services are actually implemented [Tan-2003]. Between each pair of adjacent layers there is an interface that specifies which services the lower layer offers to the upper one. The OSI reference model is shown in figure 2-1.

The significant concepts defined in the OSI reference model are layers, protocols, interfaces and services. These concepts and the seven layers of the OSI reference model will be described in this section.

Layer

When the network system gets complex, the network designer introduces another level of the abstraction. The intent of an abstraction is to define a model

that unambiguously describes functions involved in data communication in a way, which allows the capturing of some important aspects of the system, providing an interface that can be manipulated by other components of the system, and hides the details of how a component is implemented from the users of this component.

Abstraction naturally leads to layering. The general idea of layers is to start with the services offered by the underlying hardware as the physical layer, and then add a sequence of layers, each providing a higher level of services. Each layer is responsible for a certain basis services. The services provided at a layer both depend and build on the services provided by the layer below it.

Dividing communication systems into layers has two main advantages. First, it decomposes the problem of designing a network into more manageable components. Instead of implementing one piece of network software that does every thinks, several layers can be implemented, each of which solves one part of the problem. Second, if the network designers decide to add new services, they only need to modify the functionality of the layers relating to these services, using again the functions provided at all the other layers.

Design issues for the layers include a set of mechanisms, for example identification of senders and receivers, error control, congestion control, routing and admission control etc. These mechanisms will be investigated in chapter 3.

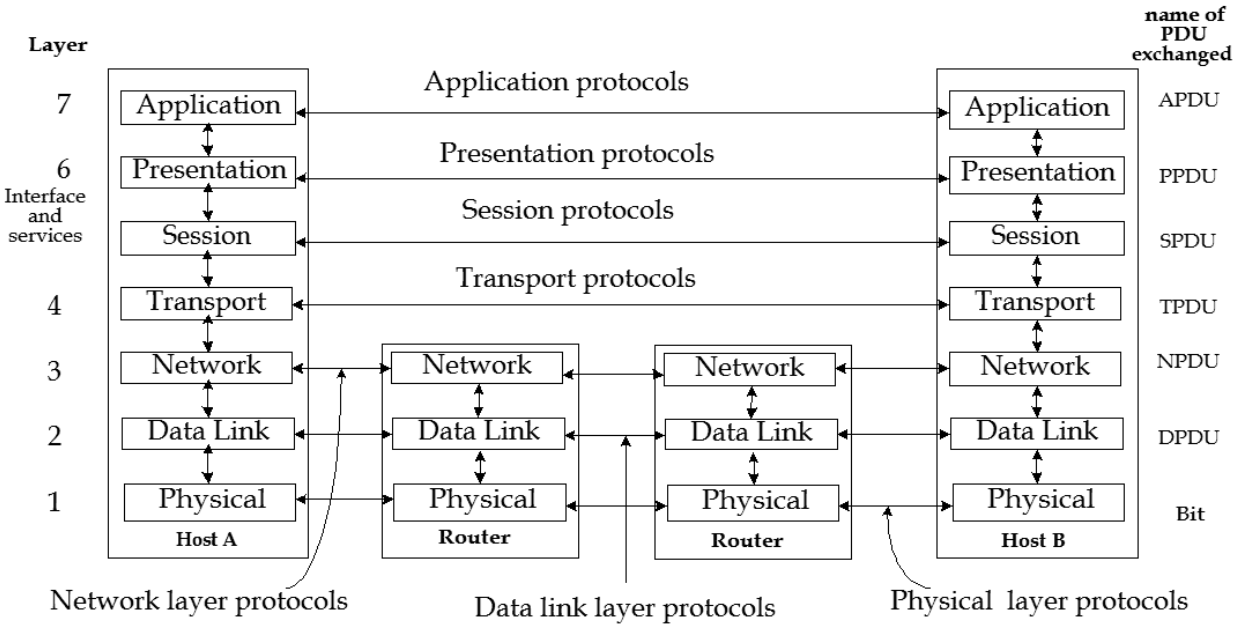

Figure 2-1: The OSI reference model

Protocols

Using the layering concept as a foundation basis, we now discuss the architecture of a network in more detail. Communication between entities at a given layer is performed via one or more protocols. Whereby, a layer-n protocol defines the rules and conventions used in the communication between the layer-n of one system to the layer-n of another system.

In particular, a layer-n protocol defines the message formats and the order of messages exchanged between the layer-n protocol instances of two or more systems, and the actions taken on the sending and receiving of messages or events.

Protocol Data Unit (PDU)

A protocol Data Unit (PDU) is a message unit (e.g. packet, datagram, segment) delivered through a layer of telecommunication systems. A Protocol Data Unit at layer N consists of a header and a payload part. While the header contains the control information (e.g source address, destination address) used for handling this PDU at the layer N, the payload part contains the headers of the upper layer protocols and the user data.

Interfaces and Services

The communication between entities at a given layer is invoked via the interface with the layer below. An interface defines a set of services the lower layer offers to the upper one.

Services can be classified into two classes: connection-oriented and connection-less services. When a connection-oriented service is used, the service user first establish a connection with its communication entity, uses this connection to delivery the data, and then teardowns the connection after finishing the data transfer. In contrast, the user of a connection-less service transmits data to its communication partner without the need of a connection establishment. Also, services can be categorized into reliable and unreliable services. Loosely speaking, reliable service guarantees that data transmitted from a sender to a receiver will be delivered to the receiver in order and in its entirety. Connectionless service does not make any guarantee about the data delivery.

A service is implemented via a set of service functions. Important service function are for example connection establishment, data transfer and connection teardown. A service function is formally specified by a set of service primitives

that are available to a user to access to this service. There are four classes of service primitives: Request, Indication, Response and Confirm [Tan-2003].

The Seven Layers

Starting at the button of the figure 2-1 and working up, the seven layers of the OSI reference model is summarized as follows.

