

NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

**WAN TECHNOLOGIES AND
ROUTING**

Graduation Project

COM- 400

Student: Jawad Iqbal Dar (971265)

Supervisor: Prof. Dr. Fakhreddin MAMEDOV

Nicosia – 2002

ACKNOWLEDGEMENT

"First of all, I feel proud to pay my special regards to "Prof. Dr. Fakhreddin Mamedov". He is one of the most senior persons in Near East University and Dean of Engineering faculty. He never disappointed me in any affair. He delivered me too much information and did his best of efforts to make me able to complete my project. He has Devine place in my heart and I am less than the half without his help. I am really thankful to my teacher.

More over I want to pay special regards to my parents who are enduring these all expenses and supporting me in all events. I am nothing without their prayers. They also encouraged me in crises. I shall never forget their sacrifices for my education so that I can enjoy my successful life as they are expecting. They may get peaceful life in Heaven. At the end I am again thankful to those all persons who helped me or even encouraged me to complete me, my project. My all efforts to complete this project might be fruitful.

To the best of my knowledge, I want to honor those all persons who have supported me or helped me in my project. I also pay my special thanks to my all friends who have helped me in my project and gave me their precious time to complete my project."

ABSTRACT

WAN is an extension of the LAN using some techniques. We need WAN as LAN can not be extended arbitrarily far or to handle arbitrarily many computers so we need a technology for larger networks. WAN can span arbitrary distances and interconnect arbitrarily many computers. We use packet switches and point-to-point connections to accomplish the task of communication. Packet switches use store-and-forward and routing tables to deliver packets to destination. We can use graph algorithms to compute routing tables. Many WAN technologies exist. These WAN technologies help in making communication for more large networks and over large network making communication faster, reliable and secure. WAN also contain some hardware for the proper network to network communication. And between two networks we use a device called router. Its work is to transfer, forward data from one network to other, repeat the weak signals and work on some protocols and finishing the best shortest error free path and send the information on that path. This process or router is called as routing.

TABLE OF CONTENTS

ACKNOWLEDGMENT	i
ABSTRACT	ii
TABLE OF CONTENTS	iii
INTRODUCTION	vii
1. INTRODUCTION TO WAN TECHNOLOGIES	1
1.1 Overview	1
1.2 Point-to-Point Links	2
1.3 Circuit Switching	2
1.4 Packet Switching	3
1.5 WAN Virtual Circuits	4
1.5.1 Switched Virtual Circuit	4
1.5.2 Permanent Virtual Circuit	4
1.6 WAN Dialup Services	5
1.6.1 Dial-on-Demand Routing	5
1.6.2 Dial Backup	6
1.7 WAN Devices	6
1.7.1 WAN Switch	6
1.7.2 Access Server	7
1.7.3 Modem	8
1.7.4 CSU/DSU	8
1.7.5 ISDN Terminal Adapter	9
1.8 WAN Technology Types	9
2. WAN TECHNOLOGIES	11
2.1 Overview	11
2.2 Frame Relay	11
2.2.1 Frame Relay Features	11
2.2.2 Frame Relay Devices	12
2.2.3 Frame Relay Virtual Circuits	12
2.2.3.1 Frame Relay Switched Virtual Circuits	13
2.2.3.2 Frame Relay Permanent Virtual Circuits	14
2.2.4 Frame Relay Error Checking	14
2.2.4.1 Frame Relay Local Management Interface	14
2.2.5 Frame Relay Network Implementation	15
2.2.5.1 Public Carrier-Provided Networks	15
2.2.5.2 Private Enterprise Networks	15
2.3 High-Speed Serial Interface (HSSI)	16
2.3.1 HSSI Specifications	17
2.3.2 HSSI Bandwidth Management	18
2.3.3 DCE Clock Control	18

2.3.4 HSSI Peer-Based Communications	18
2.3.5 HSSI Loop back Support	19
2.4 Integrated Services Digital Network	19
2.4.1 ISDN Standards	20
2.4.2 ISDN Applications	21
2.4.3 ISDN Network Components	21
2.4.3.1 ISDN Terminal Equipment	21
2.4.3.2 ISDN Network Termination Devices	22
2.4.3.3 ISDN Reference Points	22
2.4.4 ISDN Physical Layer Operation	23
2.5 Point-to-Point Protocol	24
2.5.1 PPP Standards	25
2.5.2 PPP Hardware	25
2.5.3 PPP Operation	26
2.5.4 Establishing PPP Connections	26
2.5.5 PPP Link Negotiation	27
2.5.5.1 Link Establishment and Configuration Negotiation	27
2.5.5.2 Link-Quality Determination	28
2.5.5.3 Network Layer Protocol Configuration Negotiation	28
2.5.5.4 Link Termination	28
2.6 Synchronous Data Link Control	28
2.6.1 Related Standards	29
2.6.2 SDLC Environments	29
2.6.3 SDLC Network Nodes	30
2.6.4 SDLC Node Configurations	30
2.6.5 Qualified Logical Link Control	31
2.6.6 Binary Synchronous Protocol	32
2.7 Switched Multi-megabit Data Service	32
2.7.1 SMDS Network Components	33
2.7.2 SMDS Interface Protocol	34
2.7.3 SIP Levels	34
2.7.3.1 SIP Level 3 Operation	35
2.7.3.2 SIP Level 2 Operation	35
2.7.3.3 SIP Level 1 Operation	36
2.7.4 SMDS Addressing	37
2.7.4.1 SMDS Group Addressing	37
2.7.4.2 SMDS Addressing Security	38
2.8 X.25	38
2.8.1 X.25 Network Components	38
2.8.2 Packet Assembler/Disassembler	39
2.8.3 X.25 Session Establishment	40
2.8.4 X.25 Virtual Circuit	40
2.8.5 Virtual Circuits and Multiplexing	41

3. NETWORK ESSENTIALS	42
3.1 The OSI Model	42
3.2 Protocols	44
3.2.1 How Protocols Work?	44
3.2.2 Protocol Stacks (or Suites)	45
3.2.3 The Binding Process	45
3.2.4 Standard Stacks	45
3.2.5 The IEEE protocols at the Physical Layer	46
3.2.5.1 802.3 (CSMA /CD - Ethernet)	46
3.2.5.2 802.4 (Token Passing)	46
3.2.5.3 802.5 (Token Ring)	47
3.3 Important Protocols	47
3.3.1 TCP/IP	47
3.3.2 NetBEUI	47
3.3.3 X.25	47
3.3.4 XNS	48
3.3.5 IPX/SPX and NWLink	48
3.3.6 APPC	48
3.3.7 AppleTalk	48
3.3.8 OSI Protocol Suite	48
3.3.9 DECnet	48
3.4 Network Architectures	49
3.4.1 Ethernet	49
3.4.2 Ethernet Frames	49
3.5 Network Hardware	49
3.5.1 Modems	50
3.5.1.1 Asynchronous Communications	50
3.5.1.2 Synchronous Communication	51
3.5.2 Repeaters	52
3.5.2.1 Repeater features	53
3.5.3 Bridges	54
3.5.4 Routers	56
3.5.4.1 Choosing Paths	57
3.5.5 Brouters	58
3.5.6 Hubs	58
3.5.7 Gateways	59
3.6 WAN Transmission	60
3.6.1 Analog	60
3.6.2 Digital	61
3.6.3 T1	61
3.6.4 T3	62
3.6.5 Switched 56	62
3.6.6 Packet Switching	62
3.6.7 Fiber Distributed Data Interface	63

4. ROUTING	66
4.1 Overview	66
4.2 Router	66
4.3 Operation of a Router	68
4.3.1 Forwarding	71
4.3.1.1 Process Switching	74
4.3.1.2 Fast Switching	76
4.3.1.3 The Route Processor	79
4.3.2 Packets Destined for the Router	80
4.4 Routing in the Internet	83
4.4.1 Physical Address Determination	83
4.4.2 Reverse Address Resolution Protocol	86
4.4.3 Internet Routing - Internal Routing Tables	86
4.4.4 Communication between routers	89
4.4.5 The RIP (RFC 1058) protocol	89
4.4.6 The OSPF (RFC 1247) Protocol	91
4.4.7 Allocation of IP addresses	92
4.4.8 Autonomous Systems	94
CONCLUSION	95
REFERENCES	96

INTRODUCTION

Now a days every where in this world rather a small office or big we need to have a network even in a small office we have many computers sharing a single or two printers. All this is possible because of networking. There are three main types of networking one which is in a small office called as LAN as local area network. Then there is a kind of networking which is used to connect distant offices means in other words a network in which we can connect LAN of one office to LAN of other office called as WAN. Two or more than two LAN combine to make a WAN and the third type is MAN which is more advance than LAN.

To connect two or more LAN to make WAN we use a device called router as from its name is specified that it routes the data from one network to another network. Router is the main component to make communication between many networks as it has its own operating system and program and it is its responsibility that which data must be sent to which network and this process is called routing.

My first chapter is all about explaining what are WAN technologies. It is an introduction chapter in which I have explained about WAN in detail and what are the features of WAN and what are the devices used in WAN to make communication possible between two networks.

My second chapter is all about giving details of what are the technologies used in WAN. There are about seven main technologies used in WAN such as Frame Relay which is all about high-performance, packet-switched WAN protocols. Then we have High Speed Serial Interface (HSSI). It is all about a network standard for high-speed serial communications over WAN links. Then we have Integrated Services Data Network (ISDN). It consists of communication protocols proposed by telephone companies to permit telephone networks to carry data, voice, and other source material. Further we have Point-to-Point Protocol (PPP). It provides router-to-router and host-to-network connections over

synchronous and asynchronous circuits. Then we have Synchronous Data Link Control (SDLC) & Switched Multi-megabit Data Service (SMDS). They are IBM bit-synchronous data link layer protocol and used as high-speed, packet-switched WAN technology. The last one is X.25 which is an ITU-T WAN communications protocol.

My third chapter is all about WAN essentials in other words the components of WAN which help in communication. First of all we have an OSI seven Layer model. Which is a model helping in making communication more reliable. Then we have protocols helping in communication, the most important is network architecture and the hardware we use in WAN like modems, access server, repeaters synchronous and asynchronous communication, bridges, hubs, routers and gate ways.

In the last chapter I have explained about the router and its main process called as routing. I have explained in the chapter the operation of router in detail as forwarding of packets, repeat the transmission of a packet and finding the best and shortest secure path and pass for the destination.

1. INTRODUCTION TO WAN TECHNOLOGIES

1.1 Overview

A wide-area network (WAN) is a data communications network covering a relatively broad geographic area and often using transmission facilities provided by the common carriers. WAN technologies function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

The following figure shows the relationship between the common WAN technologies and the OSI model:

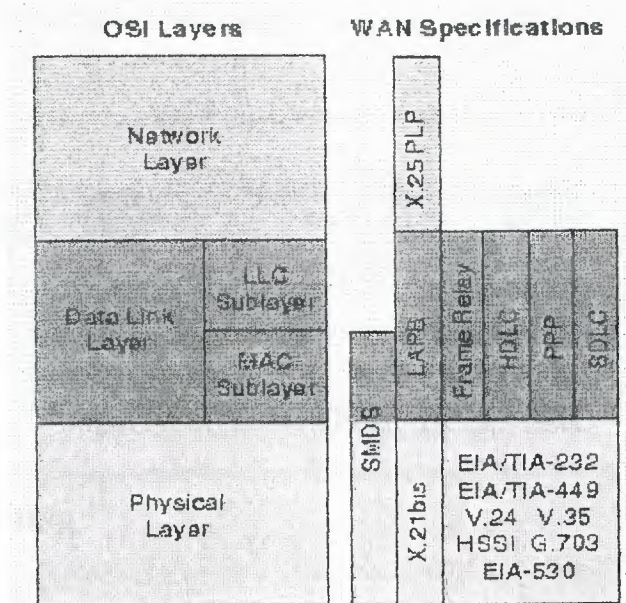


Figure 1.1: Shows WAN Specification and OSI Model

1.2 Point-to-Point Links

A point-to-point link provides a single, reestablished WAN communications path from the customer premises, through a carrier network (the telephone company), to a remote network. Point-to-point links are also known as leased lines. The established path is permanent and is fixed for each remote network reached through the carrier facilities. Point-to-point links are reserved by the carrier company for the private use of the customer.

Point-to-point links allow two types of transmission:

Datagram transmission -- Datagram transmissions are composed of individually addressed frames.

Data stream transmission -- Data stream transmissions are composed of a stream of data for which address checking occurs only once.

The following figure illustrates a typical point-to-point link through a WAN:

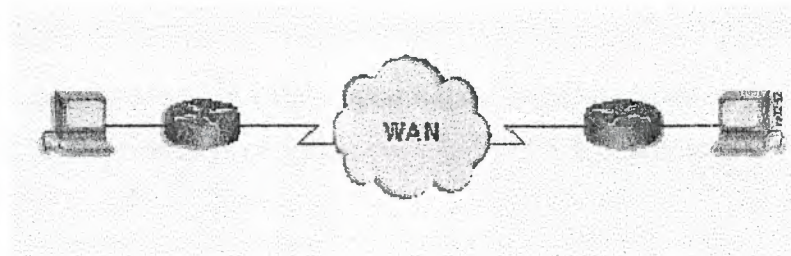


Figure 1.2: Shows a Point-to-Point Link

1.3 Circuit Switching

Circuit switching is a WAN switching method in which a dedicated physical circuit through a carrier network is established, maintained, and terminated for each communication session. Circuit switching, used extensively in telephone company networks, operates much like a normal telephone call. Integrated Services Digital Network (ISDN) is an example of a circuit-switched WAN technology.

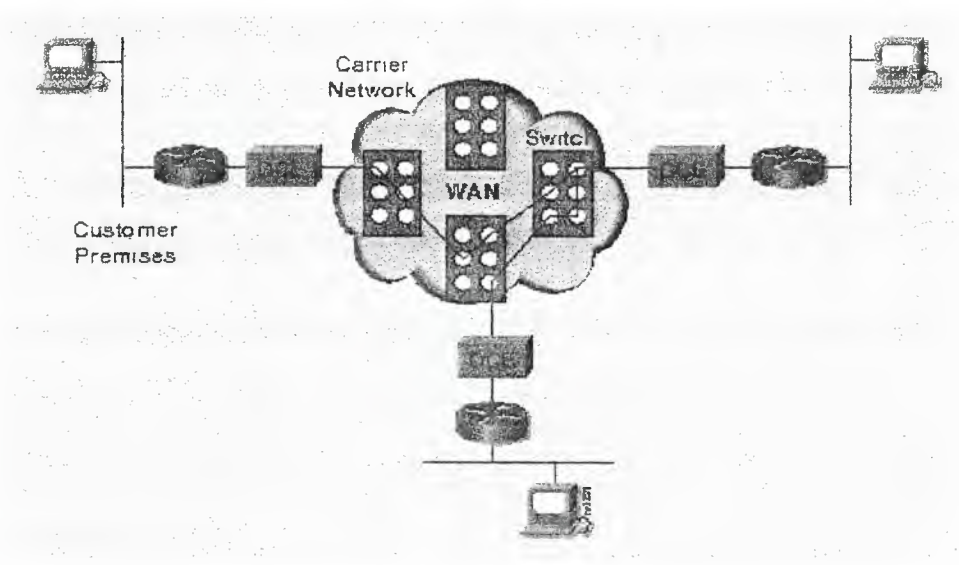


Figure 1.3: Shows a circuit-switched WAN

1.4 Packet Switching

Packet switching is a WAN switching method in which network devices share a single point-to-point link to transport packets from a source to a destination across a carrier network. Statistical multiplexing is used to allow devices to share these circuits. Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multi-megabit Data Service (SMDS), and X.25 are examples of packet-switched WAN technologies.

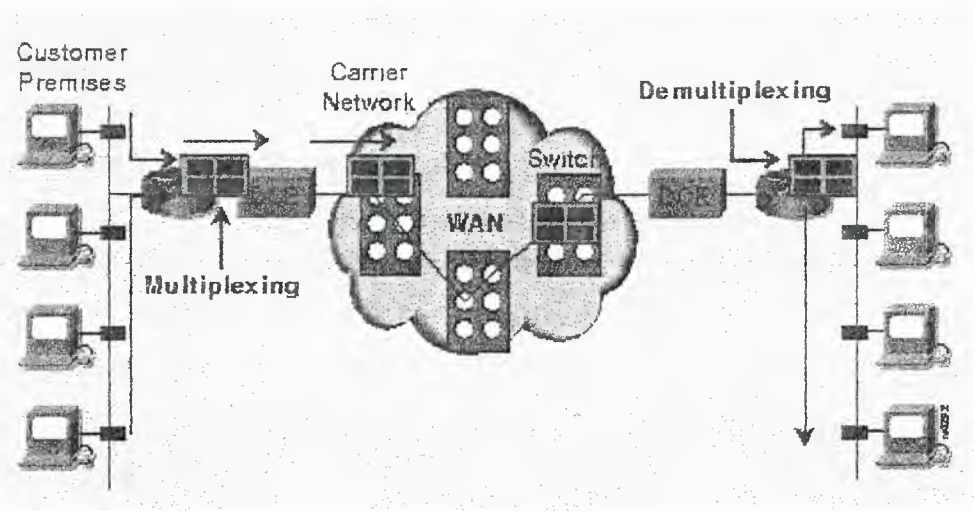


Figure 1.4: Illustrates a packet-switched WAN

1.5 WAN Virtual Circuits

A virtual circuit is a logical circuit created to ensure reliable communication between two network devices. There are two types of virtual circuits: switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).

1.5.1 Switched Virtual Circuit

A switched virtual circuit (SVC) is a virtual circuit that is dynamically established on demand and is terminated when transmission is complete. Communication over an SVC consists of three phases:

Circuit establishment -- The circuit establishment phase involves creating the virtual circuit between the source and destination devices.

Data transfer -- The data transfer phase involves transmitting data between the devices over the virtual circuit.

Circuit termination -- The circuit termination phase involves tearing down the virtual circuit between the source and destination devices.

SVCs are used in situations where data transmission between devices is sporadic. SVCs increase bandwidth use due to the circuit establishment and termination phases, but decrease the cost associated with constant virtual circuit availability.

1.5.2 Permanent Virtual Circuit

A permanent virtual circuit (PVC) is a virtual circuit that is permanently established. PVCs consist of one mode: data transfer. PVCs are used in situations where data transfer between devices is constant. PVCs decrease the bandwidth use associated with the establishment and termination of virtual circuits, but increase costs due to constant virtual circuit availability.

1.6 WAN Dialup Services

Dialup services offer cost-effective methods for connectivity across WANs. Two popular dialup implementations are dial-on-demand routing (DDR) and dial backup.

1.6.1 Dial-on-Demand Routing

Dial-on-demand routing (DDR) is a technique whereby a Cisco router can dynamically initiate and close a circuit-switched session as transmitting end stations demand. A router is configured to consider certain traffic interesting (such as traffic from a particular protocol) and other traffic uninteresting. When the router receives interesting traffic destined for a remote network, a circuit is established and the traffic is transmitted normally. If the router receives uninteresting traffic, and a circuit is already established, that traffic is transmitted normally as well.

