CHAPTER

2

LANs, MANs, and WANs

This is my LAN; that is your LAN; we are joined at the MAN, but I am also connected to a WAN . . . from sea to shining sea.

— The authors

Digital data communications has changed rapidly and continues to evolve due to the demand of many types of ''data consumers.'' High-speed data communications is no longer the preferred network of only large companies; everyday consumers use these networks for various forms of communication — voice, text, video, and teleconferencing. The past decade has seen a convergence of a wide range of services utilizing the public network simply referred to as the Internet.

The term *Internet* covers a wide range of network devices and services offered by a wide range of companies commonly referred to as the *telecommunications industry*. This chapter discusses local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs). The topics will be discussed in this order, but it is not meant to imply that this was the evolutionary process in networking technology. In reality, it is perhaps more like WANs, LANs, and then MANs. However, there have been areas of overlap where the evolution of all three occurred simultaneously.

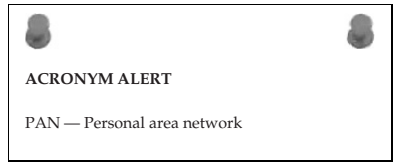
The quote above is trying to give a sense of the relationship between LAN, MAN, and WAN. Some LAN networks are a personal thing, like my LAN at home. It is mine, all mine, and not to be shared with others.[1] Strategically speaking, a LAN is owned by a person or small group, but it is fairly local

[1]Rich gets a little over-possessive at times. He is a giving soul and does go out of his way to share with others, but his LAN is his LAN.

geographically no matter how many network nodes it may have. MANs may comprise many LAN networks spread about a geographical region whereas WANs can be global. However, the purpose of the MAN or WAN is so that users on LANs, no matter where they may be located geographically, can communicate with each other in the sharing of data and network resources.

2.1 Local Area Networks

A LAN may consist of computers, printers, storage devices, and other shared devices or services available to a group of users within a ''local'' geographical area. These devices are interconnected either via copper wire, optical wire (fiber), or wireless media. Information passing over the LAN is controlled by a set of network protocols that allows for the orderly sharing of data between applications and devices, even though these may come from many different companies and manufacturers.



2.1.1 LAN Standards

As discussed in Chapter 1, the IEEE recognized that standards had to be developed in order for LAN devices from differing manufacturers to be able to communicate with one another. The IEEE 802 Overview and Architecture standard heading described how these devices are to be interconnected on both LANs and MANs.

For the purposes of this chapter, the standards that will be primarily discussed as far as LAN networks go are:

- 802.2 Logical Link Control
- 802.3 CSMA/CD Access Method and Physical Layer Specifications
- 802.5 Token Ring Access Method and Physical Layer Specifications

2.1.1.1 802.2 Logical Link Control

The lower two layers of the Open Systems Interconnection (OSI) reference model, Data Link and Physical, are addressed within the IEEE 802.2 standard. It further divides the Data Link layer into two sublayers, Logical Link Control (LLC) and Media Access Control (MAC). This allows for ease in mapping between different LAN Physical layers throughout the 802 family of LAN/MAN standards.

The 802.2 implementation uses a strategy of having the LLC sublayer as a common interface between the upper layers and the Physical layer no matter what type of media is being used in the construction of the LAN. Figure 2-1 shows the LLC structure.

RANDOM BONUS DEFINITION

hop count — A measure of the number of routers that a packet has passed through.

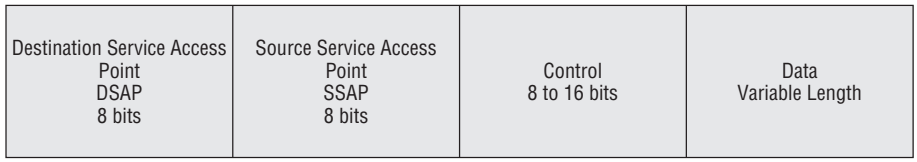


Figure 2-1 The IEEE 802.2 LLC structure

- **Destination service access point** — The type of service that is to receive the packet based on assigned SAP numbers, which are independent from the type of network being used.
- **Source service access point** — The type of service sending the packet based on assigned SAP numbers, which are independent from the network type being used.
- **Control** — Used for flow control and contains the send and receive sequence numbers ensuring packets are being received in the proper sequence.
- **Data** — A variable length field containing the information being carried within the packet.

The Media Access Control sublayer provides addressing and channel control. The MAC address, considered the physical address of the device, is a unique value that allows multiple devices to share the same LAN no matter what the physical medium being used for its implementation. Examples of shared medium networks are those utilizing bus, ring, or wireless topologies. Figure 2-2 illustrates the format of the 48-bit MAC address.

As illustrated, the address is split into two sections. The most significant three octets make up the portion of the address that is referred to as the *organizationally unique identifier* (OUI). These identify the organization that issued the identifier. The NIC specific portion of the address assigned and the serialization of the assigned numbers are under the control of the organization that owns the assigned OUI. With 24 bits of address, an organization can assign 16,777,216 unique addresses to devices they have manufactured. Assigned OUI addresses are maintained by the IEEE and can be found at `http://standards.ieee.org/regauth/oui/oui.txt`.

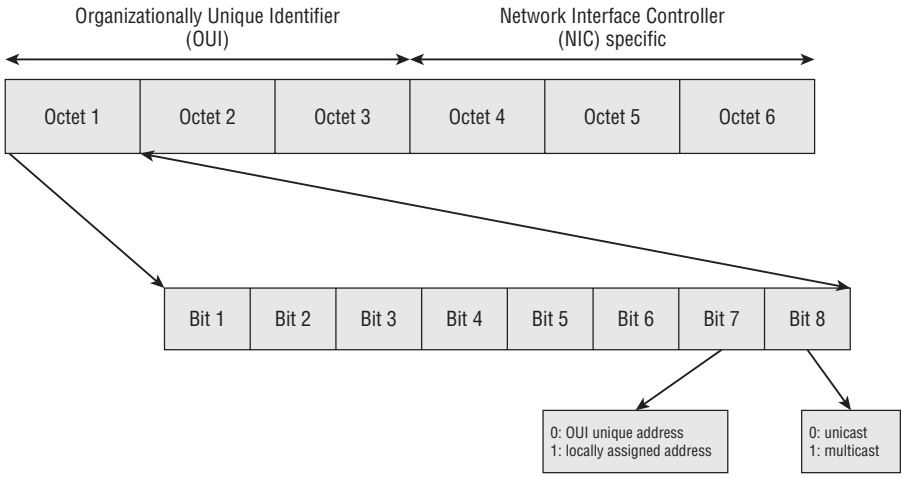


Figure 2-2 The IEEE 802 MAC address format

Bit B8 determines if the packet is either a unicast addressed packet, meaning it is directed to a single network node address, or broadcast, which is directed to all network nodes within a subnet.

MAC addresses are usually written with either hyphens or colons separating the hexadecimal numbers representing each of the octets. A MAC address annotated with the use of hyphens would look like 00-04-54-AA-B1-C2. If using colons, it would be presented as 00:04:54:AA:B1:C2.

POP QUIZ

What are the two sublayers of the Data Link layer?

There is provision for network administrators to locally assign MAC addresses to network interface controllers. If the NIC has been manufactured to allow modification of the factory-assigned MAC address, the administrator can set the bit to indicate that the MAC address has been locally assigned. The NIC portion of the address can be a number for the interface that is of administrator's choosing. Locally assigned addresses do not contain values representative of assigned OUI values. An example of a typical locally assigned MAC address would be:

```
02-00-00-01-00--F4
```

2.1.1.2 802.3 CSMA/CD Access Method and Physical Layer

The IEEE 802.3 standard contains a group of standards that addresses the unique characteristics of the network Physical layer being used on the network.

These standards were evolutionary and were issued as new types of media with differing characteristics were developed.

This standard defined the MAC structure for CSMA/CD,[2] as shown in Figure 2-3.

Figure 2-3 The CSMA/CD MAC structure

RANDOM BONUS DEFINITION

multicast address — A method of identifying a set of one or more stations as the destination for transmitted data.

When first introduced, IEEE 802.3 dealt with the use of data networking on a bus type network architecture using thick coax cable. This coax cable carried the designation of 10BASE5 and was more commonly referred to as *thicknet*. This type of cabling was rigid and difficult to work with. It required a transceiver that would tap[3] the cable to form a node on the network. A cable constructed with a 15-pin D style connector was needed to connect the transceiver to the device residing on a node of the network.

To circumvent the difficulties with 10BASE5 cabling, a new standard was developed, IEEE 802.3a, which still is bus network architecture but utilized thin coax, commonly referred to as *thinnet*.[4] The cable used was referred to as *10BASE2*, with RG-58 coax cable being the popular choice. RG-58 cable being thinner offered more flexibility over the RG-8 cable that was used in a 10BASE5 network. The network was formed by using lengths of RG-58 cable terminated with a BNC connector on each end. A BNC T connector formed the network node at the back of each workstation. The network was terminated on each end with a 50 ohm terminator. Figure 2-4 illustrates a simple 10BASE2 network with three workstations connected to the network using a BNC T connector to connect to the network interface card.

[2]Carrier Sense Multiple Access with Collision Detection is necessary in a bus architecture where any workstation may transmit randomly at any given time. The bus segment these workstations reside on is sometimes referred to as a *collision domain*.

[3]This type of tap was also referred to as a vampire tap since it had a pointed probe that pierced the protective layer of the cable insulation to strike the ''vein'' at its core, which was the center copper conductor. The bits would be allowed to flow like the life's blood of the network was being sucked out. OK, getting a little too dramatic with the class B horror movie genre references.

[4]Thinnet was also referred to as cheapernet since the cost factor was a mere fraction of the cost of 10BASE5 cabling, being more readily available at many electrical supply houses. There really is something to that supply and demand theory that I learned in my economics classes.

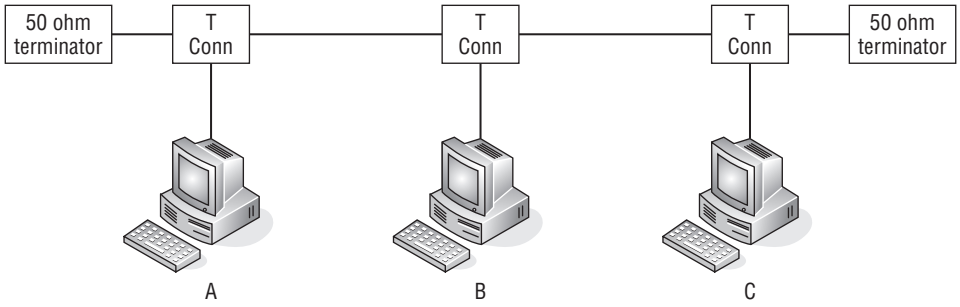


Figure 2-4 A simple 10BASE2 network

The BNC T connector on workstation B has a coax cable connected to it going to workstation A and another going to workstation C. Workstations A and C, having only one cable connected to their BNC T connector and being at each end of the network, require that the open connection on each BNC T connector be terminated with a 50 ohm BNC terminator. Although this is an improvement over 10BASE5 cabling, the one drawback is that workstations not on the end of the network required two cables to be terminated at the workstation's BNC T connector.

POP QUIZ

MAC addresses are represented with hexadecimal numbers, separated by a colon or a _____ .

Bus-based network architectures have inherent problems with cabling that don't exist in star-based networks. The development of IEEE 802.3i (a bus network that allows for wiring to have the appearance that it is physically a star-based topology while maintaining the CSMA/CD bus network architecture) provided for network cabling that uses unshielded twisted pair (UTP) and is commonly referred to as 10BASE-T. This allows for the use of Category 5 cable, which contained four twisted pairs contained within an unshielded jacket. Each end of the cable is terminated with an RJ-45 plug for short lengths of cable. Larger installations may terminate at wall jacks for workstation areas and to a patch panel at a central location. Since these appear to be spokes out to the workstations, the central location would require a device to concentrate these network nodes on a CSMA/CD network. The devices that accomplish this are appropriately called *hubs*. Figure 2-5 shows a hub and workstations in a CSMA/CD network.