- **Physical layer (layer 1):** The functions of the physical layer include all physical aspects used for communicating between two directly connected physical entities. Typically, these physical properties include electromechanical characteristics of the medium or link between the communicating physical entities such as connectors, voltages, transmission frequencies, etc.
- **Data link layer (layer 2):** the data link layer is responsible for getting the data across a link or across a physical medium. It accepts the raw bit stream provided by the physical layer and provides reliable transfer of data between to directly connected layer-2 entities.
- **Network layer (layer 3):** this layer defines necessary functions to support data communication between indirectly connected entities. It provides services for forwarding packets from a layer-3 entity to another via one or more networks until the final destination is reached. In order for routers to know how to forward packets, they must have some knowledge of network topology. This knowledge may be complete or partial, and is dynamically created and maintained via routing protocols. Thus, routing is a key service at the network layer. If two much traffic is present in a network at the same time, this network may get congested. The control of such congestion is also a service provided at the network layer.
- **Transport layer (layer 4):** The purpose of the transport layer is to provide transparent transfer of data between end users. The perspective of layer 4 is of end-to-end communications rather than the hop-by-hop perspective of layer 3. Layer 4 assumes that packets can be moved from network entities to network entities, eventually getting to the final destination host. How this is accomplished is of no concern to Layer 4 functionality.
- **Session layer (layer 5):** This layer provides mechanisms for structuring and managing the interaction between end user application processes. It provides for either duplex or half-duplex operation and establishes check pointing, termination, and restart procedures.
- **Presentation layer (layer 6):** The presentation layer is concerned with the presentation of user or system data. It presents the data into a uniform

format and masks the difference of data format between two dissimilar systems. It also translates the data from application to the network format. The presentation layer is also responsible for the protocol conversion, encryption, decryption and data compression.

- **Application layer (layer 7):** The application layer defines the interfaces for communication and data transfer. At this layer, communication partners are identified, quality of service is addressed, user authentication and privacy are considered, and any constraints on data syntax are classified.

2.1.2 The TCP/IP Reference Model

The Internet is based on the TCP/IP reference model, which is the successor of the OSI reference model described above. This reference model differs from its predecessor by layer functionalities. The TCP/IP model does not exactly match the OSI model. There is no universal agreement regarding how to describe TCP/IP with a layered model but it is generally agreed that there are fewer levels than the seven layers of the OSI model. Most descriptions present from four to five layers. In this section, TCP/IP reference model is described with five layers shown in figure 2-2.

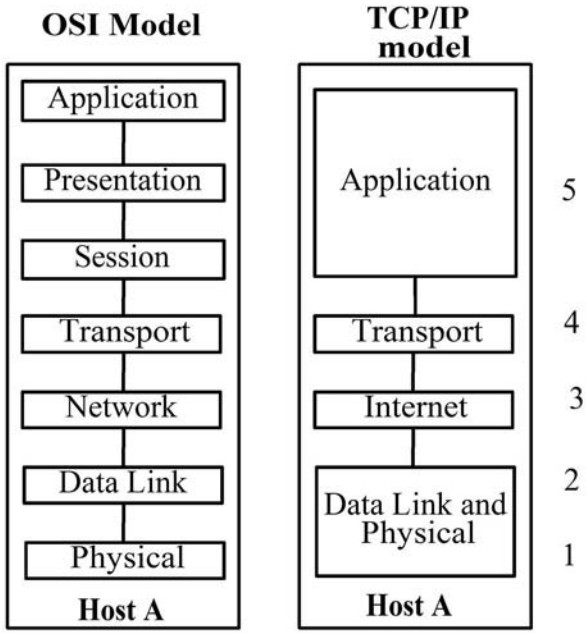

Figure 2-2: The TCP/IP reference model

The TCP/IP protocol stack made up of four layers is shown in figure 2-3. With the IETF public Request for Comments (RFC) policy of improving and updating the protocol stack, TCP/IP protocol model has established itself as the protocol suite of choice for most data communication networks.

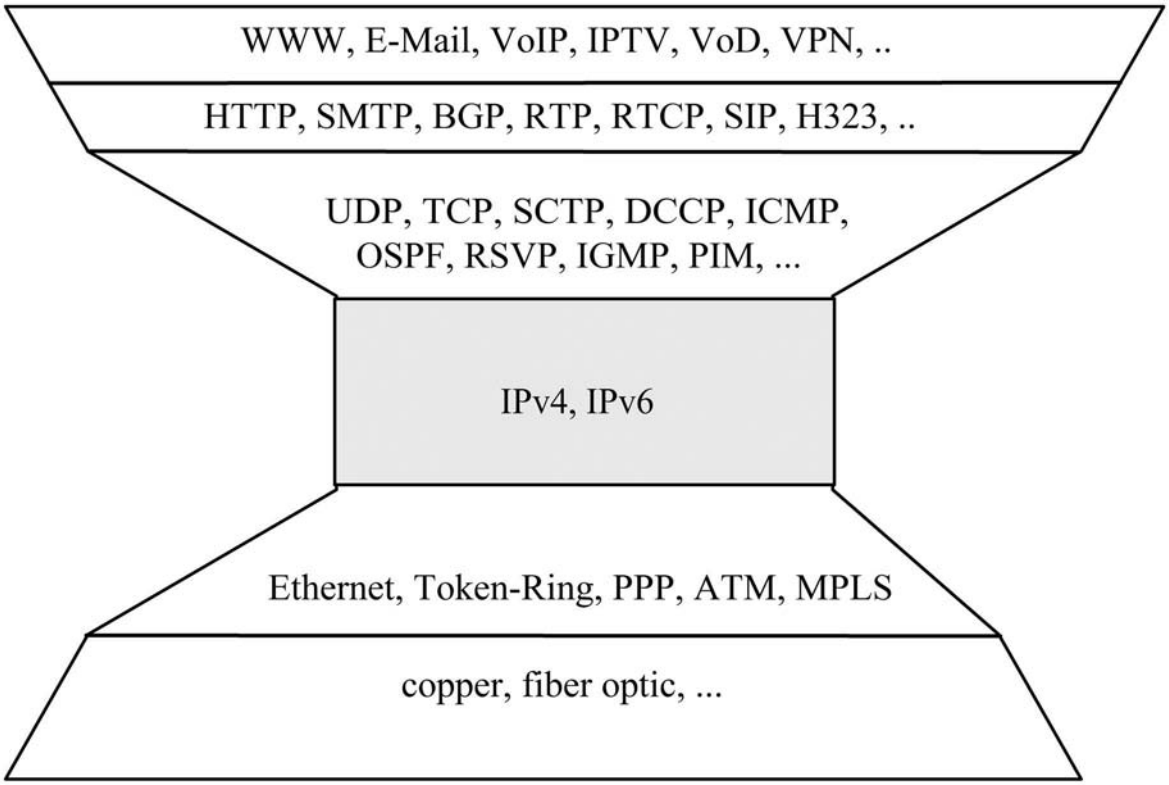

Figure 2-3: Protocol examples in the TCP/IP protocol stack

The layers of the TCP/IP model are:

