QUESTION 16/2
Preparation of handbooks for developing countries

ITU-D STUDY GROUP 2 2nd STUDY PERIOD (1998-2002)

Handbook on new technologies and new services

FASCICLE 3
IP Based Networks and Services

Telecommunication Development Bureau (BDT)
International Telecommunication Union

THE STUDY GROUPS OF ITU-D

The ITU-D Study Groups were set up in accordance with Resolutions 2 of the World Telecommunication Development Conference (WTDC) held in Buenos Aires, Argentina, in 1994. For the period 1998-2002, Study Group 1 is entrusted with the study of eleven Questions in the field of telecommunication development strategies and policies. Study Group 2 is entrusted with the study of seven Questions in the field of development and management of telecommunication services and networks. For this period, in order to respond as quickly as possible to the concerns of developing countries, instead of being approved during the WTDC, the output of each Question is published as and when it is ready.

For further information

Please contact:

Ms Alessandra PILERI
Telecommunication Development Bureau (BDT)
ITU
Place des Nations
CH-1211 GENEVA 20
Switzerland
Telephone: +41 22 730 6698
Fax: +41 22 730 5484
E-mail: alessandra.pileri@itu.int

QUESTION 16/2
Preparation of handbooks for developing countries

ITU-D STUDY GROUP 2 2nd STUDY PERIOD (1998-2002)

Handbook on new technologies and new services

FASCICLE 3
IP-based networks and services

Telecommunication Development Bureau (BDT)
International Telecommunication Union

Action required: Participants are invited to send their comments to the BDT Secretariat **by May 2001 at the latest**. After inclusion of the comments received, Fascicle 3 will be published in 2001. All the chapters relating to abbreviations will be completed during the September meeting. This fascicle has not yet been edited.

FASCICLE 3

IP-based networks and services

TABLE OF CONTENTS

Page

FASCICLE 3

IP-based networks and services

CHAPTER 1

Introduction and Definitions

1.1 Internet Definition

A network connecting many computer networks and based on a common addressing system and communications protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). From its creation in 1983 it grew rapidly beyond its largely academic origin into an increasingly commercial and popular media.

By the mid-1990s the Internet connected millions of computers throughout the world. Many commercial computer network and data services also provided at least indirect connection to the Internet.

The original uses of the Internet were electronic mail, file transfer (using ftp, or file transfer protocol), bulletin boards and newsgroups, and remote computer access (telnet). The World Wide Web, which enables simple and intuitive navigation of Internet sites through a graphical interface, expanded dramatically during the 1990s to become the most important component of the Internet.

The Internet had its origin in a U.S. Department of Defence program called ARPANET (Advanced Research Projects Agency Network), established in 1969 to provide a secure and survivable communications network for organisations engaged in defence-related research. Researchers and academics in other fields began to make use of the network. At length the National Science Foundation (NSF), which had created a similar and parallel network called NSFNet, took over much of the TCP/IP technology from ARPANET and established a distributed network of networks capable of handling far greater traffic. NSF continues to maintain the backbone of the network (which carries data at a rate of 45 million bits per second), but Internet protocol development is governed by the Internet Architecture Board, and the InterNIC (Internet Network Information Centre) administers the naming of computers and networks.

Amateur radio, cable television wires, spread spectrum radio, satellite, and fibre optics have been used to deliver Internet services. Networked games, networked monetary transactions, and virtual museums are among applications being developed that both extend the network's utility and test the limits of its technology.

1.1.1 Electronic Mail

Abbreviation: E-MAIL. Messages transmitted and received by digital computers through a network. An electronic mail, or e-mail, system allows computer users on a network to send text, graphics, and sometimes sounds and animated images to other users. On most networks, data can be simultaneously sent to a universe of users or to a selected group or individual. Network users typically have an electronic mailbox that receives, stores, and manages their correspondence. Recipients can elect to view, print, save, edit, answer, or otherwise react to communications. Many e-mail systems have advanced features that alert users to incoming messages or permit them to employ special privacy features. Large corporations and institutions use e-mail systems as an important communication link among employees and other people allowed on their networks. e-mail is also available on major public online and bulletin board systems, many of which maintain free or low-cost global communication networks.

1.1.2 World Wide Web

(WWW), byname THE WEB, the leading information retrieval service of the Internet. The Web gives users access to a vast array of documents that are connected to each other by means of hypertext or hypermedia links. The Web operates within the Internet's basic client-server format (*servers are computer programs that store and transmit documents to other computers on the network when asked to, while clients are programs that request documents from a server as the user asks for them*). Browser software allows users to view the retrieved documents.

A hypertext document with its corresponding text and hyperlinks is written in hypertext Markup Language (HTML) and is assigned an online address called a Uniform Resource Locator (URL).

Tim Berners-Lee began the development of the World Wide Web in 1989 and his colleagues at CERN, an international scientific organization based in Geneva, Switzerland. They created a protocol, hypertext Transfer Protocol (HTTP), which standardized communication between servers and clients. Their text-based Web browser was made available for general release in January 1992.

1.1.3 ARPANET

In 1969 the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense established a data communications network called ARPANET. By using packet-switching techniques, ARPANET connected heterogeneous computers located at universities and military installations anywhere in the United States. It was the first network to use layered protocols, flow control, and fault-tolerance – exemplified by the fact that a node could disappear without bringing down the entire network or requiring any operator intervention. The word "packet" was coined by ARPANET developers to distinguish between the longer messages generated by computers and the smaller segments used by ARPANET to improve data throughput. The Internet, an outgrowth of ARPANET, connects millions of computers worldwide.

1.1.4 Hyperlinks

Hyperlinks, electronic connections that link related pieces of information in order to allow a user easy access to them. Hypertext allows the user to select a word from text and thereby access other documents that contain additional information pertaining to that word; hypermedia documents feature links to images, sounds, animations, and movies.

1.2 List of Abbreviations

ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
E-MAIL	Electronic Mail
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
InterNIC	Internet Network Information Centre
NSF	National Science Foundation
TCP/IP	(Transmission Control Protocol/Internet Protocol)
URL	Uniform Resource Locator
WWW	World Wide Web

CHAPTER 2

Internet Communication

2.1 Introduction

The Internet is a large collection of networks that are linked together so that users of any one of the networks can reach users on any of the other networks. Internet communication is governed by a series of protocols which are structured to interact with each other.

2.2 Communication Architecture

There are three aspects of network communication:

- Data Exchange
- Data Interpretation
- System Management

Communication Architecture is defined in layers where each layer has its own functions but also uses the functions of the layer below. The Transmission Control Protocol (TCP) and the Internet Protocol (IP) are part of a large set of protocols which describes an entire communications architecture, called the Internet Protocol Suite.

2.2.1 Internet Protocol Suite

The Internet Protocol Suite is divided into lower level and upper level protocols.

2.2.1.1 Lower Level Protocols

At the lower level of the communications architecture are the communications protocols TCP and IP, which describe the communication aspects of the Internet Protocol Suite.

TCP/IP standards include descriptions of how IP operates over common long-distance and local physical communications networks.

2.2.1.2 Upper Level Protocols

The upper level protocols describe the standard mechanisms for interpreting and converting data for the common tasks that computer users perform, such as: File Transfer, Terminal Access, Mail Preparation and Transfer.

