Review of Information Network and Technology

OBJECTIVES

- *Network components and technologies to be managed:*
  - *Network topologies: LAN and WAN*
  - *Wired LAN topology: Bus, Ring, Star, and Hybrid Hub*
  - *Wireless LAN*
  - *WAN topology: Mesh and Tree*
  - *Fixed and mobile wireless networks*
  - *Fiber networks*
- *Ethernet LAN:*
  - *Physical media and MAC protocol*
  - *10 and 100 Mbps; 1 and 10 Gbps Ethernet LAN*
  - *Switched and Duplex Ethernet LANs*
  - *Virtual LAN*
- *Token-Ring LAN*
- *FDDI*
- *Network components:*
  - *Bridges*
  - *Routers*
  - *Gateways*
- *Circuit switching and packet switching*
- *Transmission technology:*
  - *Transmission media: Wired and wireless*
  - *Transmission modes*
  - *Multiplexing: TDM and WDM*
  - *SONET and SDH*
- *Multimedia networks and services*

In Chapter 1 we learned that a network comprises nodes and links. Nodes are switches, bridges, routers, or gateways. Links comprise Local Area Networks (LANs), Wide Area Networks (WANs), Access Networks, or Customer Premises Equipment (CPE)/Home Networks. In this chapter we will review these components from the perspectives of concept, technology, and management. We will limit our review here to Internet-based components and some of the telecommunication components. Components associated with broadband-specific networks will be covered in detail when we address them in later chapters.

Section 2.1 presents various network topologies of LANs and WANs. In Section 2.2 we start with basic Ethernet and then traverse the development of Ethernet, Fast Ethernet, Gigabit Ethernet, and switched Ethernet. Token Ring was the most commonly used LAN in the IBM mainframe environment. Fiber-optic technology uses Token-Ring architecture to develop Fiber Distributed Data Interface (FDDI). Flexibility of LAN facilities has been significantly increased by the development of virtual LANs (VLANs). Wireless LAN (WLAN) has become an important component of the modern network.

Network node components form the contents of Section 2.3. We start by describing the implementation of LAN as a discrete component, a hub. LANs are interconnected by bridges. A bridged network is made up of remote bridges in a tree topology. LANs can also be connected in a mesh WAN topology using routers as nodal components. Autonomous WANs with diverse networking protocols are interconnected with gateways that do protocol conversion at network layers and above. Half-bridge/half-router configuration is used for Internet point-to-point communication link. The discussion of Section 2.3 ends with a switching component and the part it plays in WAN topology. Wide area network is briefly discussed in Section 2.4. It is the telecommunication network that computer (or data) communication traverses a long distance.

Section 2.5 addresses transmission technology. It comprises wired and wireless technology that transports information over LANs and WANs. The mode of transmission may be either analog or digital; and a message may be transmitted in either mode, or part of the way in analog mode and the rest in digital. This becomes especially true in broadband multimedia services where data, voice, and video are integrated into a common service, Integrated Services Digital Network (ISDN). Broadband network made up of hybrid technologies is introduced in Section 2.6 for completeness and is discussed in detail in Part IV.

2.1 NETWORK TOPOLOGY

A LAN is a shared medium serving many Digital/Data Terminal Equipments (DTEs) located in close proximity, such as in a building. LANs could also be deployed in a campus environment connecting many buildings.

Three topologies are associated with LANs: bus, ring, and star topology. There exists a fourth pseudo-topology that combines a star topology with either of the other two and is known as a hub. A hub plays an important role in networking as we will soon learn.

LAN topology depicts the configuration of how DTEs are interconnected. Different protocols are used in different topological configurations. Bus architecture is implemented in LANs using Ethernet protocol. Token Ring and FDDI configurations use the ring topology. FDDI can cover a much larger geographical area than Token Ring on copper. Fiber ring topology has been extended to Synchronous Optical Network (SONET) and Resilient Packet Ring (RPR). SONET and RPR can be considered geographical extensions of LAN to WAN, also known as Metropolitan Area Network (MAN), and use different protocols. A star topology is used in cabling infrastructure and is ideally suited for hub implementation, or for WLAN using an access point (AP).

WANs are configured using either the mesh or the tree topology. The mesh topology is the most common form for Internet routing. The tree topology is employed in network using brouters, which are bridged routers that do the routing function at OSI layer 2. It is also known as spanning-tree configuration.

The three LAN topologies and hub configuration are shown in Figure 2.1. In the bus topology, Figure 2.1(a), all DTEs are on a shared bus and have equal access to the LAN. However, only one DTE can have control at any one time. A randomization algorithm determines which DTE has control of the LAN at any given time. This topology is used in Ethernet LAN. Because collisions occur when more

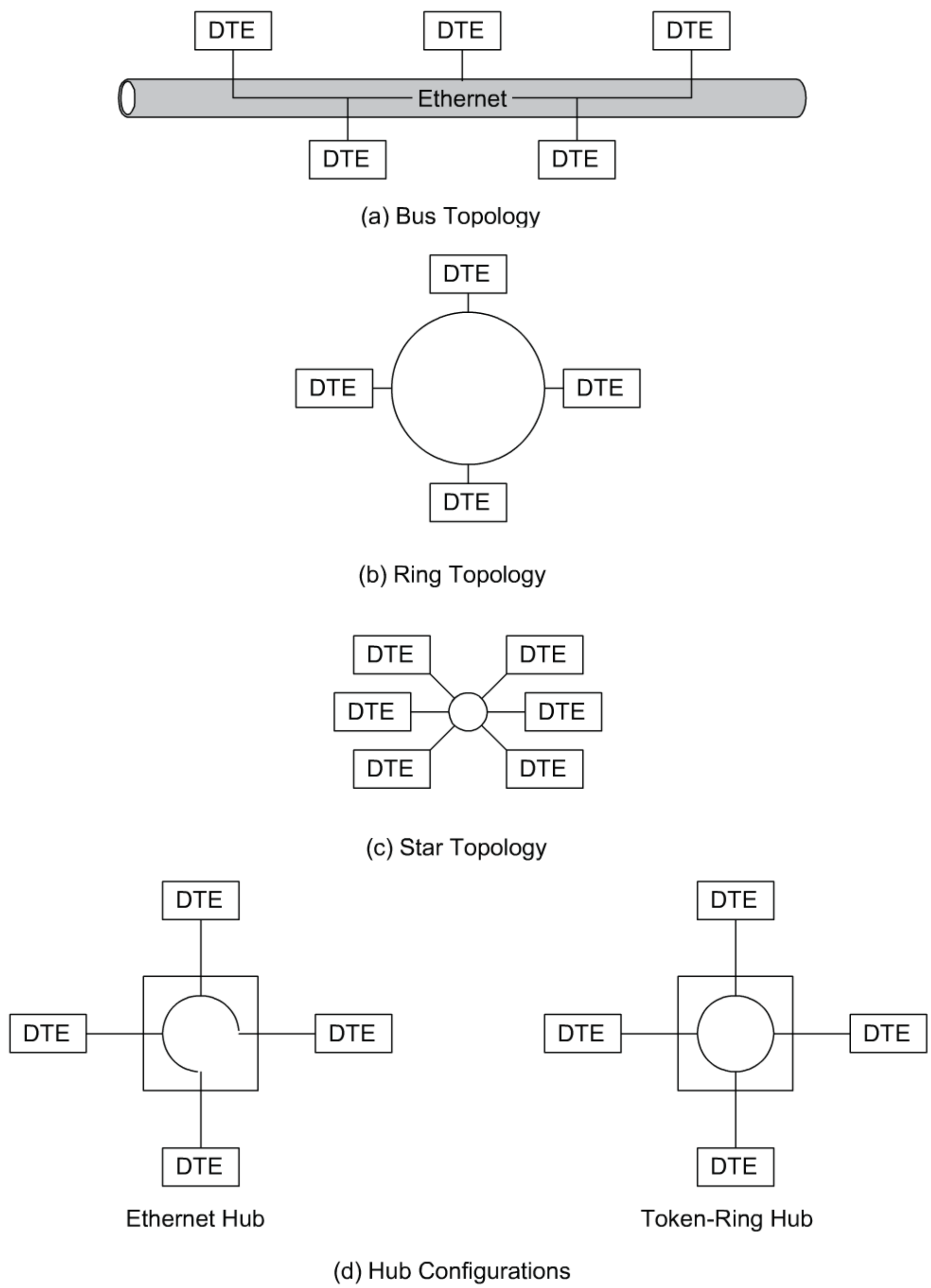


Figure 2.1 LAN Topologies

than one station tries to seize the LAN at or about the same time, the bus LAN usually functions at much less than full efficiency. Ethernet protocol is specified by IEEE 802.3 standard.

Figure 2.1(b) shows the ring topology and was most popularized by IBM's Token-Ring LAN. In this topology, each active DTE connected to the ring takes turns in sending information to another DTE in the ring, which may be either a receiving host or a gateway to an external network. At the time a DTE communicates over the ring, it is in control of the ring and control is managed by a token-passing system. The DTE holds on to the token while it is sending data and releases it to its downstream neighbor (round-robin) after its turn is finished. Thus, the process in this topology is deterministic and LAN operates at almost full bandwidth efficiency. IEEE 802.5 standard specifies token-ring protocol. FDDI technology also uses ring configuration, implementing IEEE 802.4 standard.

Figure 2.1(c) represents a star topology that was once used in star LAN. However, it is at present used in a hybrid mode, as discussed in the next paragraph. In the star topology, all DTEs are connected to a central node and interconnected in one of two modes. They can be connected in a broadcast configuration. In this configuration, all the other DTEs receive data transmitted by a DTE. This would be similar to a bus topology. In the second configuration, DTEs are connected to the central node, but are interconnected on a pair-wise basis selectively. In this situation, multiple conversations can occur concurrently between various DTEs passing through the central node.

As mentioned earlier, a hub configuration uses a star topology in combination with either a bus or a token-ring topology. The hub configurations shown in Figure 2.1(d) are the most popular LAN implementation. The hub is also known as a Layer-2 switch. It is a hybrid between (c) and either (a) or (b). DTEs are electronically connected to each other at the central node in either the bus or the ring topology. If they are connected in a broadcast configuration for an Ethernet LAN, it is called an Ethernet hub. If DTEs are connected in a ring topology for use with token-ring LAN, it is called a token-ring hub.

WAN differs from LAN in that it links networks that are geographically separated by a long distance. Typically, the WAN link connects nodes made up of switches, bridges, and routers.

WANs are connected in either a mesh or a tree topology, as shown in Figure 2.2. The mesh topology, Figure 2.2(a), provides multiple paths between nodes. Thus, a message between nodes N1 and N6 may traverse the paths N1–N2–N5–N6, N1–N3–N5–N6, N1–N2–N3–N5–N6, N1–N3–N2–N5–N6, N1–N4–N5–N6, N1–N4–N3–N5–N6, and N1–N3–N4–N5–N6. This allows packets belonging to a message to traverse different paths, thus balancing traffic load. It further provides redundancy for reliability of service. However, a broadcast message from N1 to all other nodes will be rebroadcast by neighboring nodes N2, N3, and N4 to all other nodes. This could cause flooding on the network and looping of

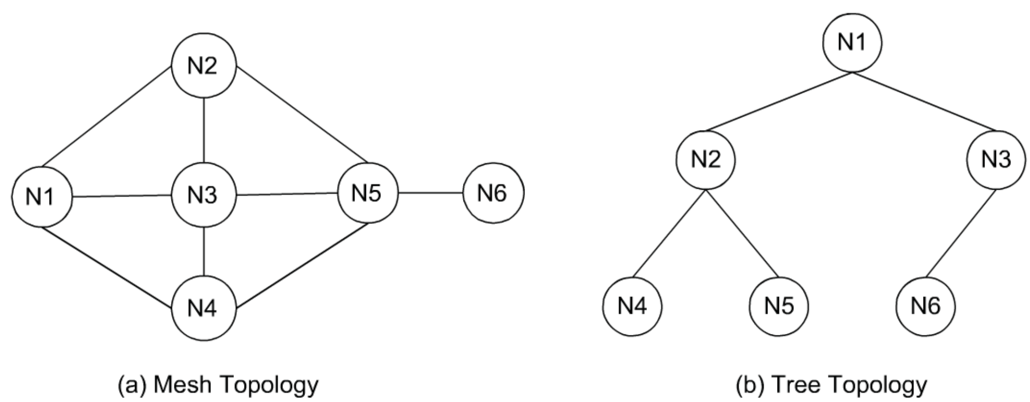


Figure 2.2 WAN Topologies

packets, which needs to be carefully addressed. Flooding is a node receiving the same packets multiple times, and looping is a packet going around nodes in a loop, such as N2–N3–N1–N2 or N4–N3–N2–N1–N4 paths. A mesh topology is usually implemented using switches and routers.

A tree topology is shown in Figure 2.2(b). It appears as a hierarchical architecture. The tree structure starts with a node, called the header node, and branches out to other nodes in a tree structure. There can be no closed loops in the network. However, paths between nodes may be longer. For example, the packet from N4 to N6 has to traverse the top of the hierarchy N1 and then down to N6. The tree topology is simpler to implement than the mesh topology and uses bridges at the OSI data link layer.

2.2 LOCAL AREA NETWORKS

There are two types of LANs that are deployed, bus based or ring based. The most common bus-based LAN is Ethernet and is the most widely deployed LAN. Ring-based LANs are Token Ring and FDDI.

A representation of a campus network with different LANs is shown in Figure 2.3. The backbone of the campus network is a fiber network 10.10.0.0. The notation of the fourth decimal position being 0 is used to represent the network address. Ethernet LAN (10.1.2.0) is connected to the backbone via a router. Workstations on this LAN have the fourth decimal position in their IP addresses from 2 to 5. IP addresses 10.1.2.1 and 10.1.2.6 are the interface addresses to the router and the bridge.

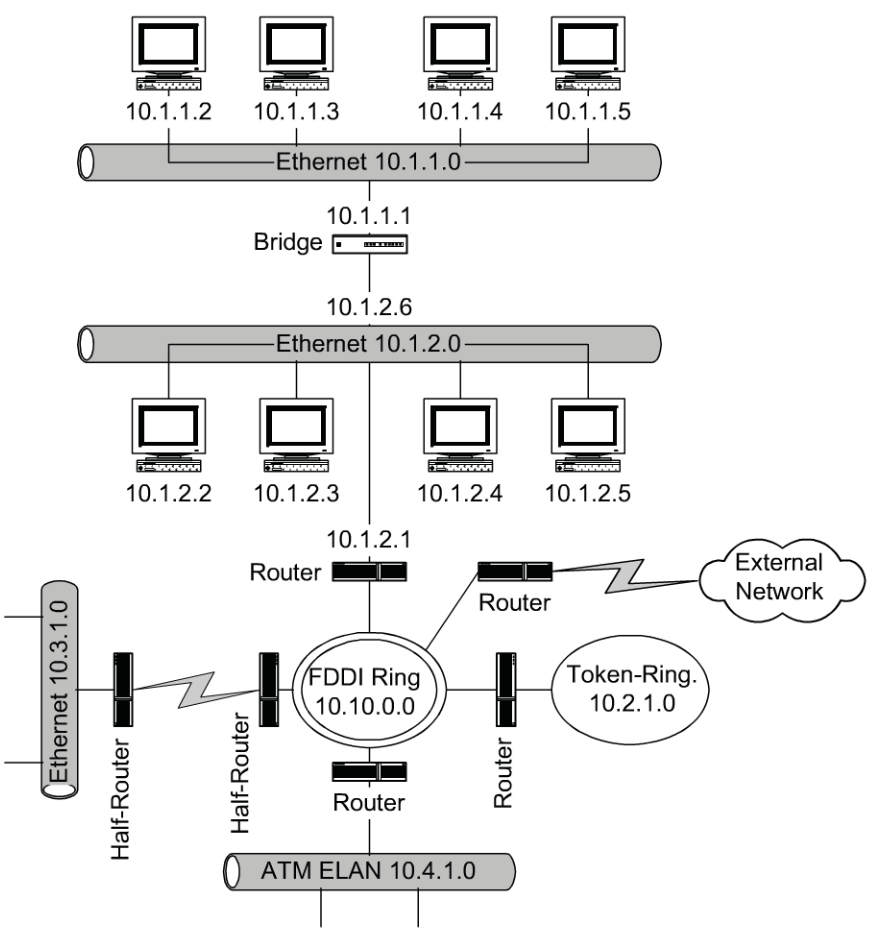


Figure 2.3 Campus Network of LANs

The second Ethernet LAN (10.1.1.0) is connected to the first Ethernet (10.1.2.0) via a bridge. IP addresses 10.1.1.2 to 10.1.2.5 are interfaces to workstations and the IP address 10.1.1.1 is the interface to the bridge. Notice that all external traffic from 10.1.1.0 Ethernet has to traverse 10.1.2.0 Ethernet LAN. 10.2.1.0 is a token-ring LAN connected to the backbone FDDI ring via a router. Two other LANs that are connected to the backbone are ATM Emulated LAN (ELAN) (10.4.1.0) via a router and an Ethernet LAN (10.3.1.0) via two half routers. The two half routers are connected via a dial-up link. It should be pointed out that most campus networks currently deploy high-speed Ethernet over fiber medium and LANs are exclusively Ethernet LANs. We will review LANs in this section and network components in Section 2.3.

