Support for Development of the Global Information Infrastructure in Africa

Guide on Managing and Developing Network Connections and Interconnections to the National Internet Nodes



Prepared by Désiré Karyabwite,
Consultant in Internet Nodes Management
Geneva, June 2000

TELECOMMUNICATION DEVELOPMENT BUREAU
International Telecommunication Union
ITU

© ITU 2000

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without written permission from ITU.

Disclaimer: opinions expressed in this publication are those of the author and do not engage ITU.

TABLE OF CONTENTS

Page

1 Introduction 1

2 Network architectures and data transmission 1

2.1 General remarks 1

2.2 The OSI reference model and the TCP/IP protocol 2

2.2.1 Standardization 2

2.2.2 TCP/IP de facto standard protocol 3

2.2.2.1 Introduction 3

2.2.2.2 How the IP protocol works 3

2.2.2.3 How IP addresses are formed 4

2.2.2.4 DNS on the Internet 4

2.2.2.5 The ARP and RARP protocols 6

2.2.2.6 The ICMP protocol 7

2.2.2.7 New IPv6 addressing system 7

2.2.2.8 Security and authentication 8

2.2.2.9 The IPv6 protocol and multimedia on the Internet 8

2.2.2.10 The TCP protocol 8

2.2.3 The other main protocols in the TCP/IP suite 10

2.2.3.1 Gateway to Gateway Protocol 10

2.2.3.2 The BOOTP protocol 10

2.2.3.3 The SMTP protocol 10

2.2.3.4 The SNMP protocol 10

2.2.3.5 The XDR and RPC protocols 10

2.3 Interconnection of transmission networks on Internet 10

2.3.1 General remarks 10

2.3.1.1 Circuit-switched networks 11

2.3.1.2 Message-switched networks 11

2.3.1.3 Packet-switched networks 11

2.3.2 Physical transmission media on Internet 12

2.3.2.1 General remarks 12

2.3.2.2 Twisted pair 12

2.3.2.3 Coaxial cable 12

2.3.2.4 Optical fibre 12

2.3.3 Access technologies 13

2.3.3.1 Carrier Sense Multiple Access (CSMA/CD) 13

2.3.3.2 Token bus 13

2.3.3.3 Token Ring 13

2.3.4 Ethernet architecture 14

2.3.4.1 How it works 14

2.3.4.2 Ethernet base components 14

2.3.4.3 Different Ethernet configurations 15

2.3.5 Token Ring architecture 16

2.3.5.1 General remarks 16

2.3.5.2 The components of the Token Ring architecture 16

Page

2.3.6 Other architectures ... 17
2.3.6.1 General remarks ... 17
2.3.6.2 Ethernet 100Base-T ... 17
2.3.6.3 Ethernet 100Base-VG or "AnyLan" ... 17
2.3.6.4 FDDI (Fibre Distributed Data Interface) ... 17
2.3.6.5 DQDB (Distributed Queue Dual Bus) ... 17
2.3.7 Network interconnection equipment ... 17
2.3.7.1 General remarks ... 17
2.3.7.2 The hardware ... 17

3 Designing and implementing a national Internet node ... 18
3.1 General remarks ... 18
3.2 Planning a national Internet node ... 18
3.2.1 General remarks ... 18
3.2.2 Network services and the layers of the OSI model ... 18
3.2.3 Encapsulation on Ethernet and TCP/IP ... 19
3.2.4 ARP protocol ... 20
3.2.5 The Ethernet segment ... 20
3.2.6 The router ... 21
3.2.7 The switch ... 22
3.2.8 The routing switch or IP switching ... 22
3.2.9 International connections and overall architecture ... 24
3.3 Basic equipment for a national Internet node ... 26
3.3.1 General remarks ... 26
3.3.2.1 Satellite link ... 26
3.3.2.2 International router ... 28
3.3.2.3 DNS ... 28
3.3.2.4 Modems ... 28
3.3.2.5 Automatic electricity supply ... 29
3.3.3 Local network ... 29
3.3.4 Provision of Internet services: Netscape SuiteSpot ... 30
3.3.4.1 General remarks ... 30
3.3.4.2 Netscape Directory Server ... 31
3.3.4.3 Netscape Certificate Server ... 31
3.3.4.4 Netscape Enterprise Server ... 33
3.3.4.5 Netscape Messaging Server ... 33
3.3.4.6 Netscape Collabra Server ... 33
3.3.4.7 Netscape Proxy Server ... 33

4 Internet services engineering and maintenance ... 35
4.1 General remarks ... 35
4.2 Network management and quality of service on the Internet ... 35
4.2.1 General remarks ... 35
4.2.2 Main management tools ... 35
4.2.3 Other system-integrated management tools ... 36
4.2.4 Main management indicators ... 36
4.2.5 Simple Network Management Protocol ... 37

Page

4.3 Measuring and analysing Internet traffic 38
4.3.1 General remarks 38
4.3.2 How it works 38
4.4 System security 39
4.4.1 General remarks 39
4.4.2 Network audits and security 39
4.4.3 Anti-virus measures 40
4.4.4 Backups 40
4.4.5 Inverters 40

5 Strategies and development of the Internet network 40
5.1 General remarks 40
5.2 Unified networks and IP telephony 41
5.2.1 General remarks 41
5.2.2 How it works 41
5.2.3 IP switching and unified networks 41
5.3 TM and backbone development 41
5.3.1 General remarks 41
5.3.2 Asynchronous Transfer Mode (ATM) backbone 42
5.3.3 Means of connection to the ATM backbone 42
5.3.4 IP communications over ATM 43
5.3.5 ATM end-to-end or RSVP? 44
5.4 Development of optical fibre networks 45
5.4.1 General remarks 45
5.4.2 Principle of converting electrical signals into optical signals 45
5.4.3 Types of optical fibre 45
5.4.4 Links and transmission quality using optical fibre 45
5.5 Connections using laser links for Internet sites 46
5.5.1 General remarks 46
5.5.2 Characteristics of laser links 46
5.6 Leading-edge technologies and Internet access 46
5.6.1 General remarks 46
5.6.2 ADSL 46
5.6.2.1 General remarks 46
5.6.2.2 How ADSL works 47
5.6.2.3 The ADSL modem 47
5.6.2.4 The access adapter 48
5.6.2.5 The POTS connectors 48
5.6.3 Internet by satellite 49
5.6.3.1 General remarks 49
5.6.3.2 Internet via VSAT satellite networks 49
5.6.4 Wireless local loop 49
5.6.4.1 General remarks 49
5.6.4.2 How it works 49
5.6.5 Microwave Multipoint Distribution System (MMDS) 50
5.6.5.1 General remarks 50
5.6.5.2 MMDS as an alternative to television cable 50
5.6.5.3 Internet access using MMDS 50

Page

6 Regulatory and legal aspects 51
6.1 General remarks 51
6.2 Protecting the new technologies 51
6.2.1 General remarks 51
6.2.2 Cryptology 52
6.2.3 Confidentiality 53
6.2.4 Responsibilities of cryptology organizations 53
6.2.5 Infringements and penalties 53
6.2.6 Definitions and standards 54
6.3 Voice over IP or Internet telephony 55
6.3.1 General remarks 55
6.3.2 Definition 55
6.3.3 Development of voice communications on the Internet 55
6.3.4 Commercial exploitation of Internet telephony 55

7 Strengthening local capacity 56
7.1 General remarks 56
7.2 UNIX operating system 56
7.3 TCP/IP in an NT environment 56
7.4 Netscape SuiteSpot 57
7.5 Internet Information Server 57
7.6 Measuring and managing quality 57

8 Conclusion 58

9 Bibliography 59

Annex I – Estimated budget 60

Annex II – Specifications 61

II.1 General remarks 61

II.2 Specifications for the national Internet node 61

II.3 Equipment 62
II.3.1 Satellite link 62
II.3.2 Routers 62
II.3.3 DNS 63
II.3.4 Other interconnection equipment 63
II.3.5 Computers 63

4 National provision of Internet services 63

5 Technical management, security and traffic analysis 64

1 Introduction

There has been considerable growth in the use of computers interconnected on local networks. In 1998, it is estimated, over 50% of machines were interconnected, a figure predicted to rise to close to 80% by the year 2000. This compares with less than 10% in 1991, and 40% in 1993. Internet, which is a series of local networks, is growing so fast that developing countries are struggling to keep up and reap the full benefits of this technological advance. There is therefore a danger of an ever-widening gap between industrialized and developing countries in terms of access to information.

One of the official tasks of the International Telecommunication Union (ITU) is to ensure that telecommunication development benefits the whole of humankind. For this reason technical cooperation between the Telecommunication Development Bureau of ITU (ITU/BDT) and the Member States revolves primarily around leading-edge technologies which facilitate the development of telecommunications at reasonable cost.

At a time when the telecommunication sector is undergoing a genuine transformation as a result of the convergence of telecommunication, computer and audiovisual technologies, this guide is designed to provide some signposting in the innovative sphere of Internet-based communications networks. The aim is to provide technical assistance to telecommunication operators in developing the Global Information Infrastructure (GII). Such is the complexity of this field that it would be impossible to be exhaustive on the subject, and this guide makes no such claim. However, it does attempt to establish a basis on which to work, and provide some pointers for the engineers responsible for planning and developing communications networks in Africa.

The second chapter deals with network architecture and data transmission on TCP/IP, the *de facto* standard on the Internet network. The third concerns the planning of a national Internet node, and Internet connections and interconnections. Chapter 4 looks at the management, metrology and quality of Internet services, while Chapter 5 sets out a basis for planning Internet network development with leading-edge technologies which may be used to connect up ISPs (Internet Service Providers) or other consumers. The sixth chapter deals with the regulatory and legal aspects of use of these leading-edge technologies on the Internet. Chapter 7 proposes a training plan designed to strengthen local capacity and thus ensure genuine development of the Internet and local decision-making. The eighth and final chapter contains concluding remarks. For information purposes, annexes are attached setting out an estimated budget for a project to set up a national Internet node, as well as specifications which may be used by African telecom operators wishing to set up as national Internet operators.

2 Network architectures and data transmission

2.1 General remarks

A few years ago, interconnection of local networks was confined to distances of some tens of metres. With the development of Internet, local networks, via gateways, allow users to communicate with extended networks including the switched telephone network and many others. The information transmitted is diverse in nature, encompassing not only computer data but also sound and images. To enable the different networks to be interconnected, use of the IP (Internet Protocol) is essential on those nodes which are to route the data between the networks. The Internet is thus a packet-switched network.

The term host refers to terminal equipment, linked by the network, which either generates or receives the data transmitted, and processes them. Each host is identified by its address on the network.

The bit rate or speed is the number of binary elements which can be transferred across the network in a given time. It is expressed in bits per second, and in multiples of this basic unit: [kbit/s] for kilobits per second, [Mbit/s] for megabits per second and [Gbit/s] for gigabits per second.

Local networks are often referred to as subnetworks, to avoid confusion with layer 3 of the OSI model. Broadly speaking, these are classified according to their scope, as follows:

- LANs (Local Area Networks) are confined to one building and deliver bit rates as high as 100 Mbit/s. The strategic alternative technology for LANs and Intranets is Gigabit Ethernet (1000 Mbit/s).
- MANs (Metropolitan Area Networks) cover an area the size of a town or city, with bit rates ranging from 2 Mbit/s to 155 Mbit/s.
- WANs (Wide Area Networks) are national or international in scope. The modern digital systems which form the Internet backbone have bit rates of 34 Mbit/s, 140 Mbit/s and even 565 Mbit/s, or multiples of these bit rates.

2.2 The OSI reference model and the TCP/IP protocol

2.2.1 Standardization

The Internet is a world of heterogeneous systems. To allow different constructors' systems to communicate, the ISO (International Organization for Standardization), which is an umbrella organization for the standardization bodies, has laid down a standard known as Open Systems Interconnection (OSI). This standard is broken down into seven operational sub-categories known as "layers".

1 The physical layer. This is responsible for transmission of the bit stream in terms of physical interconnection.

2 The data link layer is in charge of error control, applying the principle of acknowledgement.

3 The network layer is responsible for routing and flow control in order to prevent data units being lost through congestion on the transmission path and, where necessary, for ensuring compatibility of the networks to be interconnected.

4 The transport layer is responsible for end-to-end transport of information across the network (from sender to destination).

5 The session layer is responsible for setting up and monitoring the dialogue between remote tasks. It activates and synchronizes certain events, e.g. duplication of a database on a network.

6 The presentation layer is responsible for presenting the data exchanged by applications on interconnected networks. It deals with day-to-day problems of heterogeneity and presentation of data which may arise:

   - with certain processes which code whole numbers by storing the most significant octet before the least significant (big-endian), while others do the opposite (little-endian);
   - with certain machines which represent characters in the form of ASCII codes, while others use the EBCDIC code;
   - with platforms which do not conform to the standard laid down by the IEEE (Institute of Electrical and Electronic Engineers) for representing floating-point numbers.

7 The application layer. The function of this final layer is to provide services to network users. This is the level where we find file transfer programs, terminal emulation programs, e-mail exchange programs, etc. The programs used must ensure security and confidentiality of data exchanges, guarantee the integrity of the information and back it up in case of incidents.

The different layers of the destination host carry out tasks which mirror those carried out by the layers of the sender. With each layer that is reached, from layer 7 (the application layer) to level 1 (the physical layer), further information is added (encapsulation), and data units are cut up (fragmentation). On the receiving side, the same process is repeated in reverse, moving from layer 1 (the physical layer) to layer 7 (the application layer).

2.2.2 TCP/IP de facto standard protocol

2.2.2.1 Introduction

TCP/IP is a set of some twenty protocols (and as many commands), including TCP (Transmission Protocol) and IP (Internet Protocol). On local networks, fewer than ten of them are used. TCP/IP operates as an interconnection protocol for differing networks. As such, it is completely independent of the lower layers (Ethernet, Token Ring, X25, etc.). It covers layers 3 to 7 of the OSI model, although there is no precise correlation between the layers of TCP/IP and the OSI layers, as TCP/IP predates the OSI model by some time.

TCP/IP is used on small local networks as well as for international connections. It is the protocol used by the INTERNET, which is a worldwide interconnection of local TCP/IP networks.

2.2.2.2 How the IP protocol works

The IP (Internet Protocol) layer is designed to transport a data packet between a source station and a destination station, which may be located on the same network segment or on different networks linked by one or more gateways.

Each packet is an entity completely independent of all the others. IP simply forwards datagrams, i.e. units of data in non-connected mode. It is not concerned with data flow control.

The data making up the packet are provided by the transport layer. There are two possible scenarios:

- if the destination station is on the same network as the transmitting station, the packet is sent direct to its destination;
- if the destination station is on another network, IP sends the packet to a gateway, which forwards it to the destination station, or to a subnetwork, until it reaches its destination. This concept of transporting a packet through gateways within an architecture of interconnected networks is the basis for forming Internet addresses. IP performs three important services at the upper layers, namely:
  - transporting the data unit;
  - managing service requests;
  - transmission error reports.

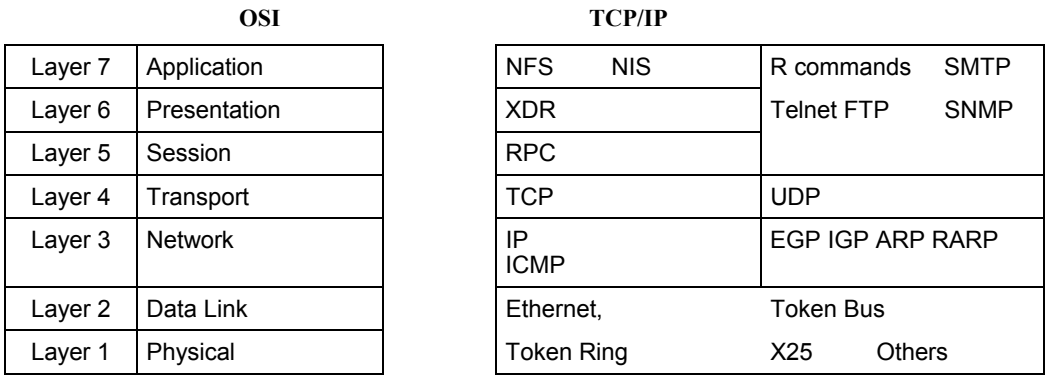

Fig. 2.1 Parallels between the OSI model and TCP/IP *(Source: Réseaux TCP/IP – Editions WAN & LASER)*

2.2.2.3 How IP addresses are formed

IP addresses (also known as *Internet addresses*) have a fixed length of 32 bits, or 4 octets (1 octet = 8 bits). They are logical addresses, as distinct from physical addresses (of Ethernet or Token Ring adapters, for instance). They are made up of two parts: the network address, and the address of the host on the network. As an IP address must be absolutely unique, the NIC (Network Information Centre) has sole authority to allocate network addresses, the host address being left to the discretion of the administrator.

IP addresses are usually written octet by octet, each separated by a dot, e.g. 156.106.194.24. There are three main classes of Internet address:

- *Class A:* addresses are characterized by an 8-bit network address where the first bit is 0. Class A addresses are of the type NNN.HHH.HHH.HHH, where NNN represents an octet of the network address, and HHH an octet of the host address. The NNN part ranges from 1 to 127. In a Class A subnetwork, only the first of the four numbers is fixed, in other words all the machines on the subnetwork will have an address starting with the same number (between 1 and 254). A class A subnetwork can therefore accommodate 254^3 machines.

- *Class B:* addresses have a 16-bit network address, the first two bits being 10. Class B addresses follow the pattern NNN.NNN.HHH.HHH. The first octet is between 128 and 191. The first two numbers are fixed on a Class B subnetwork, and it can therefore accommodate 254^2 machines.

- *Class C:* addresses have a 24-bit network address, the three first bits being 110. They are of the type NNN.NNN.NNN.HHH. The first octet is between 192 and 223. The first three numbers are fixed on a Class C subnetwork; it can therefore contain 254 machines.

In the case of all three classes, it is impossible to have addresses where all the bits are 0 or 1. In addition there are:

- *Class D:* addresses, used by multicast mechanisms, i.e. for sending a message to a group of machines using a common protocol (as opposed to broadcast, where messages are sent to a group of machines using the same network).

- *Class E*: addresses, reserved for future expansion of IP.

The addresses 0.0.0.0 and 255.255.255.255 have a particular significance, and cannot therefore be allocated to a host. The address 0.0.0.0 is transmitted by a computer which does not know its own IP address. Some obsolete versions use this destination address for broadcasting. An address in which all the bits in the host part are 1 is used for broadcasting on the designated network.

NOTE – Two stations located on the same subnetwork (i.e. with no gateway between them) will have IP addresses whose network parts (the first one, two or three octets) are identical.

It is possible to divide up a network which has a single Class A, B or C address into different subnetworks interconnected by routers. The principles governing the addresses of such configurations will vary from one case to the next, depending on the allocation of IP addresses in each country and the organization of the NIC (Network Information Centre). On a PC (Windows 95 or 98), it is very easy to check an IP address. To do this, click on "Start", and then "Run ...". In the window which appears, type "WINIPCFG" as shown in Figure 2.2. The IP address of the host will appear, together with the adapter address, the subnet mask and the default gateway address (see Figure 2.2).

2.2.2.4 DNS on the Internet

Computers which are connected up momentarily to the Internet via a modem are given a "temporary" address by the access provider, valid only for the connection session. Other computers are permanently hooked up to the Internet and have fixed IP addresses. This gives rise to some confusion. For this reason a system of symbolic names is used which are easier to read and memorize. A mechanism based on the use of hierarchical name servers (Domain Name Server – DNS) enables the digital address of a computer to be found from its symbolic name.

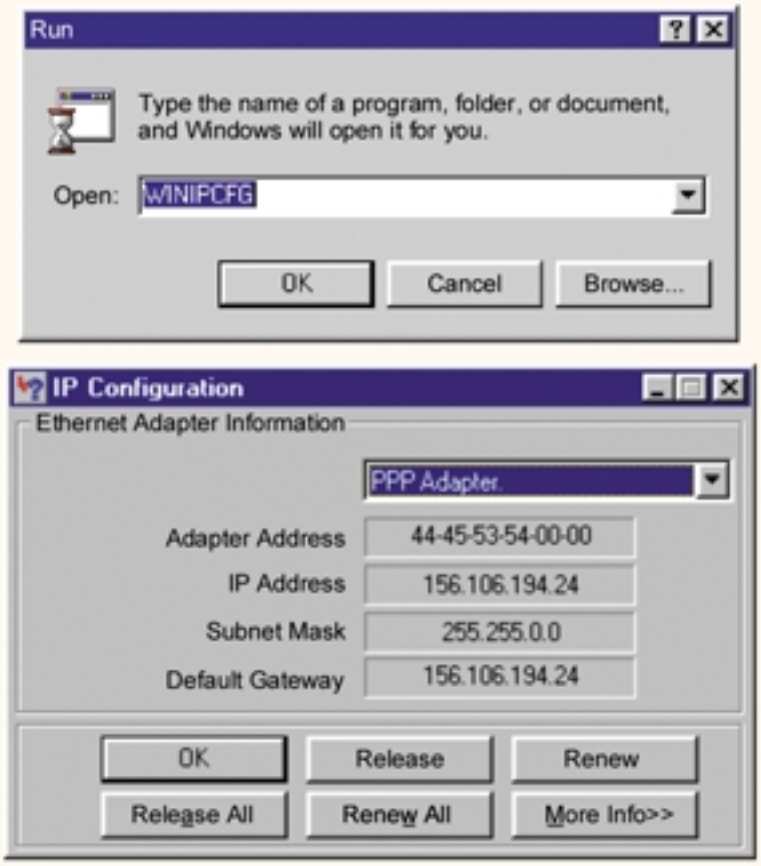

Fig. 2.2 Checking the host's IP address on the network (ITU host)

The Internet has been divided into *domains* (known as Top Level Domains) which, in turn, are divided into subdomains. These can be further divided into sub-subdomains, and so on. The DNS servers at the top of the hierarchy (level 1) know only the servers of the level immediately below (level 2) in each domain.

The domain name servers for level 2 know only the root servers (level 1) and those in level 3 which are in their domain (subdomains). And so it goes on. The number of levels may vary from one domain to another. The Internet name of a machine indicates the number of subdomains which have to be gone through, from the level of the machine itself right through to a Top Level Domain (TLD). There are two categories of TLD, national and generic.

Main domains (TLDs)

- *com:* commercial network
- *org:* non-profit-making organizations
- *gov:* US government agencies
- *mil:* US military agencies
- *edu:* US educational agencies
- *net:* organizations with a very large network
- *ml:* Mali
- *rw:* Rwanda, etc.

Some new domains were proposed in February 1997. These are:

- *firm:* businesses and firms
- *store:* businesses offering goods for sale
- *web:* entities whose activities are mainly Web-related
- *arts:* entities in the field of culture and entertainment
- *rec:* entities concerned mainly with entertainment
- *info:* entities which provide information services
- *nom:* individual or personal nomenclature.

The TLDs are managed by the Internet Assigned Number Authority (IANA). The IANA is the central coordinating body for assigning unique values for parameters such as Internet addresses, domain names, protocol numbers and port numbers, in relation to all the Internet protocols. Management of Internet addresses within a subnetwork is decentralized. DNS servers manage separate databases for electronic mail addresses and computer addresses.

To speed up response times when a request is made, the DNS servers tend to keep an updated cache containing recently requested addresses, to avoid having to go through the DNS hierarchy repeatedly in search of addresses which are requested frequently. The main problem with this mechanism is that, if an address cannot be found for whatever reason, this "negative" piece of information is also stored in the cache, even if the problem was only a temporary one. It may therefore prove impossible to connect to another machine, even once it has become operational again, as the fact that it was not accessible has been recorded in the memory.

DNS servers operate in both directions: giving the symbolic address for a certain digital address, and vice versa. The principle of aliases makes it possible to have several symbolic names corresponding to one digital address.

2.2.2.5 The ARP and RARP protocols

The physical addresses of the hosts are stored in a PROM on a network interface card, while the logical addresses are stored in files on disk. Two machines within a particular physical network (or subnetwork) can communicate only if they know the other's physical address. The addresses handled by the upper layers are logical addresses, which transcend considerations concerning the type of network architecture (Ethernet, Token Ring, X25, etc.). A mechanism is therefore needed to map these physical and logical addresses onto each other.

To illustrate the problem, let us take the case of an Ethernet network. The host's Ethernet address is stored in six octets, while its Internet address is stored in four. How can we convert a 32-bit logical address into a 48-bit physical address? The answer lies with the Address Resolution Protocol (ARP).

The case of a station with no disk is also worth looking at: it knows its physical address, but not its logical address. In order to obtain its logical address, it uses the Reverse Address Resolution Protocol (RARP). The problem of obtaining its own logical address must be solved before tackling the problem of obtaining the physical address of a remote host. A station without a disk cannot reply to an ARP request if it does not know its own logical address, since it would be unable to recognize that the ARP message was addressed to it. Accordingly, it must send out an RARP message as soon as it is switched on, even before its operating system, or any applications, are started up (via the network).