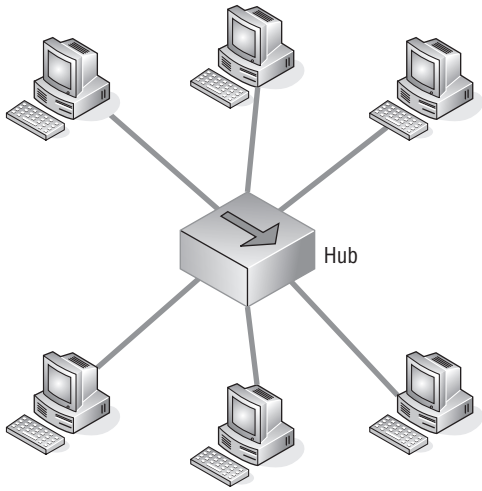


Figure 2-5 A CSMA/CD network using UTP cabling and a hub

Each workstation can be located at varying lengths from the hub. The maximum length of cable between a workstation and a hub is 100 meters.[5] This topology allows for the easy reconfiguration of the workstation. If a workstation is removed, there are no special considerations as there are with a 10BASE2 network topology.

The maximum transmission speed of the IEEE 802.3 networks discussed in this section is 10 Mbps. Subsequent standards have been added to the IEEE 802.3 standard that provide for 100 Mbps Fast Ethernet and 1Gbits/s over twisted pair wire.

RANDOM BONUS DEFINITION

nibble — A 4-bit unit of data (half of a byte).

A QUICK REMEDIAL LESSON

***Mega* represents a million of something. In decimal number notation, it is 1,000,000. This number can be represented in shorthand notation as 1M.**

(continued)

[5]Meters are a metric measurement of distance. A quick calculation would be there are roughly 3 feet to the meter. Therefore, 100 meters is about 300 feet. But to be more precise, it's 328.08 feet.

A QUICK REMEDIAL LESSON *(continued)*

Giga **represents a billion of something. In decimal number notation, it is 1,000,000,000. This number can be represented in shorthand notation as 1G.**

Now, we have millions and billions of bits, but what exactly is a bit, you ask? It is a single binary number represented by a 1 or a 0. Even if the value is 0, it still requires a signal on the wire, so this is one place where exactly zero does truly represent something.

Ten million bits per second (10 Mbps) is 10 million binary numbers having a value of either 0 or 1 being sent over some medium in a one-second interval. With giga rapidly becoming the new standard in Ethernet transmission speed, which is the equivalent of a billion bits per second (bps) hitting the wire, data that is normally referenced in bytes containing 8 bits of data would equate to 125 MBps (125,000,00 bytes per second) as the maximum number of bytes that can be sent within a second. Note that lowercase "b" signifies bits and that uppercase "B" signifies bytes in the notation used to reference these quantities. Make sure you keep your bits and bytes straight because you can be off by a factor of 8 in your calculations — usually not a problem when you overestimate but you can really feel some heat if you underestimate a network's throughput capability.

2.1.1.3 802.5 Token Ring Access Method and Physical Layer

The IEEE 802.5 standard defines a Token Ring protocol that is much different from that of a CSMA/CD protocol. With CSMA/CD, multiple workstations can transmit onto the wire at the same time, potentially causing collisions. When a collision occurs, they remedy the situation by backing off and retransmitting. With Token Ring, only one workstation is permitted to transmit onto the wire, that being the workstation currently in possession of the token.

Transmission onto the wire is sequential in a fixed pattern. After a workstation possessing the token has completed its transmission onto the wire, it passes the token to the next workstation. This is an advantage over CSMA/CD when the network has fewer workstations. As the number of workstations increases, the advantage is lost and the chattier CSMA/CD finally wins out.

POP QUIZ

What is the maximum length of a cable between a workstation and a hub?

When Token Ring was first introduced by IBM, it possessed a speed of 4 Mbps, thus not offering any advantage over CSMA/CD networks. With the introduction of 16 Mbps Token Ring, it was a toss-up between it and CSMA/CD

networks far as performance when the total number of workstations is lower. Figure 2-6 illustrates the IEEE 802.5 frame structure.

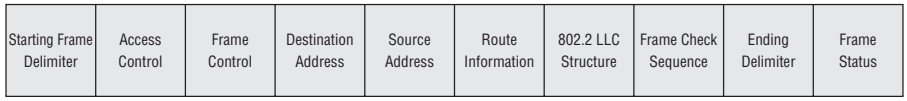


Figure 2-6 The IEEE 802.5 Token Ring frame structure

There are two minor differences between the IBM and IEEE 802.5 standards for Token Ring:

- The number of nodes on a ring is up to 260 nodes per IBM specification, and the IEEE 802.5 standard limits it to a maximum of 250 nodes.
- IBM allows up to 8 fields for route designation when source routing is employed, whereas the IEEE 802.5 standard allows for a maximum of 14 fields.

The frame format for IBM/IEEE 802.5 is as follows:

- The **Starting Frame Delimiter** and **Ending Delimiter** fields are each a single byte with deliberate breaches in certain positions of the Manchester Code[6] so that the start or end of a frame can never be recognized from any other portion of data on the wire.
- **Access Control** is a single-byte field serving to signal control and maintenance functions. The fourth bit position in this field is the token bit. If it is set to 1, this frame is a token and only consists of the Starting Frame Delimiter, Access Control, and Ending Delimiter. A token frame is only 3 bytes long.
- **Frame Control** is a single-byte field that indicates if the frame is control information or data.
- The **Destination Address** field contains either 2 or 6 bytes of addressing information, depending on whether the frame is addressed to a single node or a group of nodes.
- The **Source Address** field contains either 2 or 6 bytes of addressing information that indicates the address of the sending node.
- The **Route Information** field is present only when source routing has been enabled. It defines routing control, a route descriptor, and type of routing information contained within the packet.

[6]The Manchester Code is Phase Encoding used within telecommunications where each data bit has a minimum of one voltage transition within a fixed time slot, making it self clocking since the clocking signal can be extracted directly from the encoded data stream.

With source routing enabled there is a minimum of two fields that will be present. The 2-byte route designator field defines a ring number and the bridge number that the frame is to pass through. The last route designator will contain the ring number of the receiving node and a bridge number that is set to zero.

- **802.2 LLC Information Structure** is a variable-length field that, surprise, contains 802.2 LLC information.
- **Frame Check Sequence** is a 4-byte field containing the checksum information verifying the integrity of the frame starting from the Frame Control field through the 802.2 LLC/Data field.
- **Ending Delimiter** is an 8-bit field that indicates the end of the frame.
- **Frame Status** is a 1-byte field indicating that the intended recipient has received the frame.

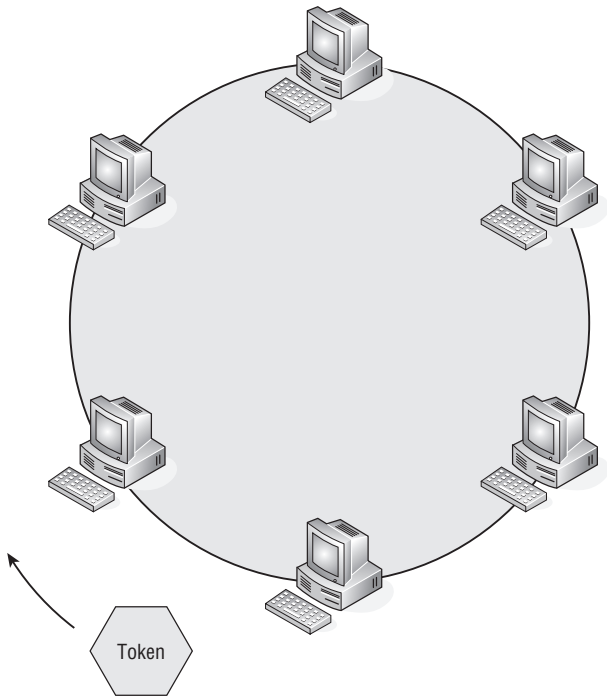


Figure 2-7 The token-passing sequence

Figure 2-7 is a logical visualization of a Token Ring network. The token is a frame type that is transmitted sequentially around the ring network. When a workstation needs to transmit on the ring, it keeps the token and modifies it with address and data information, and then transmits it onto the ring. The receiving station the data frame was intended for accepts the frame and sets a

flag in the frame to acknowledge proper receipt of the frame. The receiving station then retransmits the frame with the flag set back onto the ring network. On receipt of the frame with the flag set, the transmitting workstation transmits a new token frame onto the ring network and forwards it, allowing any of the following sequential workstations an opportunity to transmit onto the network.

In a Token Ring network, one of the workstations becomes the active ring monitor. Any workstation can be an active monitor, but only one workstation at a time. It is the role of the active monitor to detect data frames that have traveled around the ring more than once. Once a frame that traveled around the ring more than once is detected, the active monitor will remove the frame from the network and discard it. If the active monitor determines that a token frame is missing from the ring network, it purges the ring network of any frames and then transmits a new token onto the ring network. The active monitor workstation is responsible for the timing and clocking on the ring network. All workstations on the ring network use the timing from the active monitor to ensure that the same timing is being used to receive and send data.

A workstation becomes an active monitor by an election process when the absence of a ring monitor is detected. Upon detection of this message, a workstation transmits a claim token onto the ring network. Any subsequent workstation with a higher address that wishes to participate as the active monitor initiates a new claim token and transmits it onto the ring network. Through this election process the workstation with the highest address and participating in the claim token process is elected as the active monitor.

Although Token Ring is a logical ring, its topology appears as a star-based network. This is accomplished by cabling and connectors designed by IBM. The cabling consists of IBM type 1 shielded twisted pair (STP) cable and a unique connector design which is bulky, giving it a distinct space disadvantage compared to other cable connectors. To complete the ring, these connectors are plugged into a media access unit (MAU), as illustrated in Figure 2-8.

The cable is constructed with a receive pair and a transmit pair. When the Token Ring connector is inserted into the MAU,[7] the receive pair is connected to the transmit pair of the preceding workstation. The transmit pair is connected to the receive pair of the following workstation, and the MAU completes the ring. Multiple MAU units can be combined to form a larger single ring network, as needed.

2.1.1.4 The Collision Domain Battle

Both IEEE 802.3 and Ethernet are CSMA/CD network standards; however, the two are not fully compatible with each other. Although both 802.3 and

[7]MAU (media access unit) allows multiple units connected in a star topology to form a logical Token Ring. These devices are sometimes referred to as a ''ring in a box.''

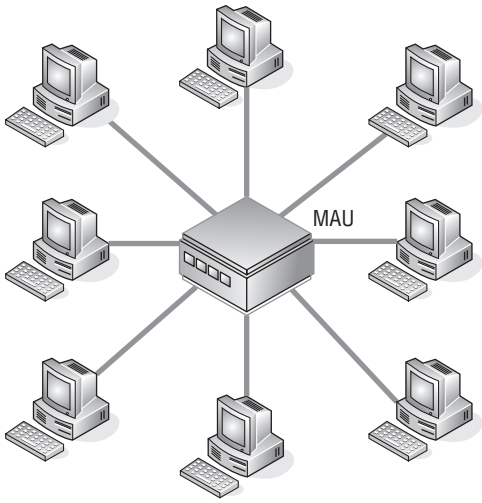


Figure 2-8 A Token Ring network using MAUs

Ethernet devices can coexist within the same LAN network, there are important differences. The major difference between IEEE 802.3 and Ethernet is the frame format. For them to coexist in the same LAN, the network software must be able to differentiate between the different frame types.

Figure 2-9 illustrates the IEEE 802.3 frame.

7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	1 Byte	1 Byte	1 or 2 Bytes	Variable Length	4 Bytes
Preamble	Start Frame Delimiter	Destination Address	Source Address	Length	Destination Service Access Point	Source Service Access Point	Control	Information (Data and Padding)	Frame Check Sequence

Figure 2-9 The 802.3 frame structure

The IEEE 802.3 frame contains the following fields:

- **Preamble** — A 7-byte binary pattern used to establish frame synchronization.
- **Start Frame Delimiter** — A single byte used to denote the start of a frame.
- **Destination Address** — The address the frame is being sent to. Although the standard allows this field to be anywhere between 2 to 6 bytes in length, the implementation in common use consists of 6 bytes.
- **Source Address** — This field contains the address of the device sending the frame. The standard allows this to be anywhere between 2 to 6 bytes in length, but most implementations use 6 bytes in defining this field.

