NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

WIDE AREA NETWORK AND NETWORK SECURITY

Graduation Project

COM- 400

Submitted By: Mohammad Alzraiqat (20000520)

Supervisor: Assoc.Prof. Dr. Rahib Abiyev

Nicosia – 2004

ACKNOWLEDGEMENTS

Firstly I would like to present my special appreciation to my supervisor Assoc.Prof. Dr. Rahib Abiyev, without whom it is not possible for me to complete the project. His trust in my work and me and his priceless awareness for the project has made me do my work with full interest. His friendly behavior and his words of encouragement kept me doing my project.

Secondly I offer special thanks to my parents, who encouraged me in every field of life and try to help whenever I needed. They enhanced my confidence in myself to make me able to face every difficulty easily. I am also grateful to my mother whose prayers and my father whose words for me had made this day comes true. And because of them I am able to complete my work.

I would also like to pay my special thanks to my all friends who helped me and encouraged me for doing my work. I want to thank them as they contributed their time and provided very helpful suggestions to me.

ABSTRACT

WAN is an extention 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 uses packet switches and point-to-point connections to accomplish the task for communication. Packets 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. 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 finding the best shortest error free path and send the infomation on that path. This process or router is called as routing.

TABLE OF CONTENTS

ACKNOWLEDGEMENT i

ABSTRACT ii
TABLE OF CONTENTS iii
INTRODUCTION 1
1. INTRODUCTION TO WIDE AREA NETWORK 3
1.1 Overview 3
1.2 Point-to-Point Links 4
1.3 Circuit Switching 4
1.4 Packet Switching 5
1.5 WAN Virtual Circuit 6
1.5.1 Switched Virtual Circuit 6
1.5.2 Permanent Virtual Circuit 6
1.6 WAN Dialup Service 7
1.6.1 Dial-on Demand Service 7
1.6.2 Dial Backup 7
1.7 WAN Technology Types 8
1.8 Network Devices 9
1.9 Transmission Media 9
1.10 Network Security 10
2. TECHNOLOGY OF WIDE AREA NETWORK 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 Circuit 12
2.2.3.1 Frame Relay Switched Virtual Circuit 13
2.2.3.2 Frame Relay Permanent Virtual Circuit 14
2.2.4 Frame Relay Network Implementation 14
2.2.4.1 Public Carrier-provided Networks 14
2.2.4.2 Private Enterprise Network 15
2.3 High Speed Serial Interface (HSSI) 15
2.3.1 HSSI Specifications 16
2.3.2 DCE Clock Control 16
2.3.3 HSSI Peer-Based Communication 16
2.3.4 HSSI Loop Back Support 17
2.4 Integrated service Digital Network (ISDN) 17
2.4.1 ISDN Standard 18

2.4.2 ISDN Application 19
2.4.3 ISDN Network Component 19
2.4.3.1 ISDN Terminal Equipment 19
2.4.3.2 ISDN Reference Point 20
2.4.4 ISDN Physical Layer Operation 21
2.5 Point to point Protocol (PPP) 21
2.5.1 PPP Operation 22
2.5.2 Establish PPP Connection 22
2.5.3 PPP Link Negotiation 23
2.5.3.1 Link Establishment And Configuration Negotiation 23
2.5.3.2 Link Quality Determination 23
2.5.3.3 Network layer protocol and Configuration Negotiation 24
2.5.3.4 Link Termination 24
2.6 Synchronous Data Link Control (SDLC) 24
2.6.1 Related Standard 25
2.6.2 SDLC Environment 25
2.6.3 SDLC Network Nodes 26
2.6.4 SDLC Node Configuration 26
2.6.5 Qualified Logical Link Control (QLLC) 27
2.6.6 Binary Synchronies Protocol 28
2.7 Switched Multi-Megabit Data Service (SMDS) 28
2.7.1 SMDS Network Component 29
2.7.2 SMDS Interface Protocol (SIP) 30
2.7.3 SMDS Addressing 30
2.7.3.1 SMDS Group Addressing 31
2.7.3.2 SMDS Addressing Security 31
2.8 X-25 31
2.8.1 X-25 Network Component 32
2.8.2 Packet Assemble/Disassemble (PAD) 32
2.8.3 X.25 Session Establishment 33
2.8.4 X.25 Virtual Circuit 34
2.8.5 Virtual Circuits and Multiplexing 34
2.9 TCP/IP References Model 34
3.NETWORK DEVICES 36
3.1 Overview 36
3.2 Network Model 36
3.3 Physical Network Type 37
3.3.1 Ethernet 37
3.3.2 Leased Line 37
3.4 Network Devices 38
3.4.1 Introduction to Router 39
3.4.1.1 Router Operation 43
3.4.1.2 Directly Attached Network 43
3.4.1.3 Routing Information Protocol 44
3.4.2 Hubs 45
3.4.2.1 General Characteristic of Hubs 45
3.4.2.2 Key Feature of Hubs 45

3.4.3 Switch 46
3.4.4 Bridge 47
3.4.5 Modem 48
3.4.5.1 The Modem plug (RS 232 Interface Overview) 48
3.4.5.2 Error Correction and Data Compression 49
3.4.6 Integrated Service Digital Network (ISDN) 50
3.4.6.1 ISDN Component 50
3.4.7 Channel Service Unit (CSU)/Data Service Unit (DSU) 56
3.4.7.1 Comparing Basic Capability 57
3.4.7.2 Single Point of Frailer 60
3.5 External Connection to WAN 61
3.5.1 Permission for External Connection 61
3.5.1.1 Example Incoming Connection 62
3.5.1.2 Example Outgoing Connection 62
3.5.2 Insecure Subnet 62
3.5.3 Network Management/Monitoring 62
4.TRANSMISSION MEDIA 64
4.1 Overview 64
4.2 Coaxial Cable 65
4.2.1 Thick Coaxial (thick-net) 66
4.2.2 Thin Coaxial (thin-net) 67
4.3 Twisted Pair Cable 67
4.3.1 Unshielded Twisted pair (UTP) 68
4.3.2 Shielded Twisted pair (STP) 69
4.4 Fiber Optic Cable 70
4.4.1 Advantages and Disadvantages of Fiber Optic 73
4.5 Wireless WAN 74
4.5.1 Interference, Security, and Reliability 75
4.5.2 Infrastructure Requirements 76
5. NETWORK SECURITY 77
5.1 Overview 77
5.2 Types and Sources of Network Threats 77
5.2.1 Denial of Service 77
5.2.2 Unauthorized Access 78
5.2.2.1 Executing Commands illicitly 78
5.2.2.2 Confidentiality Branches 79
5.2.2.3 Destructive Behavior 79
5.2.3 Avoid Systems with Single Point of Frailer 80
5.3Firewalls 80
5.3.1 Type of Firewalls 82
5.3.1.1 Application gateways 82
5.3.1.2 Packet Filtering 82
5.3.1.3 Hybrid System 83
5.4 Secure Network Devices 83
5.4.1 Secure Modem 84
5.4.2 Crypto-Capable Routing 85

5.4.3 Virtual Private Network 85
5.5 Passwords 86
5.6 RIVEST-ADI SHAMIR-LEONAR ADLEMAN (RSA) ENCRYPTION 87
5.6.1 Encryption 87
5.6.2 Public Key Cryptography 87
5.6.2.1 Trap-Door Ciphers 88
5.6.2.2 Certification 89
5.6.3 RSA Encryption 90
5.6.3.1 Simple Explanation of RSA 92
CONCLUSION 94
REFERENCES 95

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 many 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.

This WAN solutions guide can help you get started. It outlines the basic steps in designing an effective wide area network. Following this general discussion, four scenarios are presented to demonstrate the process and to illustrate some of the key features of a cost-effective solution.

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

Second chapter is all about giving details of what are the technologies used in WAN. There are seven main technologies used in WAN such as Frame Relay (a high-performance protocol), packet-switched WAN protocols. High Speed Serial Interface (HSSI), 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 (International Telecommunication Union) WAN communications protocol.

Third chapter handles Network devices and it's component. First of all we have an OSI seven Layers model. Then we have protocols helping in communication, the most important is network architecture and the hardware we use in WAN like modems, access server, repeater, switch, bridges, hubs, routers.

Fourth chapter is all about the Transmission Media and the main characteristics of coaxial, twisted pair, fiber optic cable, including the advantage and disadvantage for each.

Last chapter is about the network security. I have explained in details the network and about how they have threat for different attacks. Also I have explained about the firewall and how they make the network security possible. Then I have explained the RSA encryption.

1. INTRODUCTION TO WIDE AREA NETWORK

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(Open System Interconnection) 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:

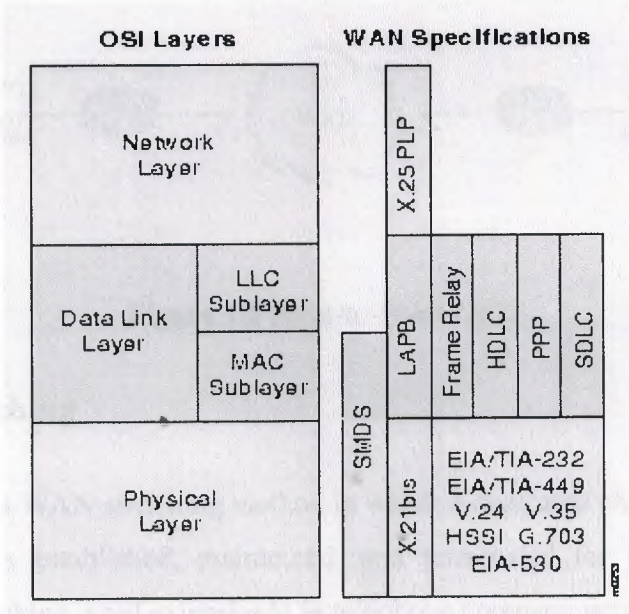

Figure 1.1 WAN Specification and OSI Model

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:

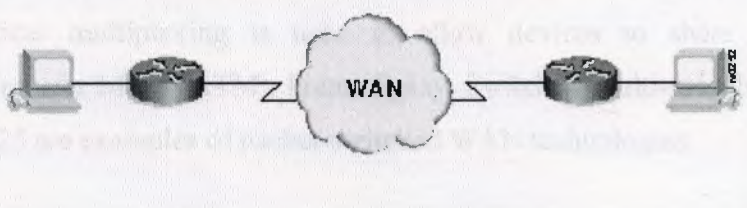

Figure 1.2 Point-to-Point Link

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.

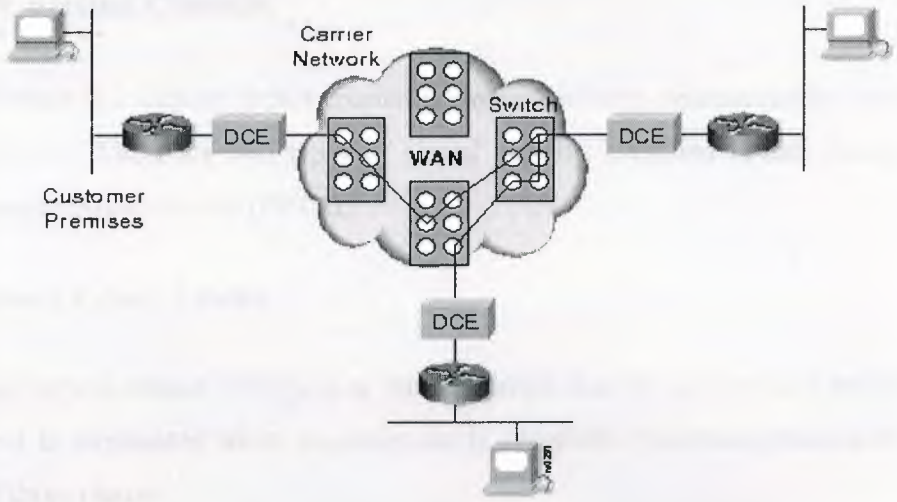

Figure 1.3 circuit-switched WAN

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.

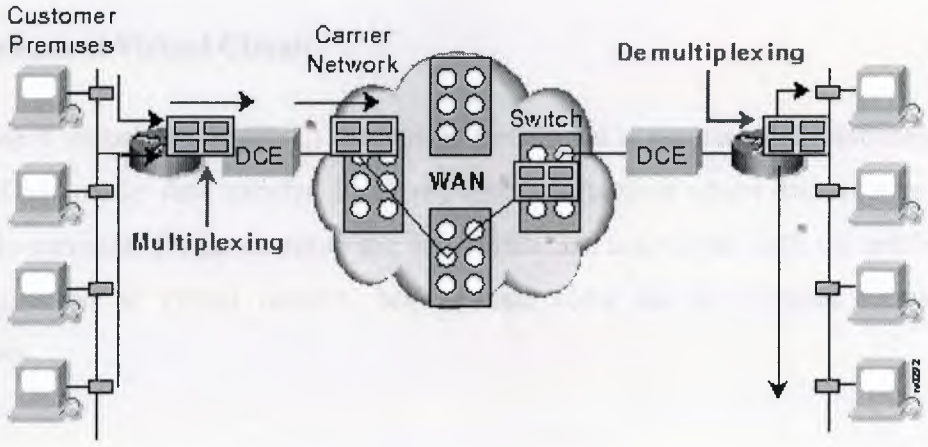

Figure 1.4 packet-switched WAN

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 where by 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.

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.

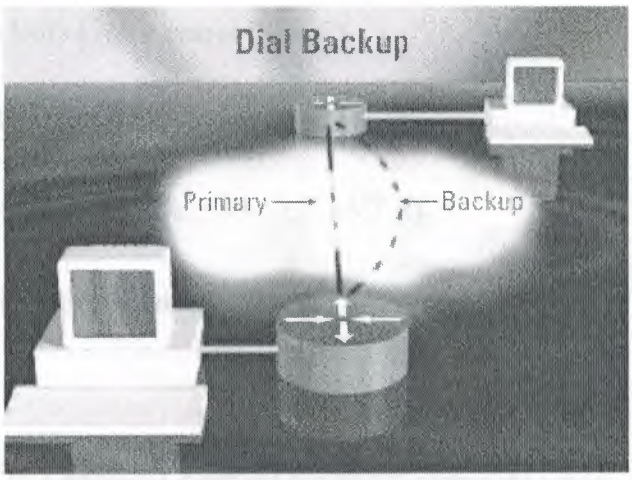

Figure 1.5 The operation of a dial backup implementation

1.7 WAN Technology Types

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

- Frame Relay

Frame Relay is a high-performance wide-area network (WAN) protocol, frame Relay was originally designed for use across Integrated Services Digital Network (ISDN) interfaces.

- High Speed Serial Interface (HSSI)

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

- Integrated Services Digital 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 protocol standard for WAN communications.

1.8 Network Devices

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

1.9 Transmission Media

Some sort of wire today connects the vast majority of networks or cabling, cable is the medium that ordinarily connects network devices. Cable's ability to transmit encoded signals enables it to carry data from one place to another.

There are varieties of cable that can meet the varying needs and sizes of networks, from small to large. Those are:

1- Coaxial Cable
2- Twisted Pair Cable
3- Fiber Optic Cable
4- Wireless WAN

1.10 Network Security

Many users expect the Wide Area Network to protect the computers on it from hacke
worms. It is impossible for the network to do this because telling the difference betw
legitimate application and a virus is hard for a human much less a computer. A
comparison would be to expect the phone company to make it impossible to place obs
phone calls. Most, if not all, security must be host based.

An important part of this security is good password security. If users pick poor passwo
then a system will be easier to penetrate. A good password should be at least six charac
long and not in the dictionary. Bad password choices include your used and parts of y
name. Some systems support a password generator, such as the VAX (it can be used
typing SET PASSWORD/GENERATE), that picks good passwords. Also, never t
anyone else what your password is. Finally, never write your password down on a sheet
paper or store it in a text file on a computer.

2. TECHNOLOGY OF WIDE AREA NETWORK

2.1 Overview

This chapter introduces the various protocols and technologies used in wide-area network (WAN) environments. Topics summarized here include frame relay, integrated service digital network, high speed serial interface, point-to-point links, packet switching, dialup services and other vital topic.