- **Data link and physical layer:** In TCP/IP model, the data link layer and physical layer are generally grouped together. The data link layer offers services to delivery data between network entities, as well as to detect and possibly correct errors that may occur in the physical layer. Important protocol mechanisms of this layer are the medium access control, framing, addressing, checksum, and error control. The data link layer protocols are for example Ethernet, Token-Ring, FDDI and X.25. The characteristics of the hardware that carries the communication signal are typically defined by the physical layer. Examples of physical layer standards are RS-232C, V.35 and IEEE 802.3
- **Internet layer:** This layer provides functions to enable logical communication between end hosts. The internet layer protocol instance accepts request to send data from the transport layer, converts the transport data to IP packet format, and sends them down to the data link layer for further processing. Services provided at the Internet layer are for example addressing, segmentation/reassemble, routing, congestion control, buffer management, switching, and admission control. Important

protocols at the Internet layer are IPv4, IPv6, ICMP, ICMP, ARP, packet ürocessing mechanisms and the routing protocol OSPF.

- **Transport layer:** This layer provides services that enable logical communication between application processes running on different end hosts. Examples of services provided at the transport layer are multiplexing, demultiplexing, connection management, congestion control and flow control. Two well known protocols at the transport layer are TCP and UDP. Each of these protocols provides a different set of transport layer services to the involving applications.
- **Application layer:** The application layer provides the services which directly support an application running on a host. It contains all higher-level protocols, such as FTP, HTTP, SMTP, DNS and Telnet etc.

2.2 Fixed-Mobile Convergence

Today, multimedia applications are becoming more popular, but they put additional problems for computer networks. The problems associated with multimedia communications include coding of multimedia data, transporting this data from one end to another end, and achieving the required QoS. To solve these problems, computer networks must be able to offer not only the traditional best-effort service but also services for enabling the multimedia communication so that they can transport combined data, voice and video traffic. Such computer networks are called multi-service computer networks. Since multimedia applications (such as VoIP and video on demand) require a certain QoS from the network sites, these networks should evolve to provide QoS guarantee to the users.

In order to facilitate multi-service networks, several technologies have been developed in the last years. Typical technologies are ATM, MPLS, multicast, VPN, VoIP, IPTV, IntServ and DiffServ. Together with these technologies, new mechanisms and protocols for managing and controlling the QoS in multi-service network have been developed.

In the following sections, we first present a selection of important drivers that mainly influence the development and the use of multi-service computer networks.

2.2.1 Multimedia Networking over Internet

Computer networks were originally designed to carry the data only. Today, they are increasingly being used for multimedia applications. The reason for this development is low cost for operators on the high performance IP technology and low prices for consumers.

But, providing an unreliable data transmission and operating as datagram switching, IP networks are not naturally suitable for real-time traffic. Thus, to run multimedia applications over IP networks, several issues must be solved.

Problem Issues

Firstly, in comparison with traditional data applications, some multimedia applications require much higher bandwidth. A single video stream consumes between 1.6 Megabits/s [Mbps] und 12 Mbps depending on the encoding method and whether the stream is standard definition or high definition. Thus the hardware devices have to provide enough buffer bandwidth. But, for most multimedia applications, the receiver has a limited buffer. If no measure is taken to smooth the data stream when data arrives too fast, the buffer will overflow and some data packets will be lost, resulting in bad quality. When data arrives too slowly, the buffer will underflow and the application will starve.

Second, most multimedia applications require the transfer of real-time traffic that must be played back continuously at the rate they are sampled. If the data does not arrive in time, it will be dropped later at the end systems. Some new transport protocols must be used to take care of the timing issues so that audio and video data can be played back continuously with correct timing and synchronization.

Third, there are a lot of multimedia applications that require guaranteed bandwidth when the transmission takes place. So there must be some mechanisms for real-time applications to reserve resources along the transmission path.

Fourth, in addition to the delay, network congestions also have a lot of effects on the quality of the real-time traffic. Packet losses most often occur due to congestion in the routers; more and more packets are dropped at the routers when congestion increases. While the packet loss is one of thinks that make TCP efficient and fair for non real-time applications, the effect of packet losses is a major issue for real-time applications using RTP over UDP and do not support congestion control. This is because the UDP does not have any reaction on packet losses. The transport protocols designed for multimedia applications must take into account the congestion control in order to reduce the packet loss.

Fifth, various multimedia applications are related to the multicast. For example, in video conference, the video data needs to be sent to all participants at the same time. Or in Internet protocol television, a TV channel needs to be sent to all receivers of this channel at the same time.

Solutions

The Internet as multi-service networks carries all type of traffic (e.g. data, video, voice); each of them has different traffic characteristics and QoS requirements. If enough bandwidth is available, the best-effort service fulfils all of these requirements. But when resources are inadequate, however, real-time traffic will suffer from the congestion.

The solution for multimedia networking at the Internet layer is to prioritize all traffic and to provide the service differentiation and QoS for all of this traffic. Technologies developed for this are first of all IPv6, MPLS, DiffServ, IntServ, RSVP, IP multicasting, VPNs, and mechanisms for regulating the traffic and controlling the QoS for these multimedia applications [Hag-2006, Arm-2000, Sna-2005]. Moreover, multicast services need to be taken into consideration in order to reduce the traffic and thus the bandwidth consumption. Thus, IP multicast protocols are specified. Examples are IGMP, PIM (PIM-SSM, PIM-SM, PIM-DM) and DVMRP [FHH-2006].