— The router maintains an idle timer that is reset only when interesting traffic is received. If the router receives no interesting traffic before the idle timer expires, the circuit is terminated. If uninteresting traffic is received, and no circuit exists, the traffic is dropped. Upon receiving interesting traffic, the router will initiate a new circuit. DDR can be used to replace point-to-point links and switched multi-access WAN services.

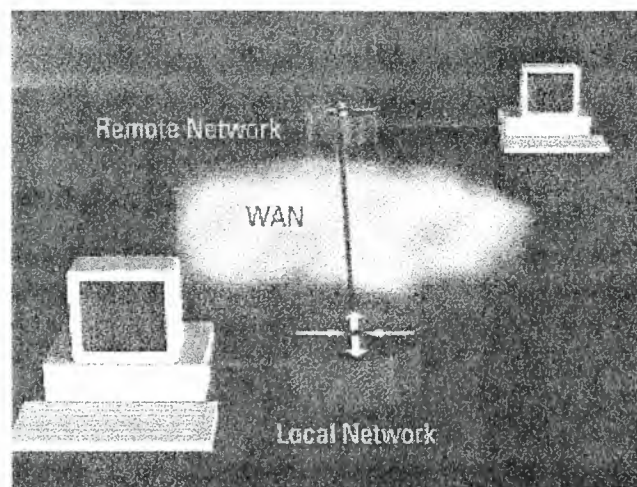


Figure 1.5: Shows the basic operation of a DDR implementation

1.6.2 Dial Backup

Dial backup is a service that activates a backup serial line under certain conditions. The secondary serial line can act as a backup link that is used when the primary link fails or as a source of additional bandwidth when the load on the primary link reaches a certain threshold. Dial backup provides protection against WAN performance degradation and downtime.

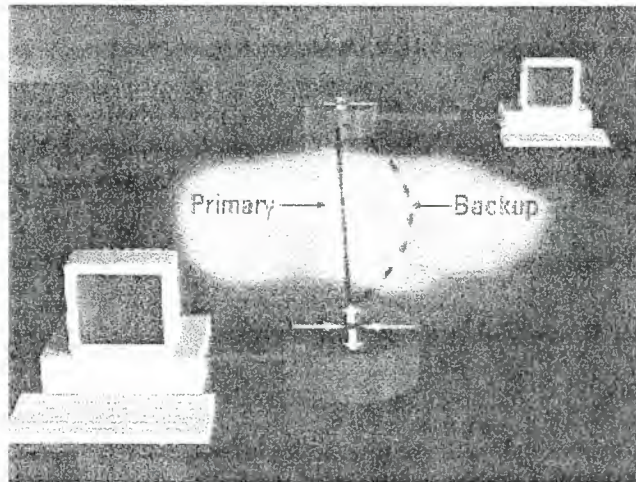


Figure 1.6: Shows the operation of a dial backup implementation

1.7 WAN Devices

There are numerous types of devices used in WANs. These include routers, ATM switches, multiplexers, various WAN switches, access servers, modems, CSU/DSUs, and terminal adapters.

1.7.1 WAN Switch

A WAN switch is a multi-port internetworking device used in carrier networks. These devices typically switch Frame Relay, X.25, SMDS, and other WAN traffic. They operate at the data link layer of the Open System Interconnection (OSI) reference model.

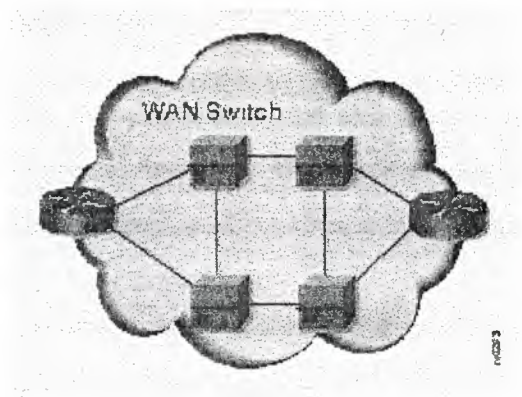


Figure 1.7: Shows Two Routers of a WAN connected by switches:

1.7.2 Access Server

An access server serves as a concentration point for dial-in and dial-out connections.

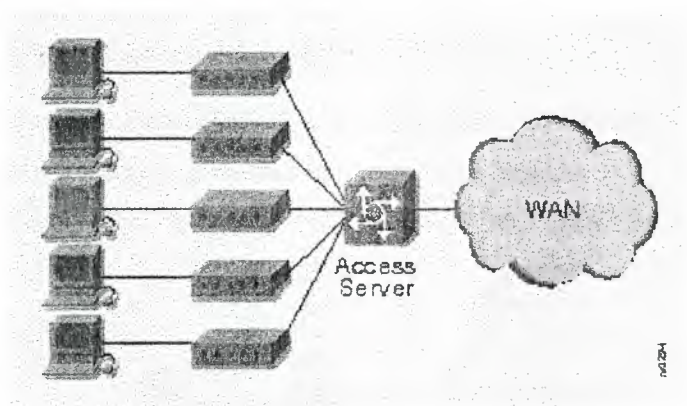


Figure 1.8: Shows an access server concentrating dial-out connections

1.7.3 Modem

A modem is a device that converts digital and analog signals, allowing data to be transmitted over voice-grade telephone lines. At the source, digital signals are converted to a form suitable for transmission over analog communication facilities. At the destination, analog signals are returned to their digital form.

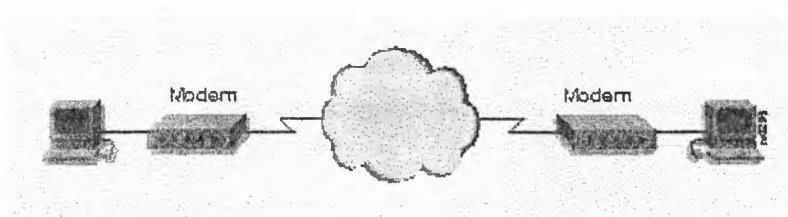


Figure 1.9: Shows a Simple modem-to-modem connection

1.7.4 CSU/DSU

A channel service unit/data service unit (CSU/DSU) is a digital interface device (or sometimes two separate digital devices) that adapts the physical interface on a data terminal equipment (DTE) device (such as a terminal) to the interface of a data circuit-terminating (DCE) device (such as a switch) in a switched carrier network. The CSU/DSU also provides signal timing for communication between these devices.

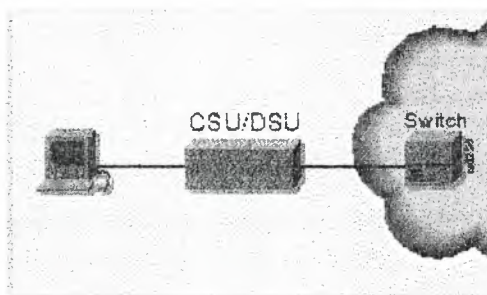


Figure 1.10: Shows the Placement of the CSU/DSU

1.7.5 ISDN Terminal Adapter

An Integrated Services Digital Network (ISDN) terminal adapter is a device used to connect ISDN Basic Rate Interface (BRI) connections to other interfaces such as EIA/TIA-232. A terminal adapter is essentially an ISDN modem.

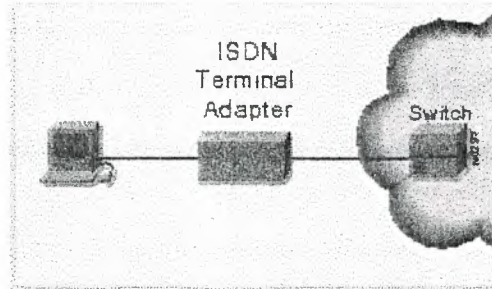


Figure 1.11: Shows Terminal Adapter in an ISDN Environment:

1.8 WAN Technology Types

Following is a list of some of the common WAN technologies:

- Frame Relay

Frame Relay is a high-performance, packet-switched WAN protocol.

- High Speed Serial Interface (HSSI)

HSSI is a network standard for high-speed serial communications over WAN links.

- Integrated Services Data Network (ISDN)

ISDN consists of communication protocols proposed by telephone companies to permit telephone networks to carry data, voice, and other source material.

- Point-to-Point Protocol (PPP)

PPP provides router-to-router and host-to-network connections over synchronous and asynchronous circuits.

- Synchronous Data Link Control (SDLC)

SDLC is an IBM bit-synchronous data link layer protocol.

- Switched Multi-megabit Data Service (SMDS)

SMDS is a high-speed, packet-switched WAN technology.

- X.25

X.25 is an ITU-T WAN communications protocol.

2. WAN TECHNOLOGIES

2.1 Overview

This chapter gives a brief description of the technologies used in the WAN now a days. A precise description of each component has been given in order to have a basic knowledge of these components.

2.2 Frame Relay

Frame Relay is a high-performance wide-area network (WAN) protocol that operates at the physical and data link layers of the Open System Interconnection (OSI) reference model. Frame Relay was originally designed for use across Integrated Services Digital Network (ISDN) interfaces. Today, it is used over a variety of other network interfaces as well.

2.2.1 Frame Relay Features

Frame Relay provides a data communications interface between user devices and network devices. This interface forms the basis for communication between user devices across a WAN. Typical communication speeds for Frame Relay are between 56 Kbps and 2 Mbps (although lower and higher speeds are supported). Frame Relay is considerably more efficient than X.25, the protocol for which it is often considered a replacement. Because it supports technological advances such as fiber-optic cabling and digital transmission, Frame Relay can eliminate time-consuming processes (such as error correction and flow control) that are necessary when using older, less reliable WAN media and protocols.

2.2.2 Frame Relay Devices

Devices attached to a Frame Relay WAN fall into two general categories:

Data terminal equipment (DTE) -- DTE is customer-owned end node and internetworking devices. Examples of DTE devices are terminals, personal computers, routers, and bridges.

Data circuit-terminating equipment (DCE) -- DCE is carrier-owned internetworking devices. In most cases, these are packet switches (although ~~routers or other devices can be~~ configured as DCE as well).

DTE and DCE devices are logical entities. That is, DTE devices initiate a communications exchange, and DCE devices respond.

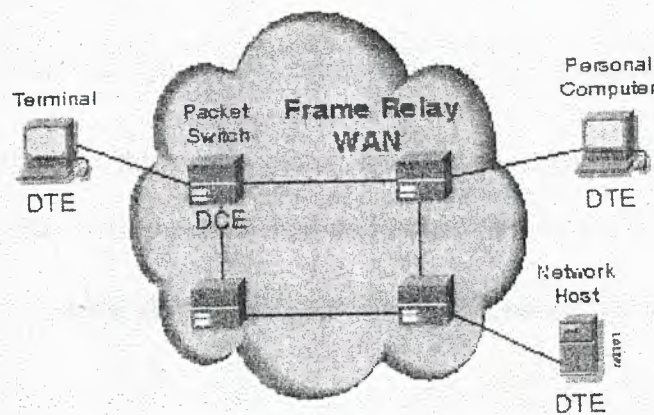


Figure 2.1: Shows the Relationship between the two Categories of Devices

2.2.3 Frame Relay Virtual Circuits

Frame Relay provides connection-oriented data link layer communication. This service is implemented using virtual circuits. A Frame Relay virtual circuit is a logical connection created between two data terminal equipment (DTE) devices across a Frame Relay packet-switched network (PSN). Virtual circuits provide a bidirectional communications path from one DTE device to another. They are uniquely identified by a data link connection identifier (DLCI). A virtual circuit can pass through any number of

intermediate data circuit-terminating equipment (DCE) devices (switches) located within the Frame Relay PSN. A number of virtual circuits can be multiplexed into a single physical circuit for transmission across the network.

Frame Relay virtual circuits fall into two categories:

- Switched virtual circuit (SVC)
- Permanent virtual circuit (PVC)

2.2.3.1 Frame Relay Switched Virtual Circuits (SVCs)

A switched virtual circuit (SVC) is one of the two types of virtual circuits used in Frame Relay implementations. SVCs are temporary connections that are used when there is only sporadic data transfer between DTE devices across the Frame Relay network.

A communication session across an SVC consists of four operational states:

Call setup -- In this state, the virtual circuit between two Frame Relay DTE devices is established.

Data transfer -- In this state, data is being transmitted between the DTE devices over the virtual circuit.

Idle -- In this state, the connection between DTE devices is still active, but no data is being transferred.

Call termination -- In this state, the virtual circuit between DTE devices is terminated.

After the virtual circuit is terminated, the DTE devices must establish a new SVC if there is additional data to be exchanged

2.2.3.2 Frame Relay Permanent Virtual Circuits (PVCs)

A permanent virtual circuit (PVC) is one of two types of virtual circuits used in Frame Relay implementations. PVCs are permanently established connections that are used when there is frequent and consistent data transfer between DTE devices across the Frame Relay network. Communication across PVC does not require the call setup and termination states that are used with SVCs. PVCs are always in one of the following two operational states:

Data transfer -- In this state, data is being transmitted between the DTE devices over the virtual circuit.

Idle -- In this state, the connection between DTE devices is active, but no data is being transferred.

DTE devices can begin transferring data whenever they are ready because the circuit is permanently established.

2.2.4 Frame Relay Error Checking

Frame Relay uses a common error checking mechanism known as the cyclic redundancy check (CRC). The CRC compares two calculated values to determine whether errors occurred during the transmission from source to destination. Frame Relay reduces network overhead by implementing error checking rather than error correction. Because Frame Relay is typically implemented on reliable network media, data integrity is not sacrificed because error correction can be left to higher-layer protocols running on top of Frame Relay.

2.2.4.1 Frame Relay Local Management Interface (LMI)

The Local Management Interface (LMI) is a set of enhancements to the basic Frame Relay specification. The LMI was developed in 1990 by Cisco Systems, Strata COM, Northern Telecom, and Digital Equipment Corporation. It offers a number of features (called extensions) for managing complex internet works.

There are three types of extensions global addressing, virtual circuit status messages and multicasting

2.2.5 Frame Relay Network Implementation

Frame Relay is implemented in both public carrier-provided networks and in private enterprise networks.

2.2.5.1 Public Carrier-Provided Networks

In public carrier-provided Frame Relay networks, the Frame Relay switching equipment (DCE) is located in the central offices of a telecommunications carrier. Subscribers are charged based on their network use, but are relieved from administering and maintaining the Frame Relay network equipment and service.

2.2.5.2 Private Enterprise Networks

In private Frame Relay networks, the administration and maintenance of the network is the responsibility of the enterprise (a private company). A common private Frame Relay network implementation is to equip a T1 multiplexer with both Frame Relay and non-Frame Relay interfaces. Frame Relay traffic is forwarded out the Frame Relay interface and onto the data network. Non-Frame Relay traffic is forwarded to the appropriate application or service (such as a private branch exchange [PBX] for telephone service or to a video-teleconferencing application).

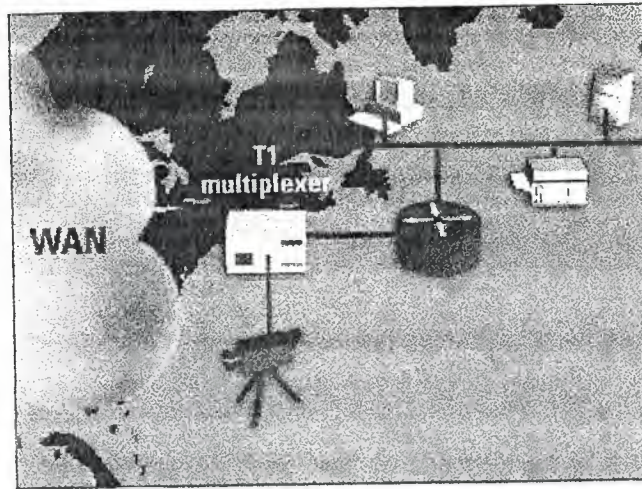


Figure 2.2: Illustrates Frame Relay Implementation

2.3 High-Speed Serial Interface (HSSI)

The High-Speed Serial Interface (HSSI) is a network standard for high-speed (up to 52 Mbps) serial communications over WAN links. HSSI employs a DTE/DCE interface developed by Cisco Systems and T3plus Networking. HSSI was originally offered to the ANSI EIA/TIA TR30.2 committee review. It has since been moved to the ITU-T standardization sector for acceptance.

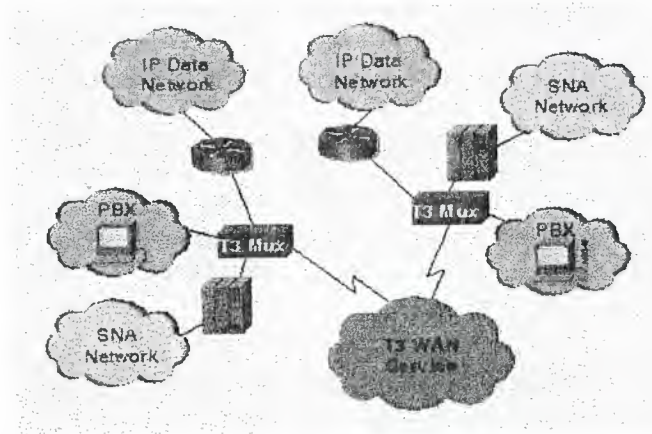


Figure 2.3: Illustrates a Typical HSSI-based T3 WAN

2.3.1 HSSI Specifications

HSSI defines an electrical and physical interface. The emitter-coupled logic (ECL) that is implemented with HSSI improves reliability at high data rates.

Table 2.1: Lists Standard HSSI Characteristics and Values:

Characteristic	Value
Maximum signaling rate	52 Mbps
Maximum cable length	50 feet (15 meters)
Number of connector pins	50
Interface	DTE-DCE
Electrical technology	Differential ECL
Typical power consumption	610 milliwatts
Topology	Point-to-point
Cable type	Shielded twisted-pair wire

HSSI specifies a subminiature, FCC-approved 50-pin connector with the HSSI connectors specified as male.

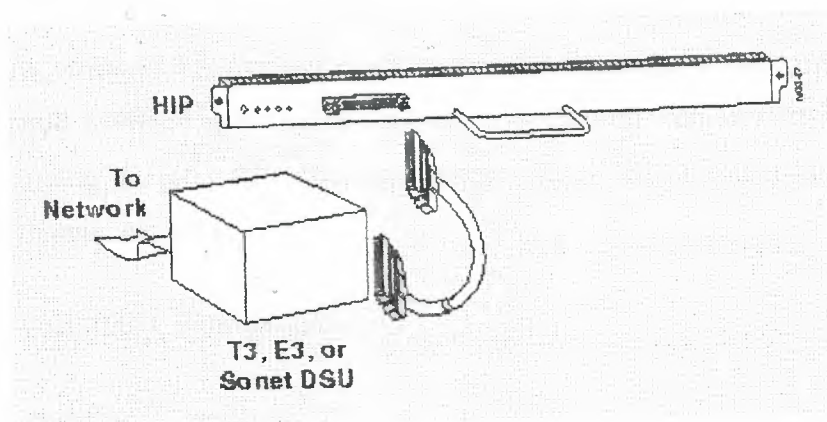


Figure 2.4: Illustrates a HSSI Interface Processor to a DSU

2.3.2 HSSI Bandwidth Management

In order to provide effective bandwidth management, HSSI implements a clock and data signaling protocol that allows device requirements to determine the bandwidth allotted.