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.

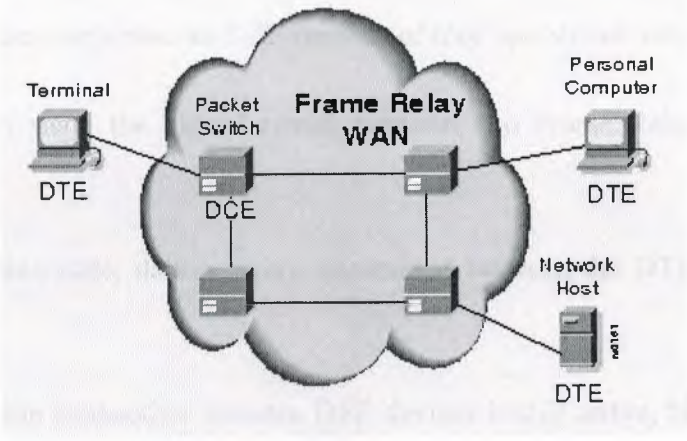

Figure 2.1 The Relationship between the two Categories of Devices

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 Network Implementation

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

2.2.4.1 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.

2.2.4.2 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).

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.

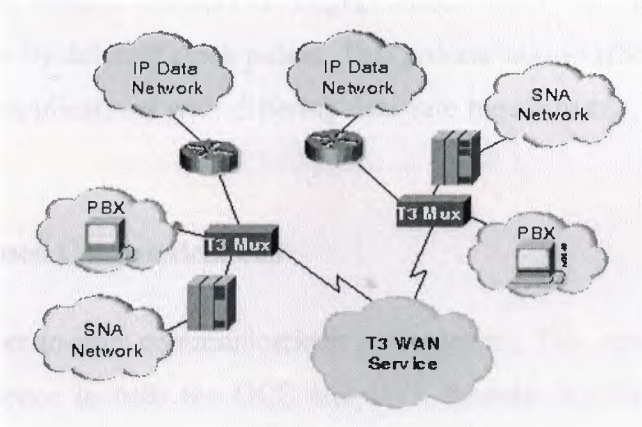

Figure 2.2 Typical HSSI-based T3 WAN

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 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

2.3.2 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 router-based on LAN.

2.3.3 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.

2.3.4 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.

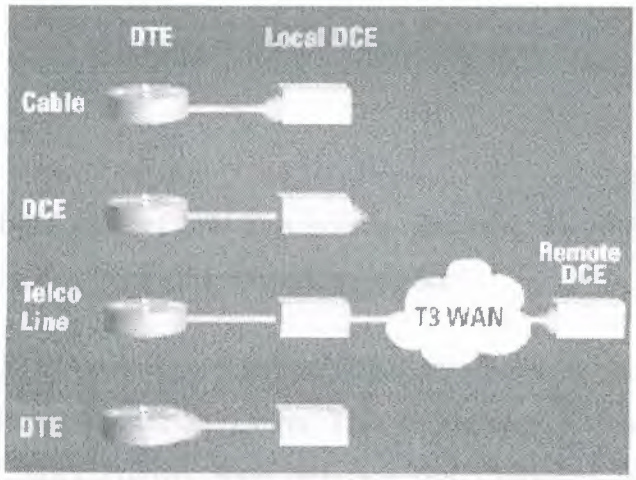

Figure 2.3 Each HSSI Loop Back Mode

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.

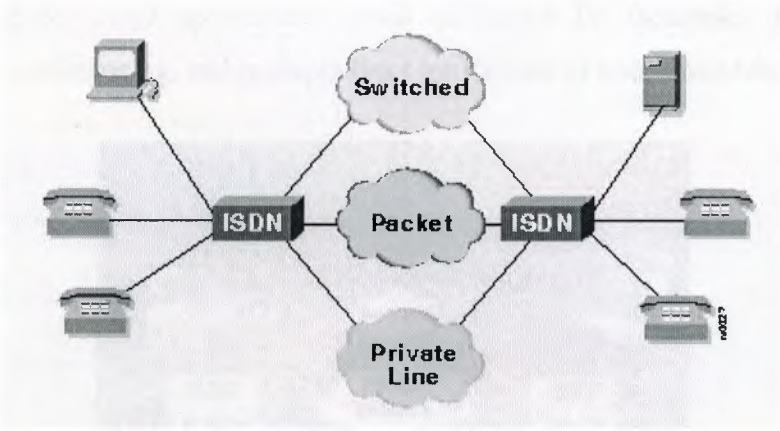

Figure 2.4 The ISDN Environment

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.

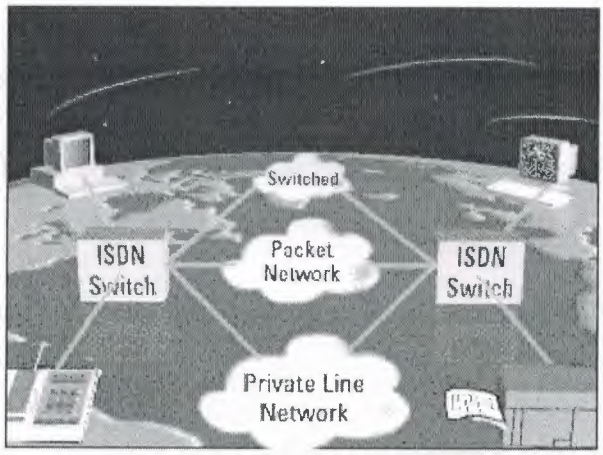

Figure 2.5 Traffic Flowing Over an ISDN Network

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 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.)

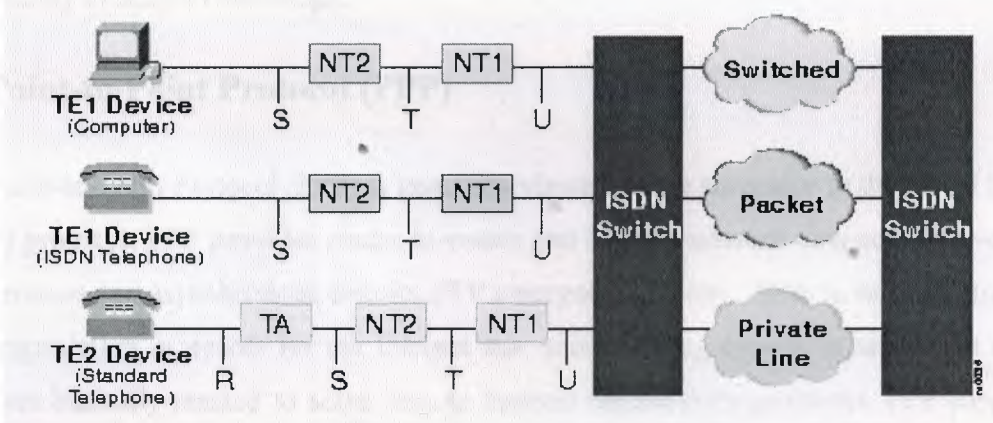

Figure 2.6 Reference Points Found in ISDN Implementations

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.

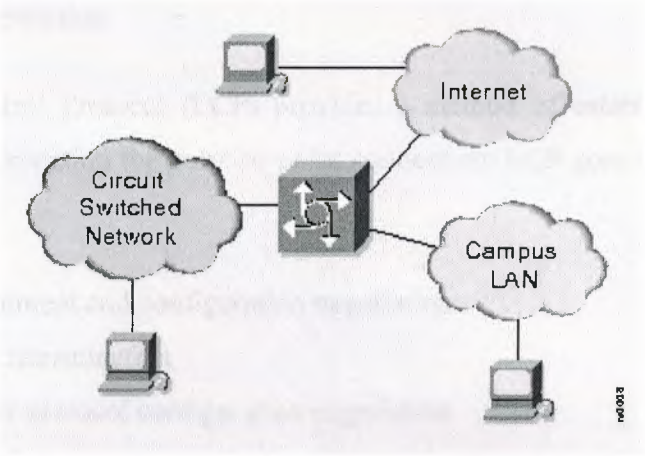

Figure 2.7 Generalized View of a PPP Environment

2.5.1 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 is used to establish and configure different network layer protocols.

2.5.2 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.

2.5.3 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:

- Link establishment and configuration negotiation
- Link quality determination
- Network layer protocol configuration negotiation
- Link termination

2.5.3.1 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.

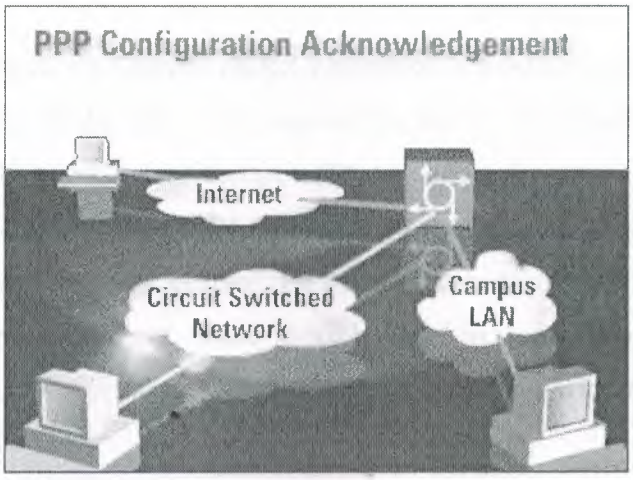

Figure 2.8 Process of Link Establishment

2.5.3.2 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.

2.5.3.3 Network Layer Protocol and 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.

2.5.3.4 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.

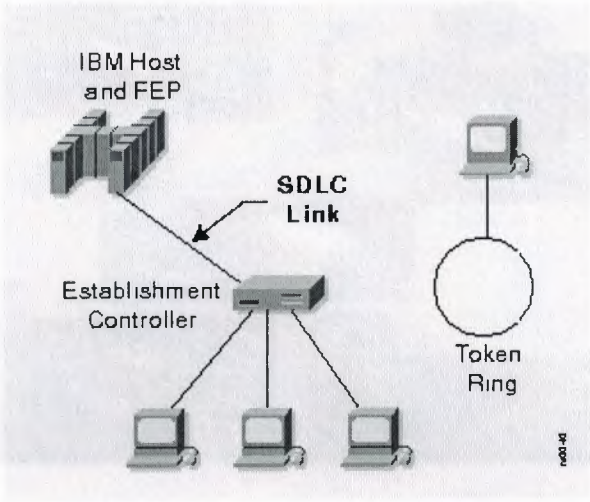

Figure 2.9 The Relative Position of SDLC Links

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

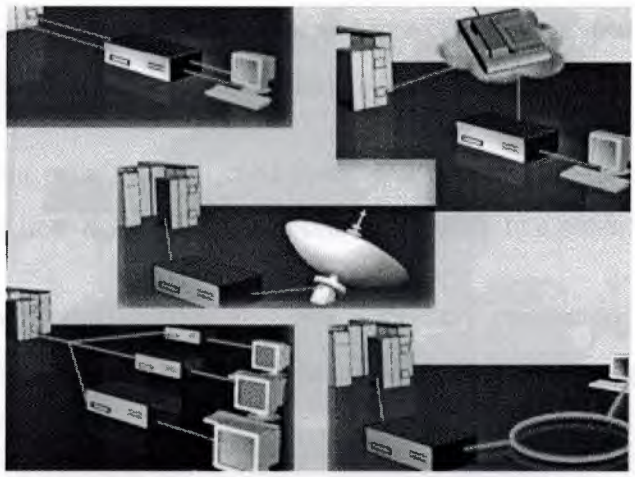

Figure 2.10 SDLC Environments

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.

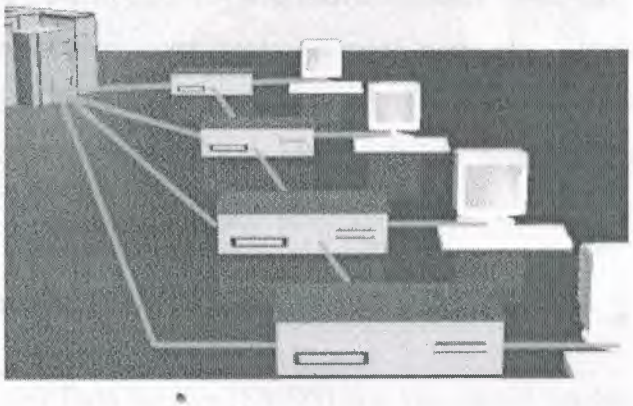

Figure 2.11 The Operation in an SDLC Arrangement

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.

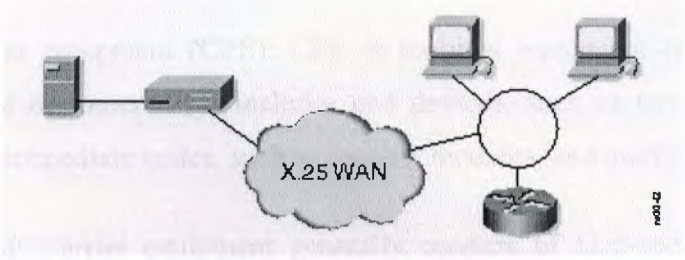

Figure 2.12 Typical X.25-based SNA Environment

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 Multi-megabit Data Service (SMDS)

Switched Multi-megabit 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.

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.

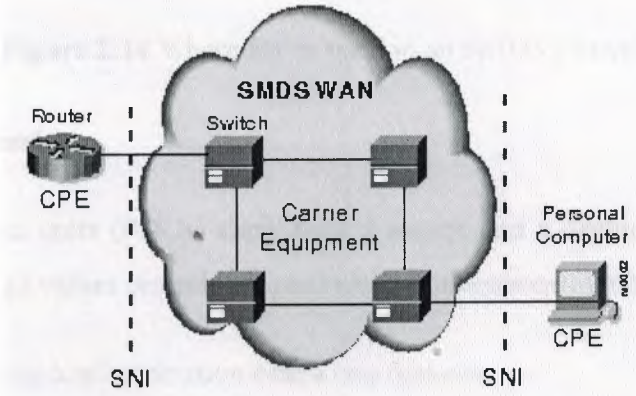

Figure 2.13 The Relationship between Primary Components

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.

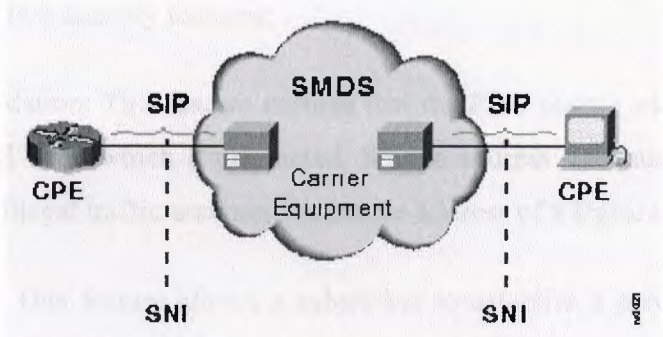

Figure 2.14 Where SIP is used in an SMDS Network:

2.7.3 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

2.7.3.1 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.

2.7.3.2 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).

