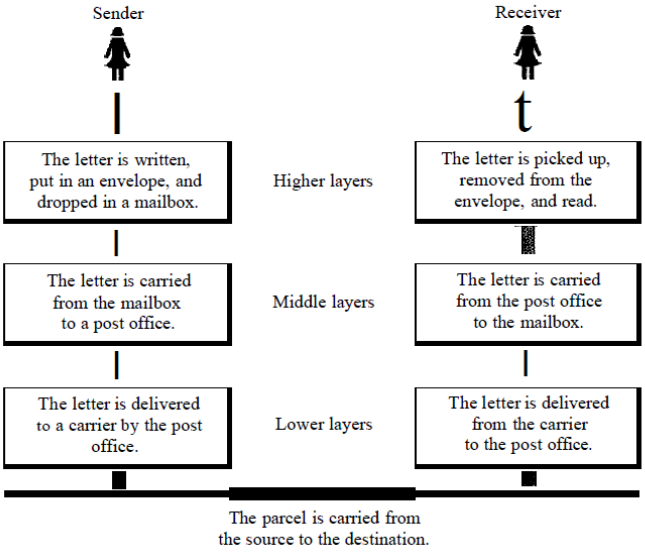
Chapter 1

Networking Basics

1.1 Layered Tasks:

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office. Figure 2.1 shows the steps in this task.

Figure 2.1 *Tasks involved in sending a letter*



In Figure 2.1 we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

At the Sender Site

Let us first describe, in order, the activities that take place at the sender site.

o Higher layer. The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.

o Middle layer. The letter is picked up by a letter carrier and delivered to the post office.

o Lower layer. The letter is sorted at the post office; a carrier transports the letter.

On the Way

The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be transported by truck, train, airplane, boat, or a combination of these.

At the Receiver Site

o Lower layer. The carrier transports the letter to the post office.

o Middle layer. The letter is sorted and delivered to the recipient's mailbox.

o Higher layer. The receiver picks up the letter, opens the envelope, and reads it.

There are three different activities at the sender site and another three activities at the receiver site. The task of transporting the letter between the sender and the receiver is done by the carrier. Something that is not obvious immediately is that the tasks must be done in the order given in the hierarchy. At the sender site, the letter must be written and dropped in the mailbox before being picked up by the letter carrier and delivered to the post office. At the receiver site, the letter must be dropped in the recipient mailbox before being picked up and read by the recipient.

Each layer at the sending site uses the services of the layer immediately below it. The sender at the higher layer uses the services of the middle layer. The middle layer uses the services of the lower layer. The lower layer uses the services of the carrier.

1.2 Introduction to OSI Model:

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols (set of rules) that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

The OSI model is a layered framework (as discussed in previous part) for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network (see Figure 2.2). An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.

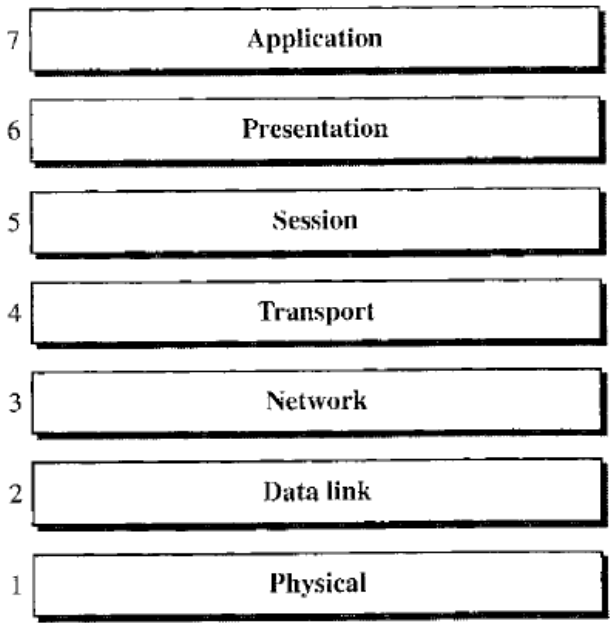


Figure 2.2: Seven layers of OSI model

This OSI layered model that dominated data communications and networking literature before 1990 was the Open Systems Interconnection (OSI) model. Everyone believed that the OSI model would become the ultimate standard for data communications, but this did not happen. The TCPIIP protocol suite became the dominant commercial architecture because it was used and tested extensively in the Internet; the OSI model was never fully implemented.