- **Length** — A 2-byte field used to denote the size of the IEEE 802.2 structure, including header and data.
- **Destination Service Access Point** — A 1-byte field that indicates which network protocol the receiving device should use in interpreting the frame.
- **Source Service Access Point** — A 1-byte field indicating which network protocol was used to create the frame. Normally this field contains the same information as the Destination Service Access Point.
- **Control** — This field may be either 2 or 6 bytes long, where the length of the field is indicated by the first 2 bits of the field. It is used for indicating various commands such as exchange identification, test, connect, disconnect or frame rejection.
- An information field containing data and any number of required padding bytes.
  - **Data** — A variable length field that contains the actual information that is being transmitted within the frame.
  - **Pad Bytes** — An optional field that contains no information but is added to ensure that the frame meets the minimum length requirement.
- **Frame Check Sequence** — A 4-byte field that contains the checksum of the fields starting with the Destination Address through the Data field.

Figure 2-10 illustrates the Ethernet frame.

7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	Variable Length	4 Bytes
Preamble	Start Frame Delimiter	Destination Address	Source Address	Type	Information (Data and Padding)	Frame Check Sequence

Figure 2-10 The Ethernet frame

The Ethernet Frame contains the following fields:

- **Preamble** — A 7-byte binary pattern used to establish frame synchronization.
- **Start Frame Delimiter** — A single byte used to denote the start of a frame.
- **Destination Address** — The address the frame is being sent to. Although the standard allows this field to be anywhere between 2 to 6 bytes in length, the implementation in common use consists of 6 bytes.

- **Source Address** — This field contains the address of the device sending the frame. The standard allows this to be anywhere between 2 to 6 bytes in length, but most implementations use 6 bytes in defining this field.
- **Type** — This is a 2-byte field that indicates the network protocol or the protocol service contained within the frame.
- **Information** — This is a variable length field that contains the actual data being carried by the frame and any number of bytes of padding to ensure the minimum frame size.
- **Frame Check Sequence** — A 4-byte field that contains the checksum of the fields starting with the Destination Address through the Data field.

The key difference between the IEEE 802.3 frame and the Ethernet frame is Ethernet's Type field. The IEEE 802.3 frame uses the IEEE 802.2 Source Service Access Point and Destination Service Access Point fields to indicate which network the frame is coming from and which network it is going to.

A list of registered Ethernet types can be found at `http://standards.ieee.org/regauth/ethertype/eth.txt`.

2.1.1.5 The Most Common Wireless Standards

As covered in Chapter 1, the IEEE 802.11 is a group of standards defining the operation of network communications using radio frequencies. These standards are loosely interchanged with the term Wi-Fi, but do have some differences with the standards of the Wi-Fi Alliance. With the proliferation of wireless network products into the marketplace, the Wi-Fi Alliance is in the process of certifying these products before amendments to the 802.11 are completed. Today's wireless products are being sold under the following standards:

- **802.11** — This is the legacy base standard for wireless networking
- **802.11a** — This standard's advantage is the use of the less crowded 5 GHz band, but its chief disadvantage is that its signals are more easily absorbed and dampen the signal quality as the signal travels through solid objects along its path.
- **802.11b** — Introduced in 1999, this standard uses the 2.4 GHz broadcast band providing a typical data rate of 4.5 Mbps with a maximum data rate of 11 Mbps. Its major disadvantage is that it can receive interference from other devices that also share the 2.4 GHz frequency band such as microwaves, cordless telephones, and a wide variety of Bluetooth

devices. The substantial increase of data rate throughput and the reduction of product cost have led to the rapid acceptance of this standard as the definitive standard for wireless LAN networks.

- **802.11g** — Consumer demand for higher data rate products led to the introduction of products that supported the older IEEE 802.11a and b standards as well as this standard, which made these products capable of supporting all three standards within a single device. However, an 802.11g standard wireless LAN network can reduce the overall speed of the network if one device participating in the wireless network is only capable of supporting the IEEE 802.11b standard. As with 802.11b, this standard also falls prey to the same interference from other devices sharing the same frequency band.
- **802.11-2007** — This is a standard that was released to be all-inclusive of the amendments to 802.11 since its introduction. To date this is the most conclusive standard document that defines wireless LAN network operation.
- **802.11n** — With a proposed release date of 2009, this is an amendment that will add additional features to the 802.11 standard and will include multiple input/multiple output (MIMO) technology. MIMO will use multiple antennas for both transmission and receiving, which would offer significant increases in range and data rate throughput without the need for increased bandwidth of transmission power. Although it is still in draft, many vendors are beginning to sell products labeled under the 802.11n standard. To avoid any interoperability problems between differing vendors, it is recommended to purchase routers and access points from the same manufacturer.

The standards listed above are not all-inclusive of the IEEE 802.11 standard. They are the most commonly known and discussed standards when there is a discussion on wireless LAN networks. Additional information can be found at the IEEE 802.11 group's website at `http://ieee802.org/11/`.

2.1.2 LAN Topologies

Chapter 1 presented a variety of network topologies. In this chapter, we will attempt to provide further information concerning the implementation and use of these topologies in the creation of a LAN.

Figure 2-11 illustrates a very basic network map. The purpose is to demonstrate that even a simple network can and probably will use a variety of media, protocols, and network devices. The media shown on this network topology is a combination of wired systems, which include both ring and bus network topologies, along with a network segment that is connected using wireless network technology. Users are connected to the network either hard-wired to a bus or ring LAN segment or through a wireless LAN access point.

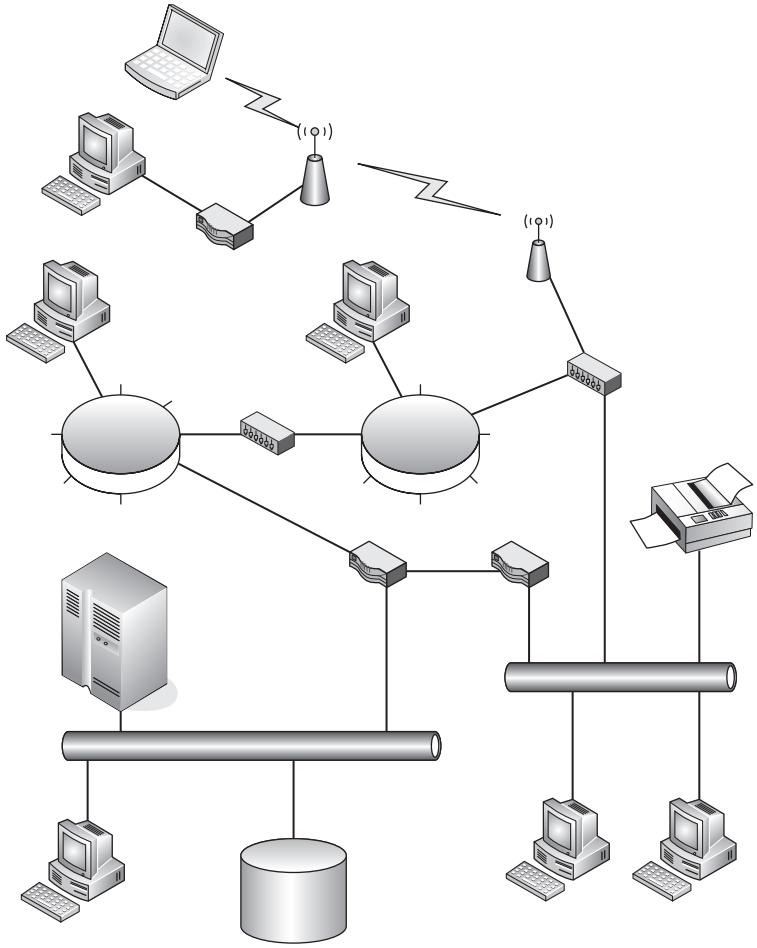


Figure 2-11 A sample LAN's topological map

The network allows for the access of users to network resources such as mainframe computers, network storage devices, network printers, and other shared resources connected to the network. The LAN segment illustrated in this figure has no access to the outside world via the Internet and is self-contained. Most of today's LAN networks ultimately do connect to the Internet and will be discussed further in the ''Metropolitan Area Networks'' and ''Wide Area Networks'' sections of this chapter. So the focus of this section is solely on the LAN. This is the section that deals with ''this is my LAN and that is your LAN'' area of networking.

A LAN can contain a single network segment of any media type, or it may be a collection of two or more of the network media currently in use today. So, if a LAN is a combination of different media types, how do they interconnect? This is where devices called gateways, bridges, and routers come into play. They

are depicted in Figure 2-11 as boxes between LAN segments. How you plan to implement your network and the networking address schemes that are to be used will determine which type of these devices would need to be used for these network nodes. These devices will be covered in depth in Chapter 3, ''Network Hardware and Transmission Media.'' For the purpose of this chapter, it will be generally accepted that these devices do allow for communications between LAN segments with different media and network protocols.

2.1.2.1 Token Ring Network Topologies

Wired Token Ring networks are still around, but the number of new installations is declining as more new network installations opt toward wired bus network implementations. The need to discuss the wired Token Ring network architecture is due to the fact that there are a number of these networks still deployed in the field today even though they are considered legacy[8] networks.

The original design of a Token Ring network was literally a ring where each node of the network was daisy-chained to the next node until the network came back around to the first node in the ring. There was a ring-in (RI) port and a ring-out (RO) port, with the RO of one station connecting to the RI of the next upstream station on the ring. This would continue until all the network nodes had been connected. The major disadvantage of this network design was that the disruption or disconnection of any one node on the ring brought the whole network down. Newer Token Ring networks were designed using hubs or media access units (MAUs), which allowed for ease in cabling while maintaining the logical ring of the Token Ring network architecture. Figure 2-12 illustrates the construction of a Token Ring network with two nodes with the use of a two-port MAU.

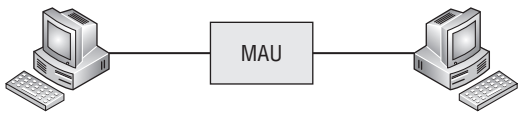


Figure 2-12 A simple Token Ring network

Obviously, a network of this construction has a limited use. To overcome this limitation, an eight-port MAU was designed with the ability to extend the Token Ring by daisy-chaining multiple eight-port MAU units together using the RI and RO ports on the eight-port MAU. Figure 2-13 illustrates this more complex Token Ring network.

[8] A legacy network is one that is installed and operational although its technology has been superseded by other network technologies. Networks in large organizations are mostly evolutionary. It is not uncommon to find some networks still operational although they are no longer sold and supported by the original manufacturer. A lot of companies work on the ''if it ain't broke, don't fix it'' mentality when it comes to their internal LAN networks.

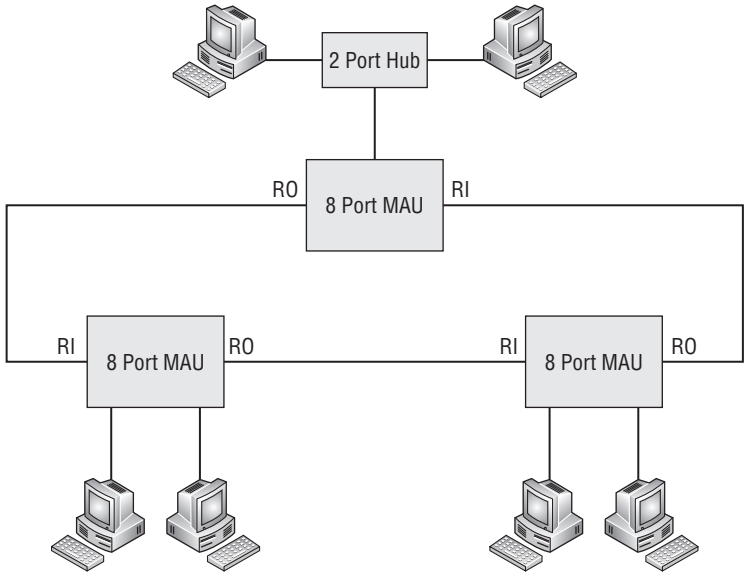


Figure 2-13 A typical Token Ring network

Up to a maximum of 33 MAU units can be interconnected to form the ring network. The distance between MAU units is determined by the cable used to interconnect them. With the use of Type 1 cable, MAU units can be placed up to a maximum of 100 meters apart. If greater distances are needed, a repeater is required. Repeaters used for copper wire network segments can increase this distance up to 740 meters. If even greater distances are required, the network segment can be further extended up to four kilometers with the use of a fiber optic repeater and fiber optic cable.

