Year	Standard	Description
1998	IEEE 802.3z 1000BaseX	Gigabit Ethernet over fiber optic.
1999	IEEE 802.3ab 1000BaseT	Gigabit Ethernet over twisted pair.
2002	IEEE 802.3ae 10GBase-xx	10 Gigabit Ethernet over fiber (various standards).
2006	IEEE 802.3an 10GBaseT	10 Gigabit Ethernet over UTP.

Physical Addressing

All communication requires a way to identify the source and destination. The source and destination in human communication are represented by names. When a name is called, the person with that name listens to the message and responds. Other people in the room might hear the message, but they ignore it because it is not addressed to them.

On Ethernet networks, a similar method exists for identifying source and destination hosts. Each host connected to an Ethernet network is assigned a physical address that serves to identify the host on the network.

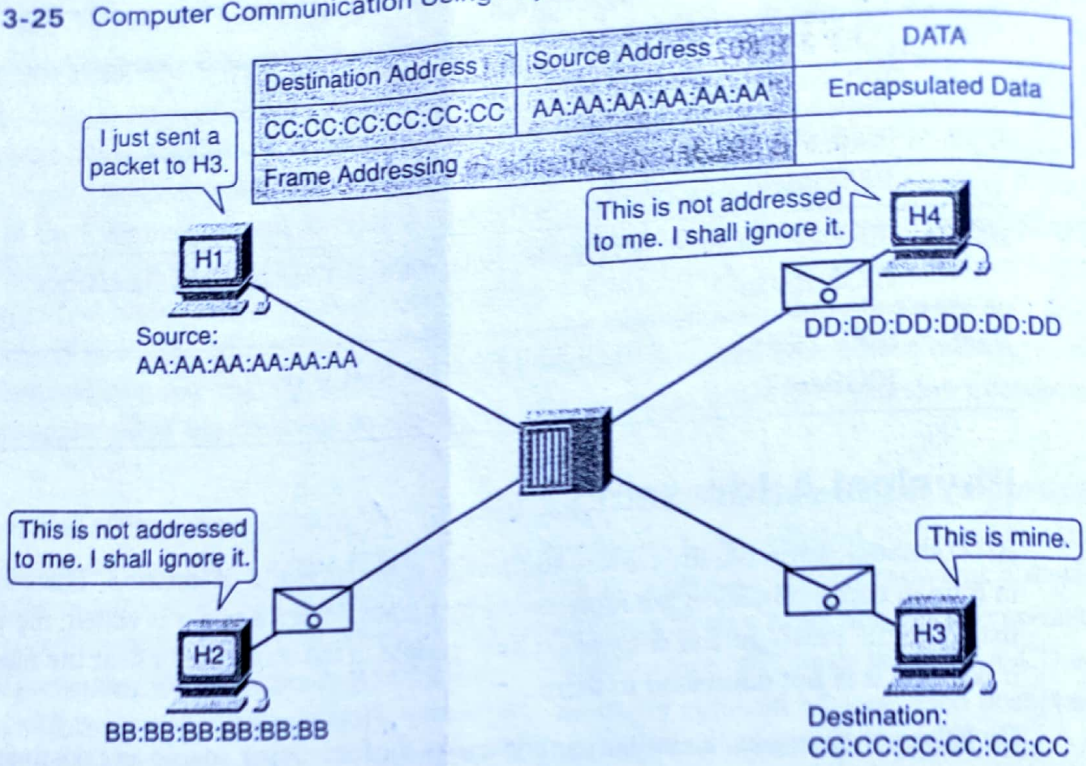
Every Ethernet network interface has a physical address assigned to it when it is manufactured. This address is known as the *Media Access Control (MAC) address*. The MAC address identifies each source and destination host on the local network. The MAC address is a 48-bit address that is normally represented as 12 hexadecimal (hex) characters of 4 bits each. An example of a MAC address is 00-1B-53-8A-4E-01. The first six hex characters (24 bits) represent the manufacturer of the Ethernet interface and are known as the Organizational Unique Identifier (OUI). The last 24 bits identify a particular interface or NIC from that manufacturer. The OUI is assigned to an organization by the IEEE to ensure that MAC addresses are not duplicated. In the example 00-1B-53-8A-4E-01, 00-1B-53 indicates that this Ethernet interface was manufactured by Cisco. In this case the interface is on a Cisco router. Cisco devices display the MAC address using the format 001B.538A.4E01. The MAC address is the same in either case, just a different display format.

Ethernet networks are cable based, meaning that a copper or fiber-optic cable connects hosts and networking devices. This is the channel used for communications between the hosts.

When a host on an Ethernet network communicates, it sends frames containing its own MAC address as the source and the MAC address of the intended recipient. Any hosts that receive the frame will decode the frame and read the destination MAC address. If the destination MAC address matches the address configured on the NIC, it will process the message and store it for the host application to use. If the destination MAC address does not match the host MAC address, the NIC will ignore the message. Figure 3-25 shows a host sending a frame out on an Ethernet network. Although other hosts might see the frame, only the host to which it is addressed will accept it.

The newer Windows operating systems provide a method of displaying the host's MAC address using a GUI Network Connection application. You may also use the command line **ipconfig** command. The UNIX and Linux operating systems can also use GUI applications to view computer addresses but use the **ifconfig** command, instead, from the command line.

Figure 3-25 Computer Communication Using Physical Addresses



Lab 3-2: Determine the MAC Address of a Host (3.3.3.2)

In this lab you use the **ipconfig /all** command to determine the MAC address of your computer. Refer to the hands-on lab in Part II of this *Learning Guide*. You may perform this lab now or wait until the end of the chapter.

Ethernet Communication

Ethernet protocol standards define many aspects of network communication including frame format, frame size, timing, and encoding.

When messages are sent between hosts on an Ethernet network, the hosts format the messages into the frame layout that is specified by the standards. Frames are one type of data grouping in a family referred to as *protocol data units (PDU)*.

The format for Ethernet frames specifies the location of the destination and source MAC addresses, and additional information including

- Preamble for sequencing and timing
- Start of frame delimiter
- Length and type of frame
- Frame check sequence to detect transmission errors

Figure 3-26 shows the structure of a standard IEEE 802.3 frame. Note that the maximum amount of data that the frame can contain is 1500 bytes.

Figure 3-26 Structure of the Ethernet Frame

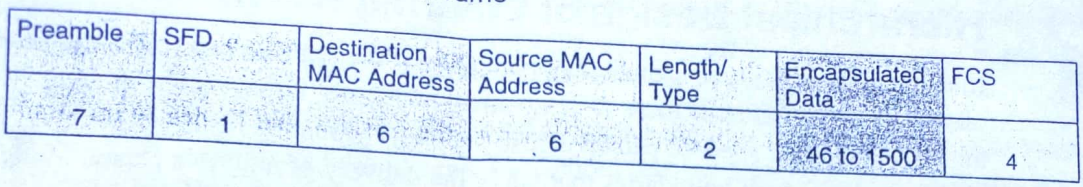


Table 3-2 lists the main components of the Ethernet frame and provides a brief description of their purpose or function.

Table 3-2 Fields in an Ethernet Frame

Frame Field	Bytes	Description / Contents
Preamble	7	Used to announce data transmission.
Start of Frame Delimiter (SFD)	1	Marks the end of the timing information and start of the frame.
Destination MAC Address	6	Contains the destination MAC address (receiver). The destination MAC address can be unicast (a specific host), multicast (a group of hosts), or broadcast (all hosts on the local network).
Source MAC Address	6	Contains the source MAC address (sender). This is the unicast address of the Ethernet node that transmitted the frame.
Length/Type	2	Supports two different uses. A type value indicates which protocol will receive the data. The length indicates the number of bytes of data that follows this field.
Encapsulated Data	46 to 1500	Contains the packet of information being sent. Ethernet requires each frame to be between 64 and 1518 bytes.
Frame Check Sequence (FCS)	4	Contains a 4-byte value that is created by the device that sends data and is recalculated by the destination device to check for damaged frames.

The size of Ethernet frames is limited to a maximum of 1518 bytes and a minimum size of 64 bytes. Frames that do not fall within these limits are not processed by the receiving hosts. By adding the number of bytes for the data (1500 bytes), destination MAC address (6 bytes), source MAC address (6 bytes), length/type (2 bytes), and the FCS (4 bytes) we arrive at the maximum Ethernet frame size of 1518 bytes. The preamble and the SFD are not counted in the total frame size because they are only there for timing and to indicate where the frame begins.

In addition to the frame format, size, and timing, Ethernet standards define how the bits making up the frames are encoded onto the channel. Bits are transmitted as either electrical impulses over copper cable or as light impulses over fiber-optic cable.

Interactive Activity 3-6: Building an Ethernet Frame (3.3.4.2)

In this interactive activity you build a standard IEEE 802.3 Ethernet frame based on the source and the destination device. Use file ia-3342 on the CD-ROM that accompanies this book to perform this interactive activity.

In networking, hierarchical design is used to group devices into multiple networks that are organized in a layered approach. It consists of smaller, more manageable groups that allow local traffic to remain local. Only traffic that is destined for other networks is moved to a higher layer.

A hierarchical, layered design provides increased efficiency, optimization of function, and increased speed. It allows the network to scale or grow as required because additional local networks can be added without impacting the performance of the existing ones.

The hierarchical design has three basic layers:

- **Access layer**: To provide connections to hosts in a local Ethernet network
- **Distribution layer**: To interconnect the smaller local networks
- **Core layer**: High-speed connections between distribution layer devices

With this new hierarchical design comes a need for a logical addressing scheme that can identify the location of a host. This is the Internet Protocol (IP) addressing scheme. Figure 3-28 shows how networks can also be hierarchical in nature.

To expand the telephone analogy, the telephone network is an extremely large physical network but it is divided logically using a phone number addressing scheme. To properly route a call, a phone number consists of a hierarchy structured using prefixes (local access networks), area codes (distribution networks), and country codes (core networks). If you make a long-distance call, you must include the area code in the number you dial. Doing so ensures that the telephone system knows to route your call to the right area. This analogy illustrates a logical division of a physical network.