2.3 The TCP/IP Protocol Stack

Communications protocols or standards are defined in layers. The Model resulting from the layers defined is often referred to as a Protocol Stack. The Internet Protocol Suite has 5 Layers. However Layer 1 and 2 are not defined in the TCP/IP protocol suite as TCP/IP is actually independent of physical media. The three layers of the TCP/IP protocol suite are:

2.3.1 The Network Layer

This layer provides a basic datagram service, that is, IP transfers data with its best effort, but with no guarantee of delivery. The Internet Control Message Protocol (ICMP) which is provided with this layer, reports problems in the transmission of data.

2.3.2 The Transport Layer

There are two possible transport options.

UDP The User Datagram Protocol extends IP's connectionless datagram service to applications that do not require reliability.

TCP Transmission Control Protocol provides a reliable transport service with error correction and flow control.

2.3.3 The Application Layer

The Application layer is responsible for interfacing between end-user applications and the Transport layer services. It provides services for the different types of application that might wish to use the network. It does not provide the application itself, although the two are closely related.

2.4 Internet Applications and their Protocols

Most TCP/IP application layer protocols are based on the client-server model, where the protocol consists of simple interactions between the client and the server.

Three basic protocols are outlined here, FTP, LDAP and Telnet.

2.4.1 File Transfer Protocol

File Transfer Protocol provides a mean for moving files from one computer system to another and provides the facilities for managing files on remote systems. FTP is used to:

- Upload files to a server
- Download files from a server
- Show or change the current disk directory
- Delete files from directory
- Rename files

During an FTP session there are two separate network connections between the client and the server. First, there is a control connection between the client and server, enabling connection requests to pass between them. When the control connection is set up, the client then usually sends out a control message, which contains the port number on which it is willing to accept an incoming data connection request.

Because of the separate connections for control and data, we can specify different types of service for both. For example, it is advantageous to have minimum delay for the control connection and maximum throughput for the data connection.

When a file transfer takes place there are four aspects of the transfer that must be specified:

- File Type: this dictates how the data in the file is to be changed into a form that is suitable for transmission. For example, a text file may be converted to NVT ASCII for transmission then converted back to a text file at the receiving end.

- Format Control. This defines the way a text file is transferred to a printing device.
- Structure. This allows the file's internal structure to be preserved on transfer to the remote host.
- Transmission mode. The file can be transferred as a series of bytes or block by block, or in compressed mode.

2.4.2 Directory Services Application Layer Protocols

The Lightweight Directory Access Protocol (LDAP) consists of a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, the X.500 standards defines how global directories should be structured. Unlike X.500, LDAP supports TCP/IP and is occasionally referred to as X.500 Lite.

LDAP is an open protocol, so applications do not need to know the type of server that hosts the directory.

LDAP enables corporate directories to be arranged in a hierarchical structure that reflects geographic and organizational boundaries.

The directories are arranged in such a way that the country information appears under the root node, followed by organizations, organizational units, for example departments within companies, then finally individuals. LDAP can also hold a global registry of public keys that are used for secure data transfer.

2.4.3 Telnet

Telnet is a virtual terminal protocol of TCP/IP. It operates over the TCP error-corrected Transport layer and provides total terminal interconnectivity and interoperability. Telnet gives terminal users the ability to logon to many different telnet hosts from a single terminal.

2.5 List of Abbreviations

ASCII	American Standard Code for Information Interchange
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol

CHAPTER 3

Internet Protocol (IP)

3.1 Introduction

IP is a connectionless protocol primary responsible for addressing and routing packets between network devices. Connectionless means that the session is not established before exchanging data.

IP is unreliable in that delivery is not guaranteed. It makes the "best effort" attempt to deliver a packet. Along the way a packet may be lost, delivered out of sequence, duplicated or delayed.

IP delivers its packets in a connectionless mode. It does not check to see if the receiving host can accept data and it does not keep a copy in case of errors. IP is therefore said to "fire and forget".

IP is also responsible for fragmenting and reassembling packets. A large packet must be divided into smaller pieces when the packet has to traverse a network that supports a smaller packet size.

3.1.1 Fragmentation

Each physical network imposes some maximum transmission (the maximum transfer unit (MTU)) size on the packets that may be sent over it. When the size of the packet exceeds the MTU of the network on the outgoing interface, it must be broken into smaller packets, each of which carries a portion of the original data. This process is called fragmentation.

The fragmented IP packets have data copied from the original packet into their data area. Each fragment contains an IP header that duplicates the original header except for the information in the flags and offset fields. They are treated as normal IP packets while transported to their destination. Therefore the fragment packets may take different routes to their final destination.

When the fragment packets arrive at their destination, the destination host must join the fragments together again before processing the original packet in the normal way.

However, if one packet gets lost, the complete IP packet is considered lost.

If a packet has a flag to "don't fragment" and the router decides to send this packet over a medium that does not support the size of the packet, then the packet is dropped.

3.2 IP Packet Structure

<table>
<tr><th colspan="8">32 bits (4 bytes)</th></tr>
<tr><th colspan="2">I</th><th colspan="2">II</th><th colspan="2">III</th><th colspan="2">IV</th></tr>
<tr><td>Version</td><td>IHL</td><td colspan="2">Type of Service</td><td colspan="4">Total Length</td></tr>
<tr><td colspan="4">Identification</td><td>Flags</td><td colspan="3">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td colspan="2">Protocol</td><td colspan="4">Header Checksum</td></tr>
<tr><td colspan="8">Source Address</td></tr>
<tr><td colspan="8">Destination Address</td></tr>
<tr><td colspan="6">Option (Variable)</td><td colspan="2">Padding</td></tr>
<tr><td colspan="8">Data (Variable)</td></tr>
</table>

Version (4 bits): This specifies the version of the IP protocol and hence the format of the IP header being used. The current protocol version is 4 (IPv4), the new version is 6 (IPv6).

IHL, Internet Header Length (4 bits): This is the length of the header in 32-bit words. The minimum value is five, which is the most common header. Thus the header must be at least 20 bytes long.

Type of Service (8 bits): This is an indication of the quality of service requested for the IP packet. It specifies reliability, precedence, delay and throughput parameters.

Total Length (16 bits): This is the total packet length, including header and data, in bytes.

Identification (16 bits): This is a unique number assigned by the sending device to assist in reassembling a fragmented packet. Its primary purpose is to allow the destination device to collect all fragments from a packet, since they will all have the same identification number.

Flags (3 bits): These provide the fragmentation control fields.

The first bit is not used and is always 0.
If the second bit is 0, it means, "May fragment".
If the second bit is 1, it means, "Don't fragment".
If the third bit is 0, it means, "Last fragment".
If the third bit is 1, it means, "More fragment".

Fragment Offset (13 bits): This is used with fragmented packets to assist in reassembling the full packet. The value is the number of 8-byte pieces (header bytes are not counted) that are contained in earlier fragments. In the first fragment or in a unique fragment, this value is always zero.

Time to Live (8 bits): This contains the time, in seconds, that the packet is allowed to remain on an internetwork. Each IP device that the packet passes through will decreases the value by the time it takes it to process the IP header. All routers must decrease this value by a minimum of one. If the value is dropped to zero the packet is discarded. This guarantees that packets cannot travel around an IP network in a loop, even if routing tables become corrupt.