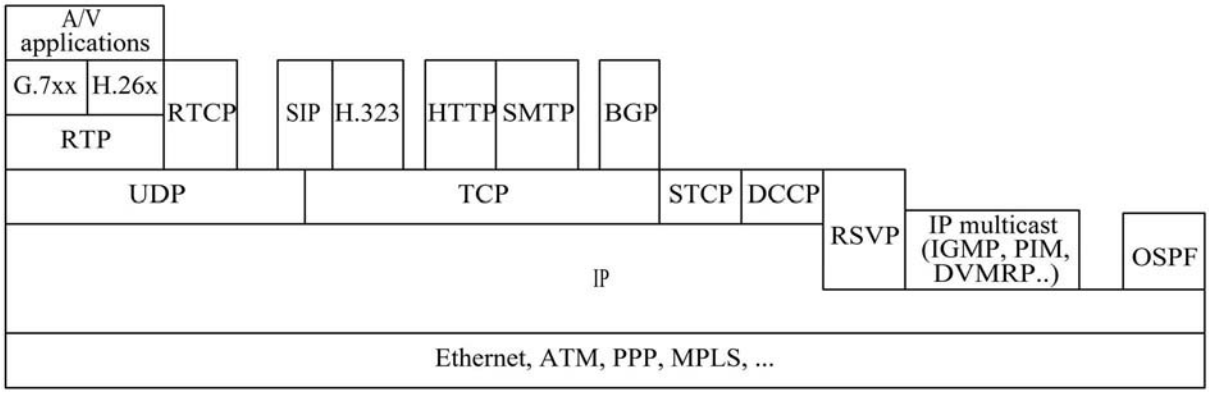

Figure 2-4: Protocols for multimedia communications

In order to provide timing, synchronization and congestion control for multimedia applications, new transport protocols are added into the transport layer. They are RTP, SCTP and DCCP [SCF-2003, CB-2006, KHF-2006]. In comparison with the services provided by TCP and UDP, these new protocols additionally offer several new services such as time reconstruction, loss detection, multi-homing, multi-streaming and congestion control, in respect of multimedia applications. Furthermore, new congestion control mechanisms for multimedia applications and new reliable multicast congestion control protocols are also developed.

At the application layer, services need to be added to compress the multimedia data before sending them over a compute network. This compression will reduce the bandwidth needed for this multimedia data since

multimedia applications require very high bandwidth. Since the best-effort Internet architecture does not provide service to multimedia applications, to support voice transfer over the Internet, two major architectures have been specified. The ITU-T has created H.323 that provides a framework for real-time service in an IP environment [DBP-2006]. The other one is the Session Initiation Protocol (SIP) [RSC-2002; SJ-2006] developed by IETF. SIP is an application-layer signaling protocol for creating, modifying, and terminating multimedia sessions such as the Internet telephony call.

An example of a TCP/IP protocol stack including protocols specified for multimedia communications over the Internet is depicted in the figure 2-4. Details about the protocols and mechanisms for supporting multimedia networking will be described in chapter 3.

2.2.2 Next Generation Networks

A Next Generation Network (NGN) is a packet-based network that enables on the one hand the deployment of access independent services over converged fixed and mobile networks, and on the other hand the use of multiple broadband and QoS-enabled transport technologies in which service-related functions are independent from underlying transport-related technologies [TR-180.000]. NGN is one of four current solutions (GAN – cellular integration; 3GPP – WLAN internetworking; Femtocells; NGNs) for the Fixed Mobile Convergence (FMC), which is the convergence technology offering a way to connect a mobile phone to a fixed line infrastructure so that operators can provide services to their users irrespective of their location, access technology and end terminal.

Next Generation Networks are based on Internet technologies including Internet Protocol (IP) and Multiprotocol Label Switching (MPLS) as the transport technology, and Session Initiation Protocol (SIP) at the application layer. Based on these technologies, NGNs allow the transport of various types of traffic (voice, video, data and signalling). Triple play services (Voice, Internet and TV) are available via Cable and xDSL already. The NGN brings mobility in to the picture and the opportunity for further bundling of high revenue services for customers.

At the core of a NGN is the IP Multimedia Subsystem (IMS), which is defined by 3GPP and 3GPP2 standards and organisations and based on Session Initiation Protocol 8SIP). IMS is a framework consisting of a set of specifications that describe the NGN architecture for implementing Voice over IP (VoIP) and multimedia services. The IMS standard defines architecture and concepts that enables the convergence of data, voice, video, fixed network technologies and mobile network technologies over an IP based infrastructure.

IMS provides an access independent platform for any type of access technologies such as a fixed line, CDMA, WCDMA, GSM/EDGE/UMTS, 3G, WIFI or WiMax. IMS allows features such as Presence, IPTV, Messaging, and Conferencing to be delivered irrespective of the network in use. IMS is anticipated that we are moving into an era where rather than having separate networks providing us with overlapping services, it is the relationship between the user and service that is important and the infrastructure will maintain and manage this relationship regardless of technology. The most obvious overlap currently is between fixed and mobile networks, and the IMS has been identified as a platform for the FMC technology.

Chapter 5 will describe the next generation network architecture, its fundamental mechanisms and the IMS as the core of each NGN and the main platform for the fixed mobile convergence.

2.2.3 Mobile Networks

With the proliferation of mobile computing devices and wireless networking products that demand for accessing to the Internet to get information and services at any time and any where, there is a strong need for the Internet infrastructure to provide mobile devices to connect to the Internet while roaming, preferably without interruption and degradation of communication quality. Mobility support for the Internet refers to the ability to keep active communication of an IP-based device continues during changing of its topological point of attachment to different networks.

Since the Internet was originally designed for communications between fixed nodes, it does not well consider the host mobility problem. The main limitations of the traditional TCP/IP protocol suits for mobility support include the following:

- Limitation of IP addresses: In mobile scenarios, the IP address of a mobile device has to be changed to indicate the change of its point of attachment to the network. But in traditional TCP/IP model, this address change makes other devices impossible to contact with this mobile device, since other devices only know the fixed IP address of the mobile device.
- Limitation of congestion controls at the transport layer: Transport layer protocols use the services provided by the network layer for congestion control. These protocols do not have any mechanisms to discovery the wireless link properties. Thus the congestion control at the transport layer does not distinguish the packet loss caused by wireless link from the normal packet loss in the wired network because of the congestion. It

recognizes the packet loss by wireless link as a congestion, which degrades the transport performance.