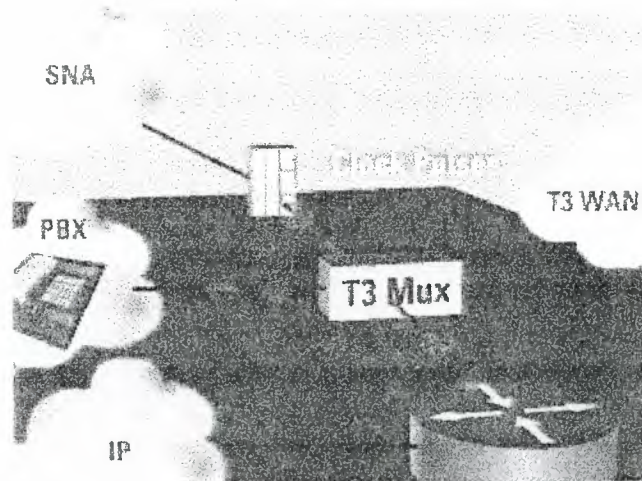


Figure 2.5: Illustrates Bandwidth Management Approach

2.3.3 DCE Clock Control

The DCE clock rate control mechanism implemented with HSSI controls the clock by changing its speed or by deleting clock pulses. This process allows HSSI devices to allocate bandwidth between applications with differing data-rate requirements. Examples of applications needing differing data-rate requirements are a PBX, a router-based LAN, and an IBM SNA channel extender.

2.3.4 HSSI Peer-Based Communications

HSSI specifies a peer-to-peer communications environment. This environment assumes a peer-to-peer intelligence in both the DCE and DTE devices. HSSI's simplified protocol requires only two control signals: one indicating that the DTE is available and another indicating that the DCE is available.

2.3.5 HSSI Loop back Support

HSSI supports four loop back tests:

Local cable -- Local cable loops back from the DCE port.

Local DCE -- Local DCE loops back from the line port of the local DCE.

Remote DCE -- Remote DCE loops back from the line port of the remote DCE.

DCE-initiated -- DCE-initiated loops back from the DTE's DCE port.

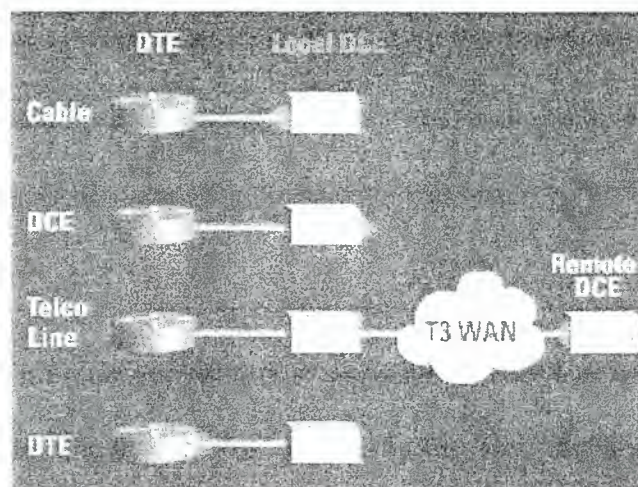


Figure 2.6: Illustrates each HSSI Loop Back Mode

2.4 Integrated Services Digital Network (ISDN)

Integrated Services Digital Network (ISDN) refers to a set of communication protocols proposed by telephone companies to permit telephone networks to carry data, voice, and other source material. In general, ISDN provides a set of digital services that concurrently deliver voice, data, text, graphics, music, video, and information to end users. ISDN was developed to permit access over existing telephone systems. ISDN services are offered by many carriers under tariff. ISDN is generally viewed as an alternative to Frame

Relay and T1 wide-area telephone services (WATS). In practical terms, ISDN has evolved into one of the leading technologies for facilitating telecommuting arrangements and internetworking small, remote offices into corporate campuses.

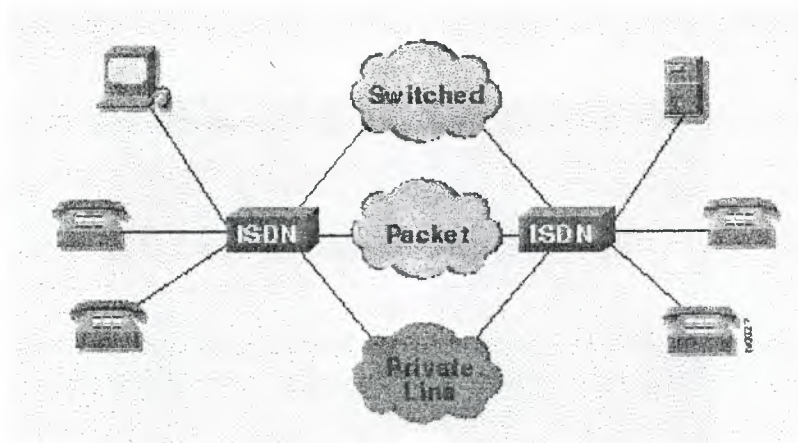


Figure 2.7: Illustrates the ISDN Environment

2.4.1 ISDN Standards

ISDN is addressed by a suite of ITU-T standards, spanning the physical, data link, and network layers of the seven-layer OSI networking model:

Physical layer -- The ISDN Basic Rate Interface (BRI) physical layer specification is defined in International Telecommunication Union Telecommunication Standardization Sector (ITU-T) I.430. The ISDN Primary Rate Interface (PRI) physical layer specification is defined in ITU-T I.431.

Data link layer -- The ISDN data link layer specification is based on Link Access Procedure on the D channels (LAPD) and is formally specified in ITU-T Q.920 and ITU-T Q.921.

Network layer -- The ISDN network layer is defined in ITU-T I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together these two standards specify user-to-user, circuit-switched, and packet-switched connections.

2.4.2 ISDN Applications

ISDN applications require bandwidth. Typical ISDN applications and implementations include high-speed image applications (such as Group IV facsimile), high-speed file transfer, video conferencing, and multiple links into homes of telecommuters.

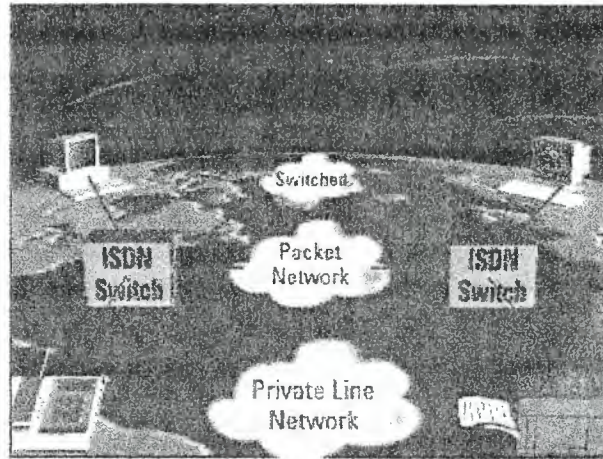


Figure 2.8: Illustrates Traffic Flowing Over an ISDN Network

2.4.3 ISDN Network Components

ISDN network components fall into three principal categories:

- ISDN terminal equipment
- ISDN termination devices
- ISDN reference points

2.4.3.1 ISDN Terminal Equipment

ISDN specifies two basic terminal equipment types:

Terminal Equipment Type 1 (TE1) -- A TE1 is a specialized ISDN terminal, including computer equipment or telephones. It is used to connect to ISDN through a four-wire, twisted-pair digital link.

Terminal Equipment Type 2 (TE2) -- A TE2 is a non-ISDN terminal such as data terminal equipment (DTE) that predates the ISDN standards. A TE2 connects to ISDN through a terminal adapter (TA). An ISDN TA can be either a standalone device or a board inside the TE2.

2.4.3.2 ISDN Network Termination Devices

ISDN specifies a type of intermediate equipment called a network termination (NT) device. NTs connect the four-wire subscriber wiring to two-wire local loops. There are three supported NT types:

NT Type 1 (NT1) device -- An NT1 device is treated as customer premises equipment (CPE) in North America, but is provided by carriers elsewhere.

NT Type 2 (NT2) device -- An NT2 device is typically found in digital private branch exchanges (PBXs). An NT2 performs Layer 2 and 3 protocol functions and concentration services.

NT Type 1/2 (NT1/2) device -- An NT1/2 device provides combined functions of separate NT1 and NT2 devices. An NT1/2 is compatible with NT1 and NT2 devices, and is used to replace separate NT1 and NT2 devices.

2.4.3.3 ISDN Reference Points

ISDN reference points define logical interfaces. Four reference points are defined in ISDN:

R reference point -- The R reference point defines the reference point between non-ISDN equipment and a TA.

S reference point -- The S reference point defines the reference point between user terminals and an NT2.

T reference point -- The T reference point defines the reference point between NT1 and NT2 devices.

U reference point -- The U reference point defines the reference point between NT1 devices and line-termination equipment in a carrier network. (This is only in North America, where the NT1 function is not provided by the carrier network.)

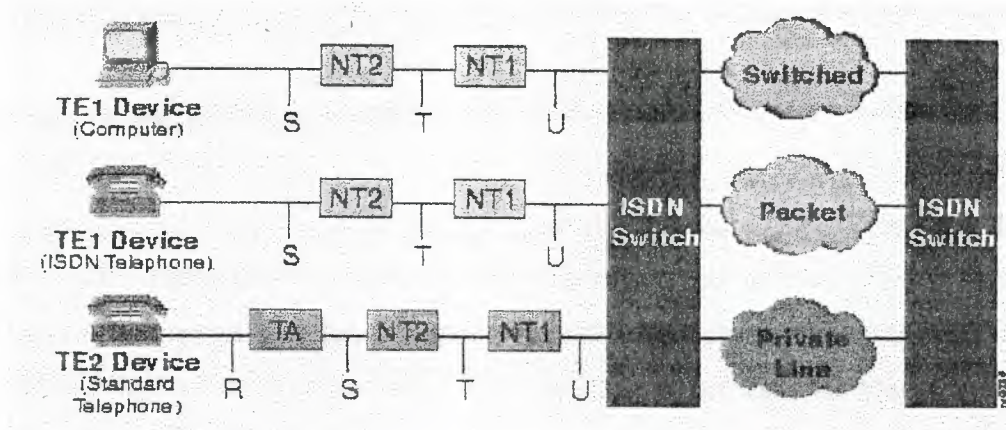


Figure 2.9: Illustrates Reference Points Found in ISDN Implementations

2.4.4 ISDN Physical Layer Operation

ISDN involves three basic physical layer operational stages:

- Contention
- D-channel transmission
- Priority negotiation

ISDN Contention--The ISDN contention process permits multiple ISDN user devices to be physically attached to a single ISDN link. When the ISDN NT device receives a D bit from a TE, the NT echoes back the bit in the next E-bit position. The TE expects the next E bit to match its last transmitted D bit.

ISDN D-Channel Transmission--Terminals transmit into the D channel after first detecting a "no signal" indication. If the TE device detects a bit in the echo (E) channel different from its D bits, it stops transmitting.

ISDN Priority Negotiation--ISDN permits devices to transmission priority over other devices. After a successful D message transmission, a terminal's priority is reduced by requiring the terminal to detect more continuous binary ones before transmitting again. A terminal cannot raise its priority until all other devices on the same line have had an opportunity to send a D message.

2.5 Point-to-Point Protocol (PPP)

The Point-to-Point Protocol (PPP) is generally viewed as the successor to the Serial Line IP (SLIP) protocol. PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits. PPP emerged in the late 1980s in response to a lack of encapsulation protocols for the Internet that was blocking growth of serial-line access. PPP was basically created to solve remote Internet connectivity problems. PPP supports a number of network layer protocols, including Novell IPX and DECnet.

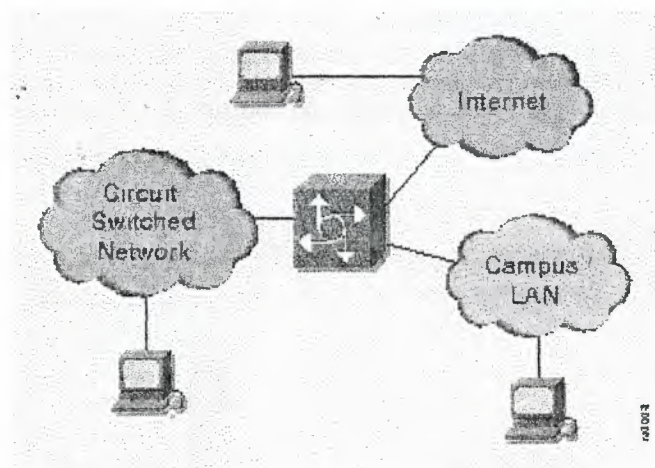


Figure 2.10: Illustrates a Generalized View of a PPP Environment

2.5.1 PPP Standards

PPP is defined using a number of International Organization for Standardization (ISO) standards:

- PPP uses the principles, terminology, and frame structure of the ISO HDLC procedures (ISO 3309-1979), as modified by ISO 3309:1984/PDAD1 "Addendum 1: Start/stop transmission."
- ISO 3309-1979 specifies the HDLC frame structure for synchronous environments.
- ISO 3309:1984/PDAD1 specifies proposed modifications to ISO 3309-1979 to permit asynchronous use.
- ISO 4335-1979 and ISO 4335-1979/Addendum 1-1979 specify control procedures.

2.5.2 PPP Hardware

PPP physical connections permit operation across any DTE/DCE interface, but require a duplex circuit that can operate in either asynchronous or synchronous bit-serial mode. PPP physical connection requirements do not impose any restrictions regarding transmission rate. Examples of supported physical interfaces include EIA/TIA-232-C, EIA/TIA-422, EIA/TIA-423, and V.35.

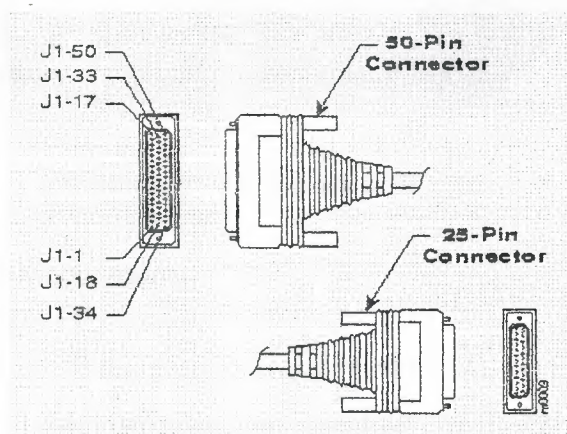


Figure 2.11: Illustrates 50-pin and 25-pin Connectors

2.5.3 PPP Operation

PPP datagram transmission employs three key components to provide effective data transmission:

Encapsulation -- PPP supports the High-Level Data Link Control (HDLC) protocol to provide encapsulation.

Link Control Protocol (LCP) -- An extensible LCP is used to establish, configure, and test the data link connection.

Network Control Protocols (NCPs) -- A family of NCPs are used to establish and configure different network layer protocols.

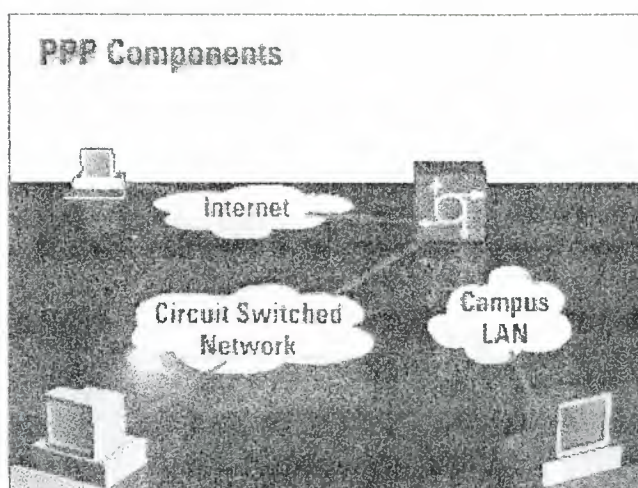


Figure 2.12: Illustrates the Relationships of Datagram Components

2.5.4 Establishing PPP Connections

PPP connections are established in stages. An originating PPP node first sends LCP frames to configure and optionally test the data link. Next, the link is established, and optional facilities are negotiated. The originating PPP node then sends NCP frames to choose and configure network layer protocols. The chosen network layer protocols are configured, and packets from each network layer protocol are sent.

2.5.5 PPP Link Negotiation

The PPP Link Control Protocol (LCP) provides a method of establishing, configuring, maintaining, and terminating the point-to-point connection. LCP goes through four distinct phases:

1. Link establishment and configuration negotiation
2. Link quality determination
3. Network layer protocol configuration negotiation
4. Link termination

2.5.5.1 Link Establishment and Configuration Negotiation

Before any network layer datagrams (for example, IP) can be exchanged, LCP must first open the connection and negotiate the configuration parameters. This phase is complete when a configuration acknowledgment frame has been both sent and received.

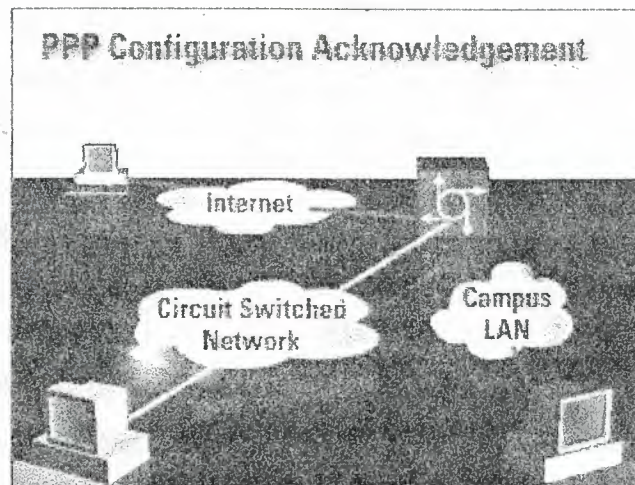


Figure 2.13: Illustrates this Process of Link Establishment

2.5.5.2 Link-Quality Determination

LCP allows an optional link-quality determination phase following the link establishment and configuration negotiation phase. In the link-quality determination phase, the link is tested to determine whether the link quality is sufficient to bring up network layer protocols. This phase is optional. LCP can delay transmission of network layer protocol information until this phase is completed.

2.5.5.3 Network Layer Protocol Configuration Negotiation

When LCP finishes the link-quality determination phase, network layer protocols can be separately configured by the appropriate NCP and can be brought up and taken down at any time. If LCP closes the link, it informs the network layer protocols so that they can take appropriate action.

2.5.5.4 Link Termination

LCP can terminate the link at any time. This will usually be done at the request of a user, but can happen because of a physical event such as the loss of carrier or the expiration of an idle-period timer.

2.6 Synchronous Data Link Control (SDLC)

The Synchronous Data Link Control (SDLC) protocol is a bit-synchronous data-link layer protocol developed by IBM Corp. SDLC was developed by IBM during the mid-1970s for use in Systems Network Architecture (SNA) environments. Subsequent to the implementation of SDLC by IBM, SDLC formed the basis for numerous similar protocols, including HDLC and LAPB. In general, bit-synchronous protocols have been successful because they are more efficient, more flexible, and in some cases faster than other technologies. SDLC is the primary SNA link layer protocol for wide-area network (WAN) links.