2.2.1 Ethernet

Ethernet uses bus architecture with Carrier Sense Multiple Access with Collision Detection (CSMA/CD). DTEs are all connected to the same bus and transmit data in a multiple access mode. In other words, several DTEs can start transmitting frames at the same time. A frame comprises user data that are encapsulated with a header containing the source and destination address. A DTE starts transmitting when there is no carrier sensed on the bus. The transmitted signal travels in both directions on the physical medium. While transmitting, if a collision with another frame is detected, the DTE stops transmitting and attempts again after a certain period. Thus, the mode of transmission is a broadcast type with probabilistic collision of the signal.

A good analogy to understand the collision phenomenon is to envision a hollow pipe with holes all along representing stations. There is a person at each hole representing a station. The ends of the pipe are sealed and do not reflect sound. Let us suppose Joe starts speaking at a hole near one end of the pipe. He makes sure that he does not hear anybody speaking before he starts (carrier sensing). Once he starts talking, he has to make sure that nobody else starts talking until he finishes. He does this by continuing to talk and at the same time listening for other messages on the pipe. If he hears nobody else, then there is no collision. If he hears somebody else, then his message has collided with another person's message; and they both have to start over again. The longest time that Joe has to wait is for a voice to reach him from a person speaking at a hole near the other end of the pipe; and that person starts speaking just before Joe's voice reaches him. From this analogy, we can calculate that the minimum duration of time that Joe has to keep talking to ensure that there is no collision is the round-trip propagation time of his voice along the length of the pipe. Thus, there is a minimum frame size for Ethernet packets, which is 64 bytes. It is left as Exercise 1 for the student to prove this.

IEEE and ISO standards have been developed for Ethernet second layer MAC. They are IEEE 802.3 and ISO 8802.3, respectively. According to these standards, a physical coaxial segment can be a maximum of 500 meters; and there can be a maximum of 100 DTEs connected to it. A maximum of five segments can be connected with four repeaters to form one Ethernet LAN. However, if there are branches in the LAN, as in a tree structure, then any one total Ethernet segment should obey the above rule.

The data rate on an Ethernet bus is normally 10 Mbps (million bits per second). When traffic on the bus reaches about 40% to 70% of the maximum data rate of 10 Mbps, depending on the packet size, performance degrades significantly due to an increased collision rate. The bus medium can either be thick (0.4" diameter, but this is no longer deployed) or thin (0.25" diameter) coaxial cable; and DTEs are tapped on to the bus in a T-connection. There is a maximum segment length for LAN depending on the medium. This is listed in Table 2.1. There is also a limit on the length of the drop cable—the cable from the LAN tap to the

Table 2.1 Ethernet LAN Topology Limits

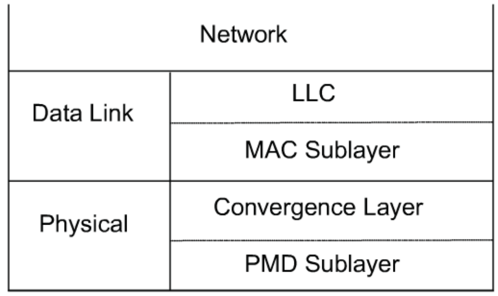
TYPE	DESCRIPTION	SEGMENT LENGTH	DROP CABLE LENGTH
10Base2	Thin coax (0.25”)	200 meters	Not allowed
10Base5	Thick coax (0.4”)	500 meters	Twisted pair: 50 meters
10Base-T	Hub topology	N/A	Twisted pair: 100 meters
10Base-F	Hub topology	N/A	2-kilometer fiber

connector on the network interface card (NIC) of the DTE. This is also shown in Table 2.1. As can be seen from the table, the original segment length defined for 10Base5 determined the minimum packet size of 64 bytes. However, with different configurations shown in the table (10Base2, 10Base5, 10Base-T, and 10Base-F), segment lengths and drop lengths vary based on the medium. However, the minimum packet size is still maintained at 64 bytes.

Ethernet LANs used to be configured by running coaxial cable around the DTEs with each DTE being tapped on to the cable. This could cause a great deal of management problem in tracking a faulty DTE. It is also difficult to isolate a DTE that caused heavy load on the LAN, or a killer DTE that has a problem and brings the network down frequently. It is likely that sometimes the maximum length of Ethernet LAN could have exceeded the allowable limit. The network could then crash intermittently at the limit length. It could also have an intermittent problem when traffic on the LAN exceeds the threshold. These problems have been eliminated by setting up the Ethernet LAN in a hub configuration, as shown in Figure 2.1(d). All DTE links, “drops,” are brought to a hub located in a central wiring closet and connected to a dedicated port of the hub. DTEs are connected inside the hub in an Ethernet configuration with active electronics. Problems associated with a DTE can now be isolated to a port in this configuration and resolved in a much easier fashion.

2.2.2 Fast Ethernet

The hub technology described above led to the development of Fast Ethernet technology. Fast Ethernet operates at a speed of 100 Mbps data rate on an unshielded twisted pair (UTP) cable and is called 100Base-T. The maximum length from the hub to the DTE is specified as a 100-meter or a 200-meter round trip. This produces a maximum path delay, which is the delay between two DTEs of 400 meters, plus a repeater delay of one repeater instead of four repeaters. This is less than one-tenth the delay in straight Ethernet MAC specifications (5,000 meters) with four repeaters. Thus, speed can be increased ten times from 10 Mbps to 100 Mbps. However, to be consistent with IEEE 802.3 standards, an additional sublayer, convergence layer, needs to be introduced in the physical layer above a physical medium-dependent (PMD) sublayer (similar to what we saw in the OSI network layer). This is shown in Figure 2.4. The physical medium should be capable of carrying a 100-Mbps data rate signal over the maximum length of the drop cable, which is 100 meters. Category 3 UTP cable cannot carry such a high data rate. Hence, four pairs of UTP cables are used to distribute the data, each pair carrying 25 Mbps. Hence, the terminology 100Base-T4 is used, that is, 100 Mbps carried over four twisted pairs. This limitation could be overcome by using two pairs of Category 5 UTP cable in full-duplex mode configuration, which we will discuss in Section 2.2.4. The minimum packet size of 64 bytes is maintained for Fast Ethernet.



LLC: Logical Link Control
MAC: Medium Access Control
PMD: Physical Medium Dependent

Figure 2.4 100Base-T Fast Ethernet Protocol Architecture

2.2.3 Gigabit Ethernet

With the successes of Ethernet and fiber-optic communications, the logical evolution in Ethernet technology led to the development of Gigabit Ethernet, Ethernet operating at 1 Gbps (gigabits per second). Gigabit Ethernet is one hundred times the speed of regular Ethernet, ten times that of Fast Ethernet, and faster than FDDI operating at 150 Mbps.

Along with the development of Gigabit Ethernet, a parallel task was undertaken to double the bandwidth of Ethernet by full-duplex operation. We have so far considered only half-duplex operation in the CSMA/CD scheme. We will first describe Gigabit Ethernet in the CSMA/CD half-duplex mode in this section and consider the full-duplex mode for all types of Ethernet in the following subsection.

An approach similar to that of Fast Ethernet was taken to make Gigabit Ethernet compatible with the existing Ethernet network. IEEE 802.3z protocol, whose architecture is shown in Figure 2.5, maintains the data link layer components, logical link control (LLC) and the media access control (MAC) the same, and modifies the physical layer. Physical layer architecture combines the physical interface of the high-speed FibreChannel (developed for fiber-optic communication) with that of IEEE 802.3 Ethernet frame format. It consists of four sublayers: physical medium-dependent (PMD), physical medium attachment (PMA), convergence, and reconciliation, which interfaces with the MAC layer.

Gigabit Ethernet specification initially permits use of three physical media. They are: long-wave laser over single-mode and multimode fiber, 1000Base-LX; short-wave laser over multimode fiber, 1000Base-SX; balanced shielded 150-ohm copper cable; and UTP cable, 1000Base-T.

Both short-wave (780 nanometer, light frequency) and long-wave (1300 nanometer, near-infra-red frequency) lasers are specified to be transmitted over multimode fiber, whereas only long-wave laser specification addresses transmission over single-mode fiber. There is no support for short-wave laser over single-mode fiber. This is based on cost performance. Long-wave laser over single-mode fiber (1300 nanometer laser over 9 micron fiber) can be used up to a ten-kilometer distance, whereas multimode fiber typically extends up to two kilometers. Commercially available multimode fibers are 50 and 62.5 microns in diameter with fiber connectors that can be plugged into equipment. Table 2.2 summarizes approximately the various combinations of media, mode, and drop length (one-way). Attenuation is in the range of 0.25 to 0.5 decibels per kilometer, after which regeneration or amplification may be required.

In Figure 2.5 the PMA is a serializer/deserializer that handles multiple encoding schemes of the upper convergence layer. The encoding scheme is different between optical (8B/10B) and copper media

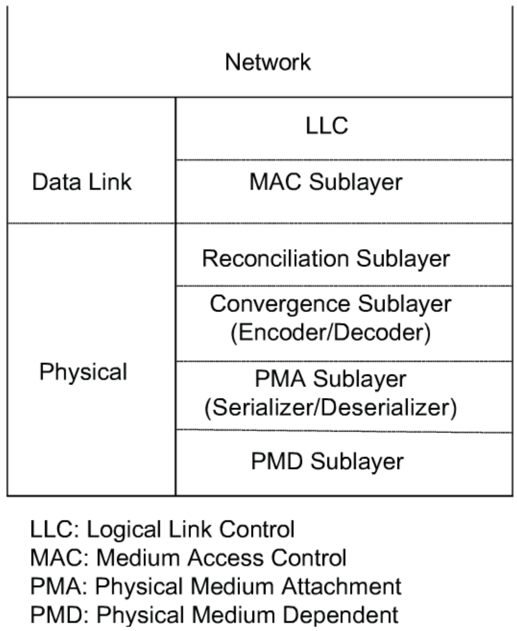


Figure 2.5 IEEE 802.3z Gigabit Ethernet Protocol Architecture

in the convergence layer. The reconciliation layer is a Media-Independent Interface (MII) between the physical media and the MAC layer of the data link control layer.

An added complication of going to 1 Gbps speed is the minimum frame size. Original Ethernet specifications, based on 2500 meters in length with four repeaters, each producing approximately a 5-microsecond delay and 10-Mbps data rate, required a minimum of a 64-byte frame, shown in Figure 2.6(a) to detect any collision. The time to accommodate the 64-byte frame is defined as the slot time, which is 51.2 microseconds. An idle time of 96 bits was allowed between frames, as shown in Figure 2.6(b). Fast Ethernet with a 100-meter drop, 100-Mbps data rate, and one repeater (minimum time each packet needs to traverse in a hub configuration) would take a little over five microseconds. Thus, a slot time of 5.12 microseconds with a 64-byte minimum frame size meets the minimum 64-byte slot size, as shown in Figure 2.6(c), to be compatible with original Ethernet specifications. A round-trip delay in Gigabit Ethernet is primarily determined by the repeater delay. To be backward compatible with original Ethernet specifications based on CSMA/CD, the minimum packet size was extended to 512 bytes, but the minimum frame size was still kept as 64 bytes. For small frames, a carrier extension was allowed, as shown in Figure 2.6(d), to increase the number of bytes in a slot to 512 bytes corresponding to 4.096 microseconds.

Table 2.2 Gigabit Ethernet Topology Limits

	9 MICRON SINGLE MODE	50 MICRON SINGLE MODE	50 MICRON MULTIMODE	62.5 MICRON MULTIMODE	BALANCE SHIELDED CABLE	UTP
1000Base-LX	10 km	3 km	550 m	440 m	–	–
1000Base-SX	–		550 m	260 m	–	–
1000Base-CX	–		–	–	25 m	–
1000Base-T	–		–	–	–	100 m

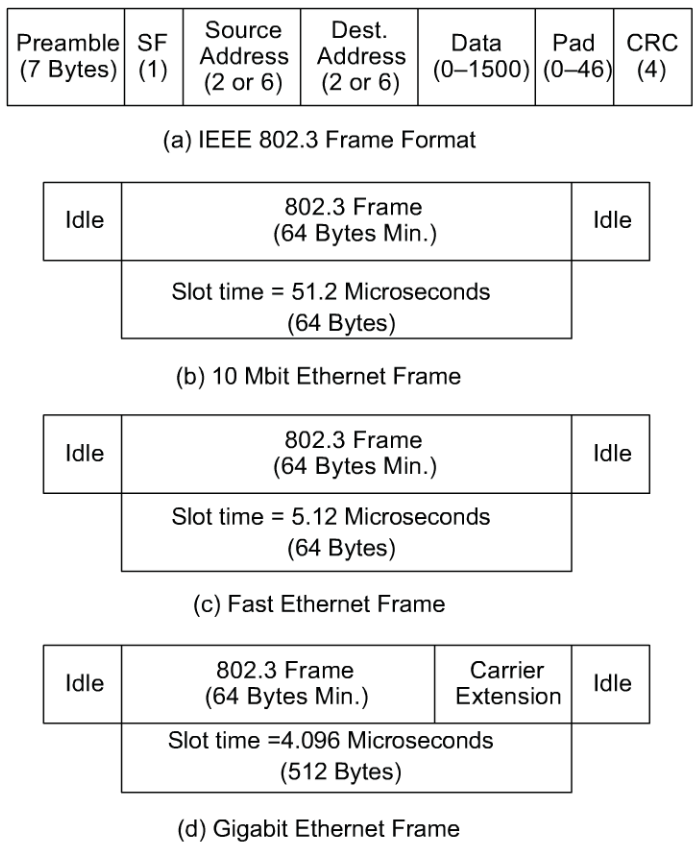


Figure 2.6 Ethernet Formats and 802.3 Frame

An additional modification was made to Gigabit Ethernet specifications to permit bursts of frames to be transmitted by a single station. This is called packet bursting. Devices could send bursts of small packets and utilize full bandwidth capacity. In such a situation, the transmitting station should not allow idle time between frames. This feature improves the efficiency of transmission, especially in the backbone configuration.

With increased data rate capability, Gigabit Ethernet can transport multimedia service that includes voice, video, and data. Quality of Service (QoS) that can establish priority of service to accomplish real-time transmission is an essential requirement for implementation of multimedia service. IEEE 802.1p specifying the class of service (CoS) meets this requirement in a limited way. In addition, Resource Reservation Protocol (RSVP) can be used for advance reservation of bandwidth for this purpose.

2.2.4 Full-Duplex Ethernet

We have so far discussed in the last two subsections increasing the bandwidth of Ethernet by two orders of magnitude by migrating from 10 Mbps Ethernet to Gigabit Ethernet. We will now discuss how data rates of Ethernet, Fast Ethernet, and Gigabit Ethernet could be doubled by migrating from a half-duplex to a full-duplex configuration.

As mentioned in the previous subsection, CSMA/CD configuration is a half-duplex operation. This means that the signal could traverse only in one direction at a given time in the cable to avoid collision with another signal. In Section 2.2.1, we gave the analogy of speaking into a hollow pipe to demonstrate the collision. Let's extend that analogy to the case where there are two hollow pipes and the sound is allowed

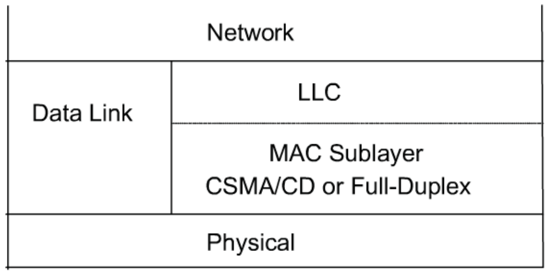


Figure 2.7 IEEE 802.3 x Protocol Architecture

to travel only in one direction. One pipe carries sound in one direction, and the other in the opposite direction. In this case, each person can be speaking on one pipe and receiving a message from somebody else on the other pipe at the same time. This analogy applies to the switched LAN where each station is connected to the hub by two channels. This is the basic concept of a full-duplex configuration. Carrier Sense Multiple Access with Carrier Detection (CSMA/CD) does not apply in this configuration.

With an active LAN implementation with repeaters and the sophistication of electronics in a hub, CSMA/CD restriction could be removed and a hub with a full-duplex operation could be implemented. IEEE 802.3x specifications, shown in Figure 2.7, were developed for this purpose. Using this scheme, the bandwidth could be doubled for each type of Ethernet configuration. Thus, the Ethernet full-duplex configuration could handle 20 Mbps, Fast Ethernet 200 Mbps, and Gigabit Ethernet 2000 Mbps. The full-duplex configuration is generally used in point-to-point communication. This feature can be turned on or off in configuring the hub. For a point-to-point link, an optional flow control feature specified in IEEE 802.3x can be exercised. The receiver can send a "pause frame" to the transmitter to control the flow in case of congestion.

Because of the 802.3x protocol extension, the notation for Ethernet type is modified with an "x" extension. Thus, 10Base-T, 100Base-T, and 100Base-F are modified to be 10Base-Tx, 100Base-Tx, and 100Base-Fx. The Gigabit Ethernet types already denoted ending in x, the option being set to either full- or half-duplex.

Limitations in Gigabit Ethernet implementation to be compatible with original Ethernet with CSMA/CD are removed in full-duplex implementation. Thus, the carrier extension, slot time extension, or packet bursting is not applicable. The Ethernet 96-bit interface gap (idle time between frames) and 64-byte minimum packet size would still apply.