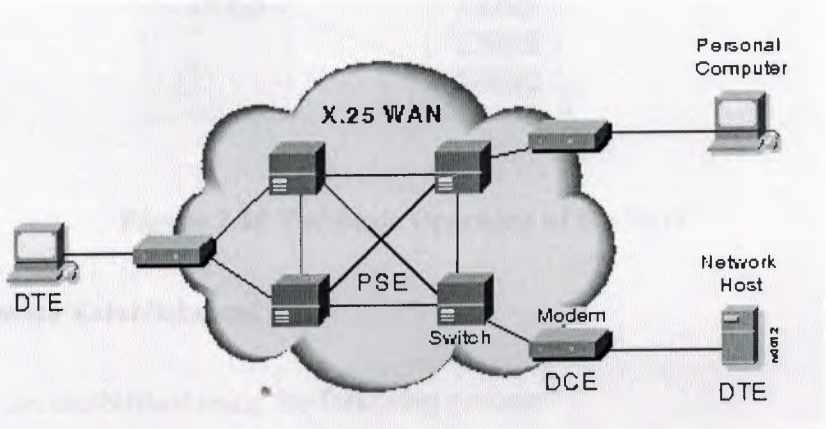

Figure 2.15 The Relationship between X.25 Network Devices

2.8.2 Packet Assemble/Disassemble (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.)

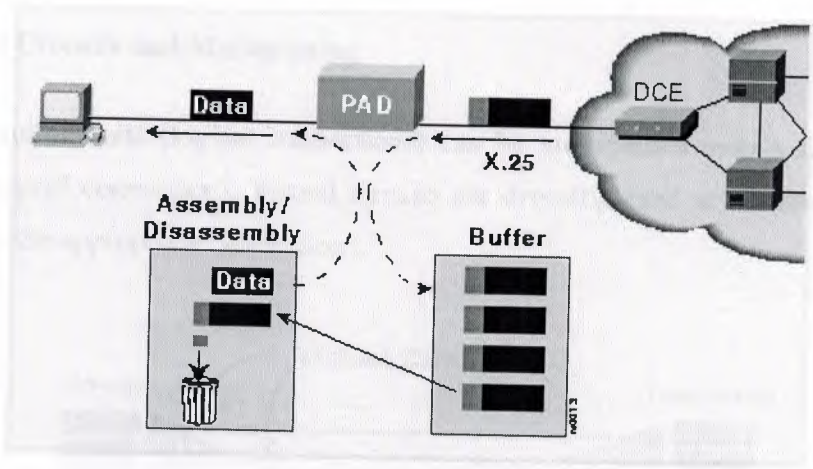

Figure 2.16 The Basic Operation of the PAD

2.8.3 X.25 Session Establishment

X.25 sessions are established using the following process:

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

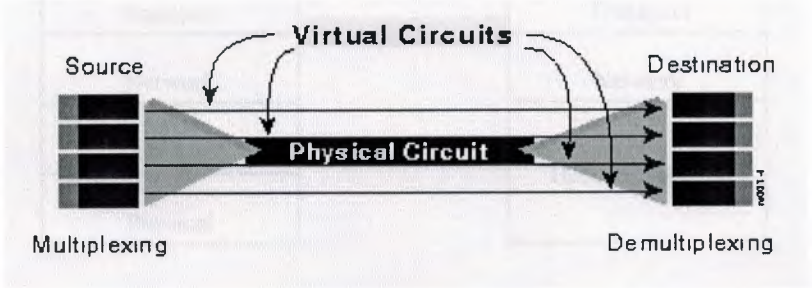

Figure 2.17 Four Separate Virtual Circuits being multiplexed

2.9 The TCP/IP Reference Model

Here we will discuss the reference model used in the grandparent of all computer networks, the APRANET, and its successor, the world wide internet. The APRANET was a research network sponsored by the DoD (U.S. Department of Defense). It eventually connected hundred of universities and government installations using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble internetworking with them, so new reference architecture was needed. Thus the ability to

connect multiple networks together in a seamless way was one of the major design goals from the very beginning. This architecture was later became known as TCP/IP Reference Model, after its two primary protocols. It was first defined in (Cerf and Kahn, 1974). A later perspective is given in (Leiner et al., 1985). The design philosophy behind the model is discussed in (Clark, 1988).

The TCP/IP model does not exactly match the OSI model. There is no universal agreement regarding how to describe TCP/IP with a layered model but it is generally agreed that there are fewer levels than the seven layers of the OSI model. Most descriptions present from three to five layers.

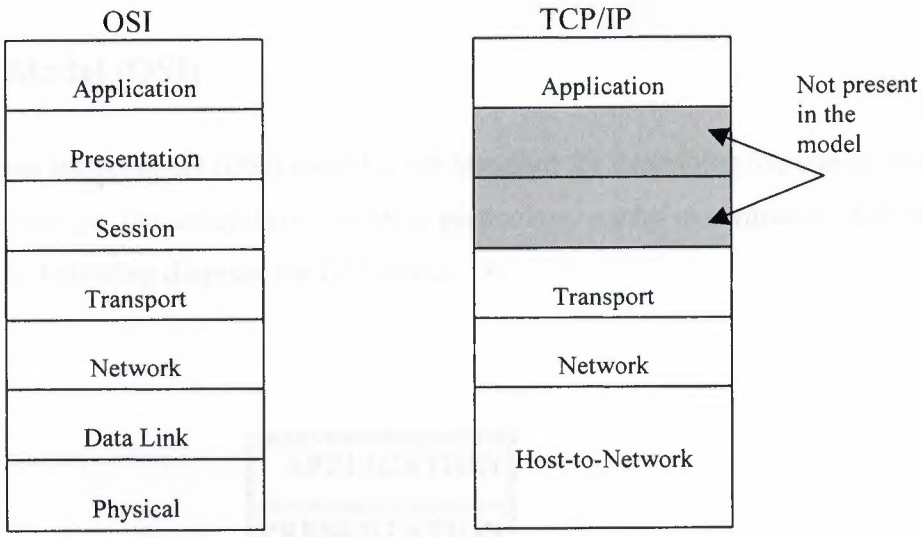

Figure 2.18 TCP/IP reference versus OSI reference model.

3. NETWORK DEVICES

3.1 Overview

It's true that WAN can be complicated, especially with various type of WAN devices and each device has its own characteristic and features, to make the network more secure, these devices can play an important rule to establish protection network.

3.2 Network Model (OSI)

The Open Systems Interconnect (OSI) model is the standard for describing the transmission of data across networks. The seven-layer model is particularly useful in comparing different architectures. The following diagram the OSI model.

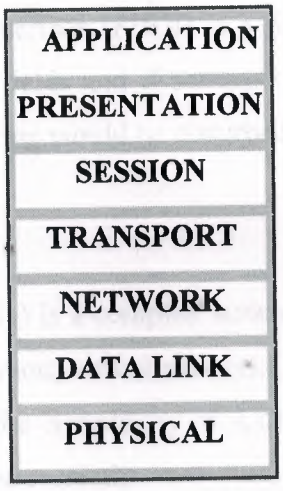

Figure 3.1 The Seven OSI Layers model

3.3 Physical Network Types

If confidentiality is a major concern, use fiber optics, they are very difficult to interrupt or sniff.

3.3.1 Ethernet

- Use hubs instead of Thin Ethernet (Star format). Use switches instead of hubs for better performance and security (all packets are not sent to all nodes).
- Avoid "unused" lived connections.
- Do not daisy chain.
- Disconnect unused sockets.
- Networks could be physically secured by using conduit.

3.3.2 Leased lines

Copper leased lines should be hardware or software encrypted.

A- FDDI

Because Fiber Distributed Data Interface (FDDI) is a fiber optic ring, it is impossible to "listen" by detection of magnetic fields and if someone tries to connect to the ring, they need specialist equipment and the ring would be disturbed - it should not go unnoticed.

B- ATM

ATM (Asynchronous transfer mode) is a complex suite of protocols with many interesting features, such as bandwidth allocation, virtual networks, and high speed... They are useful primarily by telecom providers. The complexity of ATM makes it difficult for hackers to crack, but also difficult to configure correctly.

C- High Speed Serial Interface (HSSI)

HSSI is an interface technology that was developed to fill the needs for a high-speed data communication solution over WAN links. It uses differential emitter-coupled logic (ECL), which provides high-speed data transfer with low noise level. HSSI makes bandwidth resources easy to allocate, making T3 and other broadband services available and affordable. HSSI requires the presence of only two control signals, making it highly reliable because there are fewer circuits that can fail. HSSI performs four loop back tests for reliability.

3.4 Network Devices

The Devices which are using in the network can effect on it, and allow user to access the network or not. But most attacks come from the inside, so:

- No "network analyzer" software is to be allowed on any PC unless the Network manager, the Security manager and the user, has authorized it is fully aware of his responsibilities and the PC is logged on a list of dangerous machines. The status of these machines should be reviewed yearly.
- On systems (such as SunOS, Solaris) which include such software as standard, should either

    A- Delete the utility.

    B- Change permissions on the utility so that it can only be used by root.

Of course the user must NOT have access to the root account in this case.

- Class systems should not be allowed on the same subnet as .
- Install a packet filter/firewall between internal networks and class systems.
- Network interface cards in PCs: some cards cannot be switched into promiscuous mode e.g. those based on the TROPIC chipset (HP Ether twist). Buy Ethernet cards, which do not allow promiscuous mode.

- Hubs, bridges and routers are getting very intelligent; they have more and more configuration options and are increasingly complex. This is useful for additional features, but the added complexity increases the security risk.

On critical subnets, it's important correctly configure network devices: only enable needed services, restrict access to configuration services by port/interface/IP address, disable broadcasts, source routing, choose strong (non default) passwords, and enable logging.

3.4.1 Routers

Routers are data forwarding devices but operate differently than a transparent or source Route Bridge. They separate networks into regions like each region is assigned a unique network number. These network numbers are unique for each network they are assigned to and packet forwarding is based on these network IDs. Routers route packets based on a protocol as well as a network ID as most routers today are Multiprotocol in that one box can forward different protocol packets. Routers, like bridges, can be used locally or remotely.

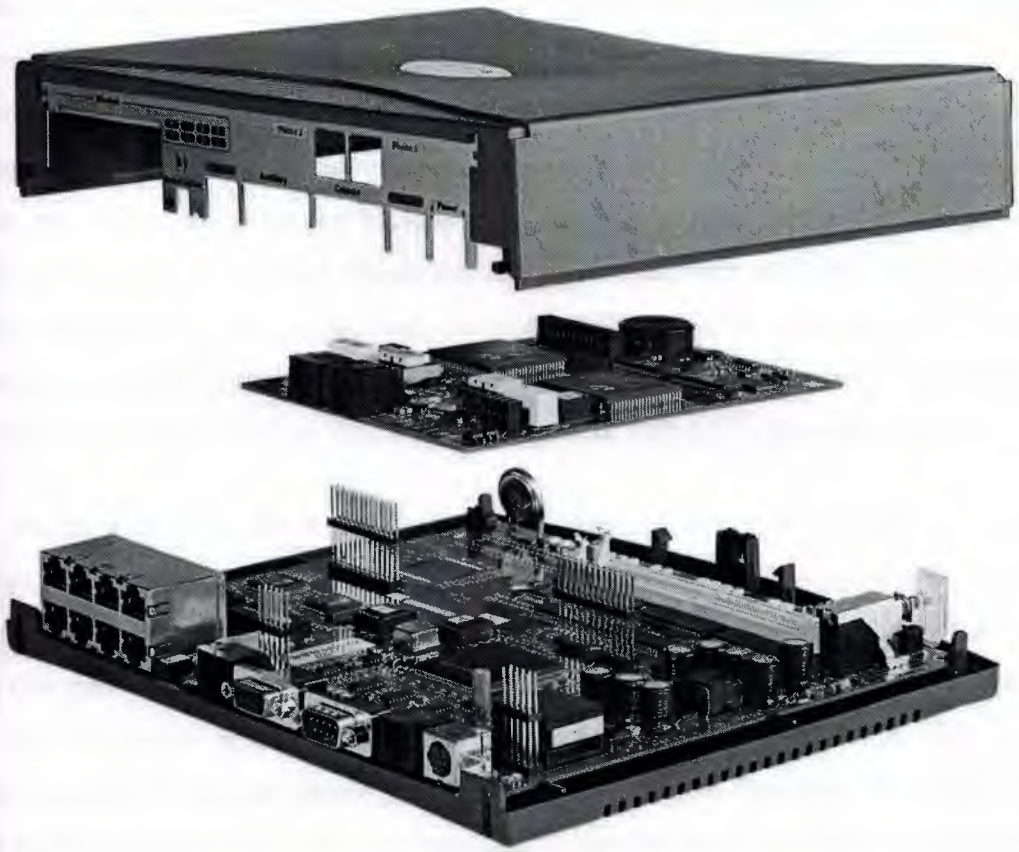

Figure 3.2 Router Diagram

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. The router into two or more smaller packets must fragment packets larger than the interface's MTU. 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 sub network 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 to simply discard excess packets. If required, these may later be retransmitted by a transport protocol.

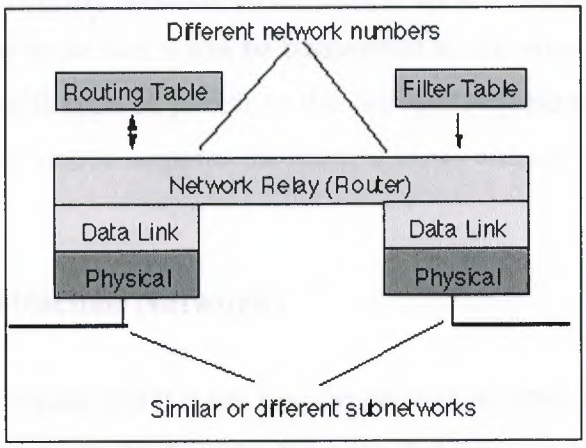

Figure 3.3 Architecture of a router

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)) are 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.

3.4.1.1 Router Operation

Routers forward packets based not on the MAC address of the packet but on the network number inside the packet. Each network separated by a router is assigned a unique network number End stations know only of the network number of the network to which they are attached. Before an end station transmits a packet, it compares the network number of the destination to the network number and if the network numbers are the same, the packet is simply transmitted on the cable, addressed to the destination station, as the destination station is local. If the network numbers do not match, the end station must find a router that it can send the packet to so that it can be transmitted to the original end. The requesting station submits a special type of packet to the network requesting information from the routers. The requesting station acquires the router's MAC address by some means specific to the protocol.

3.4.1.2 Directly Attached Networks

A router receives the request and if it can find the network number, it sends a response back to the requesting station. Node A picks the path that has the lowest cost to the final destination. There is only one router response in this example. Node A sends the packet to router Z. The source MAC address is A and the destination MAC address is B (the router 's MAC address.

The destination network number is located on the other side of the router. The router directly to the end station forwards the packet. The packet is addressed with source address as the routers address, source address C. The destination address is the destination end station, destination station D. If the destination is not on the other side of the router, the router has the next router's address in its routing table and the packet is forwarded to the next router. Different network protocols operate differently.

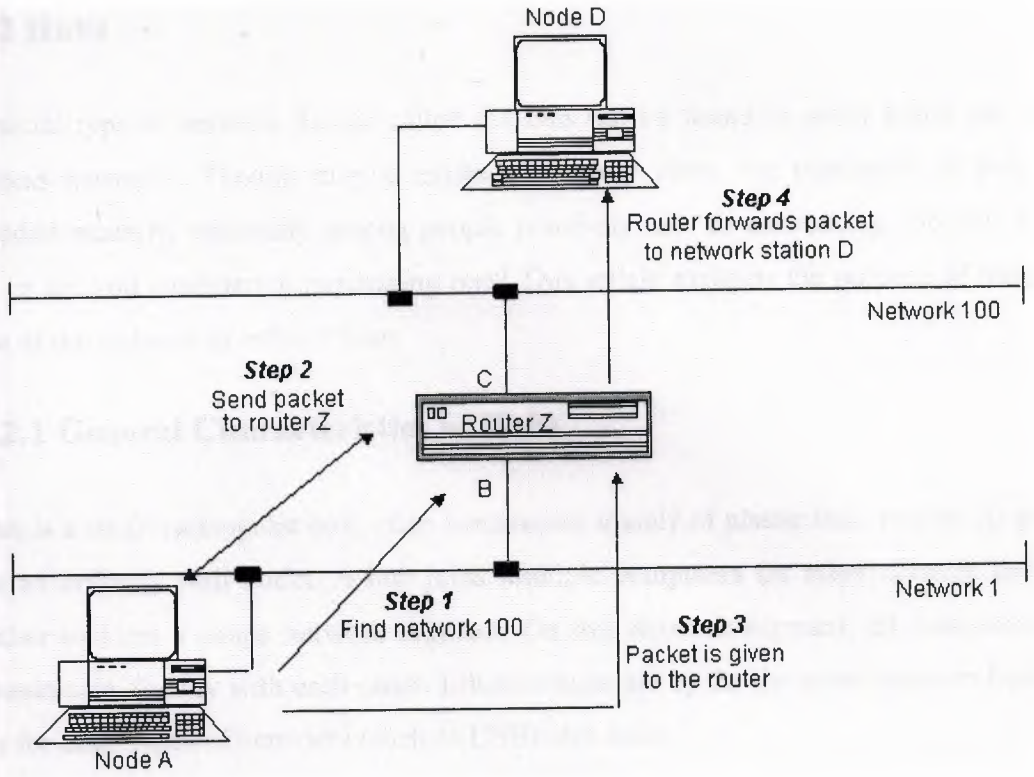

Figure 3.4 Directly Attached Network to WAN

3.4.1.3 Routing Information Protocol (RIP)

This is known as routing tables update protocol as most commonly found router update protocol is called Routing Information Protocol (RIP). Developed by Xerox and gained widespread acceptance by the proliferation of TCP/IP's implementation of it in UNIX.