Logical Addressing

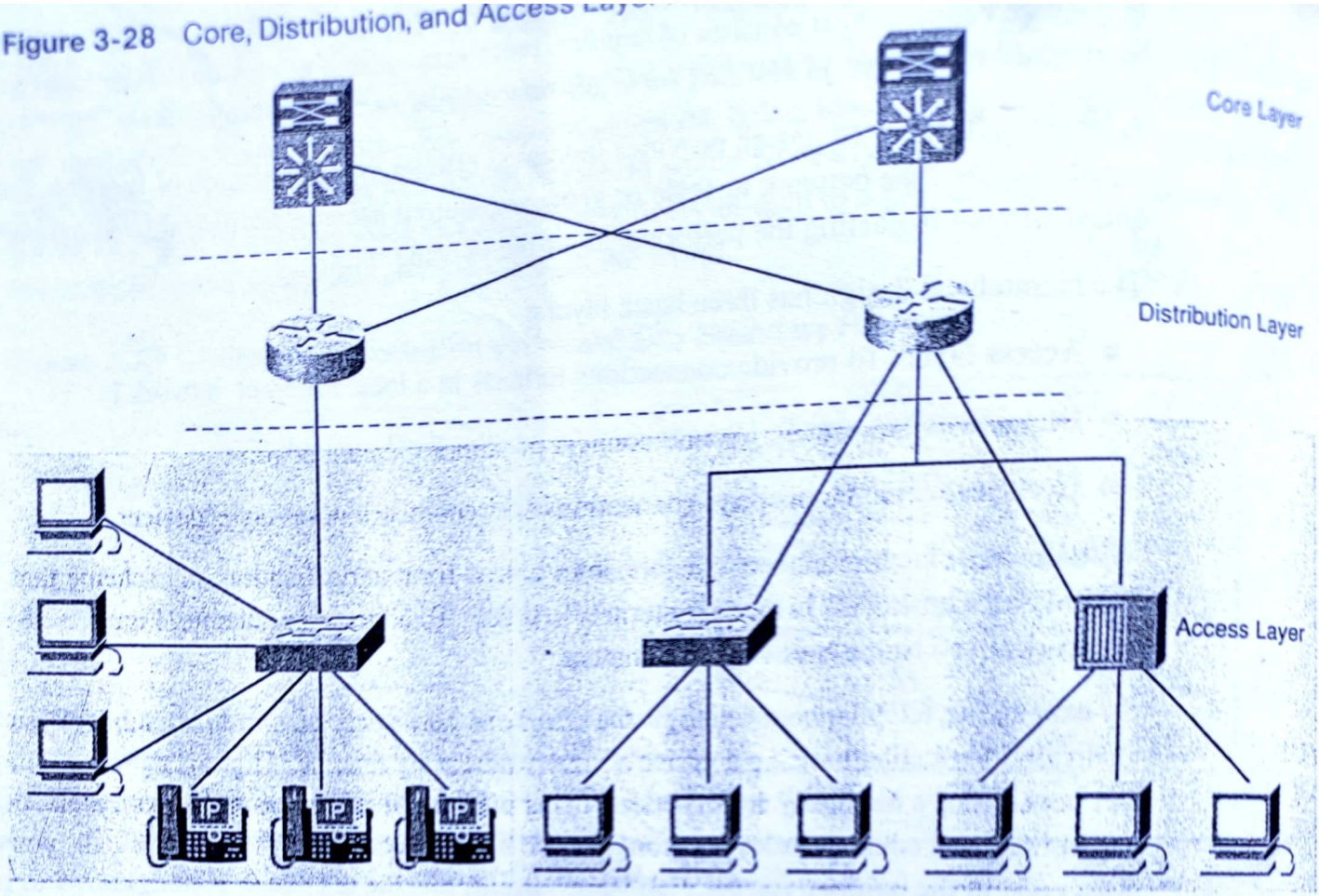
A person's given name usually does not change. A person's address, on the other hand, relates to where they live and can change. On a host, the MAC address, also known as the physical or hardware address, does not change; it is physically assigned to the host NIC. The ***physical address*** remains the same regardless of where the host is placed on the network.

The IP address is similar to the mailing address of a person. It is known as a ***logical address*** because it is assigned logically based on where the host is located. A network administrator assigns the IP address to each host based on the local network where it resides. Both the physical MAC and logical IP addresses are required for a computer to communicate on a hierarchical network, just as both the name and address of a person are required to deliver a letter.

IP addresses contain two parts: the local network and the host. The network portion of the IP address will be the same for all hosts connected to the same local network. The second part of the IP address identifies the individual host. Within the same local network, the host portion of the IP address is unique to each host.

In Figure 3-29, host H3 is on network 192.168.200 and the individual host portion of the address on that network is .3. Hosts H1, H2, and H4 are also on the 192.168.200 network. Host H8 is on the 192.168.1 network and its host address is .4. Note that the host portion of the address for host H4 (.4) is the same as for host H8 (.4). This is not a problem because they live on different networks using a hierarchical network design where a two-part address is employed. When a packet is sent to H4's IP address, it is sent to 192.168.200.4. When a packet is sent to H8's IP address, it is sent to 192.168.1.4.

Figure 3-28 Core, Distribution, and Access Layer



Lab 3-3: Determine the IP Address of a Computer (3.3.6.2)

In this lab you use the **ipconfig /all** command to display the IP address of your computer. Refer to the hands-on lab in Part II of this *Learning Guide*. You may perform this lab now or wait until the end of the chapter.

Access, Distribution, and Core Layers and Devices

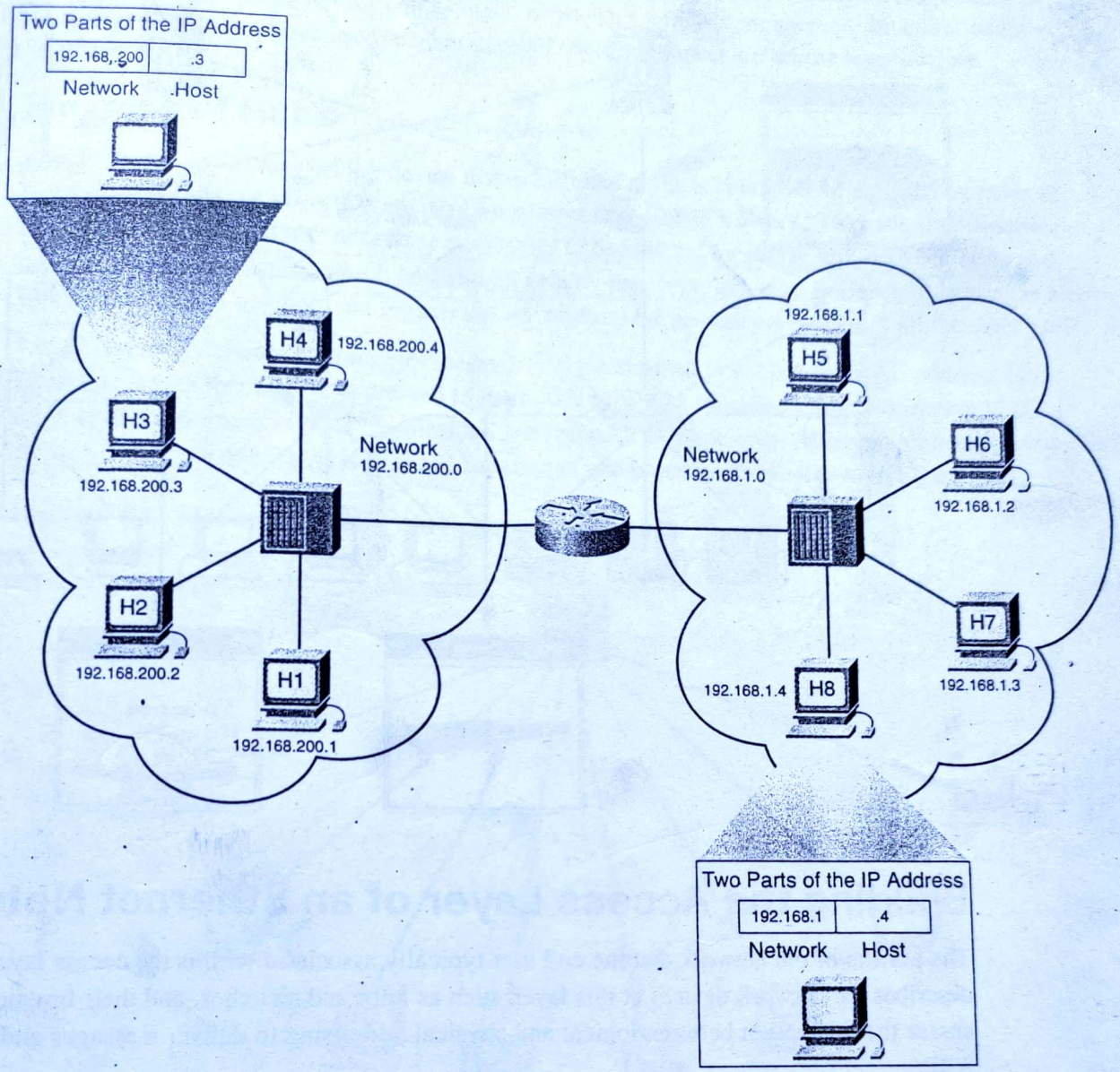
IP traffic is managed based on the characteristics and devices associated with each of the three layers: access, distribution, and core. The IP address is used to determine whether traffic should remain local or be moved up through the layers of the hierarchical network.

The access layer provides a connection point to the network for end-user devices and allows multiple hosts to connect to other hosts through a network device. Typically, all devices within a single access layer area will have the same network portion of the IP address.

If a message is destined for a local host, based on the network portion of the IP address, the message remains local. If it is destined for a different network, it is passed up to the distribution layer. Hubs and switches provide the connection to the distribution layer devices, usually a router.

The distribution layer provides a connection point for separate local networks and controls the flow of information between the networks. It typically contains more powerful switches than the access layer as well as routers for routing between networks. In a three-layer design, distribution layer devices also control the type and amount of traffic that flows from the access layer to the core layer.

Figure 3-29 Network Address and Host Address



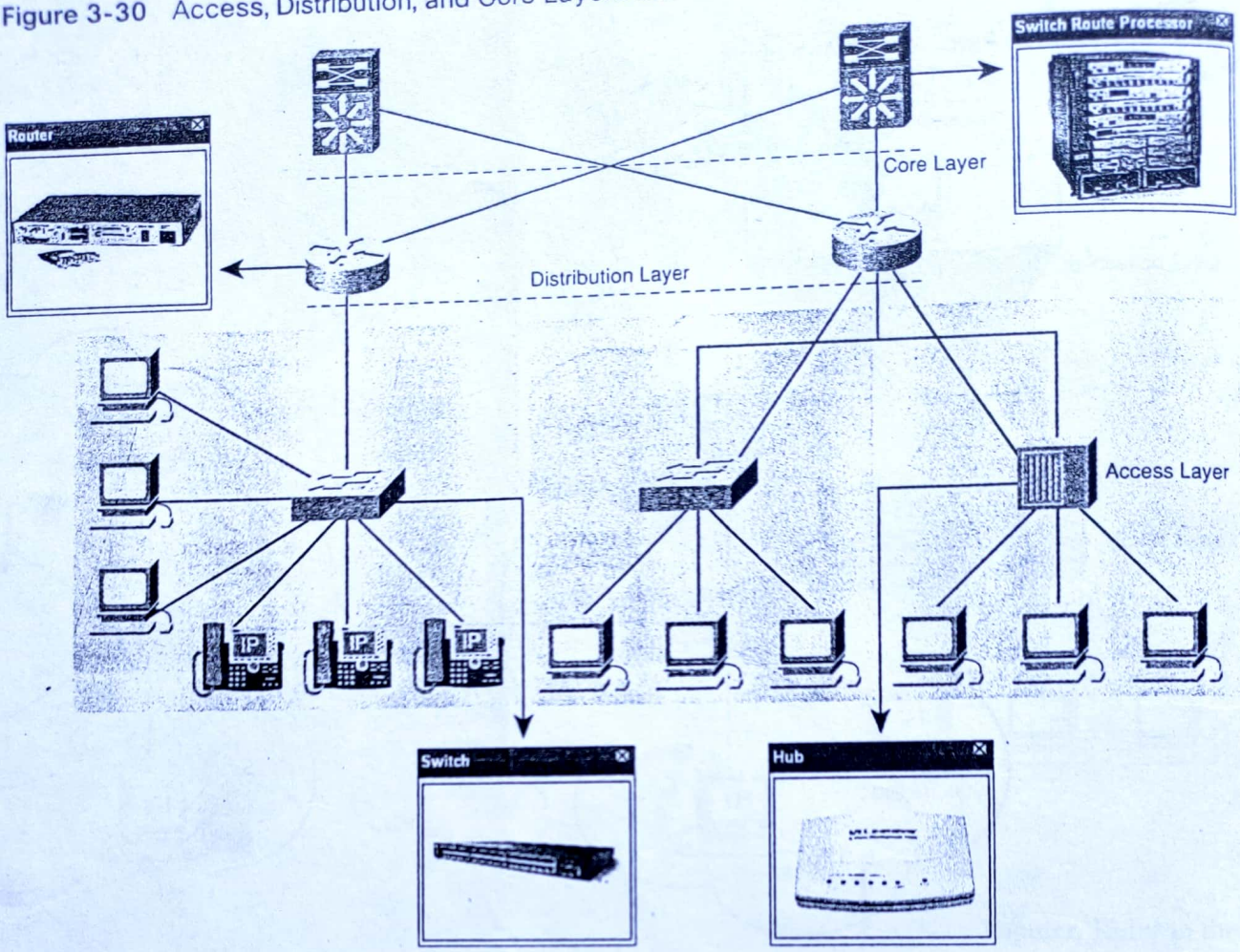
The core layer is a high-speed backbone layer with redundant (backup) connections. It is responsible for transporting large amounts of data between multiple end networks. Core layer devices typically include very powerful, high-speed switches and routers. The main goal of the core layer is to transport data quickly. Hubs, switches, and routers are discussed in more detail in the next two sections "Building the Access Layer of an Ethernet Network" and "Building the Distribution Layer of a Network."

