NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

WIDE AREA NETWORKS AND DEVICES USED IN WAN

Graduation Project
COM- 400

Student: Muhammad Ahmad Mian (2001581)

Supervisor: Dr. Jamal Fathi

Nicosia-2002

Dedicated to my Respected Father

ACKNOWLEDGEMENTS

Firstly I would like to present my special appreciation to my supervisor Dr. Jamal Fathi, 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 with me 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. Their reluctance and friendly environment for me has helped me allot. I want to thank them as they contributed their time and provided very helpful suggestions to me.

CONTENTS

1. INTRODUCTION

1.1 Overview

This chapter introduces the various protocols and technologies used in wide-area network (WAN) environments. Topics summarized here include point-to-point links, circuit switching, packet switching, virtual circuits, dialup services, and WAN devices.

1.2 What is a WAN?

A WAN is a data communications network that covers a relatively broad geographic area and that often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer. Figure 1.2 illustrates the relationship between the common WAN technologies and the OSI model.

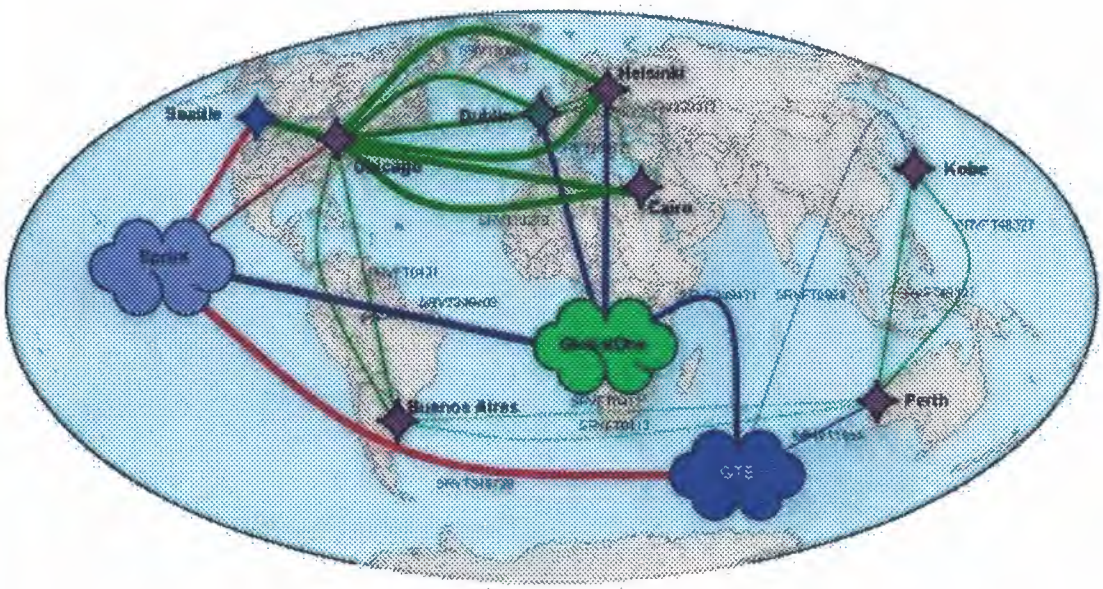

Figure 1.1: Shows Global Wide Area Network

1.3 Point-to-Point Links

A point-to-point link provides a single, pre-established WAN communications path from the customer premises through a carrier network, such as a telephone company, to a remote network. Point-to-point lines are usually leased from a carrier and thus are often called leased lines. For a point-to-point line, the carrier allocates pairs of wire and facility hardware to your line only. These circuits are generally priced based on bandwith required and distance between the two connected points. Point-to-point links

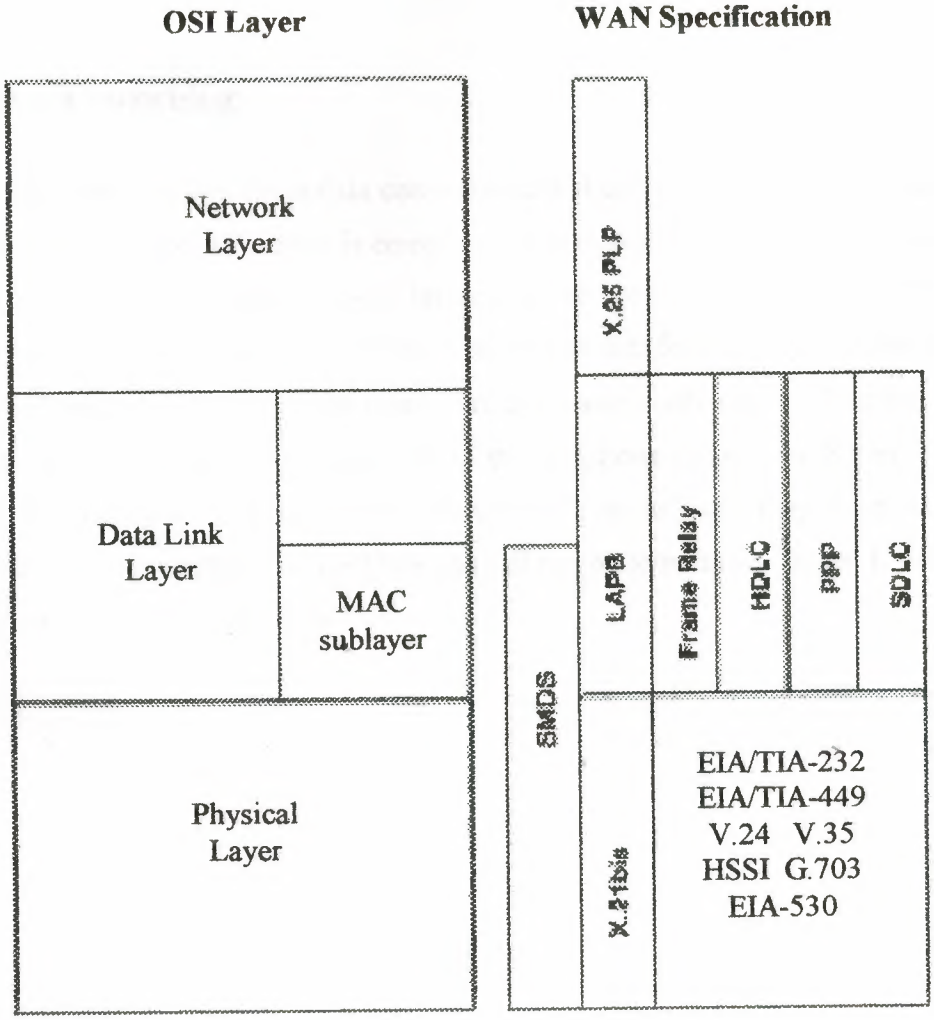

Figure 1.2: WAN Technologies Operate at the Lowest Levels of the OSI Model

are generally more expensive than shared services such as Frame Relay. Figure 1.3 illustrates a typical point-to-point link through a WAN.

Figure 1.3: A Typical Point-to-Point Link Operates Through a WAN to a Remote Network

1.4 Circuit Switching

Switched circuits allow data connections that can be initiated when needed and terminated when communication is complete. This works much like a normal telephone line works for voice communication. Integrated Services Digital Network (ISDN) is a good example of circuit switching. When a router has data for a remote site, the switched circuit is initiated with the circuit number of the remote network. In the case of ISDN circuits, the device actually places a call to the telephone number of the remote ISDN circuit. When the two networks are connected and authenticated, they can transfer data. When the data transmission is complete, the call can be terminated. Figure 1.4 illustrates an example of this type of circuit.

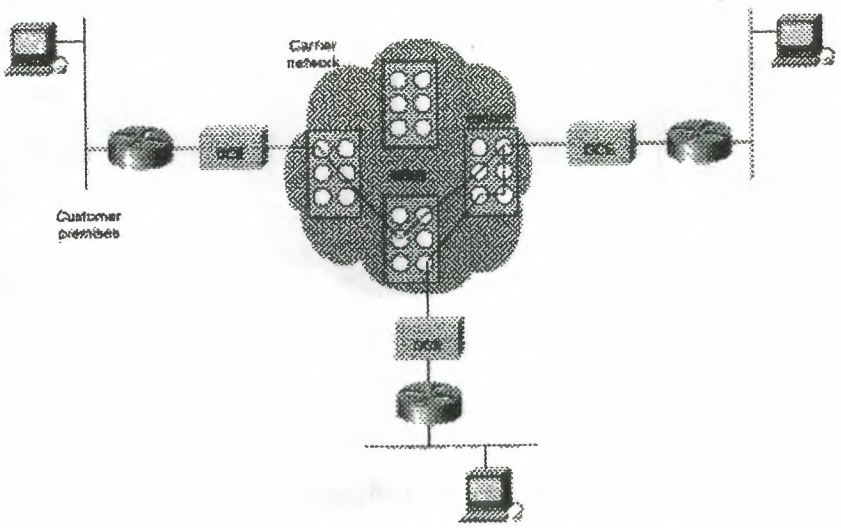

Figure 1.4: A Circuit-Switched WAN Undergoes a Process Similar to That Used for a Telephone Call

1.5 Packet Switching

Packet switching is a WAN technology in which users share common carrier resources. Because this allows the carrier to make more efficient use of its infrastructure, the cost to the customer is generally much better than with point-to-point lines. In a packet switching setup, networks have connections into the carrier's network, and many customers share the carrier's network. The carrier can then create virtual circuits between customers' sites by which packets of data are delivered from one to the other through the network. The section of the carrier's network that is shared is often referred to as a cloud.

Some examples of packet-switching networks include Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multi-megabit Data Services (SMDS), and X.25. Figure 1.5 shows an example packet-switched circuit. The virtual connections between customer sites are often referred to as a virtual circuit.

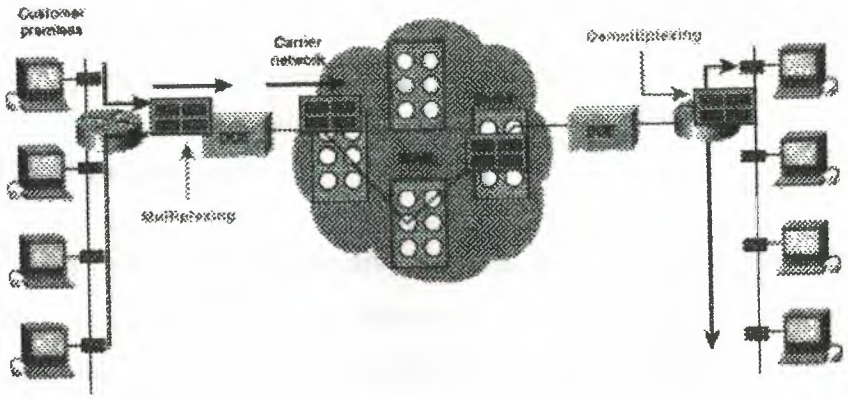

Figure 1.5: Packet Switching Transfers Packets Across a Carrier Network

1.6 WAN Virtual Circuits

A virtual circuit is a logical circuit created within a shared network between two network devices. Two types of virtual circuits exist: switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).

S VCs are virtual circuits that are dynamically established on demand and terminated when transmission is complete. Communication over an SVC consists of three phases: circuit establishment, data transfer, and circuit termination. The establishment phase involves creating the virtual circuit between the source and destination devices. Data transfer involves transmitting data between the devices over the virtual circuit, and the circuit termination phase involves tearing down the virtual circuit between the source and destination devices. SVCs are used in situations in which data transmission between devices is sporadic, largely because SVCs increase bandwidth used due to the circuit establishment and termination phases, but they decrease the cost associated with constant virtual circuit availability.

PVC is a permanently established virtual circuit that consists of one mode: data transfer. PVCs are used in situations in which data transfer between devices is constant. PVCs decrease the bandwidth use associated with the establishment and termination of

virtual circuits, but they increase costs due to constant virtual circuit availability. The service provider generally configures PVCs when an order is placed for service.

1.7 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. DDR is a technique whereby a router can dynamically initiate a call on a switched circuit when it needs to send data. In a DDR setup, the router is configured to initiate the call when certain criteria are met, such as a particular type of network traffic needing to be transmitted. When the connection is made, traffic passes over the line. The router configuration specifies an idle timer that tells the router to drop the connection when the circuit has remained idle for a certain period.

Dial backup is another way of configuring DDR. However, in dial backup, the switched circuit is used to provide backup service for another type of circuit, such as point-to-point or packet switching. The router is configured so that when a failure is detected on the primary circuit, the dial backup line is initiated. The dial backup line then supports the WAN connection until the primary circuit is restored. When this occurs, the dial backup connection is terminated.

1.8 WAN Devices

WANs use numerous types of devices that are specific to WAN environments. WAN switches, access servers, modems, CSU/DSUs, and ISDN terminal adapters are discussed in the following sections. Other devices found in WAN environments that are used in WAN implementations include routers, ATM switches, and multiplexers.

1.8.1 WAN Switch

A WAN switch is a multiport internetworking device used in carrier networks. These devices typically switch such traffic as Frame Relay, X.25, and SMDS, and operate at the data link layer of the OSI reference model. Figure 1.6 illustrates two routers at remote ends of a WAN that are connected by WAN switches.

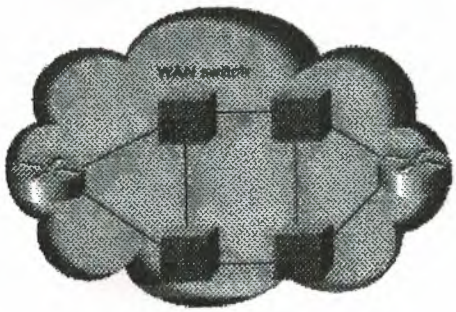

Figure 1.6: WAN Switches can connect Two Routers at Remote Ends of a WAN

1.8.2 Access Server

An access server acts as a concentration point for dial-in and dial-out connections. Figure 1.7 illustrates an access server concentrating dial-out connections into a WAN.

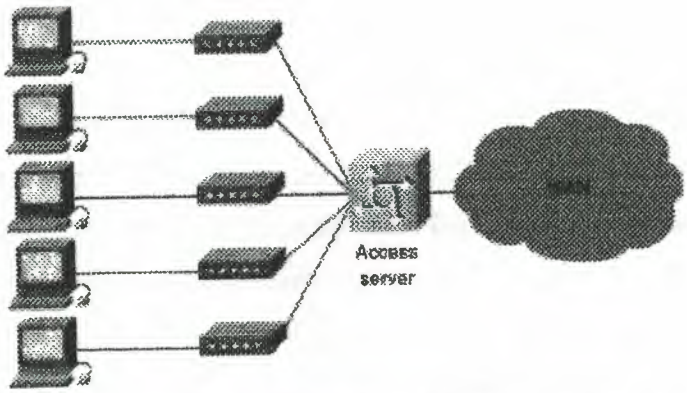

Figure 1.7: Access Server Concentrates Dial-Out Connections into a WAN

1.8.3 Modem

A modem is a device that interprets digital and analog signals, enabling data to be transmitted over voice-grade telephone lines. At the source, digital signals are converted to a form suitable for transmission over analog communication facilities. At the destination, these analog signals are returned to their digital form. Figure 1.8 illustrates a simple modem-to-modem connection through a WAN.

Figure 1.8: A Modem Connection Through a WAN Handles Analog and Digital Signals

1.8.4 CSU/DSU

A channel service unit/digital service unit (CSU/DSU) is a digital-interface device used to connect a router to a digital circuit like a T1. The CSU/DSU also provides signal timing for communication between these devices. Figure 1.9 illustrates the placement of the CSU/DSU in a WAN implementation.

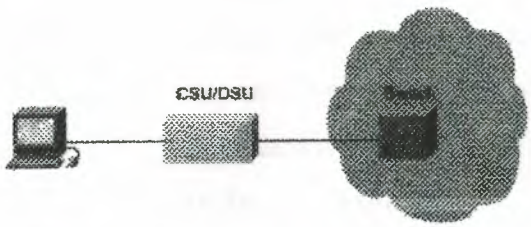

Figure 1.9: The CSU/DSU Stands Between the Switch and the Terminal

1.8.5 ISDN Terminal Adapter

An ISDN terminal adapter is a device used to connect ISDN Basic Rate Interface (BRI) connections to other interfaces, such as EIA/TIA-232 on a router. A terminal adapter is essentially an ISDN modem, although it is called a terminal adapter because it does not actually convert analog to digital signals. Figure 1.10 illustrates the placement of the terminal adapter in an ISDN environment.

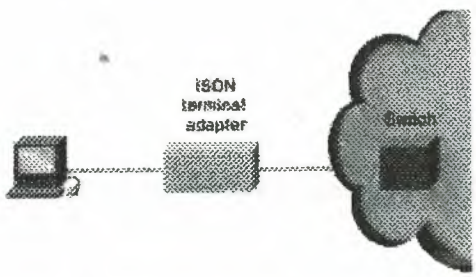

Figure 1.10: Terminal Adapter Connects the ISDN Terminal Adapter to Other Interfaces

2. IMPLEMENTING A WIDE AREA NETWORK

2.1 Overview

A lower total cost of ownership is one of the most compelling reasons for migrating to a converged data, voice, and video network. While a converged network can lower overall costs of the enterprise communications infrastructure, solid planning and design is still required for a successful deployment. Now here is this fact more evident than when running VoIP over a Wide Area Network (WAN).

As stated in Overview three basic tools must be used on every portion of the IP network to provide an environment that can ensure voice quality over the network:

- Classification
- Queuing
- Network provisioning

When the low bandwidths and slow link speeds of a WAN are introduced, you must also use several additional tools:

- Link Fragmentation and Interleaving (LFI)
- Traffic shaping
- Call admission control

All of these tools, plus several others, are described in the following sections.

2.2 Classification

Classification is the method by which certain traffic types are classified, or marked, as having unique handling requirements. These requirements might be a minimum required amount of bandwidth or a low tolerance for latency. This classification can be signaled to the network elements via a tag included in the IP Precedence or Differentiated Services Code Point (DSCP), in Layer 2 schemes such as 802.1p, in the source and destination IP addresses, or in the implicit characteristics of the data itself, such as the traffic type using the Real-time Transport Protocol (RTP) and a defined port range.

In a recommended model, classification is done at both Layer 2 and Layer 3 on the IP phone. In this model, the phone is the "edge" of the managed network, and it sets the Layer 2 802.1p CoS value to 5 and the Layer 3 IP Precedence value to 5 or the DSCP value to EF.

2.3 Queuing

As was discussed in previous chapters, interface queuing is one of the most important mechanisms for ensuring voice quality within a data network. This is even more vital in the WAN because many traffic flows are contending for a very limited amount of network resources. Once traffic has been classified, the flow can be placed into an interface egress queue that meets its handling requirements. Voice over IP, because of its extremely low tolerance for packet loss and delay, should be placed into a Priority Queue (PQ). However, other traffic types may have specific bandwidth and delay characteristics as well. These requirements are addressed with the Low-Latency Queuing (LLQ) feature in IOS.

LLQ combines the use of a PQ with a class-based weighted fair queuing scheme. Classes are defined with classification admission schemes. Traffic flows have access to either the PQ, one of the class-based queues, or a default weighted fair queue. LLQ, the recommended queuing scheme for all low-speed links, allows up to 64 traffic classes with

the ability to specify such parameters as priority queuing behavior for voice, a minimum bandwidth for Systems Network Architecture (SNA) data, and control protocols and weighted fair queuing for other traffic types.