Other protocols adopted RIP as their standard routing update protocol. Different protocol implementations of RIP cannot update each other this is known as a distance.

Vector protocol and vector is the network number and the distance is how far away (hops) the network is one hop is considered one router traversed. Devised for very stable, small-to-medium size networks (less than a few hundred nodes).

3.4.2 Hubs

A special type of network device called the hub can be found in many home and small business networks. Though they've existed for many years, the popularity of hubs has exploded recently, especially among people relatively new to networking. Do you own a hub, or are you considering purchasing one? This article explains the purpose of hubs and some of the technology behind them.

3.4.2.1 General Characteristics of Hubs

A hub is a small rectangular box, often constructed mainly of plastic that receives its power from an ordinary wall outlet. A hub joins multiple computers (or other network devices) together to form a single network segment. On this network segment, all computers can communicate directly with each other. Ethernet hubs are by far the most common type, but hubs for other types of networks (such as USB) also exist.

A hub includes a series of ports that each accepts a network cable. Small hubs network four computers. They contain four or sometimes five ports (the fifth port being reserved for "uplink" connections to another hub or similar device). Larger hubs contain eight, 12, 16, and even 24 ports.

3.4.2.2 Key Features of Hubs

Hubs classify as Layer 1 devices in the OSI model. At the physical layer, hubs can support little in the way of sophisticated networking. Hubs do not read any of the data passing through them and are not aware of a packet's source or destination. Essentially, a hub simply receives incoming packets, possibly amplifies the electrical signal, and broadcasts these packets out to all devices on the network (including the one that sent the packet!). Hubs remain a very popular device for small networks because of their low cost.

Technically speaking, three different types of hubs exist:

- Passive
- Active
- Intelligent

Passive hubs do not amplify the electrical signal of incoming packets before broadcasting them out to the network. Active hubs, on the other hand, will perform this function -- a function that is also present in a different type of dedicated network device called a repeater. Some people use the terms concentrator when referring to a passive hub and multiport repeater when referring to an active hub. Intelligent hubs add extra features to an active hub that are of particular importance to businesses. An intelligent hub typically is stackable (built in such a way that multiple units can be placed one on top of the other to conserve space). It also typically includes remote management support via SNMP support.

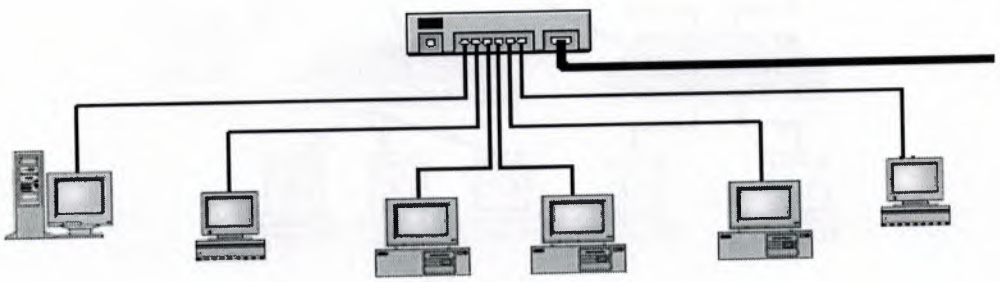

Figure 3.5 Hub in the work place

3.4.3 Switches

Switches allow you to avoid the congestion of a shared Ethernet network by permitting you to create individual segments. The improvement in network performance can be dramatic. In the figure below, the switch is being fed a 100Mbps signal. The switch is then creating four segmented networks, each with its own 10Mbps path. Net 3 and Net 4 are then connecting to a hub, creating two shared 10Mbps networks. Switches come in a variety of configurations.

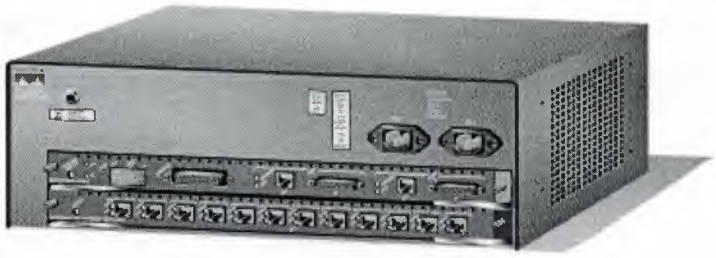

Figure 3.6 Switch

Also switch can be connected to in a large network, as shown

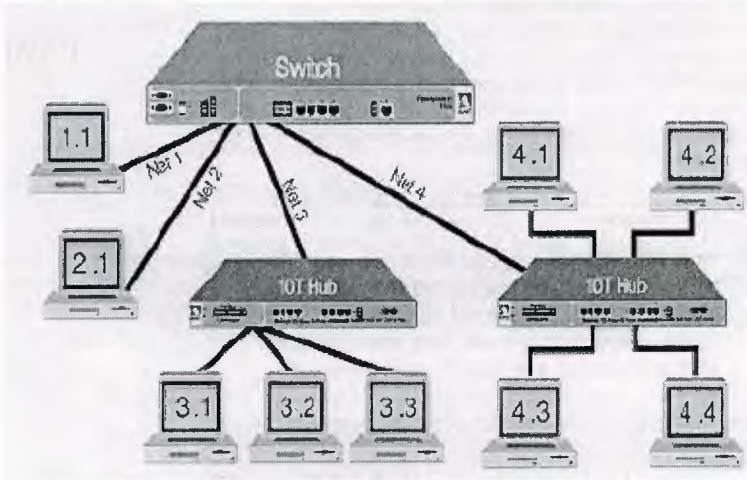

Figure 3.7 Switch connected to Hubs

3.4.4 Bridges

- Useful for breaking up subnets into small segments, making it easier to localize errors.
- Restricts traffic local to machines to that segment, by sensing what Ethernet addresses are where. This improves both network performance and privacy (makes sniffing more difficult).

- Newer bridges also have built in http servers, if possible restrict access to certain IP address/interfaces, and avoid using this service from public or potentially hostile networks.

3.4.5 Modems

A modem is used to connect a computer to the Internet. It begins with an overview of some of the basic signals the RS-232 serial interface uses to connect an external modem to a computer. The importance of these signals for proper operation of the modem will be discussed in terms of both modem and software configuration. This is known as Network Interface Card (NIC)

Figure 3.8 Modem in the work place

3.4.5.1 The Modem Plug (RS-232 Interface overview)

The EIA (Electronic Industries Association) RS-232 standard specifies signals for serial interfaces used to connect computers and modems. For technical precision, the terms Data Terminal Equipment (DTE) and Data Communication Equipment (DCE) are used to distinguish between the computer and the modem, respectively. This is useful because serial interfaces are used for many things besides computers and modems such as dumb terminals, plotters, scanners, printers, etc. These terms are important because they are used to define the interface signals. A different type of serial cable is needed to connect a modem to a computer (DTE to DCE connections use a modem cable) than is used to, say,

connect one computer to another (DTE to DTE connections use a null-modem cable). Such PC programs such as Lap-Link or the MS-DOS INTERLNK command use null modem cables.

The standard is based on a 25-pin connector, of which ten connections are commonly used. The names of the signals and the pin designations on a standard DB25 pin connector are: protective (frame) ground 1, transmit data 2, receive data 3, request to send 4, clear to send 5, data set ready 6, signal ground 7, carrier detect 8, data terminal ready 20, and ring indicator 22. Many manufacturers have designed serial connectors that use fewer connections, such as the IBM AT DB9 connector, or the Macintosh DIN 8. To simplify discussion of these signals this document will generally only refer to pin designation numbers for the standard 25-pin connector (DB25). Modem cables for computers with non-standard connectors are usually available, which provide a DB25 connector at the modem end with a subset of the 10 connections mentioned above.

Three of these connections are absolutely essential: transmit data, receive data, and signal ground. The transmit data line is where data are transmitted from the computer (DTE) to the modem (DCE). The receive data line is where data are received from the modem (DCE) by the computer (DTE). Signal ground is the reference against which all other signals apply voltage. Think of a battery and a light bulb: it is not possible for current to flow without two wires. Signal ground is the second wire for all the other signals.

3.4.5.2 Error Correction and Data Compression

Almost more confusing than the actual protocols and modem commands are the terminology used to describe error correction (also called error control). Error correction is similar to file transfer protocols such as X, Y, or Z modem. File transfer protocols break files up into chunks called packets. Error correction does the same thing except the blocks of data are called frames and are generally smaller than those typically used by modern file transfer protocols. In all cases additional information such as a checksum is added to the packet (frame) to verify that the data was undamaged in transit. If the data does not match

the checksum the entire packet or frame must be resent. This technique trades off some speed for reliability. Like sliding-windows protocol several frames may be sent before an acknowledgment is required. The maximum data block size and the number of frames allowed before an acknowledgment is required are parameters negotiated by the modems when they connect.

3.4.6 Integrated Services Digital Network (ISDN)

Integrated Services Digital Network (ISDN) is comprised of digital telephony and data transport services offered by regional telephone carriers. ISDN involves the digitalization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone. The emergence of ISDN represents an effort to standardize subscriber services, user/network interfaces, and network and Internet work capabilities. ISDN applications include high-speed image applications (such as Group IV facsimile), additional telephone lines in homes to serve the telecommuting industry, high-speed file transfer, and video conferencing. Voice service is also an application for ISDN. This chapter summarizes the underlying technologies and services associated with ISDN.

3.4.6.1 ISDN Components

ISDN components include terminals, terminal adapters (TAs), network-termination devices, line-termination equipment, and exchange-termination equipment. ISDN terminals come in two types. Specialized ISDN terminals are referred to as terminal equipment type 1 (TE1). Non-ISDN terminals, such as DTE, that predates the ISDN standards are referred to as terminal equipment type 2 (TE2). TE1s connect to the ISDN network through a four-wire, twisted-pair digital link. TE2s connect to the ISDN network through a TA. The ISDN TA can be either a standalone device or a board inside the TE2. If the TE2 is implemented as a standalone device, it connects to the TA via a standard physical-layer interface. Examples include EIA/TIA-232-C (formerly RS-232-C), V.24, and V.35. Beyond the TE1 and TE2 devices, the next connection point in the ISDN network is the network termination

type 1 (NT1) or network termination type 2 (NT2) device. These are network-termination devices that connect the four-wire subscriber wiring to the conventional two-wire local loop. In North America, the NT1 is customer premises equipment (CPE) device. In most other parts of the world, the NT1 is part of the network provided by the carrier. The NT2 is a more complicated device that typically is found in digital private branch exchanges (PBXs) and that performs Layer 2 and 3 protocol functions and concentration services. An NT1/2 device also exists as a single device that combines the functions of an NT1 and an NT2. ISDN specifies a number of reference points that define logical interfaces between functional groupings; such as TAs and NT1s. ISDN reference points include the following:

- R: The reference point between non-ISDN equipment and a TA.
- S: The reference point between user terminals and the NT2.
- T: The reference point between NT1 and NT2 devices.
- U: The reference point between NT1 devices and line-termination equipment in the carrier network. The U reference point is relevant only in North America, where the carrier network does not provide the NT1 function. Figure 12-1 illustrates a sample ISDN configuration and shows three devices attached to an ISDN switch at the central office.

Two of these devices are ISDN-compatible, so they can be attached through an S reference point to NT2 devices. The third device (a standard, non-ISDN telephone) attaches through the reference point to a TA. Any of these devices also could attach to an NT1/2 device, which would replace both the NT1 and the NT2. In addition, although they are not shown, similar user stations are attached to the far right ISDN switch.

The ISDN Basic Rate Interface (BRI) service offers two B channels and one D channel (2B+D). BRI B-channel service operates at 64 kbps and is meant to carry user data; BRI D-channel service operates at 16 kbps and is meant to carry control and signaling information, although it can support user data transmission under certain circumstances. The D channel signaling protocol comprises Layers 1 through 3 of the OSI reference model. BRI also provides for framing control and other overhead, bringing its total bit rate to 192 kbps. The BRI physical-layer specification is International Telecommunication Union

Telecommunication Standardization Sector (ITU-T) (formerly the Consultative Committee for International Telegraph and Telephone [CCITT]) I.430. ISDN Primary Rate Interface (PRI) service offers 23 B channels and one D channel in North America and Japan, yielding a total bit rate of 1.544 Mbps (the PRI D channel runs at 64 Kbps). ISDN PRI in Europe, Australia, and other parts of the world provides 30 B channels plus one 64-Kbps D channel and a total interface rate of 2.048 Mbps. The PRI physical-layer specification is

- **Layer 1**

ISDN physical-layer (Layer 1) frame formats differ depending on whether the frame is outbound (from terminal to network) or inbound (from network to terminal). The frames are 48 bits long, of which 36 bits represent data. The bits of an ISDN physical-layer frame are used as follows:

- F: Provides synchronization
- L: Adjusts the average bit value
- E: Ensures contention resolution when several terminals on a passive bus

Contend for a channel

- A: Activates devices
- S: Unassigned
- B1, B2, and D: Handles user data

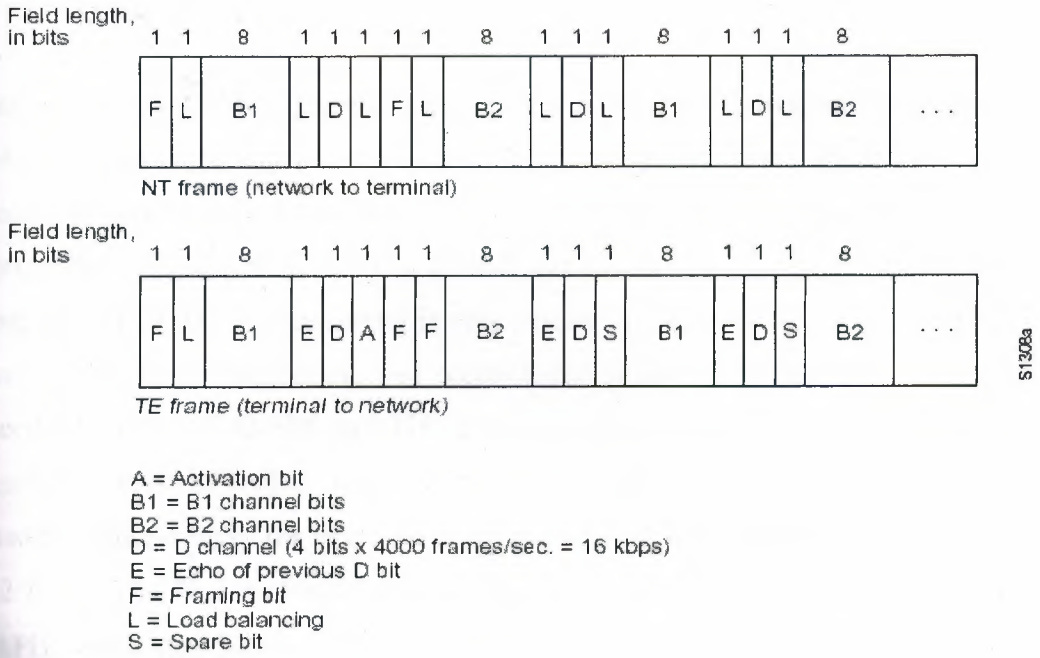

Figure 3.9 ISDN Physical-layer frame formats

Multiple ISDN user devices can be physically attached to one circuit. In this configuration, collisions can result if two terminals transmit simultaneously. ISDN therefore provides features to determine link contention. When an NT receives a D bit from the TE, it echoes back the bit in the next E-bit position. The TE expects the next E bit to be the same as its last transmitted D bit. Terminals cannot transmit into the D channel unless they first detect a specific number of ones (indicating "no signal") corresponding to a p re-established priority. If the TE detects a bit in the echo (E) channel that is different from its D bits, it must stop transmitting immediately. This simple technique ensures that only one terminal can transmit its D message at one time. After successful D- message transmission, the terminal has its priority reduced by requiring it to detect more continuous ones before transmitting. Terminals cannot raise their priority until all other devices on the same line have had an opportunity to send a D message.