Figure 3-30 shows a conceptual diagram of the three-layer network design and also provides photographs of the type of devices that represent the icons shown.

Interactive Activity 3-7: Working with Addresses, Network Components, and Layers (3.3.7.2)

In this interactive activity you determine which addresses, network components, and layers are necessary to accomplish each task. Use file ia-3372 on the CD-ROM that accompanies this book to perform this interactive activity.

Figure 3-30 Access, Distribution, and Core Layers and Devices



Building the Access Layer of an Ethernet Network

The portion of the network that the end user typically associates with is the access layer. This section describes the network devices at this layer, such as hubs and switches, and their functions. It also discusses the interaction between logical and physical addressing to deliver messages and introduces ARP.

Access Layer

The *access layer* is the most basic level of the network. It is the part of the network in which people gain access to other hosts and to shared files and printers. The access layer is composed of host devices, as well as the first line of networking devices to which they are attached.

Networking devices enable us to connect many hosts with each other and also provide these hosts access to services offered over the network. Unlike the simple network consisting of two hosts connected by a single cable, in the access layer, each host is connected to a networking device.

Within an Ethernet network, each host is able to connect directly to an access layer networking device using a point-to-point cable. These cables are manufactured to meet specific Ethernet standards and are used to connect the host NIC to a port on the networking device. Several types of networking devices can be used to connect hosts at the access layer, including Ethernet hubs and switches. Some devices, such as IP phones, should be attached only to switches in order to function properly.

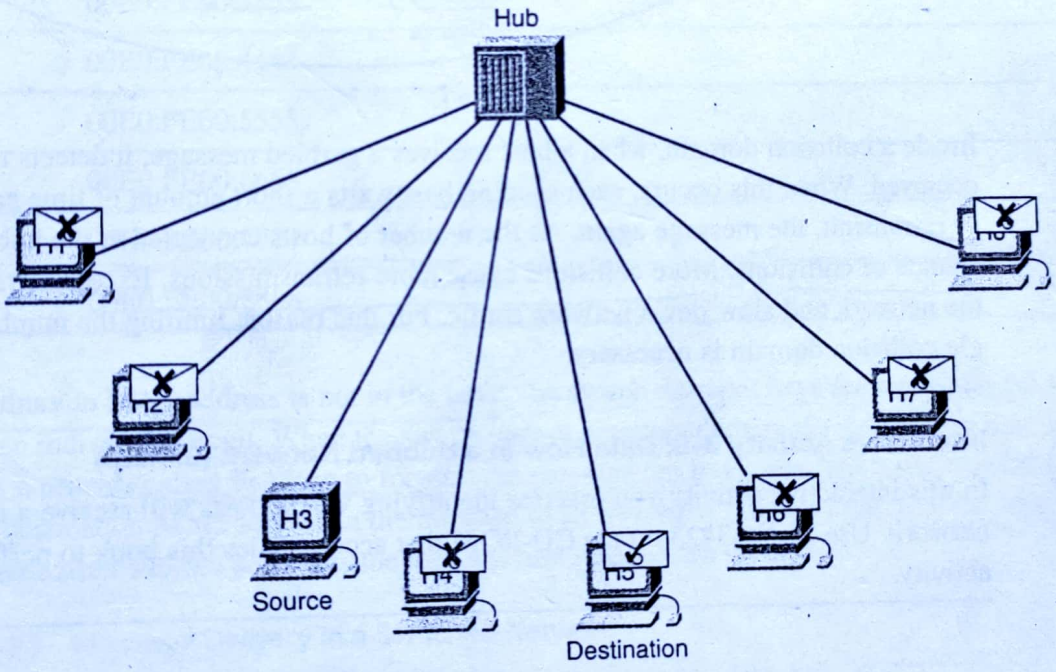
An increasing number of business and home users are installing wireless access to allow users to connect without the requirement for cumbersome wires. This wireless connectivity functions at the access layer, and the access points used to allow the end users to connect are access layer devices.

Function of Hubs

A *hub* is one type of networking device that is installed at the access layer of an Ethernet network. Hubs contain multiple ports that are used to connect hosts to the network. They are simple networking devices that do not have the necessary electronics to decode the messages sent between hosts and therefore cannot determine which host should get any particular message. A hub simply accepts electronic signals from one port and regenerates (or repeats) the same message out of all the other ports.

Recall that the NIC on a host accepts messages only addressed to the correct MAC address. Hosts ignore messages that are not addressed to them. Only the host specified in the destination MAC address of the frame processes the message and responds to the sender. Although all hosts receive the message, only the one that it is destined for accepts and processes it, as shown in Figure 3-31.

Figure 3-31 Message Delivery in a Hub-Based Network

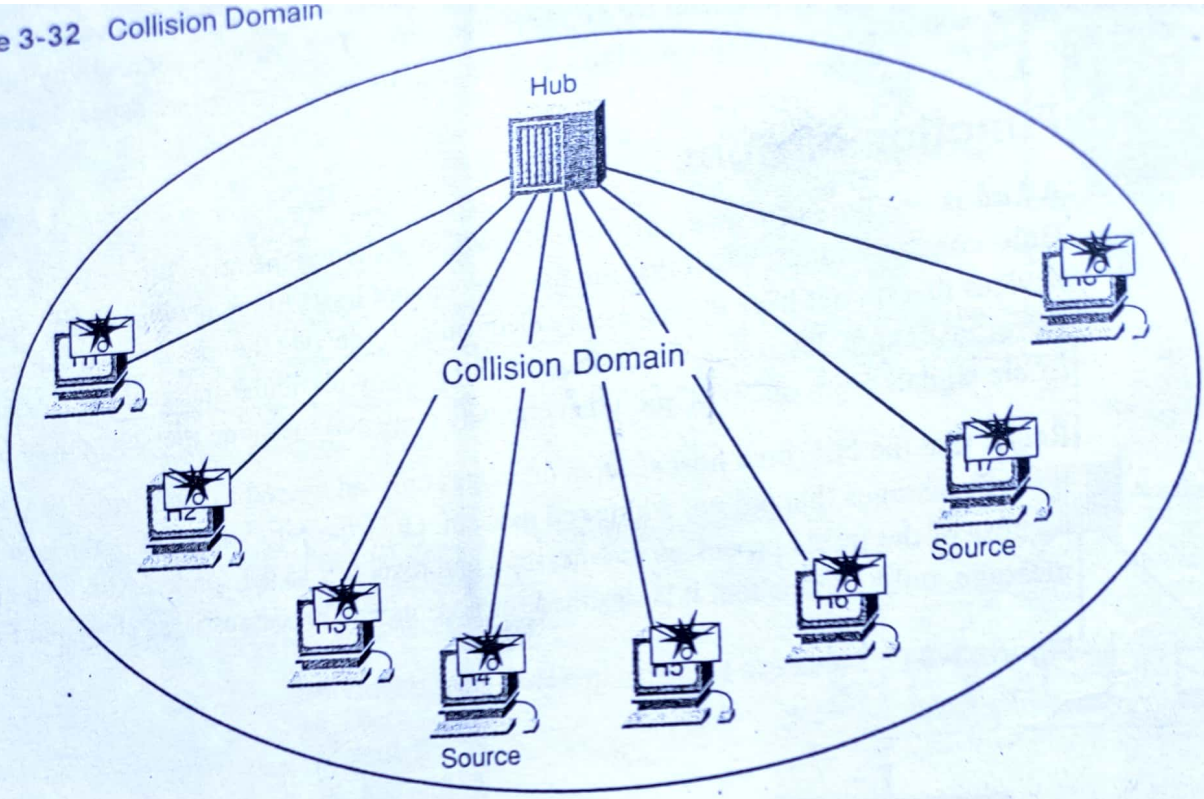


All the ports on the Ethernet hub connect to the same channel to send and receive messages. Because all hosts must share the bandwidth available on that channel, a hub is referred to as a *shared-bandwidth* device.

Because an Ethernet hub consists of a single channel, only one message can be sent through the hub at a time. If two or more hosts connected to a hub attempt to send a message at the same time, the electronic signals that make up the messages collide with each other on the channel.

A collision causes the messages to become garbled and unreadable by the hosts. A hub does not decode the messages; therefore it does not detect that the message is garbled and repeats it out all the ports, wasting valuable bandwidth. The area of the network where a host can receive a garbled message resulting from a collision is known as a ***collision domain***. Figure 3-32 illustrates such a collision domain.

Figure 3-32 Collision Domain



Inside a collision domain, when a host receives a garbled message, it detects that a collision has occurred. When this occurs, each sending host waits a short amount of time and then attempts to send, or retransmit, the message again. As the number of hosts connected to the hub increases, so does the chance of collisions. More collisions cause more retransmissions. Excessive retransmissions can clog the network and slow down network traffic. For this reason, limiting the number of hosts within a single collision domain is necessary.

Interactive Activity 3-8: Data Flow in a Hubbed Network (3.4.2.3)

In this interactive activity you practice identifying which hosts will receive a message on a hub-based network. Use file ia-3423 on the CD-ROM that accompanies this book to perform this interactive activity.