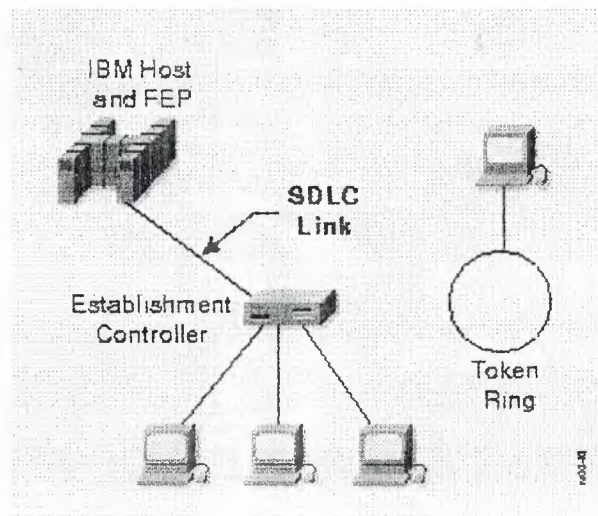


Figure 2.14: Illustrates the Relative Position of SDLC Links

2.6.1 Related Standards

SDLC was modified by the International Organization for Standardization (ISO) to create the High-Level Data Link Control (HDLC) protocol. HDLC was subsequently modified by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) to create Link Access Procedure (LAP) and then Link Access Procedure, Balanced (LAPB).

2.6.2 SDLC Environments

SDLC supports a range of link types and topologies, including the following:

- Point-to-point and multipoint links
- Bounded and unbounded media
- Half-duplex and full-duplex transmission facilities
- Circuit- and packet-switched networks

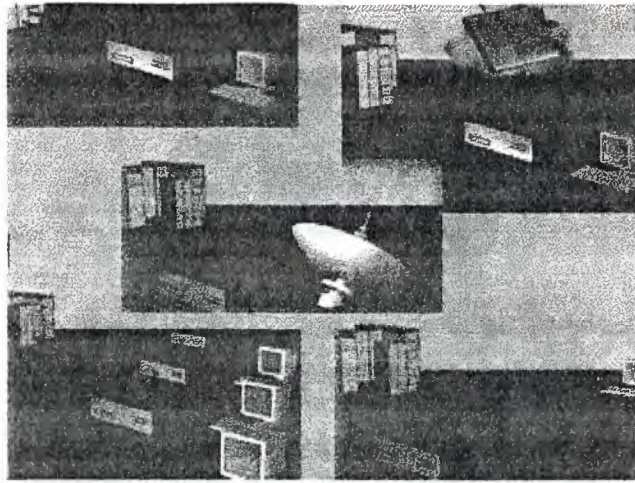


Figure 2.15: Illustrates SDLC Environments

2.6.3 SDLC Network Nodes

SDLC provides for two network node types:

SDLC primary stations -- Primary stations control the operation of other stations, poll secondaries in a predetermined order, and set up, tear down, and manage links.

SDLC secondary stations -- Secondary stations are controlled by a primary station. If a secondary is polled, it can transmit outgoing data. An SDLC secondary can send information only to the primary and only after the primary grants permission.

2.6.4 SDLC Node Configurations

SDLC supports four primary/secondary network configurations:

- Point-to-point
- Multipoint
- Loop
- Hub go-ahead

Point-to-Point -- A point-to-point link is the simplest of the SDLC arrangements. It involves only two nodes: one primary and one secondary.

Multipoint -- Multipoint or multi-drop configuration involves a single primary and multiple secondaries sharing a line. Secondaries are polled separately in a predefined sequence.

Loop -- An SDLC loop configuration involves a primary connected to the first and last secondaries in the loop. Intermediate secondaries pass messages through one another when responding to primary requests.

Hub Go-Ahead -- Hub go-ahead configurations involve inbound and outbound channels. The primary uses an outbound channel to communicate with secondaries. Secondaries use an inbound channel to communicate with the primary. The inbound channel is daisy-chained back to the primary through each secondary.

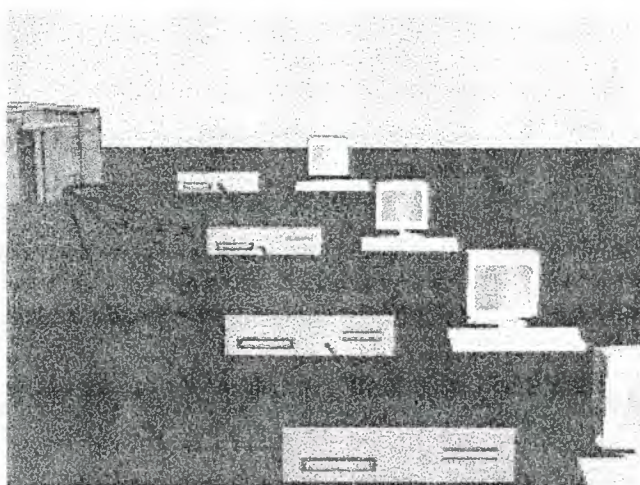


Figure 2.16: Illustrates the Operation in an SDLC Arrangement

2.6.5 Qualified Logical Link Control (QLLC)

The Qualified Logical Link Control (QLLC) protocol provides data link control capabilities required to transport SNA data across X.25 networks. It replaces SDLC in the SNA protocol stack over X.25 and uses the network layer of the X.25 protocol stack. With QLLC, the qualifier bit in the general format identifier (GFI) of the X.25 network layer packet-level header is set to one to indicate that the packet must be handled by QLLC. SNA data is carried as user data in network layer X.25 packets.

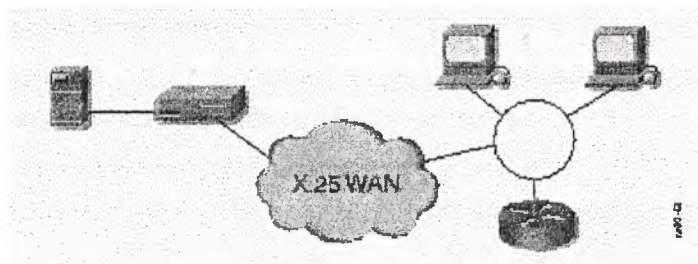


Figure 2.17: Illustrates a Typical X.25-based SNA Environment

2.6.6 Binary Synchronous Protocol

The Binary Synchronous Protocol (Bisync) is a byte-oriented, half-duplex, serial link protocol that predates SNA and SDLC. Bisync devices typically generate low traffic volumes and operate at line speeds of about 9600 bps. The maximum line speed support by Bisync is 19200 bps. Low line speeds and traffic volumes make Bisync applications good candidates for consolidation over multi-protocol networks. However, Bisync is not compatible with High-level Data Link Control (HDLC) and Synchronous Data Link Control (SDLC), the synchronous data-link protocols commonly supported by multi-protocol routers.

2.7 Switched Multimegabit Data Service (SMDS) Overview

Switched Multimegabit Data Service (SMDS) is a high-speed, packet-switched, datagram-based WAN networking technology used for communication over public data networks (PDNs). SMDS addresses two important trends in WAN technology: the proliferation of distributed processing and other applications requiring high-performance networking, and the decreasing cost and high-bandwidth potential of fiber media, which can support such applications over a WAN.

SMDS can use fiber- or copper-based media. It supports speeds of 1.544 Mbps over Digital Signal level 1 (DS-1) transmission facilities, or 44.736 Mbps over Digital Signal level 3 (DS-3) transmission facilities.

2.7.1 SMDS Network Components

There are three key components in SMDS networks:

Customer premises equipment (CPE) -- CPE is terminal equipment typically owned and maintained by the customer. CPE includes end devices, such as terminals and personal computers, and intermediate nodes, such as routers, modems, and multiplexers.

Carrier equipment -- Carrier equipment generally consists of high-speed WAN switches. Such switches must conform to certain network equipment specifications

Such specifications define network operations; the interface between a local carrier network and a long-distance carrier network; and the interface between two switches inside a single carrier network.

Subscriber Network Interface (SNI) -- The SNI is the interface between CPE and carrier equipment. This interface is the point at which the customer network ends, and the carrier network begins. The function of the SNI is to make the technology and operation of the carrier SMDS network transparent to the customer.

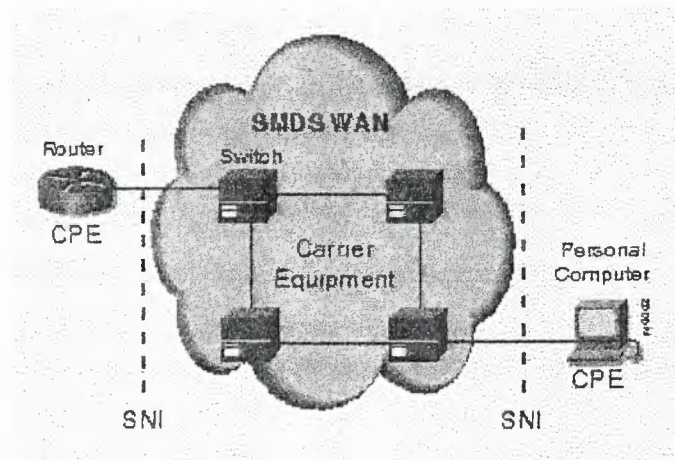


Figure 2.18: Shows the Relationship between Primary Components

2.7.2 SMDS Interface Protocol (SIP)

The SMDS Interface Protocol (SIP) is used for communications between CPE and SMDS carrier equipment. SIP provides connectionless service across the subscriber-network interface (SNI), allowing the CPE to access the SMDS network. SIP is based on the IEEE 802.6 Distributed Queue Dual Bus (DQDB) standard for cell relay across metropolitan-area networks (MANs). The Distributed Queue Dual Bus (DQDB) was chosen as the basis for SIP because it is an open standard that supports all of the SMDS service features. In addition, DQDB was designed for compatibility with current carrier transmission standards, and it is aligned with emerging standards for Broadband ISDN (BISDN), which will allow it to interoperate with broadband video and voice services.

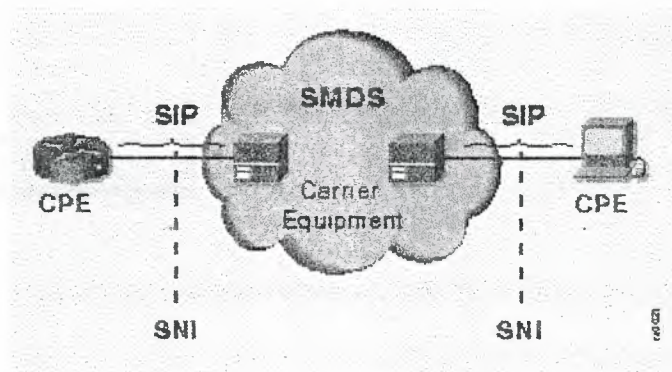


Figure 2.19: Shows where SIP is used in an SMDS Network:

2.7.3 SIP Levels

SIP consists of three levels:

- SIP Level 3

SIP Level 3 operates at the Media Access Control (MAC) sublayer of the data link layer of the OSI reference model.

- SIP Level 2

SIP Level 2 operates at the MAC sublayer of the data link layer.

- SIP Level 1

SIP Level 1 operates at the physical layer of the OSI reference model.

2.7.3.1 SIP Level 3 Operation

The SMDS Interface Protocol (SIP) is composed of three levels. SIP Level 3 operates at the Media Access Control (MAC) sublayer of the data link layer.

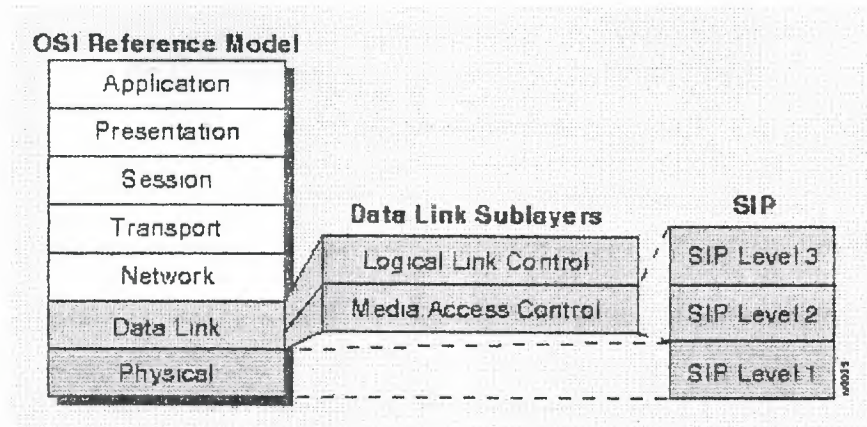


Figure 2.20: Maps the three SIP Levels to the OSI Reference Model

SIP Level 3 operates as follows:

1. User information is passed to SIP Level 3 in the form of SMDS service data units (SDUs).
2. SMDS SDUs are encapsulated in a SIP Level 3 header and trailer.
3. The resulting frame is called a Level 3 protocol data unit (PDU).
4. SIP Level 3 PDUs are subsequently passed to SIP Level 2.

2.7.3.2 SIP Level 2 Operation

The SMDS Interface Protocol (SIP) is composed of three levels. SIP Level 2 operates at the Media Access Control (MAC) sublayer of the data link layer.

SIP Level 2 operates as follows:

1. SIP Level 3 PDUs are passed to SIP Level 2.
2. The PDUs are segmented into uniformly sized (53-octet) Level 2 PDUs, called cells.
3. The cells are passed to SIP Level 1 for placement on the physical medium.

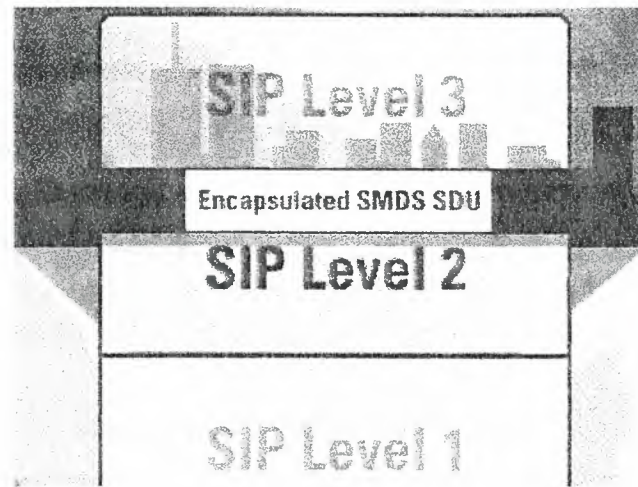


Figure 2.21: Shows the Basic Operation of SIP Level 2

2.7.3.3 SIP Level 1 Operation

The SMDS Interface Protocol (SIP) is composed of three levels. SIP Level 1 operates at the physical layer and provides the physical link protocol that operates at DS-1 or DS-3 rates between CPE devices and the network.

SIP Level 1 consists of two sublayers:

Transmission system sublayer -- This sublayer defines the characteristics and method of attachment to a DS-1 or DS-3 transmission link.

Physical Layer Convergence Protocol (PLCP) -- PLCP specifies how SIP Level 2 cells are to be arranged relative to the DS-1 or DS-3 frame. PLCP also defines other management information

2.7.4 SMDS Addressing

SMDS protocol data units (PDUs) carry both a source and a destination address. SMDS addresses are 10-digit values resembling conventional telephone numbers.

The SMDS addressing implementation offers two features:

- Group addressing
- Security features

2.7.4.1 SMDS Group Addressing

SMDS group addresses allow a single address to refer to multiple CPE stations.

A CPE station specifies the group address in the Destination Address field of the PDU. The network makes multiple copies of the PDU which are delivered to all of the members of the group.

Group addresses reduce the amount of network resources required for distributing routing information, resolving addresses, and dynamically discovering network resources.

SMDS group addressing is analogous to multicasting on LANs.

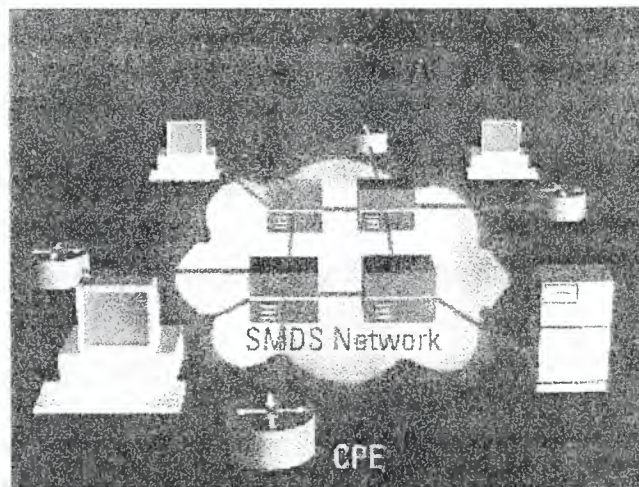


Figure 2.22: Shows SMDS Group Addresses

2.7.4.2 SMDS Addressing Security

SMDS implements two security features:

Source address validation -- This feature ensures that the PDU source address is legitimately assigned to the SNI from which it originated. Source address validation prevents address spoofing, in which illegal traffic assumes the source address of a legitimate device.

Address screening -- This feature allows a subscriber to establish a private virtual network that excludes unwanted traffic. If an address is disallowed, the data unit is not delivered.

2.8 X.25

X.25 is an ITU-T protocol standard for WAN communications. The X.25 standard defines how connections between user devices and network devices are established and maintained. X.25 is designed to operate effectively regardless of the type of systems connected to the network. It is typically used in the packet switched networks (PSNs) of common carriers (the telephone companies). Subscribers are charged based on their use of the network. At that time, there was a need for WAN protocols capable of providing connectivity across public data networks (PDNs). X.25 is now administered as an international standard by the ITU-T.

2.8.1 X.25 Network Components

X.25 network devices fall into three general categories:

Data terminal equipment (DTE) -- DTE devices are end systems that communicate across the X.25 network. They are usually terminals, personal computers, or network hosts, and are located on the premises of individual subscribers.

Data circuit-terminating equipment (DCE) -- DCE devices are special communications devices such as modems and packet switches. They provide the interface between DTE devices and a packet switching exchange (PSE), and are generally located in the carrier's facilities.

Packet switching exchanges (PSE) -- PSEs are switches that compose the bulk of the carrier's network. They transfer data from one DTE device to another through the X.25 packet switched network (PSN).