2.2.5 Switched Ethernet

Another outcome of hub technology is the switched Ethernet. Instead of just the broadcast mode inside the hub, packets are opened to see the destination address and passed through to the appropriate destination port. The switch hub can be implemented as a learning device by reading the source address and thus building a routing table to speed up the process. Pairs of DTEs can communicate with each other in parallel as long as they are different DTE pairs and consequently, multiples of 10-Mbps channels are traversing the Ethernet hub at the same time. This is shown in Figure 2.8. There will, however, be a collision if a DTE receives packets from two other DTEs simultaneously and needs resolution.

Not all ports in a switched hub have to operate at the same data rate. A typical arrangement will be for one port to operate at a high data rate and will be connected to a server DTE, with other ports connected to client DTEs. A switched hub in a client–server configuration is shown in Figure 2.9 with the server operating at 100 Mbps and the clients at 10 Mbps.

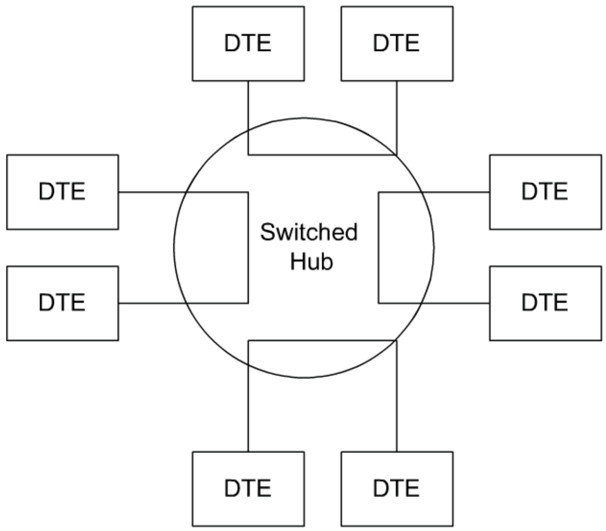


Figure 2.8 Switched Ethernet Hub

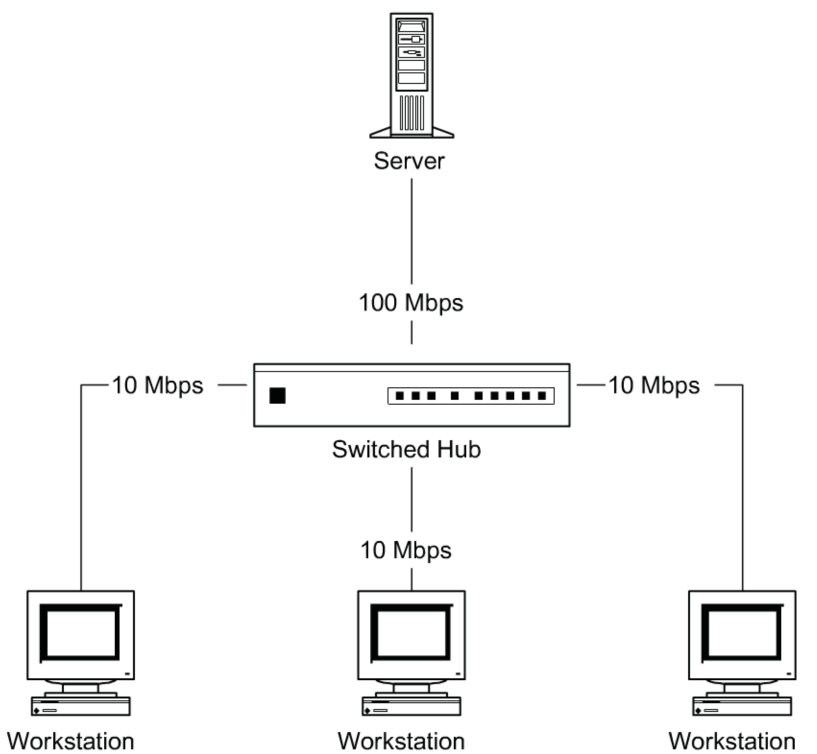


Figure 2.9 Switched Hub in a Client–Server Configuration

2.2.6 10-Gigabit Ethernet

A 10-Gigabit Ethernet or 10GbE or 10 GigE is the fastest of Ethernet standards. It combines the technology of standard Ethernet, full-duplex Ethernet, and switched Ethernet to create a LAN hub with nominal data rate of 10 Gbps over fiber, IEEE 802.3AE, and over copper UTP as specified by IEEE 802.3an standard. A 10-Gigabit Ethernet LAN does not follow the CSMA/CD protocol [Wikipedia1]. The 10-Gigabit Ethernet standard encompasses a number of different physical layer standards, with each physical port in a device supporting any of the many different modules that support different LAN or WAN PHY standards.

2.2.7 Virtual LAN

Another advantage of the switched Ethernet is the capability to establish VLAN. Using a network management system, any port can be assigned to any LAN, and thus LAN configurations can be changed without physically moving equipment. In a corporate environment, this has the advantage of grouping personnel, for example, into different administrative groups with shared LAN without physically moving their location.

As an illustration, MAC addresses for hosts in Figure 2.10 could be assigned to two different LANs. Switching occurs by the switch opening the packet received on a port, reading the OSI layer-2 MAC address, and then transmitting it on another port that may be connected to a different LAN at a different speed. We thus have switched a packet from one LAN to another, which is the function of a bridge that we will discuss in Section 2.3.2. However, it is worth noting here that the workstations that are physically connected to a switched hub belong to two LANs, each being defined as a Virtual LAN (VLAN).

The concept of VLANs is shown in Figure 2.10. The router directs all packets destined for subnets 200.100.150.1 and 200.100.160.1 to the same port on the router. They arrive at the switched hub and are routed to DTE 1 through DTE 5. Each of the five DTEs shown in the figure could be assigned an IP address belonging to either 200.100.150.1 or 200.100.160.1 and thus will be intermingled between the two VLANs. If DTE 1 and DTE 3 both belong to 200.100.150.1 VLAN, then traffic emanating from DTE 1 destined for DTE 3 would have been switched within the same VLAN. DTE 1 could be assigned an IP address 200.100.150.2 and DTE 3 could be assigned address 200.100.160.2. In this case, they belong to different VLANs. MAC addresses remaining fixed (they are assigned in the factory); the packet is now switched between the two VLANs.

Service providers now offer VLAN capability that is spread across a geographically wide area and traverses through switching offices and WAN.

2.2.8 Token Ring

Although Token-Ring LAN is a legacy LAN, we will describe it here as its ring configuration, and fail-safe redundancy aspects have been adopted in later versions of LAN and MAN, such as FDDI and RPR,

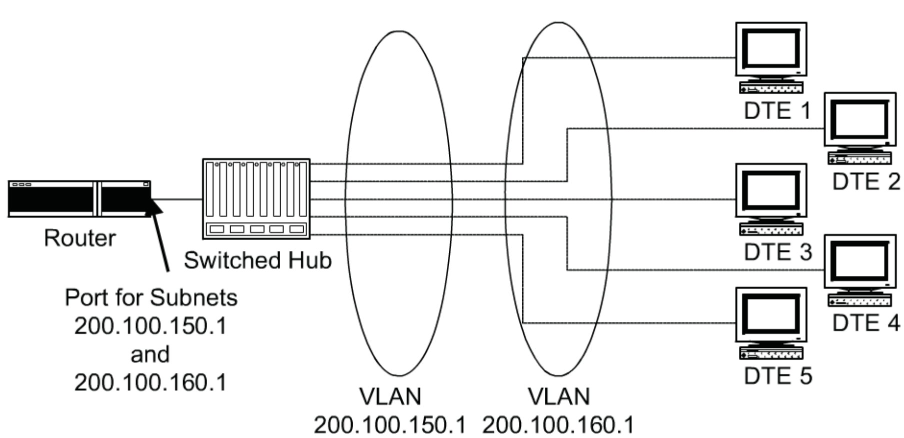


Figure 2.10 Virtual LANs

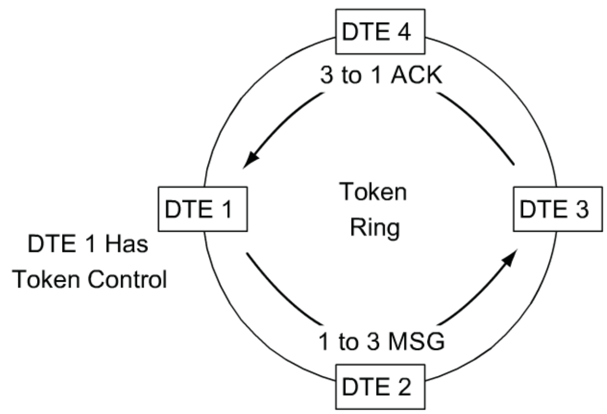


Figure 2.11 Token-Ring LAN

respectively. Token Ring uses the ring topology and is specified by IEEE 802.5 protocol. There is no segment length limit as in Ethernet LAN. All DTEs are connected in a serial fashion in a ring shown in Figure 2.11.

A token is passed around (counterclockwise in Figure 2.11) in a unidirectional mode; and the DTE that has the token is in control of the LAN. Let us consider in Figure 2.11 a situation where DTE 4 has just completed transmission of a message and has released the token. DTE 1 is waiting to pass a message to DTE 3. As soon as the token is received, DTE 1 holds on to the token and transmits its message to DTE 3. The message has the source and destination addresses. DTE 2 looks at the destination address and does not pick up the message. DTE 3 examines the destination address, and realizes that the message is for itself. It then picks up the message and retransmits it with acknowledgment marked in the trailer of the message format. The frame goes around to DTE 1 with DTE 4 just passing the message through. Recognizing that the message has been received, DTE 1 releases the control token and now DTE 2 has a chance to send a message. If the message was not accepted by DTE 3 for any reason, such as a corrupt message, then the message trailer is so marked and appropriate action is taken by DTE 1.

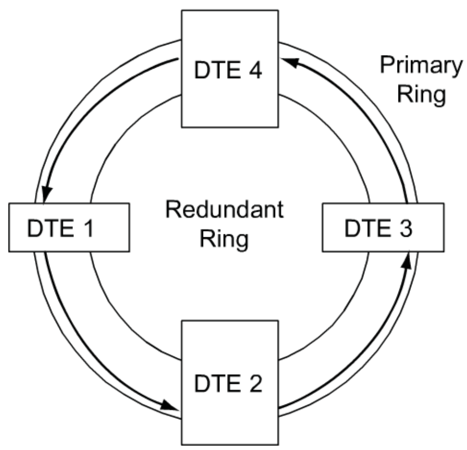
As can be seen, in the token-ring LAN, MAC is deterministic in contrast to the probabilistic nature in Ethernet LAN. Standards that specify token-ring MAC are IEEE 802.5 and ISO 8803.5. This is good configuration for heavily loaded networks.

The maximum size of a frame is not limited by the 802.5 standard. However, in order that no one station monopolizes the ring, the maximum token holding time by any station is configured, which determines the maximum frame size. The minimum frame size is the size of the token. The ring should be long enough to accommodate the entire token; otherwise, the token starts wrapping itself around and all the stations are in an idle mode.

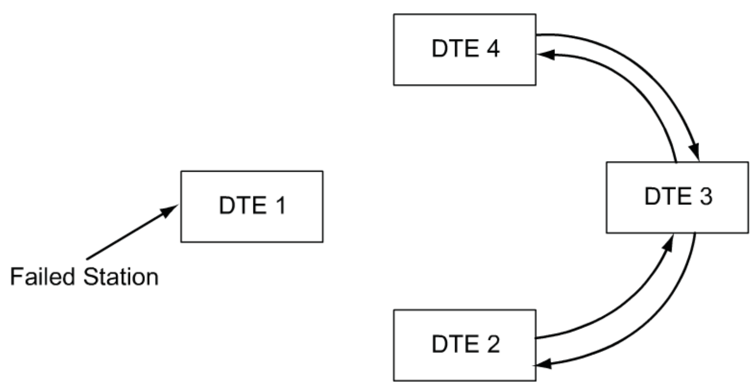
Because of the serial configuration, it is important that any failure of DTE, or turning the DTE off, should not halt the operation of LAN. One scheme to prevent this failure is to design the Token-Ring NIC to create a short whenever there is a failure or it is turned off. This is analogous to serially connected Christmas tree lights. When one bulb burns out, the bulb shorts the connection so that the rest of the lights continue to be lit.

If there is a break in the link segment of the ring, the downstream DTE sends a beacon to the others indicating a failure. For example, if the link between DTE 4 and DTE 1 breaks, DTE 1 will send the beacon.

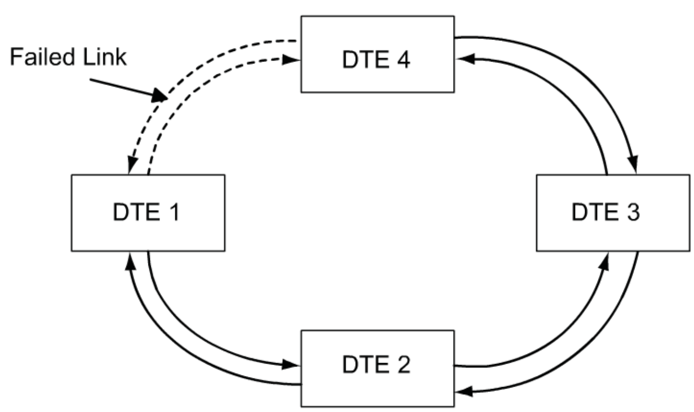
Ring failure can be permanently resolved by a dual-ring configuration, where the second ring is redundant, as shown in Figure 2.12(a). Let us assume that the normal mode of operation is along the inner ring and the token is going around in the counterclockwise direction. The outer ring is the redundant ring and acts as backup. Figure 2.12(b) shows the situation where DTE 1 has failed. DTE 2 does not receive



(a) Token-Ring Dual-Ring Management



(b) Token-Ring DTE Isolation



(c) Token-Ring Segment Isolation

Figure 2.12 Token-Ring Dual-Ring Configurations the signal from DTE 1. DTE 2 will send a beacon. Under this condition, DTE 2 and DTE 4 go into a loop-back condition. DTE 4 receives the token on the inner ring and forwards it on the outer ring to DTE 3. DTE 2 receives the token on the outer ring and forwards it on the inner ring.

Figure 2.12(c) shows the situation where the section of the ring between DTE 4 and DTE 1 is broken. DTE 1 sends a beacon. DTE 4 and DTE 1 perform loop-backs and the continuity of the rings among all four stations is established using both inner and outer rings.

2.2.9 FDDI

Fiber Distributed Data Interface (FDDI) LAN came into being to take advantage of fiber-optic transmission media for LAN technology. It operates at a data rate of 100 Mbps and can include up to 500 DTEs in a single segment of 100-kilometer length without repeaters. Separation between neighboring stations on the cable can be up to 2 kilometers. A fiber-optic cable has the advantage of low-noise interference compared to copper cable, and hence FDDI is ideally suited for a campus backbone network. As mentioned earlier, FDDI is configured as a ring topology and has a token for medium access control. Thus, it follows IEEE 802.5 token-ring standard, but with some significant differences. It is adopted as an international standard by ISO 9314 and American National Standards Institute (ANSI) H3T9.5.

Figure 2.13(a) shows the network configuration of FDDI. It is usually implemented as a dual ring for high reliability. One ring is termed as primary and the second one as secondary. Stations can be connected to the ring either as a single attached station (SAS) to the primary ring, or as a dual attached station (DAS) to both rings. A hierarchical topology can be created using concentrators, as shown in Figure 2.13(b). Concentrators permit the attachment of only SASs, but are economical for wiring and expansion of the FDDI network.