Telephone connections have higher priority than all other services, and signaling information has a higher priority than non-signaling information.

- **Layer 2**

Layer 2 of the ISDN signaling protocol is Link Access Procedure, D channel (LAPD). LAPD is similar to High-Level Data Link Control (HDLC) and Link Access Procedure, Balanced (LAPB). As the expansion of the LAPD acronym indicates, this layer it is used across the D channel to ensure that control and signaling information flows and is received properly. The LAPD frame format is very similar to that of HDLC and, like HDLC, LAPD uses supervisory, information, and unnumbered frames. The LAPD protocol is formally specified in ITU-T Q.920 and ITU-T Q.921. The LAPD Flag and Control fields are identical to those of HDLC. The LAPD Address field can be either 1 or 2 bytes long. If the extended address bit of the first byte is set, the address is 1 byte; if it is not set, the address is 2 bytes. The first Address-field byte contains identifier service access point identifier (SAPI), which identifies the portal at which LAPD services are provided to Layer 3.

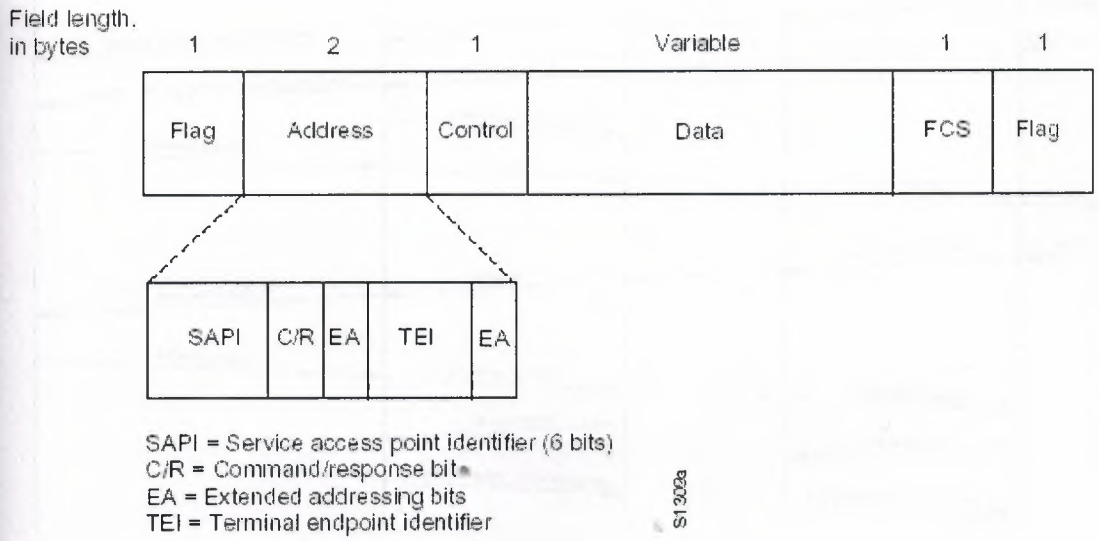

Figure 3.10 LAPD frame format is similar to HDLC and LAPB.

The C/R bit indicates whether the frame contains a command or a response. The terminal end-point identifier (TEI) field identifies either a single terminal or multiple terminals. A TEI of all ones indicates a broadcast.

- **Layer 3**

Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT.

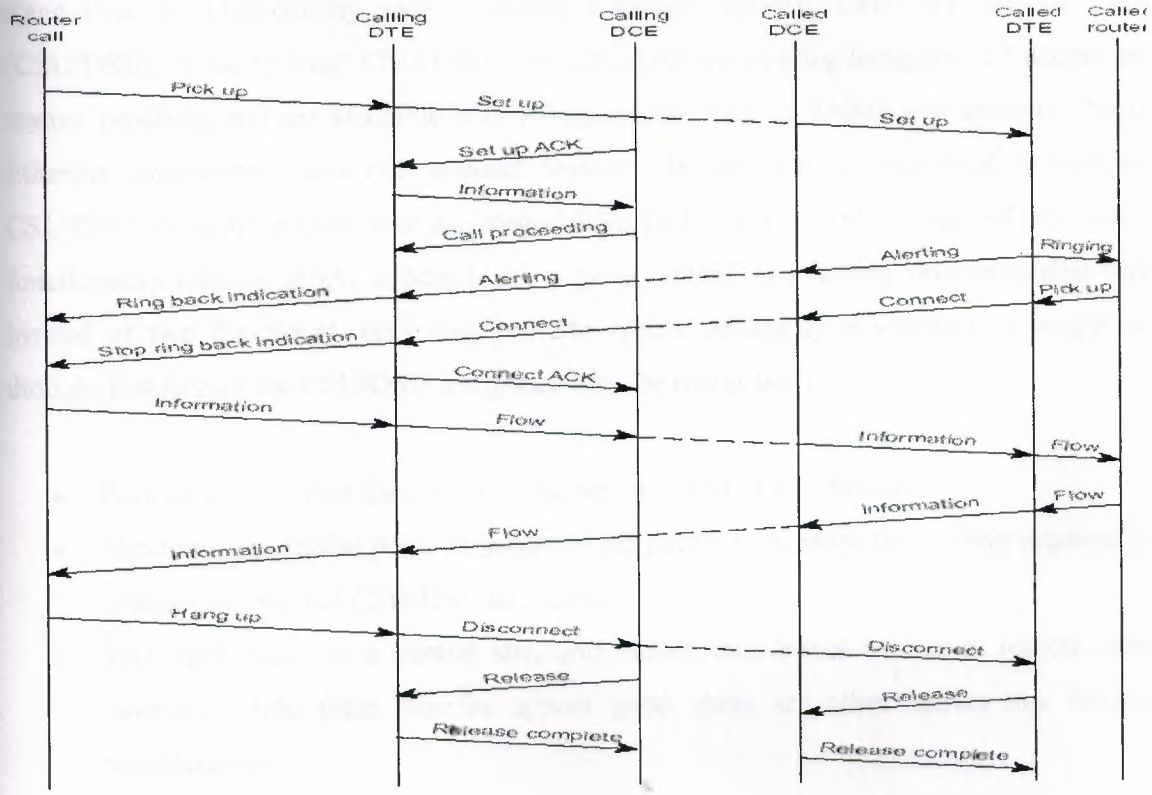

Figure 3.11 Illustration of Circuit Switch Call

3.4.7 Channel Service Unit (CSU) / Data Service Unit (DSU)

High-speed, LAN-attached applications continue to rise, generating an increasing need for cost-effective WAN access for intranet and Internet access implementation. Routed networking is today the most widely implemented network solution for organizations of all types. Digital circuits operating at speeds from 56Kbps (DDS service) to 1.544Mbps (T1 and Fractional T1 services) to T3 (45 Mbps or 28 T1's) provide the WAN infrastructure that interconnects the routers located at each location served by the network. The traditional approach to terminating DDS, T1/FT1 and T3 circuits at each location is to use a standalone or high-density rack mounted Channel Service Unit/Data Service Unit (CSU/DSU). "Line-by-line" CSU/DSUs and CSU/DSUs providing integrated T1 access are mature products, and are available with enhancements such as SNMP management, direct Ethernet connections, and dial restoral features. In addition to traditional standalone CSU/DSU solutions, routers with an integral CSU/DSU are available. Integrated CSU/DSU functionality initially might appear to be a good choice, i.e., having one integrated unit instead of two functional units may provide certain reliability advantages. It might be thought that having the CSU/DSU integrated into the router will:

- Provide a lower cost than comparable separate CSU/DSU devices
- Eliminate a potential point of failure in the network, namely, the cabling required to connect an external CSU/DSU to a router
- Save rack space at a central site, and reduce two boxes to one at remote sites however, while these benefits appear good, there are other factors that require consideration.

This management briefing will discuss that, depending on the application; integrated approaches do not necessarily save money or eliminate points of failure. In addition, this briefing will outline valuable features available only in non-integrated CSU/DSUs.

3.4.7.1 Comparing Basic Capabilities

A basic T1 network access arrangement using traditional non-integrated CSU/DSUs at both the remote and central sites.

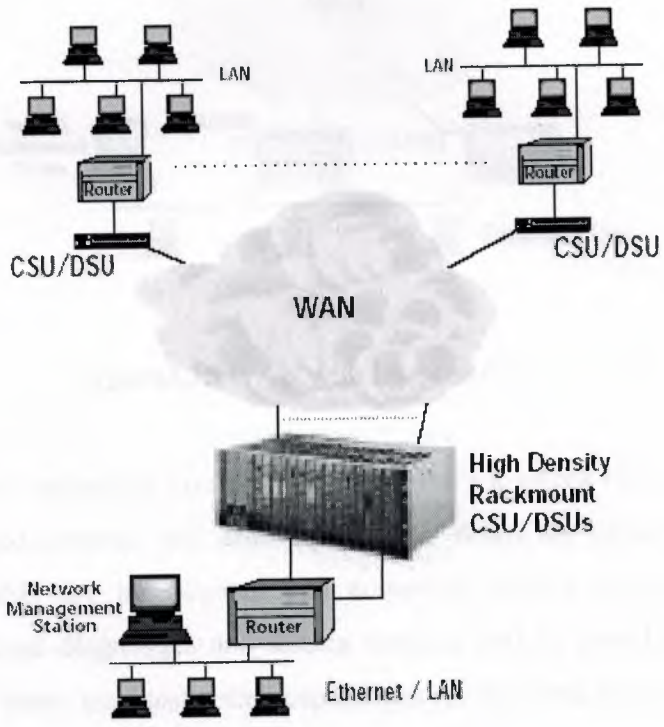

Figure 3.12 Basic T1 Network Access

The network depicted in Figure 3.14 can be viewed as either being traditional point-to-point DDS/T1 networking or as frame relay. Figure 3.16 shows the same T1 access objective achieved with integral CSU/DSUs. At first glance, it seems that the router with integral CSU/DSU approach is simpler to install and should be more cost effective. However, another look at both approaches shows that this may not be the case. Cost Savings Proponents of router-integrated T1 CSU/DSUs argue that the internal units are less costly to purchase than separate, external CSU/DSUs.

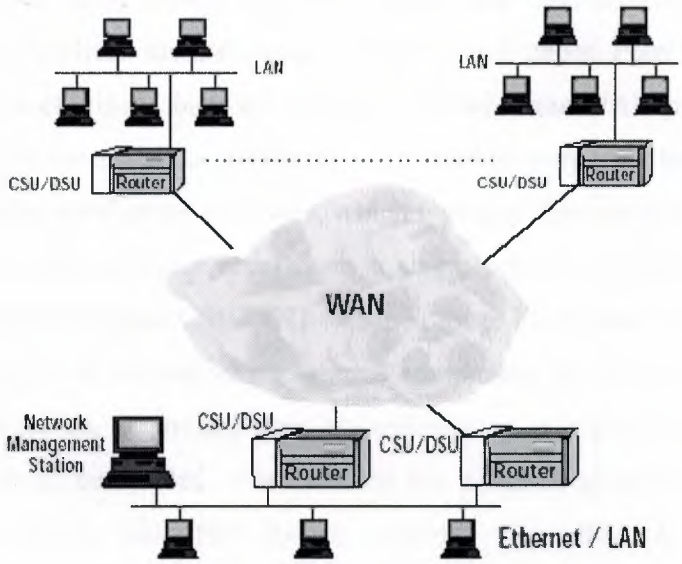

Figure3.13 WAN with Integrated Routers

Typically, however, depending on feature content, the list prices of an internal unit and a standalone managed external unit are very similar. When the capabilities of the router integrated CSU/DSU are investigated and compared against those of the standalone CSU/DSU, additional diagnostics and testing features will be found with the standalone CSU/DSU having better troubleshooting capabilities for the same price or lower. Therefore, if cost is the primary issue, external non-managed CSU/DSUs may be the lowest cost option. In many cases integral T1 DSU router ports are simply DSX type device. This means that an external Telco provided demarcation device such as a CSU or CSU/Smart Jack must be installed. Such a device introduces an additional fault point in the network and requires customer provided AC power. If a standalone CSU/DSU device is deployed, the Telco provided product and associated costs are eliminated, allowing the user to directly connect to the T1 circuit. External units offer more complete diagnostics and remote management features, providing long term operating cost savings by reducing the need to dispatch technicians to remote sites. External CSU/DSUs offer significant line cost savings by the use of efficient multiplexing. Examples of CSU/DSU features that provide the opportunity of increased network savings are multi-port CSU/DSUs that may be used to

Support inter-office PBX networking and secure and non-secure routed data paths. Examples of these applications are discussed later in this paper. Points of Failure because integral CSU/DSUs eliminate the need for a cable between the WAN port of the router and the CSU/DSU (DTE interface), a potential point of failure may have been eliminated. This may be true if cables were prone to failure, which typically they are not. However, the non-integrated solution also provides relief from a single point of failure. Should a problem occur in a router with integral CSU/DSU — much more likely than a cable failure — on-site troubleshooting to determine which internal component has failed will be necessary. If the results of the testing are in any way inconclusive or ambiguous, replacing the entire router may appear to be needed, when in fact the problem actually may be a network service problem, easily identified by an external CSU/DSU. If diagnostic testing *capabilities of an integral* CSU/DSU were deemed comparable to those of a nonintegrated CSU/DSU then the integral CSU/DSU solution would provide a superior solution. However, this is not the case by design. Many non-integrated CSU/DSUs offer superior fault isolation through comprehensive line and BERT diagnostic testing. This briefing concludes that troubleshooting the rare cable failure and its repair, is much easier and far less disruptive to the network operation than troubleshooting and replacing of a router, or the integral CSU installed in the router. Space Saving For central site rack mounting of large numbers of WAN links, the initial size of the router(s) with integral CSU/DSUs takes up much more real estate than that of a high density CSU/DSU shelf. For example, two CSU/DSUs using GDC's Spectra- Comm 2000 shelf require only 1.75" (44.45 mm) of rack height, and up to 16 CSU/DSU units can be housed in the SpectraComm 5000 shelf, which is only 7" high (180 mm).

Power Savings of power is not usually a benefit put forth by the proponents of integral CSU/DSUs. Why? Routers are designed for environmentally controlled computer rooms. Routers typically exhaust a considerable amount of heat consuming a high amount of BTUs. When a CSU/DSU is placed inside a router it becomes part of the power *consumption equation. Routers are typically AC powered with backup power (if supplied)* provided via generator.

Commercial power interruption of a router with integral CSU/DSU affects the WAN connection as well as the integral LAN. Redundant power supply modules may not be an option of many low-to-medium end routers. Lack of commercial power is a major point of failure to a router with integral CSU/DSU. Many standalone and all rack mount CSU/DSUs manufactured by GDC offer dual power options (AC and DC). Redundant power supply modules are available on all SpectraComm and Universal Access System products. All GDC CSU/DSUs, standalone as well as rack mount, use six watts or less of power. GDC CSU/DSU shelves do not use fans and due to the very low power budget design dissipate heat. Air-conditioned environments are not needed. NEBS (Network Equipment Building Standards) NEBS compliancy is a requirement when sharing Telco Central Office space, but many aspects of NEBS are beneficial to premise installations. Very few routers with integral CSU/DSUs can pass the stringent NEBS tests, and therefore, are not allowed to be installed in the Central Office. Applicable NEBS benefits include fire safety, electrical hazard and shock protection, lightning protection and power line isolation. Costly repairs and network disasters can be greatly reduced by the use of an external CSU/DSU. For example, if an integral DSU were utilized, a lightning strike of power surge on the network would travel directly into the router and conceivably pass to the LAN, which may be connected to PCs and other LAN devices. As a result, all attached users and equipment are put at risk. However, by using GDC's CSU/DSUs, which protect against hazardous line transients including power lines and transmission lines, the risk is eliminated.