IP automatically starts up ARP and RARP, in a way that is completely transparent to both programmer and user.

2.2.2.5.1 How the ARP protocol works

Host A wishes to send a message to host B, but knows only B's logical address (i.e. its Internet address). A sends a specific message containing:

- its own logical address;
- its physical address;
- B's logical address.

This message is sent to all the hosts on the network (broadcast). Only host B recognizes its Internet address, and retrieves it. It then returns a message to A (whose physical and logical addresses it knows) giving its physical address. From that point on, the two machines can begin to communicate. As broadcast is a very expensive mechanism which uses considerable amounts of network resources, it is clearly not an option to follow the above procedure each time a message is sent. Each host therefore manages a cache containing a mapping table of logical and physical addresses which it has obtained recently. Before sending a broadcast message, the protocol checks whether the physical address being sought is in the cache.

2.2.2.5.2 How the RARP protocol works

A network host which wishes to obtain its logical address sends an RARP message containing its physical address to all the hosts on the local network. Only one host, the one which has the correct configuration, recognizes the RARP message. This address server has a mapping table giving the physical addresses of stations with no disk, and their logical addresses. It therefore sends a message back to the station with no disk, giving its logical address.

To prevent overload of the address server, a network will often have a number of servers, all capable of replying to RARP messages. This protocol is used only by network hosts which do not know their logical address, e.g. stations with no disk.

2.2.2.6 The ICMP protocol

The Internet Control Message Protocol (ICMP) allows two hosts to exchange test and control messages, and authorizes the detection of any problems which might arise on the network. ICMP datagrams are encapsulated in IP datagrams. Each ICMP protocol message is linked to a type which gives information on an event which has occurred on the network, for example:

- "*Destination Unreachable*": A gateway has received a datagram which it cannot transport (its routing tables do not provide it with the necessary information). It therefore sends an ICMP message of this type to the sender of the datagram. The same principle applies if the destination's IP layer cannot convey the message to the next layer up.
- "*Time Exceeded*": This warns the sender of an IP datagram that the datagram has been destroyed because the time-to-live field of the header is 0.
- "*Parameter Problem*": This message is sent by a host which does not recognize the IP header of a datagram it has received. The message is sent when the datagram has been destroyed.
- "*Source: Quench*": This message is sent if a gateway has insufficient memory to continue to receive datagrams (network congestion).
- "*Echo*": This message is sent by a host to test the integrity of the line. The host stands by to receive an "echo reply" message in return.
- "*Echo reply*": Transmitted by a host which receives an echo message.

2.2.2.7 New IPv6 addressing system

The stock of IP addresses is running out, with a shortage expected to arise some time between 2000 and 2010, given the speed of growth of Internet connections. The current system of addressing therefore poses a problem. IPv4 addresses are composed of four octets, i.e. 32 bits. IPv6 address are coded in 16 octets, i.e.

128 bits, giving 2^{128} possible addresses. IPv6 does away with the division of addresses into classes in favour of a more hierarchical system made up of three types of address: unicast, multicast and a new format known as anycast.

- Unicast addresses. This address format is close to the IPv4-type address, and is based on the service provider. It contains the address of the service provider, the address of the client with the service provider, a network indicator for the client and an interface address.

- Multicast addresses. As with IPv4, this type of address enables packets to be sent to several hosts within the same group simultaneously.

- Anycast addresses. This new format makes it possible for the same physical address to be assigned to several interfaces on the network. Packets sent to an anycast address are directed to the nearest physical interface. The concept of proximity is managed on the basis of a formula which takes account of transmission costs and performance.

The structure of the IPv6 header has been simplified considerably: it contains only eight fields, which speeds up the processing of the packets. We do not propose to enter into details here, having outlined the basic principles. For further reading on the subject, we would recommend "IPv6 Théorie et pratique" (IPv6: Theory and Practice) by Gisèle Cizault, published by O'Reilly.

2.2.2.8 Security and authentication

Internet applications such as electronic commerce call for heightened confidentiality and security: credit card numbers are in circulation on the Net, as are electronic signatures, and also transfer orders whose origin and content must be certain. IPv4 did not provide an integrated solution to the problem, and additional software had to be used. IPv6, on the other hand, includes two methods for ensuring security within the network layer itself:

- The first of these makes it possible to prohibit a sender from addressing packets to a destination without having first established a connection and identified himself in a secure manner. The operation of the algorithm is left to the discretion of the developers. This method deals with the majority of attacks.

- A second method consists in deciphering the host data exchange, thus creating a sort of "IP tunnel" and preventing the data from being intercepted and modified.

2.2.2.9 The IPv6 protocol and multimedia on Internet

IPv6 will deliver considerable improvements to multicast, the videoconference-type application. Multicast makes it possible to send packets to several destinations at once. Rather than sending the same data to each recipient, the data are sent only once, and are distributed by intermediate IPv6-compatible routers. Figures 2.3 and 2.4 illustrate how this works.

2.2.2.10 The TCP protocol

The *Transmission Control Protocol* (TCP) was developed to ensure reliable communications between two hosts on the same physical network, or on different networks. TCP is used for the ordered, bidirectional transport of data in *connected mode*. It complements the IP protocol. The TCP protocol is responsible for cutting up the stream of data transmitted by the upper layer into segments, which constitute the data units handled by TCP.

To prevent any loss of information between hosts, TCP uses a mechanism whereby a station wishing to send a packet to another station sends it at regular intervals until such time as it receives a positive acknowledgement. TCP uses a sequence number to identify each segment, in order to avoid duplication. However, a host does not issue an acknowledgement for each segment as it is received, as this would slow down the communication to an unacceptable degree.

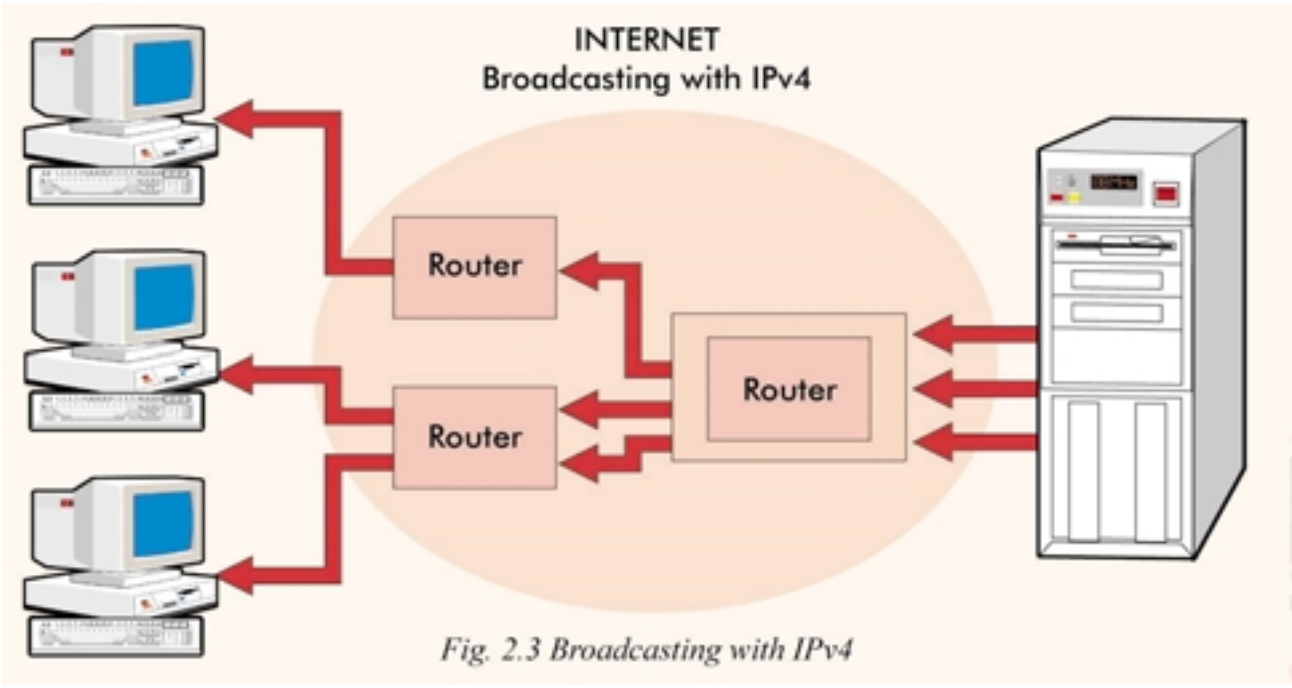

Fig. 2.3 Broadcasting with IPv4

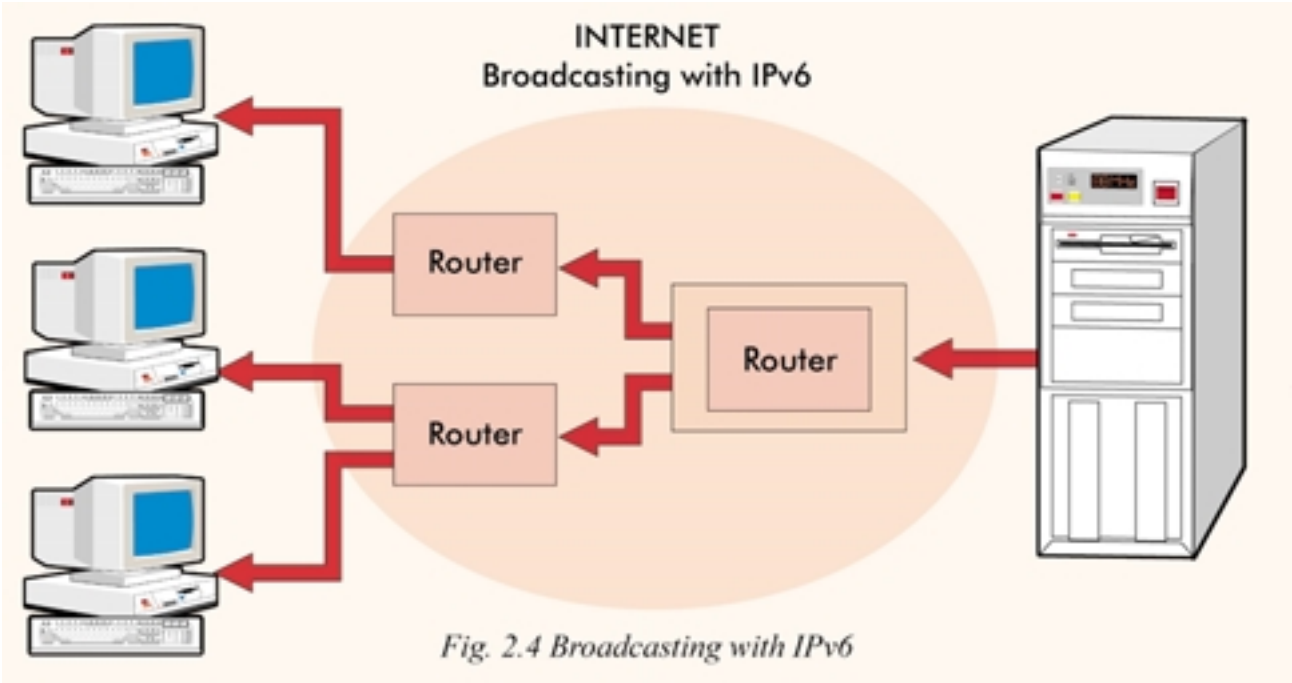

Fig. 2.4 Broadcasting with IPv6

2.2.3 The other main protocols in the TCP/IP suite

2.2.3.1 Gateway to Gateway Protocol

GGP (Gateway to Gateway Protocol) enables two gateways to exchange routing information in order to keep their routing tables up to date. It is used only on long-distance networks, where there are a number of different paths to the same host, and is of no use on local networks. The GGP data units are encapsulated in IP datagrams. The information carried by GGP consists of pairs of network addresses and distances, the distance of a network being expressed as the number of gateways to be passed in order to reach it. A gateway which stores this kind of information can thus choose the best option for transporting a data unit by the shortest possible route. The information is passed on from one gateway to its neighbour. Further details can be found in the book "Réseaux TCP/IP" (TCP/IP Networks), published by Wan & Laser.

2.2.3.2 The BOOTP protocol

This is used by stations with no disk to obtain their IP address. It is an alternative to RARP, and operates on the same principle.

2.2.3.3 The SMTP protocol

Simple Mail Transiter Protocol (SMTP) is the standard protocol for electronic mail exchange on TCP/IP networks.

2.2.3.4 The SNMP protocol

Simple Network Management Protocol (SNMP) is a network administration protocol which allows data to be obtained on the functioning of the network.

2.2.3.5 The XDR and RPC protocols

XDR (eXternal Data Representation) is a protocol used at the presentation layer of the OSI model. It allows data to be encoded in a standard manner in order to resolve problems of differences between platforms.

RPC (Remote Procedure Call) provides applications developers with a mechanism for making calls to remote procedures in virtually the same way as calls to local procedures. Both these protocols were created by Sun Microsystems in 1986, as part of the development of the NFS (Network File System) and the NIS (Network Integration Service).

2.3 Interconnection of transmission networks on Internet

2.3.1 General remarks

A transmission network enables any computer equipment connected up to it to communicate directly with all other hosts. There are three major categories of transmission network: circuit-switched networks, message-switched networks and packet-switched networks.

Circuit-switched networks were the first to emerge. The public switched telephone network (PSTN) is the oldest example, and the one most frequently used to connect subscribers to the Internet via the local loop. Further details can be found in "Réseaux TCP/IP", published by Wan & Laser.

2.3.1.1 Circuit-switched networks

A circuit is constructed between a transmitter (data terminal equipment) and a receiver (data circuit termination equipment), which is for the sole use of the two entities communicating. The circuit must be created before the information can be transported, and lasts until one of the two parties breaks off the communication. If neither correspondent has any data to transmit over a given period of time, the link remains idle. This gave rise to the idea of concentrating several communications on the same link, in order to increase the rate of use. If a large number of communications are using the same link, a queue will form. Buffer memory is therefore needed to store messages until the link becomes available.

2.3.1.2 Message-switched networks

A message is a sequence of information which forms a logical whole for both sender and recipient, e.g. a complete file, a line typed on a terminal, a sector on a disk, etc. A message-switched network is a meshed network of switching nodes. The message is sent from one node to the next until it reaches its destination, and cannot be passed on to the next node until it has been fully and correctly received. Buffer memory is needed for the intermediate nodes to memorize messages until they have been correctly stored in the next node.

A transmission management system is also needed to acknowledge receipt of messages which have been received correctly, and request retransmission of those containing errors. Furthermore, since the intermediate memories have only limited capacity, message flow control will be needed in order to prevent overflow. Message routing policies can be introduced to assist transmissions and make them more secure. If a link breaks down, for instance, provision must be made for an alternative path. If messages are too long, as in the case of some files, for example, they may be stored on disk at the intermediate nodes. This leads to a very substantial increase in response time.

2.3.1.3 Packet-switched networks

The concept of a packet-switched network was devised in order to speed up transmission times and make error recovery much simpler. A *packet* is a sequence of binary information which may not exceed a certain predetermined length. User messages are divided up into packets so that they can be transmitted more easily. The maximum length is usually between 1 000 and 2 000 bits (125 to 250 characters). The principle is the same as for message-switched networks, but the blocks of information are much shorter.

Packets are sent independently of each other, and the links between switching nodes send them on as they arrive. Packets from several messages can therefore be multiplexed at one time on the same link.

The task of the switching nodes is to direct the packets towards the right exit which may be indicated, for instance, in a routing table. The links between switches are not dedicated to a source-destination pair as in the case of circuit switching. Instead, a link is used simultaneously by all the packets which are routed that way.

Managing small blocks of information offers greater simplicity than message switching, particularly when it comes to error recovery. On the other hand, it raises the problem of reassembling the packets to form the original message again. In particular, if packets take different routes and one gets lost, it is usually necessary to recover the entire message.

2.3.2 Physical transmission media on Internet

2.3.2.1 General remarks

Three main transmission media are used on the networks: twisted pair, coaxial cable and optical fibre. The choice of medium depends largely on cost and the bit rate required. There is a choice between baseband transmission, where the message occupies the full bandwidth of the cable, and broadband transmission, where several messages are transported simultaneously, at different frequencies. The signal may be:

- *digital:* this is a square signal. A certain voltage (or combination of voltages) over a certain period of time represents a binary 1, while another voltage (or combination of voltages) over the same period represents a binary 0.
- *analog:* this is a sine-wave signal. The information is encoded by varying the frequency of the signal, or the signal phase, or by a combination of both.

As a result of technological advances and reasonable investment costs, increased use is being made of wireless technologies for transmitting data on the Internet. We will examine these technologies further on.

2.3.2.2 Twisted pair

This is the simplest physical medium, consisting of pairs of electrical wires, in some cases shielded. It enables data to be transmitted at speeds of 100 Mbit/s over distances of 100 m.

- The main advantages of this medium are the simplicity of connection, and its affordable cost.
- The disadvantages are slow bit rates, due to considerable signal attenuation and to its susceptibility to electromagnetic interference, which can be reduced by shielding. This kind of cable is used in particular by Token Ring and Ethernet 10Base-T and 100Base-T.

2.3.2.3 Coaxial cable

A coaxial cable is made up of two cylindrical conductors of the same axis separated by an insulator. The central conductor is known as the core. This medium, which is used increasingly, limits interference from external noise. If interference levels are high, shielding may be necessary.

It has been demonstrated that the relationship between the diameters of the two conductors should be 3.6. The different cables are identified by the diameter used, given in mm. The two most common are 9.5/2.6 and 4.4/1.2.

The first of these (9.5/2.6) allows bit rates of 10 Mbit/s using a 200 m cable. The second (4.4/1.2) allows data to be transmitted at similar speeds over a 500 m cable. Both have external sheaths. They are used for Ethernet 10Base5 and Ethernet 10Base2 respectively (described at 2.3.4 below).

As with metal wires and for the same reasons, the shorter the distance, the higher the bit rate which can be attained. However, certain limits cannot be exceeded, as signal attenuation increases with the frequency. Coaxial cable is more expensive than twisted pair, and connection is less straightforward.

- For 10Base2, a T connector is used;
- for 10Base5, a so-called “vampire” connector is used, one element of which goes through to the cable core.

2.3.2.4 Optical fibre

Optical fibre is a relatively new technology which is not yet in widespread use. With metal wire, the information is transmitted by means of a modulated electrical current. In the case of optical fibre, a modulated light beam is used. This type of transmission did not emerge until the advent of laser in the 1960s. With this medium, bit rates of the order of Gbit/s can be reached over a distance of several kilometres. This is the most expensive medium, but also the most reliable.

2.3.3 Access technologies

2.3.3.1 Carrier Sense Multiple Access (CSMA/CD)

This technique was developed for radio networks, and is used on bus networks. This is the technology used on Ethernet-type networks. It is based on the assumption that the traffic generated by each node comes in the form of short bursts. As long as the network is not close to saturation, the likelihood of two nodes wishing to transmit at the same time is therefore slight, and nodes send packets without prior authorization.

One refinement designed to reduce the risk of collision consists in each node listening to the network constantly when it is not sending data, to establish whether a packet is being transmitted. Nodes then commence sending when the network is free. This technique is known as Carrier Sense Multiple Access (CSMA). The risk of a collision is still there, as a packet can be sent without being detected by another station owing to the propagation delay on the network.

A further refinement consists in nodes listening during transmission in order to detect possible collisions. If a collision is detected, transmission stops. This technique does not reduce the number of collisions, but limits the damage when one occurs. With this feature incorporated, the technique is known as *CSMA/CD* (CD for Collision Detection), and is used by Ethernet networks.

The *advantages* of this technique are as follows:

- Ethernet is the most widely used network, and the first local network to have achieved consensus in industry and been standardized;
- as long as the number of collisions remains low, this method of access is fast and efficient.

The *drawbacks:*

- network performance declines rapidly if the collision rate exceeds 5%;
- in the 10Base5 version, the medium is an expensive special cable;
- the correct functioning of the access method calls for a maximum roundtrip delay for a signal on the bus, and thus a maximum bus length. As this constraint is linked to the propagation time rather than to the weakening of the signal, it cannot be overcome by using repeaters;
- there is no set limit on waiting time before transmission of a message, only a probability that it will not exceed a certain value. This raises problems for real-time applications in industry and/or for digitized voice transmissions.

2.3.3.2 Token bus

With this type of network a specific signal (the token) is propagated on the network. Any station which receives the token may retransmit it immediately if it has nothing to transmit, or intercept it and send its message before retransmission. The token is a special signal designed to be recognized and generated rapidly.

The main advantage of token bus networks is that they combine the reliability of passive bus structures with the guaranteed minimum throughput which the token technique offers, unlike CSMA/CD (see 2.3.3.1 above). In addition, as the bus operates in broadcast mode, the information is transmitted in a single stage to the destination station. Each station can therefore buffer the entire frame without reducing performance, which is not the case with ring networks.

2.3.3.3 Token Ring

On this type of network, information circulates from one station to its neighbour until it has gone around the ring. In order to minimize the impact of buffering in intermediate stations on the transfer time between two stations, stations which do not wish to send or receive simply retransmit the information.

When a station wishes to send a message, it seizes the token, interrupting retransmission, and inserts the information to be transmitted in its place. This information goes around the network, passing the destination station, which takes a copy, before returning to the transmitting station, which extracts it from the ring and reinserts the token. A very simple acknowledgement procedure can also be implemented, so that the transmitting station knows whether the information has been received.

2.3.4 Ethernet architecture

2.3.4.1 How it works

The Ethernet architecture is made up of two basic layers: the physical layer and the control layer which correspond to layers 1 and 2 respectively of the OSI model (see Figure 2.1). The advantages of this architecture are the clear demarcation of responsibilities between layers, and the degree of flexibility, which means that the control layer is transparent to any type of physical connection.

Ethernet uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD) (see 2.3.3.1 above). When a station wishes to transmit on the network, it begins by examining whether or not the carrier is occupied. If data are being transmitted, the station waits until the network becomes free before commencing transmission. Collisions are of course possible owing to the number of machines sharing the network.

When a collision does occur, the transmitting station interrupts transmission and transmits dummy bits to warn the other stations on the network. The station recommences transmission at a later time, determined by a certain algorithm. Collisions are detected by comparing the signal transmitted by the station and the signal in transit on the network.

Owing to the speed of signal propagation, which is in the region of 200 000 km per second, and the span of just 2.5 km, retransmission of frames, even on busy networks, takes just a few milliseconds at most.

2.3.4.2 Ethernet base components

Ethernet is made up of four main components: the host station, the controller (Ethernet adapter), the connecting cable between the controller and the transmission system, and the transmission system itself.

2.3.4.2.1 The host station

The station usually consists of a computer, a terminal server, or a printer. Conventional terminals cannot act as stations as they have no network interface. However, they can be connected to a terminal server which will provide access to the network. In such cases, the station houses the controller.

2.3.4.2.2 The controller

The controller provides all the functions needed for access to the medium, including data formatting, link management, and encoding and decoding of information. The controller is physically installed on an Ethernet adapter which is plugged in to the bus of the host machine.

2.3.4.2.3 The connecting cable

The connecting cable is at the junction between the controller and the transmission system. As the controller takes care of the communication functions, this interface is quite straightforward, consisting of a cable (shielded twisted pair) between the controller and the transceiver. Often referred to as the “drop cable”, its maximum length is 50 metres. Some configurations simply dispense with this cable and connect the controller directly to the transmission system.

2.3.4.2.4 The transmission system

The transmission system includes the components required for exchanging data, in the form of a transmission/reception module called a *transceiver*. This box provides the necessary electronic environment for transmitting and receiving the signal, and for recognizing the presence of a signal from another station. It must also detect collisions. This system also incorporates the transmission medium (cable).

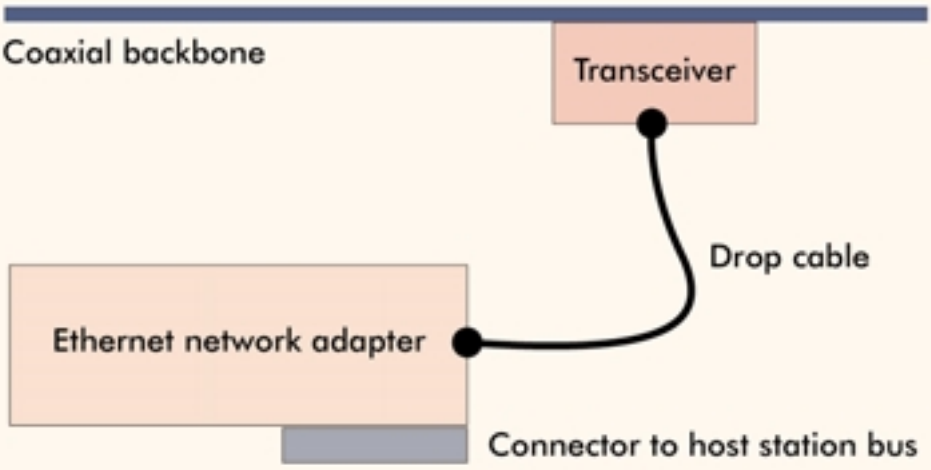

Fig. 2.5 Main components of an Ethernet network

2.3.4.3 Different Ethernet configurations

2.3.4.3.1 Standard Ethernet

A standard Ethernet network uses thick coaxial cable, known as 10Base5, as backbone, allowing baseband speeds of 10 Mbit/s to be attained. Each segment has a maximum length of 500 metres. A host can be connected every 2.5 metres, the points being marked on the cable. The total length of the network may not exceed 2 500 metres (five segments linked by four repeaters). The transmitter and cable are joined without a break, by means of vampire connectors. If the standard Ethernet network comprises more than two successive segments linked by repeaters, every second segment can be used only to extend the network, and cannot accommodate hosts. Figure 2.6 illustrates how the network is constructed.