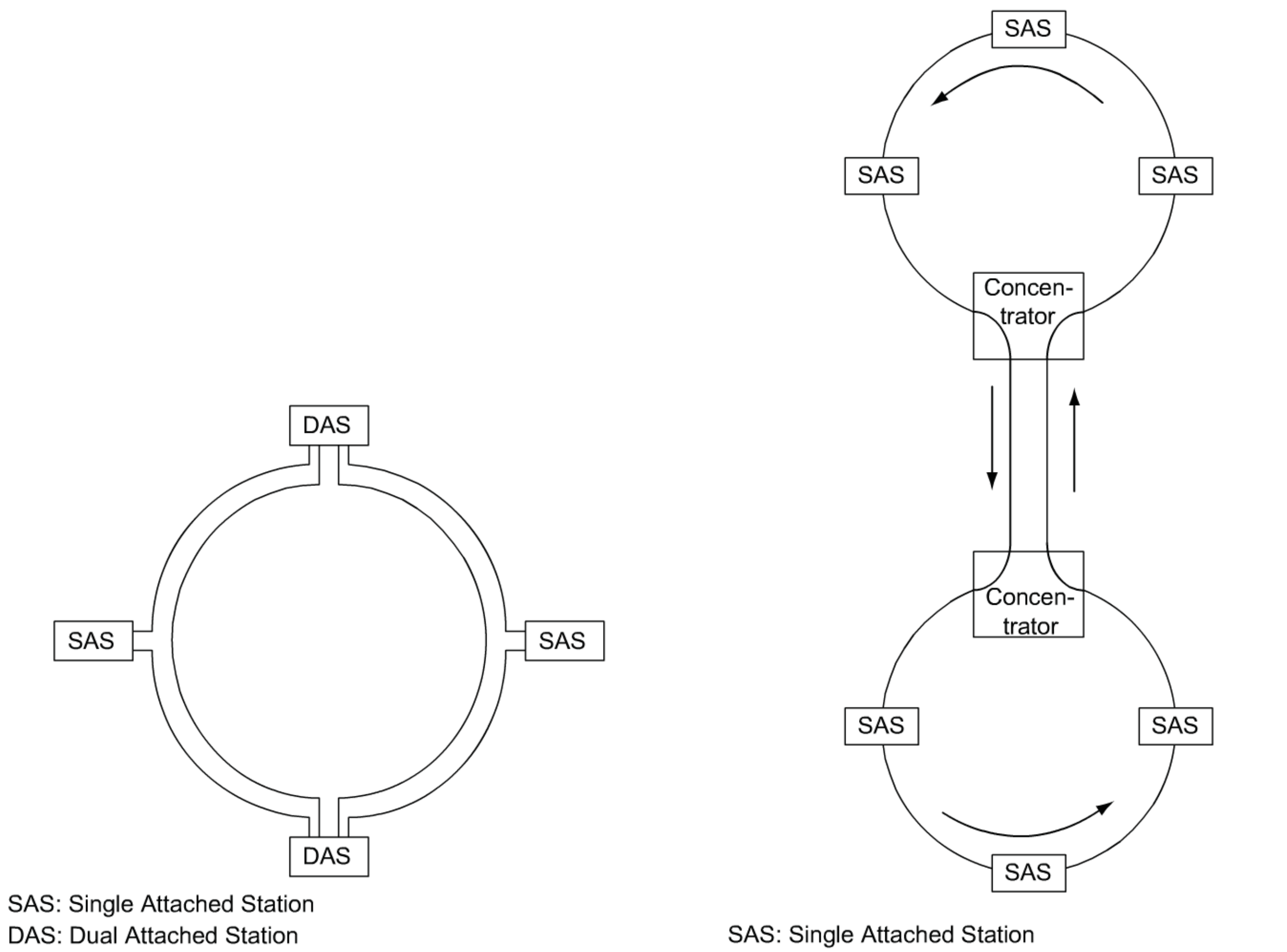
Although the topology of FDDI is similar to the Token Ring, the control token-passing algorithm is different. In the Token Ring, only one DTE utilizes the ring at any given time, whereas in FDDI there can be many frames traversing the ring with communication between multiple pairs of stations.

2.2.10 Wireless LAN

Wireless LAN (WLAN) growth has been very rapid and is being deployed at homes, enterprises, and public places. WiFi, as it is popularly known, is an IEEE 802.11 protocol LAN. 802.11b and 802.11g operate at a 2.4-GHz band and 802.11a operates at a 5-GHz band. IEEE 802.11 working groups have been making amendments to 802.11 to address scalability, provisioning, performance, QoS, and security issues. We will address these along with management issues in Chapter 15 on Home Networking.

The prevalent configuration for deployment of WiFi is a hierarchical configuration, also known as infrastructure configuration. This is shown in Figure 2.14. WLAN may be visualized as a wireless interface to a wired network. Thus, in Figure 2.14, the Access Point (AP) converts the IEEE 802.3 Ethernet protocol on a wired medium to IEEE 802.11 WiFi protocol over a wireless medium. The wired interface is connected to the external network via either a router or a layer-2 switch.

Stations 1, 2, and 3 in Figure 2.14 can be either fixed or mobile or any combination. A typical configuration in a laptop computer is either a removable interface card or built in. Communication between wireless stations passes through the AP, which is also the controller. The range of WiFi is limited, and the area that is under the control of an AP is called the basic service area. The stations associated with a basic service area are usually connected by a wired network to another basic service area.



(a) Dual-Ring FDDI Network Configuration (b) FDDI Configuration with Concentrators

Figure 2.13 FDDI Configurations

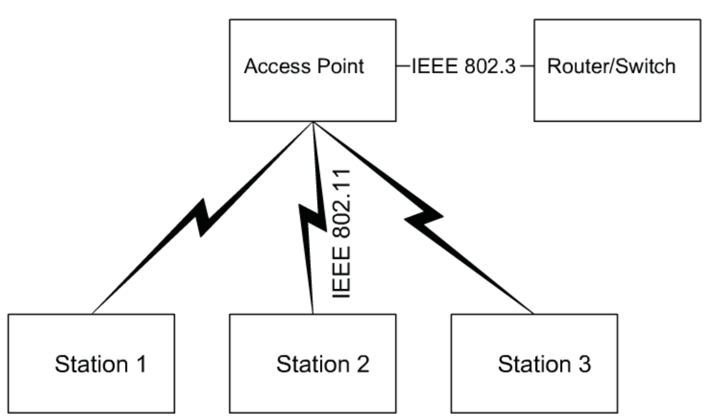


Figure 2.14 Wireless LAN: Hierarchical Topology

A second WLAN topology is the ad hoc network configuration. In this configuration, wireless stations communicate with each other on a peer-to-peer level with one of the stations acting as the controller, or a beacon as it is called.

2.3 NETWORK NODE COMPONENTS

A network node is a component at either end of a network link, such as a hub or a router. It is also a device that connects two networks, such as a bridge connecting two LANs, or a gateway connecting two autonomous networks. Resources for network node are hubs, switches, bridges, routers, and gateways, or a combination of the above such as a brouter (bridged router) and a switched hub. A DTE, such as a workstation, is not considered a node. However, a workstation that has two network interface cards (NICs) connecting to two LANs is a bridge and is considered a node. Hubs are platforms housing one or more functions. Switches now use solid-state devices. Progress in solid-state technology has contributed to the advancement of switching technology that includes an ATM switch. Other network nodes are smart switches with built-in intelligence of various degrees.

In a simplistic view, a node can be looked at as a switch, a bridge, a router, or a gateway. The basic concepts of the four primary nodal components are shown in Figure 2.15. Figure 2.15(a) shows a switch, where inputs and outputs are of the same format. For example, if the input format is an ATM format, the output is also an ATM format. The switch can be used to switch both analog and digital data. When used in the analog mode, as in circuit switching, a call is set up first (connection through the switch is made) and then the analog signal is passed through. The switch is insensitive to the information content. When it is used in the digital mode, it is used as a packet switch. Each input packet is looked at and then switched to the appropriate output port based on content.

A bridge can be viewed as an intelligent packet switch at the data link layer and is shown in Figure 2.15(b). Besides switching input packets to appropriate output ports, it can filter those packets as well. This is useful for connecting two LANs. If traffic is pertinent to the LAN only, it is filtered out. If it is to be delivered outside the LAN where it was generated, then it is switched through the bridge. In an intelligent bridge, knowledge can be learned over time by the bridge as to which packets should be delivered to which ports. Input and output protocols, in practice, are usually the same. However, some bridges can also do protocol conversion, as we will learn in Section 2.3.2.

A router cannot only do all the functions of a switch and a bridge but also route packets to the appropriate port in the correct direction of its destination. It functions at the network layer. Thus, in Figure 2.15(c), input packets from a node in an IP network are sent out as IP packets to another node in the same network or to some other network.

Not all networks use the same protocol. In this case, a gateway is used to convert one protocol format to another protocol format. In Figure 2.15(d), a gateway is shown between an IP network and an X.25 network.

2.3.1 Hubs

Figure 2.16 shows the role of various components in a network. The router, the gateway, and the half-router function at the network layer and route packets. Bridges, local and remote, operate at the data link layer and connect two LANs. Hubs are used to build LANs as we learned in the previous section. We will review various network components in this section.

As mentioned earlier, a hub is a platform with multiple ports. It is implemented to perform some specific functions or a combination of functions. For example, it could house a simple LAN or multiple LAN segments. It can perform a switching function and thus act as a switched LAN. When it switches between LANs, it performs a bridge function. In this section, we will consider a hub used to implement LAN.

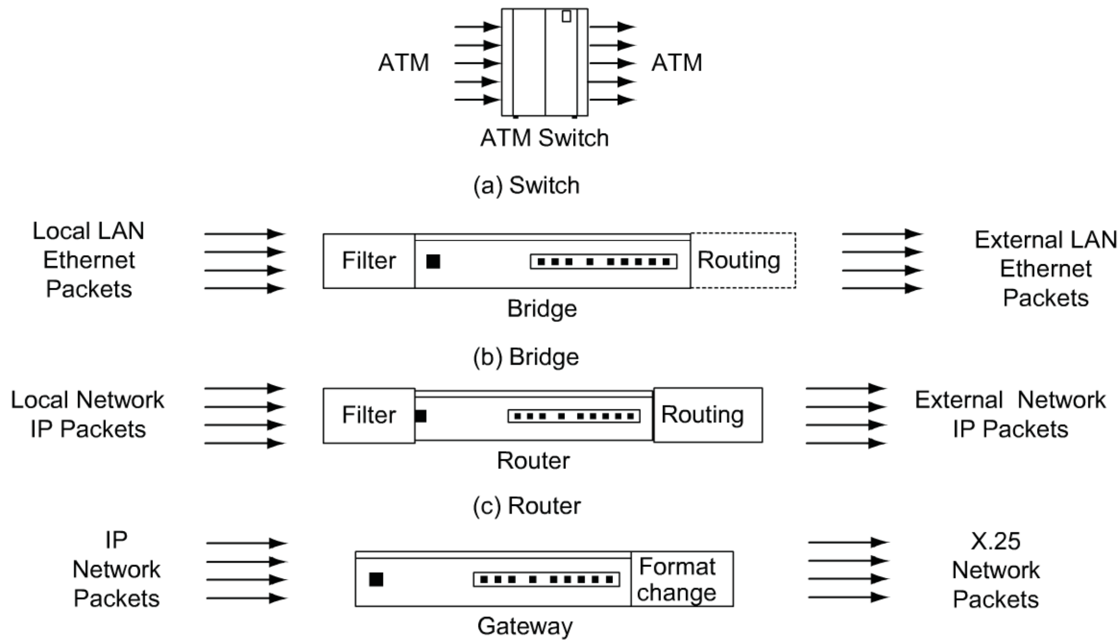


Figure 2.15 Basic Network Node Components

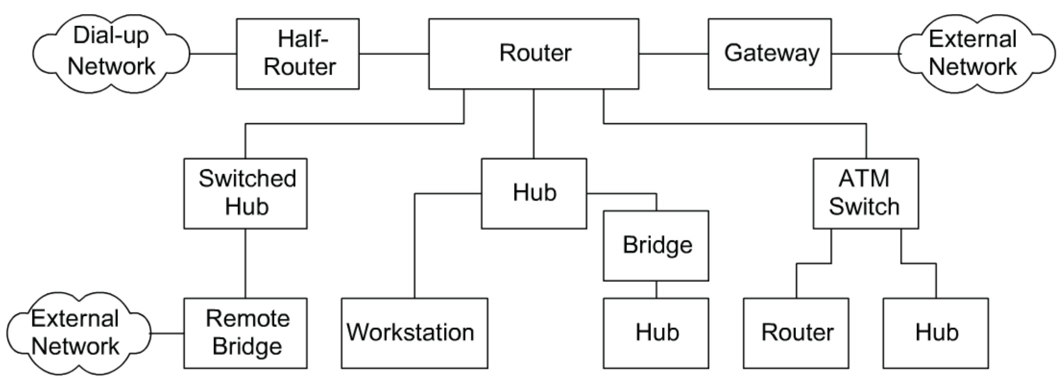


Figure 2.16 Networked Components

Hubs can be looked at as active LANs—DTEs connected with repeaters in a LAN configuration. Limitations of length and number of stations that are imposed on LANs are overcome by “homing” the wiring from the DTEs to the hub in the wiring closet and connecting them in the topology desired. The only limitation is the drop length from the hub to the station, such as the 100-meter maximum length in Ethernet configuration. Any DTE can be connected to any port of the hub. Stacking hubs and daisy chaining them can increase the number of ports. DTE configurations can be changed from a centrally located hub. Further, any DTE could easily be disconnected from the LAN for troubleshooting without impacting the operation of other stations.

Hubs can be stacked to increase the number of ports as shown in the stacked hub configuration in Figure 2.17. Stackable hubs have a common backplane. Thus, it is equivalent to increasing the number of ports in a hub. For example, two 16-port hubs will behave as a 32-port hub.

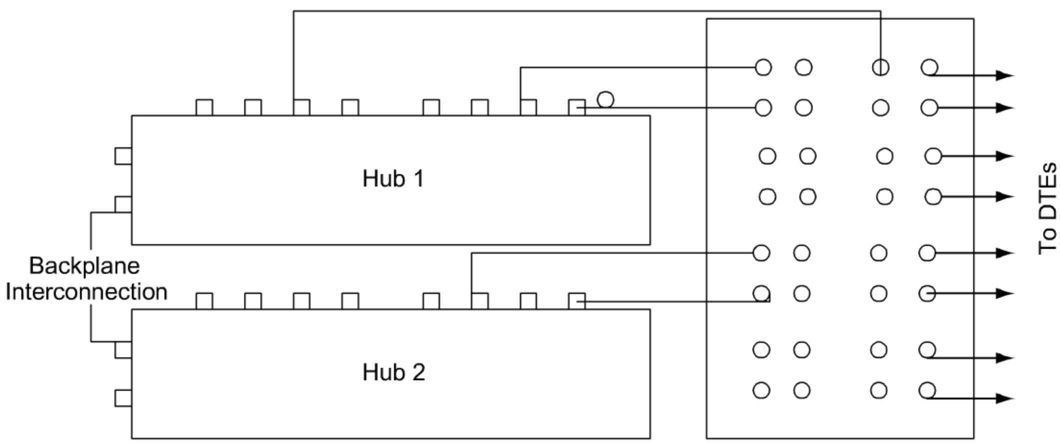


Figure 2.17 Stacked Hub Configuration

2.3.2 Bridges

Bridges are used to interconnect LANs. Three types of local bridges connecting two LANs are shown in Figure 2.18. Figure 2.18(a) shows a simple bridge configuration connecting two Ethernet LANs. This configuration can be looked at as two LANs connected by a repeater, except that now traffic among DTEs in one LAN does not go over to the other LAN. The only traffic that is exchanged between the two LANs via the bridge is that which requires inter-LAN communication. Figure 2.18(b) shows several LANs connected by a multiport bridge. In this case, the bridge opens the packet, reads the MAC address, and switches the packet to the appropriate port that is the path to the destination address. Usually the bridge is a self-learning bridge. It looks at all the packets that are received and records the source address and the port where it was received in a table. It uses this table to transmit packets. If a destination address is not in the table, it does a flooding on all ports and discovers the correct port to add to the table. The table is periodically (less than a few minutes) purged of inactive addresses.

A bridge switches data packets between LANs and to accomplish this has a store-and-forward capability. Local bridges are usually developed as a single protocol device, and have the primary features of switching and filtering out intra-LAN traffic. However, because of the store-and-forward capability in a bridge, additional features could be incorporated to convert protocol. Figure 2.18(c) shows a multiport, multiprotocol bridge configuration, where Ethernet and token-ring LANs are interconnected. Protocol conversion is done at OSI layer 2.

2.3.3 Remote Bridge

Figure 2.18 shows bridges in local LAN configurations. This implies that LANs are brought to a centralized wiring closet and are interconnected via a bridge. Figure 2.19 shows a remote bridge configuration, where two bridges at remote locations are linked via a WAN. WAN architecture mostly uses routers. However, using a remote bridge and a leased dedicated telecommunication link, we can connect remote LANs.

LANs can be connected with bridges that are networked using either the tree topology or the mesh topology. Bridged networks operate at the data link layer. There are two network-routing algorithms used in bridged networks—the spanning-tree algorithm for bridging Ethernet LANs and the source-routing algorithm for bridging token-ring LANs.