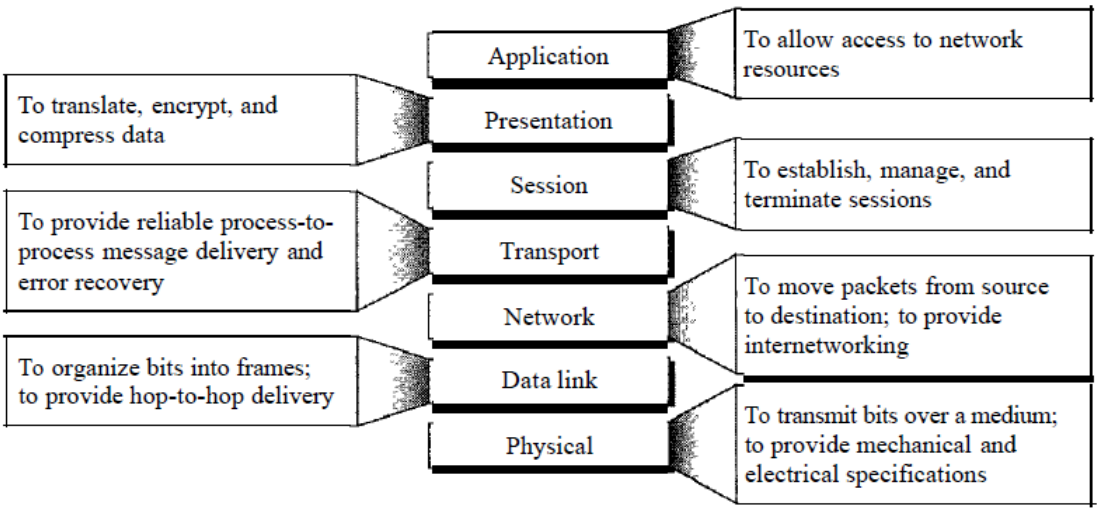


Figure 2.3: Summary of each layers

1.3 TCP/IP Protocol Suite

TCP/IP was designed to be independent of networking Hardware and should run across any connection media. The TCP/IP protocol suite consists of many protocols that operate at one of 4 layers. The protocol suite is named after two of the most common protocols – TCP (transmission Control Protocol) and IP (internet Protocol). It consists of five layers as shown in Fig. 1.1.

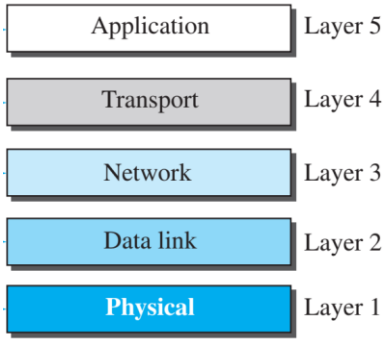


Figure 1.1 Layers of TCP/IP protocol suites

Application Layer

The top, or fifth, layer of the TCP/IP protocol suite is the Application layer. Contrary to what its name implies, the Application layer does not include software programs, such as Microsoft Word or Firefox. Instead, the Application layer facilitates communication between such programs and lower-layer network services. Services at this layer enable the network to interpret a program's request and the program to interpret data sent from the network. For example, when you choose to open a Web page in Firefox, an Application layer protocol called HTTP (Hypertext Transfer Protocol) formats and sends your request from your client's browser (a software application) to the server. It also formats and sends the Web server's response back to your client's browser. Application layer is implemented only in sender and destination devices. Other protocols in this layer include FTP, TFTP, DNS, SMTP, SNMP, POP3 and so on.

Transport Layer

Protocols in the Transport layer accept data from the Application layer and manage end-to-end delivery of data. That means they can ensure that the data are transferred from source to destination reliably, in the correct sequence, and without errors. Without Transport layer services, data could not be verified or interpreted by its recipient. Transport layer protocols also handle flow control, which is the process of gauging the appropriate rate of transmission based on how fast the recipient can accept data. It introduces port addressing to identify a specific process (application layer protocol). Transport layer protocols include transmission control protocol (TCP) and user datagram protocol (UDP). TCP is more reliable but slower protocol than UDP. Transport layer

takes data from application layer and segment them to form called segment (for TCP) or user datagram (for UDP) after including transport layer header.

Network Layer or Internet Layer

Network layer protocols accept the Transport layer segments and add logical addressing (Internet protocol (IP) addressing) information in a network header. At this point, the data unit becomes a packet (also known as IP datagram). Network layer protocols also determine the path from point A on one network to point B on another network by factoring in:

- Delivery priorities (for example, packets that make up a phone call connected through the Internet might be designated high priority, whereas a mass e-mail message is low priority)
- Network congestion
- Quality of service (for example, some packets may require faster, more reliable delivery)
- Cost of alternative routes

The process of determining the best path is known as routing. Internet layer protocols include Internet protocol (IP), Internet control message protocol (ICMP), Routing information protocol (RIP), Open shortest path first (OSPF) and so on.