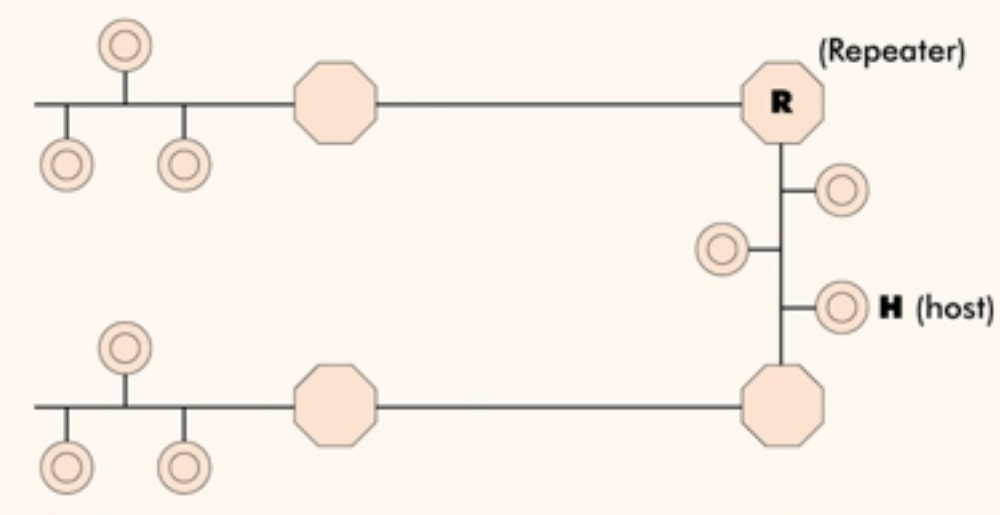

Fig. 2.6 Standard Ethernet configuration with maximum five segments

2.3.4.3.2 Thin Ethernet

Thin Ethernet uses fine unshielded coaxial cable of the type 10Base2 which delivers baseband speeds of 10 Mbit/s. Transceivers are linked to the medium by means of a BNC T connector. The physical characteristics of the cable limit the length of each segment to 185 metres. The maximum total length of the network is 925 metres, or five segments and four repeaters. Two hosts communicating with each other may not be separated by more than four repeaters.

2.3.4.3.3 Ethernet 10Base-T and Fast Ethernet 100Base-T

This type of network has a star topology. The transmission medium is made up of segments of twisted pair with a maximum length of 100 metres, which link each station to the central Host Unit Broadcast (hub). The bit rates achieved are 10 Mbit/s and 100 Mbit/s respectively. The 10Base-T and 100Base-T technologies are frequently used in conjunction with 10Base2 or 10Base5. A coaxial cable backbone links a certain number of hubs, so that the network can be extended widthways. RJ45 connectors (American telephone connectors) are used.

2.3.5 Token Ring architecture

2.3.5.1 General remarks

The Token Ring architecture was designed by IBM and adopted by the IEEE (Institute of Electrical and Electronic Engineers) as standard 802.5 (ISO standard 8802.5). The topology is ring, and access is by means of a token. There are two configurations: 4 Mbit/s and 16 Mbit/s.

2.3.5.2 The components of the Token Ring architecture

- The host station: as with Ethernet, this is usually a computer or a printer equipped with a network interface.
- The controller which is accommodated on the host's network adapter.
- The connecting cable, which links the controller to the MAU (Multistation Access Unit). It is made from twisted pair, shielded (maximum length 610 metres) or unshielded (maximum length 305 metres).
- The transmission system, which consists of an MAU which can connect up several host stations to a single point on the ring. It acts as a hub between a set of stations and the ring. The system also comprises a twisted pair cable, which may or may not be shielded.

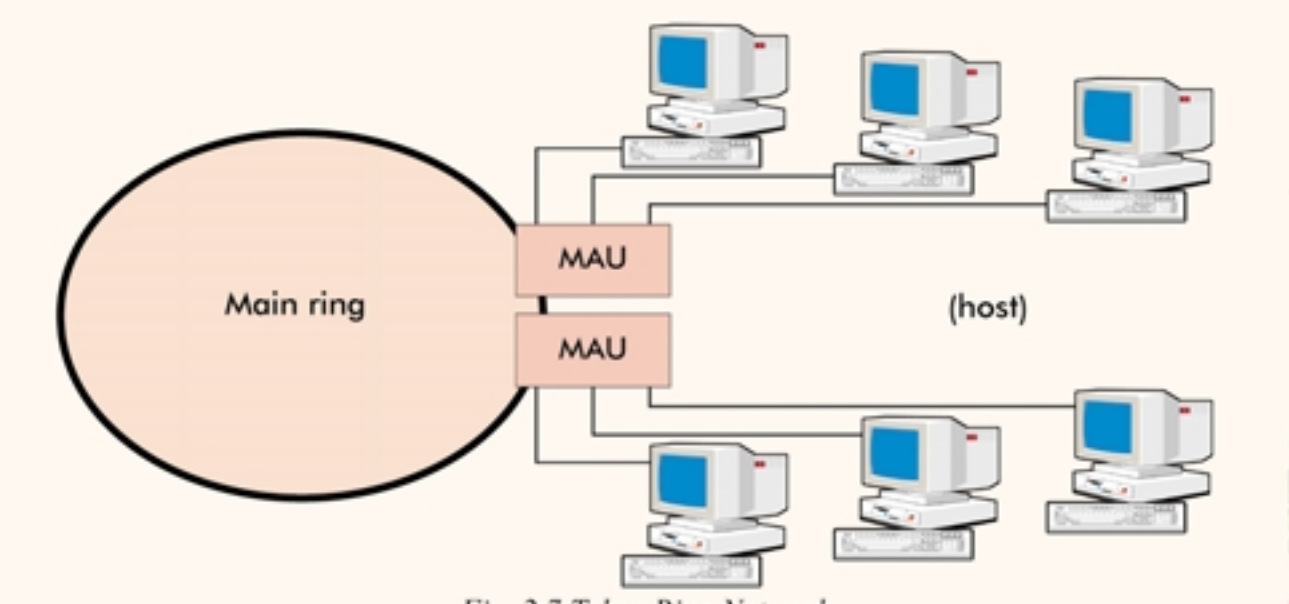

Fig. 2.7 Token Ring Network

2.3.6 Other architectures

2.3.6.1 General remarks

The architectures dealt with here are generally used to interconnect subnetworks of the conventional types (Ethernet or Token Ring). It is unusual to find hosts connected directly to these architectures, given the high costs and the fact that the conventional network interfaces do not operate at such high speeds, resulting in under-use of transmission medium capacity.

2.3.6.2 Ethernet 100Base-T

Ethernet 100Base-T delivers bit rates of 100 Mbit/s, regardless of whether twisted pair or optical fibre is used, and is deployed in a star topology around a hub. The method of access used is CSMA/CD.

2.3.6.3 Ethernet 100Base-VG or "AnyLan"

This transports both conventional Ethernet frames and Token Ring frames, over twisted pair or optical fibre.

2.3.6.4 FDDI (Fibre Distributed Data Interface)

FDDI comprises a double token ring using optical fibre, of maximum 100 kilometres length, with bit rates of 100 Mbit/s.

2.3.6.5 DQDB (Distributed Queue Dual Bus)

DQDB uses a dual bus on optical fibre at a bit rate of 155 Mbit/s.

2.3.7 Network interconnection equipment

2.3.7.1 General remarks

Interconnection equipment refers to equipment other than hosts connected to the network. Different names are used depending on the level of artificial intelligence and the role played in interconnection.

2.3.7.2 The hardware

- *Repeaters:* The sole task of repeaters is to retransmit and amplify the signal. They operate at layer 1 of the OSI model.
- *Bridges:* These operate at the data link level (layer 2) and have a certain logical function, as they make it possible to interconnect two networks with the same physical architecture, and to filter frames passing from one network to another, in order to avoid unnecessary congestion.
- *Routers:* These operate at layer 3 of the OSI model, and are responsible for routing the data units. They enable two networks of different types to be interconnected. A router transfers packets and analyses them at level 3 of the OSI model. A router can also act as a gateway between different types of networks (Ethernet to FDDI, Token Ring to Ethernet, ATM to FDDI, etc.). Finally, in the case of large, heavily meshed networks, the router will determine the best path to be taken in order to reach a particular address (the number of nodes, the quality of the line, bandwidth, etc.).
- *Gateways:* This is a generic term used to designate equipment operating at layer 3 or above. The task of gateways is the "intelligent" interconnection of different types of network.
- *Hubs (Host Unit Broadcast):* These are found at the centre of star configurations, and are responsible for interconnecting the different branches of the star.
- *MAUs (Multistation Access Units):* These are found in ring topologies, and are used to interconnect several hosts at a single point on the ring (see Figure 2.7).

3 Designing and implementing a national Internet node

3.1 General remarks

According to a report issued by the US Internet Council on 12 April 1999 (http://www.usic.org/usic_state_of_net99.htm), there were, in January 1999, more than 43 million Internet Servers (Network Wizards) worldwide, of which a mere 0.1829 million were in Africa. In 1998 there were 829 million web pages, a figure which was expected to rise to 1.45 billion at the end of 1999 (Internet Data Corporation).

At the end of 1998, according to the Computer Industry Almanac, there were 364.4 million personal computers in use throughout the globe. The breakdown was estimated as follows: 129 million (one third) in the United States, 32.8 million in Japan, 21.1 million in Germany, 18.25 million in the United Kingdom and 15.35 million in France.

The above statistics demonstrate to what extent Africa is lagging behind in terms of new information technologies, and the need to devise a specific plan of action in each country in a bid to resolve the problem.

In Chapter 2 we looked in broad terms at some topics relating to networks, network interconnections and data transmission. In this chapter, the focus will be more on designing, planning and implementing an Internet node at the national level. We will examine the active components used, and observe in each case the management and use of layer 2 (MAC) addresses and layer 3 (IP) addresses. This approach will give us a better understanding of how the various technical players in an Internet network operate. Telecommunication operators should subsequently be able, on the basis of their individual strategies, to develop the network by incorporating one or more interconnection nodes to provide regional or international access.

3.2 Planning a national Internet node

3.2.1 General remarks

In this paragraph, we will examine the various technologies involved in planning a national Internet node, and how they work. Some topics already raised in earlier chapters will be dealt with in greater detail, in order to make them comprehensible to the layman and allow professionals to conduct a rapid review of familiar concepts.

3.2.2 Network services and the layers of the OSI model

At the beginning of the 1980s, the members of various standardization committees decided to define a logical model describing the different elements which enable two computer systems to communicate. Almost ten years after work commenced, the OSI (Open Systems Interconnection) model was agreed. This model is designed to separate out all the processes and protocols which are involved in network communication, and organize them into seven levels according to their function. The aim of the standardization exercise, therefore, was to define the interfaces between each layer. The seven layers and the related services are set out in the table below.

Table 3.1 – OSI model and network services (*Source: FI-6 1998*)

OSI

Layer 7	Application	(FTP, SMTP)
Layer 6	Presentation	
Layer 5	Session	(DNS)
Layer 4	Transport	(TCP, UDP)
Layer 3	Network	(IP)
Layer 2	Data link	(Ethernet, Token Ring,)
Layer 1	Physical	(Coax, twisted pair, optical fibre)

Each layer is responsible for receiving and transmitting information to the two neighbouring layers, independent of the other layers. Figure 3.1 illustrates the relationship between the physical components of a network and the OSI model.

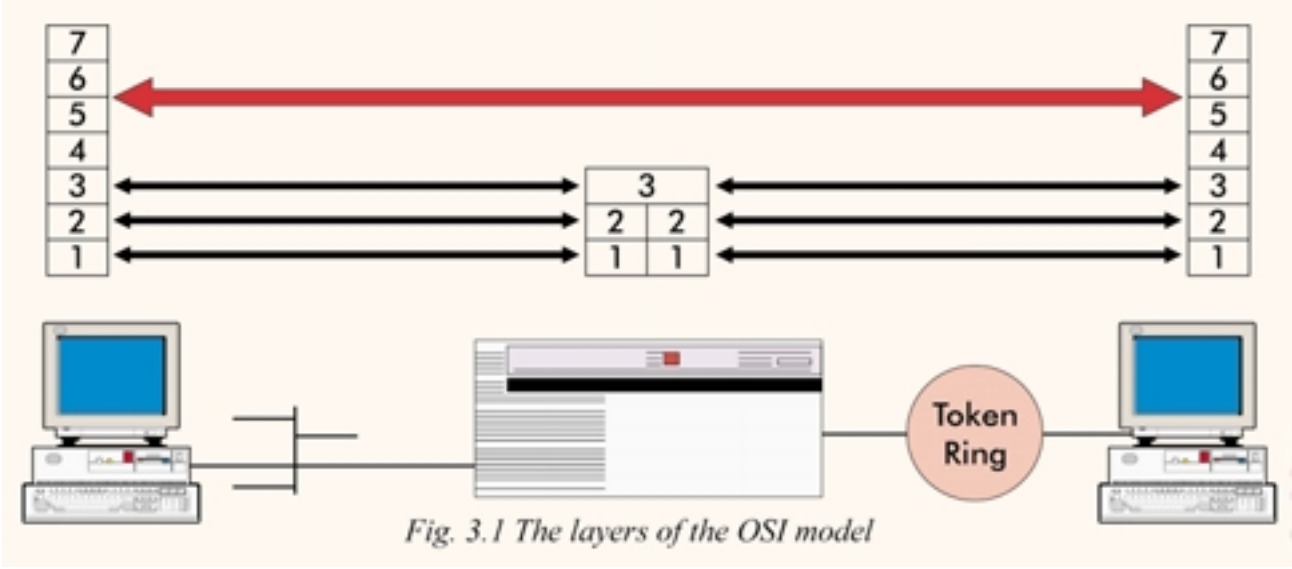

Fig. 3.1 The layers of the OSI model

Every computer must implement these seven layers if it wishes to communicate on the network to which it is connected. However, the active components of the network, such as the routers and switches, use only the first three layers (layers 1, 2 and 3) of the OSI model. As a general rule, the first two or three layers are found in all the network elements, while the four higher layers are confined to the hosts.

3.2.3 Encapsulation on Ethernet and TCP/IP

In order to illustrate how the different layers of the OSI model interact, we shall examine how the design is implemented, by taking a closer look at the addressing principles used in sending information across a network.



Fig. 3.2 Ethernet frame

The protocols described are Ethernet for layer 2 (Data link) and IP for layer 3 (Network). For further details see FI-6/1998.

Figure 3.2 shows the different addresses which are used when two stations are communicating. An IP message sent along an Ethernet segment contains four different addresses, two (a logical and a physical) indicating the destination of the message, and two indicating its source. The source addresses will be used by a station to identify and reply to its interlocutor.

The addresses used at the Ethernet level are known as MAC (Media Access Control) addresses. They are made up of six octets, and are generally expressed in hexadecimal form (A0-32-B1-98-17-D4). The MAC address is imprinted directly on the computer's network adapter or on the router interface (physical address). Each MAC address is absolutely unique.

IP addresses are allocated by users via software. They are made up of four octets, and are usually expressed in decimal form (156.106.194.24), as we saw earlier.

On a network, a station is identified by two different addresses: the MAC address and the IP address. In order to send a packet, it is not sufficient, therefore, to know the station's IP address; the MAC address is also required.

3.2.4 ARP protocol

The Address Resolution Protocol (ARP) is used to find the MAC address of a station from its IP address. Figure 3.3 illustrates how it works.

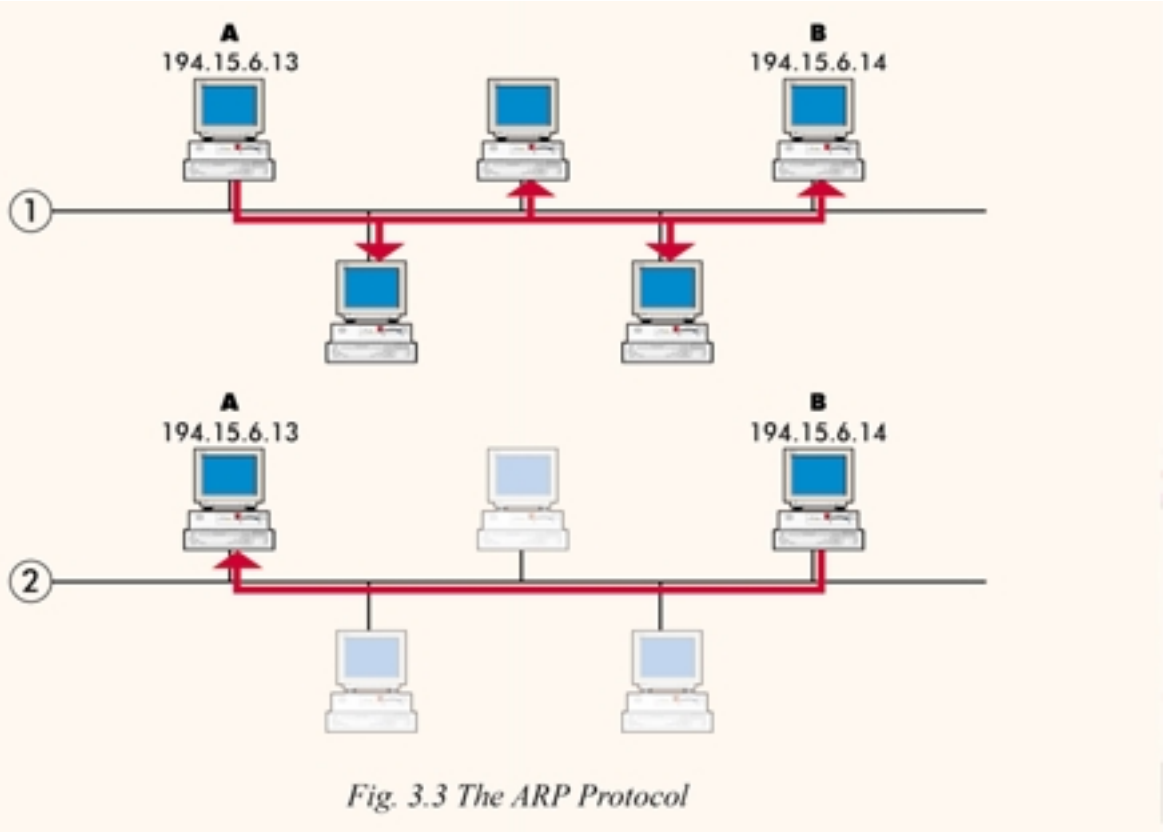

Fig. 3.3 The ARP Protocol

Station A wishes to send a message to station B, and knows its IP address, but not the MAC address to which it should send the Ethernet frame. In stage 1, it transmits an Ethernet broadcast containing the IP address in question (194.15.6.14). All stations receive this message and examine the IP address. In stage 2, station B alone replies to the ARP request, and incorporates its own MAC address in its reply. Station A can now send data to station B using this MAC address (s*ource: FI-6/1998*).

3.2.5 The Ethernet segment

The Ethernet segment is the simplest form of computer network. It is supported physically by coaxial cable or a wiring concentrator or hub. Figure 3.4 illustrates an IP communication between two stations on the same Ethernet segment.

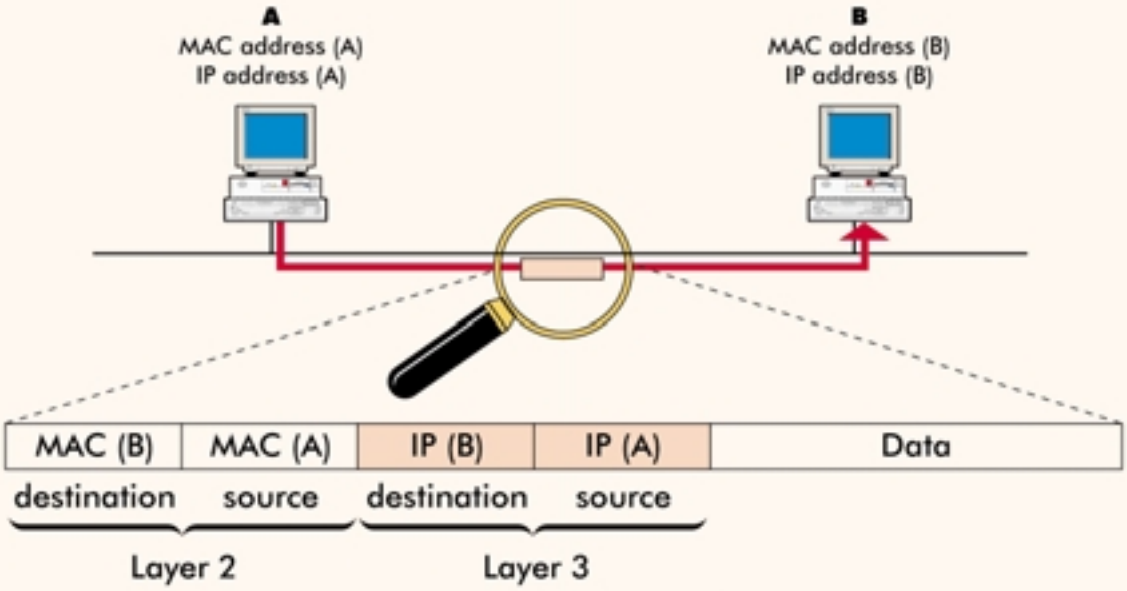

Fig. 3.4 Ethernet segment

Station A knew station B's IP address. It then sent out an ARP request to find out B's MAC address. Station A now has the two addresses needed in order to send a message to station B. All the packets sent will contain the four communication addresses: the MAC destination address and MAC source address for layer 2 of the OSI model, and the IP destination address and IP source address for layer 3.

With an Ethernet segment, the only addresses used are the four addresses belonging to the two stations which wish to communicate.

3.2.6 The router

Sharing of the transmission medium and size restrictions are a major problem on Ethernet networks. Regardless of the number of stations connected to an Ethernet segment, only one can transmit while the others wait their turn. In order to overcome this problem, routers are used. The aim of a router is to interconnect two Ethernet segments on two networks or subnetworks. Figure 3.5 illustrates how a communication works between two stations separated by a router.

This example highlights the role of the network administrator in the communication process. The IP address, the subnet mask and the default gateway have been configured on the two machines. The network administrator had to choose layer 3 parameters and assign values to the stations. He defined two subnetworks with 255 IP addresses, namely subnetwork 194.100.100.X, where station A is located under IP address 194.100.100.2, and subnetwork 194.100.200.X, where station B is located with the IP address 194.100.200.2, the two being separated by a router.

The router is a gateway between the two subnetworks. When station A decides to send a message to station B, it compares the network part of its IP address (194.100.100) with that of the destination (194.100.200). As the addresses of the two subnetworks are not the same, it will send the IP packet to its default gateway, i.e. the router. It therefore sends out an ARP request to find out the MAC address of the router, then constructs the Ethernet frame using the router's MAC address and sends it along the segment. The router receives the frame, and extracts only the IP message. It then sends out an ARP request to find the MAC address of station B, whose IP address it has obtained from station A's message, before sending the new Ethernet frame along the second segment to destination B.

The IP addresses contained in the message are those of the source and destination stations. They are never altered whilst in transit in the network; only the MAC addresses are modified.

The router is a layer 3 component, as it choose the destination of the message by reading the information contained at the IP level. For further details, see FI-6/1998.