- Limitation of applications: Many applications are based on the traditional TCP/IP model and do not support their use in mobile environments. An example is the DNS. Its statically binding a domain name to a host IP address will be invalid because of the dynamic change of IP addresses of mobile devices.

In order to provide the mobility, functional requirements and performance requirements for mobility support in the Internet must be met [LFH-2006]. Functional requirements refer to mechanisms for handover management, location management, multi-homing and security. The performance requirements for mobile environments are specified via a set of performance metrics including handover latency, packet loss, signaling overhead and throughput.

To address these problems, various solutions have been developed that extend the TCP/IP model at several layers to support mobile networking. Some selected approaches will be investigated in the following paragraphs.

Mobility Support in the Network Layer

Mobile IPv4 (MIP4) and mobile IPv6 (MIP6) represent mobility support solutions in the network layer [Per-2002; Mail-2007; JPA-2004; Koo-2007]. MIP4 introduces the address assignment concept that enables a mobile node to get a permanent home network IP address and a foreign network IP address. In order to relay packet between correspondence node (CN) and mobile node (MN), MIP4 additionally defines two new components, the home agent (HA) and the foreign agent (FA). MIP6 resolves the triangle routing problem of MIP4 through a direct communication between the mobile node and the home agent, no foreign agent is needed in MIP6.

Mobility Support in the Transport Layer

In the transport layer, a wide range of investigations has been made to provide mobility support. A lot of solutions for performance improvement and mobility enhancement of TCP has been developed over past years [BB-1995, YB-1994, BKG-2001, BPS-1996, HA-1997, FYT-1997, TXA-2005]. The concept proposed in [BB-1995, YB-1994] is to split a TCP connection between a fixed host and MN into two connections: between the fixed host and the so called mobile support station (MSS) and between MSS and MN. While the first connection is handled by normal TCP, the second connection is optimized for the wireless link.

The authors in [BKG-2001] developed the so called Performance Enhancing Proxy (PEP) network agents that break the end-to-end TCP connection into multiple connections and use different parameters to transfer the data. PEPs are used to improve degraded TCP performance caused by characteristics of specific link environments, for example, in satellite, wireless WAN and wireless LAN environments.

The authors in [FYT-1997] developed the so called TCT Redirection (TCP-R) that keeps connection actively via revising the pair of addresses in the outgoing TCP connections when the IP address associated to the TCP connection is changed by TCP redirection options.

For new transport protocols SCTP and DCCP, mobility support has been proposed [RT-2007; EQP-2006; Koh-2005]. An extension of SCTP to support mobility is proposed in [RT-2007] and called MSCTP. In MSCTP, a MN initiates an SCTP association with the CN by negotiating a list of IP addresses. One of these addresses is selected as the primary address for normal transmission, the other addresses are defined as active IP addresses. When reaching a new network and obtaining a new IP address, MN informs its CN of the new IP address via sending the Address Configuration Change (ASCONF) chunk to CN. On receiving of the ASCONF, CN adds the new IP address to the list of association addresses and reply to MN. While moving, the MN changes the primary path to the new IP address obtained for the new subnet. Thus, the SCTP association can continue to transmit the data while moving to a new network.

Extension of DCCP for supporting mobility is proposed in [Koh-2005]. There are three new features need to be added to DCCP: DCCP-Move packet, two new DCCP packets of mobility capable features, and mobility ID feature.

In order to inform CN that the MN would like to enable to change its address during connection, the MN first sends a Change L option of Mobility Capable feature. On receiving this message, CN sends a Change R option to confirm MN. In response to the Change R option message, MN sends to CN a value of mobility ID feature that will be used to identify the connection. CN replies MN by sending Conform L option. When MN reaches a new network and obtains the new IP address, it informs CN by sending a DCCP-Move packet containing mobility ID value that was chosen for connection identification. On receiving DCCP-Move packet, CN sends DCCP-Sync message to MN, and changes its connection state and begins using new address of MN.

Now we have investigated several solutions for extending the TCP/IP protocol stack for mobility support. It is clear to see that the IP and the transport protocols are considered as key technologies, since their adoptions are expected to create substantial synergies.

2.3 Consequences for Network Planning

New applications and services will change the nature of traffic in future computer networks, having an effect on the amount of traffic and its characteristics. Furthermore, multimedia and mobile applications require QoS-enabling technologies. The significances for network planning and analysis are outlined in this section.

2.3.1 Traffic Demand Characterization

The new applications have different effects on the traffic characteristics. Stream applications, such as video on demand and IPTV, generate highly asymmetric traffic stream with the majority of the data flowing from the server to the client. The amount of traffic depends on the coding scheme, the preferred bit rate, which can be set by the user, as well as the duration of the streaming session. The interactive applications such as telephony and video conferencing typically establish bi-directional sessions between two or more hosts. This results in symmetric traffic flows between end systems.

In comparison with traffic generated by streaming applications and interactive real-time application, the web traffic is sent as small request into one direction that followed by large data transfers into the opposite direction. The characteristics of traffic generated from new applications are different from traffic generated by traditional data applications. These traffics differ in their call-level, packet-level and buffer-level through various traffic variables such as traffic distribution, arrival time, service time, packet size and the scheduling used to serve them. The behavior of traffic variables specified at the packet levels depends on the flow control and congestion control. Web applications use TCP as transport protocol. Thus, TCP flow control and congestion control parameters mainly affect the characteristic of web traffic. But multimedia applications do not use TCP as their transport protocol. They use RTP/UDP with additionally rate-based or TCP-friendly congestion control. Thus the traffic characteristics of these multimedia applications at the call-level and packet-level are big different from the web traffic.

The characteristics of traffic by various applications and at different level need to be considered during network planning process. Especially, for network dimension these characteristics can be exploited for cost savings and for QoS achieving.