Function of Switches

Because of the problems associated with being a shared bandwidth device, hubs are no longer commonly deployed at the access layer. Most modern Ethernet networks employ a device known as an Ethernet switch to connect hosts into the network. Like a hub, a switch connects multiple hosts to the network. Unlike a hub, a switch can make decisions based on the information contained within the Ethernet frame and can forward a message to a specific host. When a host sends a message to another host on the switch, the switch accepts and decodes the frames to read the physical (MAC) address portion of the message.

A table on the switch, called a ***MAC address table***, contains a list of all the active ports and the host MAC addresses that are attached to them. When a message is sent between hosts, the switch checks to see whether the destination MAC address is in this table. If it is, the switch builds a temporary connection, called a circuit, between the source and destination ports. This new circuit provides a

dedicated channel over which the two hosts can communicate. Other hosts attached to the switch do not share the bandwidth on this channel and do not receive messages that are not addressed to them. A new circuit is built for every new conversation between hosts. These separate circuits allow many conversations to take place at the same time, without collisions occurring.

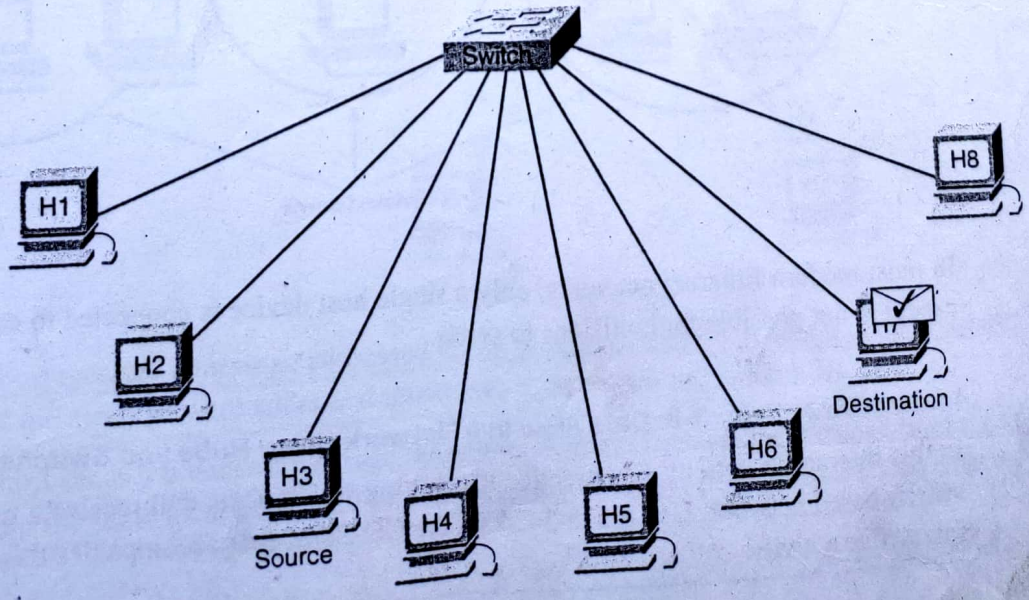
In Figure 3-33 host H3 is connected to fast Ethernet port fa0/3. H3, with a MAC address of 00E0:FE00:3333, and is sending a frame to host H7 that is connected to port fa0/7 at MAC address 00E0:FE00:7777. The MAC address table for the switch is shown in Table 3-3. Please note that the MAC addresses shown are for illustration only. The MAC addresses in the table are the MAC addresses of the connected device and are not related to the switch port number. Because the destination MAC address is already in the MAC address table, the switch forwards the message to the correct destination.

Table 3-3 A MAC Address Table

Switch Port	Device MAC Address
fa 0/1	00E0:FE00:1111
fa 0/2	00E0:FE00:2222
fa 0/3	00E0:FE00:3333
fa 0/4	00E0:FE00:4444
fa 0/5	00E0:FE00:5555
fa 0/6	00E0:FE00:6666
fa 0/7	00E0:FE00:7777
fa 0/8	00E0:FE00:8888

If the destination MAC address is not in the table, the switch does not have the necessary information to create an individual circuit. When the switch cannot determine where the destination host is located, it uses a process called ***flooding*** to forward the message out to all attached hosts. Each host compares the destination MAC address in the message to its own MAC address, but only the host with the correct destination address processes the message and responds to the sender.

Figure 3-33 Message Delivery in a Switched Network



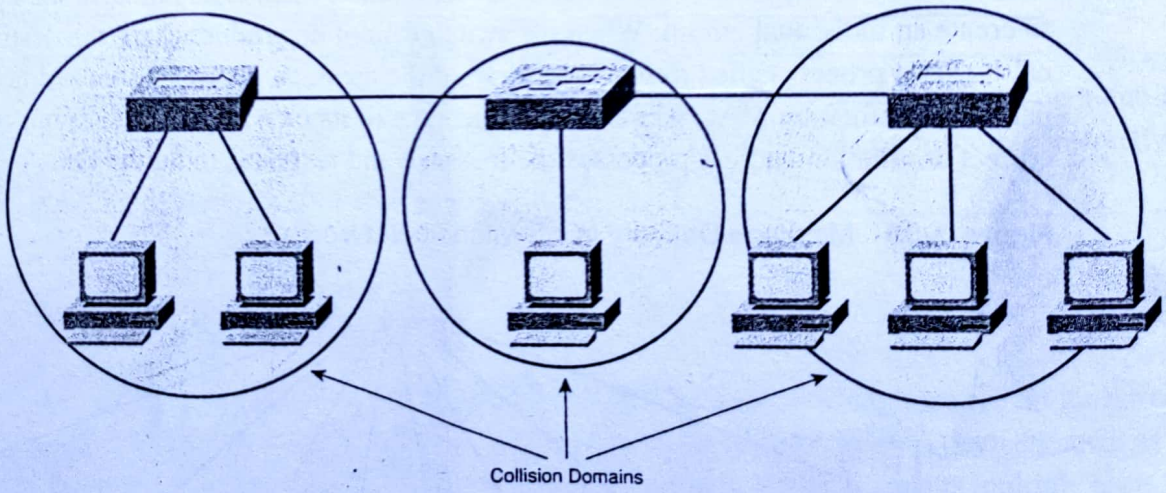
A switch builds the MAC address table by examining the source MAC address of each frame that is sent between hosts. When a new host sends a message or responds to a flooded message, the switch immediately learns its MAC address and the port to which it is connected. The table is dynamically updated each time a new source MAC address is read by the switch. In this way, a switch quickly learns the MAC addresses of all attached hosts.

In this case the destination MAC address is not in the MAC address table and the message must be flooded out all ports except the one that the message was received on. When H7 responds to the original message, the switch updates its MAC address table with the MAC address of H7 and associates it with the inbound port, fa0/7. These entries are not normally permanent and expire after a certain period of time. This reduces the chance that the switch will have a stale entry in the MAC address table, which could cause it to send frames out the wrong port.

Sometimes, connecting another networking device, such as a hub, to a switch port is necessary. Doing so increases the number of hosts that can be connected to the network. When a hub is connected to a switch port, the switch associates the MAC addresses of all hosts connected to that hub with the single port on the switch. Occasionally, one host on the attached hub sends a message to another host attached to the same hub. In this case, the switch receives the frame and checks the table to see where the destination host is located. If both the source and destination hosts are located on the same port, the switch does not forward or flood the message out any other port.

When a hub is connected to a switch port, collisions can occur. If this happens, the hub forwards the damaged message, resulting from the collision, to all ports. The switch receives the garbled message, but, unlike a hub, a switch does not forward the damaged messages. As a result, every switch port creates a separate collision domain. This is shown in Figure 3-34. The creation of multiple collision domains is good because it limits the number of hosts contained in each. The fewer hosts contained in a collision domain, the less likely it is that a collision will occur.

Figure 3-34 Collision Domains in a Switched Network



In most modern Ethernet networks, only a single host device is connected to each switch port. In this case it is not possible for collisions to occur.

Interactive Activity 3-9: Data Flow in a Network Using Hubs and Switches (3.4.3.4)

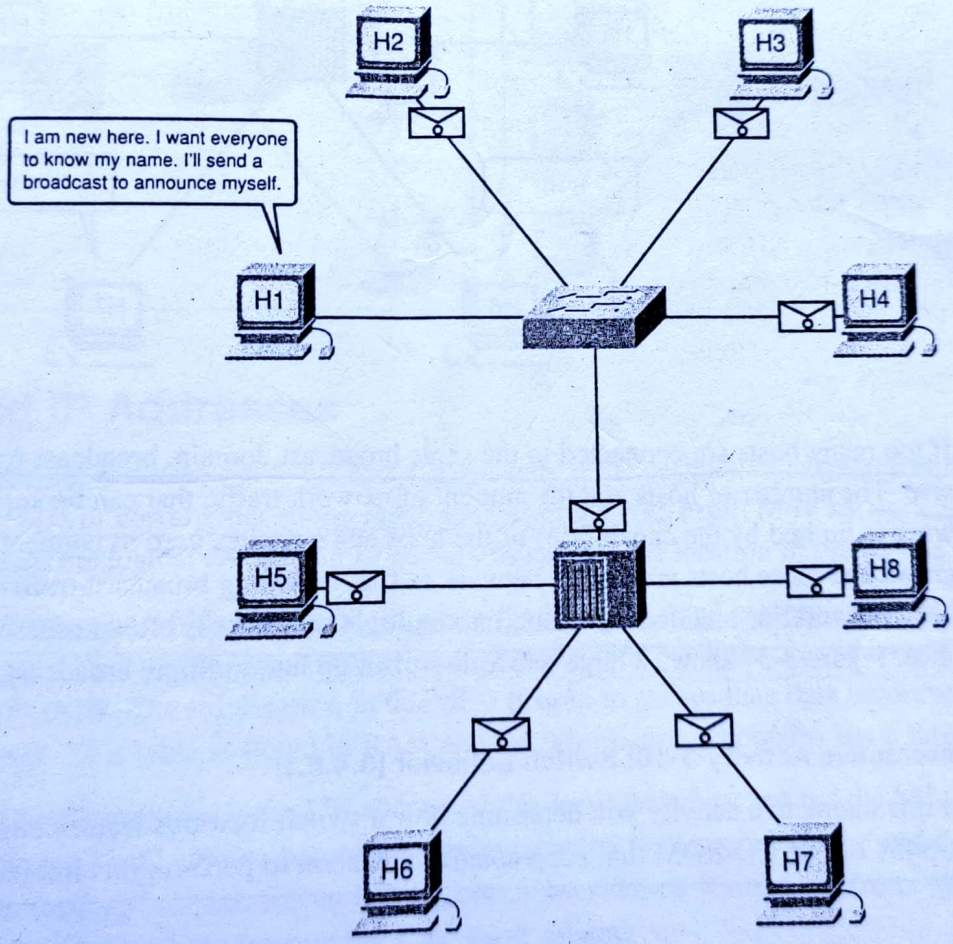
In this interactive activity you practice identifying which hosts will receive a message on a hub and switch-based network. Use file ia-3434 on the CD-ROM that accompanies this book to perform this interactive activity.