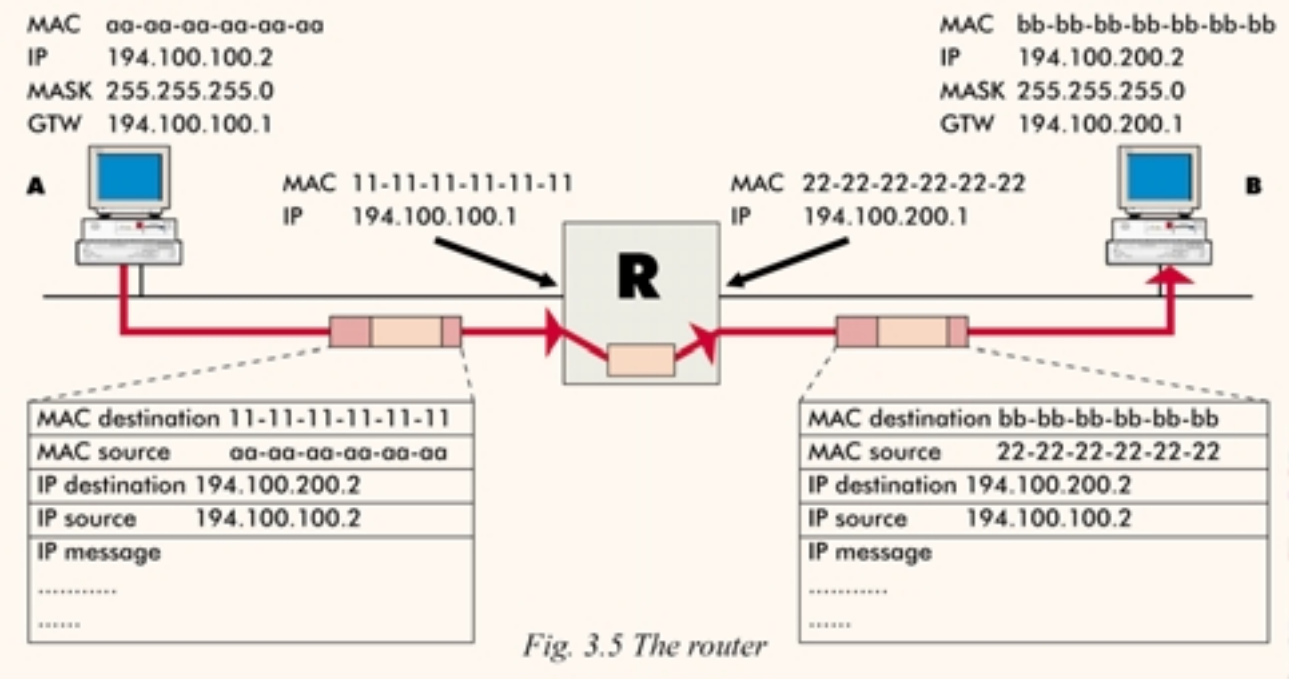

Fig. 3.5 The router

The advantage of routers is that they separate machines at layer 2. The internal Ethernet traffic on either of the segments will not go through the router, in other words ARP communications between two machines on the same subnetwork will not "contaminate" the other subnetwork which is not involved. Only the inter-segment communication goes through the router, at layer 3.

3.2.7 The switch

The switch allows an Ethernet segment to be divided up into a number of separate strands, thus allowing several stations to transmit at the same time while remaining connected logically to the same Ethernet segment. It draws up an address-port mapping table by reading the MAC source addresses, and uses it to propagate the frames received. When a frame contains an unknown address or gives a broadcast address, the switch propagates it to all ports so that all the stations can read it. Figure 3.6 illustrates how a switch works.

Switches are therefore a layer 2 component, and disregard the information transported in the Ethernet frames. Switches cannot be seen by a station. When a station wishes to send an IP packet, it makes an ARP request, which the switch propagates on all the strands (broadcast). The reply passes back through the switch, and communication between the two stations begins. The four addresses used are again those of the two stations concerned. For further details, see FI-6/1998.

With a switch, four or more stations can communicate simultaneously on the same Ethernet segment. Thus, the problems of shared medium use and size restrictions on the network are finally resolved.

3.2.8 The routing switch or IP switching

The routing switch, also known as a layer 3 switch or IP switching, was designed to deliver the same performance in terms of bit rates and latency as a switch, but at level 3 of the OSI model. In other words, it works not by extracting and routing the IP packet, but by switching it. Figure 3.7 illustrates the working of a routing switch.

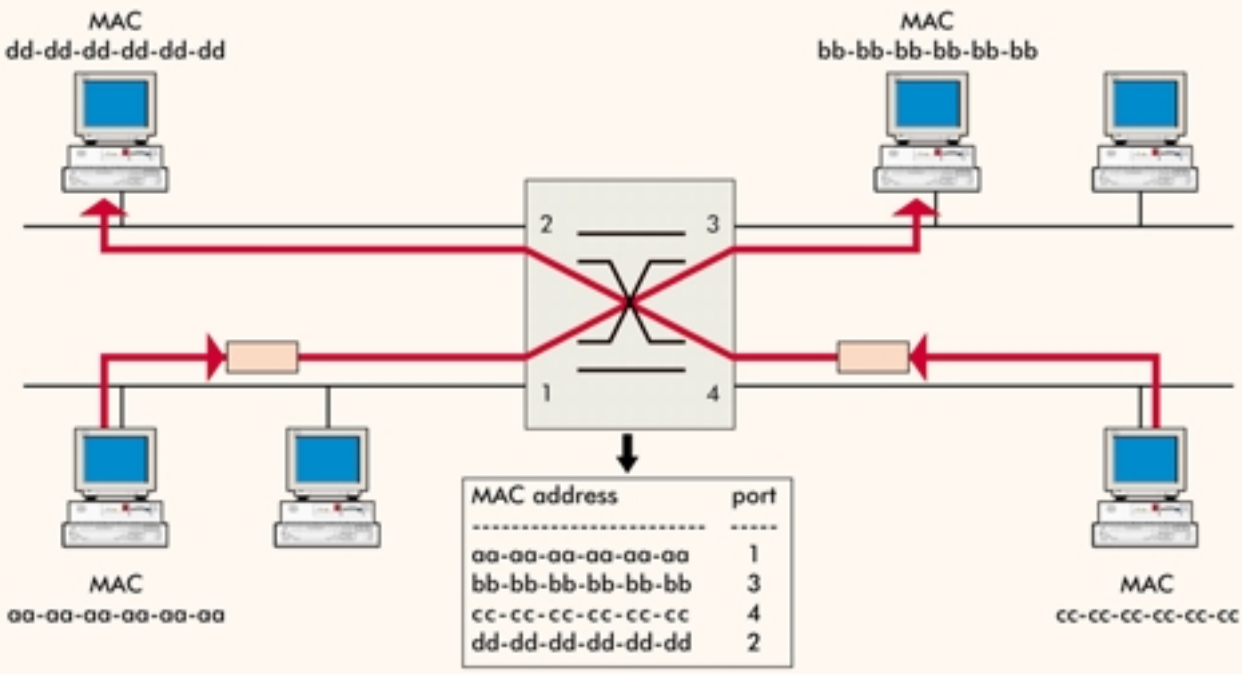

Fig. 3.6 The switch

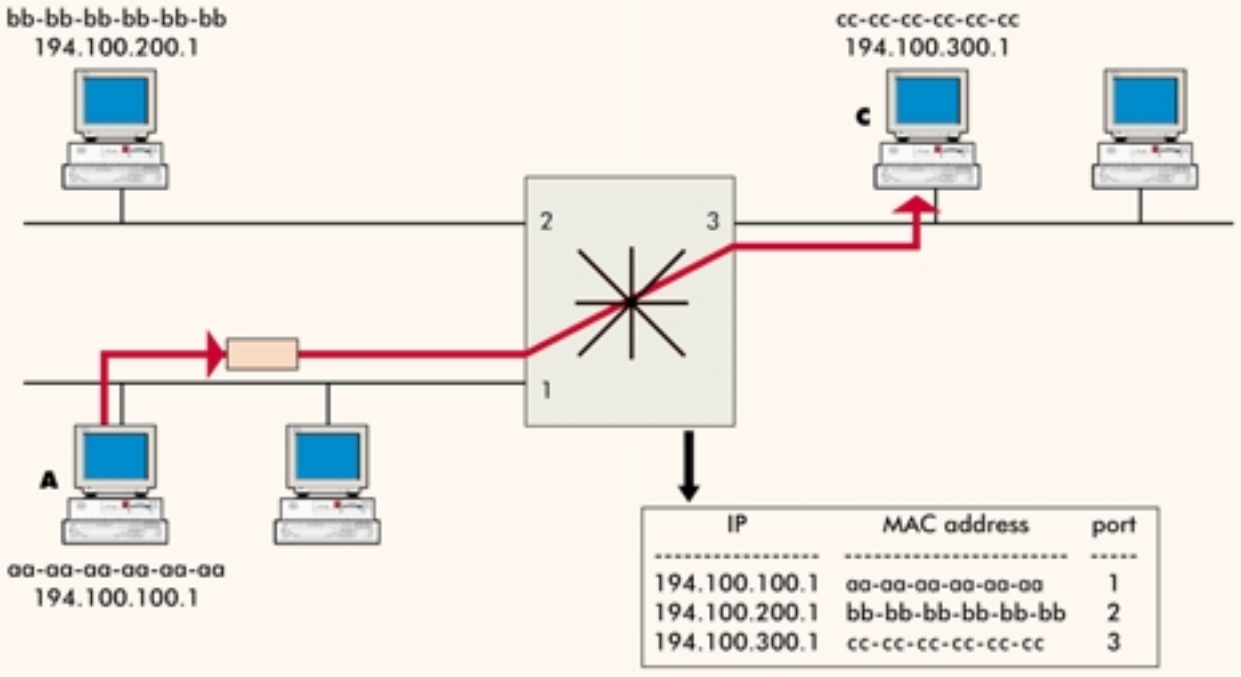

Fig 3.7 The routing switch

We saw at 3.2.6 above how a router has a routing table which maps IP addresses to ports, and, at 3.2.7, how a switch maps MAC addresses to ports. The routing switch draws up and maintains a table which combines the IP address of a station, its MAC address and the port to which it is connected. The decision to propagate a frame is taken on the basis of the IP destination address.

Taking as a basis the configuration set out in Figure 3.5, we can see that the router has been replaced in Figure 3.7 by the routing switch. The stations received the value 255.255.255.0 as a subnet mask and, as a default gateway, the address of the routing switch interface to which they are connected. The routing switch is therefore regarded as the default router, and behaves accordingly.

If station A wants to communicate with station C, it compares the two IP addresses and sends a frame to its default router, using the routing switch's MAC address. When the routing switch receives the frame, it reads the IP destination address, which corresponds to station C. It then looks up the corresponding values in the table, and discovers that station C's address, 194.100.300.1, can be accessed via port 3, and that the corresponding MAC address is cc-cc-cc-cc-cc-cc-cc.

The routing switch then modifies the MAC destination address of the frame (the address was that of its own interface), and switches it to port 3, as quickly as a layer 2 switch would have done. The routing switch therefore takes routing decisions on the basis of layer 3 addresses, but operates on the same switching principles as an Ethernet switch (s*ource: FI-6/1998*).

3.2.9 International connections and overall architecture

The choice of connection to the backbone of the international operator (MCI, SPRINT, CompuServe, UUNET, AT&T WorldN, Concert Internet Plus, etc.) must be guided by the quality of service and the topology of its network and that of its partners. A national, or even regional, operator has a wide choice of bandwidth, depending on its needs and its development strategy.

Table 3.2 – Typical bandwidths

56/64 kbit/s	448/512 kbit/s	6 Mbit/s
112/128 kbit/s	560/640 kbit/s	12 Mbit/s
2 24/256 kbit/s	672/768 kbit/s	45Mbit/s
336/384 kbit/s	1 244/1 544 Mbit/s	

For an operator with expected subscriber numbers of some tens of thousands using the World Wide Web, e-mail, newsgroups, FTP, etc., the ideal choice of bandwidth would be 1.2/15 Mbit/s (uplink/downlink).

Figure 3.8 below shows in outline the overall architecture of a meshed national Internet network, characterized by equipment redundancy. In this case we have shown two national Internet nodes, with the option for the national Internet operator to choose a connection from one or more international operators with an adequate safety margin.

The topology represented here constitutes a model for medium- and long-term planning, which can be adapted by the engineers responsible for planning and developing the network in the light of the national and regional context, incorporating the elements set out in Chapter 5 "Strategies and Development of the Internet Network".

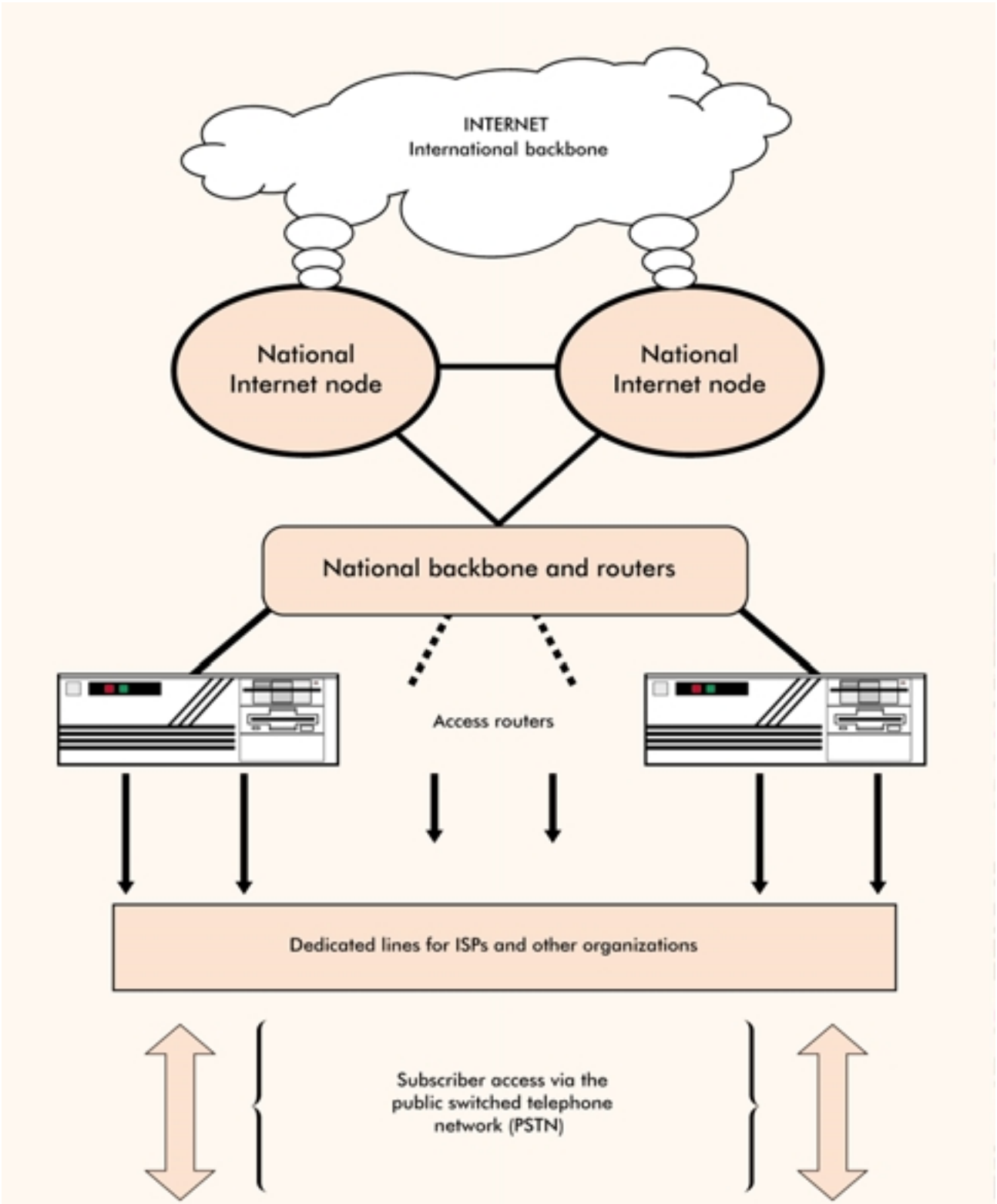

Fig. 3.8 Typical network architecture for Internet services used by a National Operator

3.3 Basic equipment for a national Internet node

3.3.1 General remarks

The access technologies which we have just described are very important for development of the Internet, particularly in Africa, which is falling further and further behind, with 0.4% of servers, compared with 65.6% in the Americas, 24.3% in Europe, 7.3% in Asia and 2.4% in Oceania (s*ource: ITU World Telecommunication Indicators Database*). Routing switch technology, although still in its infancy, should be incorporated into any planning and development strategy for the Internet network, depending on the state of development and topology of the national network.

The site accommodating the equipment for the national Internet node must be very well protected. Security should be of the highest standard at all levels, and encompass fire hazards.

3.3.2.1 Satellite link

With a satellite in geostationary orbit, i.e. on the equator, at an altitude of 36 000 km, data can be transmitted on the Internet by radio relay; three satellites are sufficient to cover the Earth.

The transponder is an essential part of a satellite, constituting the on-board module for receiving and transmitting the signal (uplink/downlink). It consists of a receiving antenna, a low-noise amplifier, a filter, a power amplifier for transmission and a transmitting antenna.

The transmitting power of the transponder depends on the width of the transmitter beam, which in turn depends on the antenna. The wider the area to be covered, the more power is needed. To transmit data on a comfortable backbone, 2 Mbit/s channels will generally suffice. The uplink and downlink frequencies are different, and about 3 MHz apart.

Good bandwidths can be achieved using satellite links. This is the most suitable solution for the African countries, given the lack of development of optical fibre links, which offer shorter propagation times. Tariffs vary depending on the operator, the bandwidth and what commercial contacts have already been established.

Depending on the infrastructure and the strategy of the operator, there are different ways of connecting up to the international operator's backbone. The following methods are commonly used:

- Point-to-point or Single Channel Per Carrier (SCPC) satellite access, at a minimum rate of 128 kbit/s. Other speeds are also offered, as we saw at 3.2.9 above (see Table 3.2). The dimensions of the parabolic antenna will depend on the choice of bit rate.

- TDMA (Time Division Multiple Access) shared satellite access. The recommended minimum rate is 128 kbit/s.

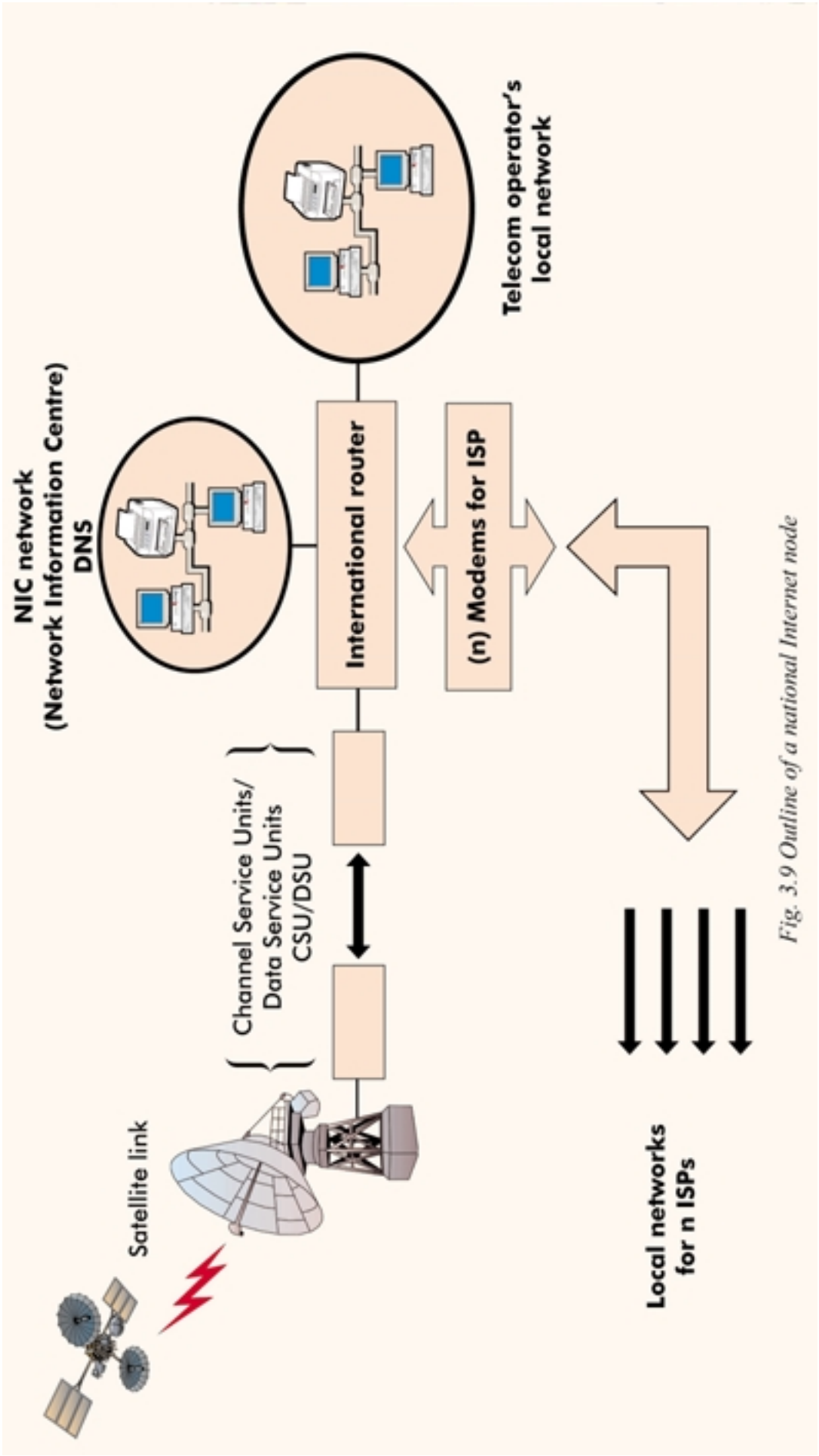

Fig. 3.9 Outline of a national Internet node

3.3.2.2 International router

The international router is connected to the earth station via a V35 CSU/DSU (Channel Service Units/Data Service Units) adapter. The router must have a port for connecting up the telecommunication operator's local network, and another for connecting to the NIC (Network Information Centre) for the DNS (Domain Name Server) and for backups. It must also have at least six ports for connecting up the Internet Service Providers (ISPs). When this router receives a packet, it looks for the address of the destination network in the routing table, and sends it to the interface concerned. If the destination address is not in the routing table, it sends the packet by the default route. The routing algorithm used takes account of some or all of the following factors:

- optimizing performance by choosing the best route in all cases. This depends on the metrics. For instance, a routing algorithm may take account of the number of hops and the delay, but may attribute greater importance to the latter in its calculations;
- simplicity and robustness;
- speed of convergence. Convergence refers to the process of finding agreement between all the routers on the best route to use. When a router makes a route unavailable or detects one which is unavailable or about to become unavailable, it informs the other routers by distributing a routing table update.

In order to make the router's work easier and facilitate the administration of the national Internet node, a network belonging to a particular address class needs to be divided up into subnetworks or subnets. To restrict the volume of traffic by geographical area and limit the number of broadcast packets, part of the address field is therefore allocated to the subnetwork. The subnet mask will enable the router to determine the route taken by packets being sent to machines on the same subnetwork (IPaddr AND Subnet Mask).

It is possible to force the use of a certain route in the routing tables by creating a specific route. This is known as a static route, as opposed to a dynamic route which is "learned" by the protocols.

The ARP (Address Resolution Protocol) table will contain the IP address-MAC address pairs needed to transport packets on the segments connected to the router interfaces. Packets issued or transmitted by this router will always contain its MAC address. The addresses contained in the ARP table have a limited lifespan, typically in the region of 240 minutes.

At the level of the router, certain addresses can be filtered out, e.g. *MAC or IP addresses which the administrator deems to be unusable for a variety of reasons*. The most frequently used routers are Cisco models 7513, 7507, 7000, 4500, 2511, 2516, etc.

3.3.2.3 DNS

One of the most important pieces of network equipment for the body which centralizes network information (the NIC), is the DNS (Domain Name Server). For this task we would recommend using a computer with a minimum configuration of 450 MHz, 128 Mb RAM, a 10 Gb hard drive, a 3COM Etherlink network interface card, a DVD drive, a 3.5″ disk drive, a 17″ SVGA monitor and the UNIX Solaris 2.x operating system. The same configuration is recommended for the secondary DNS server, which will contain backups of the primary DNS data. To maximize security, we would recommend highly restricted access. Sessions of Telnet, FTP, HTTP, SMTP, etc. should therefore be avoided.

3.3.2.4 Modems

Leased-line modems are used to connect the networks of the ISPs (Internet Service Providers) to the national Internet node. These lines do not go through any switching device. They are variously referred to as leased lines, dedicated lines and point-to-point lines. Amplifiers housed in the exchanges of the telecommunication operator can be used to reach ISPs located at a distance.

The modems used have a minimum bit rate of 64 kbit/s. The same type is used by both the national Internet node and the ISP. For instance, a pair of RAD ASM-20 or Patton 1 090 KiloStream modems might be used, connected using RJ45 connectors.

A modem (MOdulator-DEModulator) is a device which allows data for use by computers to be transmitted along telephone lines. A so-called "intelligent" modem can adjust to the parameters of the computer to which it is connected, and manage transmission over copper wire, e.g. by retransmitting if an error occurs, and compressing d

ata.

Low-speed modems (up to 64 k) use baseband transmission, i.e. the analogue image of the digital signal, while high-speed modems use the QAM (quadrature modulation) technique, but at a higher frequency and with more levels of modulation than modems for private-use switched lines:

- 64 kbit/s and 128 kbit/s on two wires;
- 256 kbit/s to 2 Mbit/s on four wires.