2.3.2 Quality of Service Requirements

Originally, the TCP/IP protocol suite was developed to support a single class of best-effort service without guarantee of data delivery and quality of service. The history of this TCP/IP protocol suite shows a clear focus on developing a technology that seeks out and establishes connectivity through sites and end systems. Given knowledge of a packet's ultimate destination, the network will (if at all possible) find a path through any available links that enables the packet's ultimate delivery. The actual time it takes to achieve delivery is at best a secondary consideration. If no path is available, because of either long-term or short-term problems within the network, packets may be discarded. If network experiences the congestion, some packets may also be dropped by routers. If guaranteed delivery is required, the source and destination must utilize additional end-to-end mechanisms, for example the transport protocol TCP, to determine whether their packets are being delivered successfully and, retransmit lost packets if they are not. On the way to destination, all traffic flows share the same resources (bandwidth, buffer space) and receive similar quality of service.

The Need for QoS

Thus, the traditional TCP/IP network mainly focuses on where to send packets and not on the when to send packets as well as not on which packets should be sent first. This has never a problem as long as most applications were data-based and therefore had similar traffic characteristics and QoS requirements. However, in the real world importance is attached to the multimedia and interactive applications, such as chat sessions, audio streaming, video streaming, Voice over IP (VoIP) and Internet Protocol television (IPTV). These multimedia applications generating traffic across an IP network have their own requirements to meet. In particular, these applications are typical less elastic and less tolerant of delay variation and packet loss than data applications. Such applications require some guarantees of quality of service from the network, e.g. a maximum packet delay or a minimal bandwidth.

To provide QoS requirements for multimedia and interactive applications, TCP/IP services must be supplemented with some added features to the nature that can differentiate traffic and provide different service levels for different users and applications.

What is QoS?

Quality of Service is the ability of a network element (application, host, router, and switch) to have some level of assurance that its traffic and service

requirements can be satisfied. To achieve QoS, cooperation of all network layers from top-to-bottom and of every network elements from end-to-end is required.

There are four different viewpoints of QoS: customer's QoS requirements, QoS offered by service provider, QoS achieved by service provider, and QoS perceived by customer [Dvo-2001]. Customer's QoS parameters are focused on user perceived effects, and do not depend on the network design. These parameters might be assured to the user by the service providers through a contrast.

QoS offered by service providers is a statement of the level of quality expected to be offered to the customer by the service provider for Service Level Agreement (SLA). Whereby, each service would have its own set of QoS parameters. QoS achieved by the service provider is a statement of the level of quality actually achieved and delivered to the customer. It is expressed by values assigned to QoS parameters. Based on the customer's QoS requirements, QoS offered and achieved by the service provider will be different from the QoS perceived by the customer.

There is more than one level of criteria to satisfy the different types of traffic (e.g. Voice, video, Internet television, interactive game, chat). The important parameters needed to describe the QoS requirements of these traffics are:

- End-to-end delay indicates the time taken to send a packet from the sender to the receiver. The end-to-end delay is composed of propagation delay, transmission delay, queuing delay and protocol delay.
- Jitter is the variable of end-to-end delay between arrivals of packets at the receiver.
- Throughput is the observed rate at which data is sent through a channel.
- Packet loss rate is the ratio of lost packets and the total packets transmitted
- System-level data rate indicated the bandwidth required, in bits per second.
- Application-level data rate indicates the bandwidth required, in application-specific units such as video frame rate
- Reliability is the percentage of network availability depending upon the various environmental.

In the last years, several fundamental mechanisms [Kes-2001] (e.g. new scheduling disciplines, new congestion controls, new admission controls and new signalling mechanisms) and protocols have been proposed - offering multi-level of services and provisioning QoS for multimedia applications. Moreover, various architectures and technologies (e.g. IntServ, DiffServ, MPLS, VPN) [Hus-2002; San-2006] have been developed that incorporate fundamental

QoS mechanisms within one architecture so that comprehensive QoS-enable networks can be achieved.

These architectures, QoS mechanisms and protocols as well as QoS parameters are necessary but insufficient to provide any service guarantee without considering them within the network planning process. They determine the constraints and objective of network planning and optimisation problems.

2.4 Network Planning Considerations

In order to design a perfect computer network, two important aspects must be considered. They are applications and the network infrastructure. These aspects will be investigated in this paragraph.

2.4.1 Application Considerations

As presented in section 2.1, the highest layer of TCP/IP model is the application layer referring to applications and services they require. Services provided by networks to the applications and the resources required by applications must be taken into consideration when designing the computer networks. In respect of applications, there are a set of issues that must be investigated for the network design.

Bandwidth requirement

Different applications require varying amounts of network bandwidths. For example, a single email application via SMTP does not have the same bandwidth requirement as a video demand application. Bandwidth sensitive applications, such as Internet telephony, require a given amount of bandwidth so that they are able to transmit data at a certain rate to be effective. But elastic applications, such as web transfer or electronic mail, can make use of as much or as little bandwidth as happen to be available.

It is therefore obvious that the bandwidth requirements of applications a network will need to provide, determine link capacities and the node types of the network you will finally design. Thus considering the bandwidth requirements for different types of applications are necessary needed during each network planning process.

Protocol requirement

The TCP/IP application layer supports various application protocols. Choosing an application protocol for a network application directly indicates the selection

of a transport protocol (e.g. TCP, UDP, RTP, SCTP, DCCP). Since TCP and SCTP provide the reliable connection-oriented service and congestion control, and UDP does not support this, the bandwidth requirement for applications using TCP (or SCTP) differs from bandwidth requirement for application using UDP. Moreover, there are applications that require multicast at the network layer. Therefore the routing and the bandwidth requirement for these multicast applications differ from those of the unicast applications. Thus, protocols used by the network applications also need to be considered in the network planning process.

Quality of Service and Type of Service (QoS and ToS)

The reason to consider QoS and ToS is that some user's data is more important than others. Thus there is a need to handle them with different services, for example premium service, controlled load service and best-effort service [San-2002].

The requirement for QoS and ToS has implications for the network planning. For example, routers and switches have to ensure the premium delivery of the traffic for a Voice over IP so as to support the QoS/ToS requirements of this application.

Multicast Communication

Multicast has been proven to be a good way for saving the network bandwidth. It is a main component of Internet Protocol TIVI (IPTV). Thus, multicast service must be taken into consideration while planning the network that supports IPTV or other multicast applications.