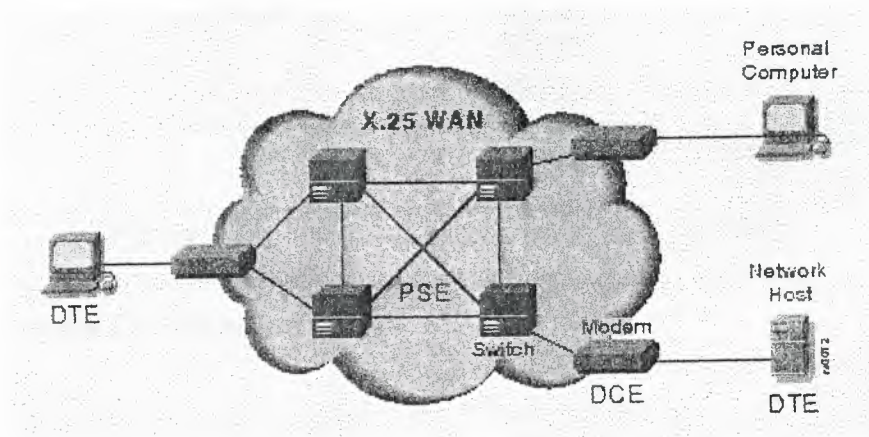


Figure 2.23: Shows the Relationship between X.25 Network Devices

2.8.2 Packet Assembler/Disassembler (PAD)

The packet assembler/disassembler (PAD) is a device commonly found in X.25 networks. PADs are used when a DTE device (such as a character-mode terminal) is too simple to implement the full X.25 functionality. The PAD is located between a DTE device and a DCE device. It performs three primary functions:

Buffering -- The PAD buffers data sent to or from the DTE device.

Packet assembly -- The PAD assembles outgoing data into packets and forwards them to the DCE device. (This includes adding an X.25 header.)

Packet disassembly -- The PAD disassembles incoming packets before forwarding the data to the DTE. (This includes removing the X.25 header.)

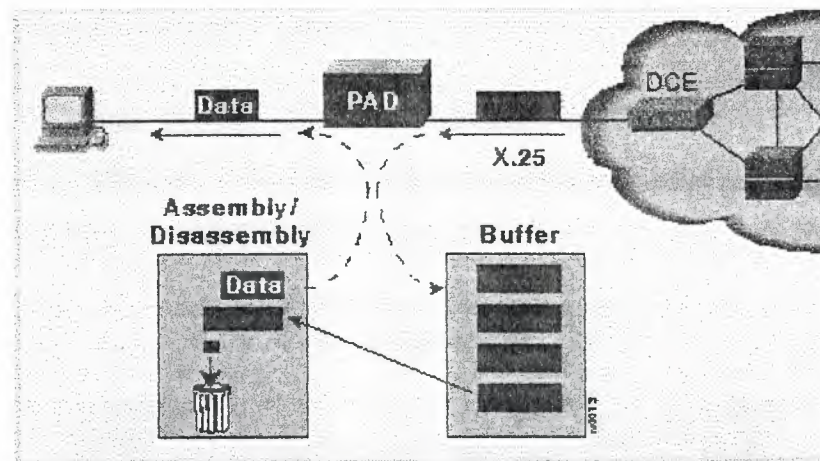


Figure 2.24: Shows the Basic Operation of the PAD

2.8.3 X.25 Session Establishment

X.25 sessions are established using the following process:

1. One DTE device contacts another to request a communication session.
2. The DTE device that receives the request can either accept or refuse the connection.
3. If the request is accepted, the two systems begin full-duplex information transfer.
4. Either DTE device can terminate the connection.

After the session is terminated, any further communication requires the establishment of a new session.

2.8.4 X.25 Virtual Circuit

A virtual circuit is a logical connection created to ensure reliable communication between two network devices. A virtual circuit denotes the existence of a logical, bidirectional path from one data terminal equipment (DTE) device to another across an X.25 network. Physically, the connection can pass through any number of intermediate

nodes, such as data circuit-terminating equipment (DCE) devices and packet switching exchanges (PSEs).

2.8.5 Virtual Circuits and Multiplexing

Multiple virtual circuits (logical connections) can be multiplexed onto a single physical circuit (a physical connection). Virtual circuits are demultiplexed at the remote end, and data is sent to the appropriate destinations.

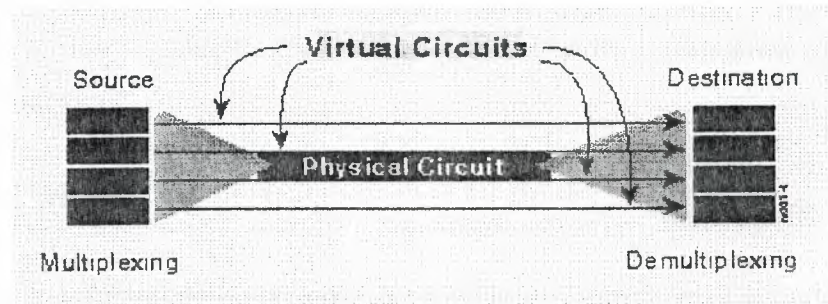


Figure 2.25: Shows Four Separate Virtual Circuits being multiplexed

3. NETWORK ESSENTIALS

This chapter explains about the network essentials. Network essentials are the things we must have to take care of to establish a good network between two or more networks. It include the OSI reference model which help in complete establishment of the network then we have protocols then we have WAN hardware all these things are very essential for a network

3.1 The OSI Model

OSI is a layer model Developed by ISO it is a seven layer architecture help in communication between two computers.

- International Standards Organization (ISO) specifications for network architecture.
- Called the Open Systems Interconnect or OSI model.
- Seven layered model, higher layers have more complex tasks.
- Each layer provides services for the next higher layer.
- Each layer communicates logically with its associated layer on the other computer.
- Packets are sent from one layer to another in the order of the layers, from top to bottom on the sending computer and then in reverse order on the receiving computer.

OSI Layers Names and a precise description is as follows

- Presentation
- Session
- Transport
- Network
- Data Link

- Network
- Data Link
- Physical

- Application Layer
 - Serves as a window for applications to access network services.
 - Handles general network access, flow control and error recovery.
- Presentation Layer
 - Determines the format used to exchange data among the networked computers.
 - Translates data from a format from the Application layer into an intermediate format.
 - Responsible for protocol conversion, data translation, data encryption, data compression, character conversion, and graphics expansion.
 - Redirector operates at this level.
- Session Layer
 - Allows two applications running on different computers to establish use and end a connection called a Session.
 - Performs name recognition and security.
 - Provides synchronization by placing checkpoints in the data stream.
 - Implements dialog control between communicating processes.
- Transport Layer
 - Responsible for packet creation.
 - Provides an additional connection level beneath the Session layer.
 - Ensures that packets are delivered error free, in sequence with no losses or duplications.
 - Unpacks, reassembles and sends receipt of messages at the receiving end.
 - Provides flow control, error handling, and solves transmission problems.

- Network Layer
 - Responsible for addressing messages and translating logical addresses and names into physical addresses.
 - Determines the route from the source to the destination computer.
 - Manages traffic such as packet switching, routing and controlling the congestion of data.
- Data Link Layer
 - Sends data frames from the Network layer to the Physical layer.
 - Packages raw bits into frames for the Network layer at the receiving end.
 - Responsible for providing error free transmission of frames through the Physical layer.
- Physical Layer
 - Transmits the unstructured raw bit stream over a physical medium.
 - Relates the electrical, optical mechanical and functional interfaces to the cable.
 - Defines how the cable is attached to the network adapter card.
 - Defines data encoding and bit synchronization.

3.2 Protocols

- Protocols are rules and procedures for communication.

3.2.1 How Protocols Work?

The Sending Computer does the following jobs

- Breaks data into packets.
- Adds addressing information to the packet
- Prepares the data for transmission.

The Receiving Computer does the following jobs

- Takes the packet off the cable.
- Strips the data from the packet.
- Copies the data to a buffer for reassembly.
- Passes the reassembled data to the application.

3.2.2 Protocol Stacks (or Suites)

- A combination of protocols, each layer performing a function of the communication process.
- Ensure that data is prepared, transferred, received and acted upon.

3.2.3 The Binding Process

- Allows more than one protocol to function on a single network adapter card. (e.g. both TCP/IP and IPX/SPX can be bound to the same card)
- Binding order dictates which protocol the operating systems uses first.
- Binding also happens with the Operating System architecture: for example, TCP/IP may be bound to the NetBIOS session layer above and network card driver below it. The NIC device driver is in turn bound to the NIC.

3.2.4 Standard Stacks

- ISO/OSI
- IBM SNA (Systems Network Architecture)
- Digital DECnet
- Novell NetWare
- Apple AppleTalk
- TCP/IP

Protocol types map roughly to the OSI Model into three layers:

Application Level Service Users

- Application Layer
- Presentation Layer
- Session Layer

Transport Services

- Transport Layer

Network Services

- Network Layer
- Data Link Layer
- Physical Layer

3.2.5 The IEEE protocols at the Physical Layer

3.2.5.1 802.3 (CSMA /CD - Ethernet)

- logical bus network
- can transmit at 10 Mbps
- data is transmitted on the wire to every computer but only those meant to receive respond
- CSMA /CD protocol listens and allows transmission when the wire is clear

3.2.5.2 802.4 (Token Passing)

- bus layout that used token passing
- every computer receives all of the data but only the addressed computers respond
- token determines which computer can send

3.2.5.3 802.5 (Token Ring)

- logical ring network; physical set up as star network
- transmits at 4 Mbps or 16 Mbps
- token determines which computer can send

3.3 Important Protocols

3.3.1 TCP/IP

- Provides communications in a heterogeneous environment.
- Routable, defacto standard for internetworking.
- SMTP, FTP, SNMP are protocols written for TCP/IP
- Disadvantages are size and speed.

3.3.2 NetBEUI

- NetBIOS extended user interface.
- Originally, NetBIOS and NetBEUI were tightly tied together but, NetBIOS has been separated out to be used with other routable protocols. NetBIOS acts as a tool to allow applications to interface with the network; by establishing a session with another program over the network
- NetBIOS operates at the Session layer.
- Small, fast and efficient.
- Compatible with most Microsoft networks.
- Not routable and compatible only with Microsoft networks.

3.3.3 X.25

- Protocols incorporated in a packet switching network of switching services.
- Originally established to connect remote terminals to mainframe hosts.

3.3.4 XNS

- Xerox Network System.
- Developed for Ethernet LANs but has been replaced by TCP/IP.
- Large, slow and produces a lot of broadcasts.

3.3.5 IPX/SPX and NWLink

- Used for Novell networks.
- Small and fast.
- Routable.

3.3.6 APPC

- Advanced Program to Program Communication
- Developed by IBM to support SNA.
- Designed to enable application programs running on different computers to communicate and exchange data directly.

3.3.7 AppleTalk

- Apple's proprietary protocol stack for Macintosh networks.

3.3.8 OSI Protocol Suite

- each protocol maps directly to a single layer of the OSI model

3.3.9 DECnet

- Digital Equipment's proprietary protocol stack
- Defines communications over Ethernet, FDDI MAN's and WAN's.
- DECnet can also use TCP/IP and OSI protocols as well as its own protocols
- Routable.

3.4 Network Architectures

3.4.1 Ethernet

- Baseband signaling.
- Linear or star-bus topology.
- Usually transmits at 10 Mbps with 100 Mbps possible.
- Uses CSMA/CD for traffic regulation.
- IEEE specification 802.3.
- Uses thicknet, thinnet or UTP cabling
- Media is passive => it draws power from the computer

3.4.2 Ethernet Frames

Ethernet breaks data into frames. A frame can be from 64 to 1,518 bytes long in total. The Ethernet frame itself takes up 18 bytes, so the actual data can be from 46 to 1,500 bytes.

- Preamble: marks the start of a frame.
- Destination and Source: addressing information.
- Type: Identifies network layer protocol.
- CRC: error checking data.

3.5 Network Hardware

Some components can be installed which will increase the size of the network within the confines of the limitations set by the topology. These components can:

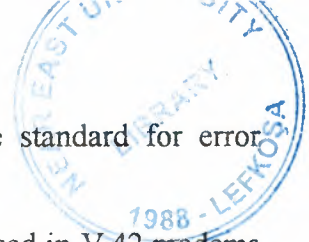
- Segment existing LANs so that each segment becomes its own LAN.
- Join two separate LANs.
- Connect to other LANs and computing environments to join them into a larger comprehensive network.

3.5.1 Modems

- Modems share these characteristics
 - a serial (RS-232) interface
 - an RJ-11C telephone line connector
- Telephones use analog signal; computers use digital signal. A modem translates between the two
- BAUD refers to the speed of the oscillation of the sound wave on which a bit of data is carried over the telephone wire
- The BPS can be greater than the baud rate due to compression and encode data so that each modulation of sound can carry more than one bit of data is carried over the telephone line. For example, a modem that modulates at 28,000 baud can actually send at 115,200 bps => bps is the most important parameter when looking at throughput.
- There are 2 types of modems

3.5.1.1 Asynchronous Communications (Async)

- use common phone lines
- data is transmitted in a serial stream
- not synchronized, no clocking device => no timing
- both sending and receiving devices must agree on a start and stop bit sequence
- error control
 - a parity bit is used in an error checking and correction scheme called parity checking
 - It checks to see if the # of bits sent = # of bits received
 - The receiving computer checks to make sure that the received data matches what was sent.
 - 25 % of the data traffic in async communications consists of data control and coordination

- 
- MNP (Microcom Network Protocol) has become the standard for error control
 - Later LAPM (Link Access Procedure for Modems) is used in V.42 modems (57,600 baud).
 - It uses MNP Class 4.
 - LAPM is used between two modems that are V.42 compliant
 - If one or the other modems is MNP 4 - compliant, the correct protocol would be MNP Class 4
 - Communication performance depends on
 1. signaling or channel speed - how fast the bits are encoded onto the communications channel
 2. throughput - amount of useful information going across the channel
 - You can double the throughput by using compression. One current data compression standard is the MNP Class 5 compression protocol
 - V.42 bis is even faster because of compression.
 - bis => second modification
 - terbo => third, the bis standard was modified
 - This is a good combination:
 0. V.32 signaling
 1. V.42 error control
 2. V.42bis compression

3.5.1.2 Synchronous Communication

- relies on a timing scheme coordinated between two devices to separate groups of bits and transmit them in blocks known as frames
- NO start and stop bits =. A continuous stream of data because both know when the data starts and stops.
- if there's error, the data is retransmitted
- some synchronous protocol perform the following that asynchronous protocols don't:
 1. format data into blocks

2. add control info
 3. check the info to provide error control
- the primary protocols in synchronous communication are:
 1. Synchronous data link control (SDLC)
 2. High-level data link control (HDLC)
 3. binary synchronous communication protocol (bisync)
 - Synchronous communications are used in almost all digital and network communications
 - 2 types of telephone lines:
 1. public dial network lines (dial-up lines) - manually dial up to make a connection
 2. leased (dedicated) lines - full time connection that do not go through a series of switches, 56 Kbps to 45 Mbps

3.5.2 Repeaters

- Repeaters
 - EXTEND the network segment by REGENERATING the signal from one segment to the next
 - Repeaters regenerate BASEBAND, digital signals
 - don't translate or filter anything
 - ~~is the least expensive alternative~~
 - work at the Physical layer of OSI
- Both segments being connected must use the same access method e.g. an 802.3 CSMA/CD (Ethernet) LAN segment can't be joined to an 802.5 (Token Ring) LAN segment. Another way of saying this is the Logical Link Protocols must be the same in order to send a signal.
- BUT repeaters CAN move packets from one physical medium to another: for example can take an Ethernet packet from a thinnet coax and pass it on to a fiber-optic segment. Same access method is being used on both segments, just a different medium to deliver the signal

- There are limits on the number of repeaters which can be used. The repeater counts as a single node in the maximum node count associated with the Ethernet standard [30 for thin coax].
- Repeaters also allow isolation of segments in the event of failures or fault conditions. Disconnecting one side of a repeater effectively isolates the associated segments from the network.
- Using repeaters simply allows you to extend your network distance limitations. It does not give you any more bandwidth or allow you to transmit data faster.
- Why only so many repeaters are allowed on a single network: "propagation delay". In cases where there are multiple repeaters on the same network, the brief time each repeater takes to clean up and amplify the signal, multiplied by the number of repeaters can cause a noticeable delay in network transmissions.
- It should be noted that in the above diagram, the network number assigned to the main network segment and the network number assigned to the other side of the repeater are the same.
- In addition, the traffic generated on one segment is propagated onto the other segment. This causes a rise in the total amount of traffic, so if the network segments are already heavily loaded, it's not a good idea to use a repeater.
- A repeater works at the Physical Layer by simply repeating all data from one segment to another.

3.5.2.1 Repeater features

- increase traffic on segments
- limitations on the number that can be used
- propagate errors in the network
- cannot be administered or controlled via remote access
- no traffic isolation or filtering

3.5.3 Bridges

- have all the abilities of a repeater
- Bridges can
 - take an overloaded network and split it into two networks, therefore they can divide the network to isolate traffic or problems and reduce the traffic on both segments
 - expand the distance of a segment
 - link UNLIKE PHYSICAL MEDIA such as twisted-pair (10Base T) and coaxial Ethernet (10Base2)
 - VERY IMPORTANT: they can link UNLIKE ACCESS CONTROL METHODS, on different segments such as Ethernet and Token Ring and forward packets between them. Exam Cram says this is a Translation Bridge that can do this - not all bridges - but my observation is questions don't necessarily mention the distinction.
- Bridges work at the Data Link Layer of the OSI model => they don't distinguish one protocol from the next and simply pass protocols along the network. (use a bridge to pass NetBEUI, a non-routable protocol, along the network)
- Bridges actually work at the MEDIA ACCESS CONTROL (MAC) sublayer. In fact they are sometimes called Media Access Control layer bridges. Here's how they deal with traffic:
 - They listen to all traffic. Each time the bridge is presented with a frame, the source address is stored. The bridge builds up a table which identifies the segment to which the device is located on. This internal table is then used to determine which segment incoming frames should be forwarded to. The size of this table is important, especially if the network has a large number of workstations/servers.
 - they check the source and destination address of each PACKET
 - They build a routing table based on the SOURCE ADDRESSES. Soon they know which computers are on which segment
 - Bridges are intelligent enough to do some routing:

- If the destination address is on the routing table and is on the SAME SEGMENT, the packet isn't forwarded. Therefore, the bridge can SEGMENT network traffic
- If the destination address is the routing table, and on a remote segment, the bridge forwards the packet to the correct segment
- If the destination address ISN'T on the routing table, the bridge forwards the packet to ALL segments.
- BRIDGES SIMPLY PASS ON BROADCAST MESSAGES, SO they too contribute to broadcast storms and don't help to reduce broadcast traffic
- Remote Bridges
 - two segments are joined by a bridge on each side, each connected to a synchronous modem and a telephone line
 - there is a possibility that data might get into a continuous loop between LANs
 - The SPANNING TREE ALGORITHM (STA)
 - senses the existence of more than one route
 - determines which is the most efficient and
 - configures the bridge to use that route
 - This route can be altered if it becomes unusable.
 - Transparent bridges (also known as spanning tree, IEEE 802.1 D) make all routing decisions. The bridge is said to be transparent (invisible) to the workstations. The bridge will automatically initialize itself and configure its own routing information after it has been enabled.
- Comparison of Bridges and Repeaters
 - Bridges
 - regenerate data at the packet level
 - accommodate more nodes than repeaters
 - provide better network performance than repeaters because they segment the network

- Implementing a Bridge
 - it can be an external, stand-alone piece of equipment
 - or be installed on a server

3.5.4 Routers

- Determine the best path for sending data and filtering broadcast traffic to the local segment. They DON'T pass on broadcast traffic
- work at the Network layer of OSI => they can switch and route packets across network segments
- They provide these functions of a bridge
 - filtering and isolating traffic
 - connecting network segments
- routing table contains
 1. all known network addresses
 2. how to connect to other networks
 3. possible paths between those routers
 4. costs of sending data over those paths
 5. not only network addresses but also media access control sublayer addresses for each node
- Routers
 - REQUIRE specific addresses: they only understand network numbers which allow them to talk to other routers and local adapter card addresses
 - Only pass Packets to the network segment they are destined for.
 - routers don't talk to remote computers, only to other routers
 - they can segment large networks into smaller ones
 - they act as a safety barrier (firewall) between segments
 - they prohibit broadcast storms, because broadcasts and bad data aren't forwarded
 - are slower than most bridges
 - can join dissimilar access methods: a router can route a packet from a TCP/IP Ethernet network to a TCP/IP Token Ring network

- Routers don't look at the destination computer address. They only look at the NETWORK address and they only pass on the data if the network address is known
=> less traffic
- Ratable protocols:
 - DECnet, IP, IPX, OSI, XNS, DDP (Apple)
 - Ratable protocols have Network layer addressing embedded
- Non-ratable protocols:
 - LAT, NetBEUI, DLC
 - Non-ratable protocols don't have network layer addressing

3.5.4.1 Choosing Paths

- routers can choose the best path for the data to follow
- Routers can accommodate multiple active paths between LAN segments. To determine the best path, it takes these things into account:
 - If one path is down, the data can be forwarded over on alternative route
 - Routers can listen and determine which parts of the network are busiest.
 - it decides the path the data packet will follow by determining the number of hops between internetwork segments
- OSPF (Open Shortest Path First)
 - is a link-state routing algorithm
 - routes are calculated based on
 - # of hops
 - line speed
 - traffic
 - cost
 - TCP/IP supports OSPF
- RIP (Routing Information Protocol)
 - RIP is the protocol used to determine the # of hops to a distant segment.
 - uses distance-vector algorithm to determine routes
 - TCP/IP & IPX support RIP

- NLSP (NetWare Link Services Protocol)
 - is a link-state algorithm for use with IPX
- There are 2 types of routers
 - Static - manually setup and configure the routing table and to specify each route
 - Dynamic
 - automatic discovery of routers
 - use information from other routers

3.5.5 Brouters

- Combine the best qualities of both bridges and routers
- First, a brouter checks to see if the protocol is routable or non-routable
- Route selected routable protocols.
- They can bridge non-routable protocols. Like a Bridge, they use the MAC address to forward to destination. They act like a router for one protocol and a bridge for all the others
- More cost effective than individual bridges and routers.
- SO, use a brouter when you have routable and non-routable protocols.