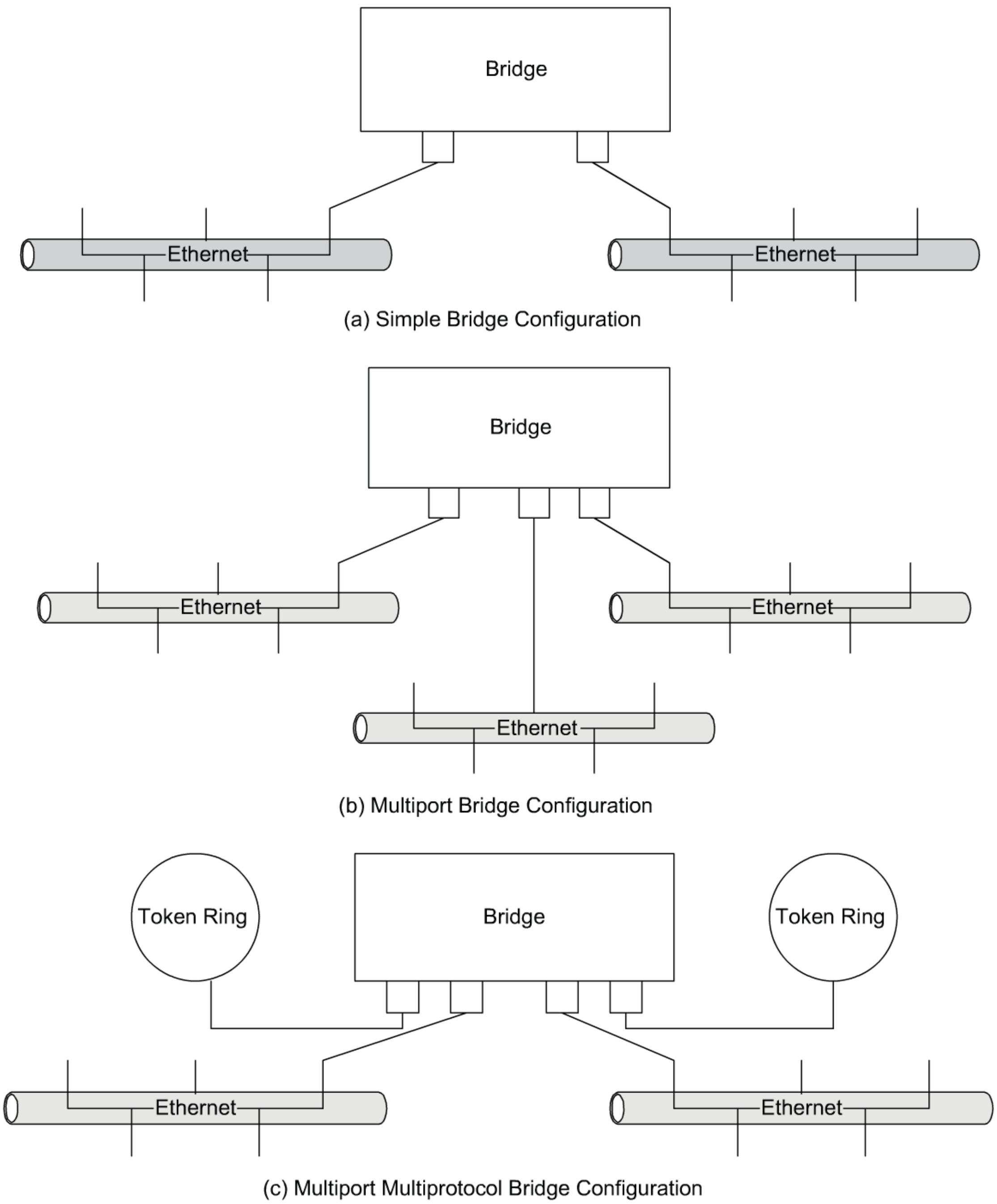


Figure 2.18 Local Bridge Configurations

2.3.4 Transparent Bridge

Figure 2.20 shows four LANs networked using three bridges in a tree topology. Each bridge has knowledge only of its neighbor and is transparent to other bridges and LANs, as described below, hence the name transparent bridge.

The transparent bridge uses a routing algorithm, called a spanning-tree algorithm. A spanning-tree algorithm builds and stores a table of ports associated with destination addresses. When a packet

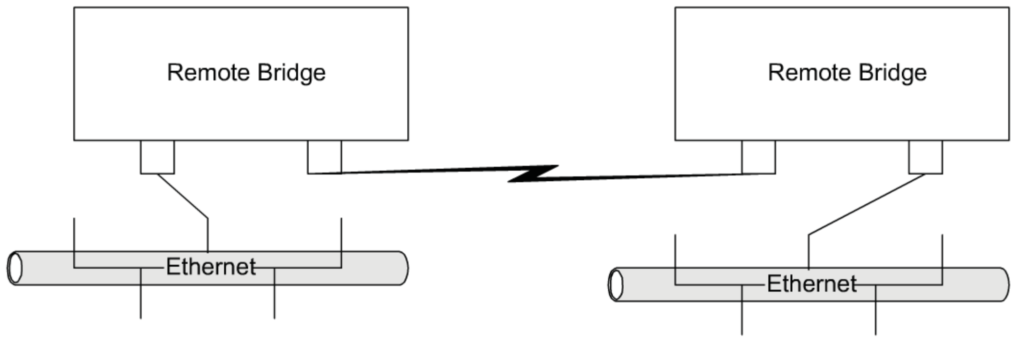


Figure 2.19 Remote Bridge

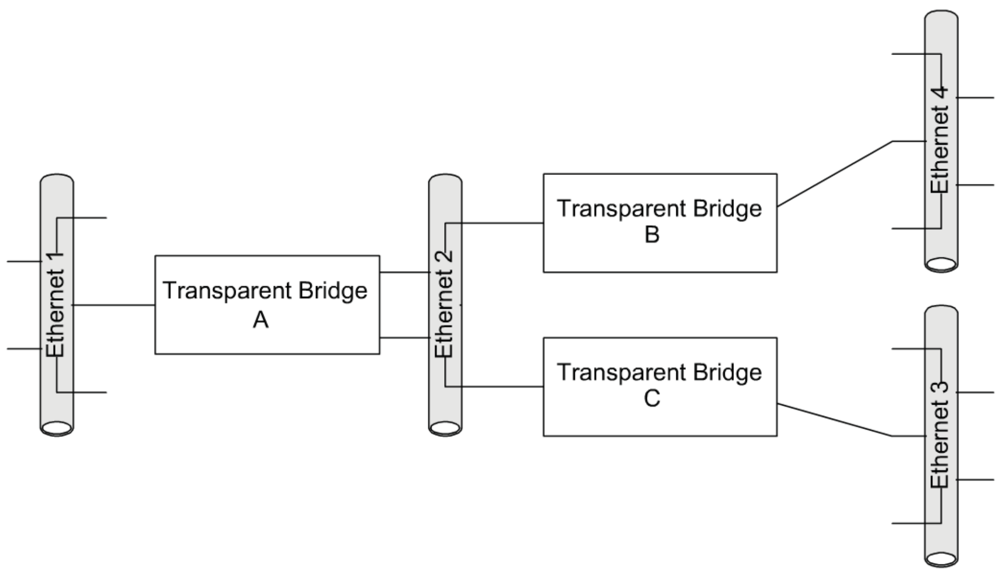


Figure 2.20 Transparent Bridge Network

arrives, the bridge sends the packet on another port to its destination. The bridge has no knowledge as to exactly where the destination LAN is. It only has knowledge of the neighboring node responsible for that destination address.

The transparent bridge learns routing information by a backward learning process. That is, when a packet arrives at a port, it notes the source address of the packet and associates that address with that port in its routing table. It then forwards the packet to the port associated with that destination. If the destination address is not in its routing table, it does a broadcast message to acquire the address.

As shown in Figure 2.20, the topology of the transparent bridge network is the tree topology, which means that there are no closed loops. One of the nodes acts as the header node, which is transparent bridge A in the figure. Although there may physically be more than one path between two LANs, the spanning-tree algorithm eliminates all but one link during the operation. For example, if transparent bridge B had links to both Ethernet 3 and Ethernet 4, then that would form a closed loop, Ethernet 3–transparent bridge B–Ethernet 2–transparent bridge C–Ethernet 3. The spanning-tree algorithm would prevent transparent bridge B from sending or receiving packets on its link to Ethernet 3.

Let us track a message from a host attached to LAN 3 sending a message to LAN 4. It takes the path all the way up the tree to the header bridge A, and then traverses down the other half of the tree to LAN 4. Thus, the header bridge normally needs to handle more traffic than other nodes.

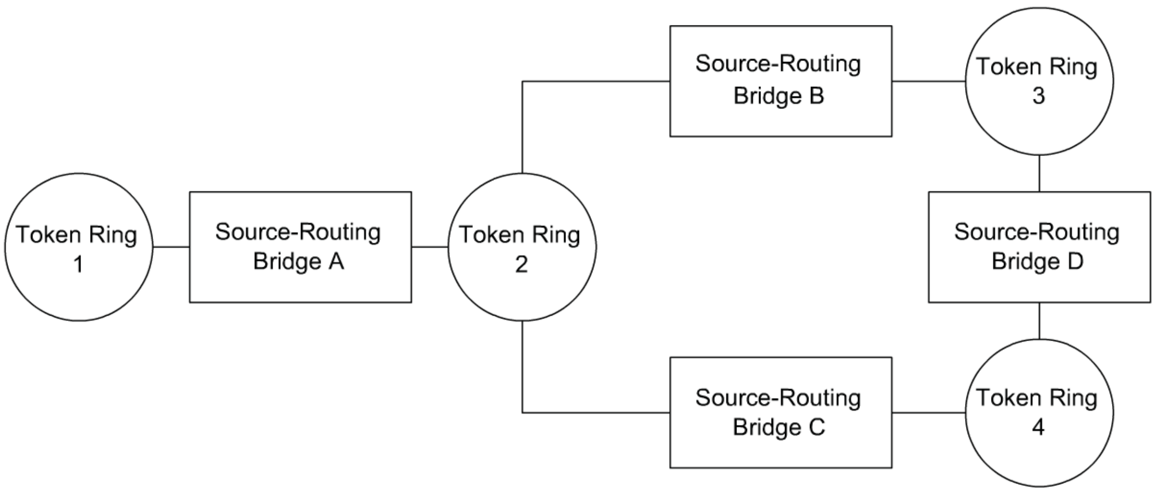


Figure 2.21 Source-Routing Bridge Network

2.3.5 Source-Routing Bridge

A source-routing bridge is used to network token-ring LANs, as shown in Figure 2.21. In the source-routing algorithm used in a bridged token-ring network, the source is aware of the entire path to the destination. In addition to the destination address, the source inserts the route that the packet should take in the packet. Thus, intermediate nodes make no decision as to the path that the packet takes. This is the reason that the token-ring bridge is called a source-routing bridge. The routing table can be stored either centrally on a server or in each source-routing bridge. The route is determined by broadcast packets flooding the entire network.

Comparing a source-routing bridge with a transparent bridge, the latter is more robust and reliable, whereas the former is faster. Thus, changes in the network due to addition or deletion of hosts, or due to failures, are tracked easier than in a source-routing bridge. In a source-routing bridge, the entire routing table has to be rediscovered, which is a heavy resource-consumption process.

Bridges are used for special-purpose networks and have several limitations. Due to dissimilarity in the routing algorithm, communication between media using different protocols becomes difficult, for example between Ethernet and Token Ring or FDDI. Besides, routing algorithms are difficult to create and to maintain. Routers, which operate at the network layer, are designed for routing and hence are better suited for this purpose. Routers and gateways can route packets between different media and different networks (using different network protocols) in a transparent manner. We will now discuss the role of routers in networking.

2.3.6 Routers

Routers and gateways form the backbone of networking. Although we have shown alternative ways of networking with bridges in the previous section—sometimes cheaper and a short cut to establish enterprise networking—the clean approach to establishing computer networks is with the use of routers.

A router, as the name indicates, routes packets through the network. Each router in a computer network has some knowledge of possible routes that a data packet could take to go from the source to the destination. It has the high-level data on what is the best overall route, as well as detailed local data on the best path for the next hop in the link. This is built into a routing table that it periodically updates

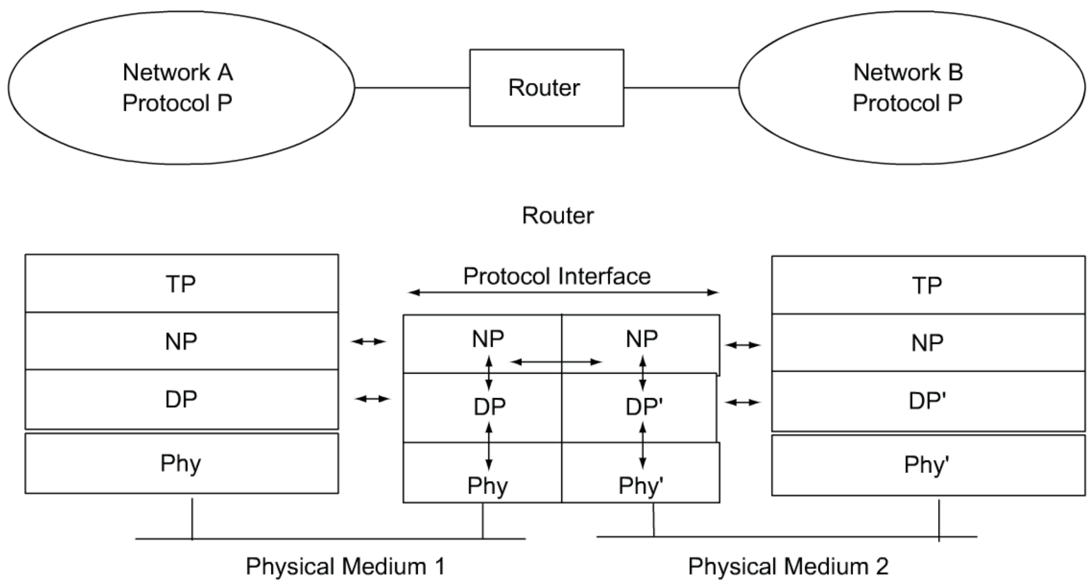


Figure 2.22 Router Configuration

and stores in its database. The router employs a broadcast scheme using an Address Resolution Protocol (ARP) to determine the port associated with destination addresses. The router may also read the contents of a data packet arriving at a given port to determine its source and destination address, as well as what type of data it is and when it was received. It then, using the routing table, intelligently routes it to one or more output ports toward its destination address. The output goes to a single port if it is a data packet going between a source and a destination; or the output is directed to multiple ports if it is a broadcast or multicast type of packet. Figure 2.22 shows a router configuration with protocol architecture. Notice that network layers have the same protocols (NP). However, the data link layer protocol (DP) and physical layer protocol (Phy), as well as the physical media 1 and 2, could be different.

Routers permit loops in their topology and thus are more universal than bridges. This enables load balancing of traffic as well as self-healing of the network in case of a link or router failure. Routers have various algorithms to optimize load balancing of traffic and economize on cost. Several routing algorithms are in use. Of those, open shortest path first (OSPF) is the most widely used. In this algorithm, each router broadcasts route–request packets on the links that it is connected to. Other routers in the network acknowledge the request and repeat the process. Thus, a distributed routing database is built using an algorithm for the shortest path and is kept updated whenever there is a change in network configuration.

Network managers can build routing tables for optimizing their network performance with respect to several parameters, such as least-cost route, delay, bandwidth, etc. The performance of a bridged network is better than a router network due to the additional network layer in the latter case. Hence, a bridged network is used in some special applications where speed is of importance. However, routers are specifically designed based on a network layer, whose main purpose is networking. Thus, degradation in performance using routers over bridges is a small price to pay for the far-reaching benefits we achieve.

2.3.7 Gateways and Protocol Converters

A gateway connects two autonomous networks. Each autonomous network is self-contained in all aspects—routing algorithms, protocol, domain name servers, and network administration procedures and policies. When such an autonomous network communicates with another autonomous network, it

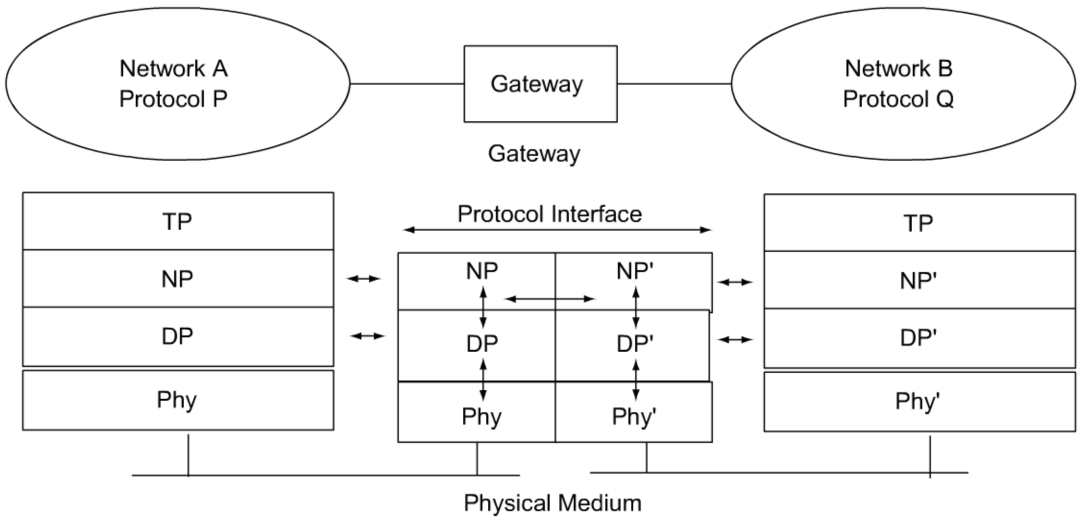


Figure 2.23 Gateway Configuration

traverses a gateway, as shown in Figure 2.23. Generally, the protocol conversion is done at the network layer as shown in the figure.

Since protocol conversion for a gateway is done at the network layer, it could generally be combined with a routing function. Thus, a router with protocol conversion could also be considered a gateway. Node N in Figure 1.16 that connects an IP network with a proprietary subnetwork is an example of this. Node N not only does protocol conversion, but also has the routing table containing information on both networks. In this scheme, Node N would have an IP address, but nodes N1, N2, and N3 may follow a proprietary addressing scheme.