3.4.7.2 Single Point of Failure

Router vendors argue that the integrated approach allows easier installation and integrating the CSU/DSU in the router eliminates two sources of possible failure:
Either the separate CSU/DSU itself or the associated cabling. Consider that the CSU/DSU is still an active component of the network and should failure occur as stated earlier, the network disruption in servicing an integrated router is much greater than that created by servicing a non-integrated CSU/DSU. Integrated CSU/DSUs do not have comparable meantime- between-failure (MTBF) ratios to that of the telecom-standard CSU/DSUs, which are typically expressed in hundreds of years. The most likely points of failure are the

local loop or the router itself, with its complicated software and integral hardware components. Strong diagnostic capabilities as described in the previous paragraphs cannot be considered an option; they are a "must have" item. If a router with a CSU/DSU fails Figure 3.20, the integral CSU/DSU functionality will be lost — or at best significantly diminished — potentially crippling any ability to troubleshoot the network.

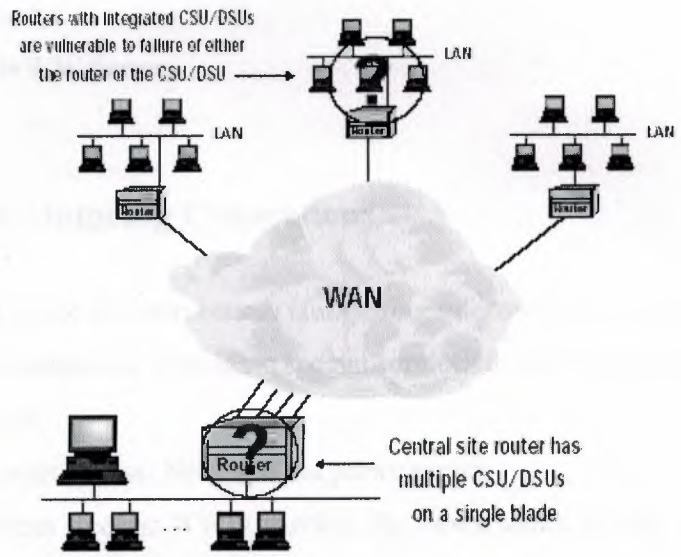

Figure Single Point of Failure Risk

3.5 External Connections to WANs

3.5.1 Permission for External Connections

For external access (via modem for example) to internal systems or from internal systems to the outside (Internet for example), a user should have the written permission. The user should prove that such an external access is absolutely necessary.

These external connections can be classed as incoming and outgoing:

3.5.1.1 Example Incoming Connections

- Dialup access for company partners.
- Dialup access for IT staff and directors.
- Access from universities (co-ordination on research projects).
- Internet Email.
- Enterprise WWW Server.
- EDI

3.5.1.2 Example Outgoing Connections

- Access to Vendor Bulletin boards (for getting information, drivers).
- Customer connections: providing special services to clients (examples?).
- Internet Email.
- Normal Internet access: Netscape via proxy server.
- Special Internet Access: WWW, Archie, ftp, news, telnet, gopher, wais.
- EDI (see above).

3.5.2 Insecure Subnets

Where many external connections are required in one building, one possibility is to group together the external connections on an "Insecure Subnet" which has direct outside access, but which is separated from the internal network via a Firewall. This minimizes cost (only one firewall) and maximizes flexibility, but great care must be taken in the daily usage on these machines on the "Insecure Subnet", as they must be considered as dangerous, penetrated hosts.

3.5.3 Network Management / Monitoring

Networks are becoming more important, data speeds and volumes are increasing and networks are becoming more and more heterogeneous. Professional Network monitoring

can help to analyze and predict problems (and increase availability). Such monitors can also be used to increase security by two methods:

- "Strange" network behavior could be an intrusion, so a monitor should be able to note "strange" (i.e. not "normal") network behavior.
- If security policy specifies that certain services are not to be used by certain hosts at specified times, network monitor software could be used to check this. e.g. if the security policy for a network specifies that ftp is not to be used between 00:00 and 06:00, then any ftp traffic on the network at this time should be monitored an reported as a security alert. This kind of monitoring is especially useful for local high security networks.
- 3- Utilities such as Satan can be used to identify devices on an IP network, as well as report on TCP/IP security problems.

Such utilities should be removed from all other machines.

4. TRANSMISSION MEDIA

4.1 Overview

Some sort of wire today connects the vast majority of networks or cabling, cable is the medium that ordinarily connects network devices. Cable's ability to transmit encoded signals enables it to carry data from one place to another. These signals may be electrical as in copper cable or light pulses as in fiber-optic cable. There are variety of cable that can meet the varying needs and sizes of networks, from small to large.

There are many cables for connecting WAN, such as:

1) Coaxial
   - Thin (thin-net)
   - Thick (thick-net)
2) Twisted Pair
   - Unshielded twisted-pair
   - Shielded twisted-pair
3) Fiber Optic
4) Wireless WAN

Table 4.1 Typical Characteristic for guided media

Medium Transmission	Total Data Rate	Bandwidth	Repeater Spacing
Twisted Pair	1-100 Mbps	100 Hz – 5 MHz	2 – 10 Km
Coaxial Cable	1 Mbps – 1 Gbps	100 Hz – 500 MHz	1 – 10 Km
Optical Fiber	2 Gbps	2 GHz	10 – 100 Km

4.2 Coaxial Cable

Coaxial cable is a cabling type where two or more separate materials share a common central axis. While several types of networking cables could be identified as having coaxial components or constructions, there are only two cable types that can support network operation using only one strand of cabling with a shared axis. These are commonly accepted as the coaxial cables, and are divided into two main categories: thick and thin coaxial cable. Broadband transmission uses the same principles as cable TV and runs on coax. Broadband and cable TV take advantage of coax's ability to transmit many signals at the same time. Each signal is called a channel. Each channel travels along at a different frequency, so it does not interfere with other channels. Coax has a large bandwidth, which means it can handle plenty of traffic at high speeds. Other advantages include its relative immunity to electromagnetic interference (as compared to twisted-pair), its ability to carry signals over a significant distance, and its familiarity to many cable installers.

Coax cable has four parts . The inner conductor is a solid metal wire surrounded by insulation. A thin, tubular piece of metal screen surrounds the insulation. Its axis of curvature coincides with that of the inner conductor, hence the name coaxial. Finally, an outer plastic cover surrounds the rest.

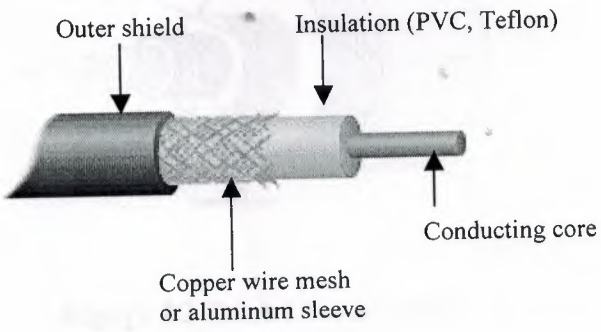

Figure 4.1 Coaxial Cable

Although coaxial cabling is not difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are: thick coaxial and thin coaxial.

4.2.1 Thick Coaxial (thick-net)

Thick coaxial is relatively rigid coaxial cable about 0.5 inch in diameter. Thick coaxial cable (also known as thick Ethernet cable, "thick-net," or 10BASE5 cable), is a cable constructed with a single solid core, which carries the network signals, and a series of Layers of shielding and insulator material. The shielding of thick coaxial cable consists of four stages. The outermost shield is a braided metal screen. The second stage shield, working inward, is usually a metal foil, but in some brands of coaxial cable may be made up of a second screen. The third stage consists of a second braided shield followed by the fourth stage, a second foil shield. The various shields are separated by non-conductive insulator materials. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

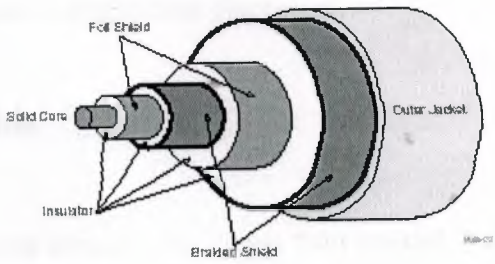

Figure 4.2 Thick Coaxial Cable

4.2.2 Thin Coaxial (thin-net)

Thin coaxial is a flexible coaxial cable about 0.25 inch thick. Thin coaxial cable (also known as thin Ethernet cable, "thin-net," "cheaper-net," RG-45, BNC or 10BASE2 cable) is a less shielded, and thus less expensive, type of coaxial cabling. Also used exclusively for Ethernet networks, thin coaxial cable is smaller, lighter, and more flexible than thick coaxial cable. The cable itself resembles (but is not identical to) television coaxial cable. Thin coaxial cable is made up of a single outer copper shield that may be braided or foil, a layer beneath that of non-conductive dielectric material, and a stranded center conductor. This shielding makes thin coaxial cable resistant to electromagnetic interference as the shielding of thick coaxial cable does, but does not provide the same extent of protection. Thin coaxial cable, due to its less extensive shielding capacity, can be run to a maximum length of 185 meters (606.7 ft).

Building Network Coax (BNC) connectors crimp onto a properly prepared cable end with a crimping tool. To prevent signal reflection on the cable, 50 Ohm terminators are used on unconnected cable ends. As with thick coaxial cable, thin coaxial cable allows multiple devices to connect to a single cable. Up to 30 transceivers may be connected to a single length of thin coaxial cable, spaced a minimum of 0.5 meter from one another. This minimum spacing requirement keeps the signals from one transceiver from interfering with the operation of others. The annular rings on the thin coaxial cable are placed 0.5 meter apart, and are a useful guide to transceiver placement.

4.3 Twisted Pair Cable

Twisted-pair cable has been around a lot longer than coaxial, but it has been carrying voice, not data. Unshielded twisted-pair is used extensively in the nationwide telephone system. Practically every home that has telephones is wired with twisted-pair cable. In the past few years, vendors have been able to transmit data over twisted-pair at reasonable speeds and distances. Some of the first PC LANs, such as Omninet or 10Net, used twisted-pair cable but could only transmit data at 1Mbit/sec. Token Ring, when it was introduced in 1984,

was able to transmit data at 4Mbits/sec over shielded twisted-pair. In 1987, several vendors announced Ethernet-like technology that could transmit data over unshielded twisted-pair, but computers can only be about 300 feet apart, not the 2,000 feet allowed by thick coax. Recent developments in technology make it possible to run even 16Mbit/sec Token Ring and 100Mbit/sec FDDI traffic over unshielded twisted-pair.

Twisted-pair offers some significant benefits. It's lighter, thinner, more flexible, and easier to install than coax or fiber-optic cable. It's also inexpensive. It is therefore ideal in offices or work groups that are free of severe electromagnetic interference.

Although there are a variety of types of twisted-pair cable types, shielded and unshielded are the two most important.

4.3.1 Unshielded Twisted pair (UTP)

Unshielded Twisted Pair cabling (referred to here as UTP, but also may be termed copper wire, 10BASE-T wire, Category 3, 4, or 5 Ethernet wire, telephone cable, or twisted pair without shielded or unshielded qualifier) is commonly made up of two, four, or 25 pairs of 22, 24, or 26 AWG unshielded copper solid or stranded wires. These pairs of wires are twisted together throughout the length of the cable, and are broken up into transmit and receive pairs. The UTP cable used in network installations is the same type of cable used in the installation of telephone lines within buildings.

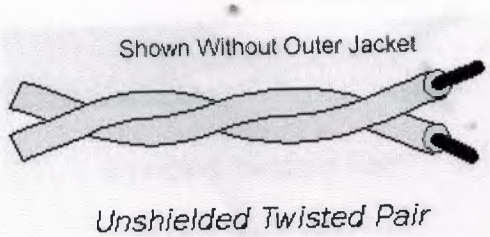

Figure 4.3 Unshielded Twisted Pair Cable

The wires that make up a length of UTP cable are numbered and color coded. These color codes allow the installer of the networking cable to determine which wires are connected to the pins of the RJ45 ports or patch panels. The numbering of the wires in EIA/TIA standard cables is based on the color of the insulating jacket that surrounds the core of each wire.

Most telephones use a type of UTP. In fact, one reason why UTP is so popular because many building are pre-wired for twisted-pair telephone systems. The potential problem in cabling is cross talk. Crosstalk is defined as the signals from one line getting mixed with signals from other line. UTP is particularly susceptible to cross talk.

4.3.2 Shielded Twisted pair (STP)

Shielded Twisted Pair cabling is a multi-stranded cable most often constructed of eight 26 AWG conductive copper solid or stranded core wires. Each wire is surrounded by a non-conductive insulating material such as Polyvinyl Chloride (PVC). These wires are twisted around one another in a specific arrangement to form pairs. The pairs are made up of associated wires - transmit wires are paired with transmit wires, receive wires are paired with receive wires. Each pair in the STP cable is then surrounded by a metallic foil shield that runs the length of the cable. Some types of STP incorporate an additional braided or foil shield that surrounds each of the shielded pairs in the cable. The overall cable is wrapped in an insulating jacket which covers the shields and holds the wires together.

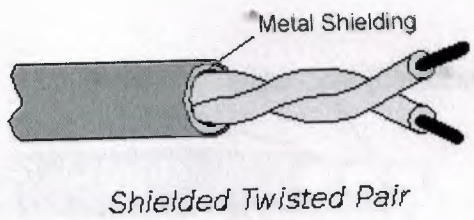

Figure 4.4 Shielded Twisted Pair Cable

Twisting the pairs together throughout the cable helps to reduce the effects of externally-induced electrical noise on the signals that pass through the cable. In each pair, one wire carries the normal network signal, while its associated wire carries a copy of the transmission that has been inverted. The twisting of associated pairs helps to reduce the interference of the other strands of wire throughout the cable. This is due to the method of transmission used with twisted pair transmissions. STP cabling is available in several different arrangements and construction styles, called Types. The type definitions are based on the IBM cabling system.

4.4 Fiber Optic Cable

A technology that uses glass (or plastic) threads (fibers) to transmit data. A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves.

Fiber optics has several advantages over traditional metal communications lines:

- Fiber optic cables have a much greater bandwidth than metal cables. This means that they can carry more data.
- Fiber optic cables are less susceptible than metal cables to interference.
- Fiber optic cables are much thinner and lighter than metal wires.
- Data can be transmitted digitally (the natural form for computer data) rather than analogically

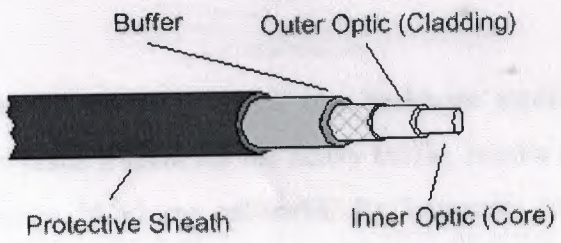

Figure 4.5 Fiber Optic Cable

ber cable consists of the following:

- Core - Thin glass center of the fiber where the light travels
- Cladding - Outer optical material surrounding the core that reflects the light back into the core
- Buffer coating - Plastic coating that protects the fiber from damage and moisture

ber-optics has been touted as the answer to all the problems of copper cable. It can carry oice, video, and data. It has enormous bandwidth and can carry signals for extremely long istances. Because it uses light pulses, not electricity to carry data, it is immune to lectromagnetic interference. It is also more secure than copper cable, because an intruder annot eavesdrop on the signals, but must physically tap into the cable. To get at the nformation inside, a device must be attached, and the light level will subsequently ecrease.