Table 3.3 – Transmission standards and speeds

CCITT standards	Speed	Modulation
V21/Bell 103	300 bit/s	FSK
V22/Bell 212a	1 200 bit/s	DPSK
V23	1 200/75 bit/s	DPSK
V22 *bis*	2 400 bit/s	QAM
V32	9 600 bit/s	QAM
V32 *bis*	14 400 bit/s	QAM
V34	28 800 bit/s	QAM
V34+	33 600 bit/s	QAM

3.3.2.5 Automatic electricity supply

The quality of the 220V alternating current electricity supply to the public cannot be guaranteed. For the basic architecture of the node, it is vital to use inverters or contingency supplies, referred to as UPS (Uninterruptible Power Supply). One inverter will be needed for the international router, one for the DNS and another for the local network. For large heavily meshed networks, some inverters equipped with an Ethernet or Token Ring interface including an SNMP agent are incorporated into the network and can be managed and monitored automatically despite their distance from the station which manages the network.

3.3.3 Local network

The Internet telecommunication operator's local network needs to have a router with at least two Ethernet ports, one to connect to the international router and the other to connect to the local Ethernet network, protected by a firewall. The recommended minimum configuration for the computers is 450 MHz, 128 Mb RAM, 512 Mb cache, a 10 Gb hard disk, a 3COM Etherlink network interface card, a DVD drive, a 3.5″ diskette drive, a 17″ SVGA monitor and the UNIX Solaris 2.x operating system. One server can be used for e-mail, the World Wide Web and file transfers. However, in the interests of better management, as we shall see later, we would recommend using one machine per Internet service (Web, e-mail, FTP, news, etc.).

For traffic analysis and accounting, a computer with a minimum configuration of 450 MHz, 128 Mb RAM, a 10 Gb hard disk, a 3COM Etherlink network interface card, a DVD drive, a 3.5″ diskette drive and a 17″ SVGA monitor is sufficient. The RADIUS public domain software can be used for authentication and billing. For further details, see the following Internet address: http://www.livingston.com/Forms/radiusform.cgi.

The communication server must be capable of establishing 100 simultaneous communications, with scope for extending that capacity. It must be modular and capable of being extended without disrupting service. The network can also be accessed via dial-up modems. The number may vary according to needs, and 16 33.6 kbit/s V.34*bis* rack-mounted modems may be sufficient to begin with, or for a pilot project.

3.3.4 Provision of Internet services: Netscape SuiteSpot

3.3.4.1 General remarks

By using Netscape SuiteSpot on the LAN (the national telecommunication operator's local network), it is possible to provide the full range of Internet services like a conventional ISP. This is a simple solution for anyone with adequate experience on Solaris 2.x. The system's general administration is very well suited to Internet services, as shown in Figure 3.10.

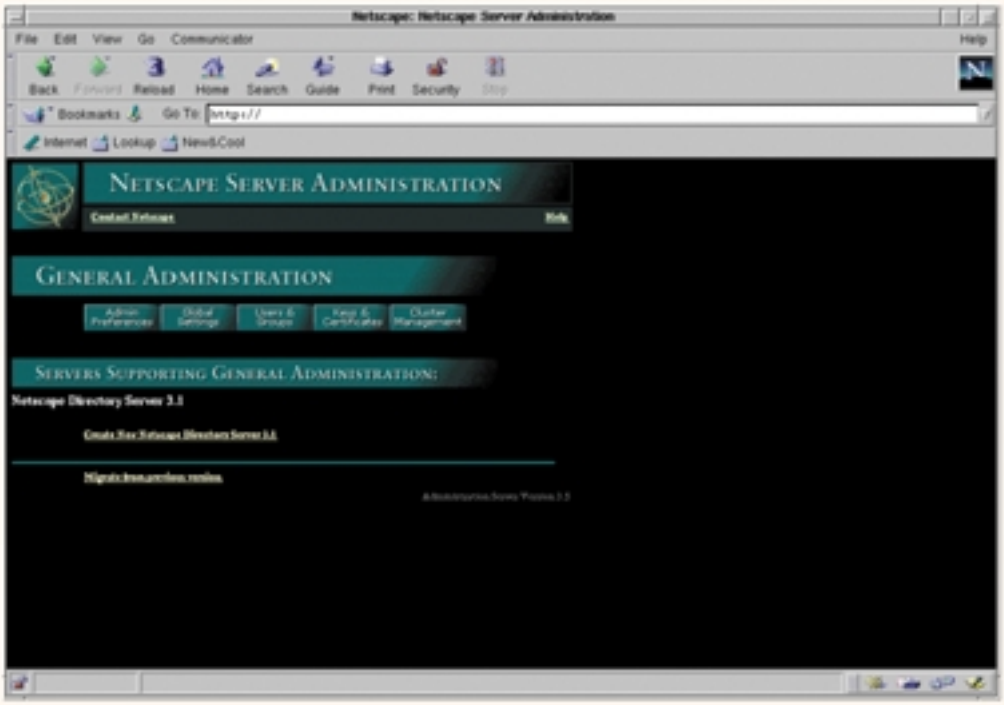

Fig. 3.10 Netscape Server Administration Interface

To enhance management and performance, it is recommended wherever possible to use a dedicated machine for each server. Microsoft's Internet Information Server 4.0 is also worth considering and has the features required. Some of its components, such as Microsoft Certificate Server, are just as valid as their SuiteSpot equivalents. The choice of Netscape SuiteSpot was dictated by the current climate, in which Sun Microsystems, AOL and Netscape have joined forces to dominate the market in Internet products, making it very difficult to dispense with this product on the Internet.

3.3.4.2 Netscape Directory Server

Netscape Directory Server is needed in order to create an LDAP (Lightweight Directory Access Protocol) directory which can be used, for instance, for electronic messaging. On installation, the application is broken down into two separate servers, the Netscape Directory server itself and a HTTP server known as the administration server, which is used to install and configure other Netscape SuiteSpot servers.

3.3.4.3 Netscape Certificate Server

Netscape Certificate Server is used for transferring confidential and sensitive information over the Internet, relating, for instance, to electronic commerce applications. In order to ensure that the content of transactions cannot be tampered with or viewed, the data are encrypted. The certificates issued by the Netscape Certificate Server comply with standard x.509v3, and are used by SSL (Secure Sockets Layer), a secure implementation of the TCP/IP transport layer in the OSI model. The certificates contain information on the identity of the owner: name, organization, address, etc. They also contain the owner's public key, the period of validity and a serial number.

Anybody can circulate encrypted information on the Internet. Some countries have clear rules on the subject, as in the case of France, where encryption is forbidden. In the United States, encrypted products may not be exported. With the growth of electronic commerce, some information is of a highly sensitive nature. Other information, such as that emanating from government bodies, may be of such importance that encryption needs to be used.

Firewalls are not adequate to ensure the security of data circulating on the network, either being sent to the Web server or emanating from it. Data encryption (or encipherment) technology prevents pirates from reading or falsifying data. In the Web environment, the Secure HTTP protocol is used to make HTTP applications secure, while the SSL (Secure Sockets Layer) protocol uses encryption to make IP sessions secure. Figures 3.11 and 3.12 show the most commonly used encryption algorithms.

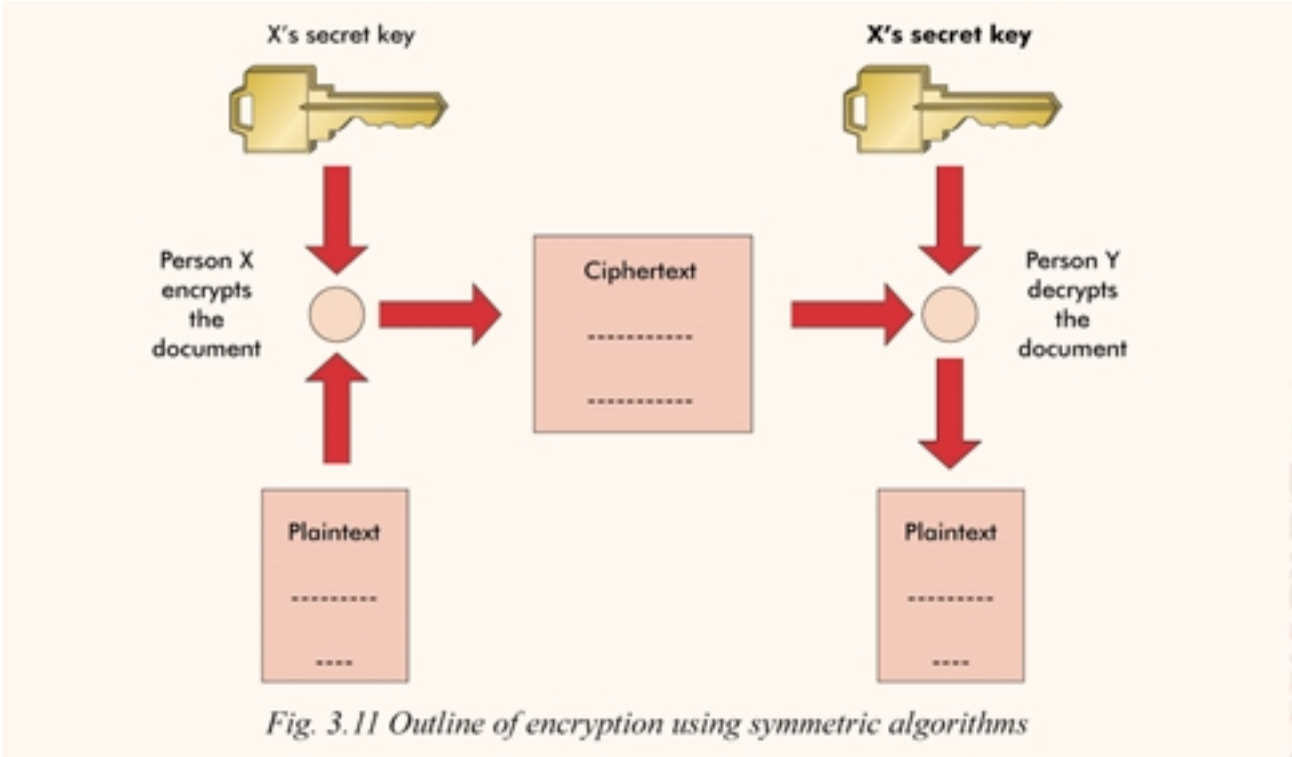

Fig. 3.11 Outline of encryption using symmetric algorithms

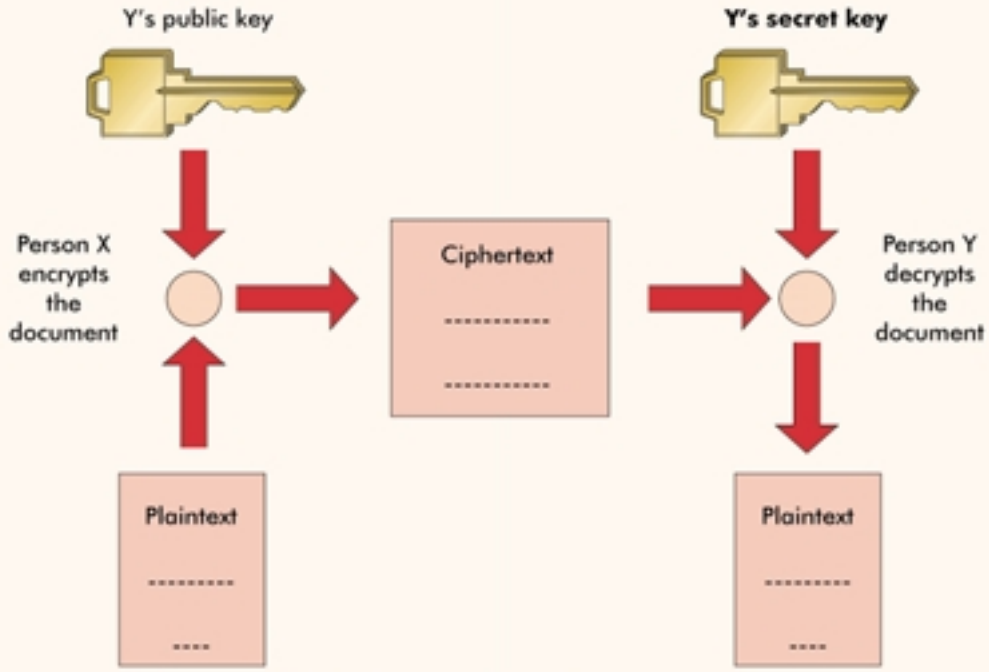

Fig. 3.12 Outline of encryption using asymmetric algorithms

Most encryption techniques use the Data Encryption Standard, an algorithm developed in 1975 by IBM. The basic principle centres around a secret key which is used by the sender to encode the message and by the recipient to decode it. The algorithms which operate on this principle are known as symmetric algorithms.

The problem with symmetric algorithms is that the secret key has to be transmitted to the recipient of the encoded message, and a secure means has to be found of doing this.

This problem was resolved with the emergence of asymmetric algorithms based on the use of two different keys, one of which is public and is used for encoding, while the other is secret and is used to decipher messages. Each user, therefore, has both a public key (which is known to all and can be looked up in a directory) and a secret key known only to himself. If a user wishes to encode a message, he uses the recipient's public key and sends the information. The other party receives the message and decodes it with his secret key. This concept is applied in Data Security Inc.'s RSA algorithm (an acronym formed from the names of its inventors: Ronald Rivest, Adi Shamir and Len Adleman: http://www.rsa.com/).

Although this system is simpler to use than software based on symmetric algorithms, it has one drawback, in that there is nothing to prevent a pirate from entering the directory of public codes and substituting his own public key for that of a genuine user. When someone wishes to encrypt a message using Y's public key, they then use what is actually the pirate's key, enabling the latter to intercept the message and decipher it with his own secret key. He might then modify it, encrypt it with Y's public key (which he will have appropriated beforehand) and send it to the real Y. Y will believe that the message received is genuine, whereas it has in fact just been tampered with.

Some very powerful authentication tools have therefore been developed. When someone wishes to send a message, he first launches what is called a hash program which, using his private key, will create a digital image of the information.

Once the message has been sent and received by the recipient, the latter can decipher the image using the sender's public key. If the message has been tampered with in the meantime, the two documents will not match. If the public key has been tampered with, it will not be able to decode the transmitted image.

3.3.4.4 Netscape Enterprise Server

On installation, Netscape Enterprise Server breaks down into three applications: the administration server, the HTTP server and the integrated search engine (or indexing engine). The most widely used version of the HTTP protocol is version 1.0. However, this version presents some problems which may confuse even the most experienced engineers. The confusion arises from use of the MIME standard, which is quite close to the HTTP standard, but in some ways quite different. Shutting down the connection after each document results in the congestion information being lost, while the opening of several connections simultaneously allows documents to be posted more quickly, but causes server congestion. Version 1.1 of the HTTP protocol will iron out these defects, which we have been unable to enumerate fully. It should deliver improved performance whilst remaining compatible with version 1.0.

3.3.4.5 Netscape Messaging Server

Netscape Messaging Server uses the same version of the administration server as Enterprise Server; there is thus no need to install the latter twice. The messaging server uses two directories to store files, namely /var/spool/mailbox for mail received by users and /var/spool/postoffice for outgoing mail and the configuration files. Mail addressed to the postmaster is retransmitted to a user responsible for managing it. Mail addressed to local users of the machine on which the server is located is usually kept under /var/mail. There is no need to specify a port number on installation, as it is impossible to change the default port (port 25) used for the SMTP protocol, since the messaging server is part of a set of servers which expect to find it at that port.

3.3.4.6 Netscape Collabra Server

The Internet is ideally suited to group work, and Netscape Collabra Server is the tool used to manage forums (news) and to facilitate the work of the moderator. The forums are based on NNTP (Network News Transfer Protocol), which is both a distributed protocol for information exchange between servers and the client-server protocol used for consulting articles. Collabra Server uses the same version of the administration server as Enterprise Server. The default port number for the NNTP protocol is 119. It can be changed, but to do so is risky, especially if the server is to be incorporated in a chain of servers.

3.3.4.7 Netscape Proxy Server

Netscape Proxy Server is a typical proxy server. It is based primarily on a firewall system which gives controlled access and protection from the outside. In a topology of this kind, the browsers must be configured to use the proxy server to manage their requests. As far as the target server is concerned, all the requests received come from the proxy server rather than from the original client (user).

As client requests are thus sent via the proxy server, it is logical to have the cache on the same server. This works very simply. A machine is configured to receive requests coming from within the national network and seeking information on the Web outside the domain. This machine examines whether the document has been requested previously. If the document in question is already on the cache, a mini-request is sent to the server where it should be located, asking whether it has been modified in the meantime. If it has been modified, the new version will be found and stored on the cache; otherwise the page already stored there is sent to the Web client. If the page is being requested for the first time, the request is sent outside in the conventional manner. However, the document when found is stored on the cache in case it is requested again.

A “parent-child” cascaded architecture can be constructed by recommending all Internet Services Providers and other institutions to adopt the same strategy. In this case, any requests which could not be met by one cache will be met by a neighbouring cache. This reduces the external traffic on each network and subnetwork considerably, and will result in substantial savings. It also improves service quality.

It is very important not to confuse the cache under discussion here with the option provided by browsers like Internet Explorer and Netscape of using a cache at local level on the machine. This cache is on disk, and, in the case of Netscape 4.xx, is configured as follows. Go to Edit and choose Preferences. Under Advanced, click on Proxy server, before choosing automatic or manual configuration. With Internet Explorer 4.xx, go to View, and choose Internet Options before clicking on Connection. Fill out the fields, click on the Advanced button and again fill out the fields as instructed by the local operator. Script files (cgi-bin) are not stored. Documents requested from a Web page by the FTP protocol are stored. Space in the cache is managed on the principle that the documents not accessed for longest are removed first.

Alternatives to Netscape Proxy Server exist, such as Squid. For further details consult the Squid home page at the following address: http://www.nlanr.net/Squid/. The commercial version of the Harvest cache can also be used. Figure 3.13 shows how a proxy server works.

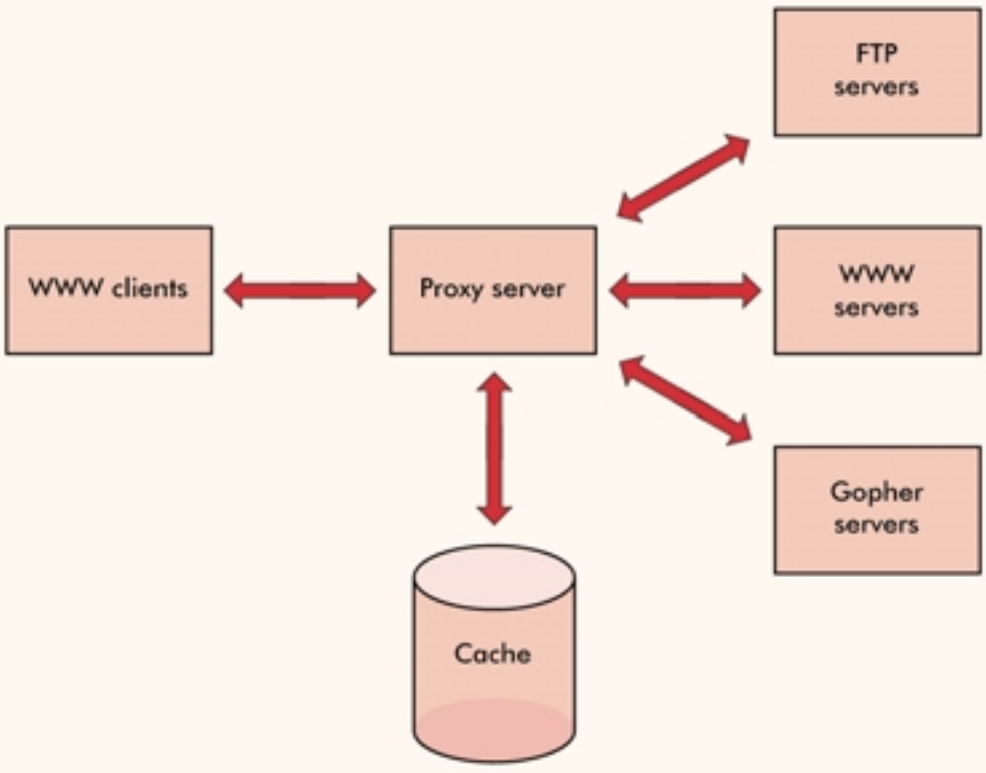

Fig. 3.13 Outline of a proxy server

4 Internet services engineering and maintenance

4.1 General remarks

The growth of electronic commerce, telemedicine, distance learning and real-time applications on the Internet (the electronic stock exchange and electronic auctions) provides Africa with an opportunity to further its overall development by harnessing all the energy and human resources required to develop the Internet, the major invention of the century.

Internet development will not be possible in Africa if quality of service (QoS) requirements are not taken into account at every stage of the project. To this end, the managing bodies must put their full weight behind the quest for total quality.

Internet services engineering generally entails measuring and analysing traffic and monitoring congestion on the operator's network. Traffic on the Internet is set to be the crucial issue of the twenty-first century, one which concerns everybody. It is important, therefore, to manage it properly, as the economic stakes are very high indeed, bearing in mind that, in 1998, the tariff for incoming traffic was around US$ 100/Gbyte (*source: SWITCH-Internet*). Internet services engineering will make it possible to draw up plans, detect problems and establish different levels of service quality on the Internet and, accordingly, to make different charges for services depending on the level of quality required.

4.2 Network management and quality of service on the Internet

4.2.1 General remarks

Technical management of the Internet network is based in essence on the Simple Network Management Protocol (SNMP), management by the World Wide Web, and on know-how in relation to leading-edge technologies.

Managing the network equipment is essentially the task of a handful of computers located at the national Internet node which pilot a number of hubs, routers, bridges and other switches as well as access via switched-line modems.

4.2.2 Main management tools

There are a number of management platforms such as HP's OpenView. OPTIVITY from Bay Networks can be used to manage that constructor's hubs and switches, as well as the Cisco routers which dominate the Internet market. Other UNIX management platforms such as Sun's SunNet Manager, ISM (Integrated System Management) from Bull and IBM's SystemView also manage network equipment. Hewlett Packard's INTERCONNECT MANAGER manages HP hubs, while WEBMANAGE from Tribelink manages 28.8 k modems (PPP).

Within each SNMP agent is an information base (MIB – Management Information Base) on the wiring of the sites and equipment connected to the national Internet node.

RMON (Remote Monitoring) gives access to the measurements of a probe which compiles statistics on packets. The management station can ask to view the results. Some hub management processors act as a RMON probe.

4.2.3 Other system-integrated management tools

Fault detection can only be effective if the information collated is clear, categorized and accessible to authorized persons. Some diagnostic tools are incorporated in the UNIX system, while others are free and available on the Internet (see RFC 1147). The main tools are the following:

ifconfig: Detection of wrong IP addresses, subnet masks and broadcast addresses. This tool is part of the UNIX system.

arp: Detects systems connected to the local network which are configured with incorrect IP addresses. Provides information on the conversion of Ethernet/IP addresses. Arp is an integral part of UNIX.

netstat: Posts detailed statistics at each network interface. Supplies a variety of information.

ping: Allows packets to be sent repeatedly to a network node using the ICMP protocol. This sends back an echo packet and indicates whether the system can reach a remote host. Ping also posts statistics relating to packet loss and length of transmission.

nslookup: Supplies information relating to the DNS names service. Performs the same task as dig.

traceroute: Indicates by which path packets have been sent between two remote systems using ICMP. It is thus possible to measure the success rate of TRACEROUTE exchanges, as it traces the path taken by the packet and gives the transit time for each node on the route.

etherfind: This tool analyses the different packets transmitted between the hosts on a network. Etherfind is a TCP/IP protocol analyser which examines packets up to their headers.

4.2.4 Main management indicators

A network administrator must keep a record of the network history, as by understanding the past, he may be able to predict the future to some extent. Constructing a baseline profile of the network entails measuring and recording the operational state of the network over a given period. The results can later be used as a basis for comparison. In this way, the network administrator can define “normal” network operating conditions on the basis of the inventory of the network, and draw up, for instance, a profile of a typical week, pinpointing “critical periods”, “heavy use periods”, “errors”, etc. He will determine what is acceptable and what not, in the light of the national context.

A properly defined traffic load profile should make it possible subsequently to identify significant changes in the behaviour of the network on the basis of the daily analysis of results, and also to predict behaviour with a given level of traffic, or anticipate problems created by the introduction of new services.

The most relevant indicators for managing and analysing traffic on a network are the following:

- *network use:* traffic load (incoming and outgoing), peak periods, etc.;
- *network nodes:* the ten busiest machines. Experience has shown that a mere 10% of the nodes on a network generate 90% of the traffic. Once identified, these machines should be studied more closely (what applications do they use, how many users, etc.);
- *maximum bandwidth or bit rate:* maximum rate of transfer which can be achieved between two terminal points;
- *applications and services:* identifying the five or six services which use virtually all the available bandwidth (Web, news, backups, etc.);
- *error statistics:* statistics on collisions and packet loss;
- *transit time per packet:* between two remote points is the main criterion of QoS. The delay is the time which elapses between transmission of a packet by the sender and its receipt by the destination station. It takes account of the propagation time along the route and the time spent by packets queuing in intermediate systems;

- *jitter:* variation in the end-to-end delay;
- *availability:* average rate of errors on a link.