Broadcast Messaging

When hosts are connected using a hub or a switch, a single *local network* is created. Within the local network often one host needs to be able to send messages to all the other hosts at the same time. It can perform this task using a broadcast message. Broadcasts are useful when a host needs to find information without knowing exactly which other host can supply the information. Broadcasts are also used to send information to all hosts on a network.

A message can contain only one destination MAC address. So, how is it possible for a host to contact every other host on the local network without sending out a separate message to each individual MAC? To solve this problem, broadcast messages are sent to a unique MAC address that is recognized by all hosts. The broadcast MAC address is a 48-bit address made up of all 1s. Because of their length, MAC addresses are usually represented in ***hexadecimal*** notation. The broadcast MAC address in hexadecimal notation is FFFF.FFFF.FFFF. Each F in the hexadecimal notation represents four ones (1111) in the binary address. Figure 3-35 shows a new host using broadcast messaging to announce its presence on the network.

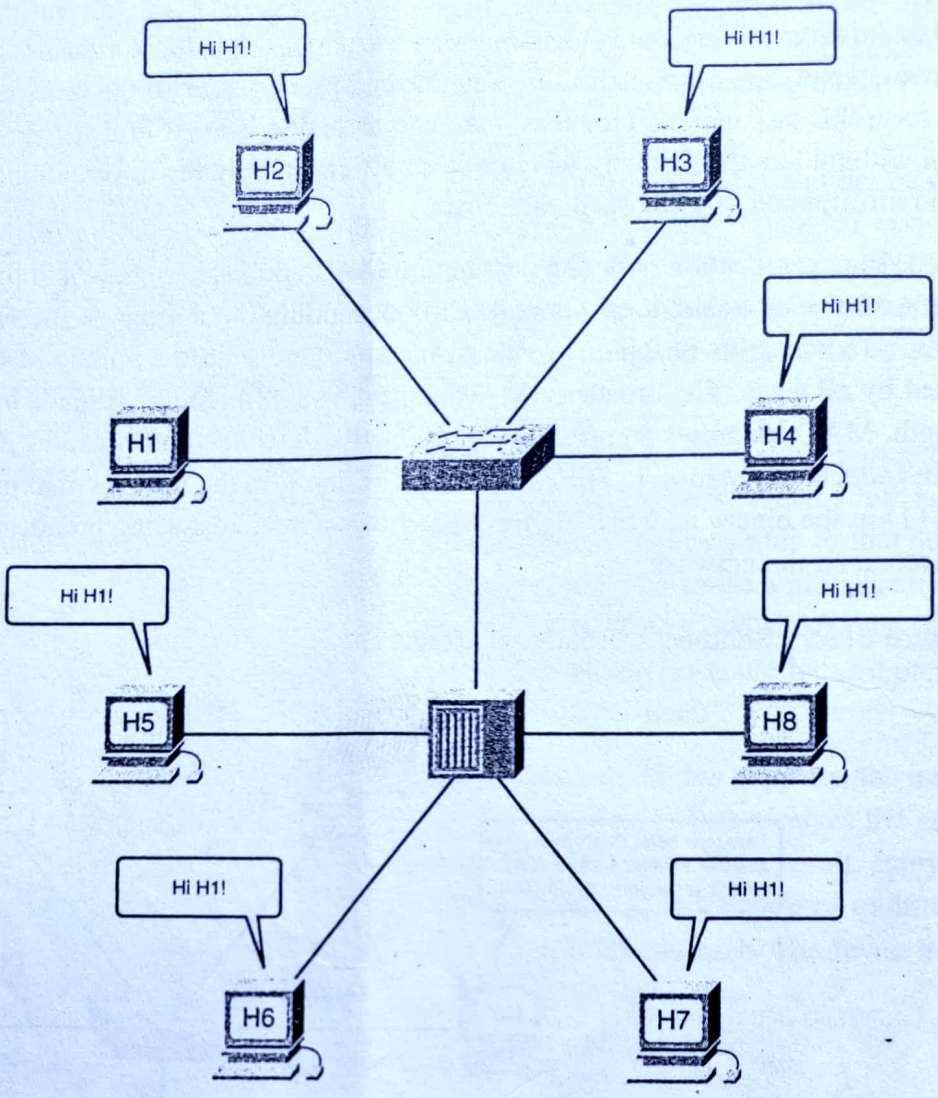
Figure 3-35 Sending a Broadcast Message



When a host receives a message addressed to the broadcast address, it accepts and processes the message as if the message were addressed directly to it, as shown in Figure 3-36.

When a host sends a broadcast message, hubs and switches forward the message to every connected host within the same local network. For this reason, a local network is also referred to as a ***broadcast domain***.

Figure 3-36 Replying to a Broadcast Message

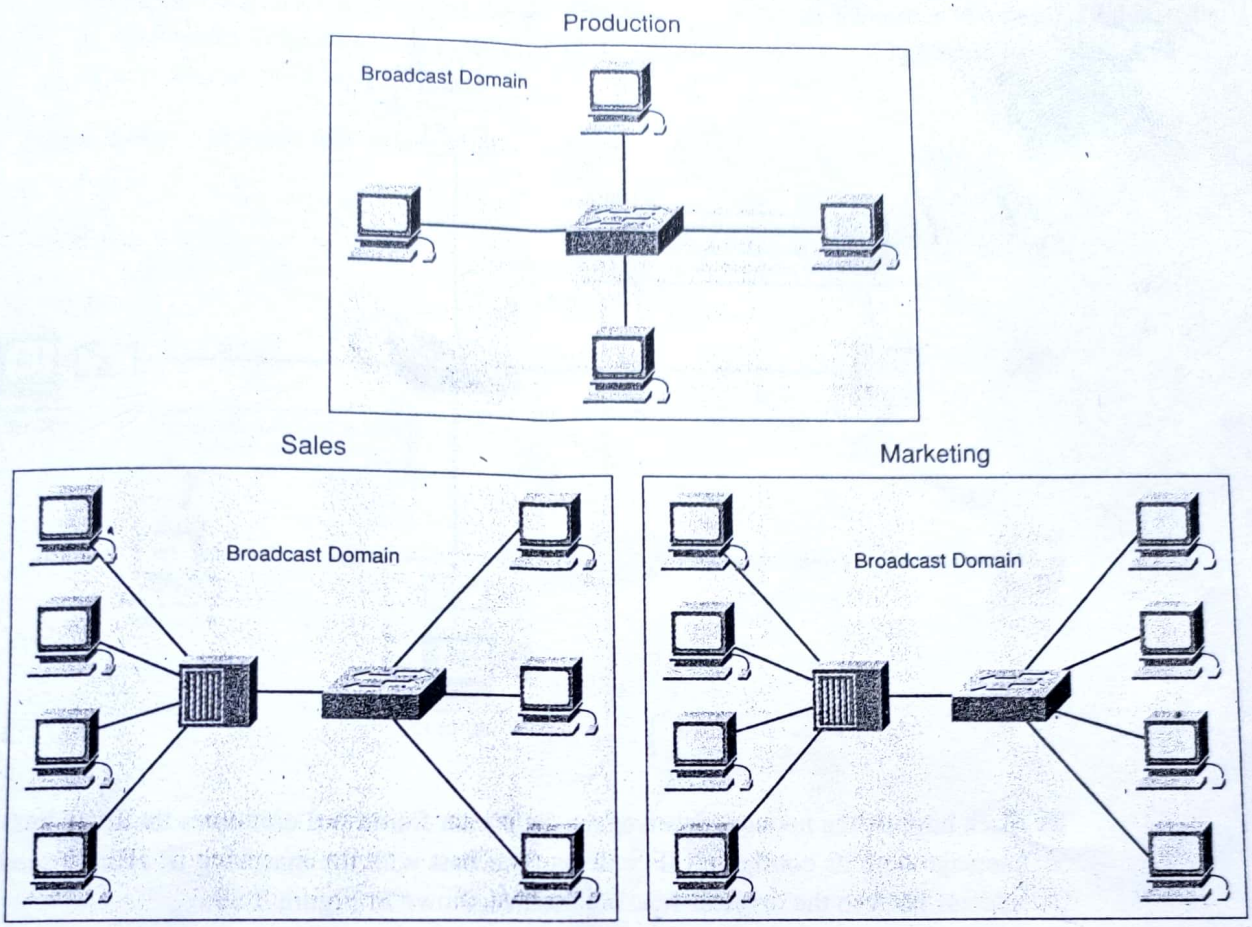


If too many hosts are connected to the same broadcast domain, broadcast traffic can become excessive. The number of hosts and the amount of network traffic that can be supported on the local network is limited by the capabilities of the hubs and switches used to connect them. As a local network grows and more hosts are added, network traffic, including broadcast traffic, increases. Dividing one local network, or broadcast domain, into multiple networks is often necessary to improve performance. Figure 3-37 shows a large network broken up into multiple broadcast domains.

Interactive Activity 3-10: Switch Behavior (3.4.5.1)

In this interactive activity you determine how a switch forwards frames based on a scenario. Use file ia-3451 on the CD-ROM that accompanies this book to perform this interactive activity.

Figure 3-37 Broadcast Domains



MAC and IP Addresses

On a local Ethernet network, a NIC accepts a frame only if the destination address is either the broadcast MAC address or corresponds to the MAC address of the NIC itself. Most network applications, however, rely on the logical destination IP address to identify the location of the servers and clients.

Each Ethernet interface builds a table that contains the IP address and corresponding MAC address of all hosts that are active on the same local network. This table is known as the ***Address Resolution Protocol (ARP) table***. The information in this table is used to encapsulate data before sending it out onto the network. This table is stored in RAM and the information it contains has a limited lifetime.

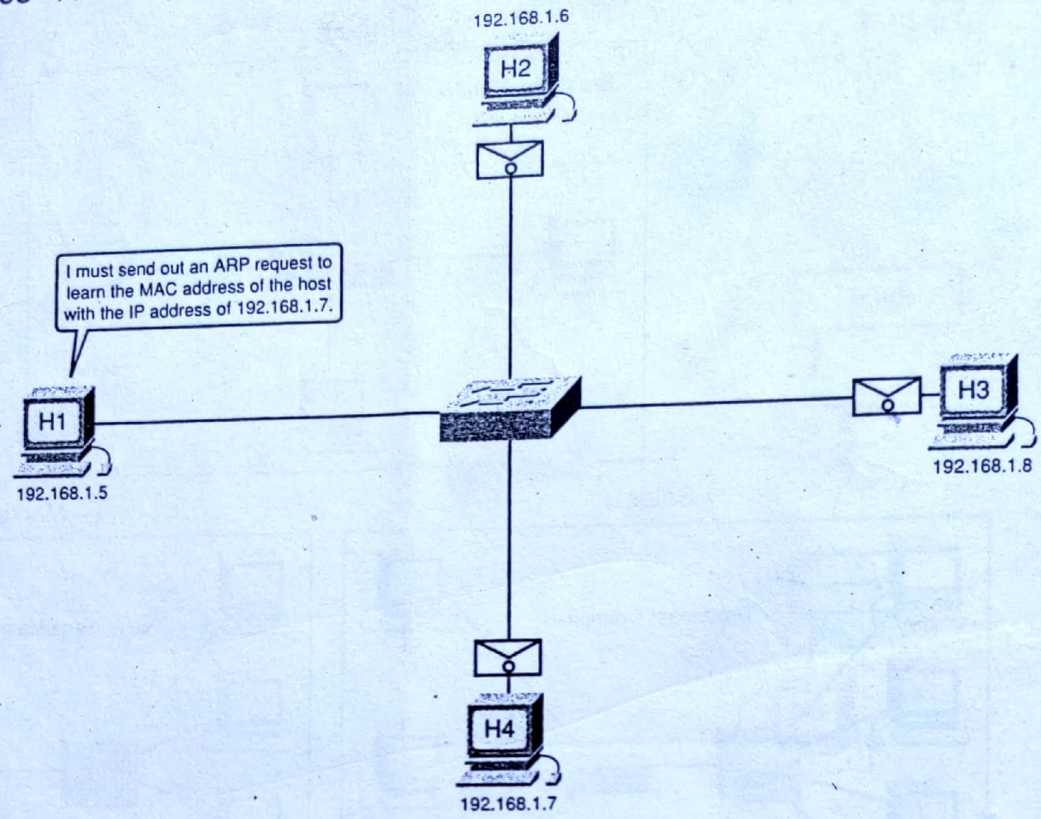
If the sending host knows the logical IP address of the destination host but not the MAC address, it must determine the MAC address before any communication between the source and destination host can occur. The sending host can use an IP protocol called Address Resolution Protocol (ARP) to discover the MAC address of any host on the same local network.

Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) uses a three-step process to discover and store the MAC address of a host on the local network when only the IP address of the host is known.

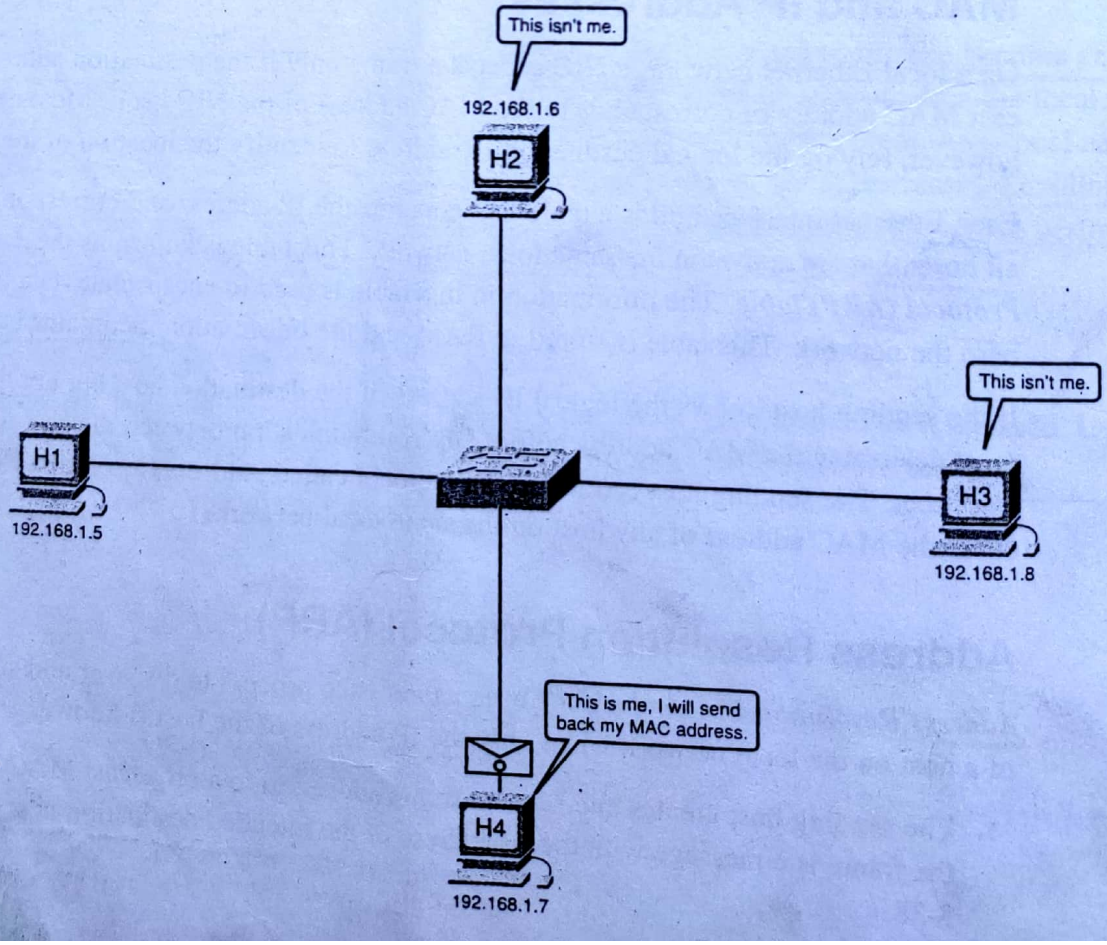
1. The sending host creates and sends a frame addressed to a broadcast MAC address. Contained in the frame is a message with the IP address of the intended destination host, as shown in Figure 3-38.

Figure 3-38 ARP Request



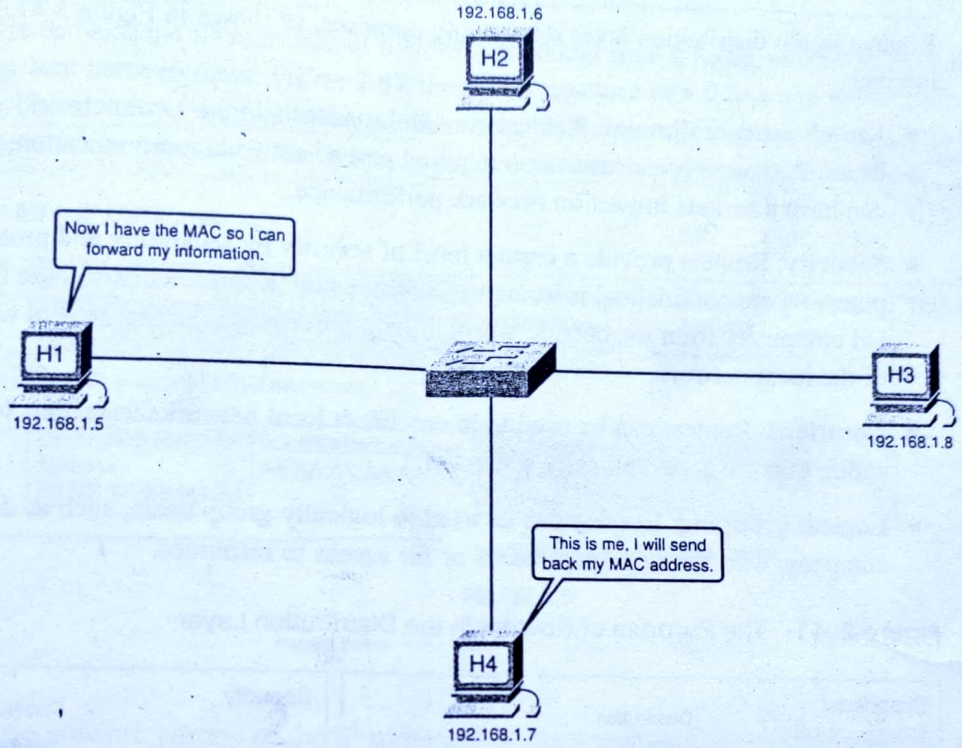
2. Each host on the network receives the broadcast frame and compares the IP address inside the message with its configured IP address. The host with the matching IP address sends its MAC address back to the original sending host, as shown in Figure 3-39.

Figure 3-39 ARP Reply



3. The sending host receives the message and stores the MAC address and IP address information in a table called an ARP table. After the sending host has the MAC address of the destination host in its ARP table, it can send frames directly to the destination without first having to send an ARP request, as shown in Figure 3-40.

Figure 3-40 Updated ARP Information



All hosts that hear the broadcast ARP request use this information to update their ARP tables with the sender's information.

Building the Distribution Layer of a Network

To interconnect multiple local networks, a distribution layer is required. This section describes the purpose of the distribution layer and the network devices that operate there. It also describes the process of sending packets outside the local network using the router as a default gateway.

Distribution Layer

As networks grow, dividing one local network into multiple access layer networks is often necessary. Many ways exist for dividing networks based on different criteria, including the following:

- Physical location
- Logical function
- Security requirements
- Application requirements

The ***distribution layer*** connects these independent local networks and controls the traffic flowing between them. It is responsible for ensuring that traffic between hosts on the local network stays local.

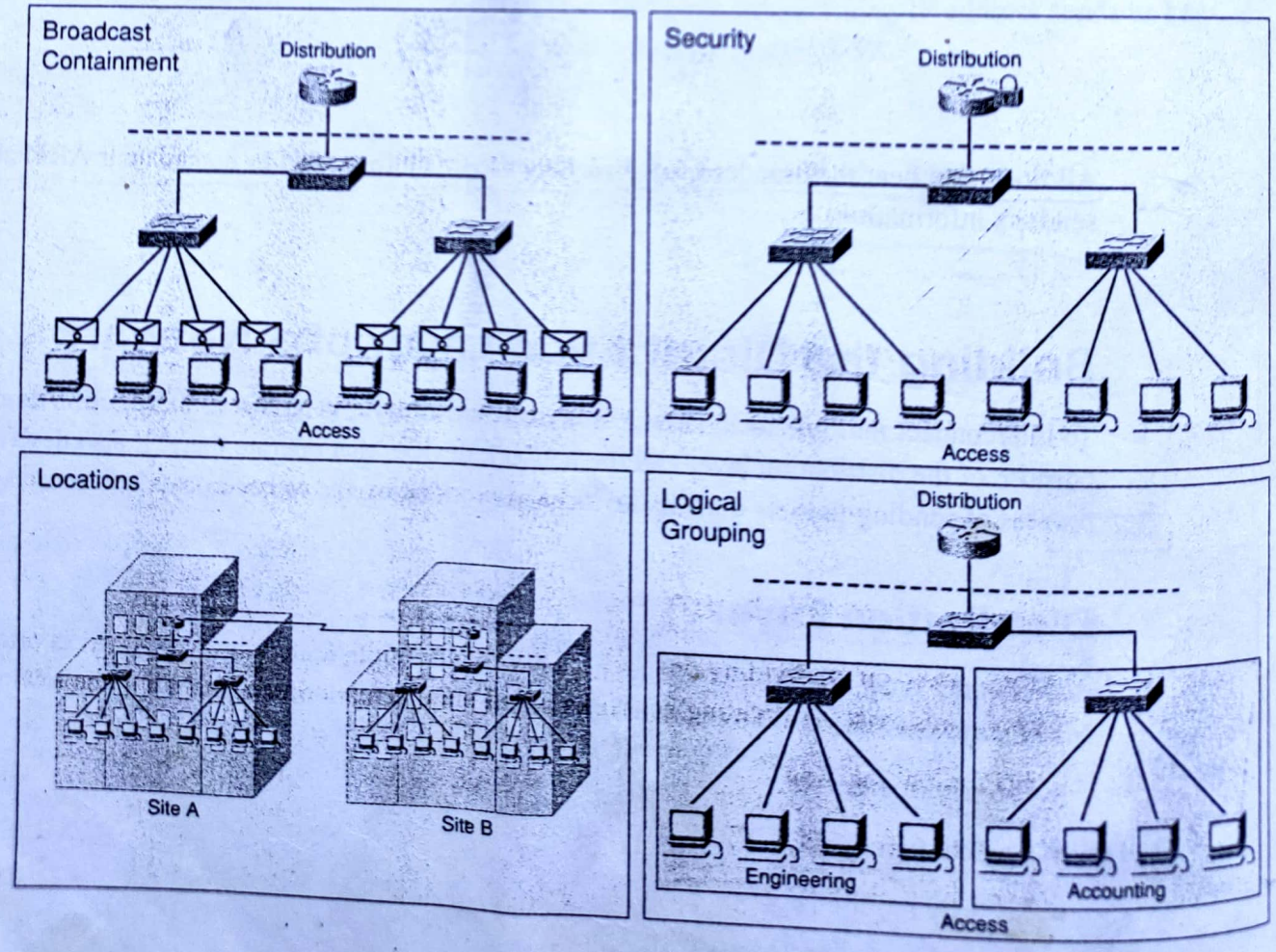
Only traffic that is destined for other networks is passed on. The distribution layer can also filter incoming and outgoing traffic for security and traffic management.