Protocol (8 bits): This indicates the higher level protocol to which IP should deliver the data in the packet, for example UDP is 17 and TCP is 6.

Header Checksum (16 bits): This is a checksum on the header only, which ensures integrity of header values. The sending IP device performs a calculation on the bits in the IP header, excluding the header checksum field, and places the result in the header checksum field. The receiving device performs the same calculation and compares the result with the value in the header checksum field. If they are different then an error has occurred and the IP packet is discarded.

Source Address (32 bits): This is the 32-bit IP address of the sending device.

Destination Address (32 bits): This is the 32-bit IP address of the receiving device.

Options (variable): These are not required in every packet. They are mainly used for network testing and debugging.

Data (variable): The total length of the data field plus header is a maximum of 65,535 bytes.

3.3 The IP Address

Every network interface on a TCP/IP device is identified by a globally unique IP address. Host devices, for example PCs, typically have a single IP address. Routers typically have two or more IP addresses, depending on the number of interfaces they have.

Each IP address is 32 bits long and is composed of four 8-bit fields called octets. This address is normally represented in "dotted decimal notation" by grouping of four octets and representing each octet in decimal form. Each octet represents a decimal number in the range 0-255.

For example 11000001 10100000 00000001 00000101 is 193.160.1.5

Each IP address defines the network ID and host ID of the device. The network ID part of the IP address is centrally administered by the Internet Network Information Centre (InterNIC) and is unique throughout the Internet. The Host ID is assigned by the authority that controls the network.

The network ID identifies the systems that are located on the same network or subnet. The network ID must be unique in the internetwork.

The host ID identifies a TCP/IP network device (or host) within a network. The address for each host must be unique to the network ID.

An IP address is 32 bits length, divided into two or three parts. The first part makes up the network address, the second part makes up the subnet address (if used) and the third part makes up the host address.

IP address = <network number><host name>

There are five different address classes supported by IP addressing. The class of an IP address can be determined from the high-order (left most) bits.

3.3.1 Class A

Class A addresses are assigned to networks with a very large number of hosts. The high-order bit in a class A is always set to zero. The next seven bits (completing the first octet) represent the network ID and provide 126 possible networks. The remaining 24 bits (the last three octets) represent the host ID; each network can have up to 16,777,214 hosts.

3.3.2 Class B

Class B addresses are assigned to medium-sized to large-sized networks. The two high-order bits in class B address are always set to binary 10. The next 14 bits (completing the first two octets) represent the network ID. The remaining 16 bits (last two octets) represent the host ID. Therefore, there can be 16,382 networks and up to 65,534 hosts per network.

3.3.3 Class C

Class C addresses are used for small networks. The three high-order bits in class C address are always set to binary 110. The next 21 bits (completing the first three octets) represent the network ID. The remaining 8 bits (last octet) represent the host ID. Therefore, there can be 2,097,150 networks and 254 hosts per network.

3.3.4 Class D

Class D addresses are used for multicast group usage. A multicast group may contain one or more hosts or none at all. The four high-order bits in class D address are always set to binary 1110. The remaining bits designate the specific group in which the client participates. There are no network or host bits in the multicast operations. Packets are passed to a selected subset of hosts on a network. Only those hosts registered for the multicast operation accept the packet.

3.3.5 Class E

Class E is an experimental address not available for general use; it is preserved for future use. The high-order bits in class E address are set to 11110.

3.4 Voice Over IP

3.4.1 Traditional Telephony vs IP Telephony

Traditional telephony uses circuit-switched technology, where an end-to-end circuit is set up between two telephones. A circuit-switched connection is established for the duration of every telephone call, with a fixed bandwidth (64 kbit/s) reserved even during silent periods.

IP telephony uses the Internet Protocol to transmit voice as packets over an IP network. In an IP telephony connection, the voice signal is digitized, compressed and converted into IP packets, which are transmitted over the IP network and shared with other IP traffic. An IP packet-based network moves information at a much lower cost by making better use of the network capacity. Not only is a packet-based shared network more efficient than a fixed 64 kbit/s circuit-switched connection, but it also compresses the voice signal.

IP telephony can be implemented, at least in principle, on any data network that uses IP, such as the Internet, Intranets or LANs. To accomplish this, a device called a “voice over IP gateway” provides the connection between the telephone network and the IP network.

3.4.2 IP Telephony Scenarios

IP telephony encompasses a number of different services including phone-to-phone, PC-to-phone, phone-to-PC, PC-to-PC and fax-to-fax, as well as videoconferencing and collaboration from the desktop.

In an IP telephony solution, it is possible to have a combination of PC-based telephony applications and phones connected to the PSTN.

In a phone-to-phone scenario, the gateway has the functionality needed in order to send and receive voice over an IP network in real time.

In a PC scenario, an IP telephony client is needed. The client digitizes, compresses and packetizes the voice signal and transmits it over the IP network. Standard telephone calls are connected to a voice gateway and IP telephony calls are connected to a telephone or a PC.

IP telephony client software may also allow users with multimedia PCs to have video and audio conferences, share documents and use a whiteboard, enabling a more efficient work environment.

Fax-to-fax IP telephony includes both real-time fax and store-and-forward fax.

In real time, the fax is sent directly from the sending machine to the receiving machine. Store-and-forward faxing connects a server to a gateway. This server acts as a destination fax, storing the fax until it is retransmitted to the real destination. Using this method, faxes can be held back when there are high network loads.

3.4.3 Benefits of IP Telephony

Cost Reduction: The possibility of making cheap calls over the Internet/Intranet generates most of the interest in IP telephony today. Internet home users can call abroad for the price of a local call, totally bypassing the long distance telephone network. Companies can do likewise. IP telephony provides company headquarters with an alternative way to contact branch offices and can result in significant cost savings, especially if the company has a corporate Intranet that it can reuse for voice traffic.

Better Use of Network: IP telephony makes more efficient use of the existing communications infrastructure. Since IP telephony uses a packet-switched network, a number of calls share the same network link, and there is better use of that link and lower transmission costs.

Bandwidth Utilization: With voice/data integration, voice and fax are converted into data and placed on the IP network for transport to a remote location. With the compression techniques now available, it is possible to use high-capacity IP networks for real-time traffic as well as for the traditional, less demanding traffic such as e-mail and file transfers.

Reduced Management and Operational Costs: IP Telephony makes it easier to integrate voice communications with different applications and services on the IP network, thereby providing a unified service. Integrating the voice and data networks into one network reduces management and operational costs.

Service Integration: Service integration makes it possible for one network to support a large number of services. As a result, operational costs can be reduced and new advanced services created.

3.4.4 Issues with IP Telephony

Voice Quality: When data is being transferred throughout an IP network, a slight delay with packets is usually not noticeable. Moreover, retransmission of discarded packets usually compensates for the loss of packets. However, when IP packets transport digitized voice the loss or delay of packets results in the disruption of speech intelligibility.

The voice gateway introduces delay because of compression, decompression, packetization and depacketization. The router-induced delay depends on the capacity of the router and the number of router hops from originating voice gateway to terminating voice gateway.

From the end-user point of view, the delay encountered in the communication has to be below a certain threshold (approximately 200 ms); otherwise the communication will be considerably less useful.