3.5.6 Hubs

There are many types of hubs:

- Passive hubs are don't require power and are simple splitters or combiners that group workstations into a single segment
- Active hubs require power and include a repeater function and are thus capable of supporting many more connections.
- Intelligent hubs provide
 - packet switching
 - traffic routing

3.5.7 Gateways

- The TRANSLATOR -- allows communications between dissimilar systems or environments
- A gateway is usually a computer running gateway software connecting two different segments. For example an Intel-based PC on one segment can both communicate and share resources with a Macintosh computer or an SNA mainframe. Use gateways when different environments need to communicate. One common use for gateways is to translate between personal computers and mainframes
- GSNW is a gateway to allow Microsoft clients using SMB to connect to a NetWare server using NCP.
- Gateways work at the Application --> Transport layer
- They make communication possible between different architectures and environments
- They perform protocol AND data conversion / translation.
- they takes the data from one environment, strip it, and re-package it in the protocol stack from the destination system
- they repackaging and convert data going from one environment to another so that each environment can understand the other environment's data
- gateway links two systems don't use the same
 1. protocols
 2. data formatting structure
 3. languages
 4. architecture
- they are task specific in that they are dedicated to a specific type of conversion: e.g. "Windows NT Server -> SNA Server Gateway"
- Usually one computer is designated as the gateway computer. This adds a lot of traffic to that segment
- Disadvantages
 - They slow things down because of the work they do
 - they are expensive
 - difficult to configure

- Remember, gateways can translate
 - protocols e.g. IPX/SPX --> TCP/IP
 - and data (PC --> Mac)
 - E-mail standards --> an e-mail gateway that translates on e-mail format into another (such as SMTP) to route across the Internet.

3.6 WAN Transmission

Communication between LANs over a WAN link will involve one of these technologies

- Analog
 - These use conventional telephone lines, with voice signaling (modem) technologies
- Digital
 - These use digital grade telephone lines, with digital technologies all the way
- Packet Switching
 - These use multiple sets of links between sender and receiver to move data

3.6.1 Analog

- dial-up line
 - via public switched telephone network (PSTN)
 - requires modems which are slow
 - inconsistent quality of service
- dedicated line
 - fast
 - reliable
 - expensive
 - service provider can implement line conditioning (a service that reduces delay and noise on the line, allowing for better transmissions) can make the leased lines even more reliable,

- Digital Data Service (DDS) provide point-to-point synchronous communications at:
 - 2.4 Kbps
 - 4.8 Kbps
 - 9.6 Kbps or
 - 56 Kbps
- guarantees full-duplex bandwidth by setting up a permanent link from each endpoint
- 99% error free
- Doesn't requires modem, requires bridge or router through a device called a CSU/DSU. This device translates standard digital signals a computer generates into bipolar digital signals used by synchronous communications
- Available in several forms:

3.6.3 T1

- Point to point transmission => no switching
- uses two-wire pairs (1 pair to send, 1 to receive)
- full-duplex signal at 1.544 Mbps
- Used to transmit digital, voice, data and video signals
- multiplexing - signals from different source are collected into a component called a multiplexer and fed into one cable 8,000 times a second
- A T1 divides into 24 64 Kbps channels. Subscribers can lease one 64 Kbps channel known as a Fractional T-1.
 - Each channel can transmit at 64 Kbps. This is called a DS-0
 - the whole 1.544 Mbps is known as DS-1
- Connecting a T1 line to your network is similar to a connecting a DDS or frame relay line. You will need a T1-compatible CSU/DSU, and a bridge or router. To distribute the T1's bandwidth between voice and data traffic, you will need a multiplexer/demultiplexer to combine voice and data signals for transmission, and separate them upon reception.

3.6.4 T3

- equivalent to 28 T-1 lines
- T3 and Fractional T-3 leased line service provides voice and data service from 6 Mbps to 45 Mbps
- REALLY expensive
- T-1 uses copper wire, while T-3 uses fiber optic cables or microwave transmission equipment.

3.6.5 Switched 56

- In reality, a Switched 56 line is nothing more than a circuit-switched version of a standard 56 Kbps DDS leased line. As customers pay only for connection time, resulting costs are usually significantly lower than those of a dedicated line.
- is a LAN to LAN digital dial-up service
- 56 Kbps
- Used on demand => not dedicated => less expensive.
- Both ends must be equipped with a Switched 56 compatible CSU/DSU to dial-up another switched 56 site.

3.6.6 Packet Switching

- Switching (as in switched connections) refers to finding a path for data transmission across a number of potential links between sender and receiver.
- On the other hand, analog and digital connections require a fixed connection to exist, at least for the duration of each communication session. Switching methods include both circuit switching and packet switching. Essentially, when data is received on an incoming line, the switching device must find an appropriate outgoing line on which to forward it. These switching devices are usually called routers, based on the functions they perform.
- Data package is broken into packets and each package is tagged with a destination address and other info.
- relayed through stations in a computer network

- Data paths for individual packets depend on the best route at any given instant. The main point is that the small, individual packets ~~are all~~ take their own route to the destination, and an error in any one of them is easier to correct than a huge chunk of data
- These networks are sometimes called "any to any networks"
- Can use a virtual circuit
 - logical connection between the sending computer and the receiving computer
 - not actual cable, but bandwidth used on demand
 - Can use a Switched Virtual Circuit to establish a connection over a specific route.
 - Permanent Virtual Circuits allow the customer to pay for only the time that the line is used.

3.6.7 Fiber Distributed Data Interface (FDDI)

- 100 Mbps token passed ring network that uses Fiber optic cable
- used for Metropolitan Area Networks (MAN) to connect within the same city so this isn't really a WAN technology
- 100 km (62 miles) max. length => not really a WAN technology
- FDDI uses fiber optic cable to serve as
 - "backend network" that handle file transfer
 - serve as a backbone for other low capacity LANs
 - LANs that require large bandwidth
 - Video
 - CAD
 - CAM
- Token Passing
 - not the same as token passing in 802.5
 - Here a computer can transmit as many frames as it can produce within a predetermined time before letting the token go. When it is finished transmitting, it lets the token go.

- Because the computer releases the token when it's finished, there may be several frames on the ring at once.
- FDDI is not like a regular Token Ring network because more than one computer at a time can transmit a token so that multiple tokens can circulate on the ring at any one time.
- This is why FDDI is faster than regular Token Ring 802.5 => 802.5 only allows one token at a time to transmit.
- Topology
 - dual-ring
 - primary ring is for traffic; a redundant second ring for backup
 - when the primary ring breaks down, the secondary ring reconfigures itself and flows in the opposite direction
 - REDUNDANCY is one of the key features of this technology.
 - 500 computers max.
 - more than one computer can transmit at a time - they share the bandwidth; for example, when 10 computers transmit, each does so at 10 Mbps
 - there must be a repeater every 2 Kms or less
 - Computers connected to both rings are CLASS A stations and help to reconfigure the network if the first ring fails. CLASS B stations are only connected to the one, primary ring.
 - FDDI can have point-to-point links to a hub => it can be set up using a star ring topology
- Beaconsing
 - all computers on an FDDI network are responsible for monitoring faults in the network
 - A computer that detects a fault sends a signal called a BEACON onto the network. If it sees its upstream neighbor is sending a beacon it stops. This goes on until the only computer sending a beacon is the one directly downstream from the faulty computer. This process stops when a beaconsing computer receives its own beacon => this means the beacon made it around the ring

- Media

- FDDI uses fiber-optic. This means
 - immune to electromagnetic interference
 - secure because fiber optic doesn't emit a signal that can be monitored and cannot be tapped
 - able to transmit long distances before needing a repeater
- FDDI on copper wire is called CDDI => can be done, but it has FAR less distance

4. ROUTING

4.1 Overview

In this chapter the complete detail of the router and its operation and how it routes the data on the internet is explained in detail. A router is simply a device that routes the data. It is used where we have more than two networks are joined. It has some specific protocols. Routing is a process by which router routes the data.

4.2 Router

A router is an Intermediate System (IS) which operates at the network layer of the OSI reference model. Routers may be used to connect two or more IP networks, or an IP network to an internet connection. A router consists of a computer with at least two network interface cards supporting the IP protocol. The router receives packets from each interface via a network interface and forwards the received packets to an appropriate output network interface. Received packets have all link layer protocol headers removed, and transmitted packets have a new link protocol header added prior to transmission.

The router uses the information held in the network layer header (i.e. IP header) to decide whether to forward each received packet, and which network interface to use to send the packet. Most packets are forwarded based on the packet's IP destination address, along with routing information held within the router in a routing table. Before a packet is forwarded, the processor checks the Maximum Transfer Unit (MTU) of the specified interface. Packets larger than the interface's MTU must be fragmented by the router into two or more smaller packets. If a packet is received which has the Don't Fragment (DF) bit set in the packet header, the packet is not fragmented, but instead discarded. In this case, an ICMP error message is returned to the sender (i.e. to the original packet's IP source address) informing it of the interface's MTU size. This forms the basis for Path MTU discovery

(PMTU). The routing and filter tables resemble similar tables in link layer bridges and switches. Except, that instead of specifying link hardware addresses (MAC addresses), the router table specify network (IP addresses). The routing table lists known IP destination addresses with the appropriate network interface to be used to reach that destination. A default entry may be specified to be used for all addresses not explicitly defined in the table. A filter table may also be used to ensure that unwanted packets are discarded. The filter may be used to deny access to particular protocols or to prevent unauthorized access from remote computers by discarding packets to specified destination addresses. A router forwards packets from one IP network to another IP network. Like other systems, it determines the IP network from the logical AND of an IP address with the associated subnetwork address mask. One exception to this rule is when a router receives an IP packet to a network broadcast address. In this case, the router discards the packet. Forwarding broadcast packet can lead to severe storms of packets, and if uncontrolled could lead to network overload.

A router introduces delay (latency) as it processes the packets it receives. The total delay observed is the sum of many components including:

- Time taken to process the frame by the data link protocol
- Time taken to select the correct output link (i.e. filtering and routing)
- Queuing delay at the output link (when the link is busy)
- Other activities which consume processor resources (computing routing tables, network management, generation of logging information)

The router queue of packets waiting to be sent also introduces a potential cause of packet loss. Since the router has a finite amount of buffer memory to hold the queue, a router which receives packets at too high a rate may experience a full queue. In this case, the router has no other option than to simply discard excess packets. If required, these may later be retransmitted by a transport protocol.

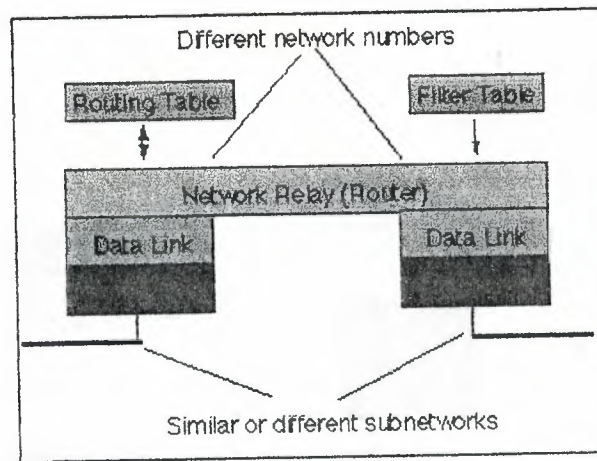


Figure 4.1: Shows Architecture of a router

Routers are often used to connect together networks which use different types of links (for instance an HDLC link connecting a WAN to a local Ethernet LAN). The optimum (and maximum) packet lengths (i.e. the Maximum Transfer Unit (MTU) is different for different types of network. A router may therefore use IP to provide segmentation of packets into a suitable size for transmission on a network. Associated protocols perform network error reporting (ICMP), communication between routers (to determine appropriate routes to each destination) and remote monitoring of the router operation (network management).

4.3 Operation of a Router

A modern router is a complex piece of equipment. The outside of the equipment is usually very simple, consisting of a number of network interface ports (shown on the left in orange in the figure 4.2) to which cables may be connected and a few indicator lights to indicate that the router is functional.

Most routers also have a serial connector to which a terminal (or a modem) may be connected, known as the "Console Port" (shown to the right in the figure 4.2). This port is usually used to control the router configuration when the router is first installed. It may be the only port which is allowed to configure the filter table (used to prevent unauthorized access between the connected networks).

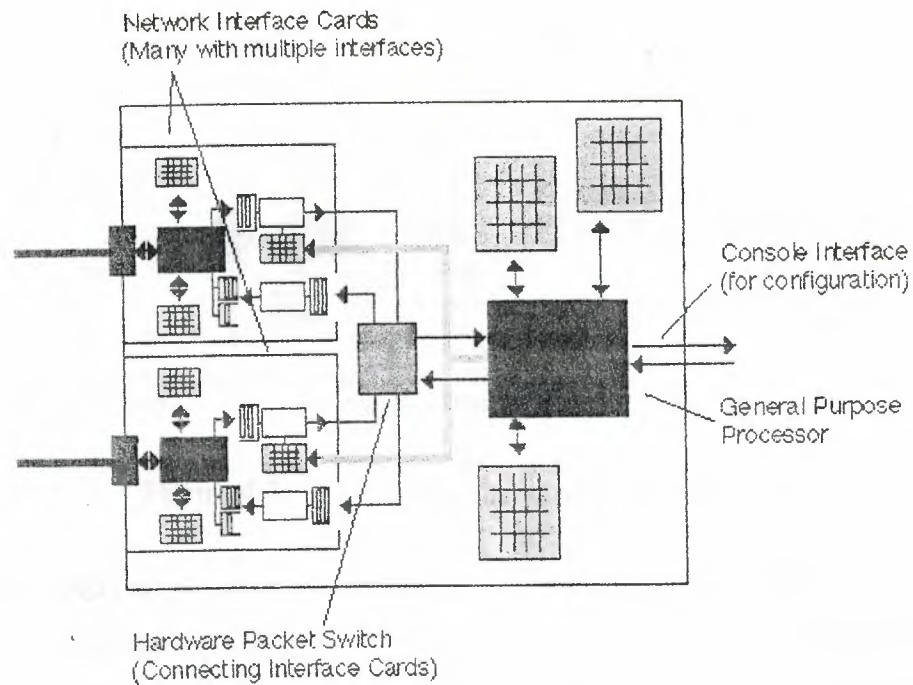


Figure 4.2: Block Diagram of a Complete Router Showing

In the simplest case, the processing of packets is implemented in the general purpose processor which implements all the algorithms. More advanced routers may separate "forwarding" (the tasks of moving packets from one interface to another) from "routing" (the task of determining the best path through the network) and include a number of processors capable of performing these tasks. A router interface card resembles the LAN Network Interface Cards (NICs) used in PCs except that the card is normally of a higher specification (faster packet processing). The very first routers were designed used standard network interface cards, but modern high performance routers use special high performance interface cards and may also include a "Forwarding Engine" on-board the card which speeds the operation.

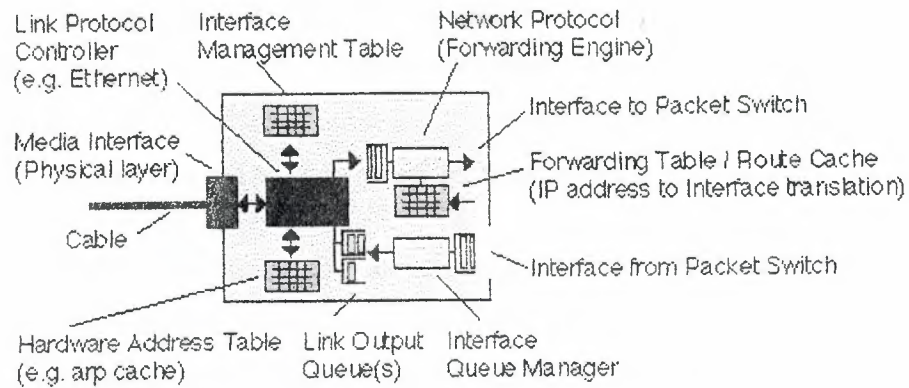


Figure 4.3: Shows a Router Network Interface Card

Received packets are processed by the link layer protocol controller, which handles the link layer protocol (e.g. HDLC, Ethernet) used over the physical link (cable). This also checks the received frame integrity (size, checksum, address, etc). Valid frames are converted to packets by removing the link layer header and are queued in the receive queue. This is usually a First-In-First-Out (FIFO) queue, often in the form of a ring of memory buffers.

The buffers are passed (drained) into the input to the forwarding engine. This takes each buffer, one at a time, and removes it from the interface receiver. The packet is then forwarded to an appropriate output interface, corresponding to the "best" path to the destination specified in the destination address of the IP packet header.