For further details relating to Internet service quality we would recommend the following documents: "Quality of Service: delivering QoS on the Internet and in Corporate Networks" by Paul Ferguson and Geoff Huston, Wiley Computer Publishing, 1998, and "Quality of Service: Fact, Fiction or Compromise?" by Paul Ferguson and Geoff Huston, INET 98, July 1998.

4.2.5 Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) defines the dialogue between a control station and a node on the network. It gives information on the state of a device on the network (hub, switch, router, etc.) and allows unusual events to be managed. It is also used for remote measurement of traffic and errors, and *facilitates the configuration of remote devices*. The management station may be a PC, a Mac or a UNIX station.

Hewlett Packard's HP OpenView software is based on requests using the SNMP protocol for managing the nodes on a network. It uses graphics, and users can choose between drawing their own network plan with only the icons of the devices they deem most important, or using the Auto-discovery option, which interrogates all the subnetworks in a LAN and draws a map of the SNMP-capable objects.

HP OpenView uses icons to represent the different active components of a network which reply to SNMP requests. OpenView consists of a series of maps and submaps arranged in a hierarchy right down to the user's workstation. It comprises a platform which manages the standard part of SNMP and is installed under UNIX, Windows 95 or Windows NT. Specific nodes (routers, switches, hubs, etc.) and their particular operating features, as well as the graphic images, are represented using the extended Management Information Base (MIB) part. MIB is the database on the wiring of sites and equipment connected to the network.

Two products, HP's INTERCONNECT MANAGER and Bay Networks' OPTIVITY, use the HP OpenView platform to manage their specific products.

The OPTIVITY network management software is a management program for Bay Networks equipment, constructed on an HP OpenView SNMP platform. In addition to managing unusual events, it can be used for measuring traffic and network errors. One of the advantages of this product is its use of graphs which measure the traffic going through an entire hub or a particular port. Error measurements can also be carried out in order to identify the node which is the source of the problem. A further worthwhile feature is the ability to manipulate a device in remote mode. A Telnet connection can be created to configure a bridge, terminal server or router by choosing the icon of the device in question. Any ICMP-capable network node can be pinged. It is also possible to cut off a hub port from the management station in order to isolate a node.

The Set Threshold function can be used to define traffic or error thresholds which, if reached, will trigger a message to the management station. If wished, an automatic function can be activated by the hub processor, such as partition of a port which has exceeded the level of errors set.

By installing the Carbon Copy program on the OPTIVITY station, and a modem on a telephone line, it is possible to control the management station in remote mode from a portable computer connected to another modem. The tendency in network management is to use Web-based management software.

4.3 Measuring and analysing Internet traffic

4.3.1 General remarks

Generally speaking, and essentially for financial reasons, Internet services cannot be operated profitably without reliable traffic measurement and analysis. Metrology is a growing force on the Internet and there are a number of products on the market, some in the public domain, designed to measure and analyse traffic.

The NNSTAT software installed on a UNIX station, for instance, measures incoming (paying) and outgoing traffic on the network. It works by seizing the *IP source and destination address* pairs, thus making it possible to quantify the Internet traffic of all partners connected to the national Internet node (e.g. incoming traffic to a certain hospital, to university and government bodies, etc.).

This software is in the public domain and can be downloaded by FTP from the site:
ftp://gatekeeper.dec.com/pub/DEC/net/NNstat_3.3beta.tar.Z.

The OPTIVITY software from Bay Networks uses the HP OpenView platform to manage Bay Networks products, but also to measure network traffic and errors. Other software packages such as IP Trafic (http://www.urec.cnrs.fr/IPtrafic/), NetraMet (Network traffic Meter) or MRTG (The Multi Router Traffic Grapher) (http://www.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg.html) can also be used.

4.3.2 How it works

Router manufacturers make systems such as Cisco's Netflow available to their customers. Traffic information is collated using flow tables drawn up by the main router connecting the national network to external sites. Use of this technique ensures the accuracy of traffic measurement in relation to the source address/destination address pairs by type and IP port. As only the IP address is known, this has to be matched to the corresponding name of the institution before the tables can be drawn up.

The information is first gathered in a continuous and formatted manner in a file which contains everything needed for compiling detailed statistics. It is then fed into a database, and processed, to produce images which can be accessed instantly when needed.

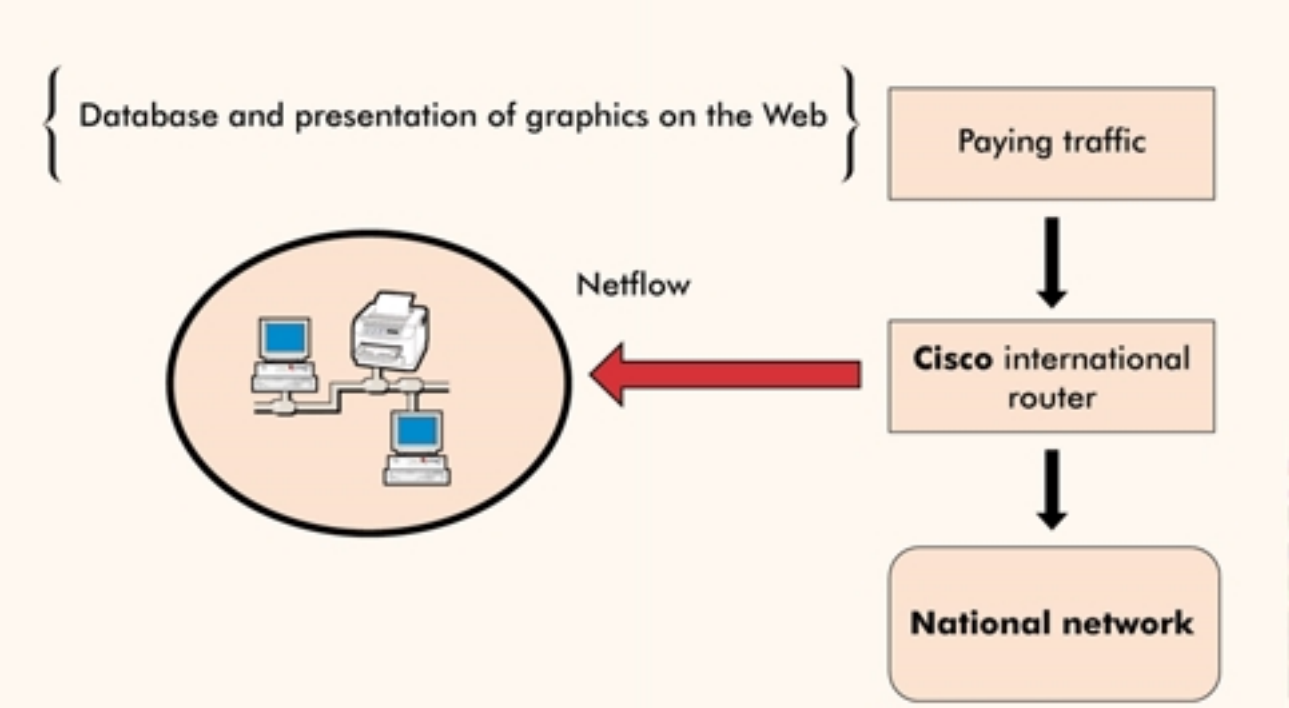

Fig. 4.1 Traffic measurement and analysis

Figure 4.2 shows the typical make-up of traffic in a major institution (*source: SWITCH Internet*).

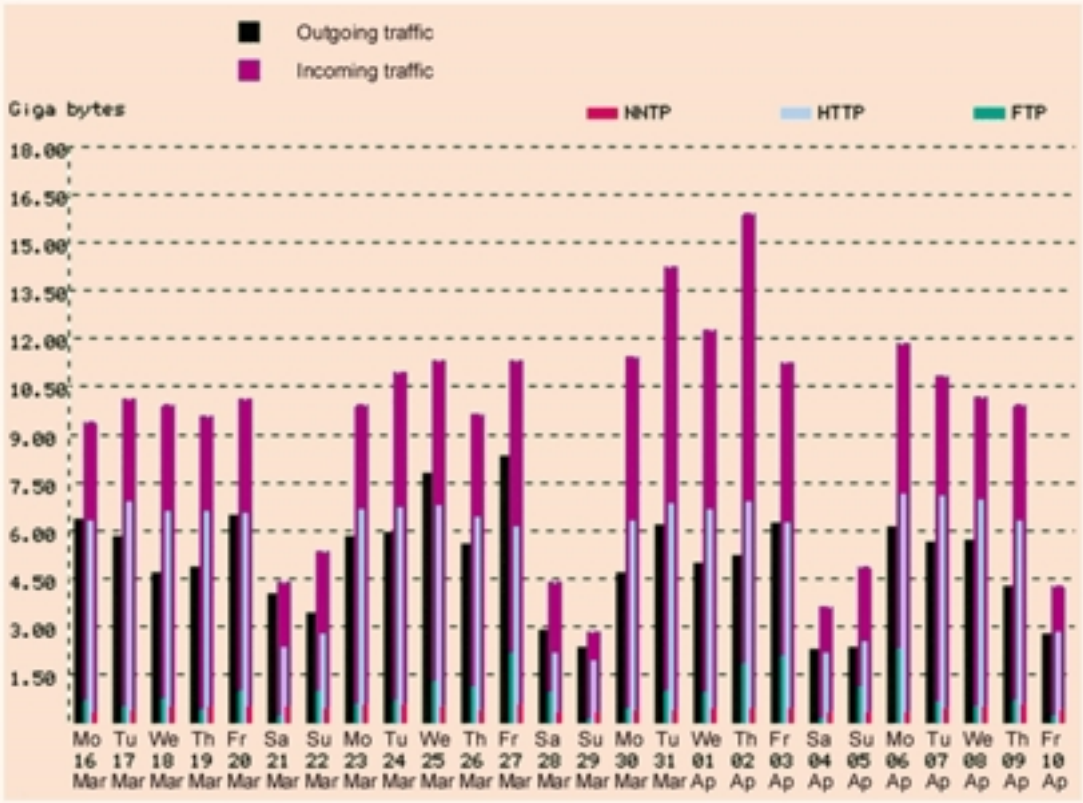

Fig. 4.2 Analysis of the make-up of Internet traffic

4.4 System security

4.4.1 General remarks

In most cases, the risks in terms of network management and information processing fall into one of three categories, namely unauthorized access, leaking of information and service failure owing to malfunctioning of the system. It is therefore vital to assess the risks and analyse the level of confidentiality of the information being processed and to be transmitted on the Internet. Breaches of the system are extremely serious as they undermine confidence and security. Government agencies, universities and banks are the most popular targets for hackers.

4.4.2 Network audits and security

The main suppliers of audit software are Cisco, Bull, Checkpoint, Digital, ISS, Matranet, Security Dynamics and Solsoft. There are some free packages, such as:

- COPS, for performing a security audit on a UNIX system. To install COPS version 1.04, see the Internet address http://www.urec.cnrs.fr/securite/outils/cops/cops-1.04.tar.Z.

- CRACK, which is used to identify the degree of security of passwords on a UNIX system. This software is available on the Internet.

- SATAN, which is used to detect the most common security problems linked to the services offered on a UNIX network. To install this software, visit the Internet site: http://www.urec.cnrs.fr/securite/outils/satan/satan-1.1.1.tar.Z.

- TCP_WRAPPERS, which can be used to limit and record access to the services offered on a UNIX network.

- TRIPWIRE, used on a UNIX system to check whether files have been altered, damaged or tampered with. To install this software, see http://www.urec.cnrs.fr/securite/outils/tripwire/tripwire-1.2.tar.Z.

4.4.3 Anti-virus measures

Computer viruses pose a very real threat to businesses, whose vital data may be irretrievably lost. There are several types of virus, and it is not the aim of this guide to identify them all. For information purposes, however, there are boot viruses, file viruses, worms, Trojan horses, logical bombs and macro viruses. They should be combated by installing anti-virus software on servers and on client stations. The most well-known are the NLM modules, specific to Netware servers. However, other products are also available for Windows NT and UNIX servers.

4.4.4 Backups

The increasing reliability of hardware, and in particular hard disks, is not a valid reason for failing to provide backup, as user error (deletion, formatting errors) can still occur. User data losses are completely irreversible and make it essential to have a number of absolutely fail-safe backup mechanisms. Backups can save several days' work per machine, and quality of service depends on them. A distinction must always be made between system backups and applications which back up user data.

4.4.5 Inverters

The quality of the 220V alternating current power supply to the public cannot be guaranteed owing to resistors, motors and connected devices which use energy in an unpredictable manner.

For computer systems, it is vital to use inverters or contingency supplies, referred to as UPS (Uninterruptible Power Supply). For large networks, some inverters may be equipped with an Ethernet or Token Ring interface including an SNMP agent. All operations are then conducted from a management station, irrespective of its geographical location, in exactly the same way as for hubs, routers, etc. As in the case of routers, a standard MIB for inverters has been agreed by the main manufacturers. For reasons of compatibility, it is important to ensure that the software provided with the SNMP interface can operate on the platform for managing the rest of the network equipment, e.g. Hewlett Packard's OpenView or IBM's NetView.

5 Strategies and development of the Internet network

5.1 General remarks

The telecommunication sector is witnessing nothing short of a revolution. With the Internet, operators are adapting their strategies to the new situation. The major network constructors will redefine the very essence of the information sector, with data and telephone networks set to converge via the Internet. Work is under way to optimize IP networks which can support voice, video and data applications, thus simplifying network functioning and reducing costs, while at the same time offering a competitive advantage in terms of

size. African decision-makers in the telecommunication sector must cope nowadays with a steady increase in traffic on their networks. The emergence of Intranet and new applications, or in some cases simply the increase in the number of subscribers, mean that they must devise new solutions to meet user expectations. Fortunately, manufacturers have anticipated these changes and are coming up with products appropriate to every situation.

Telecommunication operators in Africa are endeavouring to meet the challenge, and Internet development projects are becoming increasingly important, subject to the constraints operating in each country. In this chapter, we will examine the different technologies to be incorporated into a strategic plan to develop the Internet network in Africa.

5.2 Unified networks and IP telephony

5.2.1 General remarks

Thanks to new technologies, international calls can be made from an individual computer to any telephone in the world. From the comfort of a computer desk, it is possible to call someone on the other side of the world, and be charged only a very low telephone rate. This fact must not be overlooked in planning the development of the Internet in the different countries.

5.2.2 How it works

Internet telephony providers allow customers equipped with a PC with sound card to make calls from their computer and to communicate via the Internet with telephone switchboards. The switchboard then relays the call to its final destination instantly and automatically, to any telephone. The communication between the two parties therefore takes place in real time, uninterrupted and in full duplex.

5.2.3 IP switching and unified networks

The routing switch or layer 3 switch is the latest technological innovation and offers all the functions of a router combined with those of a switch. The technique is also known as IP switching. Its ease of integration into existing networks makes it the ideal candidate to take over from routers, but also a vital element in the deployment of backbones based on Ethernet technology. It will be one of the key players in the networks of the future, the so-called unified networks.

Unified networks combine switching, routing, optics, wire, wireless and IP transmission in a comprehensive package of products which interwork and offer a degree of predictability, control and security hitherto found only on some private dedicated networks.

By combining voice, video and data in a single unified network, telecommunication operators in Africa, Internet service providers and businesses will be able to offer customers multimedia applications and a high level of service throughout the world, while at the same time making substantial savings in overall network costs and improving their competitive position.

5.3 TM and backbone development

5.3.1 General remarks

Recent technological breakthroughs in the computer, audiovisual and telecommunication spheres mean that considerable volumes of information can now be transported and processed. Economic structures, production and organization methods, access to knowledge, leisure and working methods will all undergo profound change. The economic and social implications will certainly be worldwide, and the strategies of African

telecommunication operators will need to take account of the new situation. Modern telecommunication infrastructures and their applications, as well as the social aspects, intellectual property rights, the media society and security of information: these are all challenges which need to be met by means of a common inter-governmental approach.

The construction of the African information society depends on setting up information highways. High-speed networks, the main link in the information chain, are coming to occupy a central role thanks to two major technological breakthroughs: optical transmission and ATM (Asynchronous Transfer Mode).

5.3.2 Asynchronous Transfer Mode (ATM) backbone

ATM (Asynchronous Transfer Mode) was adopted by the main telecommunication standardization body, ITU, in the late 1980s. ATM is a direct descendant of Frame Relay, but differs from it in employing small, equal-sized packets (known as ATM cells) with speeds ranging from 1.544 Megabits to 1.2 Gigabits per second. The cells comprise 48 octets of information.

The task of routing the cells is hardware-based, in contrast to most IP routers and X25 or Frame Relay switches. With ATM also, the term "switch" tends to be used rather than cell router.

The advantage of ATM compared to earlier technologies is the ability to guarantee capacity and service quality for each connection. Thus, it is possible to create a connection between two ATM systems and specify, for instance, a guaranteed speed of 3 Mbit/s, a maximum time of 100 minutes, a time variation of less than five minutes and a certain maximum rate of cell loss. Guarantees of this kind are necessary if ATM is to be used for transporting digital circuits (2 Mbit/s, 34 Mbit/s) which are the basis for essential services of telecommunication operators. They are also useful for creating multimedia connections, e.g. for transporting audio or video streams.

In addition, ATM allows the transfer rate on the networks to be determined on a dynamic basis by the effective rate of the information source. This means that better use can be made of transmission capacity, thereby reducing the cost of transporting information.

ATM will make it possible to search for, sort, distribute and transmit information rapidly and easily at affordable cost. This opens up new horizons for development in the fields of research, health, education, financial and administrative services and industry.

ATM must be introduced in successive stages in order to meet the needs of the national and regional market gradually and in line with technological innovation and production costs.

ATM satellite links can also be implemented. This involves installing an ATM switch in one town or city, with network multiplexers in other towns or even in neighbouring countries. By this means, the Internet operator will be able to connect up ISPs and major customers to the various available multiplexers. This ATM backbone can provide connections at speeds of 34 Mbit/s or even 155 Mbit/s over Ethernet.

This strategy would be suitable for developing regional projects designed to fit into a large-scale project such as Oxygen, Africa One and others.

5.3.3 Means of connection to the ATM backbone

In order to connect up partners (other Internet operators), ISPs or major customers on ATM, operators can use 34 Mbit/s SMDS (Switched Multimegabit Data Service) access with a connection server. A DSU (Data Service Unit – e.g. from Digital Link) must be installed on each site. A HSSI (High-Speed Serial Interface) can be used to connect to a Cisco 7000 router. The router will be connected to the client's FDDI backbone, thus providing ATM access. It is also possible to connect up machines used by Internet operators directly on FDDI subnetworks, in order to take full advantage of the available bandwidth.

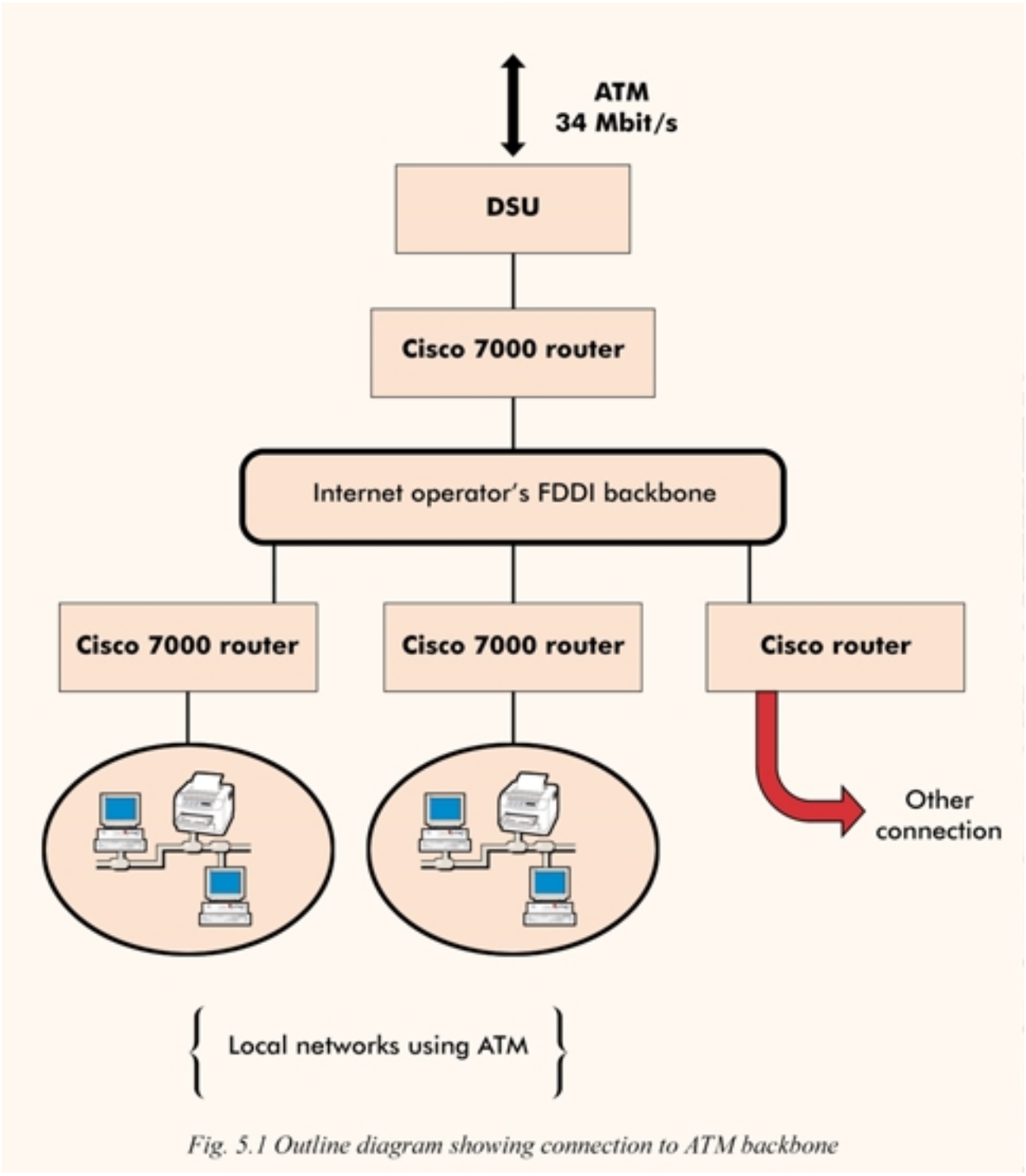

Fig. 5.1 Outline diagram showing connection to ATM backbone

5.3.4 IP communications over ATM

Implementing ATM requires the network protocols (such as IP) to be ported, without which a computer connected by ATM would be able to communicate only with other ATM computers. As we know, IP enables networks like Ethernet and Token Ring to be interconnected. It is therefore relatively simple to add ATM to the list, and the IETF (Internet Engineering Task Force) did just that in a series of RFCs (Requests for Comments, the name given to official IETF documents).

The classic solution is a model which operates as follows (see Figure 5.2). The computers have *IP addresses (A1, A2)* and *ATM addresses (a1, a2)*. At startup, Computer 1 creates an ATM connection with the *address server*. The server may be located in a router or in a computer connected to the same ATM network, and its ATM address is therefore well known. The address server therefore knows that the IP address A1 is accessible via the ATM address a1. Computer 1 wishes to send data to Computer 2 using the IP protocol. Computer 1 therefore knows Computer 2's IP address. It must now find out its ATM address, which it obtains by sending a request to the address server, using the ATM connection already created (1).

Computer 1 can now establish a connection to Computer 2, if this has not already been done, and use it to send data (2). The role of the address server is to compensate for the lack of a broadcast facility on the ATM network. We will recall that, on an Ethernet, Token Ring or FDDI network, address resolution is achieved by broadcasting the request to the whole network, which is a simple task on shared-medium networks.

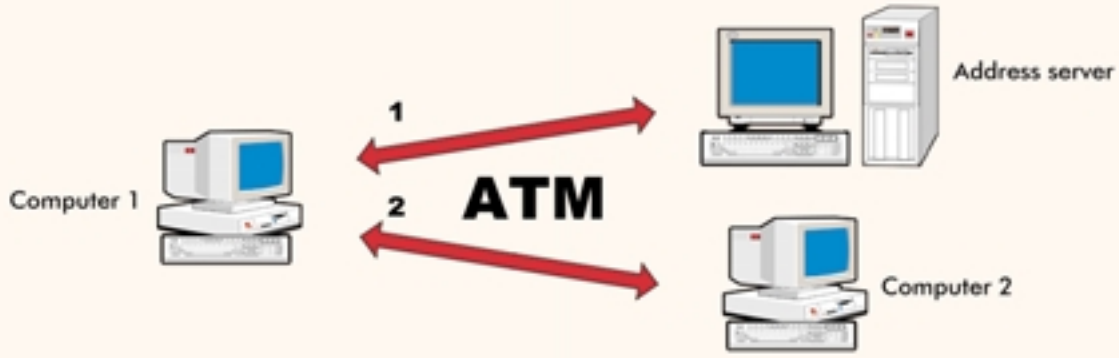

Fig. 5.2 Sketch showing IP communication over ATM

The scenario depicted in Figure 5.2 applies only if Computers 1 and 2 are defined as belonging to the same logical network. If this is not the case, a router is essential in order for the two computers to communicate.