2.4.2 Infrastructure Considerations

Network applications running at the end systems need a transport mechanism to transmit user data and control information between them. The transport mechanism is provided by the underlying network infrastructure.

The network infrastructure is an important component in computer network planning. It grows as business expands. Moreover, it not only provides the delivery of user data, but it is also able to adapt to network changes.

In order to build a network infrastructure, several layer of the TCP/IP model must be taken into consideration. Moreover, there are various technologies available for building a network. The design of the Internet Protocol IP over different protocols depends on a set of mechanisms:

- **Encapsulation and overhead**: Because each data link layer protocol has its own frame format and its own transfer mechanisms, the encapsulation of the IP packets into the data link layer frame and the resulting overhead should be evaluated for the network planning purpose.
- **Routing**: Routing is needed to determine the path a packet should follow to reach its final destination. Therefore, selecting a routing protocol to be used for a service will affect the network infrastructure that need to be designed. Thus, routing consideration is very important for the network planning
- **Maximum Transmission Unit (MTU):** Different data link layers have different MTU sizes. The MTU size has an impact on total number of IP packets generated to transmit a piece of user data. Therefore, it has influences on the capacity consumption of the links and nodes of the network infrastructure. Because of this, MTU need to be considered in the IP network design over different data link layer protocols.

Design a network infrastructure involves several decision making processes that take technologies used for the infrastructure (e.g. Ethernet, ATM, and IP/MPLS), the equipments required, the cost for devices and protocols required into consideration.

3. Traffic Management and Quality of Service Control

Protocols are needed for controlling the sending and receiving of messages within the Internet. A protocol may consist of one or several protocol mechanisms. Each of these protocol mechanisms is a method describing a complex sub-function of a protocol. It can be implemented in various communication systems, in different layers and in several protocols. For example, The Internet checksum is a protocol mechanism implemented in TCP, UDP, IP, OSPF, Ethernet, etc. and in different layers of the TCP/IP protocol stacks. In order to develop a new protocol or architecture, it is significantly to have an overview of fundamental protocols and mechanisms. The fundamental mechanisms for traffic management and QoS control will be described in this chapter.

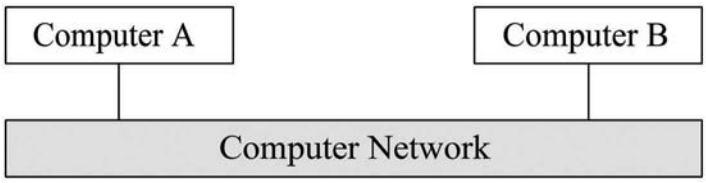

Figure 3-1: Basic scenario for data communication over the Internet

Supposed that the computer A and B are directly connected via a computer network and will exchange data through this network (figure 3-1). During the data transmission between A and B, transmission errors such as delay, loss, duplication and out-of-date of messages may occur. In order to eliminate these errors, a lot of questions must be answered, for examples:

- What is the reason for the errors? How should these errors be recognized and recovered? The answer of these questions deals with the protocol mechanisms for error detection and correction.
- How should senders, receivers and intermediate routers react to overload situations so that the packet losses will be minimal? The solutions for this question deal with the protocols and mechanisms for flow control and congestion control.
- How should senders, receivers and intermediate routers prevent the overload so that the congestion will not arise in the near future? The answer to this question addresses the mechanisms for congestion avoidance and resource reservation.
- How does a network choose a path between two nodes? What if the user wants to choose a path that has least delay, or least cost, or the most

available capacity? How can we send the same data to a group of receivers? The answer to this question addresses multicast routing protocols.

This chapter deals with fundamental mechanisms, protocols and architectures for traffic management and QoS control in Internet.

3.1 Error Control

Communication errors may occur at both bit-level and packet-level. Bit-level errors occur because of the corruption of the bits during the transmission, such as the inversion of an 0 bit to an 1 bit or an 1 bit to a 0 bit. The main reason for this error type relies on the transmission channel, which is not optimal because of noises, loss of synchronization, and of hand-off and fading. For example, the receiver has received the signal of 3 volt although the 0 volt signal was sent. The packet-level errors arise because of the corruption of the PDU (protocol data unit), e.g. packet loss, duplication or reordering of PDUs. Furthermore, the detected but uncorrected bit-level errors are treated as packet-level errors. There are several reasons for packet-level errors, e.g. overload in routers and at the end hosts, too early retransmission of packets, failure of nodes and/or transmission links, etc.

Communication errors discussed above may arise in all layers of computer networks, and, thus for a reliable data transmission, mechanisms for detection and correction of such errors are necessary needed. These mechanisms will add significant complexity to the protocols so that it can provide reliable service if this service is not already offered from the layers below. Communication protocol with an assumption of error-free transmission is very simple to implement but does not have any practical application.

In the next following sub-sections, fundamental mechanisms for detecting and correcting the bit-level and packet-level errors will be described.

3.1.1 Bit-level Error Control

The main principle of the bit-level error control is to add redundancy bits (called error detection code EDC) to the transmitted data at the sender so that the receiver can detect and/or correct the arrived data by using of this redundancy. Mechanisms for bit-level error control can be classified into two classes: bit-level error detection mechanisms, and, bit-level error detection and correction mechanisms. Error detection is done by having the sender only to set enough error-detection bits in the PDU to allow the receiver to deduce that an error occurred. The error correction is similar to error detection, except that a

receiver cannot only detect whether errors have been introduced in the frame but can also determine exactly where in the frame the errors have occurred and hence correct these errors [Kur-2004].

The basis schema for bit error detection is shown in figure 3-2. Supposed, that a datagram of d bits should be sent to a receiver. The sender first adds the error detection code (EDC) to d data bits and transmits the (D+EDC) together to the receiver through a bit-error prone link. When the datagram D' arrives at the destination, the receiver computes the new error detection code EDC' for the incoming datagram and compares with the EDC from the sender to detect the error.