At the output interface, the packet (together with a new link layer header) is placed into a transmit queue until the link layer processor is ready to transmit the packet. This, like the receive queue, is a FIFO queue, and usually also takes the form of a ring of memory buffers.

Each out-going packet requires a new link layer protocol header to be added (encapsulation) with the destination address set to the next system to receive the packet. The link protocol controller also maintains the hardware address table associated with the interface. This usually involves using the Address Resolution Protocol (arp) to find out the hardware (Medium Access Control) addresses of other computers or routers directly

connected to the same cable (or LAN). The packet is finally sent using the media interface with the hardware address set to the next hop system. When complete, the buffer (memory) allocated to the frame, is "freed", that is, it is returned as an empty buffer to the receive queue, where it may be used to store a new received packet.

You may think from this that the job of forwarding is not too difficult, and involves a lot of copying of the packet data from one place to another. You would be wrong on both counts! Forwarding actually involves lots of decisions. Modern routers avoid copying the data in a packet if at all possible - this is a significant processing cost, and may easily slow down a router to a very low throughput. Instead, where ever possible, the router will leave the packet data in the same place and instead pass information about where a packet is stored in memory.

4.3.1 Forwarding

This section gives a simple description of the forwarding process. After determining the link layer frame is valid, the forwarding engine then starts processing the network layer information. It reads the network layer (IP) packet headers and checks various parts of the header, to ensure the packet is not damaged or illegal. It then uses a local Forwarding Table (known as the "Forwarding Information Base (FIB)") to identify where in the network the packet should be routed to (i.e. which output interface should be used).

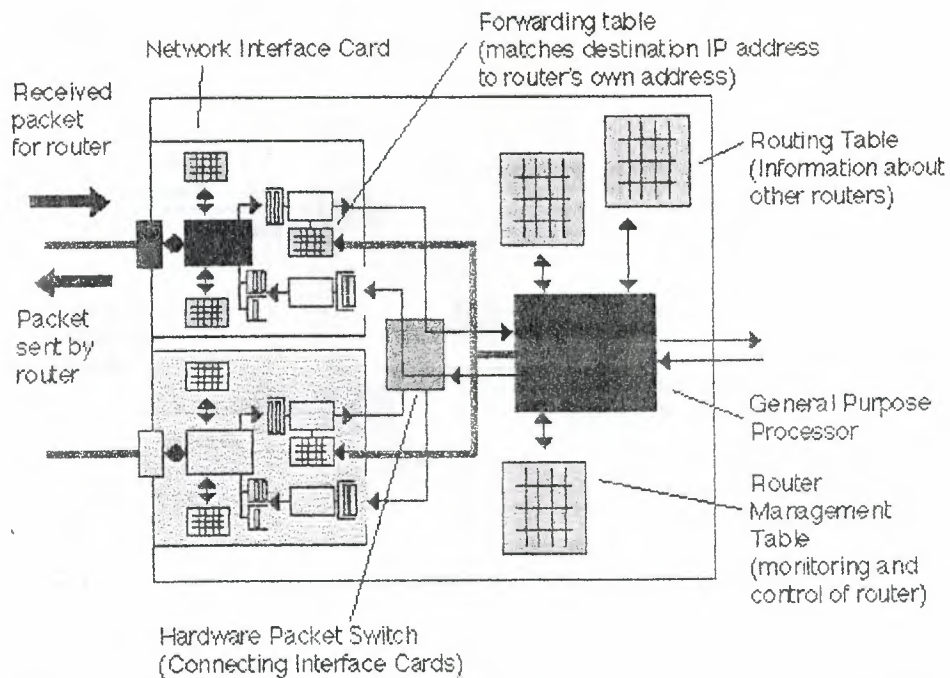


Figure 4.4: Forwarding of a Received Packet to an Output Interface

Once the appropriate output interface has been identified, the forwarding engine then requests the packet switch to form a connection to the appropriate output interface. The packet is then moved through the router to the output network interface controller. Although large routers actually implement a switch as a hardware component, smaller routers do not actually contain a "real" switch. In other routers, the switch takes the form of a shared memory data structure in which all received packets are stored. The switching operation therefore consists of removing a pointer from the receive queue, and copying the value of the pointer to the appropriate transmit queue. In some cases, the entire packet data is copied from one bank of receive memory to another transmit memory using a computer bus.

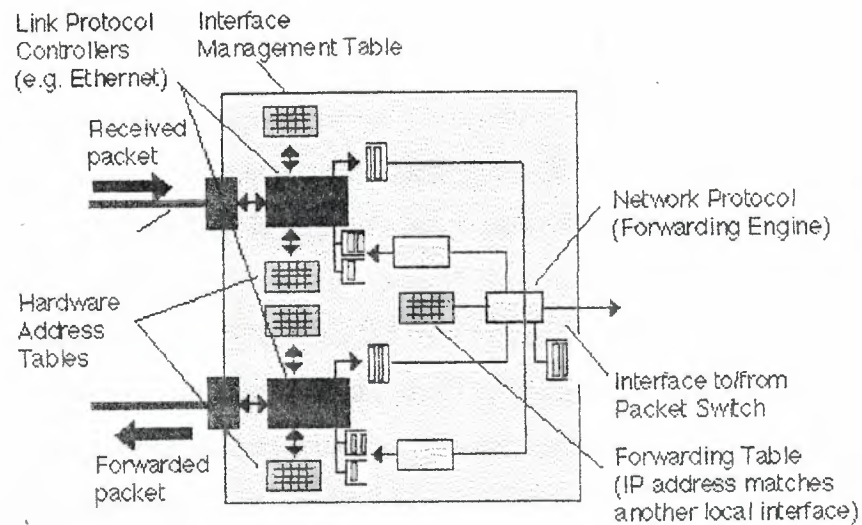


Figure 4.5: Shows Forwarding of a Packet

Packets may be directly forwarded from one controller to the other (sometimes known as "Fast Switching"). This occurs when the forwarding table has a match for the IP destination address of the received packet which indicates the packet should be sent out using one of the other interfaces on the same card, and the packet does not require any special IP processing. This type of forwarding is very efficient, since it causes very little load on the router processor.

The operation of the router is controlled by one or more general purpose processor which is usually similar to a standard high-end PC CPU. The processor's performs various tasks, which may be divided into three groups:

- Process Switching
- Fast Switching
- Routing

The first two tasks are considered first, and concern packet forwarding. The final task may in some routers be performed by a separate processor.

4.3.1.1 Process Switching

Every router allows packets to be handled by a CPU using software which implements the various protocols which define the IP network layer. This processing is known as the "Slow Path", (it is typically much slower than processing by Fast Switching, described next). Although slower, the general purpose CPU is however able to perform more sophisticated processing (e.g. packet fragmentation), and is therefore more flexible. It is also software-based, and therefore can easily be updated as new features are required. In practice, only occasional packets travel on the slow path using process switching, but since it is universally implemented, it will be described first.

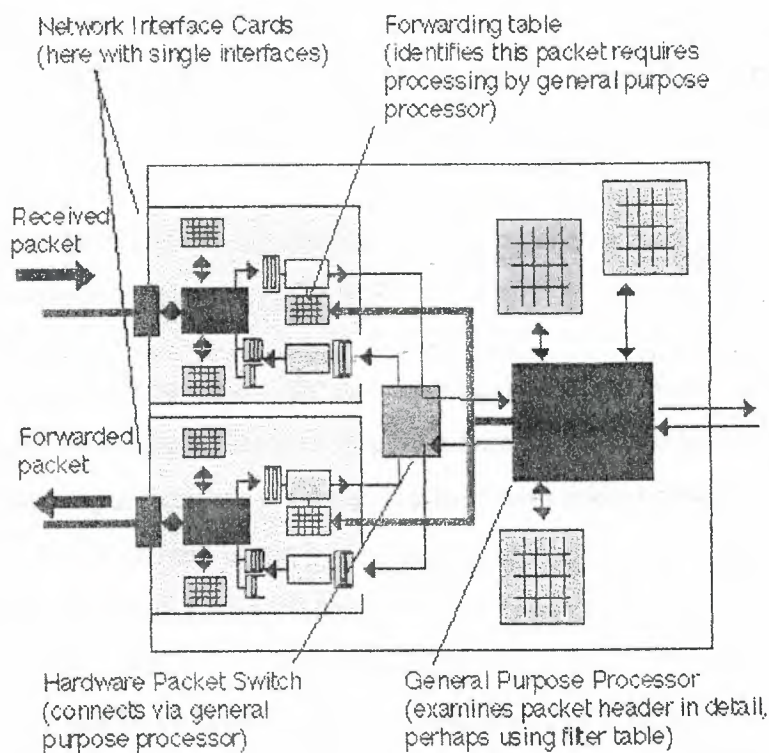


Figure 4.6: Shows Process Switching

Slow path processing of a packet routed via the processor. This type of operation is required to handle more complex processing or to implement firewall filtering to allow an administrator to control access to and from a LAN to a WAN.

The most complicated way to process a packet received by a router is Process Switching. In this scheme, the following (roughly speaking) series of tasks are performed:

Receive Processing by Interface Card

- Received packet is checked.
- The packet is placed in a shared memory pool.
- An interrupt called on the Switching Processor CPU.
- Interrupt Handling by Switching Processor (Process Switched)

The CPU records the packet's address in memory and schedules a process to find out where the packet is to be sent to (forwarding).

The interrupt returns. Switching by Switching Processor (Process Switched) some time shortly later (after all interrupts have completed, and CPU has completed its current set of tasks) the switching processor looks at the packet. The CPU checks whether the packet contains any options - if it does these are processed. IP destination address is extracted.

If the packet is for this router (IP destination address matches a router interface address), it is forwarded to the appropriate task (TCP, UDP, etc).

If it is for a remote computer, the current forwarding table is searched to find the IP address of the next hop router. This may require a number of route lookups in some cases. The corresponding output interface is found. The link layer address of the next hop router is now found (e.g. a MAC address found by looking in the Arp cache). If there is no entry, an Arp request may be sent (e.g. for an Ethernet interface) and the packet remains queued until a response (or timeout) is received. The switching processor now knows where to send the packet and the new link layer header to use. It must also check the size of the packet to see if the MTU of the output interface is large enough, if not; the packet has to be fragmented. The switching processor caches these values in the forwarding cache (see fast switching later). The link layer address is added and the packet is linked into the list of frame to be sent on the appropriate interface. The switching processor informs the corresponding interface processor that the packet is waiting.

Transmit Processing by Interface Card--When the interface transmit process is next idle (i.e. when all the frames ahead of this frame in the transmit interface queue have been sent),

the interface processor transmits the frame. The interface processor interrupts the process switching CPU to tell it the frame has been sent.

Interrupt Handling by Switching Processor--The memory buffer is now freed by returning it to the set of buffers available for new packets received. The switching processor also updates the statistics count held in the router management information base.

The above algorithm is somewhat simplified. In reality, routers also need to be able to handle tunnels (packets carrying other packets inside them), quality of service features (such as priority for some packets) and various techniques to mitigate the effects of overload.

4.3.1.2 Fast Switching

In many cases, a number of packets are sent by the same end system to the same destination IP address. Using process switching, each of these packets is handled independently - just as one would imagine for a connection-less protocol. But, this processing is costly when performed in this way. In fact, once one packet has been process switched, the router now understands the way to switch all successive packets to the same destination. That is the reason why, the process switching caches (or stores a copy of the outcome) the forwarding decision after it has been made.

Using the cached information (IP destination address, port number, link address, and any other necessary details), can significantly speed-up the forwarding by by-passing many decisions. This is known as the "Fast Path" or "Fast Packet Forwarding" and is outlined below:

Receive Processing by Interface Card

- As in process switching.
- Interrupt Handling by Switching Processor (Fast Switched)
- The Switching Processor checks whether the packet contains any options - if it does it uses process switching (i.e. a task is scheduled to process the packet).

The Switching Processor checks whether the IP destination address is in the forwarding table - if it is not, it uses process switching. The Switching Processor checks the forwarding cache to see if there is an entry for the destination IP address, if not, it uses process switching. If fragmentation is required (or anything apart from simple forwarding), it uses process switching. The Switching Processor now knows where to send the packet (interface) and the new link layer header to use by taking values from the forwarding cache. The link layer address is added and the complete frame is linked into the list of frame to be sent by the appropriate interface processor. If the process-switched output queue is empty and there is space in the transmit interface FIFO ring, the frame may be placed directly in the transmit interface output queue. The Switching Processor informs the interface processor that the packet is waiting.

The interrupt returns. Transmit Processing by Interface Card as in process switching. Interrupt Handling by Switching Processor as in process switching. This scheme is much faster than process switching. However, the fast path may only be used for packets which have previously been sent to the same address. The first packet is therefore always process switched. In practice, it is unwise to keep any cached information for too long. This prevents the information becoming stale (e.g. when a router fails). CISCO (a well-known router supplier) recommends a small part of the cache (e.g. 1/20th) is deleted every minute. Since it is very computationally expensive to find all the entries in the table referring to a single route of link layer address, the entire table is deleted (purged) whenever the routing table or an interface arp table changes. Fast switching is very effective at the edge of networks, or within private networks (where there are comparatively few destination addresses and routes). As the number of entries in the forwarding information base increases, the impact of purging the table becomes more and more significant. The rate of purges increases with the number of routers being communicated with. To help this, as the size of the forwarding table increases, the proportion of addresses may need to be deleted (e.g. 1/5th for a FIB > 200KB). Fast switching provides little advantage at the centre of the internet (core).

N.B.1) The output queue is always used if there are any packets waiting there, this helps reduce the re-ordering of packets when packets for the same destination are being both process and fast switched.

N.B. 2) Some interfaces use a number of queues (from a few to several thousands). Normally one queue is reserved for network control data (such as routing packets) to ensure these are never delayed (in overload, such packets are particularly important since failure to receive them can impact the stability of the network). If a number of additional queues are being used by the interface, the packet is placed in the output queue, rather than the FIFO ring.

a) Independent Switching Processor-- Some routers provide a separate switching processor, independent of the process used for process switching. The switching processor may use Fast Switching using a cache of previously used forwarding entries. An alternate to fast switching is to down-load a compressed form of the complete forwarding information base (in CISCO routers this is known as CISCO Express Forwarding (CEF)). It is often wise to separate the interface data (chosen interface, link layer address, MTU) from the forwarding data (whether address is reachable, interface entry to use), so that changes in the link layer protocols (such as Arp table changes) do not require purging and a complete rebuild of the entire forwarding table. This approach allows the switch processor to handle large numbers of destination IP addresses, even when there are large numbers of route changes. It therefore scales well to core routers and is used in the high-speed routers of many suppliers. The switch processor does not take part in routing operations, receiving all information from the router's route processor. The forwarding table is therefore pre-compiled by the route processor for each interface card. Since the route processor down-loads all information, there is no need to forward packets to the process switching task which do not have a forwarding information base entry. These are simply discarded. Switch processors differ in the ability to support multicast, multiple queues, access management (checking rates, authenticating users), etc. An entry is also required for completeness to allow any "special" packets to be sent to the process switching path (e.g. destined for the router itself, to be fragmented, to be authenticated, etc).

b) Multiple Interface Switching Processors--Some routers provide a number of interface switching processors. Each processor is associated with a group of interface cards and handles all packets received by the group of interface cards. Sometimes this interface switching processor is actually integrated into a single board with the interface cards. A central switching processor must still be allocated to control switching to and from the routing processor (often this is actually the same CPU - they just two different tasks). Communication between interface switching processors still requires the intervention of the main switching processor, and is therefore less optimized than communication between interfaces connected to a common interface switching processor. Network designers may therefore optimize performance by connecting networks which carry related traffic to different interfaces handled by the same interface switching processor. (CISCO calls this distributed CEF (dCEF).)

4.3.1.3 The Route Processor

The routing processor is responsible for configuring each network interface card (including the forwarding table), and collecting management information (from the management table associated with each interface) for the Router Management Table. The processor is also directly connected to the packet switch which allows the configuration to be (optionally) accessed and modified by establishing a connection from an End-System connected via the network. All configuration data and all performance data collected from the network interface cards are stored in the central router management table. In large routers, a backup routing processor may be provided, in case the main processor fails.

The route processor also processes all packets destined to the router itself (see below).

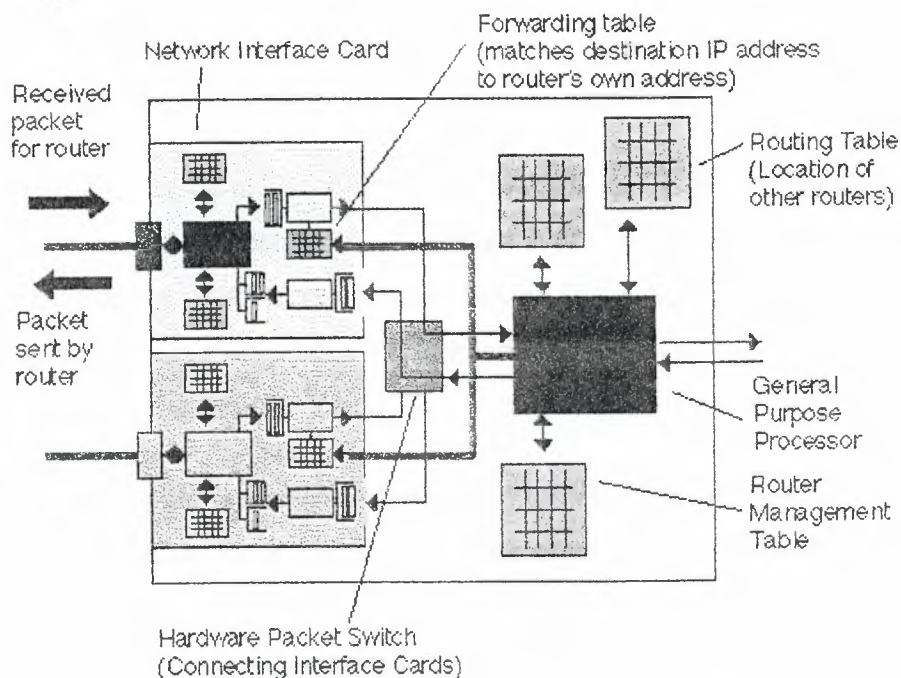


Figure 4.7: Shows the Route Processor

Sending and receiving packets which have address which match the router's own IP address. These packets may simply be ICMP echo request messages (to check the router is working) or may be packets directed to the router itself (e.g. indicating routing information from other routers or accessing the information held in the router management table).

4.3.2 Packets Destined for the Router (Route Processor)

When the router responds to received packets (with one of the router's own IP addresses) it will behave as an End-System, rather an Intermediate-System (where it forwards packets between interfaces). The router general purpose processor will also respond to any ICMP messages it receives (e.g. sent by the "Ping" program), and may generate ICMP error messages when error events are detected (such as a packet received which can not be routed because the address is not known).

The processor first performs any necessary checks on the packet header and will then determine whether the packet should be discarded, logged (in the router management table) or forwarded. The general purpose CPU is also responsible for configuring the

Forwarding Tables used by the switching process. The router computes the forwarding tables by processing two local tables: The Routing Table and the Filter Table.