The classic model therefore uses ATM like an Ethernet (hence its name), and does not generally enable ATM to be used end-to-end. A solution to this problem, known as Next Hop Resolution Protocol (NHRP) is in the pipeline, and should enable systems belonging to different logical networks to establish direct ATM connections with each other.

5.3.5 ATM end-to-end or RSVP?

It is possible to transport video streams on the Internet, but the quality is variable and unpredictable, and inadequate for most user requirements.

One of the important assets of ATM is resource reservation, which is made possible because ATM is connection-oriented. Guaranteed resources are needed in order to transport streams such as video or audio to commercial standards. In order to guarantee resources, one solution is to use ATM end-to-end for specific problems since ATM, unlike IP, is not an interconnection technology.

In order to meet the need for an IP with reservation in order to transport multimedia on the Internet, the IETF has come up with RSVP (Resource reSerVation Protocol). Unlike ATM, RSVP is a protocol designed to accompany IP, and computers do not therefore need a new communication interface card. However, for RSVP to function correctly, the routers need to be modified to enable them to perform all the tasks linked to reservation, for which the devices currently available were not designed.

ATM is the first-choice technology for public networks which charge for bandwidth (partly because it is connection-oriented). However, end-to-end communication requires a protocol such as RSVP, independent of the communication interface card. ATM will nonetheless come to be used on local networks, either

directly, or as a means of interconnecting switches (switched Ethernet, switched Token Ring), and the public networks will offer broadband services on an ATM base. However, RSVP may well be necessary in all cases involving heterogeneity. In particular, we will see RSVP installed even on ATM, to enable ATM systems to reserve resources in communications with non-ATM systems. For further details, see FI-9/1995.

5.4 Development of optical fibre networks

5.4.1 General remarks

When the national (or even regional) network has an ATM backbone with Points of Presence (PoPs), the different sites can be connected to it by optical fibre, which can be laid on high-voltage lines, with speeds of 34 Mbit/s or even 155 Mbit/s. At higher speeds, a synchronous multiplexing technology known as SDH (Synchronous Digital Hierarchy) can be used for multipoint transport over optical fibre of channels ranging from 155 Mbit/s to 10 Gbit/s. For further details, see ITU (International Telecommunication Union) Recommendations G.780 and G.783 to G.785.

5.4.2 Principle of converting electrical signals into optical signals

The Ethernet optical transceiver is designed to convert electrical impulses into optical signals transported in the core of the optical fibre. Inside a pair of transceivers, electrical signals are translated into optical impulses by a light emitting diode (LED), and read by a phototransistor or photodiode. One optical fibre is used for each direction of transmission. Three types of transmitter are used: LEDs which operate in the visible red part of the spectrum (850 nM), infra-red diodes, which transmit in the invisible part at 1 300 nM, and lasers, used with single mode fibre, on wavelengths of 1 300 nM or 1 550 nM.

5.4.3 Types of optical fibre

Three types of optical fibre are used. The first of these is 200/380 step-index fibre, made up of a core and optical cladding made of glass with different refractive indices. Owing to the large bore of the core, this kind of fibre causes significant dispersion of the signal, leading to distortion of the signal being received. Graded-index fibre has a core made up of successive layers of glass with refractive indices close to each other. As a result, delays are equalized, and nodal dispersion reduced. Bandwidth is typically 200-1500 MHz per km. Single mode fibre has such a fine core that the propagation path is virtually direct, and nodal dispersion negligible. The bandwidth is in excess of 10 GHz/km. This type of fibre is used mainly for outlying sites.

5.4.4 Links and transmission quality using optical fibre

Optical fibre is used mainly to strengthen the backbone and on networks which require a high level of security. It provides a very high degree of protection against eavesdropping and active attacks such as injection of a foreign signal designed to cause interference and deceive network users with regard to terminals and transmissions. As optical fibre does not radiate at all, a branch can only be created by cutting the fibre with a diamond saw, which cannot be done by just anyone.

Modems connected to optical fibres are equipped with detectors to pick up disappearance or attenuation of the signal due to pirating. Over long distances, a laser repeater regenerates the signal approximately every 40 km, and an optoelectronic module revitalizes weakened light signals. To improve speeds, it is advisable to replace these repeaters with 100% optical amplifiers which increase speeds by a factor of 100.

After installing an optical fibre link, losses resulting from the fibre itself and from the connections made need to be measured. A power meter made up of a calibrated light transmitter and receiver measures overall loss on the line in [dB]. Losses are measured on the wavelength used (850 nM or 1 300 nM).

A reflectometer is a device which sends an optical impulse through the fibre. The signal reflected in the glass can be viewed on a screen, thus allowing accurate measurement of the length of the link and the losses incurred with each connection. This piece of equipment is also very useful for locating any cuts to the fibre and identifying the connection which is causing excessive optical loss. A power meter measures only overall loss on the link, whereas a reflectometer pinpoints the defective connection.

5.5 Connections using laser links for Internet sites

5.5.1 General remarks

When it is not possible to create a link using optical fibre or a dedicated telephone line, a laser link can be installed, provided that the two sites being linked are no more than one kilometre apart, and there is no obstacle to the beam. Lasers are available which act like a pair of 10 Mbit/s repeaters, and even 155 Mbit/s lasers exist for ATM.

5.5.2 Characteristics of laser links

Alignment of the beams is tricky and requires considerable know-how. The undeniable advantage of these links is the mobility of systems, and their attractive cost. If a site moves, the pair of lasers can be recovered, in contrast to fibre cables which are laid under roads and bridges, for instance. Experience in Europe has shown that laser does not tolerate fog or heavy snowfall. The lasers must also be located where they cannot be tampered with, and out of the way of obstacles. Laser links are useful in difficult cases where a link is needed between buildings of the same organization which are scattered. Laser is reliable, but less secure than copper wire or fibre.

5.6 Leading-edge technologies and Internet access

5.6.1 General remarks

At present, the overall state of telecommunication networks in Africa, with copper wire telephone infrastructures dating from the 1970s, is not suitable for Internet development. Very high investment costs, a shortage of qualified staff and scattered settlements are the main factors liable to hamper the development of the Internet network. Fortunately, there is scope for introducing leading-edge technologies onto existing networks and using alternative technologies, as a basis for implementing the Global Information Infrastructure (GII) in Africa.

5.6.2 ADSL

5.6.2.1 General remarks

ADSL (Asymmetric Digital Subscriber Line) is the latest data transmission technology, with performances which rank somewhere between ISDN (Integrated Services Digital Network) and high-speed cable links. The technologies underpinning this are known collectively as xDSL, and are all derived from the DSL technology used in ISDN links (the same type of coding is used). The term xDSL encompasses four groups: ADSL, HDSL, SDSL and VDSL, each of which has its own particular uses and characteristics.

At present, ADSL is the most developed and market-ready technology. Experiments under way in France, Canada, the US and elsewhere show that information can already be transmitted at a speed of 8 Mbit/s over a distance of 3 km using the ADSL system. This technology offers an alternative to investment in expensive wired equipment, using the copper wire resources which have been in place since the 1970s without being fully exploited.

In reality, copper wire resources are not being fully used because the telephone network was designed primarily to carry voice. The bandwidth used by classic communication equipments is limited to 3.3 kHz, whereas the physical characteristics of the subscriber lines actually permit transmission of signals at frequencies of about 1 MHz. By modifying the telephone exchange and user equipment, it has therefore

proved possible to optimize use of the lines. Depending how far the subscriber is from the telephone exchange, the copper pairs can support speeds of 1.5 Mbit/s (5.5 km), 2 Mbit/s (4.9 km), 6.3 Mbit/s (915 m) and 51.8 Mbit/s (305 m). For further details, see the current ADSL standard (T1.413).

5.6.2.2 How ADSL works

The wires connecting telephone exchanges to users all have a bandwidth of about 1 MHz. Telephone communications use only about 4 kHz, leaving some 996 kHz of unused bandwidth. ADSL modems are designed to use the full available bandwidth while allowing the telephone to be used normally.

With this technique, the bandwidth is divided into three parts: the upper end of the band (1 MHz) is reserved for the high-speed (8 Mbit/s) downstream channel (exchange-subscriber). In the middle of the band (between 300 and 700 kHz) is a medium-speed bidirectional channel used for transmitting data. The third channel is reserved either for conventional analogue telephony (between 0 and 4 kHz) or for ISDN (between 0 and 80 kHz). This channel will still continue to operate if the modem fails. This "multichannel" approach also allows users to access the WWW or any other server whilst telephoning or sending a fax, for instance.

Furthermore, most ADSL modems use an Ethernet connector, which means they can be shared on the network. This asymmetry, which reserves more bandwidth for the "exchange to subscriber" stream than for the "subscriber to exchange", is very suitable for consulting multimedia documents such as direct video or sound. This technology can be used to transform the Internet into a televised channel.

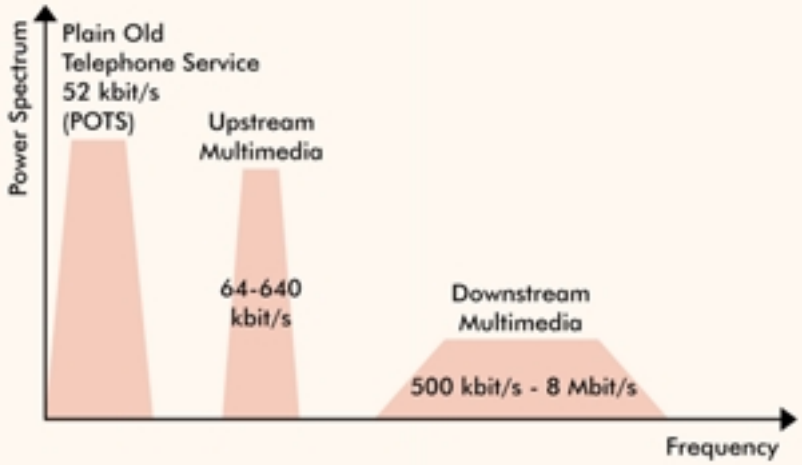

Fig. 5.3 The three ADSL communication channels

5.6.2.3 The ADSL modem

One of the advantages of ADSL is that it does not require users of the technology to make any costly and troublesome adjustments. Figure 5.4 shows some examples of modems, including one from Motorola. Other manufacturers include Alcatel-Bell, Orckit, Amati, Ericsson, Hayes and 3COM. There must be a modem at each end of the line.

The main problems standing in the way of rapid development of this technology are the price of the modems and system performance, which depends on the nature and state of repair of the copper line. This is not made up of a single continuous wire, but of several interconnected sections. In passing from one of these to the next, the signal may deteriorate and slow down transmission. In addition, two telephone lines placed too near to each other have a tendency to make spurious noise.



Fig. 5.4 Some ADSL modems

5.6.2.4 The access adapter

The access adapter is a stand containing the ADSL line termination cards, the POTS connectors and the backbone interface.



Fig. 5.5 ADSL access stand

5.6.2.5 The POTS connector

The POTS connector is based on a number of specialized filters (passband filters) which separate the baseband analogue telephone signal from the modulated digital signal. Either a passive or an active connector can be used, depending on the impedance characteristics of the local loop, and the specific requirements of the country concerned.

If an active connector is used, the modem is equipped with a relay to ensure that the connector short-circuits if the local supply is interrupted. This ensures that the basic telephone service is available in all circumstances. The POTS connector can either be separate or can be incorporated into the modem and the access adapter.

5.6.3 Internet by satellite

5.6.3.1 General remarks

Several firms, such as Netsat, Matra Grolier Network and the Pandemonium Group, offer satellite links to access providers and businesses.

An Internet telecommunication operator or group of operators in Africa may have a 34 Mbit/s space segment above the North Atlantic and a reciprocal agreement with, for instance, MCI (United States) on its 155 Mbit/s optical loop. It might install two or more transmitting/receiving stations in the designated countries and locations, connecting access providers to the Internet.

INTELSAT and BT, COMSAT, EMBRATEL and France Télécom, as well as other operators, are to distribute the Internet for the provision of multipoint broadcast satellite services. Under this system, the most frequently consulted Internet content is cached in a data storage unit for multicasting to Internet service providers worldwide, which in turn cache it for national and local use. The Internet operator has a choice between "push" or "pull" technology (*source: INTELSAT*).

5.6.3.2 Internet via VSAT satellite networks

VSAT (Very Small Aperture Terminal), a small-diameter parabolic antenna, can be used to install a telecommunication network using Internet-capable satellites, without passing through the local loop. The antennae communicate with the hub (connection to the LAN or local network) via a satellite. This technology makes it possible to establish interactive communication links. However, it is viable only for large organizations with a minimum of 50 scattered sites (*source: Salgues, 1997*), and might therefore suit an operator wishing to provide Internet services over a large area. The drawback is the relatively long average propagation time, which causes problems for telephony (echo) and data transmission (slowing-down at protocol level).

5.6.4 Wireless local loop

5.6.4.1 General remarks

Dedicated lines are often expensive. Telecommunication operators wishing to develop the Internet will find a competitive alternative in wireless local loop technology. These radio links operate at very high frequencies, and speeds up to 2 Mbit/s can be achieved, subject to a number of technical conditions. One major drawback is the susceptibility of this technology to interference, particularly during thunderstorms, when the link may be interrupted.

5.6.4.2 How it works

To use this kind of technology, the users of the dedicated lines, usually ISPs, universities, schools, hospitals, businesses and government offices, must be within seven kilometres of the operator's access point, and have a direct view of the pylon from their roof. Installation at the client's premises is quite straightforward, consisting in installing an antenna on the roof and connecting it to the transmitting and routing apparatus for the network.

At the operator's end, the apparatus is more complex. A mast is installed on the roof, with a guy about 18 metres high, and around fifty antennae are placed on it. The mast is connected to the dedicated line by means of two secure 100 Mbit/s links, which in turn are connected to a bay of radio transceivers culminating in a router specifically developed for managing radio connections.

Investment costs may be as high as US$ 250 000. For the client, the cost will depend on the size of the beam (bandwidth) and the volume of information transferred each month. Three beam sizes tend to be offered: 512 kbit/s, 1 Mbit/s and 2 Mbit/s. By way of example, a 2 Mbit/s beam with a monthly traffic flow of 15 Go would cost the client around FF 10 000 per month in France.

Wireless access is intended for ISPs and businesses or institutions which wish to have a permanent connection with bandwidth in excess of 128 kbit/s. One particular advantage of this technology is the simplicity of management: for instance, the bandwidth can be increased simply by means of software programming. The only constraint on its effective use is the line of sight between the two antennae.

5.6.5 Microwave Multipoint Distribution System (MMDS)

5.6.5.1 General remarks

Television cable which could be used for high-speed Internet is a rarity in Africa. One worthwhile and less costly alternative is to use digital transmission over MMDS (Microwave Multipoint Distribution System), regarded as the cable system for rural areas. MMDS is a method of broadcasting analogue or digital television programmes by means of microwave or hyperfrequencies. Amplitude modulation can be used or, better still, frequency modulation, used by direct television satellites. This wireless access to the local network can be used for the Internet. A further possibility exists in the form of systems covered by the European DECT (Digital European Cordless Telephone) standard.

5.6.5.2 MMDS as an alternative to television cable

The operator can receive selected television programmes from various satellites using head-end dish antennae, and redistribute them using a Hypercable transmitter. All that then needs to be done is to equip users (individually or collectively) with a 10 cm active mini-antenna (within 30 km of the transmitter – the range rises to 100 km with a 28 cm antenna) and a satellite TV receiver. No civil engineering work is involved, there are no wires to be pulled out, installation times are short and the environmental impact is low owing to the small size of the receivers. Originally invented for television, MMDS would appear to offer a worthwhile alternative to cable in Africa.

The legislation in the different countries will need to be amended to accommodate this option, which in some European countries is permitted only for extensions to a cable network in rural areas, or for transport at the end of a cable network from the main artery (cable) to households. MMDS is also an option for high-speed multimedia data transmission, which can be used for Internet access.

5.6.5.3 Internet access using MMDS

Taking as a model the case of Mexico, where a single network serves around 400 000 subscribers, MMDS technology could also be used in Africa for connecting to the Internet. In order to use MMDS for connection to the Internet, an IRS (Internet Radio Server) is installed beside the transmitter. This is a microcomputer connected up to the local network of the Internet services provider, which converts the signal to the MPEG2/DVB standard, for transmission via the Hypercable antenna (MDS-France architecture). In addition to an antenna, the Internet subscriber must have a PC card incorporating a satellite receiver (which can receive data at 2 Mbit/s, 4 Mbit/s, 8 Mbit/s or 15 Mbit/s), as well as a standard browser and a PSTN or GSM modem or an ISDN adapter for the backward channel. The most common MMDS solution operates in one direction only, and the user-to-server dialogue must use a different path. A new 2 Mbit/s bidirectional system has just been launched on the market.

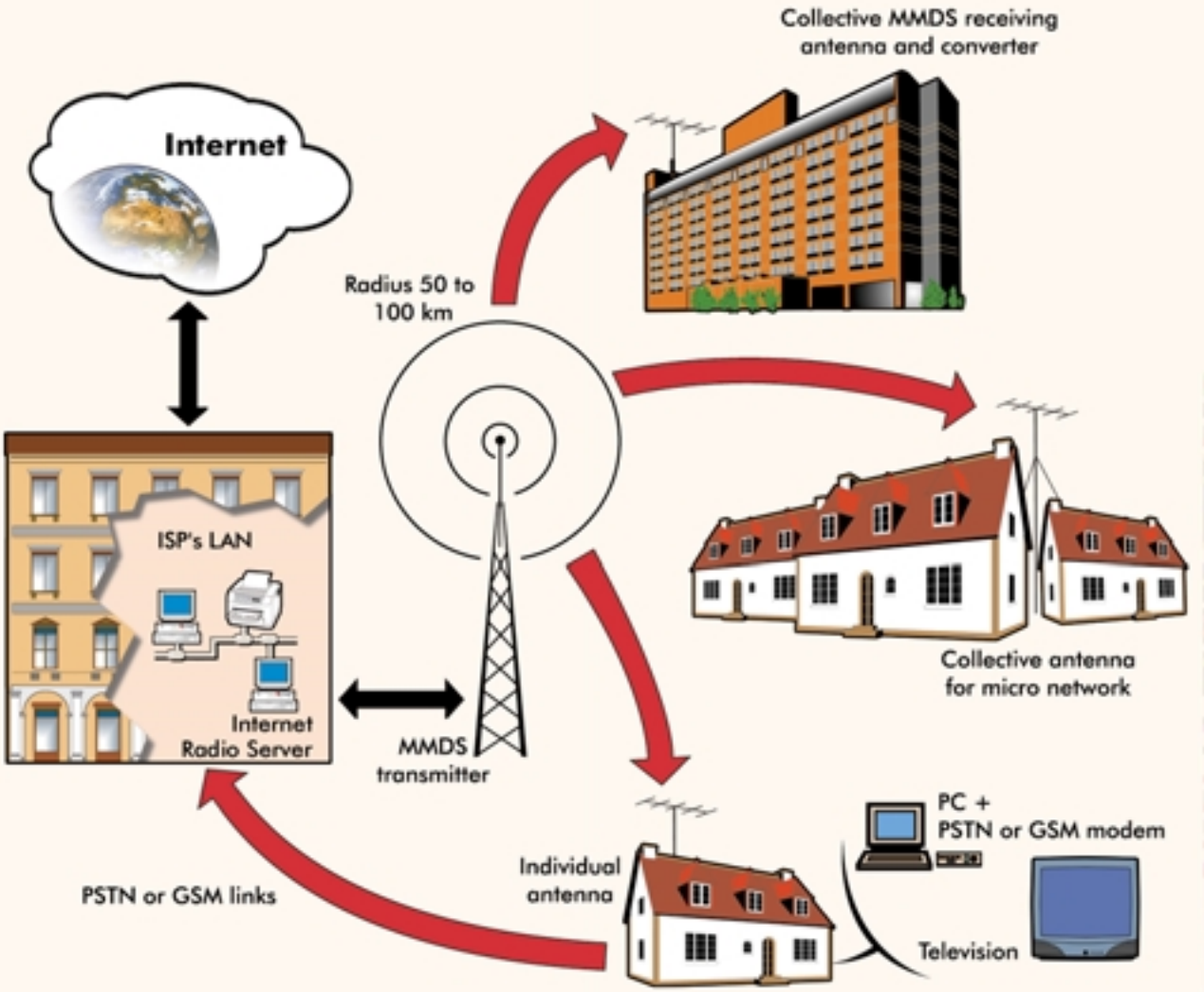

Fig. 5.6 MMDS – One way for Internet Access

6 Regulatory and legal aspects

6.1 General remarks

The telecommunication sector is undergoing profound change as a result of the convergence of telecommunication, audiovisual and computer technologies. These technological changes have a number of regulatory and legal implications. In this section, we will discuss some issues which we feel to be important, and which each telecommunication administration will have to adapt to its national context. The diagram below illustrates the state of the art of Internet technologies.

6.2 Protecting the new technologies

6.2.1 General remarks

Several new technologies are being developed, relating first and foremost to the local loop, the terminal part of the communication network, which serves individual subscribers, as we saw in the last chapter, and to information and network security. These will tend to bring down costs and promote the sale of Internet services. It is therefore important in regulating telecommunications in the African countries to make allowance for the introduction of new technologies relating to the local loop, cryptology and voice communications on the Internet.

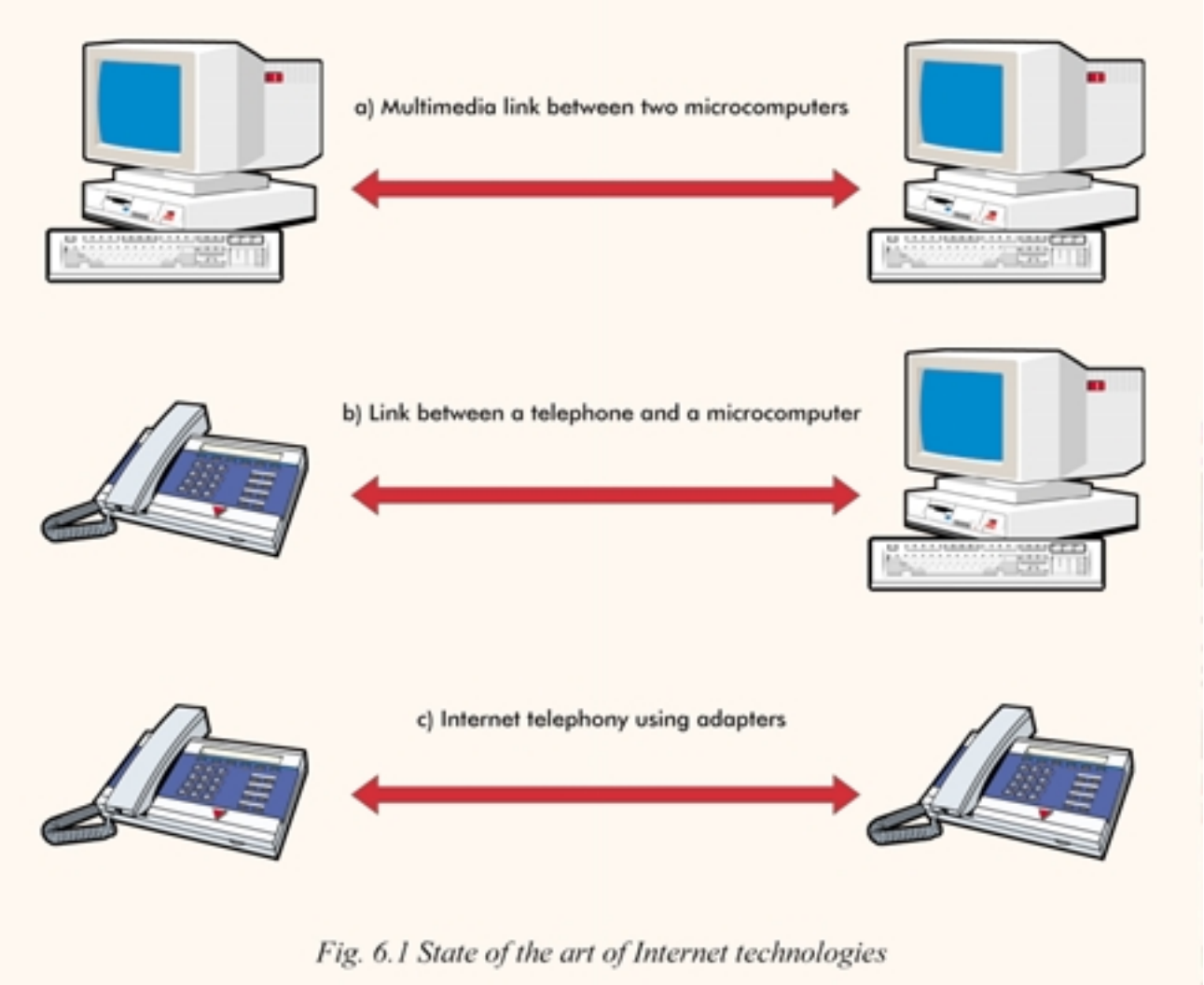

Fig. 6.1 State of the art of Internet technologies

6.2.2 Cryptology

Cryptology tools can be embedded in hardware or software. Cryptology is used to perform the following technological functions:

– *data integrity:* ensuring that information is not altered accidentally or fraudulently;

– *authentication:* digital signatures – authentication of partners and of the source of information;

– *confidentiality:* protection of information.