Interoperability: Interoperability relates to products from different vendors as well as different carrier networks. Interoperability issues exist mainly because standardization is not yet mature in IP telephony. There are no universally implemented or agreed standards for signalling, calling, accounting or billing.

The voice-over-IP forum and ITU are developing standards, such as H.232 and Tiphon (Telecommunications and Internet Protocol Harmonization Over Networks), to improve interoperability between different vendors' products.

Security: The basic security issues are:

- User and Data Authentication
- Data Privacy (Integrity and Confidentiality)
- Access Control
- Policy Management

Network security is related to the routing side of IP. In a public Internet, the packets can traverse through any router and can be intercepted by anyone. Acceptable security can be obtained by encryption (secure socket layer-SSL) and tunnelling (Layer 2 Tunnelling Protocol-L2TP).

Integration with PSTN: The major issue for integration of IP telephony and PSTN is making the PSTN and the IP telephony network appear to be one network to the end user and easy to manage by the operator.

3.5 IPv4 and IPv6

The main cause for change was due to the limited address space. When IP was defined, only a few computer networks existed. The designers decided to use 32-bit addresses which would allow them to include a million networks. However, the global Internet is growing exponentially, with the size more than doubling annually. At this current rate, all prefixes will soon be assigned and no further growth will be possible.

Secondary reasons for change are new Internet applications. For example, applications that deliver audio and video need to deliver data at a regular intervals. To keep such information flowing thought the Internet without disruption, IP must avoid changing routes frequently.

The security implemented in IPv6 guarantees that a packet is actually coming from the host indicated in its source address.

3.5.1 New Features in IPv6

The new features in IPv6 can be grouped into the following categories:

Address Size: IPv6 uses 128-bit addresses instead of 32-bit addresses of IPv4. This is an increase of address space by a factor of 2^{96}. The address space provided by IPv6 is large enough to accommodate continued growth of the Internet for many decades. There are enough addresses supported by IPv6 to provide an order of $6*10^{23}$ unique addresses per square meter of the surface of the earth.

Improved Options Mechanism: IPv6 options are placed in separate optional headers that are located between the IPv6 header and the transport layer header. Most of these optional headers are not examined or processed by any router on the packet's path, which simplifies and speeds up router processing of IPv6 packets compared to IPv4 packets.

Address Autoconfiguration: this capability provides for dynamic assignment of IPv6 addresses via stateful or stateless address autoconfiguration. DHCP is termed a stateful address configuration tool because it maintains static tables that determine which addresses are assigned to a new or moved stations.

Increased Addressing Flexibility: IPv6 included the concept of an anycast address, for which a packet is delivered to just one of a set of nodes. The scalability of multicast routing is improved by adding a scope field to multicast addresses.

Support for Resource Allocation: instead of the type of service field in IPv4, IPv6 enables the labelling of packets belonging to a particular traffic flow for which the sender requests special handling. This aids in the support of specialized traffic, such as real-time video.

Security Capabilities: IPv6 includes features that support authentication and privacy.

3.6 List of Abbreviations

DHCP	Dynamic Host Configuration Protocol
IHL	Internet Header Length
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
L2TP	Layer 2 Tunnelling Protocol
MTU	Maximum Transfer Unit
PSTN	Public Switched Telephone Network
SSL	Secure Socket Layer
Tiphon	Telecommunications and Internet Protocol Harmonization Over Networks

CHAPTER 4

E-Commerce

4.1 Introduction and Definition

Online business is no longer a prediction – it is a reality that presents new risks and new opportunities to businesses from all sectors of the economy. Online consumer and corporate purchases already exceed USD 13 billion annually and forecasts predict global electronic commerce of more than USD 3 trillion by 2003!

The most basic-form definition of Electronic Commerce would refer to transactions that are handled electronically rather than on paper. The Internet, for e-commerce merchants, is considered a virtual meeting place for buyers and sellers. It is a medium for communicating multiple aspects of a transaction from product features to competitive comparisons as well as "cashless" transactions conducted over computer networks.

Senior management in many organizations are beginning to realize that a large portion of their business will be conducted online in the very near future. Now is the time to make sure you're ready; that every department is aware of the opportunities that exist online, and are in a position to best exploit them.

The benefits for customers of using e-commerce can be summarized as follows:

- Increases customer value by making the buying process easier
- Gives customers 24-hour/365/-day accessibility and instant access to vital information
- The speed will be greater and process quality will increase

CHAPTER 5

Basic Internet Services

5.1 Introduction

Basic Internet Services, such as mail, news and web services, are offered to the end user over wide area networks. The BIS sit on top of the platform and use the platform functions, such as security, charging and data storage.

5.2 Web Services

Several services are available, which provide the end user with functions to store and retrieve and browse web information. A subscriber provides end-user storage, where they can store, retrieve and browse web information. The information can be accessed internally. This service is used by users who have permission to manipulate the information. The information can also be published externally where external users coming from the Internet can access the information. The services which facilitate mail, news and web usage are:

5.2.1 File Archive

The file archive service provides the basic functions for all file or directory transfer from the local client to file archives and other web locations. The remote archive file system uses FTP to communicate between clients and servers. All the information transfer from the remote to the local system is encrypted through SSL.

The file archive service is used for:

- Transferring files and directories between server hosts, holding storage locations for a subscriber and the end user's client machine. FTP is used for this.
- Providing functions for the end user to be able to create, rename or delete documents or catalogues.
- Providing a tool for controlling the access permissions of the directories. This tool is known as Access Control List (ACL).

5.2.2 Internal Web

The internal web service gives users the ability to browse information stored by themselves or by other users, provided they are all members of the same subscriber. A web server here is configured to server only the internal web information.

This service depends on the tools from the file archive for uploading and access control configuration.

The operator defines the root URLs to the subscriber's internal web servers. Each subscriber may define a number of different internal websites, each with a separate web server. Proprietary SSL is used to tunnel the HTTP transfer of documents from server host to the user client. The Access Control List (ACL) states which access permissions are given for each directory and which user or user groups have those permissions.

5.2.3 External Web

Information held by a subscriber can be published externally so that external users, on the Internet, can browse that information. This service also uses the tools from the File Archive. The internal and external web servers are usually different.

External webs for different organizations can be reached through separate independent web servers which are configured to respond to requests at different IP addresses. The server hosts must be configured to respond to these IP addresses.

5.2.4 Surf Access

The surf access service provides users with the ability to access the Internet. This service requires high throughput with low security. So the SSL connection with the Internet is not implemented.

5.3 List of Abbreviations

ACL	Access Control List
BIS	Basic Internet Services
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
SSL	Security Service Layer

CHAPTER 6

TeleINternet Services for Tel-E-Commerce

6.1 Introduction

E-Commerce is growing rapidly, but needs to overcome a few stumbling blocks and improve customer service to reach its full potential. Tel-E-Commerce, the combination of real-time voice communication with user-friendly websites, will make this possible. TeleINternet applications combine Internet SW technology with fixed, mobile and Voice-over-IP Intelligent Network SW technology to provide the web server driven voice communication component of Tel-E-Commerce.