As depicted in Figure 2.1, when a Priority Queuing class is configured, the PQ has direct access to the transmit (TX) ring. This is, of course, unless interleaving is configured, in which case interleaving occurs prior to placing the PQ traffic onto the TX-ring. The maximum configured bandwidth in the PQs and class-based queues cannot exceed the minimum available amount of bandwidth on the WAN connection.

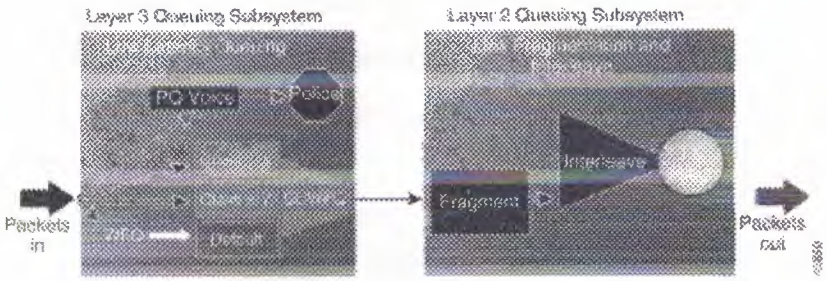

Figure 2.1: Packet Flow with Priority Queuing

A practical example is a Frame Relay LLQ with a Committed Information Rate (CIR) of 128 kbps. If the PQ for VoIP is configured for 64 kbps and both the SNA and AVVID control protocol class-based queues are configured for 20 kbps and 10 kbps, respectively, the total configured queue bandwidth is 94 kbps. IOS defaults to a minimum CIR (mincir) value of CIR/2. The mincir value is the transmit value a Frame Relay router will "rate down" to when Backward Explicit Congestion Notifications (BECNs) are received. In this example, the mincir value is 64 kbps and is lower than the configured bandwidth of the combined queues. For LLQ to work in this example, a mincir value of 128 kbps should be configured.

2.3.1 Link Fragmentation and Interleaving

For low-speed WAN connections (in practice, those with a clocking speed of 768 kbps or below), it is necessary to provide a mechanism for Link Fragmentation and Interleaving (LFI). A data frame can be sent to the physical wire only at the serialization rate of the interface. This serialization rate is the size of the frame divided by the clocking speed of the interface. For example, a 1500-byte frame takes 214 ms to serialize on a 56-kbps circuit. If a delay-sensitive voice packet is behind a large data packet in the egress interface queue, the end-to-end delay budget of 150-200 ms could be exceeded. In addition, even relatively small frames can adversely affect overall voice quality by simply increasing the jitter to a value greater than the size of the adaptive jitter buffer at the receiver. Table 2.1 shows the serialization delay for various frame sizes and link speeds.

Table 2.1: Serialization Delay

Link Speed	**Frame Size (Bytes)**					
	64	**128**	**256**	**512**	**1024**	**1500**
56 kbps	9 ms	18 ms	36 ms	72 ms	144 ms	214 ms
64 kbps	8 ms	16 ms	32 ms	64 ms	128 ms	187 ms
128 kbps	4 ms	8 ms	16 ms	32 ms	64 ms	93 ms
256 kbps	2 ms	4 ms	8 ms	16 ms	32 ms	46 ms
512 kbps	1 ms	2 ms	4 ms	8 ms	16 ms	23 ms
768 kbps	0.640 ms	1.28 ms	2.56 ms	5.12 ms	10.4 ms	15 ms

EFI tools are used to fragment large data frames into regularly sized pieces and to interleave voice frames into the flow so that the end-to-end delay can be predicted accurately. This places bounds on jitter by preventing voice traffic from being delayed behind large data frames, as illustrated in Figure2.2.

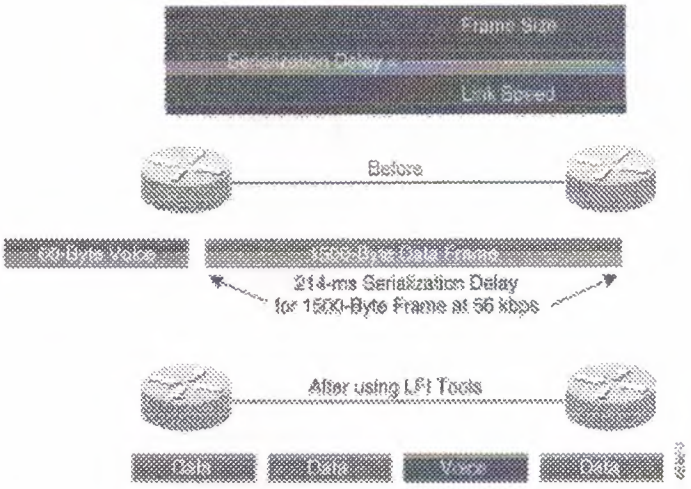

Figure 2.2: Using LFI Tools to Reduce Frame Delay

The two techniques used for this are FRF.12 for Frame Relay and Multi-link Point-to-Point Protocol (MLP) for point-to-point serial links. A 10-ms blocking delay is the recommended target to use for setting fragmentation size. To calculate the recommended fragment size, divide the recommended 10 ms of delay by one byte of traffic at the provisioned line clocking speed, as follows:

Fragment_Size = (Max_Allowed_Jitter * Link_Speed_in_kbps) / 8

For example:

Fragment_Size = (10 ms * 56) / 8 = 70 bytes

Table 2.2: Shows the recommended fragment size for various link speeds.

Link Speed	Recommended Fragment Size
56 kbps	70 bytes
64 kbps	80 bytes
128 kbps	160 bytes
256 kbps	320 bytes
512 kbps	640 bytes
768 kbps	960 bytes

2.3.2 Traffic Shaping

In ATM and Frame-Relay networks, where the physical access speed varies between two endpoints, traffic shaping is used to prevent excessive delay from congested network interface buffers caused by these speed mismatches. Traffic shaping is a tool that meters the transmit rate of frames from a source router to a destination router. This metering is typically done at a value that is lower than the line or circuit rate of the transmitting interface. The metering is done at this rate to account for the circuit speed mismatches that are common in current multiple-access, non-broadcast networks.

Traffic leaving a high-speed interface such as a T1 line at a central site often terminates at a remote site that may have a much slower link speed (for example, 56 kbps). This is quite common and, in fact, has been one of the big selling points for Frame Relay. In Figure 2.3, the T1 interface on the router at the central site sends data out at a T1 rate even if the remote site has a clock rate of 56 kbps. This causes the frames to be buffered within the carrier Frame-Relay network, increasing variable delay, as illustrated in Figure 2.3. This same scenario can be applied in reverse. For example, the

many remote sites, each with small WAN connections, when added together can oversubscribe the provisioned bandwidth or circuit speed at the central site.

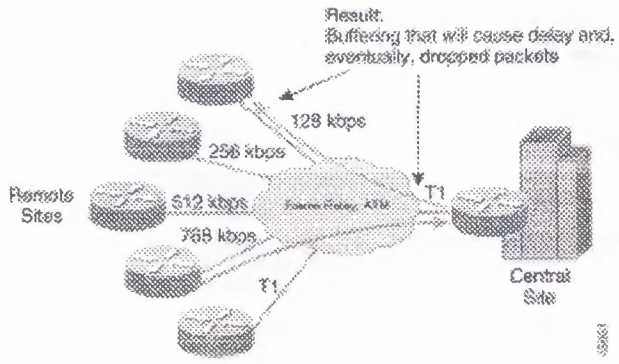

Figure 2.3: Variable Delay Caused by Buffering

2.4 Network Provisioning

Properly provisioning the network bandwidth is a major component of designing a successful AVVID network. You can calculate the required bandwidth by adding the bandwidth requirements for each major application (for example, voice, video, and data). This sum then represents the minimum bandwidth requirement for any given link, and it should not exceed approximately 75% of the total available bandwidth for the link. This 75% rule assumes that some bandwidth is required for overhead traffic, such as routing and Layer 2 keep alive, as well as for additional applications such as e-mail and Hypertext Transfer Protocol (HTTP) traffic. Figure 2.4 illustrates this bandwidth provisioning process.

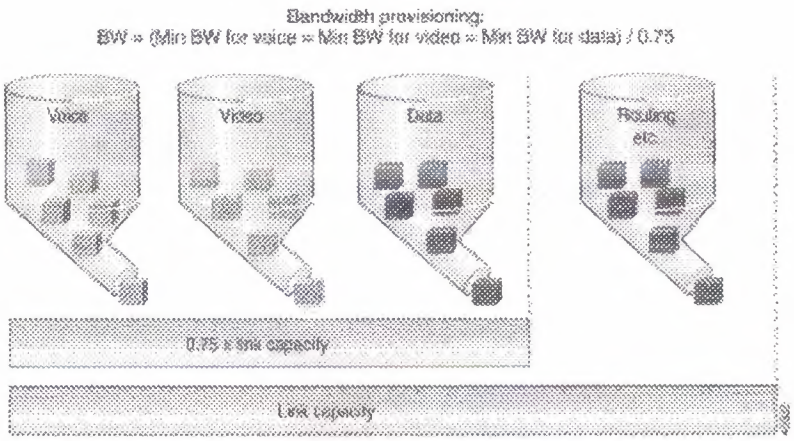

Figure 2.4: Provisioning Link Bandwidth

As illustrated in Figure 2.5, a VoIP packet consists of the payload, IP header, User Datagram Protocol (UDP) header, Real-time Transport Protocol (RTP) header, and Layer 2 Link header. At the default packetization rate of 20 ms, VoIP packets have a 160-byte payload for G.711 or a 20-byte payload for G.729. The IP header is 40 bytes, the UDP header is 8 bytes, and the RTP header is 12 bytes. The link header varies in size according to media.

Figure 2.5: Typical VoIP Packet

The bandwidth consumed by VoIP streams is calculated by adding the packet payload and all headers (in bits), then multiplying by the packet rate per second (default of 50 packets per second). Table 2.3 details the bandwidth per VoIP flow at a default packet rate of 50 packets per second (pps). This does not include Layer 2 header overhead and does not take into account any possible compression schemes, such as compressed Real-time Transport Protocol (cRTP). You can use the Service Parameters menu in CallManager Administration to adjust the packet rate.

Table 2.3: Bandwidth Consumption for Voice Payload Only.

CODEC	Sampling Rate	Voice Payload in Bytes	Packets per Second	Bandwidth per Conversation
G.711	20 ms	160	50	80 kbps
G.711	30 ms	240	33	53 kbps
G.729A	20 ms	20	50	24 kbps
G.729A	30 ms	30	33	16 kbps

A more accurate method for provisioning is to include the Layer 2 headers in the bandwidth calculations, as shown in Table 2.4.

Table 2.4: Bandwidth Consumption with Headers Included

CODEC	Ethernet 14 Bytes of Header	PPP 6 Bytes of Header	ATM 53-Byte Cells with a 48-Byte Payload	Frame-Relay 4 Bytes of Header
G.711 at 50 pps	85.6 kbps	82.4 kbps	106 kbps	81.6 kbps
G.711 at 33 pps	56.5 kbps	54.4 kbps	70 kbps	54 kbps
G.729A at 50 pps	29.6 kbps	26.4 kbps	42.4 kbps	25.6 kbps
G.729A at 33 pps	19.5 kbps	17.4 kbps	28 kbps	17 kbps

2.4.1 Call Admission Control

Call admission control is a mechanism for ensuring that voice flows do not exceed the maximum provisioned bandwidth allocated for voice conversations. After doing the calculations to provision the network with the required bandwidth to support voice, data, and possibly video applications, it is important to ensure that voice does not oversubscribe the portion of the bandwidth allocated to it. While most QoS mechanisms are used to protect voice from data, call admission control is used to protect voice from voice. This is illustrated in Figure 2.6, which shows an environment where the network has been provisioned to support two concurrent voice calls. If a third voice call is allowed to proceed, the quality of all three calls is degraded. To prevent this degradation in voice quality, you can provision call admission control in CallManager to block the third call. For more information on call admission control, see the IP Telephony

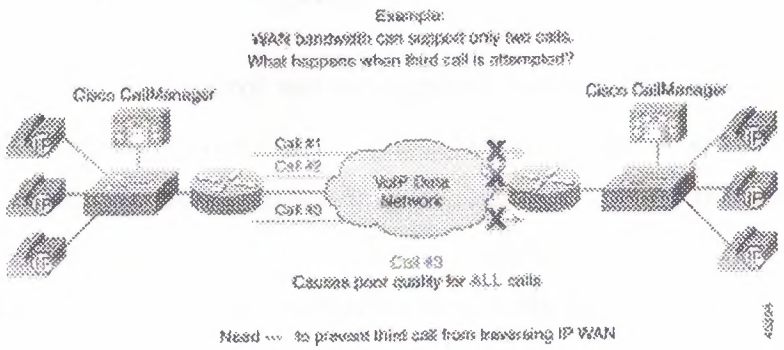

Figure 2.6: Call Admission Control

2.4.2 Miscellaneous WAN Tools

This section describes the following additional tools, which can help ensure voice quality in WAN applications:

- VoIP Control Traffic
- TX-ring sizing
- Compressed voice codecs
- Compressed RTP (cRTP)
- Voice Activity Detection (VAD)

2.4.2.1 VoIP Control Traffic

When allocating bandwidth for the IP WAN, do not overlook the CallManager control traffic. In centralized call processing designs, the IP phones use a Transmission Control Protocol (TCP) control connection to communicate with CallManager. If there is not enough bandwidth provisioned for these small control connections, callers might be adversely affected.

An example where this comes into play is with the Delay-to-Dial-Tone (DTT) time. The IP phones communicate with CallManager via Skinny Station Protocol over TCP port 2001. When an IP phone goes off-hook, it "asks" CallManager what to do. CallManager instructs the IP phone to play dial tone. If this Skinny Protocol management and control traffic is dropped or delayed within the network, the user will not receive dial tone. This same logic applies to all signaling traffic for gateways and phones.

To ensure that this control and management traffic is marked as important (but not as important as voice), Access Control Lists (ACLs) are used to classify these streams on Layer 3 or 4 Catalyst 6000 switches at the central locations. In the remote offices, a router might be the first Layer 3 or 4 devices a packet encounters before hitting the WAN. To ensure that these control connections are classified as important (but not as important as voice) access lists are used in the branch router.

2.4.2.2 TX-Ring Sizing

The TX-ring is the unprioritized FIFO buffer used to hold frames prior to transmission to drive link utilization to 100%. In the 7500 Route/Switch Processor (RSP), this is referred to as the TX-queue and can be modified using the **tx-queue-limit** command. The RSP is a very inefficient QoS platform, especially with regard to modifying the TX-queue parameters. The 7500 RSP TX-queue, which refers to the FIFO queue in MEM-D, has to copy the packet from MEM-D to the system buffers in DRAM and then back from the system buffers to MEM-D. The TX-ring is much more efficient

than the TX-queue and is used instead of it on the 7500 VIP, 7200, 3600, 2600, and 1750 routers.

While fragmentation and interleaving reduces jitter, a large TX-ring value can increase jitter when link utilization approaches saturation. Because of this, TX-ring sizing is related to fragmentation size, as shown in Table 2.5.

Table 5-5: TX-Ring Buffer Sizing Link Speed

(CIR) on Permanent Virtual Circuit	**TX-Ring Buffer Sizing (Packets)**
=< 128 kbps	5
192 kbps	6
256 kbps	7
512 kbps	14
768 kbps	21

On all Point-to-Point Protocol (PPP) and Multi-link PPP (MLP) links, TX-ring buffer size is automatically configured, and you cannot change these default buffer values. On Frame Relay links, the TX-ring is for the main interface, which all sub interfaces also use. The default TX-ring buffer size is 64 packets. You might need to change this setting when the sub interface is very small or there are many sub interfaces.

Table 2.6 summarizes TX-ring buffer sizing for various media.

Media	Default TX-Ring Buffer Sizing (Packets)
PPP	6
MLP	2
ATM	8192 (Must be changed for low-speed virtual circuits)
Frame Relay	64 (Per main T1 interface)

2.4.2.3 Compressed Voice Codecs

To utilize as much of the limited WAN bandwidth as possible, VoIP uses codecs (coding-decoding algorithms) to digitize analog voice samples. Many codecs, such as G.729, can compress a 64-kbps call down to 8 kbps. These types of codecs, termed low-bit-rate codecs, are commonly used for voice calls across the WAN.

2.4.2.4 Compressed RTP

Compressed RTP (cRTP) compresses the 40-byte header of a VoIP packet to approximately 2 to 4 bytes. Compressed RTP works on a link-by-link basis and is enabled on routers using the ip rtp header-compression command. Table 2.7 summarizes the bandwidth calculations for cRTP.

Table 2.7: Compressed RTP Bandwidth Calculations

Codec	PPP 6 Bytes of Header	ATM 53-Byte Cells with a 48-Byte Payload	Frame Relay 4 Bytes of Header
G.711 at 50 pps	68 kbps	N/A	67 kbps
G.711 at 33 pps	44 kbps	N/A	44 kbps
G.729A at 50 pps	12 kbps	N/A	11.2 kbps
G.729A at 33 pps	8 kbps	N/A	7.4 kbps

2.4.2.5 Voice Activity Detection

Voice Activity Detection (VAD) takes advantage of the fact that, in most conversations, only one party is talking at a time. The VAD algorithm in the VoIP software examines the voice conversation, looking for these gaps in conversation. When a gap is discovered, no packets are sent, and the WAN bandwidth can be recovered for use by data applications. It is recommended you always turn VAD off system wide.

2.5 Point-to-Point WAN

Point-to-point WANs, while not as popular as in the past, are still one of the most common types of networks in use today. Figure 2.7 shows the general model for point-to-point WANs described in this guide. When designing a point-to-point WAN for an AVVID network, keep the following recommendations in mind:

- IOS Release 12.1(3) T is the minimum recommended release for a point-to-point WAN.
- Use Link Fragmentation and Interleaving (LFI) techniques on all WAN connections with speeds below 768 kbps.
- Use Low-Latency Queuing (LLQ) with a priority queue for VoIP bearer streams and a class queue for VoIP control sessions.
- Call admission control is required when the number of calls across the WAN can oversubscribe the allocated VoIP bandwidth.

The following sections explain the QoS issues for this type of configuration

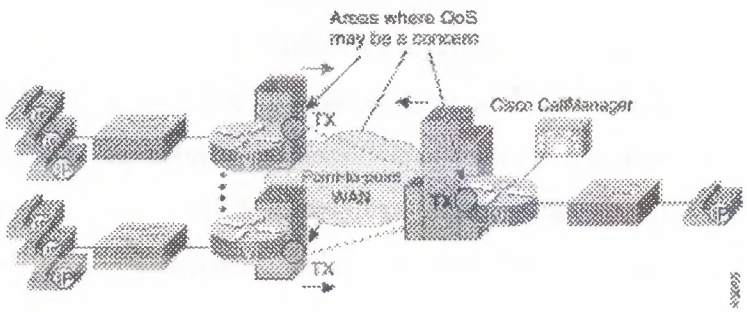

Figure 2.7: Eneral Model for a Point-to-Point WAN

2.5.1 LFI on Point-to-Point WANs

If the clocking speed of the connection is below 768 kbps, LFI must be used. Multi-link PPP (MLP) instead of PPP is required on all point-to-point links where LFI is needed. To enable LFI on point-to-point WANs, use the IOS command set for MLP.

2.5.2 cRTP on MLP Connections

Compressed RTP (cRTP) can have a dramatic impact on the amount of bandwidth each voice call uses. Prior to IOS Release 12.0(7) T, cRTP was process switched. In fact, fast switching for cRTP was not available on the Catalyst 2600 and 3600 until a bug fix was implemented in IOS Release 12.0(7) T. In addition, some of the newer versions of IOS (specifically, Release 12.1(2.x) T) still use process switching for cRTP. Always read the release notes before attempting to use any specific feature.