Despite its many advantages, fiber-optic's deployment in the WAN/LAN has been slow. According to Data requested, by 1993, fiber-optics held only 1.4 percent of the market. Cable installer's experience and fiber's high cost is holding back its widespread installation. Very simply, installing fiber-optic cable is very difficult. Splicing fiber-optic cables together is even more difficult. Putting connectors on the fiber-optic cable is also harder than for copper cable. The expense of diagnostic tools is another problem. Time domain reflectometers, ohmmeters, voltmeters, and oscilloscopes can be easily connected to any type of copper cable. But such tools must be specifically designed or adapted for fiber-optics use.

Fiber-optics has enjoyed its greatest success as a backbone medium for connecting sub-networks. Its properties make it ideal for the heavy traffic, hostile environments, and great distances that characterize backbone networks. Its immunity to electrical interference makes it ideal for the factory floor, another popular application. Fiber-optic cable it self is a core fiber surrounded by cladding.

Figure 4.6 New Fiber Optic Cable

A protective covering surrounds both. LEDs or light emitting diodes send the signals down the cable. A detector receives the signals and converts them back to the electrical impulses that computers can understand. While the bits are encoded into light in a number of ways, the most popular method is to vary the intensity of the light.

Fiber-optic cable can be multimode or single-mode. In single-mode cable, the light travels straight down the fiber, which means data can travel greater distances. But since single-mode cable has a larger diameter than multimode cable, it is harder (more expensive) to manufacture. In multimode cable, the light bounces off the cable's walls as it travels down, which causes the signals to weaken sooner, and therefore data cannot travel great distances. Single-mode cable is most often used in the nation-wide telephone system.

Standards for fiber-optic have been developed. ANSI's Fiber Distributed Data Interface (FDDI) describes a network that can transmit data at 100Mbits/sec. It also specifies a dual, counter-rotating ring, which makes it fault tolerant. The IEEE has also developed standards for fiber-optic Ethernet.

Fiber-optics has enormous potential. Its capacities are tremendous. When wiring a new building, the best strategy is to run fiber-optic backbones, with twisted-pair to the desktops.

4.4.1 Advantages and Disadvantages of Fiber Optic

There are several advantages that have been established with the development and implementation of fiber-optic cable systems. Compared to copper, optical fiber is relatively small in size and light in weight. This characteristic has made it desirable as intra-floor conduits and wiring duct space has become increasing plugged with expanded copper cable installation.

Optical fiber is also desirable because of its electromagnetic immunity. Since fiber-optics use light to transmit a signal, it is not subject to electromagnetic interference, radio frequency interference, or voltage surges. This may be an important consideration when laying cables near electronic hardware such as computers or industrial equipment. As well, since it does not use electrical impulses, it does not produce electric sparks which can be an obvious fire hazard.

Advances in optical fiber technology have lead to decreases in signal loss, or attenuation. As an electric pulse or a light pulse travels down its respective cable line, it will eventually lose signal energy due to imperfections in the transmission medium. To keep the signal going, it must be boosted every so often along the medium line. A signal regenerator is used to boost the electronic pulse in a copper cable. An optical repeater is used to boost the light pulse in a fiber-optic cable. The advantage of optical fiber is that it performs better with respect to attenuation. Fiber-optic cable needs fewer boosting devices, along the same length of line, than copper cable.

A characteristic feature of optical fiber that has yet to be fully realized is it's potentially wide bandwidth. Bandwidth refers to the amount of information that a fiber can carry. The greater the bandwidth, the greater the carrying capacity of the optical fiber., the fastest fiber circuits used in trunk connections between cities and countries carry information at up to 2.5 gigabits per second, enough to carry 40,000 telephone Conversations or 250 television

channels. Experts predict larger bandwidths than this as light frequency separation becomes available.

A disadvantage of the fiber-optic system is it's incompatibility with the electronic hardware systems that make up today's world. This inability to interconnect easily requires that current communication hardware systems be somewhat retrofitted to the fiber-optic networks. Much of the speed that is gained through optical fiber transmission can be inhibited at the conversion points of a fiber-optic chain. When a portion of the chain experiences heavy use, information becomes jammed in a bottleneck at the points where conversion to, or from, electronic signals is taking place. Bottlenecks like this should become less frequent as microprocessors become more efficient and fiber-optics reach closer to a direct electronic hardware interface.

4.5 Wireless WAN

Wireless WANs are hardly new. They have been utilized since the mid 1980s when microwave transmissions were beamed about by complex and powerful transmit-ting units that required Federal Communications Commission (FCC) licenses and radios and antennas. Today, wireless systems can deliver up to 100 Mb/s speeds at 40 miles' distance, and speeds are increasing.

Recognizing the critical need for faster data transmission and improved security, IEEE ratified what it called the 802.11b high rate standard, which permits transmissions at 5.5 and 11 Mb/s. The revised standard fostered explosive growth in wireless LANs in the business com-mutiny and, more recently, in schools because it promised wireless transmission speeds rivaling the wired Ethernet. In practice, however, IEEE 802.11b only permitted a data transmission rate of about 7 Mb/s-still impressive, but insufficient to transfer data, for instance, a digital video disk or a video file.

4.5.1 Interference, Security, and Reliability

If other cost-effective, high speed wireless products operating on the licensed 5 GHz frequency band become available, schools will be able to transmit data more securely over their wireless WANs. Experts are debating the value of the 5 GHz products for building to building connectivity. Of note are concerns over licensing issues and the shorter transmission distances possible on this frequency compared to the two lower frequencies 900 MHz and 2.4 GHz presently authorized by the FCC for unlicensed microwave transmission. Most wireless WANs operate on the 2.4 GHz band.

But there is still the security issue to consider. Present wireless WAN security technology offers two levels of encryption: 40 bit and 128 bit. Typically, 40-bit encryption should be sufficient to prevent unauthorized entry.

For greater security, experts recommend 128-bit encryption. Encrypting signals that traverse the wireless link itself is just one of several layers of security that a school should provide for its computer networks. Other appropriate security methods such as password authentication, fire-walls, and virtual private network solutions can greatly reduce security risks for users and for LAN-based resources networked over a wireless WAN.

Wireless systems sometimes can be considered more reliable than leased lines because all the wireless equipment belongs to the owner and remains on the owner.

Leased lines may experience problems caused by power failures or other interruptions, including unscheduled repairs and maintenance by utility companies. Microwave transmissions can travel up to 25 miles without significant signal degradation and can withstand most weather conditions, including wind, rain, and snow, although they are susceptible to heavy fog. But severe wind might dislodge an antenna, and caked ice and snow can degrade signals. Antennas must also be protected by lightning arrestors to avoid severe damage and consequent loss of service.

2 Infrastructure Requirements

hardware required to install a wireless WAN is simple. It consists of access points, ch provide access for all users to the wireless network, antennas with mounting ware and lightning arrestors, rooftop antenna towers of varying heights as needed, ing required to connect antennas to the LAN, and access to standard electrical outlets each access point. In each building, the wireless network terminates at an access point connects to a local hub or switch and serves as a bridge to the wired LAN. Access ts must be located as close as possible to the building antenna (less than 25 feet is erred to avoid loss of band-width) and must be protected from the elements.

5. NETWORK SECURITY

5.1 Overview

Network security is vital. Many applications send unencrypted passwords across the network. Although a network cannot be completely secured, the weakest links should be protected. It is not realistic to expect the Network to be ever 100% secure. The are two principal tendencies in network security today:

1. New applications being developed are often designed so that they can transfer data securely across insecure networks. i.e. some type of authentication / encryption is built-in.
2. IP level encryption (for TCP/IP networks) offers a secure channel between two machines, even over insecure networks.

5.2 Types and Sources of Network Threats

Now, we've covered enough background information on networking that we can actually get into the security aspects of all of this. First of all, we'll get into the types of threats there are against networked computers, and then some things that can be done to protect you against various threats.

5.2.1 Denial-of-Service

DOS (Denial-of-Service) attacks are probably the nastiest, and most difficult to address. These are the nastiest, because they're very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker, without also refusing legitimate requests for service.

The premise of a DoS attack is simple: send more requests to the machine than it can handle. There are toolkits available in the underground community that make this a simple matter of running a program and telling it which host to blast with requests. The attacker's program simply makes a connection on some service port, perhaps forging the packet's header information that says where the packet came from, and then dropping the connection. If the host is able to answer 20 requests per second, and the attacker is sending 50 per second, obviously the host will be unable to service all of the attacker's requests, much less any legitimate requests (hits on the web site running there, for example).

Some things that can be done to reduce the risk of being stung by a denial of service attack include

- Not running your visible to the world servers at a level too close to capacity
- Using packet filtering to prevent obviously forged packets from entering into your network address space.
- Keeping up to date on security-related patches for your hosts operating systems.

5.2.2 Unauthorized Access

Unauthorized access is a very high-level term that can refer to a number of different sorts of attacks. The goal of these attacks is to access some resource that your machine should not provide the attacker. For example, a host might be a web server, and should provide anyone with requested web pages. However, that host should not provide command shell access without being sure that the person making such a request is someone who should get it, such as a local administrator.

5.2.2.1 Executing Commands Illicitly

It's obviously undesirable for an unknown and un-trusted person to be able to execute commands on your server machines. There are two main classifications of the severity of this problem: normal user access, and administrator access. A normal user can do a number of things on a system (such as read files, mail them to other people, etc.) that an attacker should not be able to do. This might, then, be all the access that an attacker needs. On the

other hand, an attacker might wish to make configuration changes to a host (perhaps changing its IP address, putting a start-up script in place to cause the machine to shut down every time it's started or something similar). In this case, the attacker will need to gain administrator privileges on the host.

5.2.2.2 Confidentiality Breaches

We need to examine the threat model: what is it that you're trying to protect yourself against? There is certain information that could be quite damaging if it fell into the hands of a competitor, an enemy, or the public. In these cases, it's possible that compromise of a normal user's account on the machine can be enough to cause damage (perhaps in the form of PR, or obtaining information that can be used against the company, etc.)

While many of the perpetrators of these sorts of break-ins are merely thrill-seekers interested in nothing more than to see a shell prompt for your computer on their screen, there are those who are more malicious, as we'll consider next. (Additionally, keep in mind that it's possible that someone who is normally interested in nothing more than the thrill could be persuaded to do more: perhaps an unscrupulous competitor is willing to hire such a person to hurt you.)

5.2.2.3 Destructive Behavior

Among the destructive sorts of break-ins and attacks, there are two major categories.

Data Diddling: The data diddle is likely the worst sort, since the fact of a break-in might not be immediately obvious. Perhaps he's toying with the numbers in your spreadsheets, or changing the dates in your projections and plans. Maybe he's changing the account numbers for the auto-deposit of certain paychecks. In any case, rare is the case when you'll come in to work one day, and simply know that something is wrong. An accounting procedure might turn up a discrepancy in the books three or four months after the fact. Trying to track the problem down will certainly be difficult, and once that problem is discovered.

Data Destruction: Some of those perpetrate attacks are simply twisted jerks who like to delete things. In these cases, the impact on your computing capability and consequently

your business can be nothing less than if a fire or other disaster caused your computing equipment to be completely destroyed.

5.2.3 Avoid Systems with Single Points of Failure

Any security system that can be broken by breaking through any one component isn't really very strong. In security, a degree of redundancy is good, and can help you protect your organization from a minor security breach becoming a catastrophe.

5.3 Firewalls

As we've seen in our discussion of the Internet and similar networks, connecting an organization to the Internet provides a two-way flow of traffic. This is clearly undesirable in many organizations, as proprietary information is often displayed freely within a corporate intranet (that is, a TCP/IP network, modeled after the Internet that only works within the organization).

In order to provide some level of separation between an organization's intranet and the Internet, firewalls have been employed. A firewall is simply a group of components that collectively form a barrier between two networks.

A number of terms specific to firewalls and networking are going to be used throughout this section, so let's introduce them all together.

1- Bastion host: A general-purpose computer used to control access between the internal (private) network (intranet) and the Internet (or any other un-trusted network). Typically, these are hosts running a flavor of the UNIX operating system that has been customized in order to reduce its functionality to only what is necessary in order to support its functions. Many of the general-purpose features have been turned off, and in many cases, completely removed, in order to improve the security of the machine.

2- Router: A special purpose computer for connecting networks together. Routers also handle certain functions, such as routing, or managing the traffic on the networks they connect.

3- Access Control List (ACL): Many routers now have the ability to selectively perform their duties, based on a number of facts about a packet that comes to it. This includes things like origination address, destination address, destination service port, and so on. These can be employed to limit the sorts of packets that are allowed to come in and go out of a given network.

4- Demilitarized Zone (DMZ): The DMZ is a critical part of a firewall: it is a network that is neither part of the un-trusted network, nor part of the trusted network. But, this is a network that connects the un-trusted to the trusted. The importance of a DMZ is tremendous: someone who breaks into your network from the Internet should have to get through several layers in order to successfully do so. Those layers are provided by various components within the DMZ.

5- Proxy: This is the process of having one host act in behalf of another. A host that has the ability to fetch documents from the Internet might be configured as a proxy server, and host on the intranet might be configured to be proxy clients. In this situation, when a host on the intranet wishes to fetch the, for example, the browser will make a connection to the proxy server, and request the given URL. The proxy server will fetch the document, and return the result to the client. In this way, all hosts on the intranet are able to access resources on the Internet without having the ability to direct talk to the Internet.

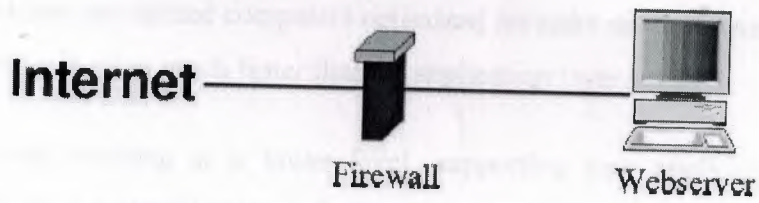

Figure 5.1 Firewall in the work place

5.3.1 Types of Firewalls

There are three basic types of firewalls, and we'll consider each of them.

5.3.1.1 Application Gateways

The first firewalls were application gateways, and are sometimes known as proxy gateways. These are made up of bastion hosts that run special software to act as a proxy server. This software runs at the Application Layer of our old friend the ISO/OSI Reference Model, hence the name. Clients behind the firewall must be proxitized (that is, must know how to use the proxy, and be configured to do so) in order to use Internet services. Traditionally, these have been the most secure, because they don't allow anything to pass by default, but need to have the programs written and turned on in order to begin passing traffic.

These are also typically the slowest, because more processes need to be started in order to have a request serviced.

5.3.1.2 Packet Filtering

Packet filtering is a technique whereby routers have ACLs (Access Control Lists) turned on. By default, a router will pass all traffic sent it, and will do so without any sort of restrictions. Employing ACLs is a method for enforcing your security policy with regard to what sorts of access you allow the outside world to have to your internal network, and vice versa.

There is less overhead in packet filtering than with an application gateway, because the feature of access control is performed at a lower ISO/OSI layer (typically, the transport or session layer). Due to the lower overhead and the fact that packet filtering is done with routers, which are specialized computers optimized for tasks related to networking, a packet filtering gateway is often much faster than its application layer cousins.

Because we are working at a lower level, supporting new applications either comes automatically, or is a simple matter of allowing a specific packet type to pass through the gateway. (Not that the possibility of something automatically makes it a good idea; opening

things up this way might very well compromise your level of security below what your policy allows.)

There are problems with this method, though. Remember, TCP/IP has absolutely no means of guaranteeing that the source address is really what it claims to be. As a result, we have to use layers of packet filters in order to localize the traffic. We can't get all the way down to the actual host, but with two layers of packet filters, we can differentiate between a packet that came from the Internet and one that came from our internal network. We can identify which network the packet came from with certainty, but we can't get more specific than that.