Datalink Layer

In the second layer, Data Link layer, protocols encapsulates Layer 3 packet into a frame that can then be transmitted by the Physical layer. A frame is a structured package for moving data that includes not only the raw data, or "payload," but also the sender's and receiver's network addresses, and error checking and control information. The addresses tell the network where to deliver the frame, whereas the error checking and control information ensure that the frame arrives without any problems. Layer 2 is required for communication inside a network. Unlike application and transport layers, the functionalities of this layer are implemented in all communication devices including connecting devices and end devices. Some example of devices which work in layer 2 include switch and bridge. Layer 2 protocols are ALOHA, CSMA, CSMA/CD, CSMA/CA.

Physical Layer

The Physical layer is the lowest, or first, layer of the OSI model. Protocols at the Physical layer accept frames from the Data Link layer and generate signals as changes in voltage at the NIC. (Signals are made of electrical impulses that, when issued in a certain pattern, represent information). When the network uses copper as its transmission medium, these signals are also issued over the wire as voltage. In the case of fiber-optic cable, signals are issued as light pulses. When a network uses wireless transmission, the signals are sent from antennas as electromagnetic waves. When receiving data, Physical layer protocols detect and accept signals, which they pass on to the Data Link layer. Physical layer protocols also set the data transmission rate and monitor data error rates. Simple connectivity devices such as hubs and repeaters operate at the Physical layer.

One of the important concepts in protocol layering in the Internet is encapsulation/decapsulation. In Figure 1.2, we show the encapsulation in the source host, decapsulation in the destination host, and encapsulation and decapsulation in the router.

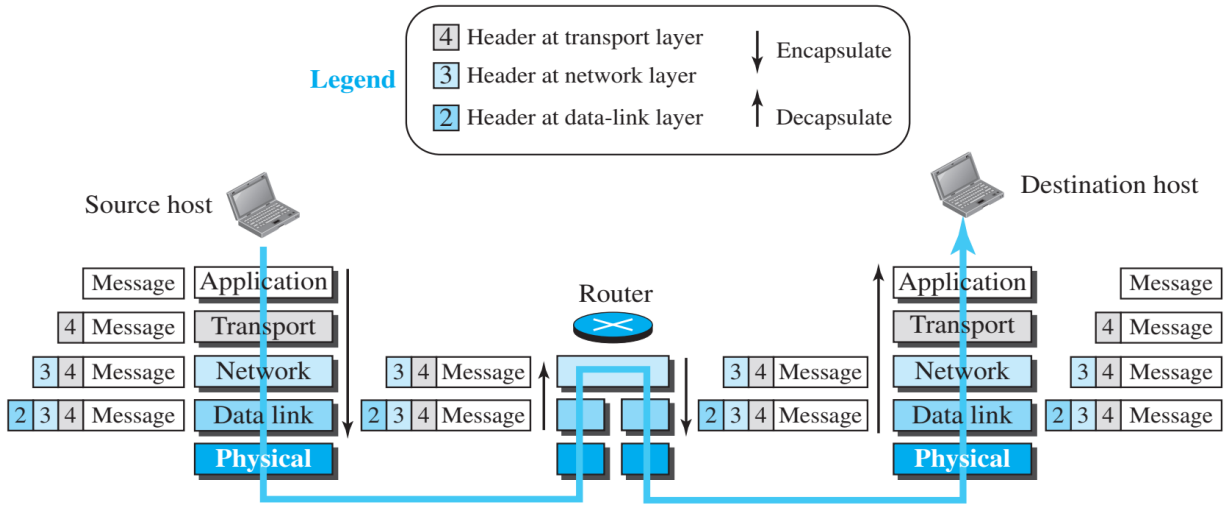


Figure 1.2 Encapsulation and decapsulation in TCP/IP protocol suite.

Encapsulation at the Source Host:

At the source, we have only encapsulation.