ACRONYM ALERT

UDP — User Datagram Protocol

Workstations and hubs connected to the MAU by cable are referred to as lobes. Normally a lobe connects a workstation to a MAU, but if multiple workstations in the same area need to be connected to the ring network, this is accomplished with the use of a lobe access unit (LAU). A LAU unit splits the lobe into two or more lobes. A LAU can be placed at the end of a cable to allow for the connection of multiple workstations in that area. Although LAU units sound as if they are the same as MAU units, there is a major difference. Unlike a MAU, a LAU cannot be used to create a standalone ring. So LAU units are basically used as hubs.

Although the difference between LAU and MAU units has become obscured because some manufacturers market products called LAU units, in reality they are functionally MAU units. However, the primary use of both MAU and

LAU units is in maintaining the functioning of the ring network as devices are disconnected from the network.

A MAU or LAU allows a lobe on the ring to be opened for the insertion of a new workstation, and it closes the ring when a workstation is removed from the network. This allows for flexibility of network construction and any necessary network reconfiguration without the problem of interruption of ring network function.

2.1.2.1.1 Token Ring Cabling

The physical layout of a Token Ring network depends not only on the placement of MAU, LAU, and hub units, but also on the cabling being used in its construction. It has been previously mentioned that the cable construction can be either STP or UTP cable.

2.1.2.1.1.1 Shielded Twisted Pair Cable STP Token Ring cable, also known as *IBM Type 1 cable*, is constructed with twisted pair wires that are shielded. The use of this cable allows for Token Ring lobe connections to be a maximum of 100 meters apart. STP cables are terminated with either DB9 connectors or patch connectors. Generally, patch connectors are used to connect to MAU units, whereas DB9 male connectors are used to connect to workstations or LAU units. DB9 female connectors are used to daisy-chain one LAU unit to another.

The signals carried by the cable are transmit and receive. Two shielded pairs are needed for these differential[9] signals. Table 2-1 lists the DB9 pin assignments.

Table 2-1 DB9 Pin Assignments

SIGNAL	PIN
Receive +	1
Receive −	6
Transmit +	9
Transmit −	5

2.1.2.1.1.2 Unshielded Twisted Pair Cable UTP Token Ring cable, also known as *IBM Type 3 cable*, is constructed with unshielded twisted pair wire similar to telephone cable. These cables are terminated with RJ-45 modular

[9]Differential Manchester encoding is used for the transmission and reception of data in the use of either STP or UTP Token Ring cabling. The balanced signals for both the send and receive data signals allow for data integrity and greater noise immunity.

plugs. This style of Token Ring cabling is dependent on the operating environment the network segment is in and the speed of the LAN itself. This cabling is used to form lobe segments that do not exceed 45 meters. Typically these cables[10] are constructed using 10BASE-T UTP cable terminated on each end with RJ-45 plugs. The RJ-45 pin assignments are listed in Table 2-2.

Table 2-2 RJ-45 Pin Assignments

SIGNAL	PIN	WIRE COLOR
Receive +	4	White with orange stripe
Receive −	5	Orange with white stripe
Transmit +	6	White with blue stripe
Transmit −	3	Blue with white stripe

2.1.2.1.1.3 Other Variations of Token Ring Cabling For special environments or applications, IBM also uses cabling that consists of Type 2, Type 5, Type 6, Type 8, and Type 9 cables.

- **Type 2** — Consists of two STPs as can be found in Type 1 cable and four UTPs as can be found in Type 3 cable.
- **Type 5** — Consists of multimode fiber optic cable used to extend the Token Ring network and to interconnect optical repeaters.
- **Type 6** — Consists of two STPs. It is considered a low cost, short distance cable with a maximum length of 45 meters and is often used for MAU-to-MAU connection.
- **Type 8** — Consists of two parallel pairs. The wires in this cable are untwisted and have a maximum length of 50 meters. The primary purpose of this wire is in installations requiring the cable to run under carpeting.
- **Type 9** — A lower cost alternative to Type 1 cable with a maximum length of 65 meters. It consists of two pairs of STPs.

2.1.2.1.2 High-Speed Token Ring

There have been efforts made to push the speed of Token Ring networks beyond the standard 16 Mbps. High-speed Token Ring has not been fully deployed with the decline in newer Token Ring installations. However, it is

[10] Although these cables appear to be similar to those used for Ethernet 10BASE-T patch cables, they are not the same. Ethernet 10BASE-T cables are constructed to use pins 1 and 2, and 3 and 6, for their twisted pair combinations.

worth mentioning since there is a high likelihood of it being encountered in the remaining legacy Token Ring networks.

- **32 Mbps Token Ring** — Both IBM and other vendors of Token Ring components and devices attempted to push Token Ring operation to a higher speed.
- **Token Ring switches** — These are in the form of switching bridges capable of speeding up how messages travel between network rings.
- **Fiber distributed data interface (FDDI)** — Although closely related to Token Ring, it is not officially considered as part of the Token Ring family. They both use a token-passing protocol.

2.1.2.2 Bus Networks Topologies

Bus networks initially were designed as a physical bus allowing devices to be connected to nodes along the bus. Figure 2-14 shows a typical bus network.

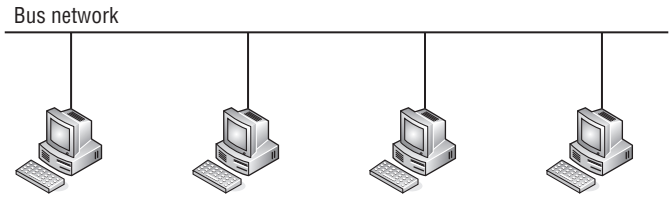


Figure 2-14 A typical bus network

In this illustration, workstations are connected to the bus with the use of transceivers. With 10BASE5 cabling being used to form the bus network, external transceivers were typically used to connect a workstation to the network. In later bus implementations using 10BASE2 cabling in the form of RG-58 coax cable to form the bus network, the transceiver was integrated into the network adapter card that was installed within the workstation.

The transceiver not only converted the digital data generated by the workstation into the appropriate data signals, it performed other functions useful to both 802.3 and Ethernet LAN networks.

- **Collision detection** — Provided by circuitry designed to detect collisions on the bus network. If a collision is detected, the transceiver notifies the transmitting function that a collision has occurred and then broadcasts a jamming signal on the network to notify other systems connected to the bus network. The LAN is then allowed to settle before the resumption of transmissions on to the bus.

- **Heartbeat** — Generation of a short signal to inform the main adapter that the transmission is successful and collision free. Although specified in the 802.3 standard and the Ethernet standard, it is rarely used because many adapters confuse this signal with the signal that signifies a collision has occurred.
- **Jabber** — The function that allows the transceiver to cease transmission if the frame being transmitted exceeds the specified limit of 1518 bytes. This helps prevent a malfunctioning system or adapter from flooding the LAN with inappropriate data.
- **Monitor** — This function monitors LAN traffic by prohibiting transmit functions while receive and collision functions are enabled. It does not generate any traffic onto the LAN.

A bus network created using 10BASE5 or thick coax cable can have a maximum overall segment length of 500 meters. Each node on the segment is created with the use of a transceiver. Nodes on a thick coax cable are to be spaced no closer than 2.5 meters with a maximum number of 100 nodes per segment. The impedance for thick coax is 50 ohms. With the use of repeaters, the overall length of the combined segments is not to exceed 2,500 meters.

Generally, bus networks that are formed by using 10BASE2 cabling use adapters that have the transceiver function built in. The network is formed using a BNC coax T connector connected to the workstation's BNC coax connector. Workstations are then daisy-chained together using lengths of coax cable terminated at both ends with coax plugs. These interconnecting cables should not be less than 0.5 meters in length with a maximum of 30 nodes and a total length of 185 meters per network segment. The BNC T connector on each end of the network segment requires a 50 ohm terminator to be attached to the open end of the T connector to maintain the cable impedance. This is essential to maintain signal integrity and the dampening of any signal reflections on the cable. With the use of repeaters, the overall length of the combined segments is not to exceed 925 meters.

RANDOM BONUS DEFINITION

twisted pair — A communications medium consisting of two copper conductors twisted together.

The maximum frame size for both IEEE 802.3 and Ethernet frames is 1518 bytes. 802.3 provides for a maximum data segment size of 1460 bytes while Ethernet allows for a maximum data size of 1500 bytes. The original speed for Ethernet was 10 Mbps.

There are two other implementations of logical bus networks: the star topology and the tree topology.

2.1.2.2.1 Star Network Topology

A star topology is implemented with the use of hubs and UTP cables terminated with RJ-45 plugs. Hubs maintain the logic of the bus network while the UTP cables radiate out in a star pattern. Figure 2-15 illustrates a star network formed with the use of a single hub and UTP cables that are no longer than 100 meters in length.

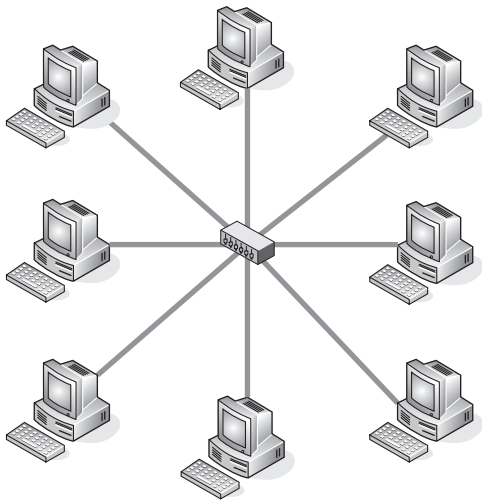


Figure 2-15 A star network

The simplicity of this type of network is the ease in which devices may be added or removed from the network. The only limiting factor for this type of network with a single hub is the number of ports contained on the hub. This type of network is only useful for a small self-contained work group with no requirement of connecting to other network segments located elsewhere.

2.1.2.2.2 Tree Network Topologies

Tree network topologies consist of network segments connected by hubs and other devices in various combinations to create the network. Network segments can either be geographically close or remote. Many networks fall into the tree network architecture. This is especially true for very large networks with many nodes. Figure 2-16 illustrates a simple logical diagram showing a series of user nodes.

This could be considered a top level drawing where the later drawings show more detail of how the segments are to be connected and the media that make up the network segments. Figure 2-17 illustrates what one of the network segments might look like. It is a combination of devices using both wired and wireless media to connect nodes within that network segment.