2.5.3 LLQ for VoIP over MLP

Low-Latency Queuing (LLQ) is required to support voice over the WAN. When configuring LLQ for MLP-enabled interfaces, put the **service-policy output** in the multi-link interface configuration. In the following example, two classes are defined: one for the VoIP media stream and one for the control traffic. Access to these classes, and therefore the queues they service, is done through access lists that match either Layer 3 ToS classification or source and destination IP addresses and ports. The access lists look slightly different for the control traffic at the central site because a Catalyst 6000 has already classified VoIP Control sessions with a DSCP value of 26 (AF31, which is backward compatible with IP Precedence 3).

All VoIP media traffic is placed into the Priority Queue (PQ), which is given 100 kbps of bandwidth. All Skinny Protocol control traffic is placed into a class-based queue and is given 10 kbps of bandwidth. All other traffic is queued using Weighted Fair Queuing.

2.6 Frame-Relay WAN

Frame-Relay networks are the most popular WANs in use today because of the low cost associated with them. However, because Frame Relay is a non-broadcast technology that uses over subscription to achieve costs savings, it is not always an easy platform on which to implement AVVID solutions. While this section outlines the basic requirements for successfully deploying AVVID solutions across a Frame-Relay WAN, extensive

explanations of Frame Relay committed information rate (CIR), committed burst rate (Bc), excess burst rate (Be), and interval configurations are not covered here.

Figure 2.8 shows the general model for Frame-Relay WANs described in this guide.

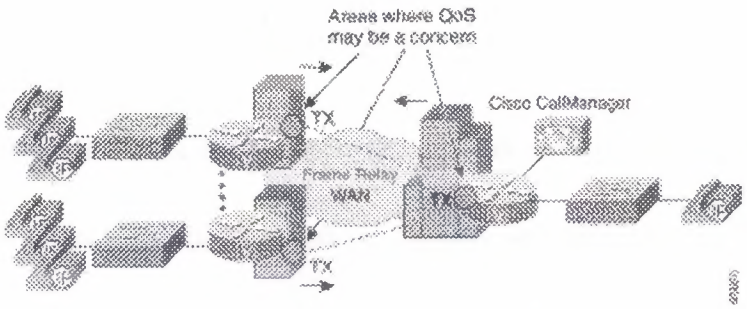

Figure 2.8: General Model for a Frame-Relay WAN

When designing a Frame-Relay WAN for an AVVID network, keep the following recommendations in mind:

- IOS Release 12.1(2) T is the minimum recommended release for a Frame-Relay WAN.
- You must use traffic shaping with Frame-Relay WANs.
- Use Link Fragmentation and Interleaving (LFI) techniques on all virtual circuits with speeds below 768 kbps.
- Use Low-Latency Queuing (LLQ) with a Priority Queue (PQ) for VoIP bearer streams and a class-based queue for VoIP control sessions.
- Call admission control is required when the number of calls across the WAN can oversubscribe the allocated VoIP bandwidth.

The following sections explain the QoS issues for this type of configuration.

2.6.1 Traffic Shaping

Traffic shaping is required for Frame-Relay networks for three reasons:

- Over subscription of sites is part of the nature of Frame-Relay networks.
- It is common for configurations to allow bursts that exceed the Committed Information Rate (CIR).
- The default interval for Frame-Relay devices can add unnecessary delay.

The following sections describe some of the aspects of traffic shaping for Frame-Relay networks.

2.6.1.1 Committed Information Rate

In most Frame-Relay networks, a central site uses a T1 link or something faster to terminate WAN connections from many remote offices. The central site sends data out at 1.536 Mbps, while a remote site may have only a 56-kbps circuit. In addition, there is typically a many-to-one ratio of remote offices to central hubs. It is quite possible for all the remote sites to send traffic at a rate that can overwhelm the T1 at the hub. Both of these scenarios can cause frame buffering in the provider network that induces delay, jitter, and drops. The only solution is to use traffic shaping at both the central and remote routers.

2.6.1.2 Committed Burst Rate

Another problem with Frame-Relay networks is the amount of data a node can transmit at any given time. A 56-kbps Permanent Virtual Circuit (PVC) can transmit a maximum of 56 kbits of traffic in 1 second. How this second is divided is called the interval. The amount of traffic a node can transmit during this interval is called the committed burst (Bc) rate. By default, all routers set Bc to CIR/8. The formula for calculating the interval is

Interval = Bc/CIR

For example, with a CIR of 56 kbps:

Interval = 7000 / 56,000 = 125 ms

In the preceding example, after a router sends its allocated 7000 bits, it must wait 125 ms before sending its next traffic. While this is a good default value for data, it is a very bad choice for voice. By setting the Bc value to a much lower number, you can decrease the interval, which means the router will send traffic more frequently. An optimal configured value for Bc is 1000.

2.6.1.3 Excess Burst Rate

If the router does not have enough traffic to send all of its Bc (1000 bits, for example), it can "credit" its account and send more traffic during a later interval. The excess burst (Be) rate defines the maximum amount that can be credited to the router's traffic account. The problem with Be in AVVID networks is that this can create a potential for buffering delays within a Frame-Relay network because the receiving side can "pull" the traffic from a circuit only at the rate of Bc, not Bc + Be.

2.6.2 FRF.12 for LFI on Frame-Relay WANs

To enable Link Fragmentation and Interleaving (LFI) on Frame-Relay WANs, you must also use traffic shaping. Unlike MLP, the actual fragment size must be configured when using LFI on Frame Relay. In Frame-Relay networks, the fragmentation size is based on the Permanent Virtual Circuit (PVC), not the actual serialization rate (clocking speed) of the interface. This method is used because the Frame-Relay traffic shaping policy allows only the specified bit rate in the Committed Information Rate (CIR) to enter the interface transmit buffer. In other words, the rate of the PVC CIR is the clocking rate to reference when estimating fragmentation requirements in a frame-relay environment.

2.6.3 LLQ for VoIP over Frame Relay

Low-Latency Queuing (LLQ) is required to support voice over the WAN. When configuring LLQ for Frame-Relay interfaces, put the service-policy output in the map-class frame-relay configuration section. In the following example, two classes are defined: one for the VoIP media stream and one for the control traffic. Access to these classes, and therefore the queues they service, is done through access lists that match either Layer 3 ToS classification or source and destination IP addresses and ports. The access lists look slightly different for the control traffic at the central site because a Catalyst 6000 has already classified VoIP Control sessions with a DSCP value of 26 (AF31, which is backward compatible with IP Precedence 3).

All VoIP media traffic is placed into the Priority Queue (PQ), which is given 100 kbps of bandwidth. All Skinny Protocol control traffic is placed into a class-based queue and given 10 kbps of bandwidth. All other traffic is queued using Weighted Fair Queuing.

2.7 ATM WAN

Asynchronous Transfer Mode (ATM) is becoming a more common medium for WANs because many service providers have adopted this technology. Figure 2.9 shows the general model for ATM WANs described in this guide.

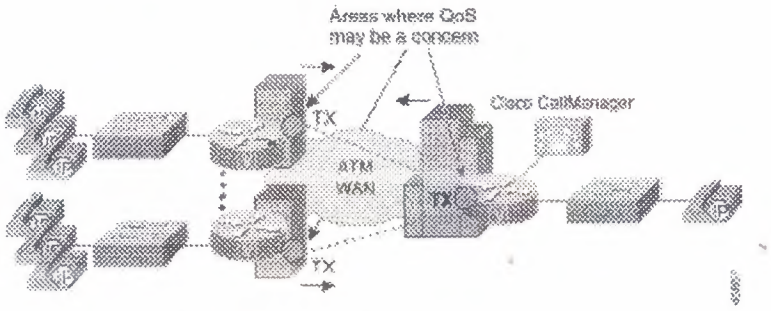

Figure 2-9: General Model for an ATM WAN

One of the difficulties with using ATM in WANs is that it was designed for high speeds, not low speeds. Many enterprises are attempting to deploy AVVID solutions over low-speed ATM connections. This generally results in complications because many of

the IOS QoS tools are not currently supported on ATM interfaces, and many of the interface defaults are automatically configured for high-speed ATM circuits.

This is evident in the default sizing of ATM TX-ring buffers. For example, by default, the 7200 router OC-3 interface (the PA-A3) sets the TX-ring buffer to 8192 bytes. This is a correct setting for an OC-3, but, for a 256-kbps Permanent Virtual Circuit (PVC) configured on the interface, very large TX-ring buffer delays can occur. Because of this, the TX-ring has to be configured to a much lower value on a sub-interface level. An ATM WAN for an AVVID network, keep the following recommendations in mind:

- IOS Release 12.1(5) T for MLP over ATM is the minimum recommended release for an ATM WAN.
- For all ATM connections below DS-3 speeds, you must adjust the TX-ring buffer size.
- It is preferable to use two Permanent Virtual Circuits (PVCs) if the PVC speed is less than 768 kbps.
- If using single PVC that is less than 768 kbps, use MLP over ATM for LFI.
- If using single PVC, use LLQ with a Priority Queue (PQ) for VoIP bearer streams and a class-based queue for VoIP control sessions.
- Call admission control is required when the number of calls across the WAN can oversubscribe the allocated VoIP bandwidth.

2.7.1 Two PVCs or LFI on Low-Speed ATM WANs

The best method of designing VoIP for ATM networks when using PVCs lower than 768 kbps is to use separate PVCs for voice and data. The following example illustrates this type of configuration:

If two PVCs are not an acceptable design alternative, the other option is to use the new MLP-over-ATM tools for link fragmentation and interleaving (LFI). Because ATM

is a cell technology using a fixed payload size, there are no inherent LFI tools. A new standard, which uses MLP over ATM, is available in IOS Release 12.1(5) T. MLP over ATM provides a Layer 2 fragmentation and interleaving method for low-speed ATM links.

The ideal fragment size for MLP over ATM should allow the fragments to fit into an exact multiple of ATM cells. It is important to include MLP and ATM Adaptation Layer 5 (AAL5) overhead in all fragmentation calculations. The header for MLP over ATM is 10 bytes, and the AAL5 packet overhead is 8 bytes.

The fragment size for MLP over ATM can be calculated as follows:

Fragment_Size = (48 * Number_of_Cells) - 10 - 8

For example, if 7 cells per fragment are desirable, the fragment size should be

Fragment_Size = (48 * 7) - 10 - 8 = 318 bytes

There are some interesting features for MLP over ATM, including the use of Virtual Template instead of Multi-link interfaces. (Virtual-Template configurations will be replaced by Multi-link interfaces in later releases of MLP over ATM because Multi-link interfaces provide more scalability and greater integration into existing MLP installations.) In addition, the configuration of PPP Challenge Handshake Authentication Protocol (CHAP) is required if remote sites want to communicate using MLP over ATM.

MLP over ATM requires the MLP bundle to classify the outgoing packets before they are sent to the ATM virtual circuit (VC). It also requires FIFO queuing to be used as the per-VC queuing strategy for the ATM VC. To use the advanced Low-Latency Queuing (LLQ) recommended for all VoIP WAN installations, attach the LLQ logic to the virtual template interface.

Only certain advanced ATM hardware supports per-VC traffic shaping (for example, ATM Deluxe PA on the 7200 router and OC-3 NM on the 3600 series). Because traffic shaping is a fundamental requirement of this design, MLP over ATM can

be supported only on the platforms that support this ATM hardware. The following example illustrates this type of configuration:

2.7.2 LLQ for VoIP over ATM

Low-Latency Queuing (LLQ) is required to support voice over the ATM WAN when single PVC is used. When configuring LLQ for ATM-enabled interfaces, place the service-policy output under the sub interface PVC configuration section. In the following example, two classes are defined: one for the VoIP media stream and one for the control traffic. Access to these classes, and therefore the queues they service, is done through access lists that match either Layer 3 ToS classification or source and destination IP addresses and ports. The access lists look slightly different for the control traffic at the central site because a Catalyst 6000 has already classified VoIP Control sessions with a DSCP value of 26 (AF31, which is backward compatible with IP Precedence 3).

All VoIP media traffic is placed into the Priority Queue (PQ), which is given 100 kbps of bandwidth. All Skinny Protocol control traffic is placed into a class-based queue and given 10 kbps of bandwidth. All other traffic is queued using Weighted Fair Queuing.

2.8 Frame-Relay-to-ATM Internetworking WAN

Many enterprises are deploying AVVID networks that use Frame Relay at the remote sites and ATM at the central location. The conversion is accomplished through ATM-to-Frame-Relay Service Internetworking (FRF.8) in the carrier network.

Figure 2.10 shows the general model for a WAN using ATM at the central site and Frame Relay at the remote sites.

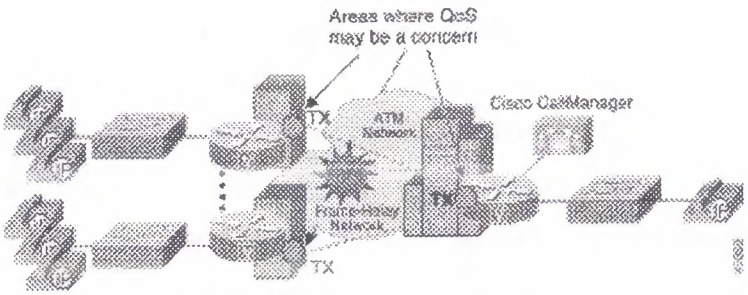

Figure 2.10: General Model of a WAN Combining ATM and Frame Relay

When designing a Frame-Relay-to-ATM Internetworking WAN for an AVVID network, keep the following recommendations in mind:

- IOS Release 12.1(5) T for MLP over ATM and MLP over Frame Relay is the minimum recommended release for this configuration.
- FRF.8 Transparent Mode is the only support method for MLP over ATM and Frame-Relay Service Internetworking.
- For all ATM connections below DS-3 speeds, you must adjust the TX-ring buffer size.
- Use two Permanent Virtual Circuits (PVCs) if the ATM and Frame-Relay PVC speed is less than 768 kbps.
- If using single PVC that is less than 768 kbps, use MLP over ATM and Frame Relay for LFI.
- If using single PVC, use LLQ with a Priority Queue (PQ) for VoIP bearer streams and a class-based queue for VoIP control sessions.
- Call admission control is required when the number of calls across the WAN can oversubscribe the allocated VoIP bandwidth.

The following sections explain the QoS issues for this type of configuration.

2.8.1 LFI on Low-Speed ATM-to-Frame-Relay Internetworking WANs

FRF.12 cannot be used because currently no service provider supports FRF.12. In fact, no WAN switching gear supports FRF.12. Tunneling FRF.12 through the service provider network does not work because there is no FRF.12 standard on the ATM side. This is a problem because fragmentation is a requirement if any of the remote Frame-Relay sites use a circuit of 768 kbps or below. The best VoIP design for ATM networks when using PVCs lower than 768 kbps is to use separate PVCs for voice and data.

If two PVCs are not an acceptable design alternative, the other option is to use the new MLP over ATM and Frame-Relay tools for Link Fragmentation and Interleaving (LFI), available in IOS Release 12.1(5) T. MLP over ATM and Frame Relay provides an end-to-end Layer 2 fragmentation and interleaving method for low-speed ATM-to-Frame-Relay FRF.8 Service Internetworking links.

FRF.8 Service Internetworking is a Frame Relay Forum (FRF) standard for connecting Frame-Relay networks with ATM networks. Service Internetworking provides a standards-based solution for service providers, enterprises, and end users. In Service Internetworking translation mode, Frame-Relay PVCs are mapped to ATM PVCs without the need for symmetric topologies because the paths can terminate on the ATM side. FRF.8 supports two modes of operation of the Internetworking Frame Relay (IWF) for upper-layer user protocol encapsulation, which differ in the following ways:

- Translation Mode — Maps between ATM and Frame-Relay encapsulation. It also supports interlocking of routed or bridged protocols.
- Transparent Mode — Does not map encapsulations but sends them unaltered. This mode is used when translation is impractical because encapsulation methods do not conform to the supported standards for Service Internetworking.

To make MLP over Frame Relay and MLP over ATM internetworking possible, the internetworking switch must be configured in Transparent Mode, and the end routers must be able to recognize headers for both MLP over Frame Relay and MLP over ATM. You can enable these options with the frame-relay interface-dlci <dlci> ppp and protocol

ppp commands for Frame Relay and ATM, respectively. When a frame is sent from the Frame-Relay side of an ATM-to-Frame-Relay Service Internetworking connection, the following actions should occur to make internetworking possible:

1. A packet is encapsulated in the MLP-over-Frame-Relay header by the sending router.

2. The carrier switch, in Transparent Mode, strips off the two-byte Frame-Relay data-link connection identifier (DLCI) field and sends the rest of the packet to its ATM interface.

3. The receiving router examines the header of the received packet. If the first two bytes of the received packet are 0x03cf, the router treats it as a legal MLP-over-ATM packet and sends it to the MLP layer for further processing.

When an ATM cell is sent from the ATM side of an ATM-to-Frame-Relay Service Internetworking connection, the following actions should occur to make internetworking possible:

1. A packet is encapsulated in the MLP-over-ATM header by the sending router.

2. The carrier switch, in Transparent Mode, pretends a two-byte Frame-Relay DLCI field to the received packet and sends the packet to its Frame-Relay interface.

3. The receiving router examines the header of the received packet. If the first four bytes after the two-byte data-link connection identifier (DLCI) field of the received packet are 0xfefe03cf, the router treats it as a legal MLP-over-Frame-Relay packet and sends it to the MLP layer for further processing.

A new ATM-to-Frame-Relay Service Internetworking standard, FRF.8.1, supports MLP over ATM and Frame Relay-Service Internetworking. However, it might be years before all switches are updated to this new standard.

The ideal fragment size for MLP over ATM should allow the fragments to fit into an exact multiple of ATM cells. It is important to include MLP and Adaptation Layer 5 (AAL5) overhead in all fragmentation calculations. The header for MLP over ATM is 10 bytes, and the AAL5 packet overhead is 8 bytes.

The fragment size for MLP over ATM can be calculated as follows:

Fragment_Size = (48 * Number_of_Cells) - 10 - 8

For example, if 7 cells per fragment are desirable, the fragment size should be

Fragment_Size = (48 * 7) - 10 - 8 = 318 bytes

There are some interesting features for MLP over ATM, including the use of Virtual Template instead of Multi-link interfaces. (Virtual-Template configurations will be replaced by Multi-link interfaces in later releases of MLP over ATM because Multi-link interfaces provide more scalability and greater integration into existing MLP installations.) In addition, the configuration of PPP Challenge Handshake Authentication Protocol (CHAP) is required if remote sites want to communicate using MLP over ATM.

MLP over ATM requires the MLP bundle to classify the outgoing packets before they are sent to the ATM virtual circuit (VC). It also requires FIFO queuing to be used as the per-VC queuing strategy for the ATM VC. To use the advanced Low-Latency Queuing (LLQ) recommended for all VoIP WAN installations, attach the LLQ logic to the virtual template interface. Only certain advanced ATM hardware supports per-VC traffic shaping (for example, ATM Deluxe PA on the 7200 router and OC-3 NM on the 3600 series). Because traffic shaping is a fundamental requirement of this design, MLP over ATM can be supported only on the platforms that support this ATM hardware. MLP over Frame Relay also has some interesting features, such as the fact that it relies on a Frame-Relay traffic shaping (FRTS) engine to control the flow of packets from the MLP bundle to the Frame-Relay virtual circuit (VC). The following sections present example configurations for ATM at the central site and Frame Relay at the remote sites.