1. At the application layer, the data to be exchanged is referred to as a message. A message normally does not contain any header or trailer, but if it does, we refer to the whole as the message. The message is passed to the transport layer.
2. The transport layer takes the message as the payload, the load that the transport layer should take care of. It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs that want to communicate plus some more information that is needed for the end-to-end delivery of the message, such as information needed for flow, error control, or congestion control. The result is the transport-layer packet, which is called the segment (in TCP) and the user datagram (in UDP). The transport layer then passes the packet to the network layer.
3. The network layer takes the transport-layer packet as data or payload and adds its own header to the payload. The header contains the addresses of the source and destination hosts and some more information used for error checking of the header, fragmentation information, and so on. The result is the network-layer packet, called a datagram. The network layer then passes the packet to the data-link layer.
4. The data-link layer takes the network-layer packet as data or payload and adds its own header, which contains the link-layer addresses of the host or the next hop (the router). The result is the link-layer packet, which is called a frame. The frame is passed to the physical layer for transmission.

Decapsulation and Encapsulation at the Router:

At the router, we have both decapsulation and encapsulation because the router is connected to two or more links.

1. After the set of bits are delivered to the data-link layer, this layer decapsulates the datagram from the frame and passes it to the network layer.
2. The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop to which the datagram is to be

delivered. The contents of the datagram should not be changed by the network layer in the router unless there is a need to fragment the datagram if it is too big to be passed through the next link. The datagram is then passed to the data-link layer of the next link.

3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

Decapsulation at the Destination Host:

At the destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer. It is necessary to say that decapsulation in the host involves error checking

1.4 Connecting Devices

To connect different end devices like PC, we need different connecting devices or networking devices depending on the network. Examples of the connecting devices include: Repeater, Hub, Switch and Router. The functionalities of each of these devices are explained next.

Repeater

A repeater is a Layer 1 device that takes voltage from the line, amplifies the voltage, and sends it down the line. This device cannot translate, analyze, manipulate, or do any processing of the voltage. It is a simple amplifier that will increase the signal strength of the signal. If there is any "noise" caused by EMI on the wire it will also amplify the noise and send it on. The general rule of thumb is to have no more than three repeaters in a row. Once you get past the third repeater you will be sending only noise. These devices work with only one media type. If you have Thinnet coming in, you must have Thinnet going out; it cannot do any media conversion. Repeater is normally used for extending the maximum allowable length of a cable segment. Figure 1.3 shows such a network scenario.

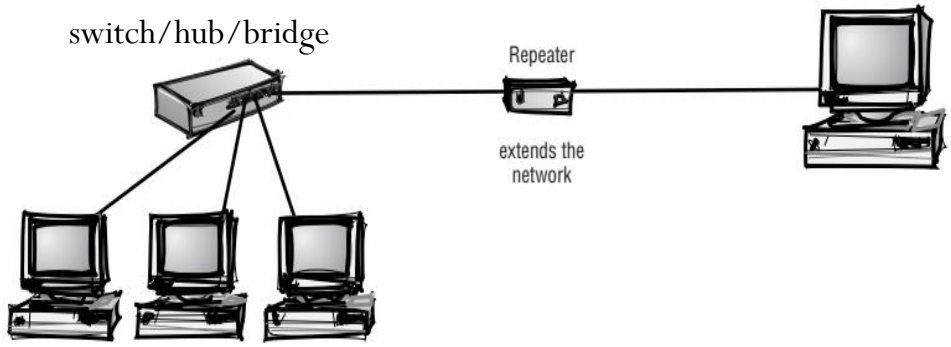


Figure 1.3 Use of repeaters and switch/hub/bridge

Hub

A hub, a layer 1 device, is nothing more than a multiport repeater. Electrical signal comes through one port of the hub and gets amplified and sent out through all ports of the hub (see Fig. 1.4). Like the repeater you cannot mix and match media. Hubs and repeaters create what is called a collision domain. You can only have one signal on the wire at any one time. If two signals are on the wires at the same time they will collide and cause a collision. This collision means that no data is delivered to the remote receiver. The more ports you have on the hubs (and the more hubs connected together), the more likely you are to have collisions. It can connect segments or a network but cannot segment a network. Most hubs come with a minimum of 4 ports but can have as many as 48. Most hubs require no configuration. And remember that the devices connected to hubs all share the same bandwidth. In other words, if you have a 10-Mbps hub and three devices are transmitting at the same time, each device gets one third of the bandwidth.