A protocol converter, shown in Figure 2.24, does protocol conversion at the application layer. The protocol converter used to be distinguished from a gateway, but this is no longer the case. Gateway

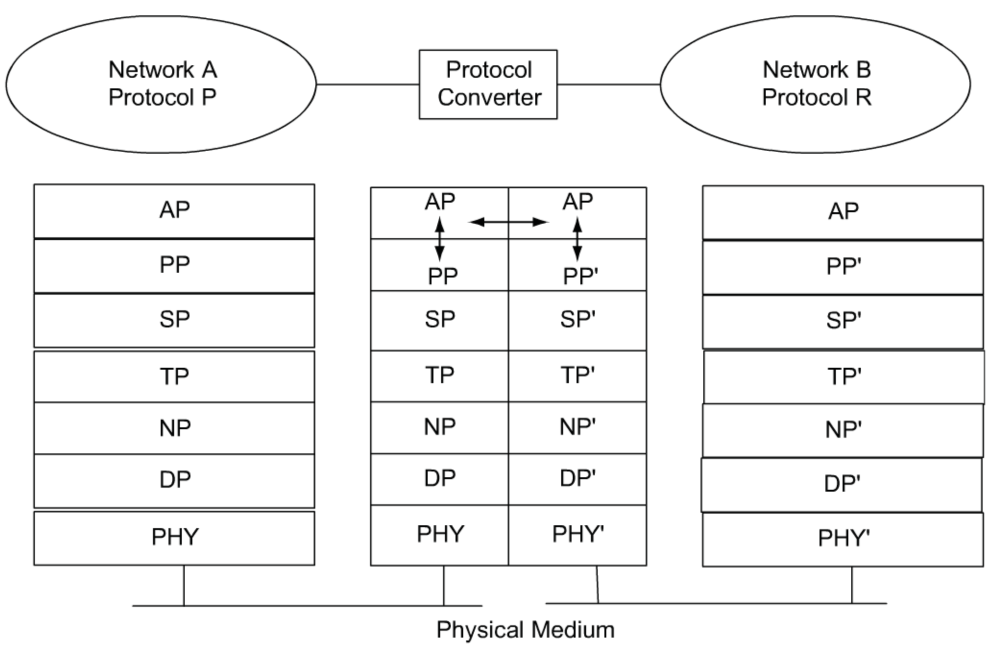


Figure 2.24 Protocol Converter Configuration

is the generic term that is currently in vogue. An example of this would be a protocol converter that would be used between two email systems. Let us consider a company that uses X.400, an ITU-T messaging system. When a person wants to send an email on the Internet to another person, who is using Internet standard Simple Mail Transfer Protocol (SMTP), a protocol converter (gateway) converts X.400 protocol to SMTP.

2.3.8 Multiprotocol Routers and Tunneling

An alternative to the use of gateway to communicate between autonomous networks is tunneling using multiprotocol router. Tunneling is generally used when the source and destination stations are on similar networks, but the data have to traverse intermediate network systems, which may be using different protocols. In this case, the data frame does not go through a protocol conversion in the intermediate networks, but is encapsulated and "tunneled" through as pass-through traffic.

Figure 2.25 shows communications between two Ethernet LANs on IP networks. One of them could be in the USA and the other in India. However, the data have to go through Europe, which is on a X.25 packet-switched data network. The multiprotocol router at the near end encapsulates the IP packet in an X.25 frame and transmits it to the far-end multiprotocol router. The far-end multiprotocol router de-encapsulates the frame and routes it as an IP packet again. The path through Europe behaves very similar to a serial link.

Another application for tunneling is when a station with an IP address belonging to a LAN wants to communicate with another LAN in a distant location, but from a location other than the local LAN. This would be the situation if the station were a portable PC and the person traveling needs to communicate from a foreign location. Let us picture the scenario where Joe wants to communicate from Seattle in northwest United States to Sally at Los Angeles on the West Coast of the United States. Joe's PC belongs to a network domain in New York, which is in the East Coast of the United States. The initial message is routed to the server of the LAN that the station belongs to, in this case New York. The server, recognizing that the station is currently outside of its domain, locates the foreign agent who handles the domain that Joe is currently at and informs Joe and the foreign agent. From then on, the sender "tunnels" the packets directly to the user via the foreign agent.

2.3.9 Half-Bridge Configuration of Router

There are situations where it is desired to have point-to-point communication. For example, when a residential station communicates with an Internet Service Provider (ISP), Point-to-Point Protocol (PPP) could be used. It provides a standard method for multiprotocol datagrams over point-to-point links. This method of communication has been extended to PPP Multilink Protocol (MP). Using MP, datagrams

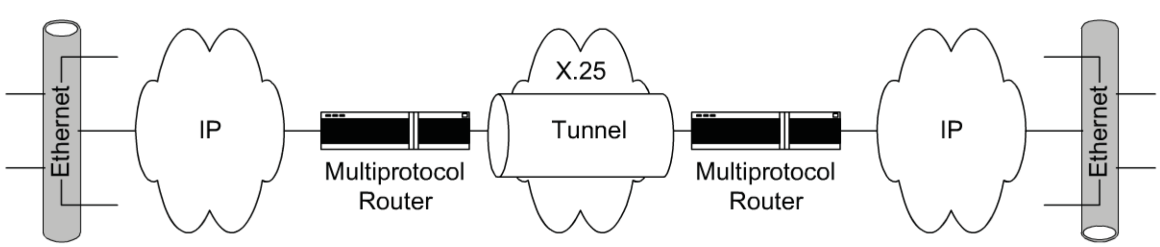


Figure 2.25 Tunneling Using Multiprotocol Routers

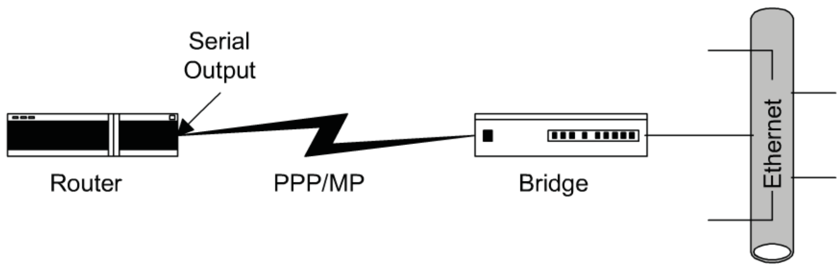


Figure 2.26 Half-Bridge Configuration

could be split, sequenced, transmitted over multiple parallel links, and recombined to construct the original message. This increases the bandwidth and efficiency of point-to-point link communication.

With the expanding universe of the Internet, there are small corporations, as well as small ISPs, who would like to establish dial-up serial links. They require connections to the Internet from their local LAN only when they need them. Typically, they do not need permanent dedicated links. A number of proprietary PPP protocols are currently in use. The most common protocol is the Serial Link Internet Protocol (SLIP) for UNIX. IETF has standardized the Internet DP to be used with point-to-point links. Half-bridge provides a method to connect the LAN via a bridge to a router.

Figure 2.26 shows a half-bridge configuration. The router port connecting to the bridge is configured as a serial interface to the PPP half-bridge. The interface functions as a virtual node on the Ethernet subnetwork on the bridge. The serial interface has an IP address associated with the Ethernet subnetwork. Thus, if the Ethernet subnetwork address is 155.55.123.1, the serial interface on the router could be assigned an IP address 155.55.123.5.

When a packet destined to the Ethernet arrives at the router, it is converted to Ethernet packets, encapsulated in PPP frames, and sent on the Ethernet bridge link. In the reverse direction, Ethernet packets encapsulated in PPP frames are extracted by the router, which converts them to IP packets, and routes them on the Internet.

2.3.10 Edge Routers

Edge routers may in general be considered as those elements that perform routing functions at the edge of a network. In other words, they are ingress and egress network elements of a typical WAN. Depending on the application, the functions of this router vary. For example, if it is an edge router to access network, it needs to handle the “triple play” function of real and non-real time traffic. If it is for an MPLS application, it serves the function of an MPLS edge router, which we will learn more about in Chapter 12.

2.3.11 Switches

It would have been logical for us to start reviewing the switch component before we discussed bridges and routers as network components. However, we have chosen to delay its discussion up to now for a good reason, as it logically flows into discussing WANs.

Switches operate at the physical layer of the OSI Reference Model that we discussed in Section 1.5.1. In Section 2.3 we described a switch as a component that makes a physical connection between input and output ports and that the bits and bytes coming in go out exactly the same way. Bridges and routers use the switching function when they route packets.

Most switching technology is based on solid-state technology, and the speed of switching is getting faster and faster. This enables networks to achieve a digital rate of gigabits per second. The performance of a network is determined by how fast we can switch and multiplex data using switches (and consequently in routers and bridges). More importantly, end-to-end performance of the network depends on the speed, latency, and latency variation in transporting data from the source to the destination. Voice, video, and data have different quality-of-service requirements. Based on these requirements, different types of end-to-end circuits are established using switches.

The switching function accomplished in establishing circuits can be classified into circuit switching and packet switching depending on how it is used. Telephone communication uses circuit switching. A physical path from end-to-end is established prior to talking, which is termed call setup. During the actual telephone conversation, the path remains connected whether there is a conversation actually happening or not. That is, the allocated bandwidth for the path is wasted during the idle time of the conversation. Thus, when you are on the telephone and the other party gives you a telephone number, you may say "Please wait while I get a paper and pencil to write." The facilities remain idle during that time and could have been used by others. A "nailed up circuit," where a permanent path is established for the session, is good for voice and video communications where latency and latency variations are intolerable.

Computer traffic is bursty in nature and lends itself more to packet switching. It would be a waste of bandwidth to use circuit switching for computer data networks. Packet switching utilizes the facilities and, hence, the bandwidth available more efficiently. Data are framed into packets and each packet is switched independently. Data from multiple sources are multiplexed and thus the total available bandwidth is shared.

Packet switching is used in routers. The maximum size of the packet is limited to make the router efficient. Packet sizes can vary from source to source, as well as from the same source. The message from a single source is divided into multiple packets and transmitted over the network to the destination. Each packet may take a different path from the source to the destination and may arrive out of sequence. Thus, they have to be reordered at the destination. This is termed datagram service and is shown in Figure 2.27(a). The message from DTE A has been split into three packets. Packets 1 and 3 take path A–B–D, and Packet 2 travels path A–C–B–D. At DTE Z, Packets 1 and 3 arrive before Packet 2 and hence have to be reassembled in the correct order.

It is desirable in many situations, such as in broadband service using ATM (covered in Section 2.6), to have all the packets from a given source to a given destination take the same path. This is analogous to circuit switching in that the path is fixed for the entire session. The concept of session is the same as in circuit switching. A virtual path–virtual circuit is established during the call setup between the source and the destination and a "virtual circuit identification" (one for each hop) is associated with the channel carrying the traffic. The path and circuit identifications are termed virtual as they resemble the operation in circuit switching, but different in that the connection is not physical. Figure 2.27(b) shows the virtual circuit path for the same message as in Figure 2.27(a) from DTE A to DTE Z. Packets arrive in the correct order at DTE Z in this situation. Although the initial call setup is an overhead, subsequent data transmission is faster than in datagram service. We will discuss more how the virtual path–virtual circuit configuration is used in Asynchronous Transfer Mode (ATM) service in Chapter 12.

Circuit and packet switching are applicable to a WAN, which we will review now.

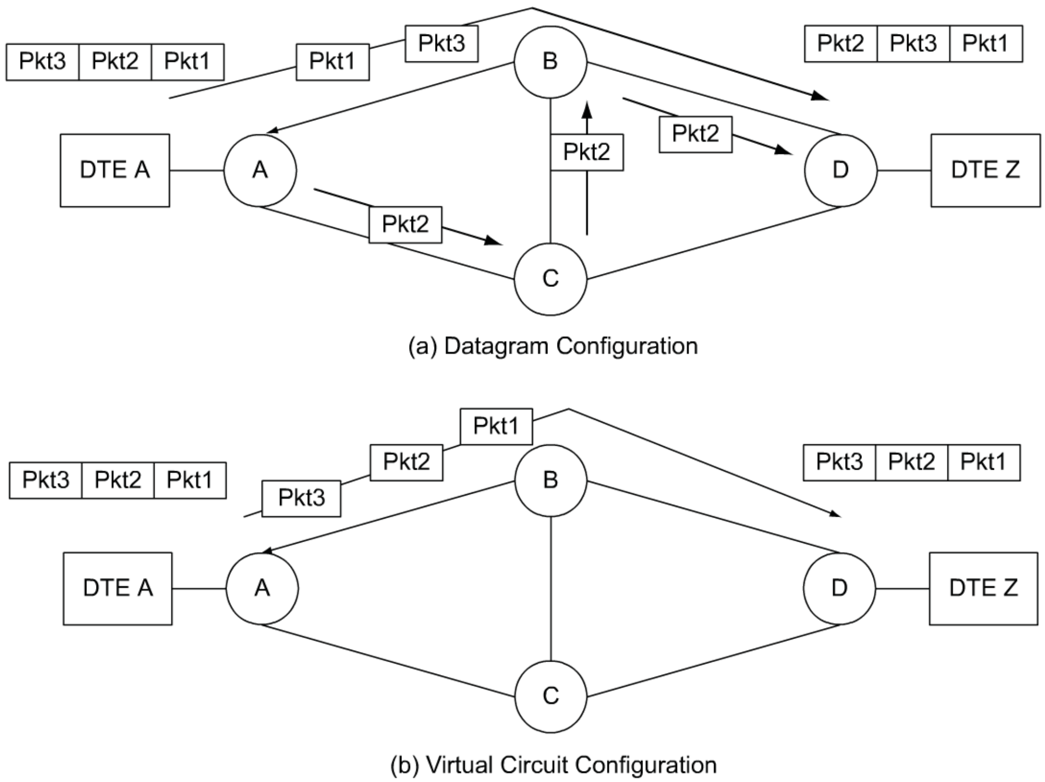


Figure 2.27 Packet Switch Configurations

2.4 WIDE AREA NETWORKS

The main difference between a WAN and a LAN is the geographical separation between sources and destinations. If the end stations are within a building or campus of buildings, it is still considered a LAN with a possible high-speed backbone LAN, such as FDDI.

As we saw in Section 1.2, computer communication network rides on top of telecommunication network, which is a WAN. Although most telephone and video communications traversing the WAN are still circuit switched, data traffic generated by computer communications is packet switched. We previously discussed two kinds of packet-switched services—datagram service and virtual circuit service.

Virtual circuit can be established on a session basis or on a permanent basis. The former is called a switched virtual circuit (SVC) and the latter a permanent virtual circuit (PVC). Geographically distributed organizations would lease PVCs from public service providers to handle large amounts of traffic. Otherwise, SVC service is used more often. Public telecommunication service providers offer these services. However, private corporations, using their own switches and leased lines from public service providers, set up large enterprise data networks.

We can partition WAN from a network management perspective into two sections and analyze the components and services that need to be managed in each. The two end sections of WAN are the subscriber loop sections, where information flows from central offices of the service provider(s) to customers' premises. The other section is transmission between switching offices.

Subscriber loop sections could be either passive, such as dedicated pairs of wires from the central office to the customer premises, or active links such as coaxial cable interspersed with amplifiers to boost the signal along the way. In either case, a digital subscriber line (DSL) terminates in a network interface unit (NIU) at the customer premises. Examples of NIU are Channel Service Unit (CSU) for interfacing DSL with analog equipment at customer premises, and Digital Service Unit (DSU) for DSL interface with digital equipment. The responsibility of the service provider is up to the NIU. Thus, components that need to be managed are the NIUs and the active components on the loop transmission line.

The transmission section consists of link transmission facilities and nodal components. These are between central offices in the case of a public switched network, and between the routers of service providers in private networks. We have looked at nodal components already. We will now consider transmission media and modes of LANs and WANs.

2.5 TRANSMISSION TECHNOLOGY

2.5.1 Introduction

Transmission technology deals with transmission media and transmission modes. We will look at transmission media first and then at transmission modes.

A transmission medium consists of the link that carries data between two physical systems. There is a coupling mechanism—a transceiver (denoting transmitter and receiver) that delivers to and receives data from the medium. Transmission media can be broadly classified into wired media and wireless media. Transportation of information is accomplished using physical transmission facilities, such as wires and optical fiber, or via wireless media using technology like radio frequency spectrum, infrared, and light waves. In the former case information is transmitted from point to point, whereas in the latter case it is generally done on a broadcast basis.

Both wired and wireless transmissions are used for local as well as WANs. The physical connection and the electronics of the transceiver play an important part in LAN, as they determine how fast and accurately information can be transmitted to and received from the various transmission media. We observed that the bandwidth of all types of Ethernet LANs could be doubled by changing from simplex to duplex configuration. In fact, advancement of new technologies depends on enhancements to existing ones. For example, ATM to the desktop has been aborted because of Ethernet technology's increased ability to handle large bandwidth (in gigabits per second) to the desktop. We also saw in Section 2.3.1 how hub technology has increased throughput in handling a large number of stations on a LAN.

Wireless LAN has so far found only limited use for high-speed communication. However, wireless technology is very extensively used for laptops, mobile communication, satellite transmission, and television access in rural areas.

2.5.2 Wired Transmission

Wired transmission technology uses three media: coaxial cable, twisted-pair cable, and optical fiber. The key parameters to look for in choosing the transmission medium are the following: loss of signal, insensitivity to environmental noise sources (such as cross talk and spurious radio frequency signals generated by appliances), bandwidth handling capability, and transmission delay. The selection of the medium is also determined by the type of stations on the medium and their access control mechanism. We listed the limitations and capabilities of various LAN media for Ethernet LAN in Tables 2.1 and 2.2.

There are two types of coaxial cables—thick and thin. The thick cable is 0.4 centimeters in diameter and is not used anymore. The thin coaxial cable is 0.25 centimeters in diameter and is present in legacy systems or small LANs, where it can be economically installed without a hub.