6.2 Tel-E-Commerce

Tel-E-Commerce is telephony-supported e-commerce, or web-supported telephony-based commerce. The combination of the Internet, websites and e-mail, and personal phone conversations through operator network is even stronger than pure e-commerce in explaining, supporting, marketing, selling, trading and other commerce-related business activities.

Tel-E-Commerce is the use of real-time voice communication together with web-based commerce: sales, marketing, purchasing, service, support, training, etc.

These are some major driving forces for Tel-E-Commerce:

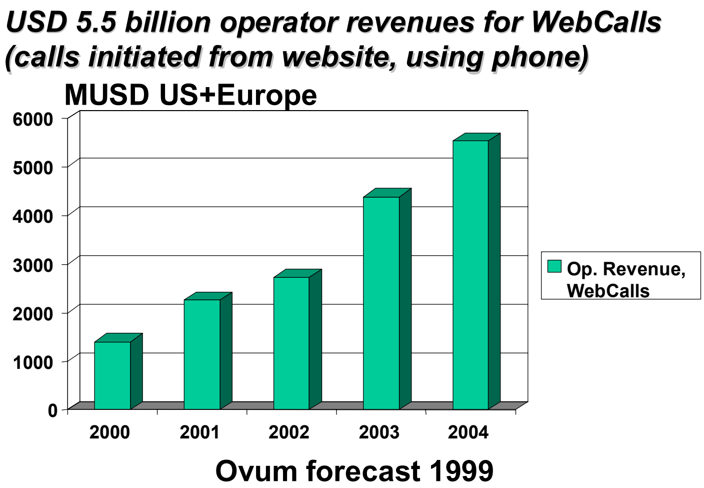
- Internet commerce brings comparison shopping to a new level

- In a business environment where the buyer can instantly compare prices, offering something extra becomes necessary in order to build brand loyalty

Inevitably, that extra will in most cases be Customer Service. To be ahead in the market and have the highest market share, it is very important to be one step ahead of the competition, to be able to spread costs on a higher volume than competitors, to be able to offer comparable prices to low-price competitors while offering better service – getting into a positive competitive circle position, where one competitive factor influences the other positively. Better customer service through Tel-E-Commerce, real-time voice communication, is an obvious competitive weapon. By making it easier for customers to get in contact and get service, you gain competitive edge. By putting the phone call capability right on the web page, the customer interface to service improves, giving a competitive edge.

In the beginning, the leading e-commerce companies will provide this capability though their network operator of choice, but within a few years, it will become, not a competitive edge but a must-have.

6.3 TeleINternet



TeleINternet services are communication services that combine the telecom network and the Internet using Intelligent Network SW technology. Using TeleINternet services, it is possible to provide telephony-assisted e-commerce, and web-assisted telephony services. Users of both wireless and wireline phones and Internet-connected PCs can be reached.

6.3.1 Click-to-Talk

Click-to-Talk (C-t-T) enables the user to click on a phone button or on a phone number displayed in a web browser and set up a phone call from his/her phone to a called party. The phone number may be retrieved from a network directory or from a PC personal directory; it may be typed/pasted/clicked in through a web interface; or it may be predetermined for web + phone marketing. The user simply clicks on the displayed phone number/call button and the call is made (the first time he/she has to enter his own number).

Click-to-Talk can be used for web-supported t(elephony)-commerce or telephony-supported e(lectronic)-commerce applications to generate in-bound sales lead calls from company web pages, for customer support, etc. Whenever a company wants to be called, and has a website, Click-to-Talk provides a better service.

For example, instead of spending time in a voice-response tree, the choices can be outlined on a web page, where complex information is more easily assimilated, and the call be made directly to the right department/number.

6.3.2 Internet Directory Inquiry

Internet Directory Inquiry (IDQ) provides the functionality of interfacing to inter/intranet directories accessed through a web interface. With IDQ, end users benefit from a convenient, cost-effective online service. Users may search for phone numbers, e-mail addresses, or other directory information/search criteria, all of which is configurable by the service provider.

For the operator, IDQ offers an additional, low cost-of-operation for providing chargeable directory information, compared to call-centre-based number directory information. IDQ can also be used to provide chargeable information of other kinds, e.g. used car directories, auction directories, company information, etc.

IDQ connects to standard LDAP directories, which enables the service provider to offer customer self-service to both residential and business users.

The IDQ charging functionality allows the service provider to charge end users by usage for every directory query or by subscription. Alternatively, revenue from IDQ may be provided by advertisements on the web pages.

6.3.3 MatchMaker

MatchMaker enables the end user to request to be called when certain conditions are met, e.g., in an Internet classified ads database. If the user is searching for a car, he/she can input the criteria (brand, model, price, mileage, colour, etc.) and be called on his phone (mobile and wireline) when such a car becomes available. The MatchMaker application announces the match and sets up a call to the seller.

MatchMaker can be used together with all types of business (and personal) “search-and match” applications, such as procurement, stock trading, web auctions, travel arrangements, property purchases. MatchMaker can provide the contact function whenever the user wants something that is not immediately available, or wants to know if something specific happens (his/her stock reaches a certain limit, the pre-owned red Porsche he/she has been searching for is advertised, etc.).

6.3.4 WebCall API

WebCall API is a TeleINternet application providing a web server application programming interface to create applications that initiate telephone calls. WCAPI provides a common interface for other TeleINternet applications, such as Click-to-Talk and MatchMaker. It gives the network operator the possibility to create its own web-server-initiated telephony services by web server programming only, or the possibility to offer this to partners.

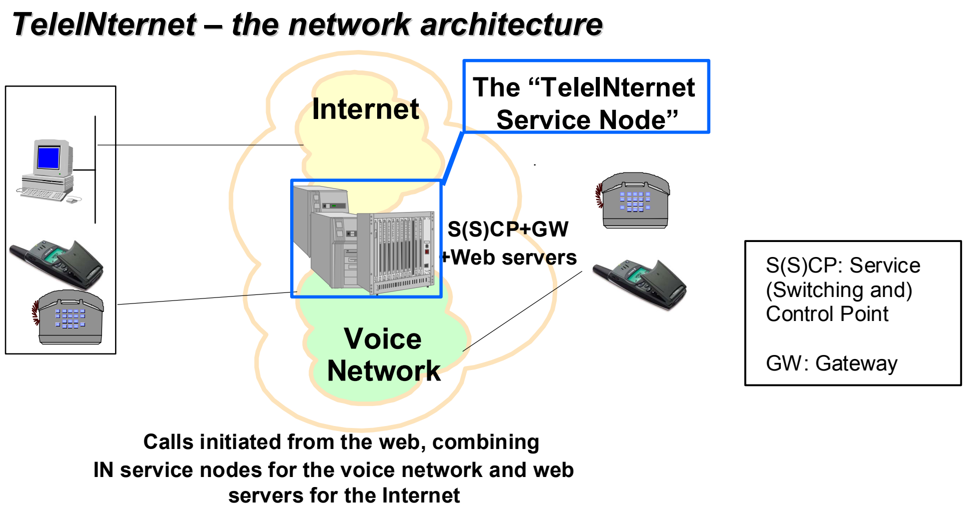
The WCAPI has two components: an SCP service script application component and a web server application component with the API. The service script application is used to set up the calls in the SCP/SSCP.