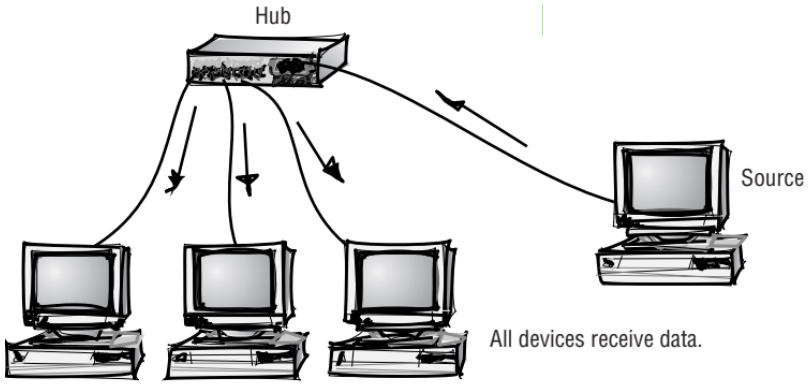


Figure 1.4 Broadcasting of a Hub

Bridge

A bridge is a device that connects two or more segments of a network to make them one. It could be described as a device that determines whether a message from you to someone else is going to the local area network or to someone on the LAN in the next building. A bridge examines each message, passing on those known to be within the same LAN, and forwarding those known to be on the other connected LANs (see Fig. 1.5). It looks similar to a hub but functions at the next layer of the OSI model, the Data Link layer. Bridges have a single input and a single output port. It stores the MAC address for each device and then analyzes the incoming packets to determine what to do with them as they come through. Basically, it learns all the MAC addresses of the network to construct a database used for forwarding or filtering packets.

A bridge can connect two different types of topologies because it does not understand anything above the Data Link layer. It doesn't matter whether one machine is using TCP/IP and another is using International Packet Exchange (IPX), Sequenced Packet Exchange (SPX) because they are only concerned with the MAC addresses and not the protocols. This allows them to move data more rapidly, but it takes longer to transmit because a bridge analyzes each packet.

Bridge separates collision domains by determining what MAC addresses are on each side of the bridge and only passing traffic if the destination address is on the other side of the bridge. The bridge will also handle the placing of the data on the collision domain to try and reduce the collisions. Bridges create broadcast domains. Frames with a MAC address of FF:FF:FF:FF:FF:FF are called broadcast frames and every network device must look at the data; therefore, any frame that is a broadcast must cross all bridges.