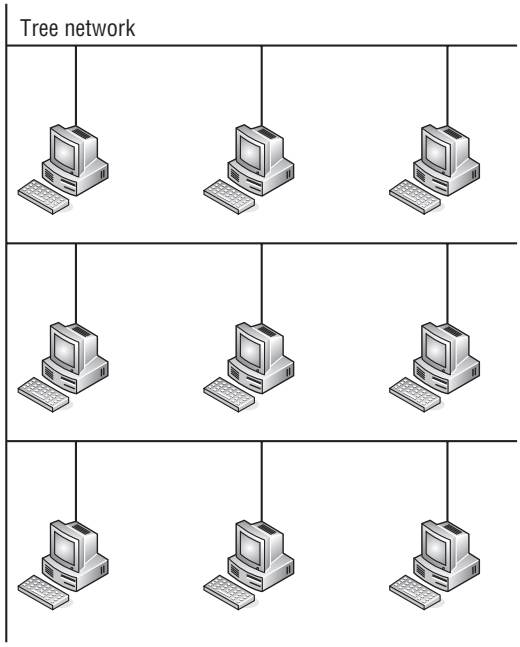


Figure 2-16 A logical drawing of tree network topology

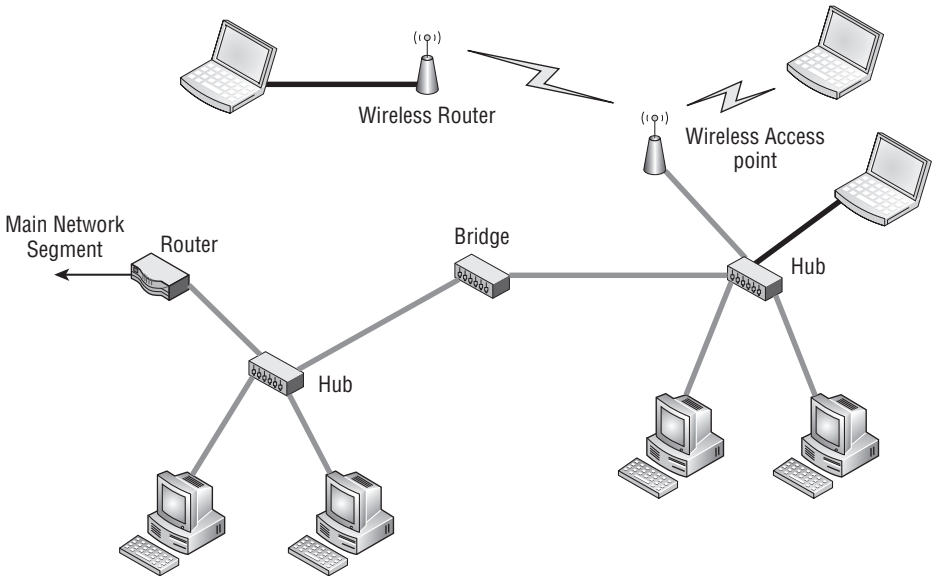


Figure 2-17 A tree topology network segment

Laptop users with wireless enabled laptops can communicate directly from their laptop to a wireless access point to gain access to the network. Laptops that are not wireless enabled can be directly connected to the wired network segment using the network interface card, which is internal to the laptop. Another option, if needed, is to connect the laptop to a wireless router that is able to communicate to the wireless access point to gain access to the network. Workstations on the network segment are connected to the network with the use of a hub. Separate local network segments are connected with the use of a bridge. This whole network segment is connected to other network segments with the use of a router.

2.1.2.2.3 Devices that Make Up a Network

True bus networks[11] can still be found, but they are considered legacy networks by today's standards. Most newly deployed networks, although they are bus networks, logically make use of devices to maintain the bus while nodes are placed in either a star or tree network topology or, in many cases, a combination of both. The majority of cabling used is 10BASE-T UTP cable connected to the bus network devices with the use of RJ-45 plugs.

The following devices may be found in a variety of network topologies:

- **Hubs** — Considered to be passive network devices.[12] Passive hubs allow the connection of multiple nodes to the network. They can be stand-alone or daisy-chained to other hubs to form a larger network segment.
- **Repeaters** — Used to extend network segments beyond the recommended distance over wire cabling by performing signal regeneration to ensure that data integrity is maintained over the long network segment.
- **Bridges** — Used to divide a network into smaller segments to reduce the number of network devices contending on the network segment for network access. The bridge only passes network traffic that is specifically intended for the other network segment that it is connected to.
- **Ethernet switches** — These are more predominately used today in LAN networks to perform the role of bridges in dividing a network into smaller segments to reduce network contention between network devices. A single Ethernet switch is capable of having multiple network segments contained within it. This is accomplished by programmable ports, which may be dedicated to virtual LAN (VLAN)

[11]The term *true bus network* refers to networks that are physically constructed as a bus. They consist of either thick or thin coax cable. These networks use 10BASE5 and 10BASE2 cabling to form the network segment.

[12]Passive network devices such as hubs are designed to maintain the electrical characteristics of a bus network while physically giving the appearance that they are interconnected in either a star or tree network topology.

segments on that device. They usually contain multiple ports and are similar in appearance to hubs but differ in that hubs are not able to reduce network contention on the network segment they are being used on. Some Ethernet switches provide the ability to gang multiple devices together to form a larger network segment.

- **Routers** — Used to connect multiple network segments but differ vastly from bridge devices. Bridges operate solely on the information contained within the 802.3 data frame and are not effected by the routing protocols being run over the network. Routers operate at the network protocol level and forward network traffic based upon the network protocol information contained within the data frame being forwarded from one network segment to another.
- **Network interface cards (NIC)** — A term used predominately to refer to the cards contained within devices connected to the network. However, the devices that fall under this category are wide and diverse, from cards meant to fit into a PC slot to other devices intended to connect via a USB port. Some NIC devices fit into a PCMCIA card slot on a laptop and allow it to gain network access via a wireless link. They all serve the same purpose: to allow a device to connect to a LAN.

The devices briefly described in this section are covered in further depth in Chapter 3.

2.1.2.2.4 Bus Network Cabling

This section discusses the following bus wire types: 10BASE5 coax (thicknet), 10BASE2 (thinnet), and 10BASE-T (UTP). The predominant wiring used in today's network is 10BASE-T, which is commonly referred to as *Ethernet cabling*. The characteristics and limitations of each cable type will be discussed in this section.

2.1.2.2.4.1 10BASE5 Thicknet This cable type was the initial introduction to CSMA/CD bus network topology. The network segment is formed using this thick coax cable, which has a maximum segment length of 500 meters. Being thick and heavy, the cable is difficult to handle when routing the cable throughout a building. A network node is formed with the use of what is commonly referred to as a *vampire tap*. This device pierces the jacket of the coax cable to make contact to the center conductor of the coax cable and provide the signal to the network node with the use of a transceiver. The physical construction of the transceiver appears the same for both Ethernet and IEEE 802.3, both using a DB15 connector style. However, where they differ is in the circuit assignment for each pin. Table 2-3 shows the DB15 pin assignments for both Ethernet and IEEE 802.3.

Table 2-3 DB15 Pin Assignments

PIN	ETHERNET	IEEE 802.3
1	Ground	Ground control in
2	Collision detected +	Control in A
3	Transmit +	Data out A
4	Ground	Data in
5	Receive +	Data in A
6	Voltage	Common
7	Control	Out A
8	Ground	Control out
9	Collision detected −	Control in B
10	Transmit −	Data out B
11	Ground	Data out
12	Receive −	Data in B
13	Power	
14	Power ground	
15	Control	Out B

The Ethernet transceiver specifies the pinout for three signals, transmit, receive, and collision detect, whereas the IEEE 802.3 standard provides for an added signal of control out (which is not used). Although the pin assignments are such that a cable manufactured for either standard would work with the other standard's transceiver, it is not recommended due to differences used in signal grounding.

Vampire taps may not be located any closer together than 2.5 meters with a maximum of 100 taps per network segment. Network segments can be combined with the use of repeaters to increase the overall combined network length to 2,500 meters. The characteristic impedance of 10BASE5 cable is 50 ohms.

2.1.2.2.4.2 10BASE2 Thinnet 10BASE2 networks are constructed mostly with the use of RG-58 coax cable, which has a characteristic impedance of 50 ohms. This cabling is more desirable for use in network segments due to its lower cost and greater flexibility than that of 10BASE5 cable. Network nodes are easily formed with lower cost BNC T connectors, whereas 10BASE5 cabling requires a more expensive vampire tap transceiver. However, 10BASE5 cable

is capable of far greater network segment length than 10BASE2, which makes it more suitable for a network backbone. The 10BASE2 network, with its lower cost and ease of reconfiguration if needed, is more suited for a work group environment clustered in a smaller geographical area. To properly terminate a 10BASE2 network to maintain the characteristic 50 ohm impedance across the network and reduce signal reflections on the wire, the last BNC T connector on each end of the network segment must have a 50 ohm BNC terminating plug connected to the open tap on that BNC T connector.

The overall segment length for a 10BASE2 cabled network is 185 meters with a maximum of 30 network nodes per segment. The minimum distance between network nodes is 0.5 meter. The overall network length that can be achieved with the use of repeaters for 10BASE2 is 925 meters.

2.1.2.2.4.3 10BASE-T UTP Cabling These days, 10BASE-T cable and Ethernet UTP cable are simply synonymously called *Ethernet cable*. Although logically it is considered as bus topology cable, it is point-to-point between a network node device and a device that completes the logical bus. Cable construction is similar to telephone cable, which makes it easily routable through a building. Similar to telephone cable in larger installation sites, patch panels are used to terminate cables from differing locations throughout the facility.

Ethernet cables of various lengths terminated with RJ-45 plugs on both ends are usually referred to as *patch cables* or *straight-through cables*. These cables are used to connect a network node device to a network device that completes the logical bus. Table 2-4 shows the pinout for an RJ-45 plug on an Ethernet cable.

Table 2-4 RJ-45 Pin Assignments

PIN	SIGNAL
1	Transmit +
2	Transmit −
3	Receive +
4	
5	
6	Receive −
7	
8	

It can be seen that a patch cable or straight-through cable carries the same signal from one end to the other on the same pin if both RJ-45 jacks are wired

exactly alike. However, there is another cable that appears physically identical but is wired differently, called a crossover cable. These cables do literally just that — they cross over the transmit signals to the receive signals. The purpose of these cables is to connect two network devices whose connectors are wired exactly the same. A simple example of this would be two computers connected by a crossover cable to use the network cable to transfer files between them.

Many of today's network devices such as hubs and switches use auto-sensing, auto-switching ports to sense the cable and dynamically configure the port to ensure that the transmit signal from another network device is connected to its receive signal input. This was not always the case, so in order to expand a network segment, crossover cables were necessary to daisy-chain multiple hubs together. Figure 2-18 illustrates how hubs can be daisy-chained to form a larger network segment.

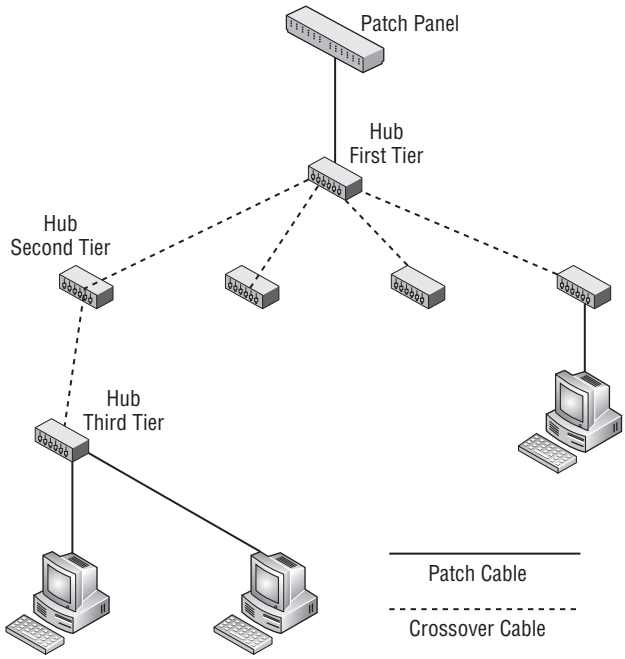


Figure 2-18 Daisy-chaining for an expanded network segment

In Figure 2-18, a local geographical area is serviced by a series of hubs to allow network devices in that location to gain access to the network. The feed for this network is from a patch panel over a patch cable to the first tier hub device. This device with the use of crossover cables is attached to a number of second tier hubs. In this illustration, one of the second tier hubs is connected using a crossover cable to a third tier hub, which services some computers attached to the network. This appears at first to be an unlimited geometric

progression, but in reality it is a bus network, so network devices do contend for network bandwidth. It can be readily seen that all devices on this network segment that send traffic to other network segments need to have it pass over the single cable between the patch panel and the first tier hub device. This is often referred to as a single point of access.[13]

Hub manufacturers saw the inconvenience of having two cable types and began to design and sell hubs with a mechanical switch on one of the ports so that a patch cable could be used between hubs in place of a crossover cable. More recent Ethernet port designs have led to the development of a port device using electronic auto-sensing, auto-switching to configure the port to match transmit and receive signals no matter if a patch or crossover cable is connected to the port.

Any segment of the network shown in Figure 2-18 may not have a cable linking two network devices that exceeds 100 meters. The overall combined length of the entire segment with the use of hubs and repeaters may not exceed 2,500 meters. For smaller local networks, these lengths are more than adequate. For much larger installations, special considerations will be required to ensure data integrity on the network.

2.1.2.2.4.4 So What about Speed and Duplex? The initial speed standard for CSMA/CD bus networks over UTP cable was 10 Mbps. Since the initial introduction, devices that can pass network traffic at 100 Mbps (100BASE-TX) are now fairly common. Many of today's installations make use of gigabit speeds (1000BASE-T), which sometimes is referred to as *gig-E*. These advances in technology have allowed for the attainment of greater network speeds without the need for changing the current wiring infrastructure. Devices capable of any of the speeds listed are able to do so over existing Category 5 cabling.