The web server API provides an interface to other applications to pass the call parameters (A-number, B-number, etc.) to the service script application.

In addition to call setup, the WCAPI service script can provide static and variable announcement facilities with digit collection and charging capability for interfacing applications.

6.4 TeleINternet Network Architecture

The TeleINternet network architecture is very simple. The TeleINternet Service Node consists of a web server farm, a Service Control Point and a Gateway between the two.



6.5 Tel-E-Commerce Applications of TeleINternet Services

6.5.1 Click-to-Talk and Internet Directory Inquiry

6.5.1.1 Application case 1

Dall Computers have a thriving call-centre and web-based e-commerce business selling customized Personal Computers. Using Click-to-Talk call buttons on their website, browsers can make immediate calls directly from the web page they are looking at.

Step 1: Mike Kadowski is a purchaser with CGE Electric, and responsible for acquiring PCs, LANs, routers, gateways, printers, mass storage, etc. To improve customer support, Dall Computers have created a CGE specific sub-website on the Dall website, where information about CGE's earlier purchases, deliveries, invoices, support, etc., can be found, and where CGE can place orders directly.

Mike is surfing the CGE specific sub-site on the Dall website. He is looking for information about an order, but he cannot find it.

Step 2: In order to take advantage of Dalls call-centre support capabilities, Dall has also placed a Click-to-Talk call button link on the GCE web page, in the form of a photo of the Dall Account Manager responsible for CGE, John Brown.

Mike clicks on the photo of John Brown, his phone rings, he picks up and is connected to John Brown directly. Mike and John can solve the issue over the phone while looking at the CGE web pages together.

6.5.1.2 Application case 2

TeleRomana, a European-based telephony operator and ISP company, offers the Click-to-Talk service to their customers, including many large airlines. KLN Airline is one of TeleRomana's customers who rely on C-t-T to promote their business using their website.

Step 1: Initial search John Smith, an executive, is looking for a non-stop flight from Amsterdam to New York. He surfs the Internet from his hotel room (using his laptop PC via the hotel room fixed phone line), uses the Yellow web pages search functionality provided by TeleRomana (which uses the Internet Directory inQuiry application – IDQ) and locates the KLN web page. He is interested in flight # 8641 departing at 2:00 PM from Amsterdam to JFK New York, but he wants to discuss the connections and price alternatives, as well as seating and meals.

Step 2: Connection John Smith clicks on the "Call Reservations" button on the KLN web page, and connects via his mobile phone to the KLN reservation desk (using the Click-to-Talk application). KLN pays for the wireline charges. The KLN reservation clerk can now answer John Smith's questions on the phone, while directing him to other KLN web pages, e.g. to show airplane type and free seating for a specific flight. John can give his credit card number over the phone to book the flight, and does not have to send his credit card number over the Internet.

6.5.1.3 Application case 3

Our executive John Smith is visiting a client company, but he needs to make a few phone calls relating to another client.

Step 1: Log-on He enters the TeleRomana Click-to-Talk web page. Since he is already a registered user, he logs on (using his user ID and password).

Step 2: New phone (number) to be used He enters the number of the phone in the office he has borrowed, which replaces his mobile phone number used earlier.

Step 3: Calling He proceeds to set up calls conveniently, calls that are subsequently billed to his registered account, in this case registered specifically for the client.

6.5.1.4 Business values and benefits

The network operator provides his customer, the airline, with an attractive service. By servicing the airline's potential customers better when searching for a flight, more requests and bookings are generated. The end user experiences an easier, more convenient information-gathering, customer service and purchase process.

6.5.2 Internet Directory Inquiry

6.5.2.1 Application case 1 – White Pages

Tony is a senior marketing manager with a global company based in New York, USA. Tony is travelling to Tokyo to meet his company's new Japanese customer. Tony had a very good college friend from Japan – Eiji Kunaki – and would like to get in touch with Eiji. He does not know if Eiji is still in the US or if he moved back to Japan.

Tony's company subscribes to directory services from Global Directories. Global Directories has agreements with all major directory service providers worldwide, which makes it possible to reach and search many countries/directories from one starting point. Tony uses the Internet Directory Inquiry service from Global Directories to search for Eiji in both Japan and the US, without any language problem. He finds Eiji's phone number, then uses Click-to-Talk to call by clicking on the number.

6.5.2.2 Application case 2 – Yellow Pages

John is looking for a used car in Dallas, Texas. He would like to find all the Honda or Toyota used car dealers in the Dallas/Fort Worth area in Texas.

As usual, John searches the directory information using the Internet Directory Inquiry (IDQ) service provided by Bell Southwest. He simply specifies the preferred used car dealers criteria (i.e. Honda or Toyota) and the city, which is Dallas/Fort Worth, and then clicks on the search button.

The search results provide him with a list of Honda or Toyota used car dealers in the Dallas/Fort Worth area along with dealers' phone numbers, e-mails, and addresses. Some dealers' phone numbers are highlighted, meaning they are "clickable" to make the call. John clicks on one of those, because he likes the convenience.

With the addition of the Internet Directory Inquiry server connecting to the Bell Southwest's existing LDAP database, Bell Southwest is able to provide the same directory information for both Internet and telephone users.

6.5.2.3 Business values and benefits

The Yellow Page IDQ application provides service providers with additional revenue from the following sources:

- Retailers who would like to put their addresses and phone numbers in the directory databases
- Retailers who want their phone numbers to be clickable to increase the probability of winning new business
- Advertisers, who put web banner ads, etc., on the search result pages shown to users

6.5.3 MatchMaker

6.5.3.1 Application case 1

A South American operator, Telebrás, is using MatchMaker to generate high-revenue phone calls for its valued ISP customer CarPoint, a nationwide used car dealership.

Step 1: Searching Jose Cangas is "surfing" the WWW in São Paulo, Brazil, looking for used cars. He opens Telebrás's CarPoint web page and enters car search criteria (make, model, colour, etc.) into a web form.

Step 2: Notify request After having entered the car search criteria, he selects the MatchMaker icon. MatchMaker presents him with a web form, where he enters his personal phone contact profile information, specifying the phone number(s) and the time periods per weekday he prefers to be called (e.g., wireless No. 972 123-4567 Monday-Friday/ Home Phone No. Saturday and Sunday 972 234-7654). He then submits the information.

Step 3: MatchMaker notification call As soon as the car search criteria gets a match in the CarPoint database (e.g., within 2-3 business days), CarPoint sends an e-mail to MatchMaker, with the information.

Step 4: MatchMaker notification call In response to CarPoint's e-mail notification, MatchMaker initiates a call to Mr Cangas, according to his personal contact profile.

Step 5: Notification announcement and call forwarding On receiving the call, he hears a voice announcement message: "Your CarPoint search has a hit, please press 1 if you want to be connected to the seller." He then responds (via DTMF) to connect to the matched car dealership. Following the acceptance, a call is set up to the car dealership.

6.5.3.2 Application case 2

For Application case 2, **steps 1** and **2** are the same as those for Application case 1.

Step 3: No database hit If the car search criteria does not get a database match within a specified time (e.g., elapsed time more than 20 business days), CarPoint sends an e-mail to MatchMaker to call Mr Cangas and play an announcement.