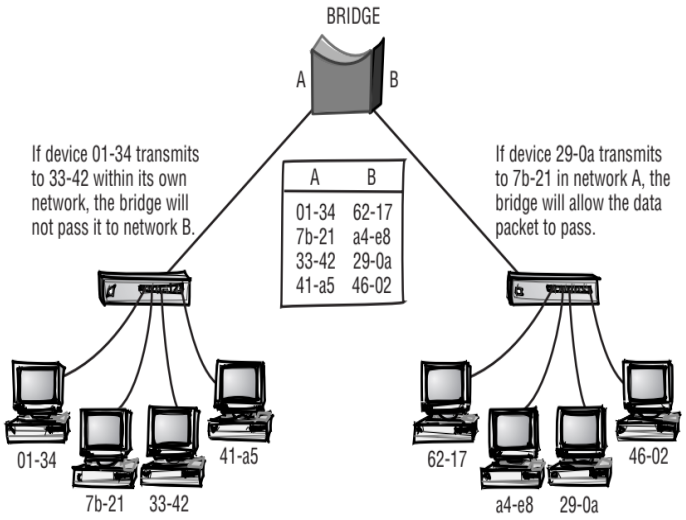


Figure 1.5 Filtering of a Bridge

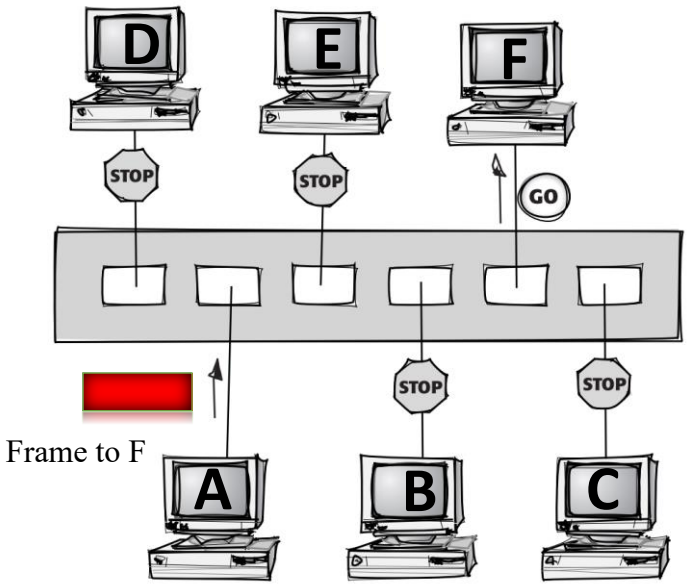


Figure 1.6 Filtering of a Switch

Switch

A switch is a multiport bridge. Their packet-forwarding decisions are based on MAC addresses. That is, a switch simply looks at each packet and determines from a physical address (the MAC address) which device a packet is intended for and then switches it out toward that device. For example, let's consider Fig. 1.6. When the switch receives the frame from computer A with a MAC address F. Then, it checks its MAC address table to know the interface to which a device with MAC address F is connected. After getting a match, it will forward the frame only through that interface. Switches allow LANs to be segmented, thereby increasing the amount of bandwidth that goes to each device. This means that, unlike a hub, each port on the switch is like a network segment itself. If you have a 10-Mpbs switch with three devices connected to it, all three devices can use 10-Mbps of bandwidth. A switch repeats data only to the specified port, whereas a hub sends the data to all ports. In this context, it is said that each segment is a separate collision domain but all segments are in the same broadcast domain. The basic functions of a switch include filtering and forwarding frames, learning media access control (MAC) addresses, and preventing loops.

In wide area networks such as the Internet, the destination address requires them to be looked up in a routing table by a device known as a router. Some newer switches also perform routing functions. These switches are sometimes called IP switches or layer 3 switches.

Router

A router is a three-layer device. A router can connect LANs together; a router can connect WANs together; and a router can connect LANs and WANs together. In other words, a router is an internetworking device; it connects independent networks together to form an internetwork.

According to this definition, two networks (LANs or WANs) connected by a router become an internetwork or an internet. There are three major differences between a router and a repeater or a bridge.

1. A router has a physical and logical (IP) address for each of its interfaces.
2. A router acts only on those packets in which the physical destination address matches the address of the interface at which the packet arrives.
3. A router changes the physical address of the packet (both source and destination) when it forwards the packet.

Let us see an example. In Fig. 1.7, assume an organization has two separate buildings with a Gigabit Ethernet LANs installed in each building. The organization uses switch in each LAN. The two LANs can be connected together to form a larger LAN using Ten-Gigabit Ethernet technology that speeds up the connection to the Ethernet and the connection to the organization server. A router then can connect the whole system to the Internet.

In the setup depicted in Fig. 1.8, if a workstation in workgroup A wants to print to the printer in workgroup B, it creates a transmission containing the address of the workgroup B printer. Then, it sends its packets to switch A. When switch A receives the transmission, it checks the MAC address for the printer and determines that the message needs to be forwarded. It forwards the message to router A. Router A examines the destination network address in each packet and consults its router

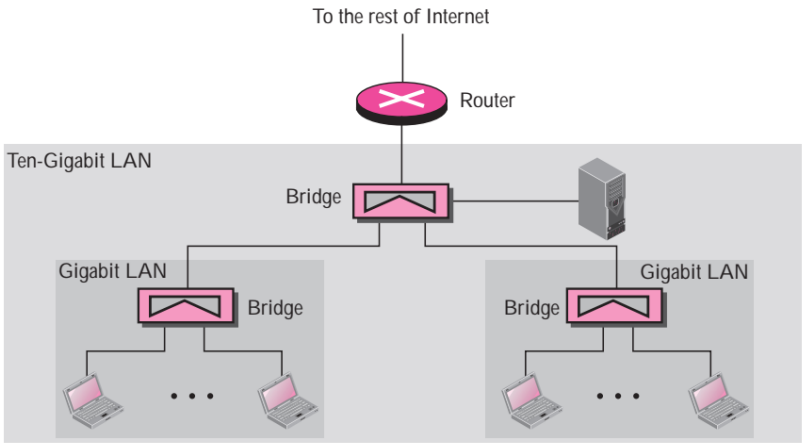


Figure 1.7 Routing example

table to find out where the packet needs to go and then determines the most efficient way of delivering the message. In this example, it sends the data to router B. Before it forwards the data, however, router A increments (increases) the number of hops tallied in all the packets. Each time a packet passes through a router, it has made a hop. Packets can only take a certain number of hops before they are discarded. After it increments the number of hops tallied in each packet, router A forwards the data to router B. Router B increments each packet's hop count, reads each packet's destination network address, and sends them to switch B. Based on the destination MAC address in the packets, switch B delivers the transmission to workgroup B. The printer picks up the message, and then begins printing.