The "Routing Table" contains lists of internet addresses and their corresponding location in the network. A router connected to the Internet will need to be able to identify which interface is to be used to reach every other connected end system. Routers near the centre of a network generally have very large routing tables; those nearer the edges have smaller tables.

The routing table is constructed by using information supplied when the router is configured (installed) by the manager which it stores in the routing table. Although the routing table may be configured by hand, it is usually configured automatically using a "Routing Protocol". The routing protocol allows routers to periodically (e.g. every few tens of seconds) exchange information about the contents of their own routing tables. After a period of time, the router becomes aware of all the possible ways to reach each end system connected at any point in the network. It therefore adds information to its own routing table about the other routers to which it is connected, building a picture of how to reach other parts of the network. This is achieved by periodically sending packets to all neighboring routers.

The filter table is usually manually configured, and contains a list of addresses and other packet header details which, if they match a received packet, will cause the packet to be examined in detail and possibly rejected. This may be used to prevent unauthorized packets being forwarded (e.g. to act as a firewall). When a packet is detected by a network interface card (i.e. it matches an entry in the forwarding table), it may be either discarded by the network interface immediately or forwarded directly to the general purpose processor for further processing. This table is often called an Access Control List (ACL), and may become very complex in some applications.

As the router discovers changes in the routing tables and filter tables it may either

1. Invalidate the forwarding cache, causing the fast switching process to start build a new forwarding cache.

2. Constructs a new forwarding information base for each network interface card, with the appropriate modifications.

This ensures the forwarding engines (switching processors) to be updated. The forwarding information base is optimized for speed (since it needs to be consulted for each received packet), in contrast, the routing table is optimized to ease updating, since received packets received via the routing protocol may require many changes to be made to the routing table (e.g. after the network topology changes following a failure of a communications link).

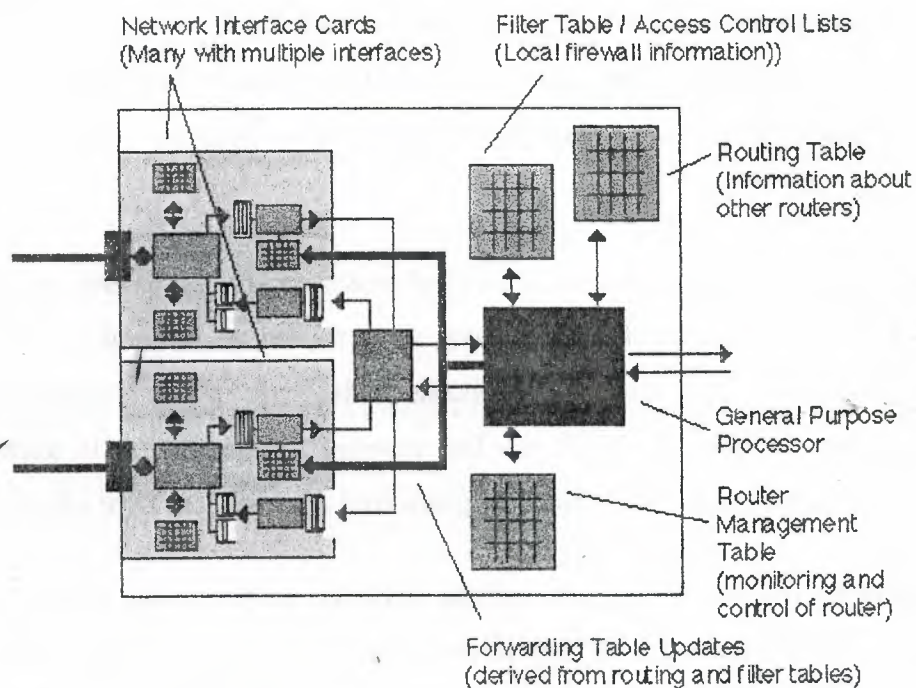


Figure 4.8: Shows Packet Destined Process

As required, network interface cards must be reloaded with new forwarding information which reflects any changes to the network topology. This information is based on the information configured in the filter table and collected from the network and stored in the routing information base.

4.4 Routing in the Internet

Routing is the technique by which data finds its way from one host computer to another. In the Internet context there are three major aspects of routing

1. Physical Address Determination
2. Selection of inter-network gateways
3. Symbolic and Numeric Addresses

The first of these is necessary when an IP datagram is to be transmitted from a computer. It is necessary to encapsulate the IP datagram within whatever frame format is in use on the local network or networks to which the computer is attached. This encapsulation clearly requires the inclusion of a local network address or physical address within the frame.

The second of these is necessary because the Internet consists of a number of local networks interconnected by one or more gateways. Such gateways, generally known as routers, sometimes have physical connections or ports onto many networks. The determination of the appropriate gateway and port for a particular IP datagram is called routing and also involves gateways interchanging information in standard ways.

The third aspect which involves address translation from a reasonably human friendly form to numeric IP addresses is performed by a system known as the Domain Name System or DNS for short. It is not considered further at this stage.

4.4.1 Physical Address Determination

If a computer wishes to transmit an IP datagram it needs to encapsulate in a frame appropriate to the physical medium of the network it is attached to. For the successful transmission of such a frame it is necessary to determine the physical address of the destination computer. This can be achieved fairly simply using a table that will map IP addresses to physical addresses, such a table may include addresses for IP nets and a

default address as well as the physical addresses corresponding to the IP addresses of locally connected computers.

Such a table could be configured into a file and read into memory at boot up time. However it is normal practice for a computer to use a protocol known as ARP (Address Resolution Protocol) and defined by RFC 826. This operates dynamically to maintain the translation table known as the ARP cache.

On most UNIX systems the contents of the ARP cache can be displayed using the command `Arp -a`.

Here is typical output from the `Arp -a` command

```
scitsc16.wlv.ac.uk (134.220.4.16) at 8:0:20:b:ca:2  
scitsc17.wlv.ac.uk (134.220.4.17) at 8:0:20:c:41:70  
ccuf.wlv.ac.uk (134.220.4.202) at 8:0:20:10:e6:6  
Scit-sun-gw1.wlv.ac.uk (134.220.4.203) at 0:0:c0:fd:80:a4  
scitstd.wlv.ac.uk (134.220.4.205) at 8:0:20:77:cf:18  
scitsc31.wlv.ac.uk (134.220.4.31) at 8:0:20:4:96:83
```

A computer determines its own physical address at boot up by examining the hardware and its own IP address by reading a configuration file at boot up time but it is necessary to fill the ARP cache. This is done by the computer making ARP request broadcasts whenever it encounters an IP address that cannot be mapped to a physical address by consulting the cache.

The format of an ARP request on an Ethernet is

Table 4.1: Shows Format of ARP on Ethernet

General	Use	Size in bytes	Typical values
Ethernet Header	Ethernet Destination Address	6	A broadcast address
	Ethernet Source Address	6	Identifies computer making request
	Frame Type	2	Set to 0x0806 for ARP request and 0x8035 for an ARP reply
ARP request/reply	Hardware Type	2	Set to 1 for an Ethernet
	Protocol Type	2	Set to 0x0800 for IP addresses
	Hardware Address Size in bytes	1	Set to 6 for Ethernet
	Protocol Address Size in bytes	1	Set to 4 for IP
	Operation	2	1 for request, 2 for reply
	Sender Ethernet Address	6	-
	Sender IP Address	4	-
	Destination Ethernet Address	6	Not filled in on ARP request
	Destination IP Address	4	-

By making such requests a host can fill up the ARP cache. ARP cache entries will eventually time-out and a new query will have to be made. This allows a computer to respond to changing topology. Typical timeouts are about 20 minutes. An ARP request to a non-existent computer may be repeated after a few seconds up to a modest maximum number of times.

If a computer is connected to more than one network via separate ports then a separate ARP cache will be maintained for each interface. Alternatively there will be a further entry in the ARP cache associating an entry with a particular interface.

It may be thought that ARP requests will be made for every Internet computer a computer wishes to contact. This is not true; a reference to an IP address not on a local or directly connected network will be re-directed to an IP router computer with an IP address that is on a local directly connected network.

Since ARP requests are broadcast any computer maintaining an ARP cache can monitor all such broadcasts and extract the sending computer's physical and IP address and update its own ARP cache as necessary. When a computer boots up it can send an ARP request (perhaps to itself!) as a means of announcing its presence on the local network it is possible to associate more than one IP address with a single physical address.

4.4.2 Reverse Address Resolution Protocol

Diskless workstations were once widely used. These had a local processor and RAM but all disc space was supplied from a server using NFS or some similar system. In the absence of local configuration files, boot-up involved the use of a very simple file transfer protocol known as TFTP, however before this could be used the workstation needed to know its IP address. In order to determine this Reverse Address Resolution Protocol (RARP) described in RFC 903 was used. This used the same message format as ARP but used operation types 3 and 4 for requests and responses. Only suitably configured RARP servers would reply to such requests. RARP may still be encountered in conjunction with devices such as laser printers.

4.4.3 Internet Routing - Internal Routing Tables

Within any host there will be a routing table that the host uses to determine which physical interface address to use for outgoing IP datagrams. Once this table has been consulted the ARP cache(s) will be consulted to determine the physical address.

If a computer receives an IP datagram on any interface there are two possibilities, one is that the datagram is intended for that computer in which case it will be passed to the relevant application. The other is that the datagram is addressed to some other computer in

which case the computer will attempt to re-transmit on one or other of the available interfaces.

On UNIX systems the command `netstat -nr` can usually be used to display the state of the routing table.

Here is typical output from the `netstat -nr` command

Routing tables

Destination	Gateway	Flags	Refcnt	Use	Interface
127.0.0.1	127.0.0.1	UH	6	1748676	lo0
Default	134.220.4.203	UG	74	17345705	le0
134.220.40.0	134.220.4.203	UG	0	0	le0
134.220.32.0	134.220.4.203	UG	0	15516	le0
134.220.8.0	134.220.4.203	UG	0	359006	le0
134.220.17.0	134.220.4.203	UG	0	0	le0
134.220.1.0	134.220.4.203	UG	3	1346065	le0
134.220.18.0	134.220.4.203	UG	0	4708	le0
134.220.10.0	134.220.4.203	UG	0	103836	le0
134.220.35.0	134.220.4.203	UG	0	0	le0
134.220.3.0	134.220.4.203	UG	0	643	le0
134.220.19.0	134.220.4.203	UG	0	469	le0
134.220.11.0	134.220.4.203	UG	0	211689	le0
134.220.20.0	134.220.4.203	UG	0	6525	le0
134.220.12.0	134.220.4.203	UG	0	107309	le0
134.220.4.0	134.220.4.1	U	114	28841321	le0
134.220.13.0	134.220.4.203	UG	0	8748	le0
134.220.37.0	134.220.4.204	UG	0	567	le0
134.220.6.0	134.220.4.203	UG	0	1202340	le0
134.220.15.0	134.220.4.203	UG	0	2566	le0
134.220.7.0	134.220.4.203	UG	7	1207070	le0
134.220.39.0	134.220.4.203	UG	0	0	le0

So if, for example, the host wanted to send an IP datagram to 134.220.6.12, it would use the above table to determine that it had to go via 134.220.4.203 (a gateway) and then use the ARP cache to determine the physical address of the gateway (it was 0:0:c0:fd:80:a4). The datagram is then sent to the gateway which uses a similar table to the physical interface for the datagram and then uses it's ARP cache to determine the physical address for the datagram.

There are four basic items of information in such a table

1. A destination IP address.
2. A gateway IP address. This will be the same as the destination IP address for directly connected destinations.
3. Various flags usually displayed as U, G, H and sometimes D and M. U means the route is up. G means the route is via a gateway. H means the destination address is a host address as distinct from a network address.
4. The physical interface identification.

The destination address may appear as "default".

The host operation is to first look for the destination address as a host address in the routing table, if it is not found then look for the destination net address in the routing table and if that is not found then use one of the default addresses (there may be several).

A host dedicated to providing a gateway service between several networks is known as a router and may have a very large routing table (64 MB is not unknown) and will run special protocols to interchange routing information with other hosts and routers.

A general purpose host may have connections to at most two or three networks and a correspondingly simple table.

4.4.4 Communication between routers

The complete Internet consists of a large number of interconnected autonomous systems (ASs) each of which constitutes a distinct routing domain. Such autonomous systems are usually run by a single organization such as a company or university. Within an AS, routers communicate with each other using one of several possible intra-domain routing protocols also known as interior gateway protocols. ASs are connected via gateways, these exchange information using inter domain routing protocol also known as exterior gateway protocols.

The commonest interior gateway protocols are the Routing Information Protocol (RIP) defined in RFC 1058 and the more recent Open Shortest Path First (OSPF) protocol defined in RFC 1247. The purpose of these protocols is to enable routers to exchange locally obtained information so that all routers within an AS have a coherent and up to date picture of how to reach any host within the AS.

Whenever a host receives routing information it is expected to revise its routing tables in the light of the new information. This update may cause the host to send new routing information to further hosts so that changes will propagate across the network.

4.4.5 The RIP (RFC 1058) protocol

Using RIP hosts will periodically broadcast (or send to all neighbor routers if there is no broadcast facility) its entire routing table or those parts that have changed recently. RIP information is transmitted using UDP/IP using messages of the form

The metric is the hop-count to the host whose IP address is quoted. A value of 16 implies the host is unreachable. The 20 bytes specifying address family, IP address and metric may be repeated up to 25 times. An IP address of 0.0.0.0 is regarded as a default address.

Routers will receive RIP information and will use it to determine their shortest route to a particular host. RIP information is sent to neighbors or broadcast every 30 seconds.

RIP information is processed by daemon processes (either routed or gated on UNIX hosts) listening on the well known port number 520.

Table 4.2: Shows the RIP (RFC 1058) Protocol Values

Field	Bytes	Typical Values
command	1	1. Request 2. Reply 3. Obsolete 4. Obsolete 5. Poll 6. Poll Entry
Version	1	1 or 2
Reserved	2	Must be zero
Address Family	2	2 for IP addresses
Reserved	2	Must be zero
IP Address	4	Address of host
Reserved	8	Must be Zero
Metric	4	A number in the range 1 to 16

RIP suffers from very slow convergence in the face of topology changes because routers are not under any obligation to identify failed links and, more importantly, their consequences and propagate the facts to other routers. RIP is an example of a distance vector protocol.

4.4.6 The OSPF (RFC 1247) Protocol

The O means open, i.e. non-proprietary protocol. OSPF is a link state protocol (LSP). This means that each router maintains link status information and this is exchanged between routers wishing to build routing tables. Unlike RIP OSPF uses IP directly, OSPF packets being identified by a special value in the IP datagram protocol field.

All OSPF messages have a common initial 8 bytes

Table 4.3: Shows the OSPF (RFC 1247) Protocol Values

Field	Bytes	Typical values
Version	1	2
Packet Type	1	1. Hello 2. Database Description 3. Link state request 4. Link state update 5. link state acknowledgment
Packet Length	2	Packet length in bytes
Router ID	4	IP address of sending host
Area ID	4	ID of area to which packet belongs
Checksum	2	As for IP datagram
Authentication type	2	1. No authentication 2. Simple password
Authentication data	8	For type 1 only

- Hello Packets

These are used between routers to identify each other and establish common operating procedures.

- Database description packets

These are used to enable routers to transmit a complete database of link states. Link states are expressed in terms of source and destination addresses and the type of service bits used in IP datagrams. These specify a low delay link state, a high throughput link state and a high reliability link state. There are proposals to include a low monetary cost link state.

The individual link status information records are known as link state advertisements.

- LSP requests

These enable a router to request specific link information from a neighbour

- LSP Update

At any time a router may transmit new link state advertisements.

- Link state acknowledgment

These acknowledge receipt of advertisements. They consist of just the advertisement headers.

4.4.7 Allocation of IP addresses

IP addresses are allocated via the Network Information Center. When the Internet was young a message to the Network Information Center was all that was necessary to obtain a block of IP addresses. Today it is more usual to obtain a block of addresses from your Internet Service Provider or direct from one of several regional registries. All the

regional registries maintain databases that can be queried using the whois command, however it is sometimes necessary to try several registries.

Here's an example of a registry being queried to determine the ownership of an IP network. RIPE is the European Internet registry.

```
bash$ whois -h whois.ripe.net 194.62.148
```

```
% Rights restricted by copyright. See http://www.ripe.net/db/dbcopyright.html
```

```
inetnum:      194.62.148.0 - 194.62.151.0
netname:      BILSTONCC
descr:        Bilston Community College
country:      GB
admin-c:      Martin George
tech-c:       Martin George
changed:      hostmaster@nosc.ja.net 941117
source:       RIPE
route:        194.62.148.0/24
descr:        BILSTONCC-1
origin:       AS786
mnt-by:       JIPS-NOSC
changed:      kevin@nosc.ja.net 951116
source:       RIPE
person:       Martin George
address:      Bilston Community College
address:      Westfield Rd
address:      Bilston
address:      Wv14 6ER
address:      United Kingdom
phone:        +44 902 353 877 x213
fax-no:       +44 902 401 897
e-mail:       ex2009@ccub.wlv.ac.uk
changed:      hostmaster@nosc.ja.net 941117
source:       RIPE
```

The full list of whose servers is

- o whois.arin.net
- o whois.apnic.net
- o whois.nic.mil
- o rs.internic.net
- o whois.ripe.net

Details of the physical locations and ownership of IP networks are available on the World Wide Web in the IP Network Index.

4.4.8 Autonomous Systems

The key to high level internet routing is the grouping of Internet hosts into autonomous systems which usually correspond to commercial or administrative entities. All autonomous systems have a distinctive and unique number. Details of autonomous systems are available from the servers in the same way as details of IP networks. Unfortunately the syntax of such queries differs between the various servers, the ripe server requires ASnnnn whereas the arin server requires just the number.

CONCLUSION

From my project about WAN Technologies and Routing i have concluded that as there is need for advancement in any field of life with due time and accordint to the needs of the day. Like there can be a simple WAN working but may be it can slow when too many networks connected together due to heavy traffic there can be problem like path is not secure also sometimes we need information very fast as this the era of multimedia and if we have to send a multimedia file over a network it will take too much time so we have new and new technologies of WAN in order to compensate with the needs of the day. All these WAN technologies which i have explained are not essential componets to make communication but there are some WAN essentails which include software and hardware part without which communication may cannot be possible. About routers they are just to rout the data and there can be many kinds of routers some can be smarter and some can be just routing. Smarter routers are those especially who can calculate the cost of sending a data over a network as how much time will take and how many ways must be used to make the cost low and time fast. So, while using a WAN its technologies and routing may not be essential but important.

REFERENCES

- [1] Edward G. Amoroso, "*Fundamentals of Computer Security and Network Technology*", Second Edition, Prentice Hall, May 1994.
- [2] Michael Alexander, "*The Underground Guide to Computer Networks*", Fourth Edition, Addison-Wesley Press, November 1995.
- [3] James Thomos, "*Data and Computer Communication*", Fourth Edition, North Holland publishing Company, August 1994.
- [4] Tanenbaum Andrew S., "*Computer Networks*", 1996
- [5] Mahler, Kevin, "*CCNA Training Guide*", Indianapolis: New Riders, 1999
- [6] Cisco IOS, "*Wide Area Networking Solutions*", Indianapolis: Cisco Press, 1999