Step 4: No hit notification and marketing message In response to CarPoint's e-mail, MatchMaker initiates a call to Mr Cangas. After he receives the call, the requested announcement is played:

"We are sorry, but no car corresponding to your request has been found. However, there are similar new cars available at the Colombo Car dealership. Would you like to be connected to Colombo Cars? Press 1 to be connected!"

6.6 Conclusion

The convergence of telecom and Internet technologies now allows convenient and efficient services that save time and money and provides corporate customers and end users with better service. Click-to-Talk, Internet Directory Inquiry, MatchMaker and WebCallAPI's WebCall functionality enhance the service provider's ability to provide more valuable Intelligent Network and Internet-based communication services.

6.7 List of Abbreviations

API	Application Programming Interface
C-t-T	Click-to-Talk
DTMF	Dual Tone Multi-Frequency
IDQ	Internet Directory Inquiry
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
SW	Software

CHAPTER 7

Public IP Network

7.1 From the Internet to the Public IP Network

The growth of the Internet in the past five years, fuelled by the popularity of the World Wide Web and increased use of intra- and inter-company e-mail, has been unprecedented, and has shaken the foundations of the data communications and telecommunication industries. Both industries are aggressively moving towards a common future, based on IP protocol and a packet-switched infrastructure model – a vision of "IP Convergence". Today's Internet is an ad-hoc overlay built above existing telecommunications and wide-area data communications networks. Entrepreneurial Internet Service Providers (ISPs) have for the most part built it around existing carrier networks, with minimal participation from carriers. The Internet today scores points for its ubiquity – it is accessible from virtually anywhere on the planet via modem, and over existing high-speed telecommunication services in all major markets. But it falls far short of meeting the reliability and performance of traditional wide-area data communications services. The vision of "IP Convergence", along with many bold predictions on IP telephony, e-commerce, and the transformation of the workplace, could not be fulfilled by today's Internet.

New Public IP Networks are already being built to supplant and replace not just today's Internet, but also major elements of the telecommunication network. The Public IP Network is not being built simply as an overlay by independent ISPs; it's an integrated part of the carrier network, built and delivered by innovative, entrepreneurial carrier-service provider hybrids. The Public IP Network will maintain the ubiquity of today's Internet, augmented with the reliability of a telecommunication service and with performance enhancements that enable the most aggressive applications to operate seamlessly. Today's Internet has grown in a short time to a multi-billion dollar market, has changed the shape of the communications industry and has become a social phenomenon. But today's Internet is only the beginning.

7.2 Converged IP Services

To some, the term "IP Convergence" describes the transition from today's telecommunications infrastructure technologies (ATM/Frame Relay Switching, SONET/SDH TDM) to new, IP-centric solutions. To others, it describes a transformation of today's multi-protocol service model to a bundled service model based on IP. The former concept – "IP Infrastructure Convergence" – is technologically fascinating and will certainly have a major impact on carrier backbones over a 5-10 year period. But the latter concept of "IP Service Convergence" is happening far more quickly and will have a much more visible near-term impact. The concept of IP Service Convergence is a simple one. Today, the typical business contracts with a variety of different providers of diverse communications services. A medium-sized corporation could have different providers for basic telephony (POTS, FAX, etc.), videoconferencing service, private wide-area networking, remote LAN access and Internet access. Each of these services potentially requires its own WAN connection and its own CPE; each service also likely demands specialized expertise from the subscriber. What IP Service Convergence promises is a simplified model, where all the services above (along with new ones not yet imagined!) are delivered via one connection (optionally redundant) to an IP network. Via one wire from one service provider, subscribers will be able to access a full menu of communications services. Today's Internet can be used to prototype new services, but is not equipped to deliver converged IP services on a large scale. The routers used to forward IP traffic within the Internet today, and the IP protocol suite running as a distributed operating system within these routers, is weak in two key areas: performance and topology. The New Public IP Network will rely on innovations in both areas to enable a bundled service model.

7.2.1 Performance

Performance issues in the Internet today are easy to observe – anyone who has used a browser to surf the web has first-hand experience with them. Statistical multiplexing of bandwidth is an inherent characteristic of packet-switched networks, and contention for use of the network creates variations in latency ("jitter") and non-zero data loss. IP routers today make no effort to improve upon these issues for any traffic types; all service is unreserved, best effort and connectionless. The converged service model will require more intelligent handling of different traffic classes within the public IP network, ensuring that certain applications (e.g. voice) get prioritized handling over other traffic types.

7.2.2 Topology

Topology is a more subtle issue than performance in today's Internet. Today's routers maintain a single topology database (the "routing table") for the global Internet; from any specific router to any point in the Internet, there is one unique path, dynamically maintained through exchange of topology information between routers. The protocols used to exchange this information today make no accommodation of "private" traffic (e.g. a corporation's own WAN backbone), are unable to re-route traffic around congestion points and do not easily allow topologies to be constrained by commercial factors. The Public IP Network will require enhancements to topology management allowing IP-based Virtual Private Networks (VPNs), topologies based on Class of Service (CoS) and easier implementation of commercial constraints (e.g., preferring one backbone alternative over another due to lower transport costs). With enhanced Quality of Service/Class of Service (QoS/CoS) capability and more flexible topologies supporting IP-VPNs, the Public IP Network will be able to deliver the full range of telecommunications and data communications services available today, with "public" Internet access as a bundled feature. New architectures, products and standards are being developed that will be used to build the Public IP Network and make IP Service Convergence a near-term reality.

7.3 Building the Public IP Network

Like today's Internet (and today's telecommunication networks), the Public IP Network will not be one single network, but a mesh of parallel networks interconnected at major "peering points". Each of these parallel networks will be an IP network on its own, and may in turn be broken into different elements owned and operated by different carriers. The structure of each parallel IP network can be broken into two major elements.

7.3.1 Backbone Networks

Large carriers and service providers will operate backbone networks nationally and internationally. These will always run over large fibre plants, typically with a DWDM[1] layer enabling terabits per second of aggregate bandwidth in the network. These networks are always built as a mesh of interconnected IP routing nodes richly interconnected by point-to-point links, although there are numerous approaches to how the IP network is layered over the fibre optic backbone. These approaches can be loosely grouped as follows:

*IP over ATM Multiservice Backbone*s: These networks use ATM Switching to multiplex IP traffic with other traffic types across the backbone. Routers interconnect via point-to-point virtual circuits over the ATM backbones; in some cases, ATM switches are active routing nodes as well, using 00MPLS technologies (more on this below). The advantage of this architecture is its ability to support existing backbone traffic (non-IP data, non-data) alongside IP, enabling easy migration to the New Internet. However, it carries a price both in the loss of throughput to ATM overhead and in the cost of ATM network management, and not all network architects believe this price is offset by ATM's benefits.

*IP over SONET/SDH Backbone*s: These networks eliminate the ATM layer, implementing point-to-point links between IP routers directly over SONET/SDH rings (which in turn run over DWDM). If non-IP traffic is carried at all, it is carried over separate point-to-point connections in the same SONET/SDH structure. Like the IP over ATM approach, this can be implemented today, based on proven standards.