RANDOM BONUS DEFINITION

ping — A utility program used to test for network connectivity by using the echo request and echo response mechanisms of ICMP.

Duplex is either half-duplex or full-duplex. The difference between the two is that full-duplex devices are capable of transmitting and receiving at the same time, whereas half-duplex devices are either in transmit or receive mode but never both simultaneously.

Since UTP cabling is connected in a point-to-point fashion, the ports connected to each end of the cable must be able to transmit and receive at the same speed. On some devices, these are only manually configurable. Some devices

[13]Single point of access is also a single point of network failure. Depending on the number of devices in a local area or how critical network availability is to those users, some thought should be given to network segmentation and redundancy. There will be further discussions and examples of this throughout this book.

are able to negotiate speed and duplex with their peer port to set the speed and duplex to be used over the link.[14] This mode of operation is referred to as auto-negotiation.

Careful attention must be paid to the speed and duplex of an interface. If there is a mismatch between the devices, network performance will be degraded and full network speed cannot be realized. This is a small detail that's often overlooked but has major implications in overall network performance.

2.2 Metropolitan Area Networks

The term *metropolitan area network* is a bit nebulous and embraces a variety of differing network scenarios. The common denominator in all these networks is that they cover areas that are much larger than a conventional LAN is capable of, as discussed in Chapter 1.

The technological development of fiber optic network devices has facilitated the growth of both private and public MAN networks. Fiber optics allowed the network to stretch to over several kilometers, which made extended networks more feasible. Fiber distributed data interface (FDDI) is used for the backbone that interconnects distant portions of the MAN. So what exactly is an FDDI?

2.2.1 Fiber Distributed Data Interface

Fiber optic cabling presents several advantages over conventional copper wiring. It is lighter in weight than copper, weighing in at roughly 10 percent of a copper cable of the same length. It is capable of driving data signals much further with less loss and is immune to crosstalk and noise caused by electromagnetic interference (EMI). Fiber optic cable, being electrically inert, aids in the elimination of ground loops between sending and receiving nodes.

Since fiber optic cable does not emit any radio frequency interference (RFI) when data is transmitted on the cable, it cannot be snooped using radio frequency detectors as copper wire can. The only way data can be eavesdropped on is by actually breaking the cable and placing a receiver in the line. Since this action would not go undetected, fiber optic cabling offers greater security over copper.

All this stuff about fiber optic cable is great, but how is it used in a network, you ask? Well, knowing you read the section on Token Ring LAN segments, the authors feel we do not have to review the concept of token passing. If we are wrong, you should go back and read the Token Ring section about how a token is passed about a ring. Although the token-passing concept is

[14] *Link* is a reference to a cable connecting (linking) two network devices' ports. Many interface connectors on network devices have an LED indicator to indicate the presence of link. Link on an interface indicates that the transmit and receive signals are properly connected and the two devices are capable of communicating over the cable (link).

similar, FDDI is not the same as the IEEE 802.5 Token Ring standard. FDDI was standardized under ANSI standard X3T9.

From the previous paragraph, you are already aware that FDDI is implemented using token passing over a ring topology consisting of fiber optic cable. Construction of the network consists of dual rings, a primary ring and a secondary ring. Both rings are capable of passing data, but usually the counter-rotating secondary ring, which can carry data in the opposite direction, is reserved to be used as a backup in case of ring failure. Figure 2-19 shows a logical representation of an FDDI network.

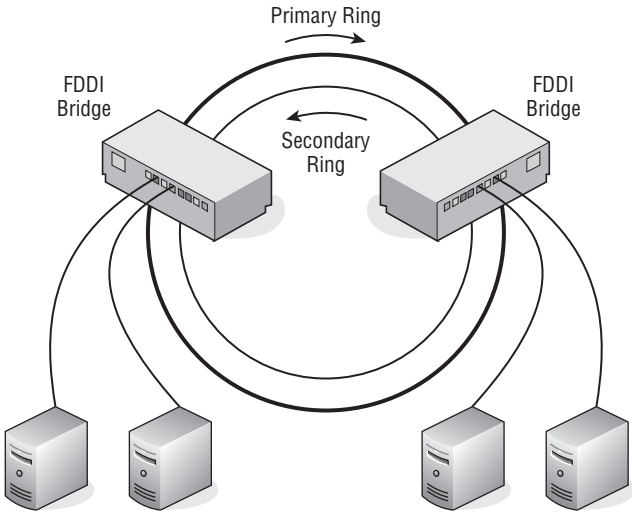


Figure 2-19 An FDDI network

Although this network is shown logically as a ring, it is physically deployed in a star topology similar to that of wired Token Ring networks. FDDI bridge/concentrators complete the logical ring while also providing the optical to electrical signal conversion to allow data to be transferred from an optical network segment to a wired network segment and in the reverse direction.

To facilitate the star physical topology, fiber optic cable is dual strand cable. There is one fiber optic strand carrying intelligent light information to the FDDI bridge concentrator while the other strand allows for the transmission of data from that FDDI concentrator to the next. These fiber optic network cables are sometime called *light pipes*.[15]

[15]Don't confuse fiber optic data cables with those fiber strands you see at the mall emitting all those wild colors. Although similar in terms of light being transmitted through an optical fiber, the quality and construction are far different. After all, it is for the purpose of sending intelligent data.

FDDI networks are capable of transmitting data at 100 Mbps for a maximum ring circumference of 100 kilometers. If both the primary and secondary rings are used, an effective data rate of 200 Mbps can be achieved. This is what makes FDDI the preferred choice for backbones on large LAN networks and for deploying a MAN over a wide geographical area.

To pass data from either an Ethernet or Token Ring LAN segment requires a bridge to transform electrical signals into intelligent light impulses. These bridges fall into two categories, encapsulating bridges and translating bridges. Encapsulating bridges encapsulate Ethernet frames into FDDI frames, and translating bridges translate the received frame source and destination MAC addresses into FDDI addresses. The maximum FDDI frame size is 4500 bytes.

A dual ring FDDI network can connect up to a maximum of 500 stations. Since FDDI requires a repeater every 2 kilometers, it is unsuitable for a WAN network deployment. FDDI lends itself easily within existing metropolitan infrastructures where cabling is routed in hostile environments under streets and overhead lines. It is impervious to EMI, so no special shielding is required other than having the fiber jacketed to withstand the environment it is to be placed in. Since fiber cable depends on a continuous, undistorted fiber to transmit data without degradation, care must be taken to maintain a minimum bending radius for the type of fiber cable being used, to prevent a possible crimp in the fiber. A distortion of the fiber can cause light reflections that could render the total cable length unusable for the transmission of data.

Fault tolerance is built into the dual ring FDDI network. When an interruption on the primary ring is detected, beaconing is used to determine where the break occurred. Beaconing is also used to monitor the health of the ring network token-passing process. Each station on the ring is responsible for checking the token-passing status of the ring. If a fault is detected by a station, it transmits a beacon onto the ring. The upstream station receives the beacon and begins to transmit its own beacon. The downstream station ceases beaconing after receiving a beacon from its upstream station. The process keeps moving to the next upstream station around the ring until the beaconing station does not detect a beacon from its upstream station. The fault has been isolated between the beaconing station and its upstream station. The secondary ring can then be placed into service by allowing for data traffic flow in the opposite direction. When the beaconing station detects its own beacon being received on the primary ring, it is notified that the fault has been isolated and repaired. Upon receipt of its own beacon, the station shuts off beaconing and returns to normal service.

2.2.2 A MAN Example

Anytown, USA, considers itself a happening place. Not wanting to miss out on being part of the ''connected'' age, the city fathers have launched a plan to provide computer services to all city departments. In order for the local citizenry to see their tax dollars at work, they decided as part of the overall project they would provide Internet access to the general populace. The greater Anytown metropolitan area spans several miles, with some buildings as far as five miles away from city hall.

The mayor called in the heads of Anytown's IS department, told them of his great vision, and asked how they would go about implementing his great plan. The IS department managers went away scratching their heads and wondered how they were to pull this one off. The general thought within the group was that, since the mayor's vision was pie in the sky, they would draw up a proposal that would be doable while still maintaining their control over the administration of Anytown's information services.

After several weeks of thrashing about among the IS department's staff, the plan was devised and drawn up. The big night arrived, and the chief of Anytown's IS department wore his Sunday best for the presentation of the devised plan to the mayor and the city counselors.

When the slide was placed on the overhead projector, the mayor and counselors saw what is shown in Figure 2-20.

The IS chief's explanation went as follows. The main departments within Anytown's government already had LAN technology deployed within the areas they were responsible for. General communication and the passing of data between departments was being done via e-mail. By implementing a citywide FDDI network, each department's LAN would be able to send data directly from station to station over the newly connected LAN networks. He went on to explain that servers located on each individual LAN would be centrally located within the IS department at city hall. Each department location would be connected directly to city hall via high-speed fiber optic cable, shown as dashed lines on the MAN network diagram.

He went on to further explain that each department currently was responsible for its own Internet access. With the proposed high-speed fiber optic network, this could be consolidated under the control of the city hall IS staff. A single high-speed network connection would give Internet access to not only all city departments but also the general public. It was stated that there would be

POP QUIZ

IEEE 802.5 limits the number of nodes on a ring to _____ nodes.

security precautions put in place to prevent unauthorized access to servers maintained by the city.

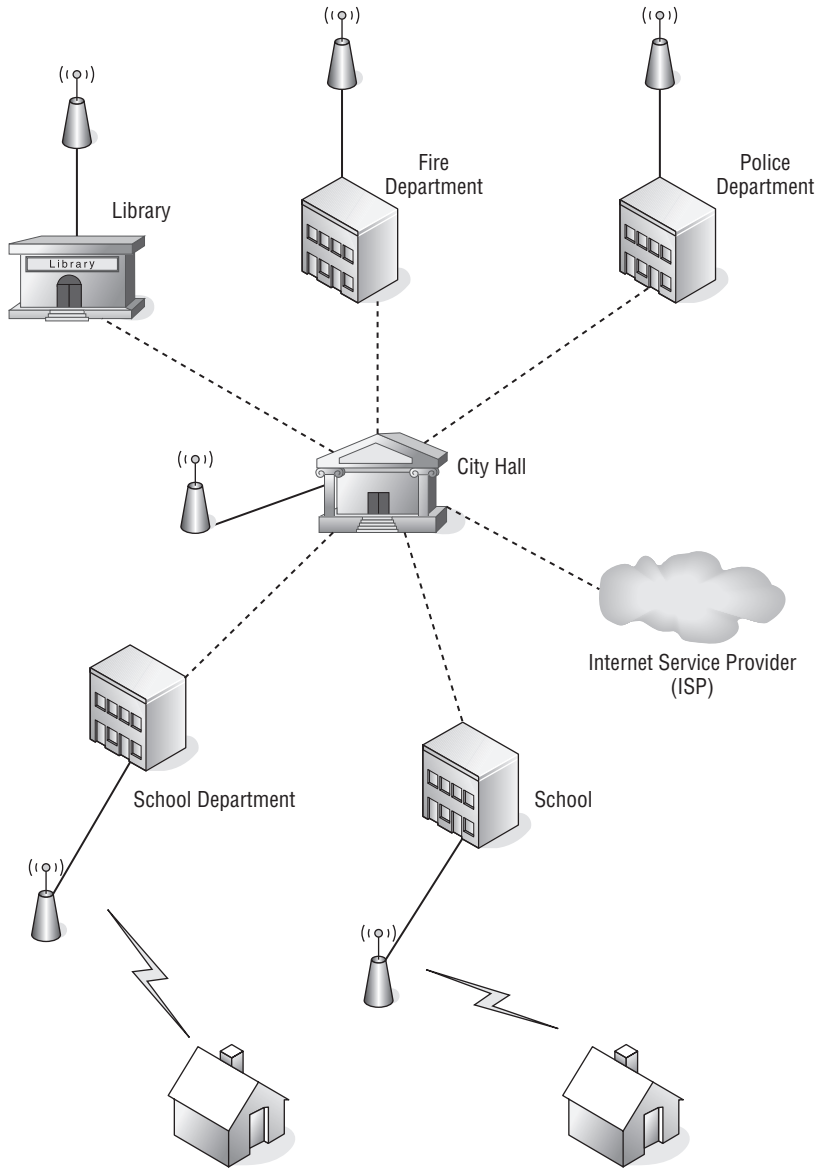


Figure 2-20 Anytown's MAN

The local telephone company would be contracted to run the dedicated fiber optic cable from city hall to the remote buildings over their current cableways and overhead lines. The general public would have access over wireless links

to access points located throughout the city to ensure that all of Anytown's citizenry would have equal access to the Internet service provided by the city. For those without personal computers or unable to connect to the citywide wireless network, public access computers would be located at schools and libraries.