3. WAN DEVICES

3.1 Overview

Network security is vital. Many applications (IBM 3270 telnet emulation, Telnet, ftp...) 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. One example is SKIP.

Network security could easily be enhanced if Vendors replaced relics such as ftp, telnet and rlogin with more secure alternatives such as ssh, if NIS+ and/or Kerberos clients were bundled with all major OSs and a secure email system such as pgp were fully integrated into vendors email clients. But history shows that this is unlikely to happen... Centralized network management is important for maintaining network security. The Network (meaning both LAN and WAN) is analyzed here in terms of:

- Protocols: Net bios, TCP/IP, SNA, IPX, DECnet...
- Physical network types: leased lines, ISDN, X25, FDDI, Ethernet, ATM, radio, infra red, Microwave, GSM, satellite.
- Pure Network devices: routers, bridges, encryption units and modems. Firewalls are discussed in the next chapter.

WINS (Windows Internet Naming Service) allows Net bios name to IP address resolution via a highly automated dynamic database. It reduces the need for LMHOSTS files. RAS (Remote Access Service).

3.3.2 TCP/IP

- **Weaknesses**

TCP/IP was not designed for high security:

- Protection through the use of privileged ports (0-1000) has little value since PCs have become TCP/IP clients.
- No traffic priority (easy to flood the network).
- Traffic can be injected; packets can be stolen or hijacked, so ensure routers and firewall implement anti-spoofing.
- UDP (datagram based) offers no authentication.
- TCP (connection based) offers weak authentication.
- No confidentiality (no encryption).
- IP spoofing is easy (weak authentication), machines can lie about IP addresses. Routers can be tricked. Header checksums are not sufficient.
- Checksums are easy to cheat (weak algorithm).

However, TCP/IP is reliable, robust and the de-facto standard.

- **DNS (Domain Name Service)**

- The DNS, which is used on the internal network, should not be visible to the outside world (Internet). Firewalls, which provide DNS information to the Internet, should only resolve firewall addresses/names (i.e. for email, an MX record which points to the firewall itself) and not provide any information about hosts on the internal network.
    - The internal DNS server can be set up to send unresolved queries to the external DNS server, which will then search the Internet.

- Internal clients should point to the internal DNS server(s).

- Clients with very few, designated connections do not need to use DNS.
- DNS servers should be configured as class .
- Use replica (secondary) servers to increase availability.
- Up the latest version of the Public Domain BIND for the Internet exposed DNS servers, the public versions evolves more quickly and bug are fixed more rapidly than most vendors.

- **DHCP (Dynamic Host Configuration Protocol)**

DHCP is very practical, especially for Laptops and in environments where reorganizations are constant. However, dynamic DHCP makes it difficult to uniquely identify machines, so for class networks, avoid the use of dynamic IP addressing. Static DHCP may be useful for centralizing the management of IP addresses.

- An IP address should uniquely identify a machine (to prevent host spoofing and allow use of IP address access control i.e. inetd tcp_wrappers on UNIX machines).
- If DHCP is to be used (for large laptop populations for example), class servers should have static IP address and not be configured via DHCP.
- Ethernet MAC addresses can also be used to uniquely identify a host's traffic, if the MAC addresses are recorded and a database kept up to date and relevant network monitoring software exists.

3.4 Physical network types

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

3.4.1 Ethernet

- Use hubs instead of Thin Ethernet (Star formation). 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.

3.4.2 Leased lines

Copper leased lines should be hardware or software encrypted.

- **FDDI**

Because 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.

- **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.

- **HSSI**

HSSI (High speed serial interface) is an interface technology that was developed to fill the need 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 levels. 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.

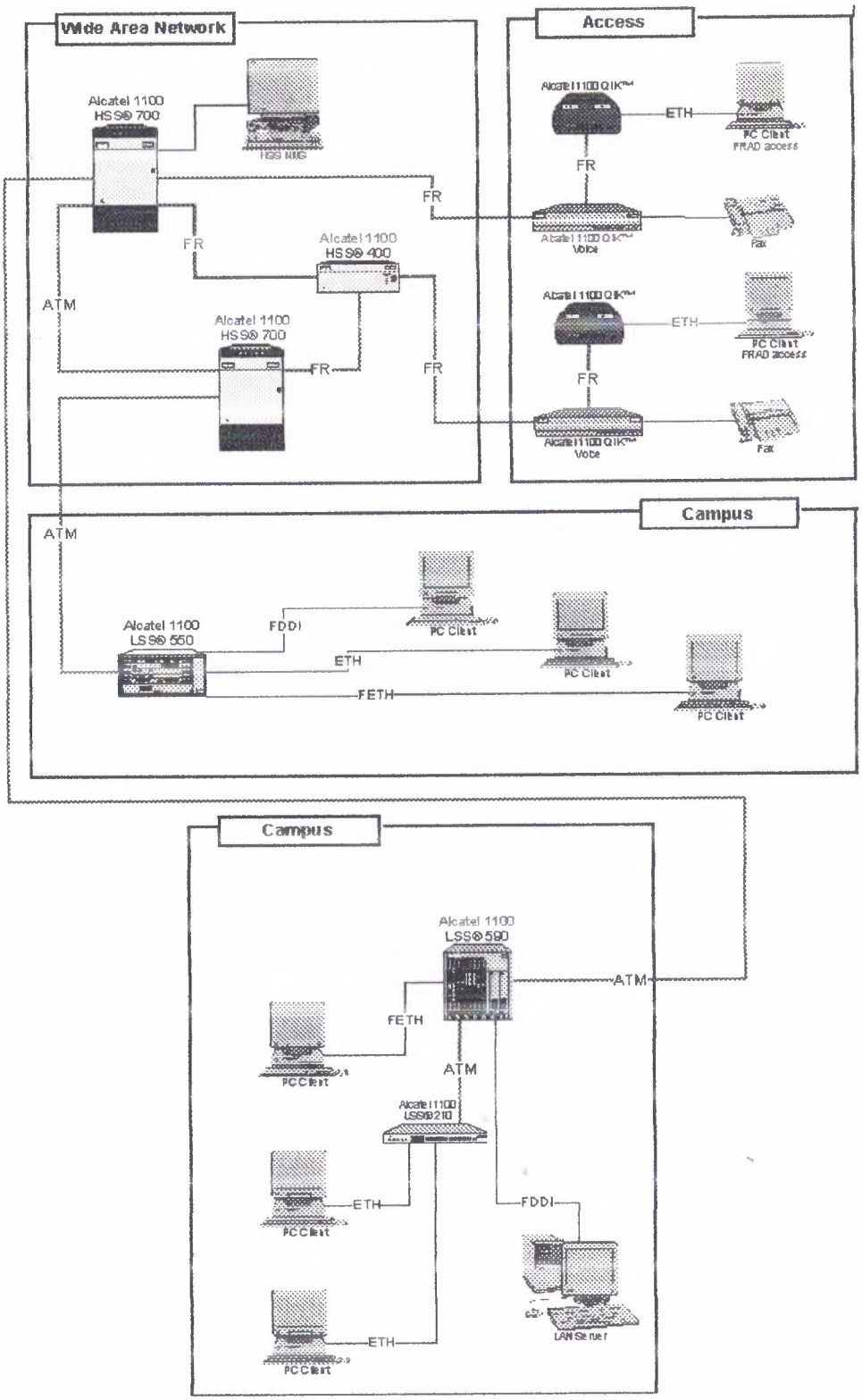

Figure 3.2: Shows a Physical Components of WAN

3.5 Network Devices

Most attacks come from the inside, so:

- No "sniffer" or "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
    - Delete the utility or
    - 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, enable logging, choose carefully who has user/enable/admin access, etc.

3.5.1 Introduction to 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.

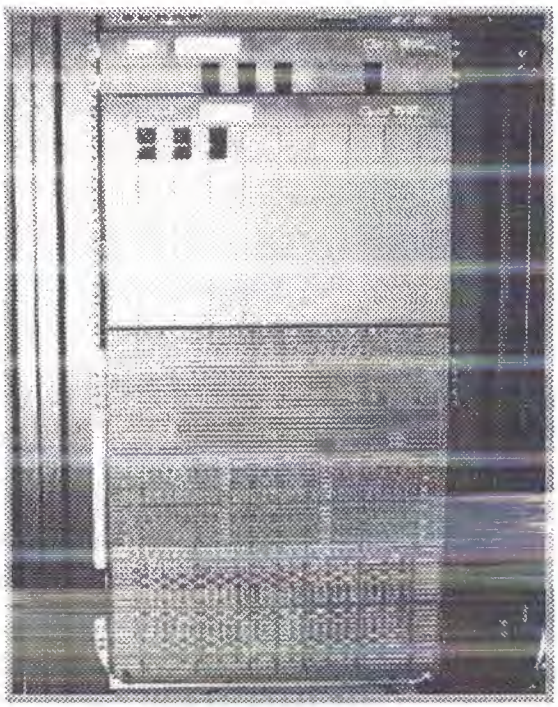

Figure 3.3: Shows a Router Diagram

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 card 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 or 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).

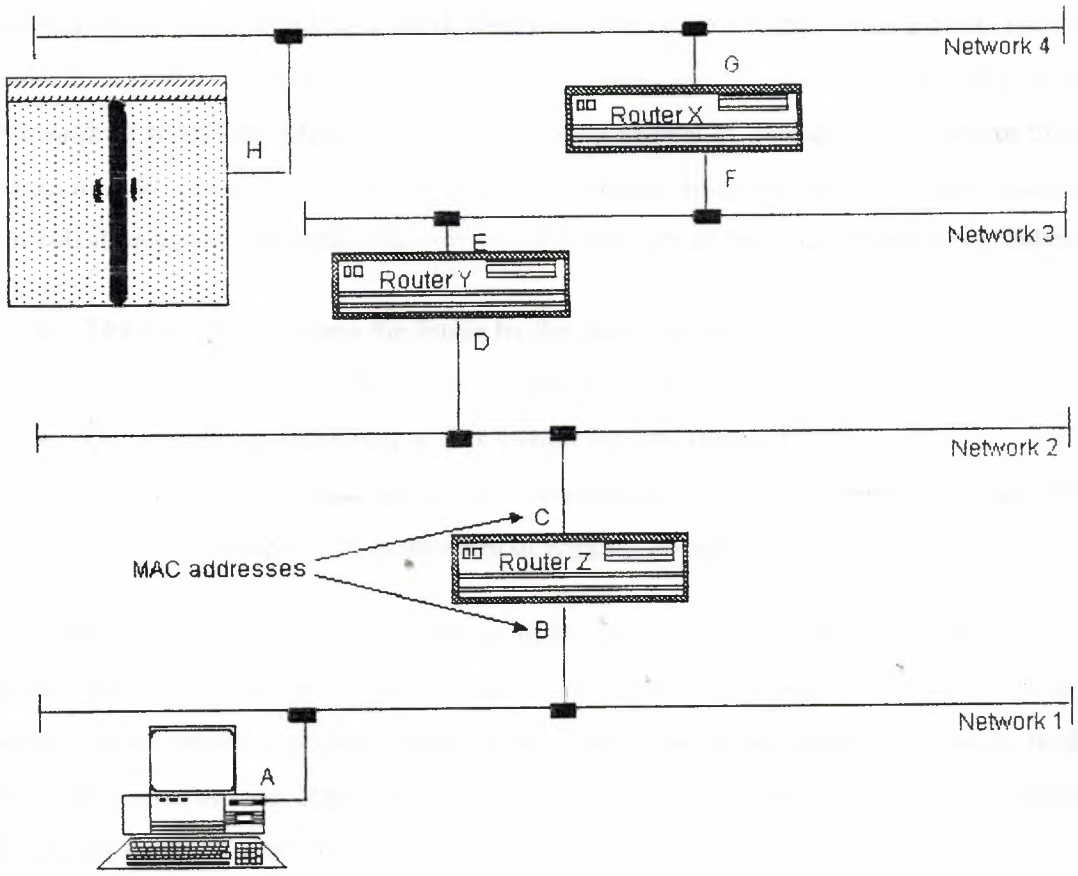

Figure 3.4: Shows a Routing of a Router

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 ahs no other option than to simply discard excess packets. If required, these may later be retransmitted by a transport protocol.

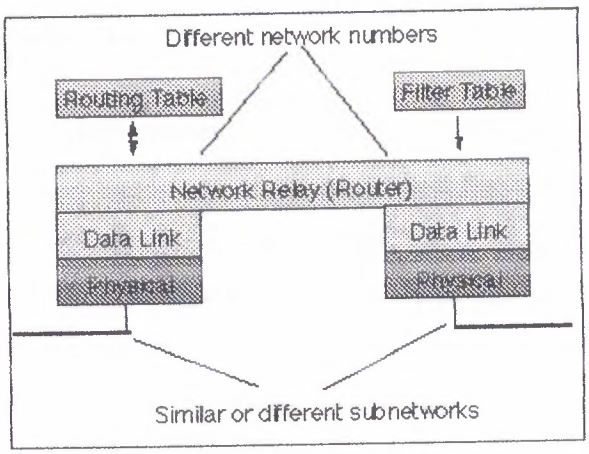

Figure 3.5: Shows Architecture of a router

Routers are often used to connect together networks, which use different types of links (for instance an HDLC link connecting a WAN to a local Ethernet LAN). The optimum (and maximum) packet lengths (i.e. the Maximum Transfer Unit (MTU)) 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.

3.5.1.1 Routing

Most network protocols were designed with network-layer routing. Routers base forwarding decisions on an embedded network number in the network layer header of the packet. They Include network numbers that can be thought of as area codes in the phone system as we must use the area code to call different areas. Any number of end stations may be assigned to one network number like routers do not keep track of individual end stations' addresses. Network numbers used for to group network stations into one or more network numbers. Routers combine networks and form Internets.

3.5.1.2 Information in a Packet

Each OSI layer implementation in the hardware and software of a WAN controller will be placed in the packet. Network layer information is placed in the data field of a packet, which is placed in this header for the network numbers, and this layer header contains more than just network numbers. Source and destination MAC address fields are reserved for the beginning of the packet. Whatever bytes in the packet the hardware and software headers do not consume are left for user data or control information.

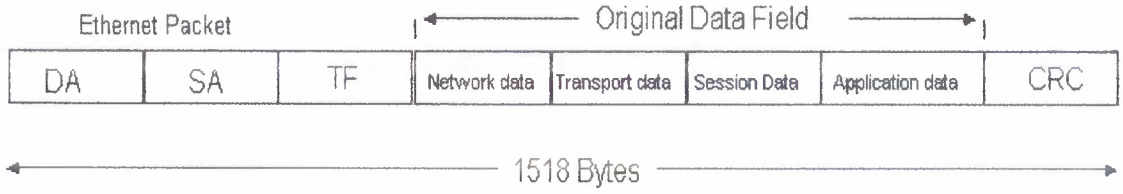

Figure 3.6: Shows the Information in a Packet

3.5.1.3 Router Operations

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 its 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 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.

3.5.1.4 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.

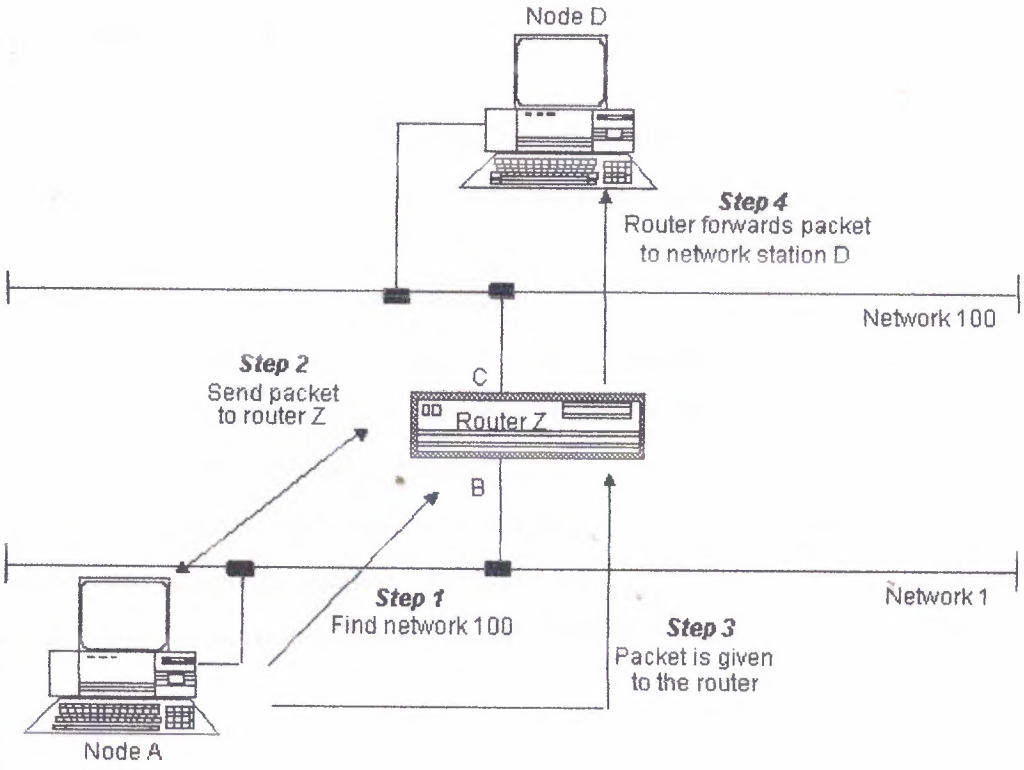

Figure 3.7: Shows a Directly Attached Network to WAN

3.5.1.5 Non-Directly Attached Networks

If the destination network is not directly attached to the router, the router will forward the packet to another router in the forwarding path of the destination network. Router-to-router communication is directly MAC addressed. All routers in the path will perform the same decisions as the previous router. The last router in the path to the destination will forward the packet directly to the destination. Important to note that the data link MAC headers will constantly change while the packet is being forwarded. Very little information in the network header will change the network layer header in the packet will contain the originator's full address and final destination address of the packet. The full address of a network station is the combination of the network ID and its MAC address. This uniquely identifies any station on the Internet.

3.5.1.6 Network Numbers

With the addition of routers, there are now two types of addresses on the network one is network numbers, and other is MAC address. The XNS network numbers are 32 bits long, allowing for 4,294,967,294 unique network numbers. Multiple methods for acquiring a network number are as follows:

- Routers are assigned their network numbers, usually one per port.
- End stations can listen to the network (router updates).
- It can be assigned to an end station.
- End stations can build passive tables based on router updates.
- An end station can request it from a router.

An end station can acquire a remote stations network address from a name server.

3.5.1.7 Routing Information Protocol (RIP)

This is known as a routing table 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 and one hop is considered one router traversed. Devised for very stable, small-to-medium size networks (less than a few hundred nodes).

3.5.1.8 Multiprotocol Routers

LANs currently operate with many different types of protocols.

- Apple Computers can use AppleTalk.
- UNIX workstations use TCP/IP.
- Client/Server applications could use Novell NetWare.