*IP0 over DWDM Backbone*s: These networks exist today only in theory; the idea is to replace the SONET/SDH layer with a new, lightweight physical layer mapping IP traffic directly to DWDM fibres. The argument for this approach is logical; much of the structure of SONET/SDH is optimized for circuit, not packet switching, and a simpler approach optimized for IP packets will result in better price-performance. IP/DWDM nodes could use IP over SDH/SONET as an interoperable interface to IP over DWDM networks and optimize performance for IP traffic. The vision of IP Infrastructure Convergence calls for rapid migration to IP over DWDM backbones. In reality, all three types will exist; migration to a common approach in the backbone may take many years.

7.3.2 Aggregation Networks

Both large and small carriers and ISPs will operate aggregation networks within service areas (as large as a country or even a few states, or as small as an industrial park). Logically, an IP Aggregation Network will look like a funnel: thousands or even tens of thousands of subscriber connections will be transported via carrier switching and multiplexing networks into an IP Aggregation Point, where powerful Aggregation Routers map the subscriber traffic streams to backbone connections. Functionality in these new IP Aggregation Networks can be viewed in three domains:

---

[1] See more details about DWDM in Chapter 6 of Fascicle 1 (*New technologies supporting new networks*).

Subscriber Access: The connection between the subscriber and the IP aggregation point will logically be a point-to-point IP connection, and carrier networks will use diverse Layer 1/Layer 2 multiplexing and switching technologies to deliver thousands of these connections within a service area. Alternatives will range from high-speed leased lines and ATM/Frame Relay PVCs to IP/PPP/ATM connections over xDSL networks to wireless and cable modem networks. IP Aggregation Routers will need to offer tens of thousands of virtual IP interfaces on a variety of physical port types to insure easy integration with these diverse networks.

Subscriber Traffic Processing: At the IP aggregation point, many thousands of subscriber streams are being terminated and aggregated. The IP Aggregation Router must be able to quickly classify received packets according to pre-defined policies, per subscriber and per application. This must be more than simple classification into a finite pool of priorities – each traffic class may require mapping to a different VPN, and may require unique shaping and prioritization.

Backbone Integration: A primary function of IP Aggregation Routers is to route the aggregated traffic onto IP backbone networks. This demands comprehensive support for routing protocols (OSPF, IS-IS and BGP-4) as well as the ability to map traffic to supported backbone CoS levels and traffic-engineered topologies. Two new standards for IP networks nearing completion by the Internet Engineering Task Force (IETF) will play a key role here: DiffServ and MPLS. The new Differentiated Services, or DiffServ, standard is used to allow IP traffic to be marked for preferred handling by the network. DiffServ redefines a byte in the existing IP header (the Type of Service, or ToS byte) to include a 6-bit "DS" field indicating the service requirements for the packet. DS-capable nodes will examine this field on each packet and condition forwarding operations according to its value. Of the 64 possible DS values, the IETF intends to define up to 32 as "global" service classes and to leave the other 32 open to network specific definition. Nodes can also rewrite DS values in transit. The DS value will allow certain packets to be prioritized ahead of others at each network node, reducing jitter and increasing "goodput" (throughput of payload packets) for specific traffic streams (albeit at the expense of less important traffic). The Multi-Protocol Label Switching (MPLS) initiative is much broader than DiffServ, and has evolved into a family of standards within the IETF. The basic concept of MPLS is to prepend the IP packet with an extra label, allowing intermediate nodes in an IP network to perform simple label processing to determine the packet's egress path instead of the more complex lookup normally used to find the destination. Since the forwarding within an MPLS "cloud" is based only on the label, it supports IP-based Virtual Private Networks (VPNs) readily. And because the process that manages the labels in an MPLS network is decoupled from the basic topology processes of the network, MPLS can be used to augment the basic topology with new paths – a capability called "traffic engineering". By engineering extra "Label Switched Paths" (LSPs) for certain traffic classes, and by using MPLS LSPs to optimize use of a complex mesh, network operators can improve goodput and jitter across the board. MPLS and DiffServ are both enhancements to basic IP networks, but they don't make any presumptions about the underlying protocol sandwich. Standards have been defined to allow MPLS to run directly over ATM or Frame Relay backbones, as well as over any network carrying IP traffic in PPP frames. And DiffServ operates strictly within the IP packet; it can be used in any IP network. Infrastructure convergence isn't necessary to take advantage of these new standards – all that's required is that IP routing nodes within the infrastructure be upgraded to support them.

Major telecommunication equipment providers are rolling out a new generation of solutions designed for these Public IP Networks.

7.4 ITU References and Publications

a) ITU-T SG 13 is dealing with Internet issues. The following is the framework for the Y.1000 Recommendation Series on IP-related issues:

Y.1000 Series. General
Y.1000 Full Featured IP Integrated Networks
Y.1010 Vocabulary
Y.1100 Series. Services and Applications (including Multimedia)
Y.1200 Series. Architecture, Access, Network Capabilities and Resource Management
Y.1200 General Network Considerations
Y.1210 Reference Models
Y.1220 Functional Architecture
Y.1230 Access Architectures
Y.1231 Access Capabilities
Y.1232 Access Interfaces
Y.1240 Network Capabilities
Y.1250 Resource Management
Y.1260 Traffic Engineering
Y.1270 IP Network Security
Y.1300 Series. Transport
Y.1300 General Transport Considerations
Y.1310 IP over ATM
Y.1320 IP over SDH
Y.1330 IP over Optical (WDM)
Y.1340 IP over Satellite
Y.1350 IP over Cable
Y.1360 IP over Wireless
Y.1400 Series. Interworking
Y.1400 General Interworking Considerations
Y.1410 Narrowband ISDN
Y.1420 Broadband ISDN
Y.1430 Wireless
Y.1440 Satellite
Y.1450 Cables
Y.1500 Series. Quality of Service and Network Performance
Y.1500 General QoS and NP Considerations
Y.1510 Customer-Perceived QoS Including Customer Equipment Effects
Y.1520 Reliability, Availability, Survivability, and Emergency Services
Y.1530 Signalling, Call, and Connection Processing Performance
Y.1540 User Information Transfer Performance
Y.1550 Timing and Synchronization Performance
Y.1560 QoS and NP Across Heterogeneous Networks
Y.1570 Performance of Network Components
Y.1580 Performance Monitoring and Measurement
Y.1600 Series. Signalling
Y.1700 Series. OAM
Y.1800 Series. Charging

b) ITU-D issued two reports (1997 and 1999) in the Challenges to the Network series "*Internet for Development*".

The first report from 1997 looks at the challenges presented by the Internet to public telecommunication operators.

The subject of the second report is on the role of the Internet in economic and social development, with a focus on developing nations.

7.5 List of Abbreviations

ATM	Asynchronous Transfer Mode
CoS	Class of Service
Diff Serv	Differentiated Service
DSL	Digital Subscriber Line
DWDM	Dense Wavelength Division Multiplexing
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LSP	Label Switched Path
MPLS	Multi-Protocol Label Switching
OSPF	Open Shortest Path First
POTS	Plain Old Telephone Network
PPP	Point-to-Point Protocol
PVC	Permanent Virtual Circuit
QoS	Quality of Service
SDH	Synchronous Digital Hierarchy
SONET	Synchronous Optical Network
ToS	Type of Service
VPN	Virtual Private Network
WAN	Wide Area Network

Printed in Switzerland
Geneva, 2002

Photo credits: ITU Photo Library