With his presentation completed, the IS chief asked if there were any questions. The mayor seemed pensive at first and then asked, ''Can you explain why there is only wireless Internet for the public?'' The IS chief said, ''Yes, sir, I can.'' He went on to explain that the infrastructure cost to bring a wired Internet alternative to all of the city inhabitants would drive costs for the project beyond reach of the city's budget. Also, some of the expenses for the FDDI network could be recouped over time from consolidation of common services utilized by each city department. Providing a citywide wired public network would be cost-prohibitive. The IS chief went on to explain that there were already a few Internet providers servicing the Anytown greater metropolitan area, and those citizens desiring a wired Internet access were more likely to already be subscribed to their service or would do so in the future.

The mayor thanked the IS chief for his presentation. The counselors all voted their approval, and the mayor began drawing up his new campaign speech on how he was instrumental in getting Anytown connected.

This example of how a MAN might come about is largely tongue-in-cheek. However, it does demonstrate that the basic definition of a MAN is a network that covers a wide geographical area that can be either a city or include the greater metropolitan area of a city. The feasibility of MAN networks would not be possible without the availability of high-speed networks such as Metro Ethernet or FDDI optical networks.

The chief piece of information that the student should take from this section is the awareness that a high-speed data link is required when connecting LAN networks located some distance apart. When users and services on both ends of the link are contending for use of the link, the speed at which the link is able to pass traffic will be the determining factor of the performance of the interconnected LAN networks over that link. A safe rule of thumb is the more bandwidth the better. It gives better performance and allows for future growth and expansion of the connected LAN networks.

2.3 Wide Area Networks

As discussed in Chapter 1, the main use of a WAN is to provide a high-speed data network between two geographically distant networks. This chapter will discuss a few WAN telecommunications services most used in the makeup of a WAN network.

WAN networks are constructed from a wide range of service levels that can be obtained from the telephone companies. These can range from slow, low-grade analog circuits to high-speed digital signal services. The most widely used and available WAN standards are POTS, ISDN, and frame relay.

2.3.1 Whose POTS?

POTS stands for plain old telephone service. It refers to the use of voice-grade telephone lines to form a point-to-point data connection. Because these voice lines can be found in many places around the world, it is possible to create a WAN connection between two LAN networks that are far apart. Figure 2-21 illustrates a dialup modem[16] connection between two offices.

This figure shows two LAN networks, one located in Boston and the other in Santa Fe. This is a manual WAN connection operation. Each modem can be set to auto-answer so that when another modem dials in, it will answer the call and allow the connection to be completed. This is a very rudimentary WAN network. It works and is still the only available WAN-type connection that can be made from some very rural areas of the country.

The speed of the WAN connection is determined by the type of modem and the signal quality of the telephone line it is connected to. Customary speeds that can be attained are between 28.8 and 57.6 Kbps. There are devices in the marketplace that automate the dialing process. These are considered to be dial-on-demand routers. These devices reside on the LAN and will automatically dial a preprogrammed number when they detect that the data received from the network is destined for a LAN at the other end of the dialup WAN connection.

With a clear line and the use of compression, some modem-based devices are capable of throughput of 115 Kbps. As other access technologies have rolled out, such as DSL and Internet access over cable and fiber to the home, modem use has fallen off. These newer technologies can provide higher speed access to the Internet, but they are unable to provide a point-to-point WAN connection, which some organizations require. Later in this section we will discuss how these technologies can be used to provide a virtual point-to-point WAN connection.

[16]Modem takes its name from modulate/demodulate. It is a device able to both modulate and demodulate a digital signal into an analog signal that can be sent across standard voice-grade telephone lines.

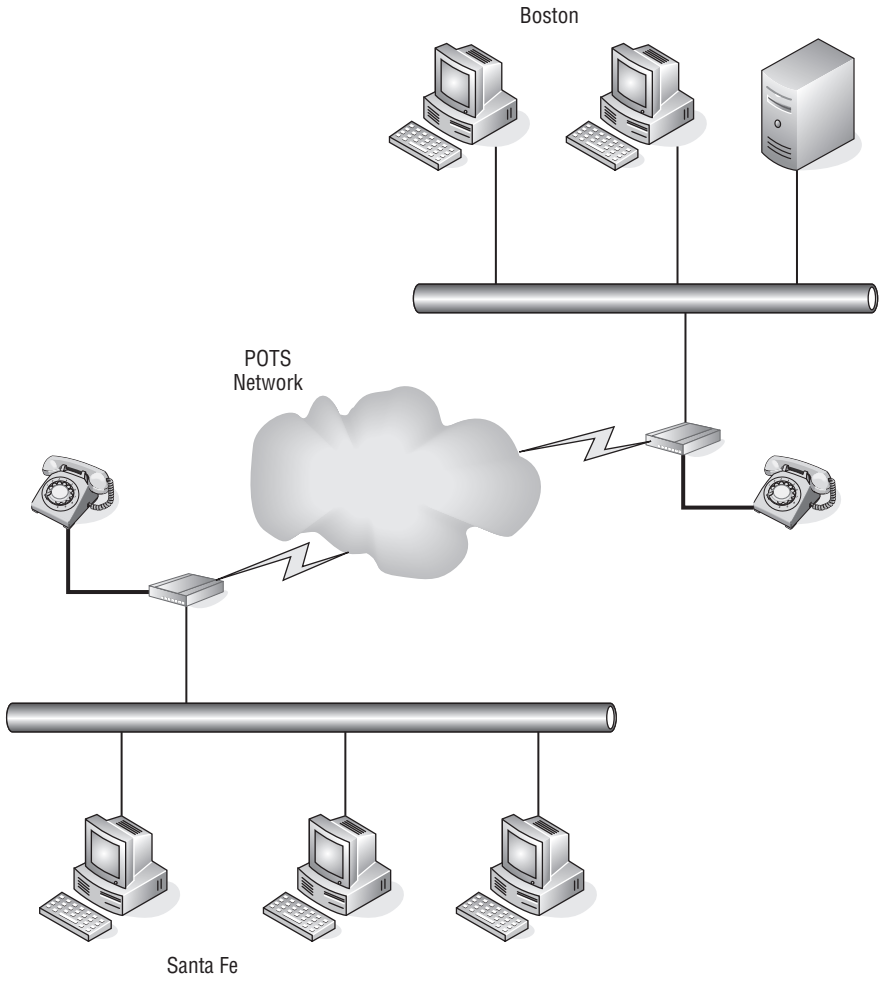


Figure 2-21 A POTS WAN connection

2.3.2 Integrated Services Digital Network

Integrated services digital network (ISDN) is a set of standards to provide voice, data, and video transmission over a digital telephone network. It is similar to a POTS line and modem in that it is able to use existing premises wiring to make a called connection to another ISDN subscriber. However, it can only call another ISDN subscriber, whereas a POTS setup can call any number

POP QUIZ

What is the major difference between Ethernet and IEEE 802.3?

that has an analog telephone connection to it. By integrating analog and digital signal transmissions using a digital network, ISDN is capable of delivering an improved data rate over typical modem connections. Unlike POTS, ISDN service is mostly concentrated in major metropolitan areas.

Taking advantage of LAN-to-LAN connectivity with ISDN providing the link can best be accomplished with the use of ISDN routers. They are typically configured for on-demand dialing. When there is data to be sent from one LAN to a remote LAN, the router will dial the remote ISDN router. When the remote ISDN router answers the call, data can be sent across the link. Since most ISDN service usage is typically billed by the number of calls and total minutes connected, ISDN routers may utilize an idle timer. This timer determines when there is no traffic being passed across the link. When the idle time interval has been reached, the call is terminated. These timers need to be set properly to eliminate excessive dialing and increased telephone charges. It is recommended that you understand how your local ISDN provider bills for this service. It could be by connected minutes, number of calls, or a combination of both. The only advantage that ISDN has over leased lines is that for low usage data connections it is cheaper than paying for a point-to-point leased line connection. ISDN is at a cost disadvantage in situations where the line is up for great periods of time. In those circumstances, it is best to look into using a leased line.

The two most commonly found ISDN services are:

- **Basic rate** — Provides two B channels of 64 Kbps and a single D channel of 16 Kbps.
- **Primary rate** — Provides 23 B channels of 64 Kbps and a single D channel of 64 Kbps for U.S.- and Japan-based subscribers. Subscribers in Europe and Australia are provided with 30 B channels.

An advantage that ISDN has over other WAN connection types when connecting to sites located in other countries is the service levels have been standardized by the International Telegraph and Telephone Consultative Committee (CCITT), so subscribers with ISDN service around the globe are able to interconnect to form a WAN network.

2.3.3 Point-to-Point WANs

In reality, all the WAN connections we spoke of in the two previous sections are also point-to-point WAN connections even though they require a manual or automated dial from a modem-based router. For the most part, when people refer to a point-to-point connection in the telecommunications arena, the first thought that comes to mind is directly connected point-to-point leased line connections. Figure 2-22 illustrates an organization with three major offices

located in New York, Los Angeles, and Miami. The amount of data traffic between these locations warrants dedicated point-to-point WAN connections. The lines in use are considered to be of the T class variety.

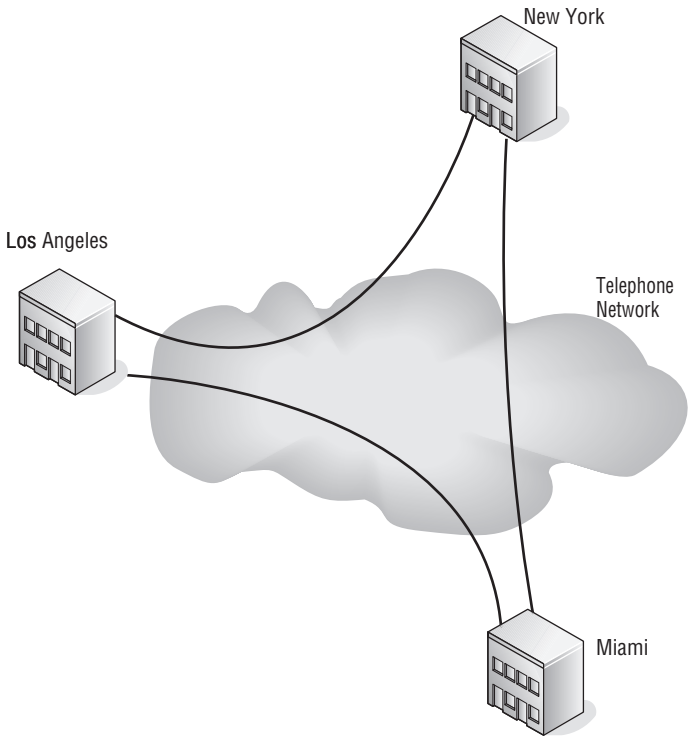


Figure 2-22 A point-to-point WAN network

Organizations do not only use these lines for data transmission. The lines can also be used for telephone, teleconferencing, and other forms of communications. The most common services used for these T class connections are T1, fractional T1, and T3. T1 can provide 1.544 Mbps of speed while T3 can deliver 44.736 Mbps.

RANDOM BONUS DEFINITION

preamble — A frame field used to allow a receiver to properly synchronize its clock before decoding incoming data.

A full T1 line provides 24 channels, each with 64 Kbps of bandwidth. When an organization leases a dedicated full T1 line, they are responsible for the T1 multiplexer equipment located at each endpoint. They can then dedicate the channels in any manner they choose. An example of this would be 6

channels dedicated to telephone service, 2 channels for teleconferencing, and the remaining 16 channels dedicated to moving data between locations. For organizations with demands for more bandwidth, the option would be to move up to T3 service. These services are point-to-point through the telephone network, but the service level is guaranteed by the telecommunications company. The lease cost is determined by the required bandwidth and distance between locations.