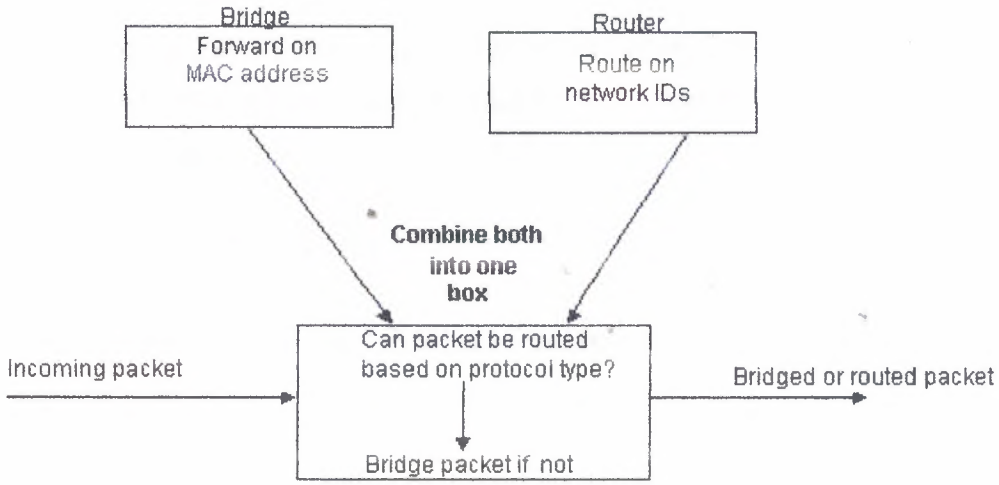

Figure 3.8: Shows a Block Diagram of Multiprotocols Router

Routes not only based on the network IDs but also are able to pass the packet to the correct protocol processor by examining the Type of packet.

3.5.2 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.

3.5.2.1 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.

3.5.2.2 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. A good five-port Ethernet hub can be purchased for less than $50 USD

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.

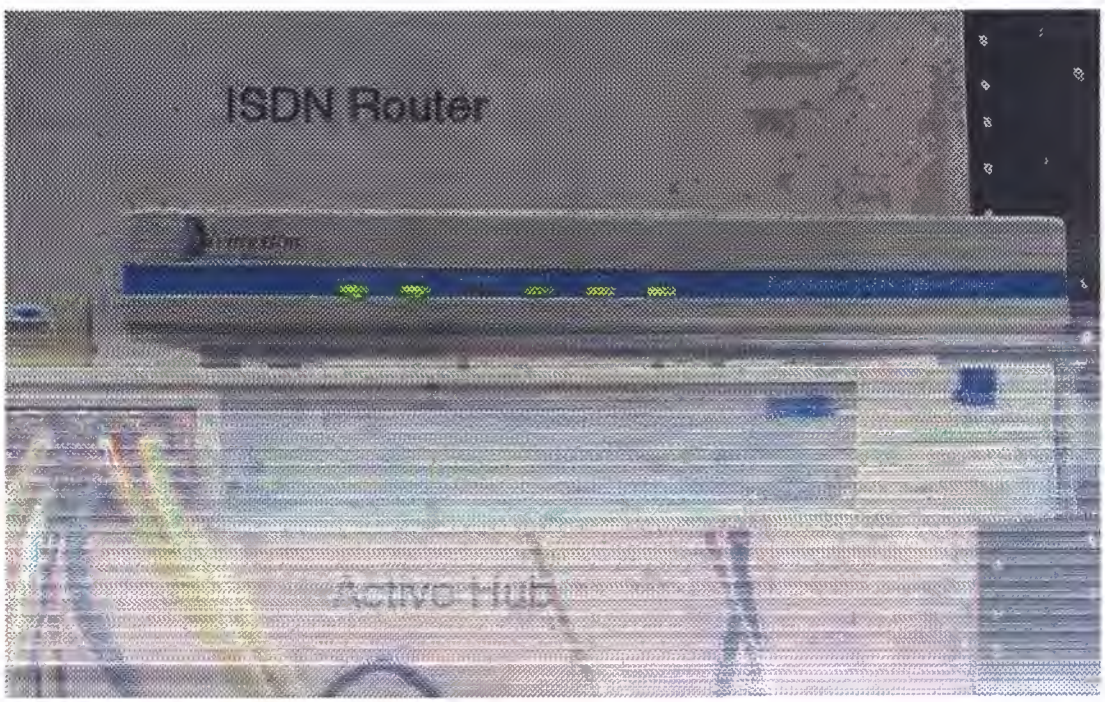

Figure 3.9: Shows a Active Hub Used with ISDN Router

3.5.3 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 addresses/interfaces, and avoid using this service from public or potentially hostile networks.

3.5.4 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. These are also known as Network Interface Card (NIC).

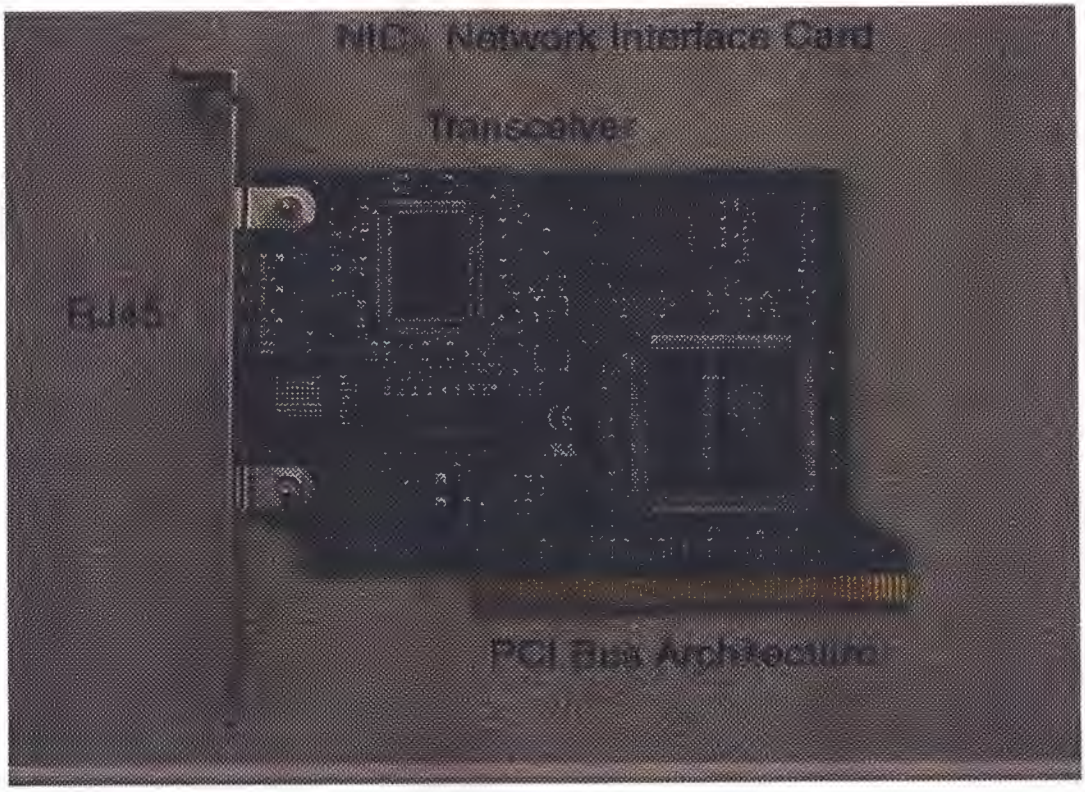

Figure 3.10: Shows a Network Interface Card

3.5.4.1 The Modem Plug (RS-232 Interface)

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.

3.5.4.2 Error Correction and Data Compression

Almost more confusing than the actual protocols and modem commands is the terminology used to describe error correction (also called error control). Error correction is similar to file transfer protocols such as Kermit, 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 protocols 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.

3.5.4.3 Direct, Normal, and Reliable Connections.

Many modems will use these terms to distinguish between several types of modem configurations. A direct connection is the old-fashioned sort with no error correction or data compression. In a direct connection the DTE rate (computer serial speed) and the link rate (modem connection speed) must match. A normal connection uses flow control for speed buffering so the DTE and link rates may differ. A reliable connection uses flow control and will often hang up if error correction and data compression cannot be established. An auto-reliable connection is like a reliable one except the modem will fall back to normal or direct mode automatically rather than hang up.

3.5.5 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.

3.5.5.1 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 a 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 3.11 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.

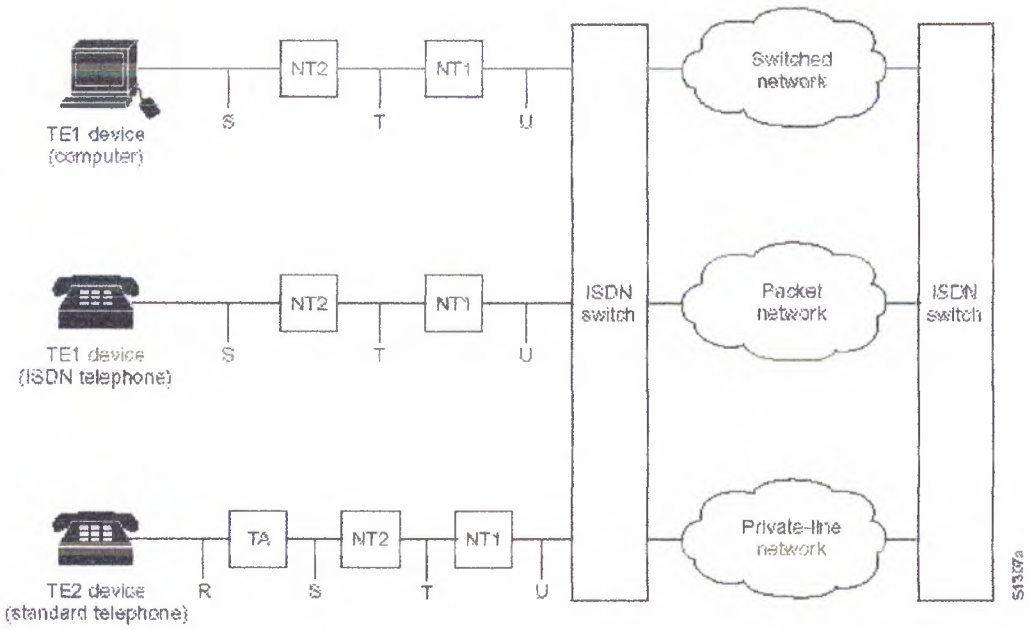

Figure 3.11: Shows a Sample ISDN configuration is illustrated

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). Both physical-layer interfaces are shown in Figure 3.12). 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

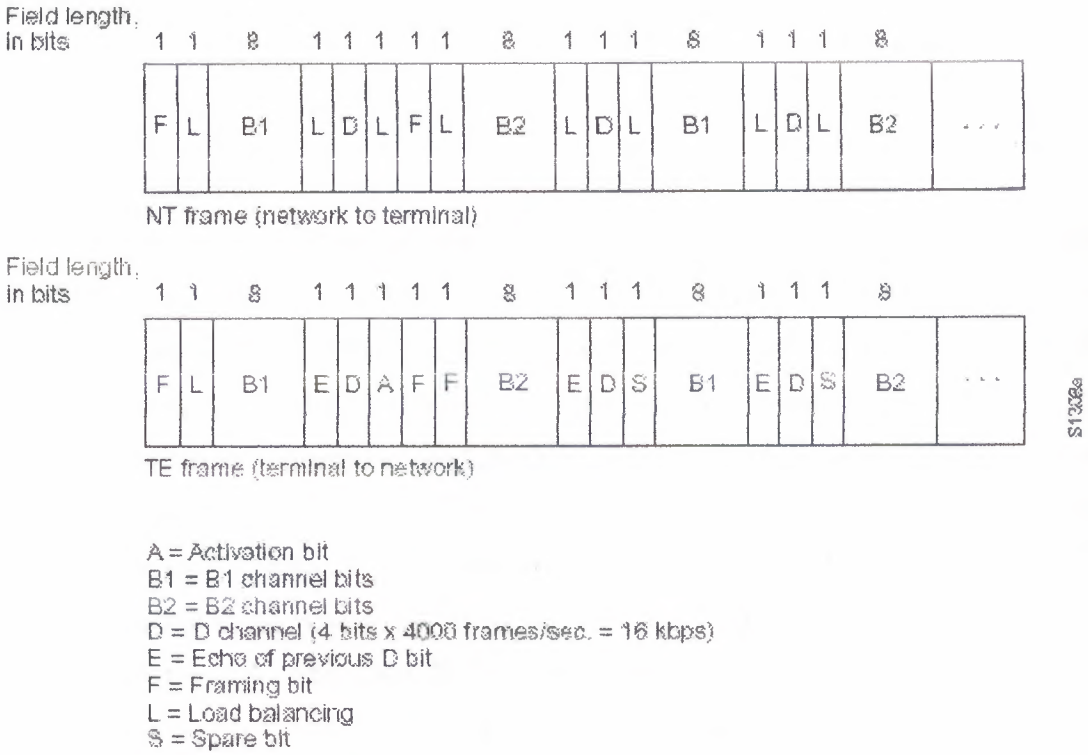

Figure 3.12: Shows ISDN Physical-layer frame formats

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 pre-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 (see Figure 3.13) 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.

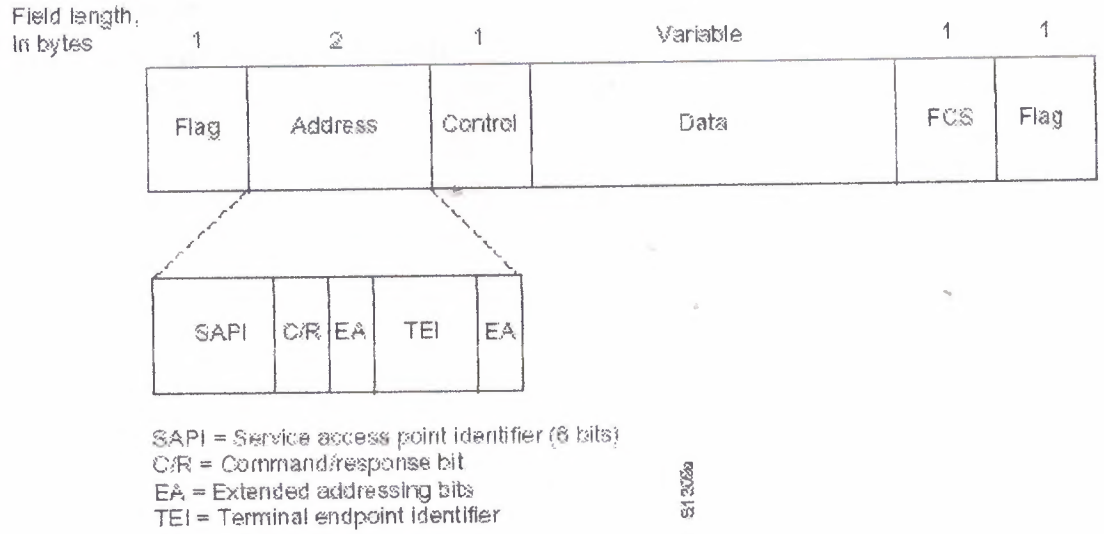

Figure 3.13: Shows LAPD frame format is similar to HDLC and LAPB.

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

Two 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. This Address Flag Control Data FCS Flag Field length, in bytes variable messages are functionally similar to those provided by the X.25 Figure 3.14, from ITU-T I.451, shows the typical stages of an ISDN circuit-switched call.

TEI EA C/R SAPI

SAPI = Service access point identifier (6 bits)

C/R = Command/response bit

EA = Extended addressing bits

TEI = Terminal endpoint identifier

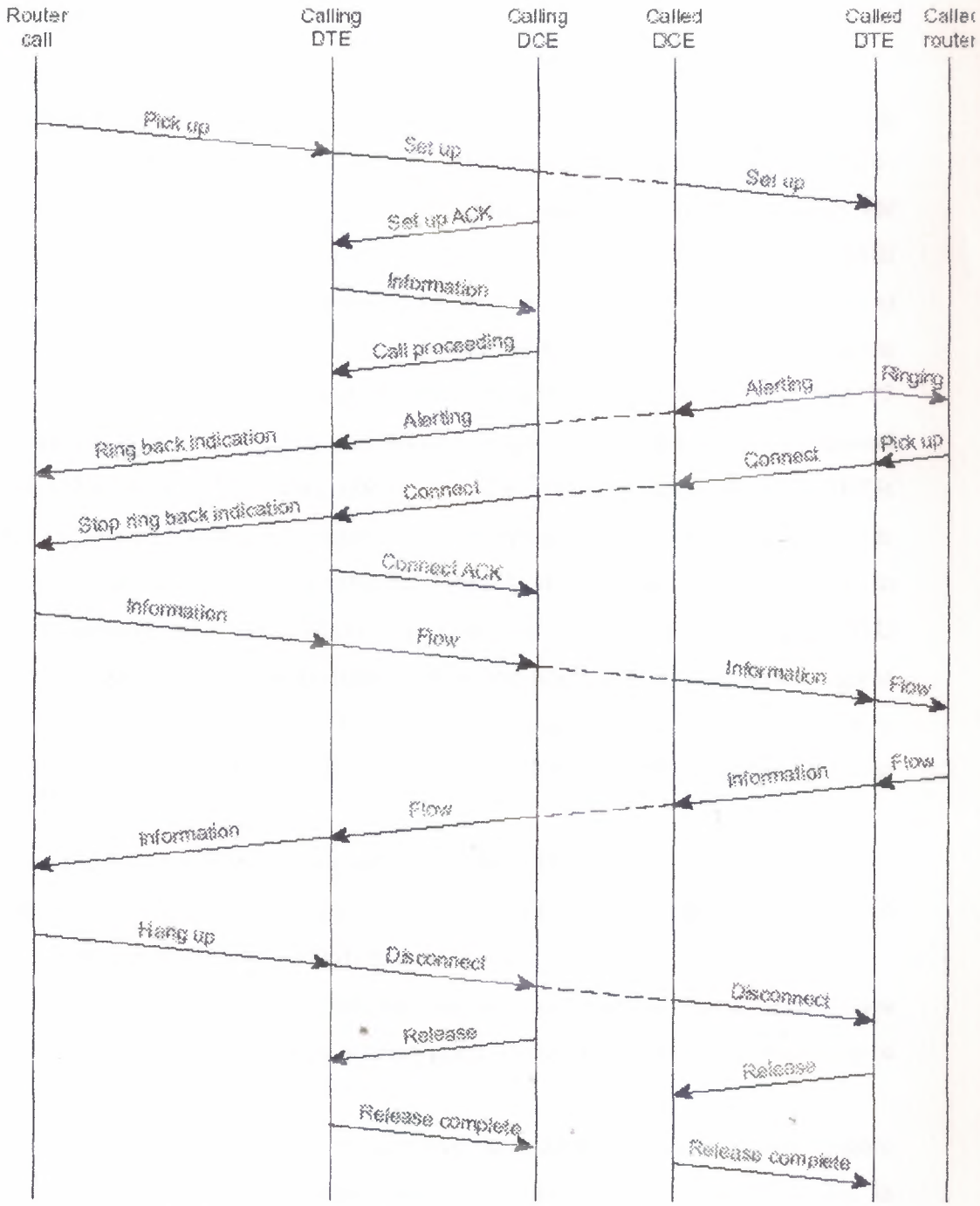

Figure 3.14: Shows an Illustration of Circuit Switched Call

3.5.6 CSU/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:

1. Provide a lower cost than comparable separate CSU/DSU devices
2. Eliminate a potential point of failure in the network, namely, the cabling required to connect an external CSU/DSU to a router
3. 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.

3.5.6.1 Comparing Basic Capabilities

Figure 3.15 shows a basic T1 network access arrangement using traditional non-integrated CSU/DSUs at both the remote and central sites.