A twisted-pair cable consists of a pair of wires that are twisted. The gauge of the wire and the type of twist determine the quality of transmission. They are available as unshielded twisted pair (UTP) and shielded twisted pair (STP). Obviously, the latter reduces the interference of radio frequency noise better than the former. Most twisted-pair cabling that is used in LAN is Category 5 (cat-5) UTP. With cat-5 cable, the drop length for IEEE 802.3 LAN given in Table 2.1 can be extended from 100 to 150 meters at 100 Mbps. cat-6a cable extends the data rate to 10 Gbps.

The fiber-optic medium provides the best quality transmission. Of course, it is the most expensive. However, it is economical when LANs need to be networked in a campus environment or building with multiple stories. As shown in Tables 2.1 and 2.2, point-to-point drop for Ethernet could be as high as 2 kilometers, and in Gigabit Ethernet, we can extend it up to 9 kilometers.

It is worth noting the importance of cabling in geographically placed network components. As we all know, implementers always try to stretch the limits of specifications or economize in the installation process. For example, the maximum distance for a cat-3 cable would be stretched beyond the standard distance of 100 meters. Alternatively, instead of cabling all workstations using cat-5 and optical fibers to a central location where patch panels and hubs are collocated, hubs would be distributed to economize in cabling cost and only cat-3 cable is used. However, there is a price to pay in operations and maintenance for this approach since hubs could not be shared and any failure of a remote hub would take much longer for service restoration.

Wired WAN media comprises bundles of twisted pairs (such as in T1 and loop facilities), coaxial cable for analog transmission (for example, N1), and optical fiber (underwater sea cable).

2.5.3 Wireless Transmission Media

Wireless medium is used in WLAN as well as in mobile and satellite communications.

Wireless LAN uses input sources such as a hand-held portable communication device or a computer with a wireless antenna. Wireless LAN technology focuses primarily on transmitting data from portable stations to a wired LAN access point by radio frequency, infrared, or optical transmission. Since the range of transmission is limited for all these, they all function within a given region or cell. If the portable station is a moving target, then the signal has to be handed over from one cell to another cell.

Two fast-growing segments of wireless technology in the non-LAN environment are of interest for data communication. They are Personal Communication Services (PCS) and digital cellular services. Both of these are based on cell-based technology. Data are transmitted by wireless to local cell antennas from where they go to the central location by wired network. PCS is all-digital technology. It operates at lower power (100 watts) and antennas are more closely spaced (1/2 to 1 mile). The digital cellular technology, although analog, carries digitized signal. It needs higher-power antennas, which are separated farther apart (several miles).

Another area of wireless technology is broadband multimedia services. Multimedia is transmitted using satellite wireless technology from a central office to the customer's premises. The return path is via telephone lines.

2.5.4 Transmission Modes

The data transmission mode can be either digital or analog. Narrow-band LAN technology uses digital mode of transmission. Broadband and WAN technologies employ both analog and digital modes of transmission. When information is transmitted in an analog transmission mode, it can be transmitted in either baseband or on a carrier.

In a physical medium, digital transmission is a series of ones and zeros. A physical medium is shared by multiple sources to transport information to multiple destinations. The distinction between various transmission technologies is how information between pairs of end users is coded to share the same medium. They should be multiplexed and de-multiplexed efficiently at the nodes to provide the least and as constant a delay as possible, as well as high throughput.

Figure 2.28 shows three basic modes of transmission. They are Time Division Multiplexing (TDM) transmission, packet transmission, and cell transmission. T1 is the early implementation of TDM digital transmission in the United States by the Bell System. Figure 2.28(a) shows TDM transmission of T1 carrier, which carries 24 voice channels. The T1 carrier has a bandwidth of 1.544 MHz and is equally divided among 24 voice channels, each with a bandwidth of 64 kHz. The top of Figure 2.28(a) shows how the 1.544 MHz transmission "pipe" is divided into 24 small dedicated pipes among the 24 channels. The bottom half of the figure shows the multiplexing of the 24 channels as bit stream on the physical medium. They are multiplexed cyclically from Channel 1 through Channel 24. The maximum bandwidth available for each channel is 64 kHz, but it is all available during a complete session. A session is defined as the duration from establishment of a connection to tearing it down between a pair of users.

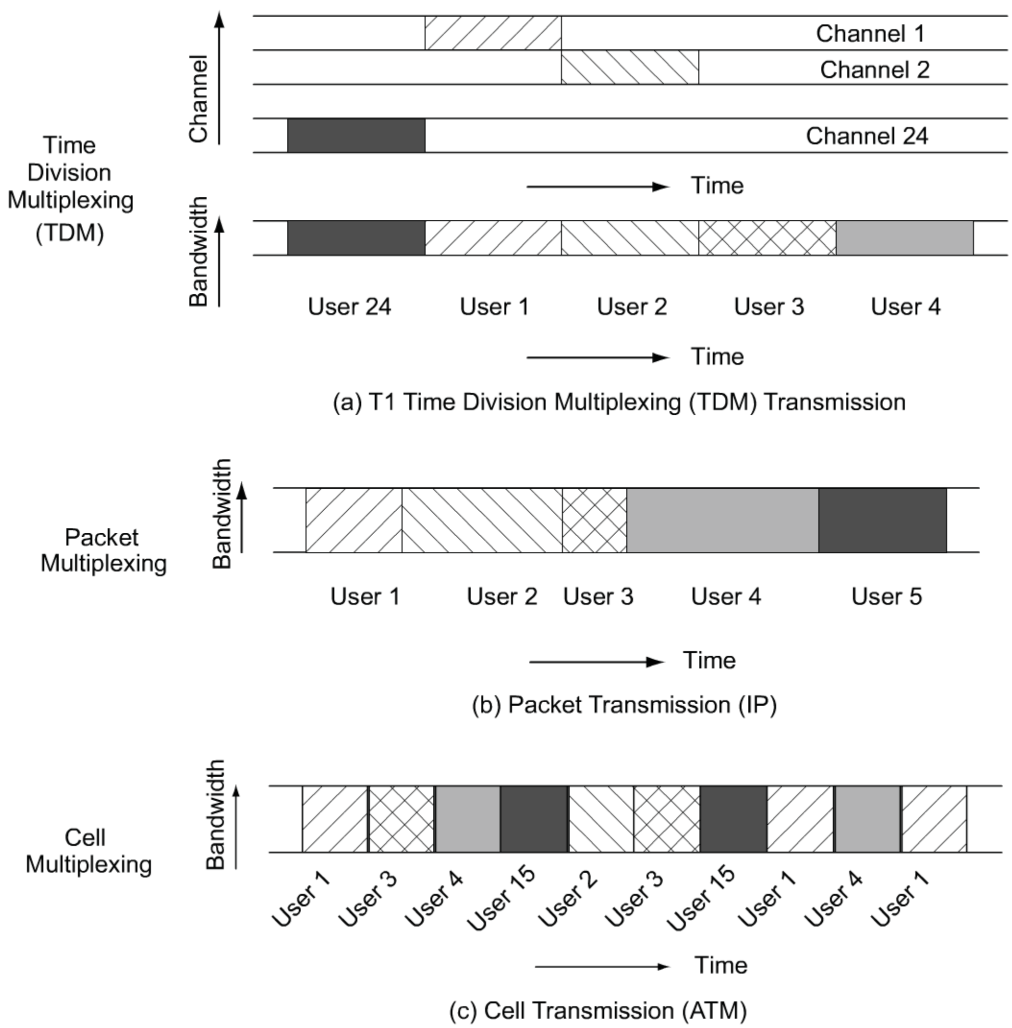


Figure 2.28 TDM, Packet, and Cell Transmission Modes

Notice that all channels have equal bandwidth and occupy the same slot in the transmission channel. When the receiver synchronizes to the transmitter, it is able to de-multiplex the channels, but both the transmitter and the receiver know exactly which slot each user's data occupy. Since a physical connection is set up between the two end stations prior to data transmission, the time delay is constant, which is essential for voice and video transmission. Nodes in the network using TDM are circuit switches. As mentioned in Section 2.3.11, the end-to-end connection is physical. The video channel, which requires more bandwidth (exact bandwidth depends on compression of data and quality of service required), occupies more channels.

Figure 2.28(b) shows the packet transmission mode. We notice that packets of different users are randomly multiplexed. While each user's data is traversing the medium, the full bandwidth of the medium is available to it. This is in contrast to TDM, where only a fraction of the medium bandwidth is available to any user. It can also be noticed that the size of all the user packets need not be the same. Another noticeable factor is that since the circuit connection is not pre-established, each packet contains addresses of the originator and the destination. We briefly described a packet switch in Section 2.3.11. Obviously, packet switches are used with packet transmission. A packet switch at each node looks at the address of the destination and routes it using the appropriate path. Each packet can take a different route depending on the availability of links and bandwidth based on different algorithms used. The packets may arrive out of sequence at the receiver, and the end-to-end transmission time for each packet is different. This transmission mode is acceptable for data transmission, but not for voice and video. Data transmission can tolerate bursty traffic.

The cell transmission mode, shown in Figure 2.28(c), combines the best of the above modes of transmission. The packets are all of the same size and are small in size. Each packet has the full bandwidth of the medium and the packets are statistically multiplexed. The packets all take the same path as in the circuit-switched TDM mode, using the virtual path–virtual circuit concept. This mode of transmission is called the ATM and is one of the fundamental concepts of ATM technology.

A recent development in WAN transport technologies is the evolution of the multiprotocol label switching (MPLS) transmission mode using the MPLS protocol. It can be visualized as an enhancement over IP and ATM protocols and backward compatible with either of them. A label, called the MPLS label, is inserted between layer 2 and layer 3, as shown in Figure 2.29. Thus, for an IP-based protocol,

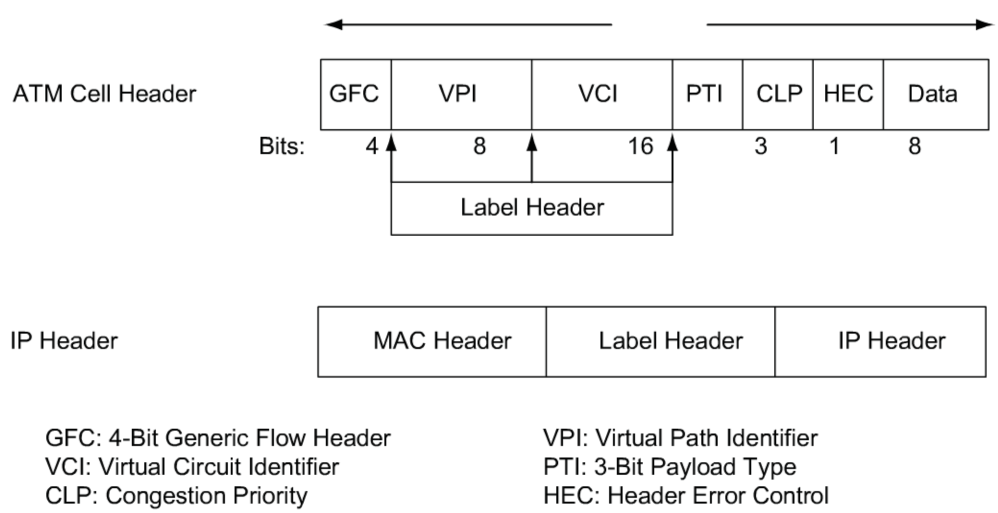


Figure 2.29 MPLS Transmission Mode

the MPLS label is inserted between the IEEE 802.3 MAC header and the network layer IP header. In the case of the ATM protocol, MPLS shim without the TTL field replaces VPI and VCI fields. The MPLS transmission mode attempts to take advantage of the richness of IP characteristics and high performance of ATM.

An IP-based network is feature rich because of its extensive implementation and compatibility with Ethernet LAN. It routes packets intelligently. However, it is slow in performance as it has to open each packet at layer 3 to determine its next hop and its output port. Simultaneous transport of real-time and non-real-time traffic is difficult.

In contrast to IP, the ATM protocol is a high-performance cell-based protocol switching cells at layer 2. It is capable of handling real-time and non-real-time traffic simultaneously, and thus is superior to the IP-based network. However, its address incompatibility with the popular Ethernet LAN, along with difficult end-to-end circuit provisioning, has limited its usage at the customer premises network and hence related applications.

In general, the packet header contains forwarding equivalence class (FEC) information to choose the next hop in a router. In so far as the forwarding decision is concerned, all packets belonging to a particular FEC are assigned the same path leaving the node. The MPLS label is a short, fixed length, locally significant identifier, which is used to identify an FEC.

An MPLS protocol is being deployed in a convergent network for broadband services handling real-time and non-real-time traffic simultaneously, thus achieving high quality of service transport. It can be deployed in the legacy network of either IP or ATM base.

Currently most information is transmitted in digital mode. The legacy digital system is a T-based hierarchy (T1, T3…) in North America and an E-based hierarchy (E1, E2...) in the UK and Europe and uses packet or frame technology. The later implementation of digital mode of transmission in many WANs is the Synchronous Optical Network (SONET), which is addressed in the next section. More recently, the WAN transmission mode has started migrating to MPLS over IP.

We can visualize the above transmission modes as modes of transmission at the basic or atomic level (although not quite true). Each of the modes—TDM, ATM cell mode, IP packet mode, MPLS packet mode—is transmitted using its own protocol. Thus, they can be considered as modes based on protocol. However, modern transmission technology is capable of carrying a large amount of information; i.e., large bandwidth of information; and this should be taken advantage of in designing transmission systems. For instance, optical fiber can carry a terahertz (THz) bandwidth signal. However, the quality of the signal transmission gets worse when the signal bandwidth is large. It is due to network element limitations and propagation constraints. Fortunately, we can transmit a large amount of information using the same physical medium by employing the multiplexing principle discussed in TDM. In T1 or E1 TDM, 24 or 32 channels can be multiplexed by logically partitioning the physical medium into 24 or 32 channels.

Using multiplexing approach, the physical optical-fiber medium can be used to carry multiplexed lower bandwidth signals using Synchronous Digital Hierarchy (SDH). This mode of transmission is known as SONET in North America and SDH in Europe and Asia and is discussed more in Chapter 12. Nodes in the optical transmission network are used to regenerate the signal using regenerators, change path by using optical or digital cross-connect network elements, and drop and add lower-level digital signals at various intermediate points along the path by using Add–Drop Multiplexers (ADM). Figure 2.30 shows a SONET transmission mode. The lower-speed digital signals DS1/E1, DS1C, DS2, designated as Virtual Tributaries (VTs) are multiplexed into a VT Group. A SONET frame comprises an overhead and synchronous payload called a synchronous payload envelope (SPE). The speed of digital data

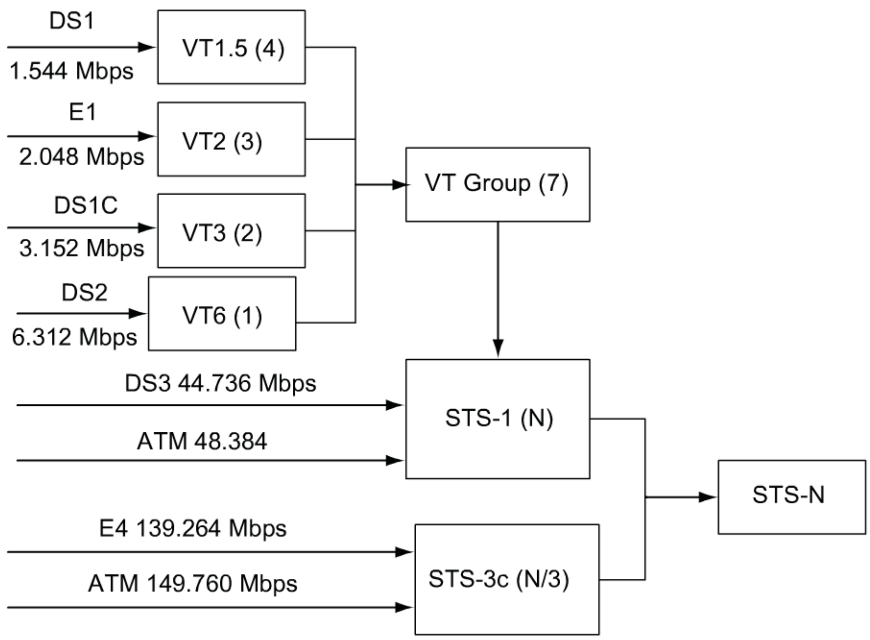


Figure 2.30 SONET Transmission Mode

is synchronized using a SONET basic signal rate of 51.84 Mbps called synchronous transport signal level-1 (STS-1). Higher-rate signals STS-N are generated by interleaving bytes from lower-level STS-1s. The numbers in parentheses in Figure 2.30 indicate the number of input signals that need to be multiplexed.

In Figure 2.30, STS-1 comprises seven VT Group signals, or a DS3 signal, or a 48-Mbps ATM signal. STS-3 SONET signal, also known as STM-1 in SDH, is made up of a 150-Mbps ATM or E4 signal. Transmission rates for SONET/SDH signals are presented in Table 2.3.

The second method of the increasing capacity of information in an optical transmission medium is to take advantage of the optical wavelength of transmission. This is known as wavelength division multiplexing (WDM). This is identical to frequency division multiplexing at (relatively) lower frequencies. Information can be transmitted over multiple wavelengths using multiple transmission protocols, as shown in Figure 2.31. In order to illustrate this point, transmission modes shown in Figure 2.28 are depicted in Figure 2.31 as components in the WDM transmission, each submode traversing at a different wavelength. Several hundreds of tens-of-gigabits signals can be transmitted over the long-haul WAN and short-haul MANs.