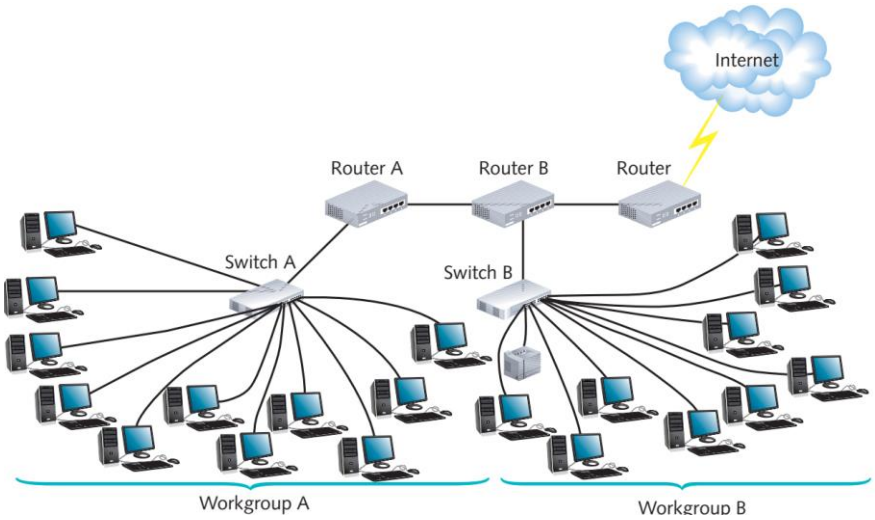


Figure 1.8 Router connecting multiple networks

1.5 Collision domain and broadcast domain

Collision Domain

The “collision domain” describes a network where packet collisions can occur when two devices on a shared network medium send packets simultaneously. The colliding packets are discarded and must be sent again, which reduces network speed and efficiency. Usually, collisions occur in a hub environment, because each port on a hub is in the same collision domain. So, all devices connected to the hub are in the same collision domain and only one device can transmit at a time, and all other devices must listen to the network in order to avoid collisions. Total network bandwidth is shared among all devices.

In contrast to hubs, each port on a bridge, switch, or a router is in different collision domain which reduces and eliminates the possibility of collisions and enables the devices to use the full-duplex communication. The full-duplex communication effectively doubles the speed of data capacity. To understand the collision domains, examine Fig.1.9.

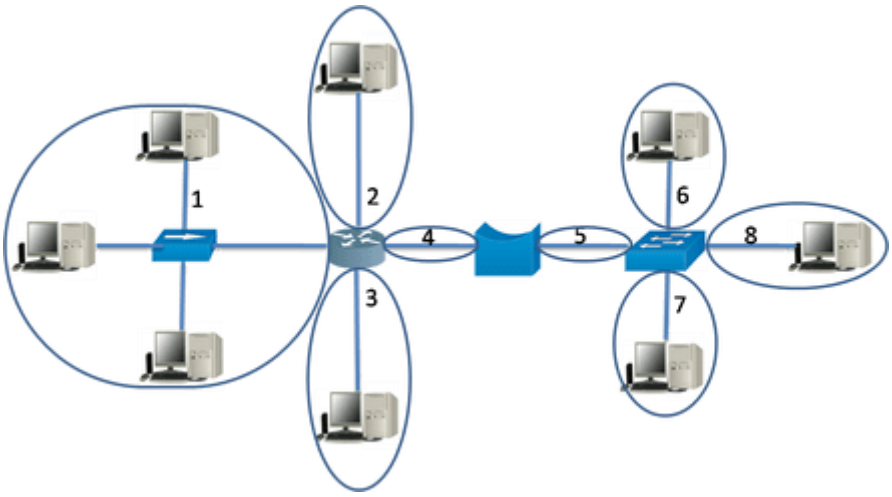


Figure 1.9 Illustration of collision domain

You can see that there is eight collision domain marked in the above topology. Because the hub is single collision domain or all ports of the hub are in single collision domain but each port of the router, bridge and switch are separate collision domain.

Broadcast Domain

All the devices in the broadcast domain can reach via broadcast at the data link layer. A Broadcast domain can receive any broadcast packet originating from any device within the network segment. All ports of hub and switch belong to same broadcast domain but all ports of the router belong to a different broadcast domain.

All ports of the hub and switch are in the same broadcast domain. Hub and Switches send broadcasts out all interfaces except the interface on which it received. Routers do not transmit broadcasts because when a router receives a broadcast, it does not forward it out to other interfaces.