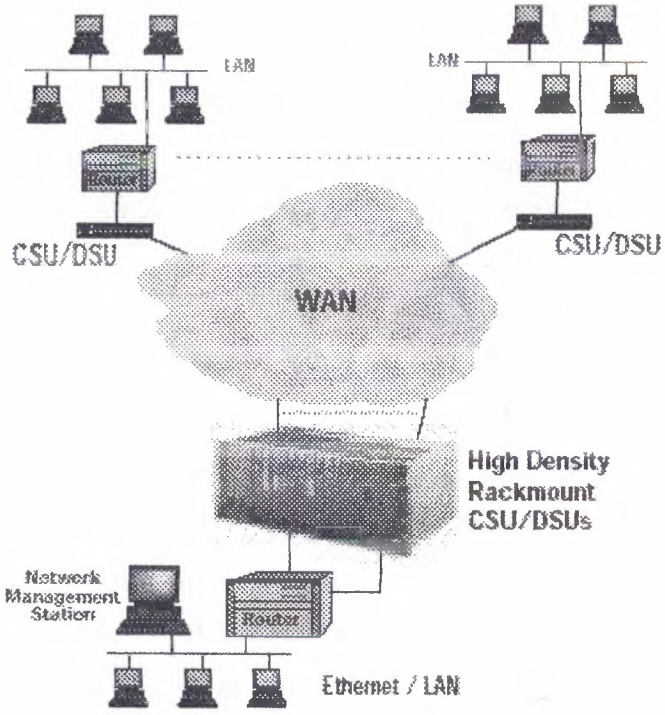

Figure 3.15: Shows a Basic T1 Network Access

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.

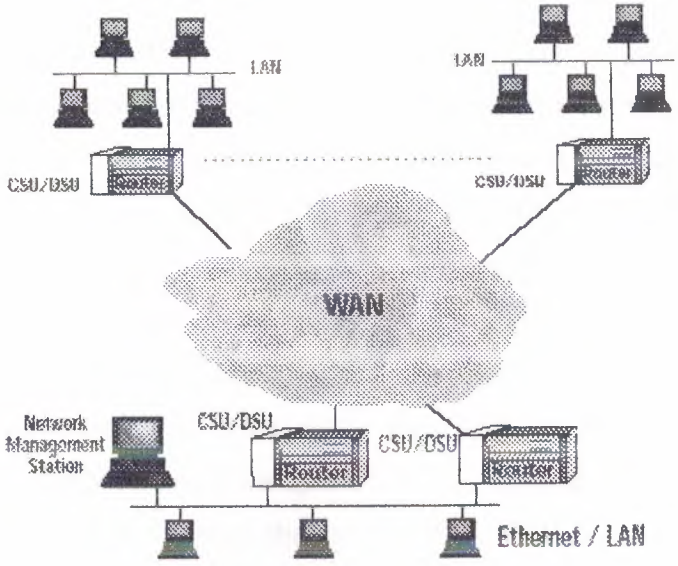

Figure3.16: Shows WAN with Integrated Routers

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.

3.5.6.2 Value Added

Most standalone CSU/DSUs offer additional capabilities typically not provided by integral CSU/DSU offerings. These include:

- DSL Services
- Multiport Capability
- Drop-and-Insert Capability
- Upgradeable
- Portable
- Demarcation of Service Point
- Variable Line Equalization / Build outs
- Automatic Service Rate Selection

- Service Line Isolation / Protection

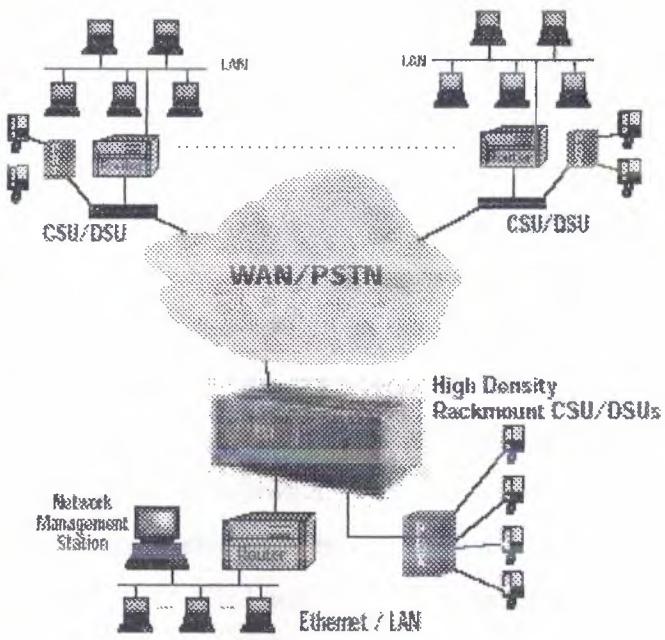

Figure 3.17: Shows a PBX and Router Sharing Single

T1 Access with "Drop-and-Insert" CSU/DSU Depending upon the application, these capabilities can be critical to the resiliency, manageability, and cost effectiveness of a network; and any one of them can make a strong case for a non-integrated as opposed to a router-integrated approach. Unlike integrated T1 CSU/DSUs, non-integrated T1 CSU/DSUs support multiple ports and/or drop-and insert capabilities. The advantage of this is far greater applications flexibility — assuming incremental T1 channel capacity is available. For example, as shown in Figure 3.18, users can easily add via drop-and-insert an additional application, such as voice from a PBX, saving the cost of a separate new T1 circuit. DSL Services The ILEC's competitors, known as the CLECs, are emerging and offering comparable T1 replacement services such as DSL. These services provide an external NTU device, which connects conventional WAN traffic to DSL. An integral CSU/DSU within a router prevents customers from leveraging this future cost savings, which is predicted to dominate service markets for years to come. Multiport Capability allows individual DS0 channels (56/64Kbps) of a T1 to be segmented to support a legacy

application. This can be an effective way of eliminating the cost of an analog leased line between corporate headquarters and a regional facility. The ability to support multiple applications over a simple T1 without adding multiplexing equipment allows maximum use of the T1 line and saves on multiple line costs. Only a non-integrated solution has this capability. Many non-integrated T1 access devices support up to four separate data terminal equipment (DTE) ports with standard physical interfaces such as V.35, EIA-530/422, and EIA/TIA-232-E. This capability can be in addition to the drop-and-insert capability and can be used to support an additional application, such as a PBX, via a DSX-1 interface port. The DSX-1 port also allows the standalone unit to act as a CSU, thus supporting applications where CSU-only functions are required. Figure 3.18 shows a dual router application – again a single T1 access circuit is shared to reduce network costs. Drop-and-Insert Capability allows a T1 circuit to be groomed into two or more "channels" each comprising a selected number of DS0s. For example, the data network could be assigned 512Kbps (8 DS0s) and a PBX assigned the remaining 1024 kbps (16 DS0s) for voice. This mapping or DS0s would eliminate the need for two separate circuits; one for data and one for voice. If two circuits were required to meet the total bandwidth requirement, network diversity could be implemented for the data network (or the voice network), without having to purchase additional circuits. Drop-and-insert can also be used to split a T1 circuit between two routers, each being assigned a fractional T1 circuit speed, for example, 1,024Kbps (16 DS0s) and 512Kbps (8 DS0s) respectively. This accommodates situations where secure server access has to be provided for Internet access, but the firewall is not required (or desired) on the organization's intranet. Upgradeable Unlike an integrated CSU/DSU that is limited to its basic functionality, a non-integrated CSU/DSU can easily be upgraded to support drop-and- Access with "Drop-and Insert" CSU/DSU insert and/or multiport features.

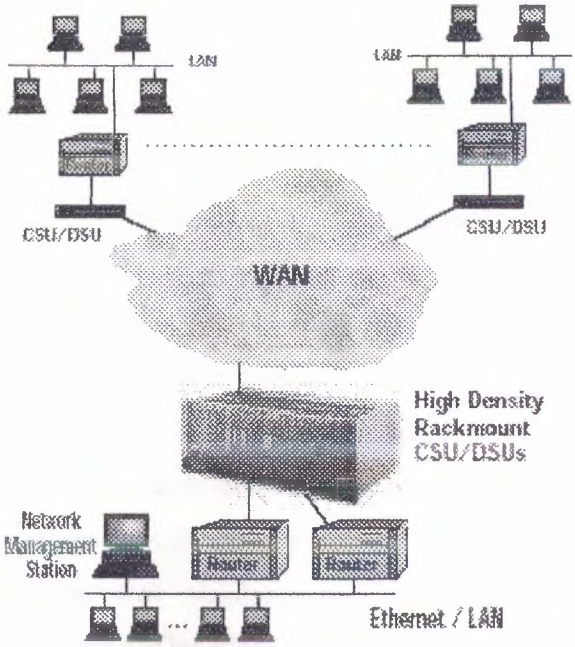

Figure 3.18: Shows Dual Routers Sharing Single T1

In this way, non-integrated access greatly increases the flexibility to accommodate network change and growth and match the best router and best access features to the application. Portable a non-integrated CSU/DSU, whether directly or indirectly LAN connected, can be easily relocated. A non-integrated unit can also be used with any manufacturer's router and also within non-routed applications in the same T1 network.

3.5.6.3 Diagnostic Testing

Fault Insulation and Troubleshooting With an integral CSU/DSU, fault isolation troubleshooting can be difficult. Should the router at the central site fail, the network administrator cannot immediately isolate the problem as to an integral CSU/DSU failure, a T1 line failure, or a network failure. If the router at the remote site fails the network manager will probably have to dispatch a technician to test the router or at the very least contact the Telco to check the T1 circuit. In contrast, as illustrated in Figure 18, a non-integrated solution can include a LAN-connected, out-of-band management path to the CSU/DSU at the central site and an in-band management path at the remote site.

Consequently, if the central site router fails, the condition of the central site CSU/DSU and router — and the router DTE connection and corresponding leads can be determined via a LAN-attached Network Manager. If the remote router fails, the condition of the remote router and CSU/DSU can be determined directly from the central site. If the circuit fails, management communications can be maintained to the remote CSU/DSU via the switched network using a collocated analog modem. The necessary T1 line diagnostic tests can be run without the need to contact the Telco, further reducing the cost of ownership for the standalone solution. Comprehensive Diagnostic Loop back Testing As figure 19 shows, in fractional T1 and multiport applications, loop-back testing at the channel level is essential for isolating problems within the T1 24 DS0 channel bundle. However, most router-integrated CSU/DSUs support only full T1 payload loop backs, while Out-of-Band Management non-integrated CSU/DSUs support non-intrusive channel loop back tests that do not interfere with data passing through other channels.

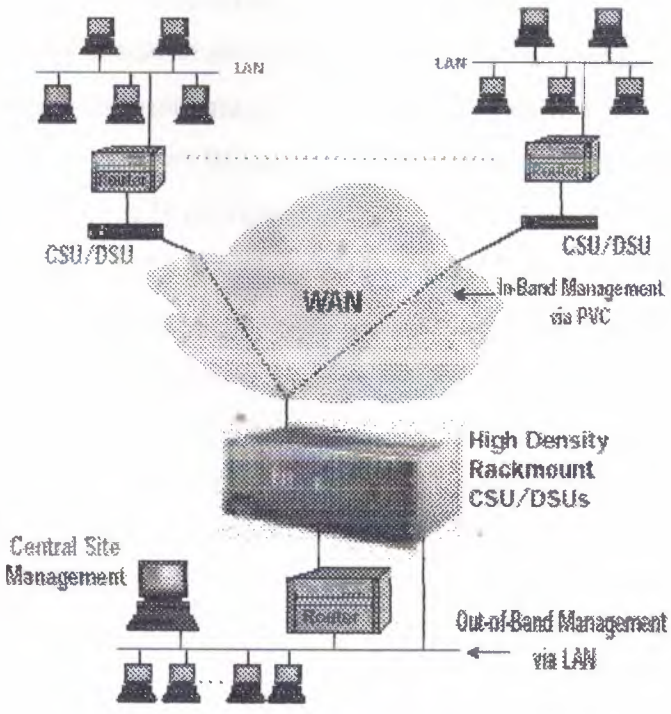

Figure3.19: Shows Centralized, In-Band and

Line Monitoring Break-in line monitoring and testing are standard T1 CSU/DSU features that allow a technician to break into the T1 path to monitor the condition of the circuit and corresponding T1 channels, as well as to trouble shoot by sending specific test transmit/ receive signals. Break-in line monitoring and testing is done using external test equipment without disturbing the data flow via a convenient front panel connector on the CSU/DSU. Most integrated CSU/DSUs do not have this feature. When they do, the break-in connector is inconveniently located at the back of the router lost among all the cables.

3.5.6.4 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 an CSU/DSU fails (Figure 20), the integral CSU/DSU functionality will be lost — or at best significantly diminished — potentially crippling any ability to troubleshoot the network.

3.5.6.5 Frame Relay Applications

A major portion of installed data networks consist of routed frame relay. Frame relay networks offer many obvious benefits, including an economic advantage over multiple point-to-point networks. With frame relay, optimum network design requires good knowledge of the traffic volumes actually being carried. If a frame relay network is over-designed, much of the economic advantage will be lost. If the network is under-specified the network response times during busy periods will become unacceptable, resulting in loss of productivity, not to mention complaints from users. In addition, due to the bursty nature of LAN-to-LAN traffic, it may be difficult without actual monitoring of the traffic, to know whether poor response times are the result of congestion in the carriers network or the result of under-sized (i.e. under specified) frame relay circuits, or the result of server response times. The solution to these potential problems is the Frame Relay Probe or "Frame-Aware" CSU/DSU, which can provide real-time network traffic information and network status information. Frame Relay analysis capabilities found within routers is not enough.

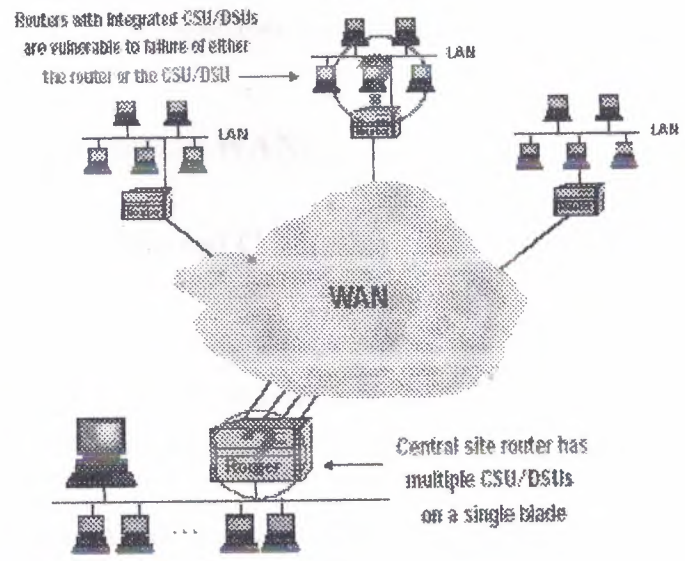

Figure 3.20: Sows Single Point of Failure Risk

Frame Probe For example, GDC's Frame Relay Probe provides both the probe and the CSU/DSU functionalities in one unit providing valuable information on:

- Network Availability
- PVC Availability
- Network Delay
- PVC Throughput
- End-to-End Frame Loss
- Forward and Backward Explicit Congestion

Notifications (FECNs and BECNs)

- Discard Eligibility (DE) Frames
- Local Management Interface (LMI) Statistics

(Timeouts and No Responses)

- Bandwidth Utilization
- Committed Information Rate (CIR) Utilization.

Data can be retrieved from each innovx unit via the web and can be stored in a PC network management station. Using either Innovx Frame Manager software or industry available network management software such as Concord's Network Health; weekly, monthly, quarterly and yearly trend analysis and data reporting is readily available.

3.6 External Connections to WANs

3.6.1 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:

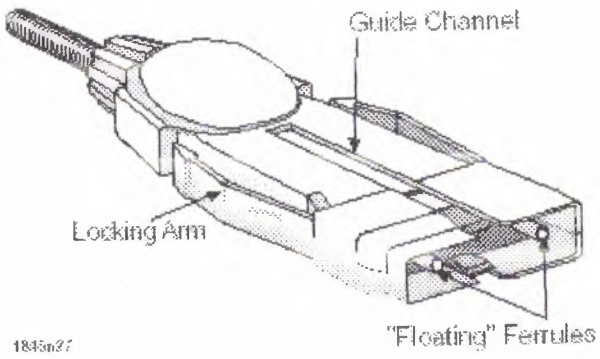

Figure 3.23 FDDI MIC

The MIC connector is designed to prevent the mis-connection of segments and devices. It is specifically constructed in an asymmetrical fashion that prevents the connection of transmit strands in the connector to the transmit devices of an FDDI device.

The sides of the FDDI MIC connector have built-in locking arms that snap the connector into place once it has been fully inserted and keep it from being pulled out.

3.2 LAN Technologies

Each computer in a LAN can effectively send and receive any information addressed to it. This information is in the form of data 'packets'. The standards followed to regularize the transmission of packets, are called LAN standards. Usually LAN standards differ due to their media access technology and the physical transmission medium. Some popular technologies and standards are being covered in this article. The following are the most popular standards.

- Ethernet / IEEE 802.3
- Token Ring / IEEE 802.5
- FDDI (Fiber Distributed Data Interface)
- ARCnet
- LocalTalk (Macintosh Neworks)
- Wireless / IEEE 802.11b

3.6.6 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:

a) "Strange" network behavior could be an intrusion, so a monitor should be able to note "strange" (i.e. not "normal") network behavior.
b) 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.

- The Solaris 1 utility etherfind or the Solaris 2 utility snoop or the VMS utility ethermon could be used to monitor the network for unusual behavior, but only from qualified, trusted personnel!
- 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. ADVANCED FEATURES OF WAN

4.1 Overview

It's true that WAN can be complicated, especially for large, multi-site businesses. There are many variables that must be considered, from the availability of WAN services. All of this can be quite technical. And the needs of each business are different, so there's no one-size-fits-all solution.

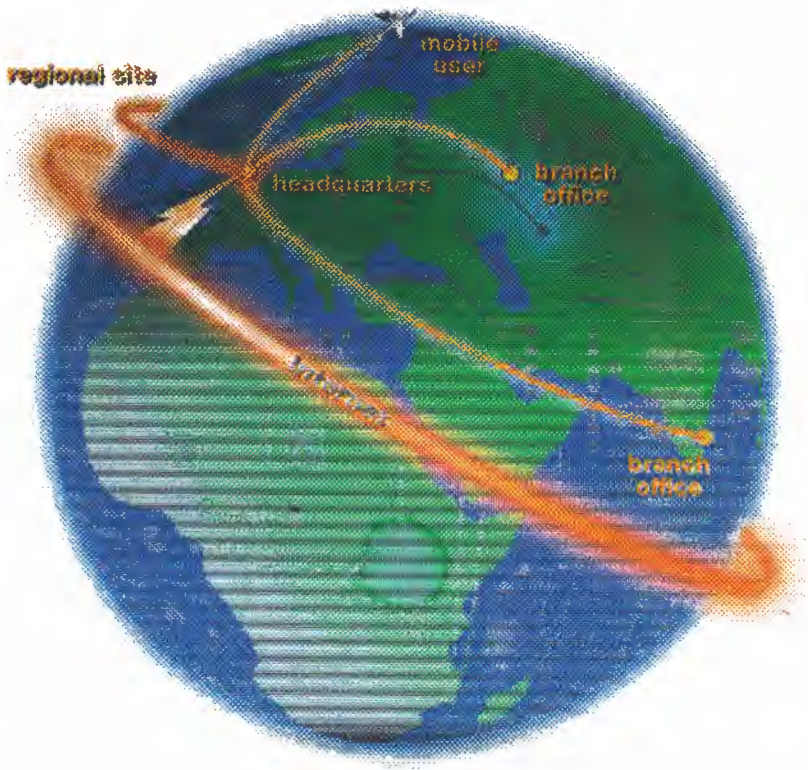

Figure 4.1: Shows a Global Network

Your business - how many sites and where are they located?