Table 2.3 SONET/SDH Transmission Rates

SONET SIGNAL	SDH SIGNAL	BIT RATE (Mbps)
STS-1		51.84
STS-3	STM-1	155.52
STS-12	STM-4	622.08
STS-24		1,244.16
STS-48	STM-16	2,488.32
STS-192	STM-64	9,953.28
STS-768	STM-256	39,814.32

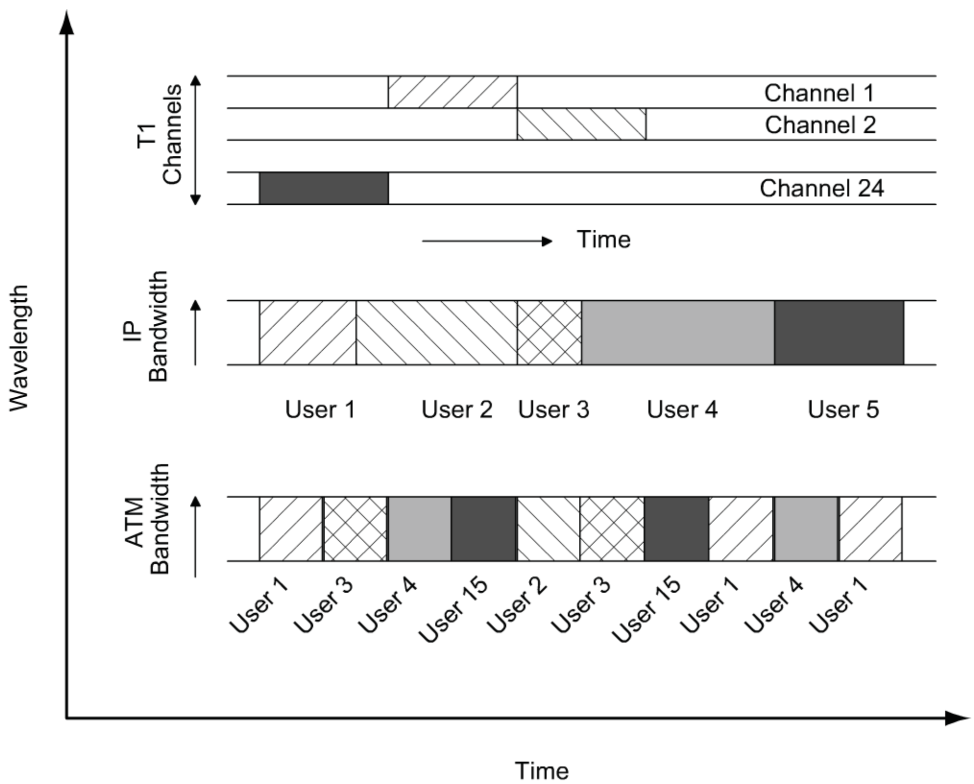


Figure 2.31 Multiwavelength Fiber: WDM

2.6 INTEGRATED SERVICES: ISDN, FRAME RELAY, AND BROADBAND

Integrated Services Digital Network (ISDN) can be divided into narrow band and broadband ISDN. Broadband ISDN is called broadband services. ISDN was introduced by Bell System to integrate voice and data over telephone loop facilities. The same principle is used in integrating voice, video, and data and providing them as broadband multimedia service.

The early form of integrated services network is Basic ISDN. It is a full-duplex digital interface between the subscriber and the central office. It consists of two basic channels, 56-kilobaud rate each, combined with an 8-kilobaud signaling channel, referred to as 2B+D.

Basic ISDN was extended to T1 and E1 rates of 1.544 Mbps and 2.048 Mbps. This is called the Primary ISDN interface. The T1 interface carries 24 channels and the E1 interface 32 channels.

With the improved quality of transmission media, the ISDN concept was extended from the subscriber interface to a WAN. To achieve near real-time quality for voice, the performance of WAN needs to be improved. This was done by a frame relay service, which eliminates hop-to-hop flow and error controls in a traditional packet switching network, including X.25. Flow and error controls are relegated to higher layers at the ends of a link. The frame relay access speed can go up to 2 Mbps.

However, on-line videos require a much larger bandwidth than could be achieved with frame relay. This has led to early implementation of broadband ISDN, or, as mentioned in the beginning of this section, more succinctly, broadband network. Broadband network and service have contributed significantly to advances in three areas. They are ATM (Asynchronous Transfer Mode), SONET (Synchronous Optical

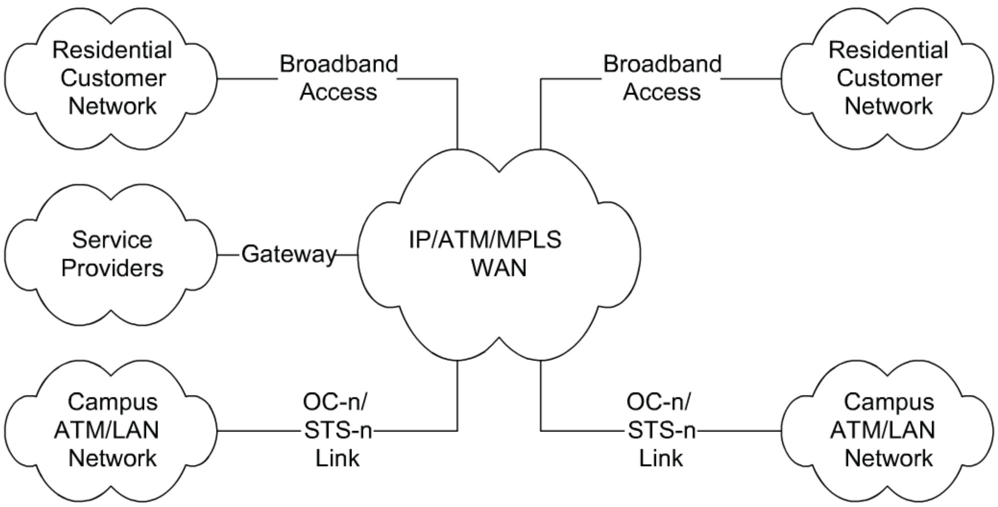


Figure 2.32 Broadband Services Network

Network)/SDH (Synchronous Digital Hierarchy), and broadband access technology. In Chapter 12, we will discuss ATM, which is a cell-based transmission mode, and SONET, which is a digital hierarchy adopted universally.

Broadband access technology, which addresses the link from the central office to the customer's premises, is implemented using one of three technologies. Hybrid fiber coax (HFC) technology is a two-way interactive multimedia communication system using fiber and coaxial cable facilities and cable modems. The second technology uses a DSL. There are several variations of implementing this, generically referred to as xDSL. For example, ADSL stands for asymmetric DSL. The third technology uses wireless transmission from the switching office or head end to the customer's premises via satellite transmission. We will learn in detail about broadband service and access network technologies in Part IV.

Figure 2.32 shows a broadband services network. The WAN is IP, ATM, or MPLS. The WAN is linked to the customer's premises using either optical links, OC-n (Optical Carrier-n)/STS (Synchronous Transport Signal), or one of the three access technologies (HFC, xDSL, or wireless). The customer network consists of two classes, residential customers and corporate customers with a campus-like network. Residential customers are either residential homes or small and medium enterprises (SMEs) that use broadband services, but do not maintain high-speed access network to WAN. Service providers perform that function bringing radio, video, Internet, and other services to homes. Multiple services are multiplexed by multiple service operators (MSO) and are piped to the customer's premises via common facilities. Service providers interface with each other via gateways, which could be either generalized routers or ATM switches.

Summary

In this chapter we learned network concepts and technologies that would help us understand network management in Parts II, III, and IV.

Network topologies can be classified as LAN and WAN topologies. There are three network topologies associated with wired LANs. They are bus, ring, and star. The most predominant commercially employed LANs are a hybrid of the star topology with either the bus or the ring topology—the hub topology.

WAN is implemented using either a mesh or a tree topology. Mesh topology is the common implementation and is the topology of the Internet. Tree topology is used when a network is made up of bridges.

We discussed different types of common LAN implementation—Ethernet, Fast Ethernet, Gigabit Ethernet, switched hub, Token Ring, and FDDI. Of these, IEEE 802.3 Ethernet LAN is the predominant type. This uses CSMA/CD MAC protocol. We addressed the introduction of full-duplex types of Ethernet that double the bandwidth. Ethernet can be implemented using various types of transmission media—coaxial cable, UTP, and optical fiber. Fast Ethernet at 100 Mbps and Gigabit Ethernet at 1 Gbps speed can be implemented by employing hub technology. Switched hub multiplies the throughput by simultaneous conversations between pairs of nodes. Virtual LANs, implemented using switched hub, enable logical association of workstations with VLANs.

Token Ring and FDDI both use deterministic MAC and hence are more efficient over random access Ethernet. IEEE 802.5 defines the speed of the Token Ring as either 4 Mbps or 16 Mbps.

FDDI is based on IEEE 802.5 protocol and operates at 100 Mbps. It is typically used for backbone LAN. Because of the need for reliability of the backbone, FDDI can be configured as a dual ring with DAS, in contrast to a single ring with SAS.

Network nodes comprise hubs, bridges, routers, gateways, and switches. Hubs play a significant role in forming LANs as discussed above. Bridges function at the data link layer and can be interconnected to form a network. A network consisting of Ethernet bridges is called a transparent bridge network and should meet the criterion of not having any loop in the network. In contrast, a network made up of Token-Ring bridges, source routing bridges, can have loops in the network. This is because the source specifies the route in the data packet and intermediate nodes do not make any routing decisions.

Routers and gateways function at the network layer. Routers and gateways form the backbone of the Internet. The difference between a router and a gateway is that the former just routes, whereas the latter does protocol conversion. If protocol conversion is done at the application layer, it is called a protocol converter.

Packet switching is the switching of data packets. Packet switches, in general, perform datagram service. That means each packet of the same message can take different routes and may arrive out of sequence. Hence, they have to be reassembled at the receiver in the correct sequence.

We can also configure packet switches to form a virtual circuit. In this case, all packets of a session between the source and the destination take the same path in the network and arrive in the same sequence that they were sent. A virtual circuit can be established on a per-session basis, in which case, it is called a switched virtual circuit (SVC). The virtual circuit is set up and torn down each time. In contrast, for a permanent virtual circuit (PVC), call setup is done and left there permanently.

A WAN is established using either SVC or PVC. WAN is distinguished from LAN by large geographical separation between the source and the destination. It is generally carried over the facilities of telecommunications network.

In discussing transmission technology, we covered wired and WLAN technologies. The role of coaxial cable, twisted-pair cable, and optical fiber was reviewed. LAN transmits data in digital format. WAN and broadband technology services transmit information in both digital and analog modes. We addressed the various transmission modes of TDM, cell, and packet technologies. Optical-fiber technology was presented, which can carry information in the tens of gigahertz bandwidth in the SONET/SDH and WDM transmission modes.

We ended our discussion of network technology by introducing ISDN and broadband multimedia services. They handle voice, video, and data transmission in an integrated manner. The WAN in broadband services is ATM-based SONET and the access to customer premises uses HFC, xDSL, or wireless technology.

Exercises

1. The maximum allowed segment for Ethernet is 500 meters and the maximum number of segments that can be connected by repeaters is limited to five. The minimum length of the frame that can be transmitted is the sum of the round-trip delay and the repeater delays. Assume that the speed of transmission on the cable is 200 meters/microsecond and that the total round-trip delay in traversing all the repeaters is 25 microseconds. Show that the minimum frame size (number of bits per frame) of an Ethernet frame is 64 bytes.

   Note: The maximum frame size is 1,518 bytes.
2. Gigabit Ethernet using CSMA/CD is specified to have a 100-meter drop cable. Show that this corresponds to a slot time of 512 bytes to detect collision. Assume a repeater delay of two microseconds.
3. The Engineering Department of 12 persons in a small corporation is on a regular 10Base-T Ethernet LAN hub with 16 ports. The busy group started complaining because of the slow network performance. The network was operating at 50% utilization, whereas 30% utilization is acceptable. If you are the Information Technology Engineer of the corporation and have to resolve the problem technically,

   (a) Describe four choices for resolving the problem, maintaining the LAN as Ethernet LAN.

   (b) State the advantages and disadvantages of each approach.
4. In Exercise 3, you are told by the IT Manager that the problem is to be resolved by using bridges and the existing hub that could be configured for four subnets. A good rule of thumb is that a LAN utilization of 4% yields good and satisfactory performance. Assume that 12 workstations are functioning at a peer-to-peer level with distribution of traffic between any two stations being the same. What would your new configuration be?
5. Design an Ethernet LAN using a 10/100 Mbps switched Ethernet hub to handle the following specifications:

   Number of clients = 16 operating at 10 Mbps

   Number of server = 1

   50% of the traffic is directed to the server

   Draw the configuration and indicate the transmission modes (half-duplex or duplex) on the ports.
6. Repeat Exercise 4 if the traffic to the server increases to 80.
7. Two virtual LANs, 145.50.50.1 belonging to NM lab and 145.50.60.1 belonging to Networking lab, each have three workstations. The former has workstations 140.50.50.11-13 and the latter 140.50.60.21-23. They are connected to a switched hub as shown in Figure 2.10 on ports 2 through 7. The NICs associated with ports are made by Cabletron and their MAC addresses start with the vendor's global prefix 00-00-D (hexadecimal notation) and end with 11, 12, 13, 21, 22, and 23 (same as the fourth decimal position of the IP address).

   (a) Create a conceptual matrix table, as shown below, which would be generated by the hub that relates the IP address, the MAC address, and the port number.

IP ADDRESS	MAC ADDRESS	PORT NUMBER

   (b) The workstation 23 is moved from Networking lab to NM lab. Show the appropriate parameter changes on the hub and the workstation.
8. In Exercise 7, Port 1 of the hub is connected to a router as shown in Figure 2.10. The IP and MAC addresses associated with the NIC on the hub interfacing to the router are 145.50.50.1

and 00-00-100-00-00-01 and that with the NIC on the router interfacing with the switched hub of 130.30.40.1 and 00-00-10-00.00-64. Extend the matrix of Exercise 7(a) to include Port 1, using the same convention for the MAC address.

9. In Exercise 8, the router is connected to the switched hub by a single physical cable. The router maintains two sets of tables, one to determine the subnets on its network and other to determine the host on the subnet as shown below. The third decimal of the IP address is allocated to subnet designation.

Network Table

NETWORK	SUBNET	HOST
145.50	50	0
…	…	0
145.50	60	0

Subnet Address Tables

NETWORK	SUBNET	HOST	PORT
145.50	50	1	1
145.50	50	11	1
“	“	12	1
“	“	13	1
145.50	60	1	1
“	“	21	1
“	“	22	1
“	“	23	1

(a) What is the mask used by the router to filter the subnet?
(b) Show how two packets arriving in the router and addressed to 145.50.50.11 and 145.50.60.21 are directed to the switched hub by using the above table.

10. Design a client–server network with two servers operating at 100Base-T Fast Ethernet speed and the clients operating at regular 10Base-T Ethernet speed using a 10/100 Mbps NIC. The hub is located in a wiring closet, but the servers and clients are not. Assume that a satisfactory performance is achieved at 40% utilization of the LAN.

11. Which of the following is correct? The maximum throughput of an 8-port switched hub over an 8-port non-switched hub is:

    (a) the same
    (b) 2 times
    (c) 4 times
    (d) 8 times

12. It is assumed in Exercise 11 that the LAN operates at maximum utilization. However, a regular LAN can degrade in performance to an intolerable level at 50% utilization. What is the approximate (ignore contention of more than one station trying to reach the same destination at the same time) percentage utilization improvement of a 12-port switched hub Ethernet LAN over a non-switched hub Ethernet LAN?

13. The minimum size of the frame in a token-ring LAN is determined by the token size, which is 3 bytes long and should be contained in the ring under idle condition. Assume a 16-Mbps LAN and the speed of transmission as 200 meters/microsecond.
    - (a) What should be the minimum length of the ring in meters?
    - (b) Each station normally adds a bit delay in processing the data. What is the additional length gained by adding one station at a time?
14. Repeat Exercise 13 for an FDDI ring. Assume the speed of transmission as 300 meters/microsecond.
15. Explain the reason why the performance of an Ethernet LAN decreases with increase in the number of stations on the LAN, whereas it increases (at least initially) with the increase in the number of stations in a token-ring LAN.
16. Draw network configuration and protocol layer interface architecture for a multiprotocol bridge that interconnects an Ethernet LAN to a token-ring LAN.
17. A short message is transmitted from a source at Switch A to a destination at Switch Z. The shortest path traverses through 5 intermediate switches. A switch causes an average delay of 5 milliseconds to process a packet. Assume all the packets of the message leave at approximately the same time (although they leave sequentially), as the duration of the message is short compared to the transmission delay in the switches.
    - (a) A ssume the message is sent as a datagram and the datagram packets take multiple paths, each packet traversing the shortest path going through 5 intermediate switches and the longest path going through 10 intermediate switches. Calculate the latency time if the packet reassembling time is ignored at the destination.
    - (b) What is latency if a virtual circuit is established along the shortest path?
18. How many (a) E1 channels and (b) DS1 (T1) channels comprise an STM-1 SDH signal?