The legal provisions regulating the use of cryptology in Internet communications must gradually adapt to the use of this technology, as it is a fact of life for most Internet applications, and of prime importance for electronic commerce. The proposals outlined below take account of both the development of information technology and the security of the State and its citizens.

The following measures, therefore, are very important and deserve close attention in all African countries, in order to safeguard the interests of national defence and internal and external security, while at the same time protecting information and the development of secure communications and transactions on the Internet.

- *Import and export of cryptology systems:* The supply, import and export of cryptology tools or services shall be subject to prior authorization by the national telecommunication regulatory authority, when they are designed to ensure confidentiality. As a condition of authorization, the supplier may be required to give the name of the buyer.

- *Freedom for users to use cryptology:* Users shall be free to make use of cryptology tools or services which cannot be used to ensure confidentiality, notably when they can be intended only to authenticate a communication or ensure the integrity of the message (or for digital signatures), or if the tools or services perform functions relating to confidentiality based only on secret conventions managed by the national security authorities.

- *User authorization to use cryptology:* In all other cases, use of cryptology tools or services shall be subject to authorization by the aforementioned national authorities.

6.2.3 Confidentiality

In the majority of African countries, including those where the telecommunication sector has been liberalized, the Ministry is still the agency responsible for managing on behalf of other parties the secret conventions governing cryptology tools or services designed to ensure confidentiality.

Freedom to use cryptology to make messages confidential should be unrestricted, provided that the service is managed by a trusted third party, in other words an approved body which manages the encryption keys on behalf of the user. The user concludes a contract with the trusted third party, which forwards the keys to him on a regular basis so that information can be encrypted. The licence of the trusted third party includes a clause obliging it by law to hand over the encryption keys to the designated authorities should the need arise.

The trusted third party must be clearly designated in each country, so that users have access to a high quality professional cryptology service and the State can, if necessary, gain access to the content of information for compelling reasons of national security.

6.2.4 Responsibilities of cryptology organizations

The organizations which carry out this task must be approved in advance by the competent authority. They shall be covered by professional secrecy in the exercise of their activities. They shall be obliged to keep secret the conventions which they manage, and to hand them over to the judiciary or the competent authorities or implement them, if called upon to do so under the terms of the legislation on the secrecy of telecommunications correspondence or in the course of criminal investigations. They must exercise their activities within the national territory.

The provisions concerning users place the regulatory onus on the cryptology organizations. Other Internet service providers (ISPs) must inform the authorities of any products they place on the market intended for this use and for which they have obtained a licence. They must also seek approval if they wish to become a trusted third party, and shall be bound strictly by the rules. Failure to adhere to the rules shall result in specific penalties being imposed.

6.2.5 Infringements and penalties

- Without prejudice to application of the customs code, the fact of supplying, importing or exporting cryptology tools or services without prior authorization from the authorities, or in breach of the conditions of the authorization given, shall be punishable by law (imprisonment and fine, the length and amount to be determined by the competent authorities).

- The fact of managing on behalf of others the secret conventions governing cryptology tools or services designed to ensure confidentiality, without authorization, or in breach of the conditions of such authorization, shall be punishable by law (imprisonment and fine, the length and amount to be determined by the competent authorities).

- The fact of supplying, importing, exporting or using cryptology tools or services with a view to assisting in the preparation or committing of a crime or offence shall be punishable by law (imprisonment and fine, the length and amount to be determined by the competent authorities).
- Attempted infringements of the kind described above shall be subject to the same penalties.
- Withholding information or documents, or obstructing the course of the authorities' enquiries shall be punishable by law (imprisonment and fine, the length and amount to be determined by the competent authorities).

6.2.6 Definitions and standards

The standardization bodies such as ITU-T and ISO in the international sphere, and AFNOR in France, have laid down the vocabulary used in the field of cryptology. The reference text is ISO 7498-2 of September 1990.

authentication	A procedure applied by sender and recipient to guarantee the integrity of data and authenticate the source (ISO 8730);
data origin authentication	The corroboration that the source of data received is as claimed (ISO 8730);
authentication algorithm	Algorithm used in conjunction with an authentication key and one or more authentication elements for the purposes of authentication (ISO 8730);
authentication element	An element of a message which one wishes to protect by means of authentication (ISO 8730);
data integrity	The property that data has not been altered or destroyed in an unauthorized manner (ISO 8730);
encipherment (encryption)	Cryptographic transformation of data to produce ciphertext (ISO 8730);
cryptogram	Encrypted information (ISO 8732);
decipherment (decryption)	The reversal of a corresponding reversible encipherment (ISO 8730);
cryptography	The discipline which embodies principles, means and methods for the transformation of data in order to hide its content or prevent its alteration or unauthorized use (ISO 8732); *Note* – Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle is called cryptanalysis;
keys	A series of symbols that controls the operation of encipherment and decipherment (ISO 7498-2, 1989);
key management	The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy (ISO 7498-2, 1989);
security policy	The set of criteria for the provision of security services (ISO 7498-2, 1989).

6.3 Voice over IP or Internet telephony

6.3.1 General remarks

The emergence of ever more powerful services, the wish of Internet access providers to market voice services, and the financial attractions for users all point towards significant future development of this type of services. Depending on the legislation in force in each country and on liberalization programmes in the telecommunication sector, the State may or may not hold a monopoly for operating the public telephone service. In the light of advances in information technology and the different agreements between governments and ISPs, it is important to define the status to be accorded to voice communications on the Internet, in order to avoid differing interpretations and confusion when a decision is taken to operate them.

6.3.2 Definition

The definition of voice telephony is subject to different interpretations relating to its technical and operational aspects. According to Article 1 of Directive 90/388/EEC, the term "voice telephony" means the commercial provision for the public of the direct transport and switching of speech in real-time between public switched network termination points, enabling any user to use equipment connected to such a network termination point in order to communicate with another termination point. The Directive also stresses that the service should offer the possibility of connecting any subscriber automatically, if it is to be classified as voice telephony.

Some administrations, including the French, have quite rightly contested this restrictive interpretation, which refers only to communications with "another termination point". They take the view that it is not necessary for all public switched network termination points to be capable of being connected in order for the service to be described as a public telephone service. According to their definition, restricted services and operators offering only international communications services come under the description of voice telephony.

6.3.3 Development of voice communications on the Internet

There are two broad categories of voice communication on the Internet:

- *First-generation voice communications*: These concern certain users who have obtained privately the software needed to convert voice into data and *vice versa* and who can use their computer to conduct a conversation with another Internet user connected at the same time, who also has compatible conversion equipment and software, without any special action on the part of the access provider.

- *Second-generation voice communications*: These involve active intervention from the access provider, who installs software on his server to enable voice to be converted into data and *vice versa*, as well as the interfaces needed to connect any subscriber to the public switched telephone network (PSTN). The user may then, using either a computer or a telephone, depending on the service offered, call his Internet access provider, who will transport the communication over the Internet. Technically, these IP systems must be compatible with Signalling System 7 (SS7) and in conformity with standards specified in ITU-T Recommendations H.323 and H.248.

6.3.4 Commercial exploitation of Internet telephony

"Second generation" services are already up and running in the United States, and are available on an experimental basis in many countries. If all Internet service providers were to begin to offer such services, they would pose a very real competitive threat in the short term to operators of conventional telephony, as regards long-distance communications.

We have come up with the following proposals, prompted by the need to safeguard user interests, maintain a coherent, balanced and non-discriminatory regulatory framework, guarantee fair competition between the various players and provide a *universal service* supported by durable financing, while at the same time encouraging innovation:

- Administrations should consider second-generation voice communications as part of the reserved services subject to operating licences in the context of telecommunications liberalization. Operators of such services would therefore be governed by the relevant rights and obligations, in particular as regards *interconnection* and contributing to financing the *universal service*.
- First-generation voice communications on the Internet should not be considered as voice telephony, implying that the supply of such services should be liberalized and they should not be subject to individual licences or bound to contribute to financing the universal service.

However, technological and market developments could make it necessary to review these proposals at any time.

7 Strengthening local capacity

7.1 General remarks

The development of the information society in Africa depends on strengthening local capacity. As regards the administration of computer systems, e.g. the management of national Internet nodes, it is essential for those concerned to be thoroughly trained in the administration of UNIX and Windows NT, the systems most commonly used on the Internet, and to attend regular training seminars on new information technologies.

7.2 UNIX operating system

Basic training in UNIX Solaris 2.x is necessary in order to have an overview and thus be in a position to extract the full potential from Internet applications (TCP/IP and network administration). We would advise telecommunication operators in Africa to train engineers in UNIX administration. This training could take place in well-equipped national training centres. The course might be divided into ten parts, as follows:

1 General issues
2 Tree hierarchies
3 Peripherals
4 Files system
5 System startup and shutdown
6 Messaging and communication
7 Process management
8 User management
9 Print management
10 Security under UNIX

7.3 TCP/IP in an NT environment

Given the very rapid growth of local networks in an NT environment, and Microsoft's increasing presence on the Internet market, it is also important to strengthen local capacity in relation to the management and administration of TCP/IP networks in an NT environment, in order to exploit the full potential of the Internet Information Server in managing the Internet, intranets and extranets. The training course might be divided up under 15 headings, as follows:

1 Internet addressing
2 Subnetwork addressing
3 TCP/IP routing
4 Installation and configuration of a Windows NT server router

5 The DHCP service

6 ARP address resolution

7 NetBios on TCP/IP

8 WINS servers

9 Name domain servers

10 The SNMP protocol

11 TCP/IP commands and utilities

12 The IP protocol

13 The ICMP protocol

14 The UDP protocol

15 The TCP protocol

7.4 Netscape SuiteSpot

Given the merging of the leading players on the Internet market, with Netscape, AOL and Sun Microsystems having joined forces to dominate the market, we feel it essential for telecommunication operators in Africa to place particular emphasis on, and train local leaders in, the configuration and administration of the Internet server based on Netscape SuiteSpot. The training course might comprise several sections dealing with the following topics:

- Network procedures and Internet services architecture
- Directory Server v 3.11 installation, administration, db management
- Certificate Server v 1.0.1 installation, configuration, startup, LDAP synchronization
- Enterprise Server v 3.5.1 installation, configuration, directory server gateway
- Messaging Server v 3.5 installation and configuration
- Collabra Server v. 3.51 installation and configuration
- Proxy Server v 3.5 installation and configuration

7.5 Internet Information Server

Internet Information Server should not be overlooked, as it also offers all the tools needed for the creation and deployment of applications, and day-to-day administration and analysis of activities on the websites. A successful and comprehensive training package should revolve around the following concepts:

- Installation and configuration of IIS (Internet Information Server 4.0)
- Configuration and management of resource access
- Integration and interactivity
- The functioning of applications
- Monitoring and optimizing performance
- Troubleshooting

7.6 Measuring and managing quality

Quality of service (QoS) in the Internet context is still being worked upon. The method used hitherto consists in supplying vast networks; since the Internet is growing daily, this method cannot be applied indefinitely. The quality of service culture is very important if Internet services are to be operated on a sound footing. In Africa, services engineering is in danger of lagging behind, owing to a shortage of local capacity to manage

network performance and ensure a high standard of service. There is therefore an urgent need to train engineers to implement quality of service in relation to the Internet, in the form of differentiated services, together with the Integrated Services architecture developed by the IETF (Internet Engineering Task Force). A training course or seminars might encompass the following software packages and issues:

- NNSTAT software: ftp://gatekeeper.dec.com/pub/DEC/net/NNstat_3.3beta.tar.Z
- Bay Networks' Optivity software package
- IP Trafic (http://www.urec.cnrs.fr/IPtrafic/)
- NetraMet (Network traffic Meter)
- MRTG (The Multi Router Traffic Grapher) (http://www.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg.html)
- General quality of service issues
- Basic criteria for quality of service in relation to Internet
- Implementing QoS on Internet
- IETF Integrated Services model
- Measuring QoS
- Routing, ATM and QoS

8 Conclusion

The Internet and the information highways transport sound, images and data. According to the California-based company RateXchange, which specializes in negotiating telephone minutes and bandwidth on the Web, data will account for 40% of traffic in 2004, compared with 18% in 1998. At the same time, the current figure of 78% for voice communications is set to fall to 30% by 2004. The Internet is therefore an inescapable part of modern economic life.

The Internet is vital for African development. The challenge is immense, and all the Member States of the Union are looking to ITU/BDT to devote every effort to developing this technology in Africa. This task will cover a number of areas: connectivity, technical management, systems administration, services engineering and metrology, not to mention the strengthening of local capacity and centres of excellence for computer assembly in each country, as the basis for a modern telecommunication industry in the twenty-first century.

Action plans for the implementation of network infrastructure based on the most recent technological advances should be encouraged. This will mean going beyond classic Internet technology and moving away from a dependence on conventional telephone traffic. Particular attention will need to be paid to broadening the target population through the installation of local loops and the provision of diversified and innovative services which reflect customer needs.

ITU will assist members in promoting the information highways in Africa and equipping the continent with a telecommunication infrastructure enabling it to rise to the unprecedented global challenge represented by the Internet.

9 Bibliography

[1] Karyabwite, Désiré, UIT/MAL/R.126, *Gestion technique du nœud et stratégie de développement d'Internet au Mali*, Société des Télécommunications du Mali, SOTELMA, 1998.

[2] Karyabwite, Désiré, UIT/COI/185, *Propositions et formation pour l'amélioration du système d'information de gestion des télécommunications aux Comores*, SNPT, 1997.

[3] Karyabwite, Désiré, UIT/MAG/186, *Propositions et formation pour l'amélioration du système d'information de gestion des télécommunications au Madagascar,* TELMA, 1997.

[4] Karyabwite, Désiré, *Management des technologies Internet pour les PME de hautes technologies*, EPFL, 1996.

[5] ITU Year 2000 Guide, 1999.

[6] ITU-T Recommendation H.233, C*onfidentiality system for audiovisual services*, 1995.

[7] ITU-T Recommendation H.234, *Encryption key management and authentication system for audiovisual services*, November 1994.

[8] *Challenges to the Network: Internet for Development 1999*, ITU, 1999.

[9] *Réseaux TCP/IP*, Wan & Laser, 1997.

[10] Hunt, Craig, O'Reilly & Associates, Inc., Addison Wesley.

[11] Du Bois, Robert, *Structures et applications des émetteurs et des récepteurs*, PPR, 1995.

[12] Bouyer, Gérard, *Transmission et réseaux de données*, Dunod, 1995.

[13] Vialle, Pierre, *Stratégies des opérateurs de télécoms,* Hermes, 1998.

[14] Boisseau, Marc, *Les communications par satellite*, Hermes, 1991.

[15] Perrichon, J.-M., *Les réseaux sans fil*, Masson, 1994.

[16] Servin, Claude, *Télécoms de la transmission à l'architecture de réseaux*, InterEditions, 1998.

[17] *Netsurf*, No. 34.

[18] Site for exchange of telecom minutes: www.Pulver.com

[19] Authentication and traffic analysis: RADIUS software (http://www.livingston.com/Forms/radiusform.cgi OR http://www.merit.edu/aaa/).

[20] Security and firewalls (http://www.tis.com/docs/products/fwtk/).

[21] Books on Internet (http://www.ora.com/).

[22] Cizault, Gisèle, *IPv6 Théorie et pratique*, O'Reilly.

[23] Le Boudec, J.Y., FI-9/1995.

[24] Ferguson, Paul and Huston, Geoff, *Quality of Service: Delivering QoS on the Internet and in Corporate Networks*, Wiley Computer Publishing, 1998.

[25] Articles on QoS: http://www.wiley.com/compbooks/ferguson/.

[26] Ferguson, Paul and Huston, Geoff, *Quality of Service: Fact, Fiction or Compromise?*, INET 98.

Annex I

Estimated budget

Equipment for a national Internet node	
Routers (2 × Cisco 4000)	US$ 20 000
Concentrator (Synoptics) and routers for ISPs (5 × Cisco 2511)	15 000
PC for public WWW server (Pentium)	7 000
PC for WWW development (Pentium)	7 000
PC for network monitoring and compatibility	7 000
Workstation for managing security system	20 000
Backup system	3 000
Software	11 000
Freight	10 000
Subtotal	100 000
Training equipment	
Router	5 000
PC for WWW server (Pentium)	7 000
PC for monitoring and compatibility	7 000
Terminal server (with 16 modems)	10 000
Software	4 000
Freight	7 000
Subtotal	40 000
Engineering, training and technical backup	
UNIX bases	15 000
Configuration and installation of Internet	15 000
To be decided (training bursaries, experts, etc.)	50 000
Subtotal	80 000
International satellite link	
One year	60 000
Subtotal	60 000
Unforeseen expenditure	
Unforeseen expenditure	20 000
TOTAL	300 000

Prices and brand names are indicative, as equipment prices and performance change depending on the manufacturer and the time when the order is placed. We based our figures on those of USAID for the Leland project concerning the setting-up of a basic national Internet node with comfortable data rates. This estimated budget is intended as a basis for work, to be adapted to circumstances in individual countries.

Annex II

Specifications

Internet Operator – Installation and development of a national Internet node

II.1 General remarks

These specifications are based on the technologies discussed in the Guide. They are intended for use by any African country wishing to invite offers for the supply and installation of Internet access.

For developing Internet, one national node may be sufficient initially, but a second, and possibly a third, will soon become a necessity, depending on the area to be covered, the backbone required and the standard of service being sought.

The Internet connection will be established via an earth station with wire, radio-relay or optical fibre links forming an overall connection system.

Each tenderer will be asked to use high bit rates (minimum 128 kbit/s) and a dedicated backbone connection. The ultimate goal of an Internet project is to provide an extension to the backbone in the country concerned, and to allow the national operator to supply the usual Internet services (WWW, e-mail, FTP, etc.) to ISPs (Internet Service Providers) and other subscribers.

II.2 Specifications for the national Internet node

The national Internet node should be so designed as to enable the national operator, local ISPs and user businesses to be connected up without difficulty via conventional dedicated lines or using leading-edge technologies.

High-speed links will also be incorporated. The architecture of the node must comply with the approved standards. The main criteria for choosing a node should be as follows:

- The node must be easily adaptable, so that capacity can be extended without disrupting services completely.
- Future interconnection options must be clear if the network is to be extended to cover a larger area.
- The node must be compatible with local telecommunication infrastructures, and the proposed architecture must allow for easy extension.
- Redundancy.
- Quality of equipment, technical specifications and compliance with standards.
- Ease of maintenance.
- The node must incorporate backup switches.
- Communications security system and associated monitoring equipment.
- Supervision function and possibility of taking corrective action.
- Quality of measuring and traffic analysis instruments.
- Clarity and simplicity of the accompanying documentation.
- User-friendliness of the system.

II.3 Equipment

II.3.1 Satellite link

The satellite link must be structured clearly. The transmission power of the transponder depends on the width of the transmitter beam, which in turn is dependent on the antenna. The wider the area to be covered, the more power is needed.

The following items of information must be provided:

- The name of the company which owns the satellite.
- The name of the international operator for Internet access and a map of its backbone at global level.
- Transmission speed (bit rate) and power.
- Uplink and downlink frequencies.
- The technical characteristics of the antenna and type of polarization.

II.3.2 Routers

The proposed routers must be capable of acting as a gateway between different types of network (Ethernet to FDDI, Token Ring to Ethernet, ATM to FDDI). If the network should become meshed, they must be capable of determining the best path to a particular address (number of nodes, quality of line, bandwidth, etc.).

The routers must therefore be configured to allow connectivity with the network of the international operator and other local networks (to be specified for each country). The configuration must be easily modifiable for future growth.

Details must be given of the functions permitted by the routing algorithm, and whether it provides for some or all of the following:

- Optimization, i.e. selecting the best route in all cases. (This depends on the metrics. For instance, a routing algorithm may use the number of hops and the delay, but attribute more weight to the latter in its calculations.)
- Simplicity and robustness.
- Speed of convergence. (Convergence is agreement between all the routers as to the best route.)

The number of ports must be adequate for interconnection to:

- The earth station.
- A sufficient number of ISPs via dedicated lines.
- Other local networks (the LAN of the telecommunication operator, universities, hospitals, etc.).

To summarize, the routers must:

- Operate principally at layer 3 of the OSI model.
- Be able to act as a bridge for certain protocols.
- Make it possible to divide an address class into subnetworks, thereby reducing the amount of broadcast traffic and the number of broadcasts.
- Be able to filter IP and MAC addresses.
- Determine the best path to take on the basis of the bandwidth of the line and the number of hops.
- Maintain routing tables and transmit them to the next node.

- Collate IP and MAC address pairs in an ARP table.

- Act as an NTP server. (Routers can act as time servers by broadcasting the precise time, obtained by a clock using the Network Time Protocol (NTP), on the various subnetworks.)

The number of routers is to be specified for each country. The routers will use the standard TCP/IP protocols: IP, ICMP, ARP, RARP, IDP, RIP. They must be SNMP-compatible for management purposes.

II.3.3 DNS

Tenderers must supply the local network equipment for the body which centralizes information (the NIC), with particular reference to the primary and secondary DNS servers (Domain Name Servers). They must specify the number of computers required and their characteristics. The minimum configuration for each computer is as follows: 450 MHz, 128 Mb RAM, 10 Gb hard disk, a 3COM Etherlink network interface card, a DVD drive, a 3.5″ disk drive, a 17″ SVGA monitor, and the UNIX Solaris 2.x operating system. The same configuration may be used for other servers, e.g. the secondary DNS server.

II.3.4 Other interconnection equipment

Tenderers must provide a list of the equipment they consider necessary for their proposed system, i.e. repeaters, bridges, routers, gateways, hubs (Host Unit Broadcast), MAUs (Multistation Access Unit). They must specify the mode of operation of each modem (asynchronous and synchronous mode for ISPs).

II.3.5 Computers

The computers used for the security and management system shall be workstations with printers. Memory must be sufficient to ensure that all tasks can be performed, and a high standard of response offered, without affecting service quality.

II.4 National provision of Internet services

If national operators are to develop Internet services (to major customers and individuals), their LANs must be configured accordingly. A firewall system must be used to protect the Internet services provided by the operator, with the exception of public services such as the World Wide Web.

To ensure sound technical management and proper functioning of all Internet services, it is recommended where possible to set aside a dedicated machine for each server corresponding to a particular Internet service. (This implies providing for extensions to the system and ease of maintenance.)

Tenderers must provide details of the configuration of machines, the proposed topology (standard Ethernet, thin Ethernet, Ethernet 10Base-T or Fast Ethernet 100Base-T), as well as the server software for the following main Internet services:

- www.

- Electronic messaging.

- FTP (file transfer).

- Forums and news.
- Secure access (authentication and certificates).
- Proxy.

The communication server must be capable of establishing several hundred communications simultaneously, with the possibility of increasing to a figure deemed sufficient by market studies. It must be modular and capable of being extended without disrupting service.

The servers and machines must be able to operate on UNIX Solaris 2.x or Windows NT (please specify).

II.5 Technical management, security and traffic analysis

Tenderers must supply an audit and security system, anti-virus protection, a backup system and power supply safeguards in the form of inverters or UPS (Uninterruptible Power Supply). Management and administration of the system shall be based on the SNMP protocol. Each tenderer must specify the number of computers needed to manage the network equipment, and give their technical characteristics. They must specify the number of hubs, routers, bridges and other switches which it is capable of managing.

The network management tools must be clearly designated, as must the management platform used, e.g. HP OpenView, SunNet Manager or IBM's Netview, etc. The system must also be capable of supporting basic management tools such as PING, which allows packets to be sent repeatedly to a node on the network using the ICMP protocol, and TRACEROUTE, also ICMP-based, which traces the route taken by the packet and gives transit times for each node on the route, etc.

Measurement and traffic analysis must be user friendly. The network information database must be clearly defined and incorporated into the network management system.

The following is a non-exhaustive list of desired operations:

- Fault management: detection, location and correction of network disturbances.
- Configuration management: access to the configuration parameters (IP addresses) and easy modification thereof.
- Client management and related database: monitoring mechanisms and data necessary for invoicing.
- Maintenance management: monitoring operation of the network when it is set up or when changes are made in the use, identification, addressing and maintenance of hardware or software.
- Management performances: network performance based on targets relating to level of use.
- Firewall protection system and reliability: filtering and protection of the network against unauthorized access and use.
- Capacity forecasting: changes in capacity and growth based on statistics concerning network use, performance and user input.
- Remote assistance.
- Process management via the Web; ISP management.