5.3.1.3 Hybrid Systems

In an attempt to marry the security of the application layer gateways with the flexibility and speed of packet filtering, some vendors have created systems that use the principles of both.

In some of these systems, new connections must be authenticated and approved at the application layer. Once this has been done, the remainder of the connection is passed down to the session layer, where packet filters watch the connection to ensure that only packets that are part of an ongoing (already authenticated and approved) conversation are being passed.

Other possibilities include using both packet filtering and application layer proxies. The benefits here include providing a measure of protection against your machines that provide services to the Internet (such as a public web server), as well as provide the security of an application layer gateway to the internal network. Additionally, using this method, an attacker, in order to get to services on the internal network, will have to break through the access router, the bastion host, and the choke router.

5.4 Secure Network Devices

It's important to remember that the firewall only one entry point to your network. Modems, if you allow them to answer incoming calls, can provide an easy means for an attacker to

sneak around (rather than through) your front door (or, firewall). Just as castles weren't built with moats only in the front, your network needs to be protected at all of its entry points.

5.4.1 Secure Modems: Dial-Back Systems

If modem access is to be provided, this should be guarded carefully. The terminal server, or network device that provides dial-up access to your network needs to be actively administered, and its logs need to be examined for strange behavior. Its password need to be strong -- not ones that can be guessed. Accounts that aren't actively used should be disabled. In short, it's the easiest way to get into your network from remote: guard it carefully.

There are some remote access systems that have the feature of a two-part procedure to establish a connection. The first part is the remote user dialing into the system, and providing the correct used and password. The system will then drop the connection, and call the authenticated user back at a known telephone number. Once the remote user's system answers that call, the connection is established, and the user is on the network. This works well for folks working at home, but can be problematic for users wishing to dial in from hotel rooms and such when on business trips.

Other possibilities include one-time password schemes, where the user enters his used, and is presented with a ``challenge," a string of between six and eight numbers. He types this challenge into a small device that he carries with him that looks like a calculator. He then presses enter, and a ``response" is displayed on the LCD screen. The user types the response, and if all is correct, he login will proceed. These are useful devices for solving the problem of good passwords, without requiring dial-back access. However, these have their own problems, as they require the user to carry them, and they must be tracked, much like building and office keys.

No doubt many other schemes exist. Take a look at your options, and find out how what the vendors have to offer will help you enforce your security policy effectively.

5.4.2 Crypto-Capable Routers

A feature that is being built into some routers is the ability to session encryption between specified routers. Because traffic traveling across the Internet can be seen by people in the middle who have the resources (and time) to snoop around, these are advantageous for providing connectivity between two sites, such that there can be secure routes.

5.4.3 Virtual Private Networks

Given the ubiquity of the Internet, and the considerable expense in private leased lines, many organizations have been building VPNs (Virtual Private Networks). Traditionally, for an organization to provide connectivity between a main office and a satellite one, an expensive data line had to be leased in order to provide direct connectivity between the two offices. Now, a solution that is often more economical is to provide both offices connectivity to the Internet. Then, using the Internet as the medium, the two offices can communicate.

The danger in doing this, of course, is that there is no privacy on this channel, and it's difficult to provide the other office access to ``internal'' resources without providing those resources to everyone on the Internet.

VPNs provide the ability for two offices to communicate with each other in such a way that it looks like they're directly connected over a private leased line. The session between them, although going over the Internet, is private (because the link is encrypted), and the link is convenient, because each can see each others' internal resources without showing them off to the entire world.

A number of firewall vendors are including the ability to build VPNs in their offerings, either directly with their base product, or as an add-on. If you have needed to connect several offices together, this might very well be the best way to do it.

5.5 Passwords

The most basic lock for your front door is a password. Ensure that every computer on your network requires a password before anyone from the network can read your information or write to your hard drive. If a password isn't required, there is no front door at all. If you're not sure how to ensure that passwords are necessary, I strongly recommend getting hold of a computer expert, or at least a very good manual. Most computer systems will not password-lock someone sitting at the computer it self.

There are ways to do it, but there's usually a way that someone at the computer itself (not on the network) can get in and change the passwords. This is to prevent the computer from becoming an expensive doorstop if the passwords are forgotten. This does, however, mean that you still need physical security.

Changing forgotten passwords isn't easy, however. It's better not to forget them in the first place. If your system has a 'master password' that has access to everything, make sure two people in your company or household know that password. If there's only one, what happens when that person is on vacation on that tropical island with no phones?

Passwords are only as secure as they are difficult to guess, if your password is your name, for instance, or the word 'password', it's like putting a lock on the front door and never bothering to actually lock it.

There are a lot of suggestions for how to make passwords difficult to guess, here're a few of them:

1- No less than eight characters long include upper and lower case letters, numbers and punctuation marks.

2- Don't use anything which can be guessed by someone who knows you or has your information no names of family members or pets, no license numbers or passport numbers or phone numbers or similar, not a street address (current or past!), not any words which are visible from your desk.

3- No legitimate words in any language, brand names or logos.

4- Not a simple substitution as (ABC or 123).

5- Not the same password as on as another computer, or the same one you had last year. Any password can be figured out in time, and if someone guesses one of your passwords the might try the same thing for another computer.

Suggestions for good passwords include:

1- Take something you'll recognize a line from a book or a line of poetry and use the third letter of each word. Include punctuation (but not spaces).

2- A really, bad misspelling of a word · two words from different languages stuck together with punctuation marks · a short phrase.

5.6 RIVEST-ADI SHAMIR-LEONARD ADLEMAN (RSA) ENCRYPTION

5.6.1 Encryption

Encryption is the act of encoding text so that others not privy to the decryption mechanism (the "key") cannot understand the content of the text. Encryption has long been the domain of spies and diplomats, but recently it has moved into the public eye with the concern of the protection of electronic transmissions and digitally stored data.

6.2 Public Key Cryptography

ne of the biggest problems in cryptography is the distribution of keys. Suppose you live in e United States and want to pass information secretly to your friend in Europe. If you

truly want to keep the information secret, you need to agree on some sort of key that you and he can use to encode/decode messages. But you don't want to keep using the same key, or you will make it easier and easier for others to crack your cipher. But it's also a pain to get keys to your friend. If you mail them, they might be stolen. If you send them cryptographically, and someone has broken your code, that person will also have the next key. If you have to go to Europe regularly to hand-deliver the next key, that is also expensive. If you hire some courier to deliver the new key, you have to trust the courier, etc.

5.6.2.1 Trap-Door Ciphers

But imagine the following situation. Suppose you have a special method of encoding and decoding that is "one way" in a sense. Imagine that the encoding is easy to do, but decoding is very difficult. Then anyone in the world can encode a message, but only one person can decode it. Such methods exist, and they are called "one way ciphers" or "trap door ciphers".

Here's how they work. For each cipher, there is a key for encoding and a different key for decoding. If you know the key for decoding, it is very easy to make the key for encoding, but it is almost impossible to do the opposite to start with the encoding key and work out the decoding key.

So to communicate with your friend in Europe, each of you has a trap door cipher. You make up a decoding key **Da** and generate the corresponding encoding key **Ea** your friend does exactly the same thing, but he makes up a decoding key **Db** and generates the corresponding encoding key **Eb** You tell him **Ea** (but not **Da_**) and he tells you **Eb** _ (but not **Db**) Then you can send him messages by encoding using **Eb**_ _ (which only he can decode) and vice-versa—he encodes messages to you using **Ea** (which only you can decode, since you're the only person with access to **Da**).

Now if you want to change to a new key, it is no big problem. Just make up new pairs and exchange the encoding keys. If the encoding keys are stolen, it's not a big deal.

The person who steals them can only encode messages—they can't decode them. In fact, he encoding keys (sometimes called "public keys") could just be published in a well-known location. It's like saying, "If you want to send me a private message, encode it using this key, and I will be the only person in the world who can read it." But be sure to keep the decoding key (the "private key") secret.

5.6.2.2 Certification

There is, of course, a problem with the scheme above. Since the public keys are really public, anyone can "forge" a message to you. So your enemy can pretend to be your friend and send you a message just like your friend can—they both have access to the public key. Your enemy's information can completely mislead you. So how can you be certain that a message that says it is from your friend is really from your friend? Here is one way to do it, assuming that you both have the public and private keys **Ea Eb Da Db** and as discussed in the previous section. Suppose I wish to send my friend a message that only he can read, but in such a way that he is certain that the message is from me. Here's how to do it. I will take my name, and pretend that it is an encoded message, and decode it using Da I am the only person who can do this, since I am the only person who knows **Da** Then I include that text in the real message I wish to send, and I encode the whole mess Using **Eb** which only my friend knows how to decode. When he receives it, he will decode it using **Db** and he will have a message with an additional piece of what looks to him like junk characters. The junk characters are what I got by "decoding" my name. So he simply encodes the junk using my public key **Ea** and makes certain that it is my name. Since I am the only one who knows how to make text that will encode to my name, he knows the message is from me.

We can encode any text for certification, and in fact, you should probably change it with each message, but it's easy to do. Your message to your friend would look like this: "Attack at dawn. Here is my decoding of 'ABCDEFG': 'JDLEODK'." To assure privacy, for each message, change the "ABCDEFG" and the corresponding "JDLEODK".

5.6.3 RSA Encryption

OK, in the previous section we described what is meant by a trap-door cipher, but how do you make one? One commonly used cipher of this form is called "RSA Encryption",
It is based on the following idea:

It is very simple to multiply numbers together, especially with computers. But it can be very difficult to factor numbers. For example, if I ask you to multiply together 34537 and 99991, it is a simple matter to punch those numbers into a calculator and 3453389167. But the reverse problem is much harder. Suppose I give you the number 1459160519. I'll even tell you that I got it by plying together two integers. Can you tell me what they are? This is a very difficult problem. A computer can factor that number fairly quickly, but (although there are some tricks) it basically does it by trying most of the possible combinations. For any size number, the computer has to check something that is of the order of the size of the square-root of the number to be factored. In this case, that square-root is roughly 38000.

Now it doesn't take a computer long to try out 38000 possibilities, but what if the number to be factored is not ten digits, but rather 400 digits? The square-root of a number with 400 digits is a number with 200 digits. The lifetime of the universe is approximately 10/18 seconds – an 18 digit number. Assuming a computer could test one million factorizations per second, in the lifetime of the universe it could check 10/24 possibilities. But for a 400 digit product, there are 10/200 possibilities. This means the computer would have to run for 10/176 times the life of the universe to factor the large number.
It is, however, not too hard to check to see if a number is prime in other words to check to see that it cannot be factored. If it is not prime, it is difficult to factor, but if it is prime, it is not hard to show it is prime.

So RSA encryption works like this. I will find two huge prime numbers, p and q _ that have 100 or maybe 200 digits each. I will keep those two numbers secret (they are my private key), and I will multiply them together to make a number N=pq That number N is

basically my public key. It is relatively easy for me to get N I just need to multiply my two numbers. But if you know N it is basically impossible for you to find p and q To get them, you need to factor N, which seems to be an incredibly difficult problem.

But exactly how is N used to encode a message, and how are p and q used to decode it? Below is presented a complete example, but I will use tiny prime numbers so it is easy to follow the arithmetic. In a real RSA encryption system, keep in mind that the prime numbers are huge.

In the following example, suppose that person A wants to make a public key, and that person B wants to use that key to send A a message. In this example, we will suppose that the message A sends to B is just a number. We assume that A and B have agreed on a method to encode text as numbers. Here are the steps:

1. Person A selects two prime numbers. We will use p=23 and q=41 for this example, but keep in mind that the real numbers person A should use should be *much* larger.
2. Person A multiplies p and q together to get pq= (23)(41)=943 _ is the "public key", which he tells to person B (and to the rest of the world, if he wishes).
3. Person A also chooses another number which must be relatively prime to (p-1)(q-1) In this case, (p-1)(q-1)=(22)(40)=880 so e=7 is fine. E is also part of the public key, so B also is told the value of e.
4. Now B knows enough to encode a message to A. Suppose, for this example, that the message is the number M=35
5. B calculates the $C=M^e \pmod N = 35^7 \pmod{943}$ value of 35^7 =64339296875 and 6433929875(mod 943)=545.

the number 545 is the encoding that B sends to A

1. Now A wants to decode 545. To do so, he needs to find a number d such that $ed = 1 \pmod{(p-1)(q-1)}$ or in this case, such that 7d= 1(mod 880).

A solution is d=503, since 7*503=3521=4(880)+1=1(mod 880).

8. To find the decoding, A must calculate $C^d \pmod N = 545^{503} \pmod{943}$ This looks like it will be a horrible calculation, and at first it seems like it is, but notice that

503=256+128+64+32+16+4+2+1 (this is just the binary expansion of 503). So this means that $545^{503} = 545^{256+128+64+32+16+4+2+1} = 545^{256}\ 545^{128} \ldots 545^{1}$.

But since we only care about the result (mod943), we can calculate all the partial results in that modulus, and by repeated squaring of 545, we can get all the exponents that are powers of 2. For example, $545^{2} (\text{mod}\, 943) = 545.545 = 297025 (\text{mod}\, 943) = 923$

Then square again:

$545^{4} (\text{mod}\, 943) = 545^{2^{2}} (\text{mod}\ 943) = 923.923 = 851929 (\text{mod}\ 943) = 400$

and so on. We obtain the following table:

$545^{1} (\text{mod}\, 943) = 545$

$545^{2} (\text{mod}\, 943) = 923$

$545^{4} (\text{mod}\, 943) = 400$

$545^{8} (\text{mod}\, 943) = 633$

$545^{16} (\text{mod}\, 943) = 857$

$545^{32} (\text{mod}\, 943) = 795$

$545^{64} (\text{mod}\, 943) = 215$

$545^{128} (\text{mod}\, 943) = 18$

$545^{256} (\text{mod}\, 943) = 324$

So the result we want is:

$545^{503} (\text{mod}\, 943) = 324.18.215.795.400.923.545 (\text{mod}\, 943) = 35.$

Using this tedious (but simple for a computer) calculation, A can decode B's message and obtain the original message N=35

5.6.3.1 Simple Explanation of RSA

Let p and q be distinct large primes and let n be their product. Assume that we also computed two integers, d (for decryption) and e (for encryption) such that d * e 1 (mod ø(n)) where $ø(n)$ is the number of positive integers smaller than n that have no factor except

1 in common with n The integers n and e are made public, while p, q, and d are kept secret. Let m be the message to be sent, where m is a positive integer less than and relatively prime to n. A plaintext message is easily converted to a number by using either the alphabet position of each letter (a=01, b=02,..., z=26) or using the standard ASCII table. If necessary (so that $m<n$), the message can be broken into several blocks.
The encoder computes and sends the number

$m' = m^e \bmod n$

To decode, we simply compute
$e^d \bmod n$

Now, since both n and e are public, the question arises: can we compute d from them ? The answer: it is possible, if n is factored into prime numbers. The security of RSA depends on the fact that it takes an impractical amount of time to factor large numbers.

CONCLUSION

This Project presented inclusive information for implementing Wide Area Network (WAN). Wide Area Networks are today's need as we can connect many LANs working in different buildings. We can establish communication between many regions and their terminals. Every one can share information easily without wastage of time from any terminal attached to a WAN. There are some basic components for WAN which help to accomplish this communication between each terminal and other LANs. It also uses some reference models, which are standards communications and protocols.

All these technologies, which I had explained, are basic components to make communication; in other hand there are some WAN essentials, which include software and hardware parts without which communication may can not be possible.

REFERENCES

[1] Michael Alexander, "*The Underground Guide to Computer Networks*", Fourth Edition, Addison-Wesley Press, November 1995.

[2] James Thomos, "*Data and Computer Communication*", Fourth Edition, North Holland publishing Company, August 1994.

[3] Tanebaum Andrew S., "*Computer Networks*", 1996

[4] *Cisco IOS Wide Area Networking Solutions.* Indianapolis: Cisco Press, 1999.

[5] Edward G. Amoroso, "*Fundamentals of Computer Security and Network Technology*", Second Edition, Prentice Hall, May1994.