Organizations that require guaranteed throughput between organizations but do not need the speed of a full T1 can purchase a number of channels split out from an existing trunk circuit. This does provide a cost advantage, but it has its downside — the organization does not have control over where that circuit is routed. Cost is determined by the number of channels required and the distance between the locations. As the number of channels begins to increase, the cost advantage of fractional T1 is lost.

2.3.4 Frame Relay

So far, we have talked about WAN circuits being directly connected endpoint to endpoint, although traveling through a switched telephone network. Those connections were dedicated to creating a full-time fixed bandwidth connection. Frame relay[17] is designed for data traffic that tends to move in bursts. This is accomplished by using packet switching in a switched cloud provided by the telecommunications companies.

Because frame relay lends itself to burst-oriented traffic, it is not suitable for real-time applications such as telephones or teleconferencing. As information is moved in packets, the service is provided as a committed information rate (CIR). It is listed as a bandwidth number, but that does not necessarily mean you have continuous access at that bandwidth.

POP QUIZ

What are the two most common ISDN services?

The level of service is measured for frame relay using a formula that includes committed burst size (CBS) over an interval of time. The basic formula is as follows:

```
Time = Committed Burst Size (CBS) / Committed Information Rate (CIR)
```

[17]Frame relay is based on X.25 packet-switching technology, which was developed to move data signals that were primarily analog, such as voice conversations. X.25 works in Layers 1, 2, and 3 of the OSI model. Frame relay only uses Layers 1 and 2, giving it greater speed that is about a factor of 20 over X.25. This is accomplished by dropping packets that are found to be in error and relying on the endpoints to process packet-drop detection and request retransmission of packets.

To illustrate this further, a customer has chosen a service that provides a CIR of 64 Kbps and a CBS of 256 Kbps. At first glance, it appears that traffic can burst up to 256 Kbps, but that is not the case. If CBS is divided by CIR, the resulting value is four seconds. This means the circuit needs to be capable of moving 256 Kbps in any four-second interval. This is far different from what most people think burst rate means. So the CIR and CBS need to be carefully looked at when subscribing to a frame relay service. If the network burst rate begins to exceed the CBS, network congestion will occur and data traffic will be affected. When selecting a frame relay service, it is best to have a good knowledge of the networks to be interconnected over frame relay. Figure 2-23 illustrates how a frame relay network may be implemented.

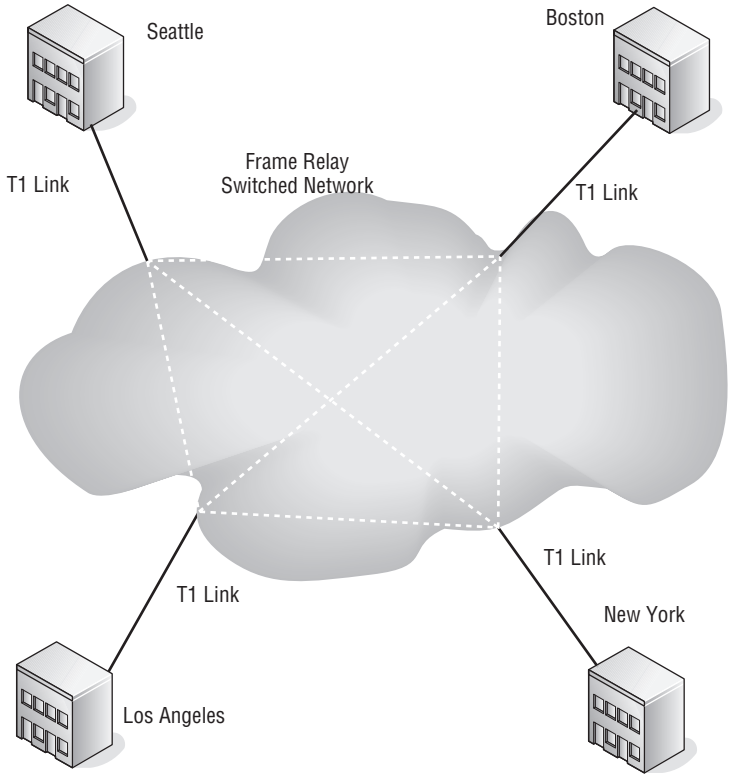


Figure 2-23 A frame relay network

This figure shows an organization with offices in Boston, New York, Seattle, and Los Angeles. Each has a T1 connection to the frame relay switched network. In this figure, each office is connected to every other office within the frame relay switched network using a private virtual circuit (PVC), which is illustrated by the dashed lines between each of the nodes connected to the switched network. This does have an advantage over pure point-to-point

WAN implementations, but it is best suited for burst type traffic and not traffic requiring a continuous guaranteed rate.

2.3.5 Using the Internet for Your WAN

The Internet is a network mesh that covers most of the globe. So it is possible to connect remote LAN networks over the Internet. However, the Internet is really a best-attempt-possible service. It is not guaranteed far as performance and is open to the public, which makes security a major concern. The chief advantage of using the Internet over other subscriber services is cost. Other than local Internet access fees, there are no other charges involved such as can be found when using a dedicated long line solution. Unlike dedicated point-to-point services, it is inconsequential how these devices connect to the Internet. The type of connection to the Internet is not a factor in the creation of the virtual point-to-point connection. Factors that can affect performance include the speed of the connection and its reliability where connectivity is concerned. Although electrons move at the speed of light, intelligent electrical signals are also subject to latency problems the greater the distance is between two endpoints of a network.

The solution of using virtual private networks (VPN)[18] is only viable in scenarios that require a remote office to connect to a central office. It is not intended to replace dedicated high-speed point-to-point network connections. Data integrity and security are maintained and ensured using encryption and encapsulation of the data packets that are transmitted over the Internet. Authentication is used to confirm that an endpoint device or user is fully authorized to send and receive data from the VPN connection. Figure 2-24 illustrates how VPN connections may be used as a substitute for a dedicated WAN network connection.

A remote office in Boston is connected to the corporate office in New York using the Internet to form its VPN tunnel. This is a peer-to-peer tunnel where each endpoint knows the other and is part of the security as the peers are known to each other. Authentication security is increased with the use of preshared keys (PSK), and other authentication methods such as certificates and tokens may also be added. Once the VPN

POP QUIZ

True or false: Virtual private networking is networking that does not require any hardware at all.

[18]For further information on how to use VPN tunnels, check out *Nortel Guide to VPN Routing for Security and VoIP*, by James Edwards, Richard Bramante, and Al Martin (Wiley Publishing, Inc., 2006).

tunnel is formed, traffic destined for either LAN is passed through the tunnel as if it were a dedicated link. The end-user workstations only need to be concerned with the address of the device on the other LAN. The VPN routers are the only devices that need to be aware of the endpoint address of its peer VPN routers. So for this purpose, the peer-to-peer tunnel functions as if a dedicated point-to-point link is in place between the two LAN networks.

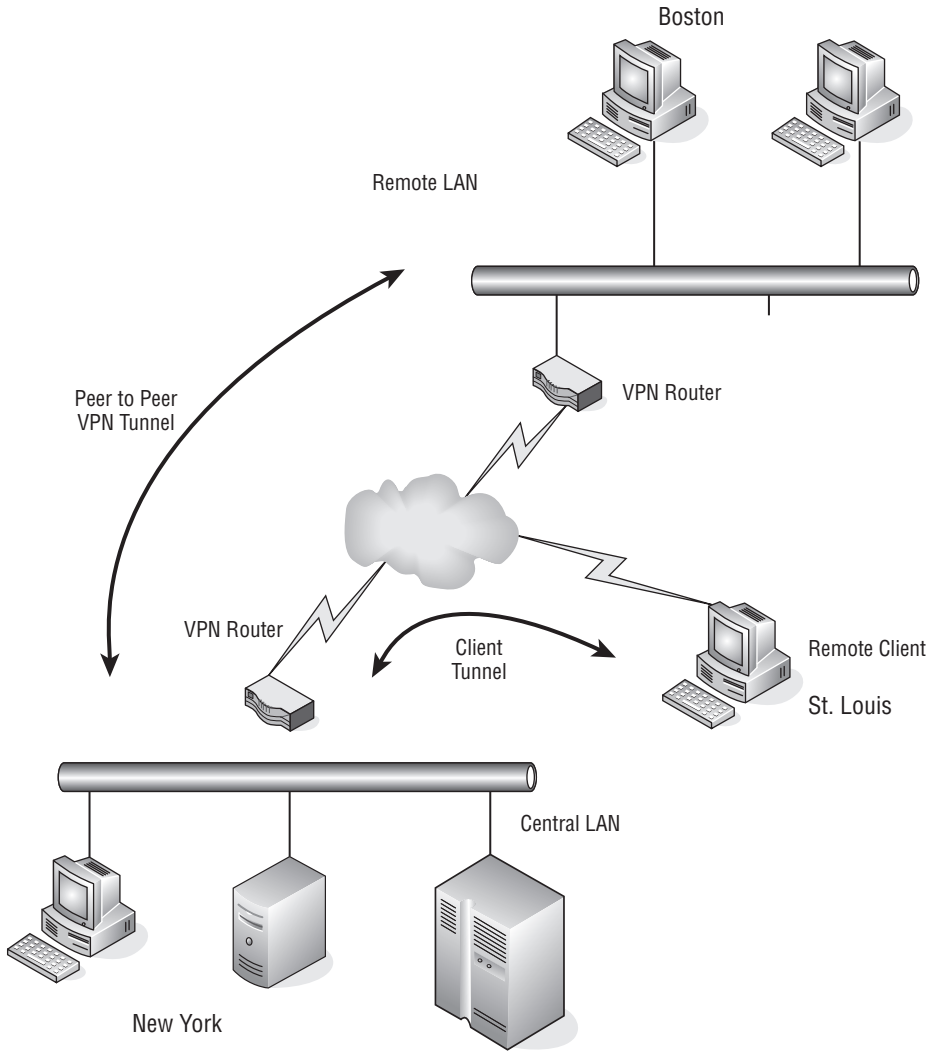


Figure 2-24 A VPN as a WAN

VPN routers are also able to accommodate end-user tunnel connections. For this example in Figure 2-24, a user in St. Louis is able to connect to the central office in New York to gain access to the network and use the

services on that network. Since remote users can contact the central office from almost anywhere, their endpoint addresses would not be previously known. However, users are required to be authenticated in the same manner as a peer-to-peer tunnel, which may include multiple forms of authentication processes. Once authorized, a user is able to access the services they are authorized to use. Many installations require additional authentication to access internal servers. Access to the network does not necessarily mean access to all devices. VPN routers are capable of applying security policies on both peer-to-peer and end-user client tunnel connections.

The protocols used for VPN tunneling are Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IPSec (IP Security).

2.4 Chapter Exercises

1. The term *modem* is short for _____ .
2. A _____ is a network where network devices are located within close proximity to each other.
3. CSMA/CD is an acronym for _____ and is associated with a network using a _____ network topology.
4. Which network topology allows for orderly network access for the stations connected to that network?
5. What two standards define a CSMA/CD network?

   _____

   _____
6. Name three media types that can be used to connect devices located on a LAN?

   _____

   _____

   _____
7. The major characteristic of 10BASE-T cable is:

   _____
8. A personal computer (PC) requires a _____ to be connected to a local area network (LAN).
9. FDDI is an acronym for _____, which is often used to construct citywide networks called _____ .
10. POTS is an acronym for _____ .

11. A dialup service that connects to a digital network is _____ .
12. What technology can be used to create a point-to-point network connection over the Internet?

2.5 Pop Quiz Answers

1. What are the 2 sublayers of the Data Link layer?

   Logical Link Control (LLC) and Media Access Control (MAC)
2. MAC addresses are represented with hexadecimal numbers, separated by a colon or a *hyphen*.
3. What is the maximum length of a cable between a workstation and a hub?

   100 meters
4. IEEE 802.5 limits the number of nodes on a ring to *250* nodes.
5. What is the major difference between Ethernet and IEEE 802.3?

   Frame format
6. What are the two most common ISDN services?

   Primary rate and basic rate
7. True or false: Virtual private networking is networking that does not require any hardware at all.

   False