- Single
- Multiple Domestic
- Multiple International

As in the early days of long distance telephone service, the design of a modern WAN solution requires a careful consideration of the present and future locations of your business sites, as well as the distances between locations. This is essential, since not all WAN services are available in all locations. And for most services, the distance between locations is a key factor in determining monthly costs.

To begin, it's useful to create a hierarchical diagram of your business sites Figure 4.2. You'll also want to start a file for each site, to collect site-specific information about available services, monthly rates and other criteria for your WAN solution. Later, as you further analyze your wide area networking needs and expand your diagram, you'll need to think more in terms of the logical data flow of your network. This can be very different from geographical, political or organizational structure.

4.2 WAN connectivity

Many small businesses want no more than to establish an Internet connection. Others need to share e-mail, files and applications between LANs and remote users at distant sites. The connections you wish to establish may vary from site to site, so you'll need to assess your requirements at each location. Be sure to consider the implications of business growth. This can help you plan a scalable WAN solution that will expand easily as your needs evolve. In assessing your needs, consider each of the following WAN applications:

- Internet access - For global e-mail, as well as marketing, sales and research via the Internet

database servers that will be accessed from all your users over the WAN, traffic might be heavy and continuous at that location. However, a single site with a great many users might need only occasional Internet access. In this case, WAN traffic would be light and sporadic.

- Traffic characteristics—Not only the quantity, but the quality of your WAN traffic is important in designing an effective solution. Traffic depends on the applications you want to use over your WAN (e-mail, database, file access, etc.) as well as on how data and communications need to flow within your particular business. It can be useful to add this information to the diagram of your company sites Figure 4.3. Also indicate the locations of servers that must be accessed over the WAN.

Evaluate the traffic for your selected applications with respect to each of the following criteria:

- Constant vs. intermittent. For constant traffic, you'll need a continuous WAN link. For intermittent traffic, a dial-up connection might be more economical.
- Business-critical vs. convenient. Depending on how critical your WAN connection is, you might need a backup link to protect against any potential disruption in service.
- Time-sensitive vs. time-insensitive (latency). If you'll be running time-sensitive applications across your WAN, such as audio, video or a real-time database, you may need the guaranteed low-latency of a dedicated connection. If you'll only be supporting applications such as e-mail and intranet access where short delays in transmission are acceptable, a less expensive type of connection might better serve your needs.
- Private vs. public (security). If you plan on connecting to a public WAN, especially the Internet, you'll probably want to restrict unauthorized access to your LAN. So you'll need to consider firewalling capabilities in your choice of routers. If you want to send confidential business data across the WAN, you'll also want to consider encryption and VPN capabilities, as well.

- One-to-one vs. many-to-many. Will each site need to access information from multiple sites or is traffic exchanged on a one-to-one basis, as for a remote office connected to a central site?
- LAN/WAN protocols. You'll need a router that can support both your LAN and WAN protocols. Give strong consideration to routers with multiple protocol support as this will increase your flexibility in selecting WAN services should your needs or location change.

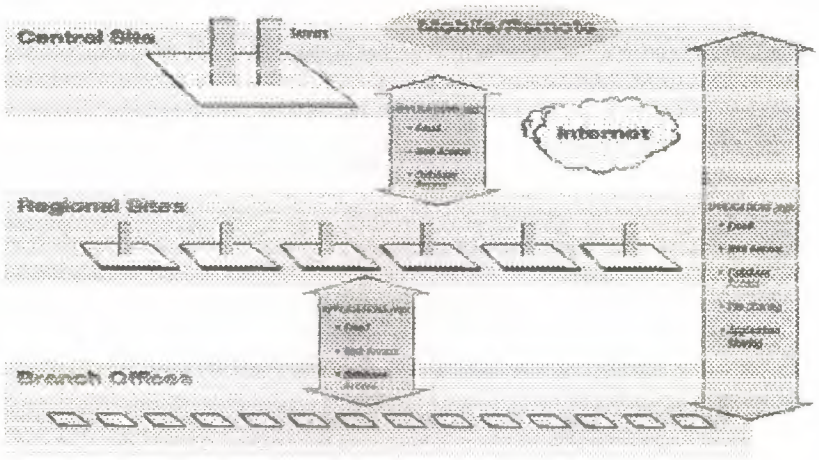

Figure 4.3: Shows Adding of Server locations of WAN applications

4.3 Determining the Appropriate WAN Service

Once you've analyzed your WAN requirements in terms of your business needs and the kind and amount of traffic you wish to route, it's time to select the best available WAN service—or combination of WAN services—for your particular situation. WAN service availability and costs vary by country, by region and by individual service provider. So you'll need to assess both costs and availability for each business site that you wish to connect. This may take considerable research. When dealing with multiple international sites, you might not be able to choose a single type of service to link all your sites.

WAN service options - advantages and disadvantages can be seen in Table 4.1: as it comes in four basic varieties as such

4.3.1 Dial-up (ISDN and analog modem)

Like a mesh network, a single dial-up connection supports links to many remote sites Figure 4.4. However, for the most common dial-up services, only a maximum of two links can be established at any one time. As a rule of thumb, dial-up connections are cost-effective when communication between sites is limited to four hours or less per day. Additional savings are possible for applications that can be time-controlled, such as daily database updates. It's generally better to have fewer long calls than many short calls, since each call is normally charged per full minute.

Analog modem connections travel over standard telephone lines and standard phone rates apply. ISDN comes in two varieties, BRI and PRI. Both are more expensive than analog connections, but offer greater bandwidth with no dial-up time. PRI ISDN is a higher performance alternative suitable for a busy central site. Unlike BRI ISDN, it allows many simultaneous connections.

4.3.2 Dedicated Point to Point (Leased Line)

A leased line provides a dedicated point-to-point connection between two sites Figure 4.5. The key advantages of a leased line are guaranteed bandwidth and high reliability. However, you can't connect multiple sites with a single leased line. You need a separate line for each link. Leased lines are also expensive, especially over long distances, since charges depend on transmission distance as well as bandwidth. A leased line between New York and London, for example, could cost several hundred thousand dollars a year. Recently, leased line services have been regaining popularity, because they're being used for short connections to local Internet Service Providers (ISPs). The dedicated line guarantees a quick connection to the Internet or a switched network, and costs are reasonable because the distances are short.

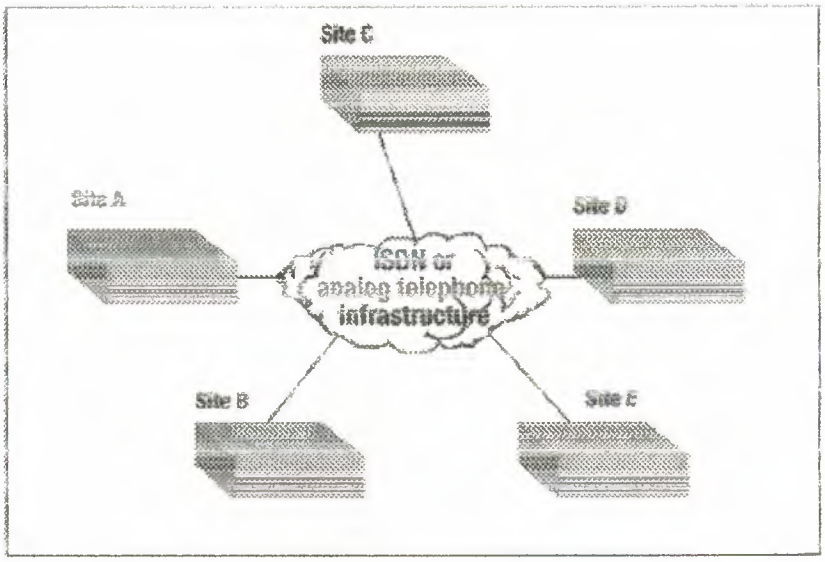

Figure 4.4: Shows Dial-up Connections for multiple PPP connections

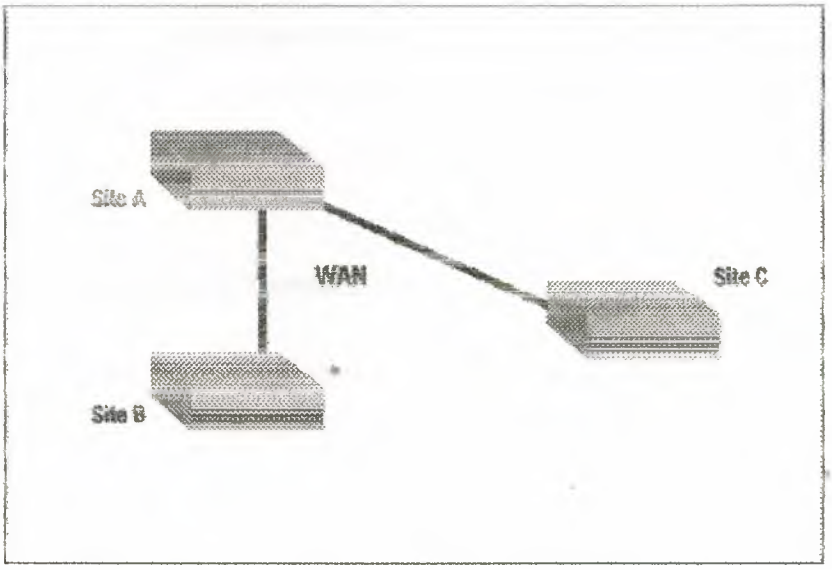

Figure 4.5: Shows Dedicated PPP Connection between Sites.

4.3.3 Mesh Network (Frame Relay or X.25)

Mesh networks allow many remote sites using just a single connection (usually a leased line) to the Telco or carrier. The carrier routes the data to the destination address according to available bandwidth Figure 4.6.

Mesh networks are generally less expensive than leased lines, and offer a more flexible solution. Each site can connect to their local Telco or carrier using a different bandwidth, depending on traffic demands. Additional sites can also be added easily. The only limitation is in the number of sites that can be defined in the router being used (Intel Express Routers are unique in supporting up to 60 links). Because of their flexibility, switched networks are increasingly popular. Frame Relay is a newer technology than X.25, and supports higher bandwidth traffic.

- Internet VPN - Internet VPNs let you take advantage of the Internet for enormous cost savings when networking business sites over long distances. Since a single Internet connection can be used to link multiple business sites as needed, VPNs combine many of the advantages of PPP, dial-up and mesh network connections. They also add a layer of abstraction above the level of the WAN service protocol, which makes it easy to integrate traffic of different WAN protocols.

4.3.4 WAN Service Providers

4.3.4.1 Your Networking Reseller

If you have an existing relationship with a networking reseller, they're probably your best WAN service resource. Most resellers have broad experience with WAN communications. Many also have working relationships with Telcos and ISPs, enabling them to provide good rates on Internet access and services. Based on their knowledge and understanding of your network structure and needs, they can help you design and implement a complete solution—one that is customized to meet your business needs and to fit your networking environment.

4.3.4.2 Your Telephone Company (Telco)

Though a Telco may not know your network or understand the particular needs of your business, they can offer wide-ranging expertise on WAN service options. Most will gladly help you evaluate cost and benefit tradeoffs for particular services. They also offer turnkey Internet solutions for business customers.

To order WAN services you'll probably need to contact both a local Telco (PacBell, USWest, BellSouth, etc.), and a long-distance Telco (AT&T, MCI, US Sprint, etc.). You can connect to the Telco's long-distance network using existing telephone lines or by leasing a dedicated line from the local Telco.

Internet Service Providers (ISP) - ISPs traditionally provide Internet access and related services such as web page hosting, management and development. Some also include hardware and software sales, but most rely on partner relationships with networking resellers to provide complete WAN solutions. You can connect to an ISP through dedicated lines leased from local Telcos or via dial-up links over standard telephone lines. Billing usually includes two fixed rates charges, one for the connection and another for Internet services, but other charges may apply.

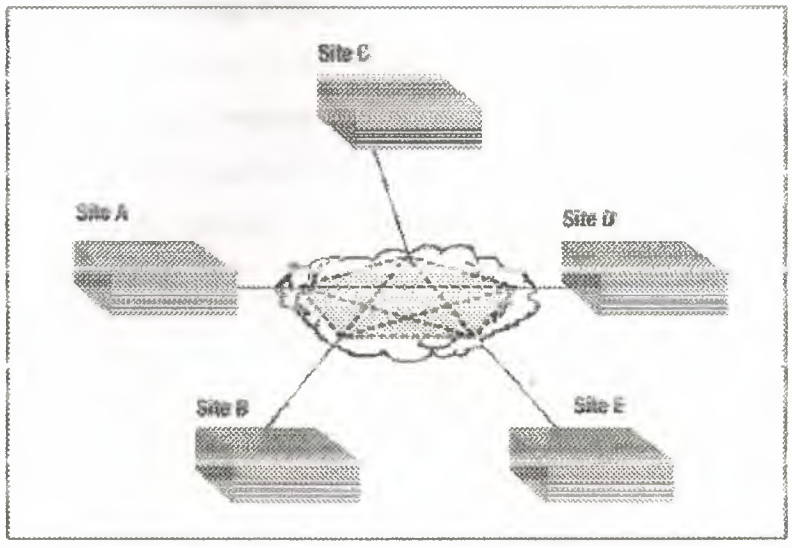

Figure 4.6: Shows Multiple Links Via a Single Physical Connection.

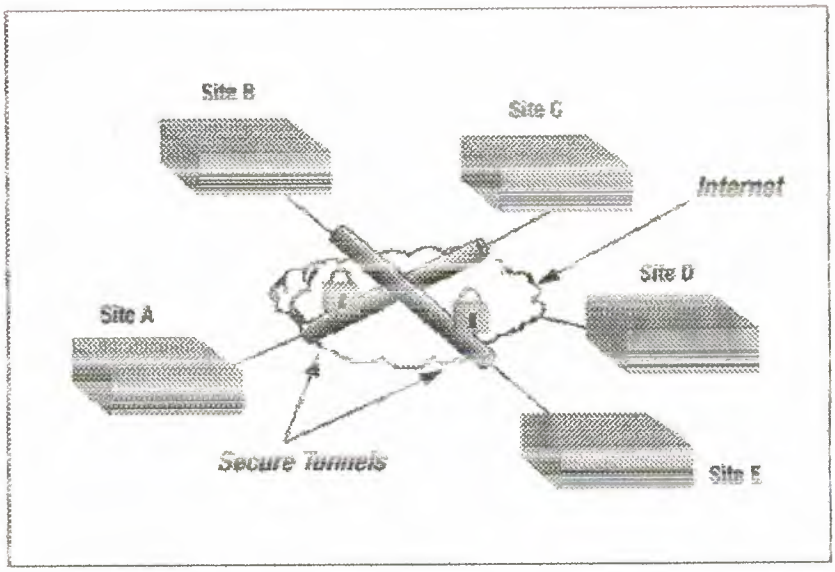

Figure 4.7: Shows Multiple Secure Links Via a Single Internet Connection.

4.4 Saving Money with Internet VPNs

The use of the Internet for long-distance LAN-to-LAN communication can cut as much as 80% off the cost of traditional WAN routing. Currently, many companies aren't taking advantage of these savings, because they're concerned about security. Virtual Private Networking (VPN) provides an effective solution. VPNs also provide a secure and affordable technology for remote LAN access, helping to connect remote and mobile users to their central LAN.

Table 4.1: Shows WAN Service Features

WAN Service	One WAN port gives	Simultaneous Connection	Key Points
Dial-up			
Analog	Multiple connections	Single	• One site to one site • Slow speed and long dial-up
ISDN Dial-up (BRI)	Multiple connections	1 link (128K) or 2 links (64K each)	• One site to one site • Virtually no dial-up time
ISDN Dial-up (PRI)	Multiple connections	30 links (up to 64K per channel)	• Central site • Many simultaneous connections • Virtually no dial-up time
Leased Line	One Connection	Single	• Fixed site to site • Guaranteed bandwidth • High reliability
Mesh Network			
Frame Relay	Multiple Connections	Multiple	• One to many • Guaranteed bandwidth • Scalable bandwidth
X.25	Multiple Connections	Multiple	• One to many • Mostly used with old communication infrastructure
Internet VPN	Multiple Connections	Multiple	• One to many • Cheaper for long distance WANs • Flexible bandwidth • Higher latency • Local WAN service independent

Table 4.2: Shows Some Special Features of WAN

WAN Service	Bandwidth	Pricing	Geographic Availability
Dial-up			
Analog	• Up to 56 K	• Normal telephone rates plus time-metered long distance	Available everywhere
ISDN Dial-up (BRI)	• Up to 64 K per channel • 128 K bonded	• Time-metered local and long distance; often per dial-up charge	Primarily Europe, and parts of Asia, growing in North America, Latin America and emerging markets
ISDN Dial-up (PRI)	• 64 K per channel	• Time metered local and long-distance; often per dial-up charge	Primarily Europe, and parts of Asia, growing in North America, Latin America and emerging markets
Leased Line	• 56 K-1.5 Mb (for T1) • 64 K-2 Mb (for E1) • 45 Mb (T3)	• Based on distance and bandwidth	Available everywhere, affordability is highly variable
Mesh Network			
Frame Relay	• 56 K-1.5 Mb (for T1) • 64 K-2 Mb (for E1) • 45 Mb (T3)	• Based on distance and bandwidth; sometimes data volume	Primarily North America and Western Europe
X.25	• Up to 64 K	• Based on bandwidth: often also a usage and per dial-up charge	Typically in emerging markets in Asia, Latin America and Eastern Europe
Internet VPN	• 56 K-1.5 Mb (for T1) • 64 K-2 Mb (for E1) • 45 Mb (T3)	• Based on "local" WAN service connection to ISP Point of Presence plus Internet Access fee	Where Internet access is available

4.5 High-Speed Serial Interface

The High-Speed Serial Interface (HSSI) is a DTE/DCE interface that was developed by Cisco Systems and T3plus Networking to address the need for high-speed communication over WAN links. The HSSI specification is available to any organization wanting to implement HSSI.

4.5.1 HSSI Interface Basics

HSSI defines both electrical and physical interfaces on DTE and DCE devices. It operates at the physical layer of the OSI reference model.

Table 4.3: Shows HSSI technical characteristics are summarized

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

The maximum signaling rate of HSSI is 52 Mbps. At this rate, HSSI can handle the T3 speeds (45 Mbps) of many of today's fast WAN technologies, as well as the Office Channel-1 (OC-1) speeds (52 Mbps) of the synchronous digital hierarchy (SDH). In addition, HSSI easily can provide high-speed connectivity between LANs, such as Token Ring and Ethernet.

The use of differential emitter-coupled logic (ECL) helps HSSI achieve high data rates and low noise levels. ECL has been used in Cray computer system interfaces for years and is specified by the ANSI High-Performance Parallel Interface (HIPPI) communications standard for supercomputer LAN communications. ECL is an off-the-shelf technology that permits excellent retiming on the receiver, resulting in reliable timing margins.

HSSI uses a subminiature, FCC-approved 50-pin connector that is smaller than its V.35 counterpart. To reduce the need for male-male and female-female adapters, HSSI cable connectors are specified as male. The HSSI cable uses the same number of pins and wires as the Small Computer Systems Interface 2 (SCSI-2) cable, but the HSSI electrical specification is more concise.