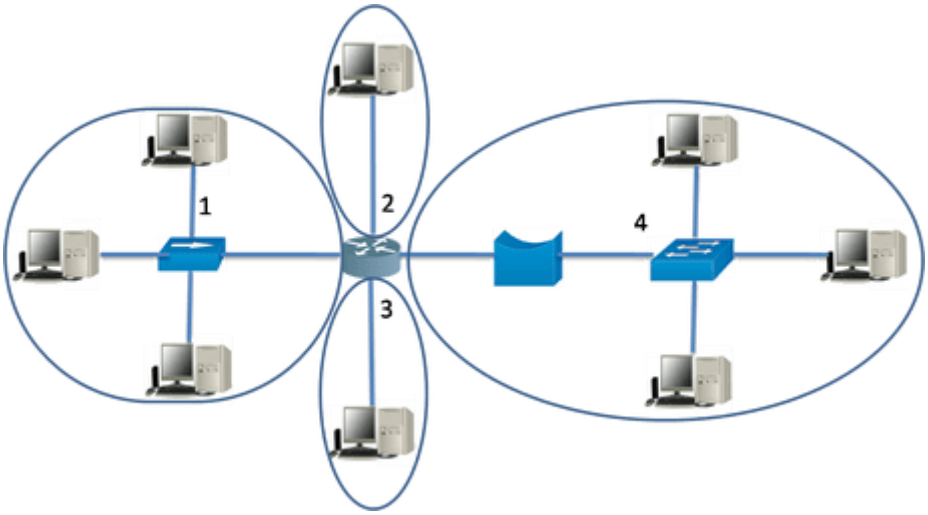


Figure 1.10 Illustration of broadcast domain

Each interface of the router belongs to the different broadcast domain and each broadcast is only propagated within its specific domain. Routers separate the boundaries of the broadcast domains. Now examine the previous network (Fig. 1.9) for the broadcast domain analysis (see Fig. 1.10). In Fig. 1.10, we can see four broadcast domains marked. Because all ports on a hub, bridge and a switch are in the same broadcast domain and all interfaces of the router are in a different broadcast domain.

Layer 2 devices send broadcasts known as ARP to a known IPv4 address on the local network to discover the associated MAC address. The host can get IP address configuration using the Dynamic Host Configuration Protocol (DHCP) from the DHCP server. A large broadcast domain can connect many hosts. A problem with a large broadcast domain is to generate excessive broadcasts and negatively affect the network.

A large number of Broadcasts also decrease the bandwidth of the network for normal traffic because the broadcast traffic is forwarded to all the devices in the domain. It also decreases the processing power of computers and network devices. Because the computers and network devices need to process all the broadcast packets received a part of the CPU power spent on processing the broadcast packets.

1.6 Network Standards

Ethernet Standards

Speed	Common Name	Informal Standard Name	Formal Standard Name	Cable Type	Max. Length
10 Mbps	Ethernet	10BASE-T	802.3	Cat3	100 m
100 Mbps	Fast Ethernet	100BASE-T	802.3u	Cat5	100 m
1000 Mbps	Gigabit Ethernet	1000BASE-LX	802.3z	Single mode fiber	5000 m
				50-micron multimode fiber	550 m
				62.5-micron multimode fiber	440 m
1000 Mbps	Gigabit Ethernet	1000BASE-T	802.3ab	Cat5, Cat5e	100 m
10 Gbps	10 Gig bit Ethernet	10GBASE-T	802.3an	Cat6, Cat6a	100 m

WLAN Standards

Release date	Standard	Frequency band	Bandwidth	Transmission scheme	Max modulation	MIMO	Max data rate
1997	802.11	2.4 GHz	20 MHz	DSSS, FHSS	QPSK	N/A	2 Mbps
1999	802.11b	2.4 GHz	20 MHz	DSSS	QPSK	N/A	11 Mbps
1999	802.11a	5 GHz	20 MHz	OFDM	64 QAM	N/A	54 Mbps
2003	802.11g	2.4 GHz	20 MHz	DSSS, OFDM	64 QAM	N/A	54 Mbps
2009	802.11n	2.4 GHz 5 GHz	20 MHz 40 MHz	OFDM	64 QAM	4×4	600 Mbps
2013	802.11ac	5 GHz	20 MHz 40 MHz 80 MHz 160 MHz	OFDM	256 QAM	8×8	6.93 Gbps
2018	802.11ad	60 GHz	2160 MHz	SC-FDM, OFDM	256 QAM	Beamforming	6.93 Mbps

Abbreviations:

DSSS: Direct sequence spread spectrum

FHSS: Frequency hop spread spectrum

OFDM: Orthogonal Frequency Division Multiplexing

SC FDM: Single carrier frequency domain multiplexing

QPSK: Quadrature phase shift keying

QAM: Quadrature amplitude modulation

MIMO: Multiple input multiple output

Beamforming: Technique of focusing a wireless signal towards a specific receiving device