Networking devices that make up the distribution layer are designed to interconnect networks, not individual hosts. Individual hosts are connected to the network via access layer devices, such as hubs and switches. The access layer devices in each network are in turn connected to each other via a distribution layer device, such as a router.

Routers in the distribution layer serve many purposes, as shown in Figure 3-41. These include the following:

- **Broadcast containment**: Routers contain broadcasts in the local network where they must be heard. Although broadcasts are a required part of network communication, too many broadcasts can have a serious impact on network performance.
- **Security**: Routers provide a certain level of security by separating and protecting groups of computers where confidential information might reside. Routers can also hide the addresses of internal computers from the outside world to help prevent attacks and control who can get into or out of the local network.
- **Locations**: Routers can be used to interconnect local networks at various locations of an organization that are geographically separated.
- **Logical grouping**: Routers can be used to logically group users, such as departments within a company, who have common needs or for access to resources.

Figure 3-41 The Purpose of Routers in the Distribution Layer

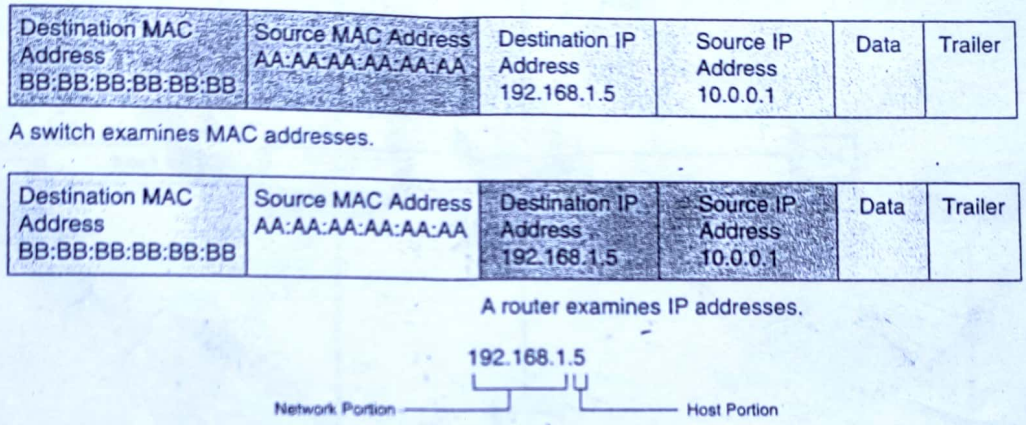


Function of Routers

A *router* is a networking device that connects a local network to other local networks. At the distribution layer of the network, routers direct traffic and perform other functions critical to efficient network operation. Routers, like switches, are able to decode and read the messages that are sent to them. Unlike switches, which only decode (unencapsulate) the frame containing the MAC address information, routers decode the packet that is encapsulated within the frame.

The packet contains the IP addresses of the destination and source hosts, as well as the actual message data being sent between them. Figure 3-42 shows the structure of a frame and the IP packet that it contains. The router reads the network portion of the destination IP address and uses it to find which one of the attached networks is the best way to forward the message to the destination.

Figure 3-42 IP Datagram



Anytime the network portion of the IP addresses of the source and destination hosts do not match, a router must be used to forward the message. For example, if a host located on network 1.1.1.0 needs to send a message to a host on network 5.5.5.0, the host will forward the message to the router. The router receives the message and unencapsulates it to read the destination IP address to determine which network it needs to be sent to. The router then determines how to forward the message to that network through one of its network interfaces. It re-encapsulates the packet back into a frame and forwards the frame on to its destination.

Each port, or interface, on a router connects to a different network. Every router contains a table of all locally connected networks and the interfaces that connect to them. These routing tables can also contain information about the routes, or paths, that the router can use to reach other remote networks that are not locally attached.

When a host sends a message to another host on the same local network, the destination host receives the message because it is connected to the same medium. If a message is sent to a host on a different network, as shown in Figure 3-43, the message must be sent to a router for processing.

When a router receives a frame, it decodes the frame to get to the packet containing the destination IP address. It matches the network portion of the destination address to all the networks that are contained in the routing table as shown in Figure 3-44. If the destination network address is in the table, the router encapsulates the packet in a new frame in order to send it out. It forwards the new frame out of the interface associated with the path and to the destination network, as shown in Figure 3-45. The process of forwarding the packets toward their final destination network is called ***routing***.