4.5.2 HSSI Operation

The flexibility of the HSSI clock and data-signaling protocol makes user (or vendor) bandwidth allocation possible. The DCE controls the clock by changing its speed or by deleting clock pulses. In this way, the DCE can allocate bandwidth between applications. For example, a PBX may require a particular amount of bandwidth, a router another amount, and a channel extender a third amount. Bandwidth allocation is key to making T3 and other broadband services affordable and popular.

HSSI assumes a peer-to-peer intelligence in the DCE and DTE. The control protocol is simplified, with just two control signals required ("DTE available" and "DCE available"). Both signals must be asserted before the data circuit can become valid. The DCE and DTE are expected to be capable of managing the networks behind their

interfaces. Reducing the number of control signals improves circuit reliability by reducing the number of circuits that can fail.

4.5.3 Loop back Tests

HSSI provides four loop back tests, which are illustrated in Figure 4.8. The first provides a local cable test as the signal loops back after it reaches the DTE port. The second test reaches the line port of the local DCE. The third test reaches the line port of the remote DCE. Finally, the fourth test is a DCE-initiated test of the DTE's DCE port.

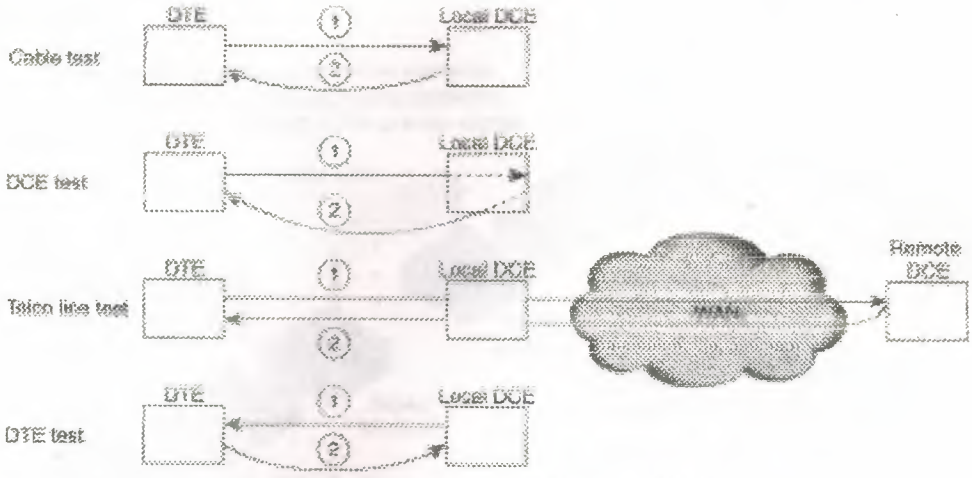

Figure 4.8: Shows the Model of HSSI

4.6 Remote Terminals Wireless WAN Links Reduce the Cost

Overview: Radio modem links connect remote terminals to a host computer without phone company charges. Use unlicensed spread-spectrum radios in the 900 Mhz and 2.4 GHz band or licensed microwave units in the 23 GHz band. Available speeds vary from 38.4Kbps to multiple T-1s of 1.544 Mbps each. This communications technology can save hundreds of dollars per month by completely eliminating telephone company charges. In this application note, we show how one customer used radio modems to connect terminals and multiplexers to a remote host computer. The most common method used to connect remote office terminals with a host computer is a

dedicated phone line, 56 Kbps DSUs (or slower modems), and multiplexers. By replacing the DSUs and phone line with two radio modems running 64Kbps, you can achieve equivalent performance without the phone line. The installed cost of radios is usually returned in less than a year since DSUs aren't needed and phone line costs are normally several hundred dollars per month. Figure 4.9. One details one installation that provides low cost 64Kbps connectivity between two locations at an installed cost of about $3,500.00 for the radio modems. If using radio modems, you don't have to purchase DSUs (typically $1,000 per pair or more). When compared to leased telephone lines that normally cost $200.00 or more per month, a one year payback is easily achieved.

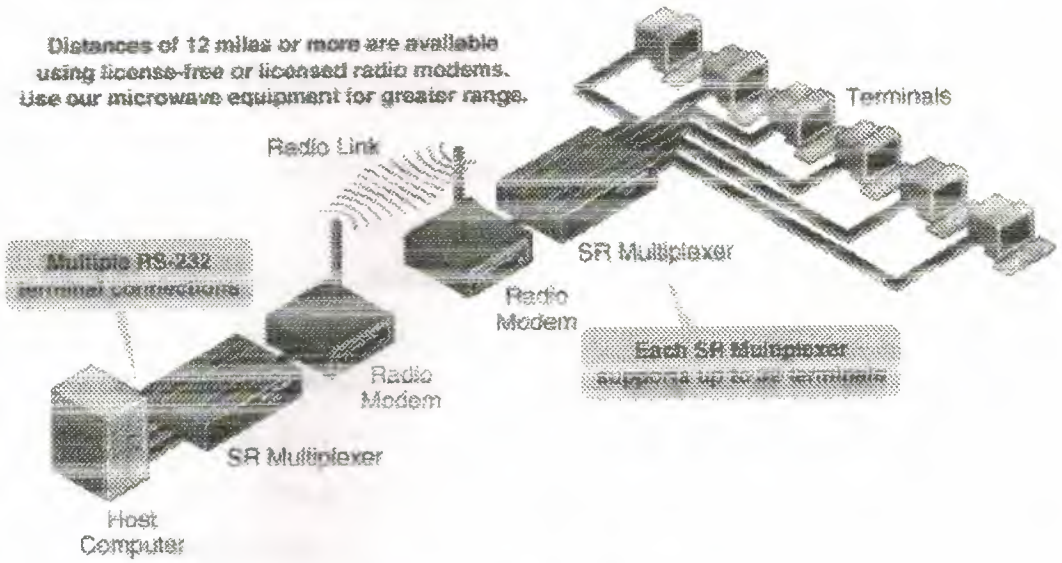

Figure 4.9: Shows Typical Wireless System.

By using more expensive microwave radios, the performance of this system can increase to either T-1 speeds of 1.544 Mbps (24 56Kbps channels) or as many as 4 T-1 paths through the same radio. Most multiplexer installations run at 56 Kbps or slower and medium speed radio links are ideal for their application.

4.6.1 Multiplexers

Multiplexers allow multiple terminals (or PCs emulating terminals) to communicate over the same line. Using DCB multiplexers in a wireless systems is almost identical to wired systems. The same considerations used with DDS, analog leased lines, frame relay, or ISDN circuits come into play. Consider the system throughput requirements and select appropriate radio equipment. All DCB SR and SPL series multiplexers work through appropriate radio links. Where supported by the radios, multi-drop systems are even feasible. DCB multi-drop multiplexer systems support as many as 64 terminals using multiple radio locations.... all on the same license-free spread spectrum system.

4.6.2 Distance Limititations

The maximum distance covered by these sytems varies from several hundred feet to over 20 miles. Most systems require paths termed "line of sight". This is a relative term; as in the case of many short hops, you can't actually see one site from the other. In other cases (especially the high speed microwave systems), the antennae must be within view of each other... no obstructions are allowed. Distances can be extended greatly and obstructions skirted by using repeaters. DCB's Customer Support staff can help design a system that works for your location. The chart shown in Table 4.4. Two shows typical ranges for different system configurations.

Table 4.4: Shows Typical System Characteristics

Model	Max. Range	Max imum Speed	Frequency	Licensed	Antenna
875	3 Miles LOS*	LAN PlusT1	23 GHz	Yes	9□ Dish
950	10 Miles LOS*	T1	23 GHz	Yes	2□ Dish
950	Over 10 Miles LOS*	T1 or Multiple (4) T1	23 GHz	Yes	4□ Dish
RL2	3 Miles LOS*	T-1	2.4 Ghz	NO	Yagi
Sierra	2 Miles LOS*	T-1	31GHz	Yes	9□ Dish

4.6.3 Frequencies

The most economical systems use a license-free band in the 900MHz range. All license-free systems use "spread-spectrum" techniques that were once exclusive military communications methods. This method reduces frequency congestion and minimizes interference. Some spread-spectrum systems also operate in a license-free portion of the 2.4 Ghz band. This frequency is much more "like" microwaves. It has a very narrow beamwidth and typically has shorter ranges. While the 900 Mhz radios often work adequately without a true line of sight path, 2.4 Ghz systems almost always require direct line of sight paths. Another factor to consider is frequency congestion. With a proliferation of devices operating on the 900 Mhz band and no license requirements, interference between unrelated systems will become more of a problem in the future. The characteristics of higher frequency bands such as 2.4 Ghz reduce this probability. We generally recommend 900 MHz for our rural customers and 2.4 GHz for those in urban or built-up areas. For short hops in urban areas, 900 MHz is probably a safe bet. With cost savings between 900 MHz and 2.4 GHz at about $1,000 per link, many customers prefer to go with 900 MHz for their price-consious applications. Since systems in the spread-spectrum license-free bands require no license preparation and little systems engineering, the installation cost is less than 23 GHz systems. The radios are also much less expensive than the higher performance 23 GHz radios.

Licensed radios in the 23 GHz band offer the maximum in reliability and protection. The frequencies are government licensed and must be co-ordinated with other users in the same frequency band. Licensing can take several months and adds to the expense of the system. These radios require precise "aiming" and a true line of sight between the antennae. Systems range from the low end using a nine inch dish with a range of several hundred feet to three miles up to large systems with four foot diameter dishes and ranges of 20 miles or more. The most popular systems use either nine inch or two foot diameter dishes and ranges of one to 10 miles, however, four foot dishes are available for longer ranges. Obstructions are skirted by using repeater systems or higher mounting locations. The 23 GHz systems require systems engineering. In areas where frequency congestion is a problem, 31 GHz radios are available with ranges of two to

three miles. At the 31 GHz frequency, the radios are licensed, but not coordinated. The beam width of these radios is very narrow, so you are less likely to receive interference from other users. These systems also require some systems engineering.

4.7 Implementation of WAN Security

Many users expect the Wide Area Network to protect the computers on it from hackers and worms. It is impossible for the network to do this because telling the difference between a legitimate application and a virus is hard for a human much less a computer. A good comparison would be to expect the phone company to make it impossible to place obscene 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 passwords, then a system will be easier to penetrate. A good password should be at least six characters long and not in the dictionary. Bad password choices include your userid and parts of your name. Some systems support a password generator, such as the VAX (it can be used by typing SET PASSWORD/GENERATE), that picks good passwords. Also, never tell anyone else what your password is. Finally, never write your password down on a sheet of paper or store it in a text file on a computer.

Another key is for the System Manager to install security fixes immediately. Related to this is to never run any executable programs from an unknown source. If other users on the network give you a program, it is wise to get the source code for the program, look over the source, and then compile it yourself. Finally, it is important to keep the number of people that can write files into an account or the system of a computer to an absolute minimum. Unfortunately, many systems take this to an extreme where the computer's usability suffers.

4.8 The Evolution of a Wide Area Network

These days there is little doubt that connectivity is an important part of being a multimedia school. That connectivity includes links to the Internet, to cable/satellite TV, telephone services, district computer systems and servers, and more. It amazes me how important access to these services has become to teachers in our classrooms. At my district our focus is always to look for better ways to integrate technology across the curriculum, and those of us who work on that task at the district level often feel that progress toward this goal is painfully slow. But, if we ever want to feel better about how important technology has become, we just need to be around when a wide area network link to one of our schools goes down. Within seconds, the phone starts incessantly ringing with trouble reports and exclamations of, "My whole class is doing Internet research today! What do I do now?!"

The nature of discussions about connectivity has also changed. Just a couple of years ago the discussions with teachers focused around, "What is the Internet?" or, "When will my school get connected?" or even, "What do I need this for?" Now the questions are, "Can I get more computers in my classroom?" or, "Do you know of a school that would be e-mail pals with my kids?" or more often, "Why does the Internet go so slow?"

My district believes in the Wide Area Network (WAN) concept and it has evolved to include every school in the district, even ones located in remote mountainous areas. We started out using frame-relay connections at 56 Kbps to each of our schools, with multiple T-1 frame-relay connections at our district hub, a building we call the Support Services Center. The concept is simple. First, install a local area network (LAN) inside each school to network the computers together. Next, connect the LANs together using frame-relay circuits to form a WAN. The result is that each school has better access to in-district centralized systems, such as our student records systems and finance systems, as well as access to the Internet through a single Internet connection to the WAN. And, through the WAN, schools are connected to each other, which facilitates collaboration and sharing between schools. The leased-line cost for a 56 Kbps frame-relay connection

to a school is roughly $100 per month (costs vary in different areas). A T-1 frame-relay connection is roughly $350 per month. This has been a tremendously cost-effective strategy, and as it has taken shape over the past four years, we have impressed ourselves, our parents, and our students with all the services now accessible in classrooms.

Unfortunately, as more and more classes started using networked services, the load on our WAN increased dramatically. If you think about a 56 Kbps frame-relay circuit, just what is its capacity? When we started building our WAN, the World Wide Web was something few of us had heard about. Nearly everything we accessed was text-based. E-mail, telnet, and gopher were the buzz-words. Every now and then, someone wanted to transfer a file using FTP. But multimedia over the network? Who ever thought of doing that? Web browser? What's that? Not only were these things lurking just over the horizon, but these were the things people really wanted to do. And now they have arrived, and those 56 Kbps circuits, which were wonderful in a text-based world, have become woefully inadequate. Ten computers running a graphical Web browser can completely saturate the link. And then there are the teaching styles. I remember visiting a class in a computer lab where the teacher was saying, "Class, today we are going to learn how to download a picture. OK, all together now, click on Yoda." I had visions of the 56 Kbps circuit having a melt-down and some server out on the Internet emitting smoke as the simultaneous download request for the full-color, high-resolution, 5x7 image of Yoda was passed along the network from 28 computers. Meanwhile, down in the school office, the office clerk using the district central computer system was wondering why there was suddenly a 10-second delay between each character she typed in a student ID number.

We have tried a number of strategies to better utilize our network resources. Teacher training has been particularly helpful in assisting staff in developing teaching strategies to best utilize the network. Teachers using the Internet in a lab have learned that the network works much better if all the stations aren't doing the same thing at the same time. (Do all those students really need to download a picture of Yoda?) We also have experimented with products such as Web Whacker to pre-download Web sites. This strategy has really not had much success due to the extra planning and time the teacher must spend and some very inconsistent success with the software. We have also added a

proxy server to our Internet connection to minimize the traffic and provide filtering services. But, the bottom line is that we must increase the speed of our WAN links to schools, and we are now in that process. Unfortunately, evolution of a leased communications line is to go from 56 Kbps to T-1, making the cost jump 3-1/2 times! And the cost never goes away. It is there month-after-month. Our district simply can't afford this type of ongoing cost. We needed some other alternatives and have found a couple of great ones.

First, we have begun to invest in wireless WAN links. The advantages of wireless links are obvious. First, after the initial investment in equipment and installation, you own the network. There are no ongoing charges except for maintenance to the system. Second, speeds of even slow wireless links are faster than T-1. T-1 throughput is roughly 1.4 Mbps, and even relatively slow, unlicensed, spread-spectrum radio links are at least 2 Mbps. These systems operate in the 900 Mhz frequency range and can be installed without the need for licensing from the FCC. More powerful wireless systems are available that operate in the microwave range (2.5 Ghz) that do require licensing from the FCC. The system that one chooses is based upon distances that need to be traversed and the capacity and speed needed.

Planning a wireless system is not trivial, and we have been working with a company who specializes in these types of systems. Since building a wireless network can be viewed as a one-time expense, we were able to secure a grant to get us started. The first step was to complete a site-survey of our district. This process involved finding line-of-sight requirements for antennas. We thought our district was a perfect candidate for wireless WAN links, since much of it is relatively flat. But, we didn't realize how many trees are in our town and how tall they are! We soon learned that while we could make a line-of-sight link with a small roof antenna to many of our schools, some school sites would require a very tall pole (up to 100 feet) on which to mount the antenna. Have you ever seen a 100-foot pole? (That's tall!) Would want one next to your house? Would your city want you putting one up next to your school? We wanted to be sensitive to our community and started looking for alternatives to the poles. We worked with our nearby college (Colorado State University), which allowed us to put some relay antennas on top

of their tallest dormitory. We looked at the football field next to one of our high schools and found that one set of field lights was already atop a 100-foot pole. We added an antenna to the same pole. And we used roof-mounting locations where possible. Because of our distances, and because we wanted a system with excess capacity, we chose mostly licensed microwave links that operate at 10 Mbps full-duplex, meaning that the system can transmit 10 million bits per second each direction simultaneously. This is actually faster than the standard Ethernet we use for the LANs inside our schools.

All has not been smooth sailing with our wireless project. We already had plans to light one of our baseball fields and decided this was an opportunity to build one light pole a little taller to accommodate antennas. Even though we held neighborhood meetings before construction to talk with neighbors about the lighting project, some people didn't react until the lights and poles were up. This has turned in to a major political issue for us. I must say that I never thought I would be at a meeting where people were told we needed to light a field so we could have a better computer network! Kind of boggles your mind, doesn't it? We also have learned that antennas are subject to the whims of the weather. One antenna was dislodged from its building mount due to severe wind. And, during one snowstorm last spring, an unusual combination of wind direction and wet snow caused the snow to cake onto an antenna so that it couldn't work. Trust me, being up on a roof in a snowstorm to scrape snow off of a microwave dish is not my idea of a good time. Fortunately, that antenna was not at the top of a 100-foot pole! Part of our evolution is learning techniques to avoid these problems.

Another alternative we are now implementing is a partnership with our city and regional power company. The regional power company, owned by several cities in northern Colorado, is connecting together their power substations using fiber-optic cable. Their purpose is to have a better control system for their power distribution network. But, the company had the foresight to seek partnership with other government agencies. As a result, we will have the opportunity to own or lease fiber strands in their network and use it to connect schools to our WAN. A fiber connection will provide super-fast connectivity and has the promise, thanks to the partnership of government agencies, to be extremely cost-effective for us.

Over the next few years, I expect most of those 56 Kbps connections will have been upgraded. Faster leased lines such as T-1, or wireless links, or maybe fiber-optic will have replaced them. Each of these technologies has its limitations and advantages. By combining all of these methods into one network, we hope to be able to afford better connectivity for all the schools in our district. We are also looking at integrating our voice telephone service, security systems, and networking needs using these technologies. By eliminating numerous individual phone lines to each building and replacing them with a pool of lines shared across our WAN, we have the potential to realize some significant savings as well as better connectivity for all our communications needs.

CONCLUSION

This Project presents inclusive information for implementing the Wide Area Network (WAN) and its devices. 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 between 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 establish this communication between each terminal and between other LANs. It also uses some reference models, which are some standards communications and protocols. One of the main disadvantages of WAN is security. As WAN is use to communicate between the systems at a distance ad many terminals are attached so it is difficult to maintain security and also difficult to reduce bad traffic on a line. The main advantage of WAN is only subscribed user can share or manipulate information. Today many big companies are using WANs. Such as all the Air reservation Companies Uses WAN for reservation of a person from any of their regional office or travel agency.

REFERENCES

[1] Tanebaum Andrew S., *Computer Networks*, 1996

[2] Martin Michael J., *Understanding the Network: A Practical Guide to Internetworking*, Macmillan Computer publishing, USA, 2000

[3] Mahler, Kevin. *CCNA Training Guide*. Indianapolis: New Riders, 1999.

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