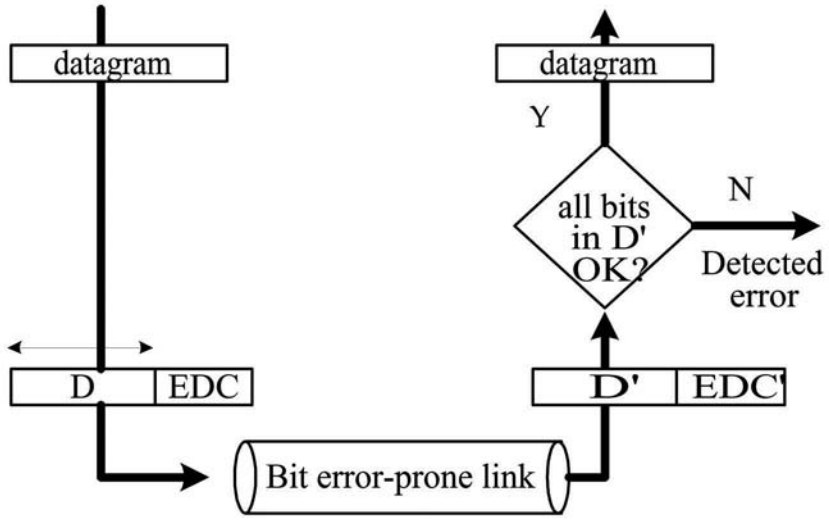

Figure 3-2: Bit error detection schema [Kur-2004]

There are several mechanisms for the bit error detection and correction. Fundamental well-known mechanisms used in Internet are for example parity check, Internet checksum, cyclic redundancy check and forward error correction (FEC) [Kur-2004, Tan-2002, LD-2003].

- **Parity check**. The basic idea of parity check is that the sender includes one addition bit to the data and set its value equal to 1 if the total number of 1s in the d+1 bits (d data bits plus a parity bit) is even. The sender then sends these d+1 bits to the destination. If these bits arrive at the receiver, the receiver counts the number of 1s. If an odd number of 1-valued bits are found with an even parity bit, the receiver knows that at least one bit error has occurred.
- **Internet checksum**. The d bits of data in figure 3-2 are treated as a sequence of 16-bit integers. The concept of Internet checksum is to sum these 16-bit integers and uses the resulting sum as the error detection bits. The sender sends the data together with the calculated Internet checksum.

If the data packet arrives at the receiver, the receiver again calculates the checksum over the received data and checks whether it is equal to the checksum carried in the received data. If it does not match, the receiver recognizes that there are bit errors in the data packet. Internet checksum is implemented in several TCP/IP protocols, for examples TCP, UDP, IPv4, OSPF routing protocol, Ethernet etc.

- **Cyclic redundancy checks (CRC).** CRC is based upon treating bit strings as representations of polynomials with coefficients of 0 and 1 only. A k-bit frame is regarded as the coefficient list for a polynomial with k terms, ranging from xk-1 to x0. The sender and receiver must agree a generator polynomial G(x) in advance. For given d data bits D, the sender will choose r addition bits, EDC, and append them at the end of D in such a way that the polynomial represented by d+r bit pattern is exactly divisible by G(x) by using the modulo 2 arithmetic. The sender then sends this d+r bits to the destination. When this data arrives at the receiver, the receiver divides the d+r bits by G(x). If the remainder is nonzero, the receiver knows that a bit error has occurred; otherwise the data is accepted as being correct.
- **Forward Error Correction (FEC).** FEC enables the receiver to detect and correct the bit errors. The sender adds redundant information to the original packet and sends it to the receiver. The receiver uses this redundant information to reconstruct approximations of exact versions of some of lost packets. FEC is implemented in a lot of protocols used for multimedia communications, e.g. Free Phone and RAT [Kur-2004].

3.1.2 Packet-level Error Control

The packet level error control refers to mechanisms for detecting and correcting the packet-level errors such as loss, duplication and reordering of PDUs. Like bit-level error control, the packet-level error control can be implemented in several protocols and in different layers of communication systems. There are several fundamental mechanisms for detecting and correcting the packet errors, such as sequence number, acknowledgement, timer management, retransmission, automatic repeat request (ARQ), etc. These mechanisms are founded in a lot of communication protocols, e.g. TCP, STCP, and OSPF. Until now, these mechanisms are only described superficial within a particular protocol and were not considered as a separate one. In this section, mechanisms for detecting and correcting the packet level errors will be described.

3.1.2.1 Sequence Number

Senders and receivers use sequence numbers for implementing a reliable data transfer service. The basic principle of packet error detection by using of sequence numbers is very simple. A sequence number in the header of a PDU indicates its unique position in the sequence number of PDUs transmitted by the source. For using the sequence number, before sending the PDU to its destination, the sender labels each PDU that has not been previously transmitted with a consecutive sequence number in the PDU header. The receiver knows which sequence numbers already arrived and thus which sequence number the receiver expects to receive as the next. When a PDU arrives at the receiver, the receiver then reads the sequence number from the header of this PDU and compares with the expected sequence numbers. By this way, the receiver can detect losses, duplication and reordering of packets. If this sequence number is less than receiver's expected sequence number, the receiver knows that this PDU is duplicated and drops it. If this sequence number higher than receiver's expected sequence number, the receiver knows that the packet with the expected sequence number was lost and thus it can request the sender to resend it. Otherwise, if the sequence number is equal to the expected sequence number, the receiver knows that the PDU is correctly arrived. The receiver then processes its header, taking actions depending on header information and on the events arrived.

A well-known example for the using of sequence numbers is found in TCP. Each TCP segment header contains a 32-bit sequence number field. Each TCP segment carries its own sequence number not only during data transmission but also during the TCP connection establishment and release.

3.1.2.2 Acknowledgement

In order to develop a reliable data transfer service, acknowledgement mechanism is used together with sequence number. Acknowledgement enables the receiver to let the sender know whether its data is correctly received or a packet error has occurred. Thus, acknowledgement is used for detecting the packet level error. This mechanism functions as follows. Each time when the data arrives at the receiver, the receiver sends an acknowledgement PDU to the sender of this data. The acknowledgement number field in each acknowledgement PDU will tell the sender about the PDUs arrived at the destination. There are four variants of acknowledgements which can be implemented in each reliable protocol:

- **Positive acknowledgement (ACK):** The receiver informs the sender that it correctly received the data.