Figure 3-43 Sending a Message to a Host on a Different Network

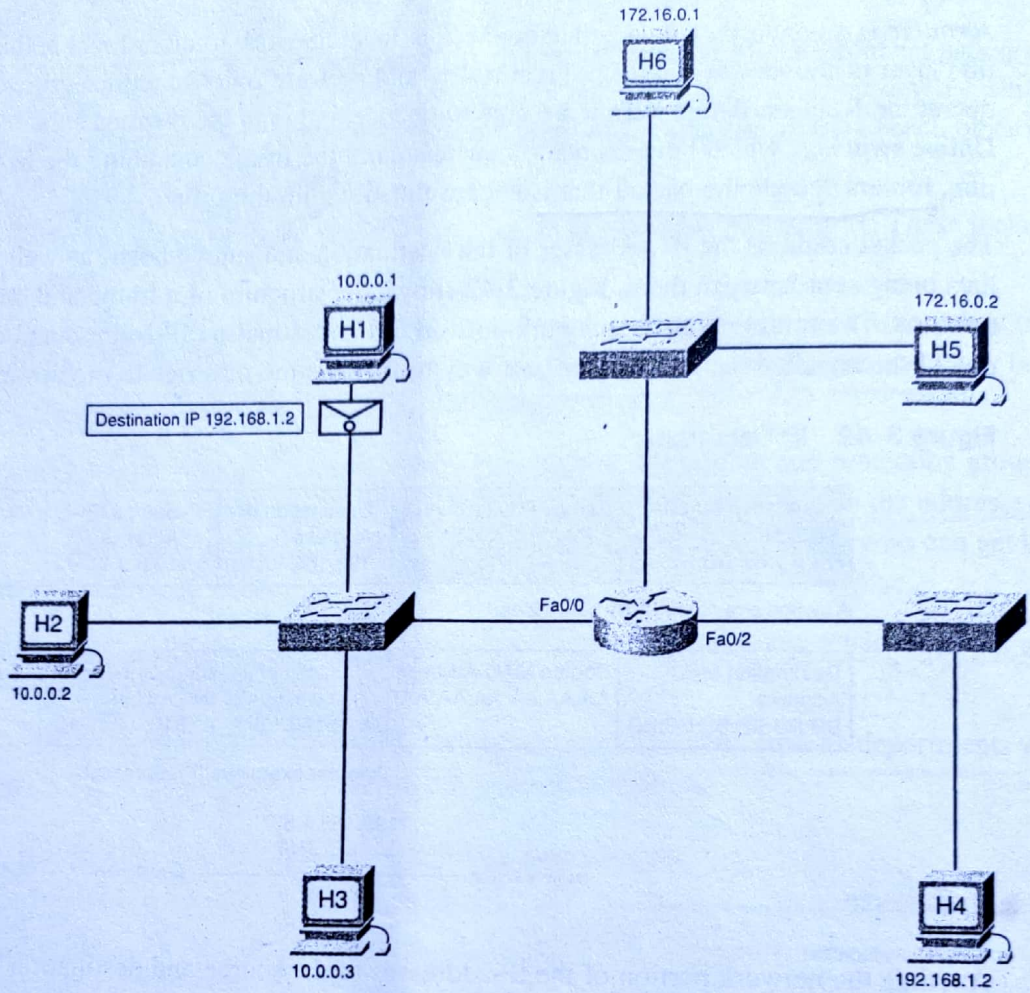


Figure 3-44 Consulting the Routing Table

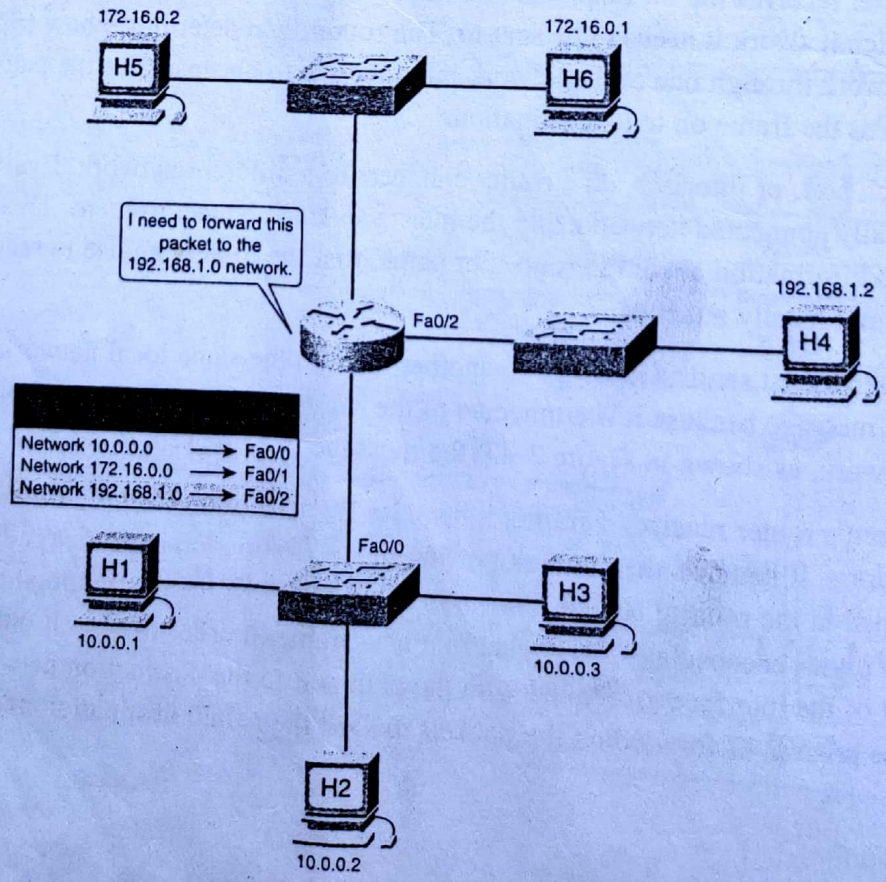
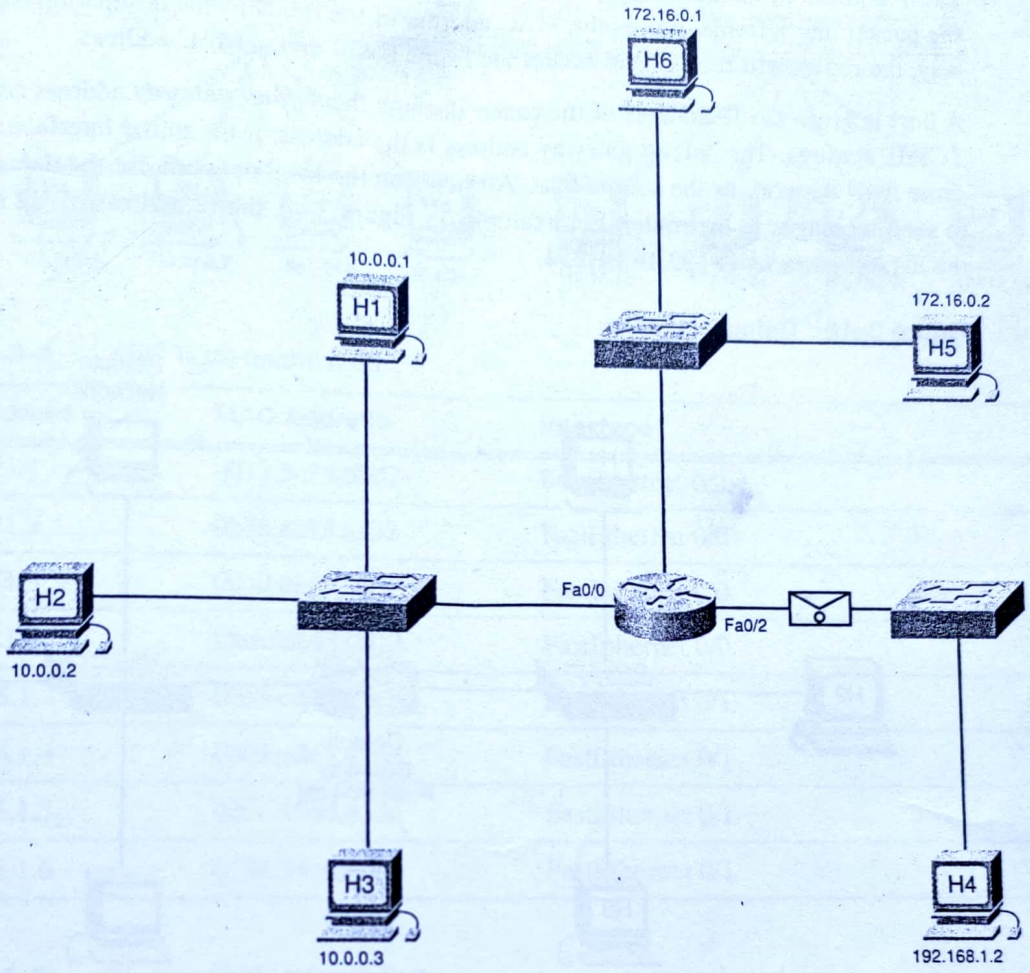


Figure 3-45 Routing the Packet



Router interfaces do not forward messages that are addressed to the broadcast MAC address. As a result, local network broadcasts are not sent across routers to other local networks.

Lab 3-4: IP Addresses and Network Communication (3.5.2.2)

In this lab you build a simple network and work with host IP addresses to see the effect on network communication. Refer to the hands-on lab in Part II of this *Learning Guide*. You may perform this lab now or wait until the end of the chapter.

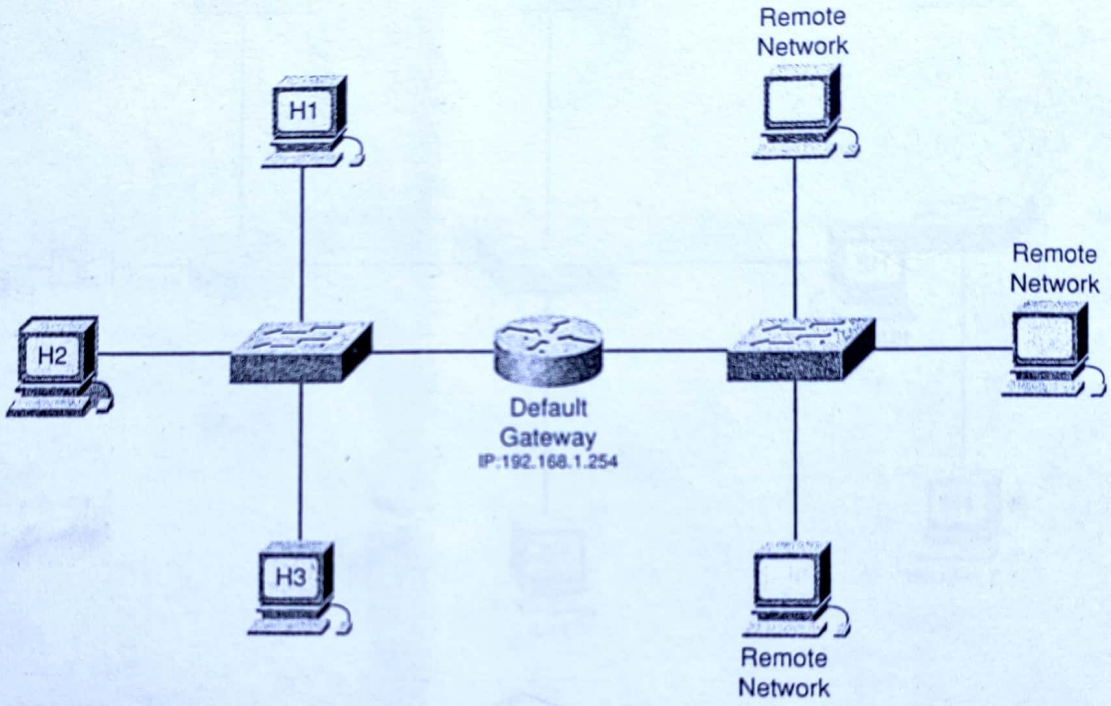
Default Gateway

The method that a host uses to send messages to a destination on a remote network differs from the way a host sends a message to another host on the same local network. When a host needs to send a message to another host located on the same network, it will forward the message directly. A host uses ARP to discover the MAC address of the destination host. Once the MAC address of the destination host is known, the sending host includes the destination IP address within the packet and encapsulates the packet into a frame containing the MAC address of the destination. This frame is then forwarded out onto the network.

When a host needs to send a message to a remote network, it must use the router. The host includes the IP address of the destination host within the packet just like before. However, when it encapsulates the packet into a frame, it uses the MAC address of the router as the destination for the frame. In this way, the router will receive and accept the frame based on the MAC address.

A host is given the IP address of the router through the *default gateway* address configured in its TCP/IP settings. The default gateway address is the address of the router interface connected to the same local network as the source host. All hosts on the local network use the default gateway address to send messages to the router. For example, in Figure 3-46, the IP address of H2 is 192.168.1.2 and the default gateway is 192.168.1.254.

Figure 3-46 Default Gateway



After the host knows the default gateway IP address, it can use ARP to determine the MAC address. The MAC address of the router interface is then placed in any frames that are destined for another network.

Ensuring that the correct default gateway is configured on each host on the local network is important. If no default gateway is configured in the host TCP/IP settings, or if the wrong default gateway is specified, messages addressed to hosts on remote networks cannot be delivered.

Interactive Activity 3-11: Configuring a Default Gateway Address (3.5.3.2)

In this interactive activity you configure the proper default gateway address for multiple hosts. Use file ia-3532 on the CD-ROM that accompanies this book to perform this interactive activity.

Tables Maintained by Routers

Routers move information between local and remote networks. To do this, routers must use both ARP and routing tables to store information, as shown in Figure 3-47. ARP tables map the IP addresses of the remote host to their MAC addresses as shown in Table 3-4. ***Routing tables*** are not concerned with the addresses of individual hosts. Routing tables contain the addresses of networks and the best path to reach those networks as shown in Table 3-5.

Figure 3-47 ARP and Routing Tables

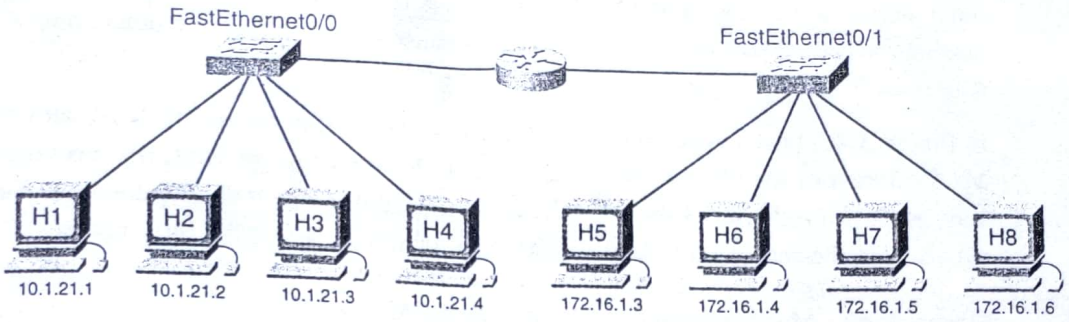


Table 3-4 ARP Table Information

IP Address	MAC Address	Interface
10.1.21.1	0072.5e34.6bd2	FastEthernet 0/0
10.1.21.2	0b76.ac13.a132	FastEthernet 0/0
10.1.21.3	00c0.dee5.7ec3	FastEthernet 0/0
10.1.21.4	Oaac.de43.0013	FastEthernet 0/0
172.16.1.3	00c3.cd45.00c3	FastEthernet 0/1
172.16.1.4	0d01.cde2.456e	FastEthernet 0/1
172.16.1.5	000e.456d.435c	FastEthernet 0/1
172.16.1.6	0124.54cd.ae56	FastEthernet 0/1

Table 3-5 Routing Table Information

Type	Network	Port
C	10.0.0.0/8	FastEthernet 0/0
C	172.16.0.0/16	FastEthernet 0/1

Entries can be made to the routing table in two ways:

- Dynamically updated by information received from other routers in the network
- Manually entered by a network administrator

Routers use the routing tables to determine which interface to use to forward a message to its intended destination. If the router cannot determine where to forward a message, it will drop it. To prevent this from occurring, network administrators usually configure a default route in the routing table. A ***default route*** is the interface through which the router forwards a packet containing an unknown destination IP network address. This default route usually connects to another router that can forward the packet toward its final destination network.

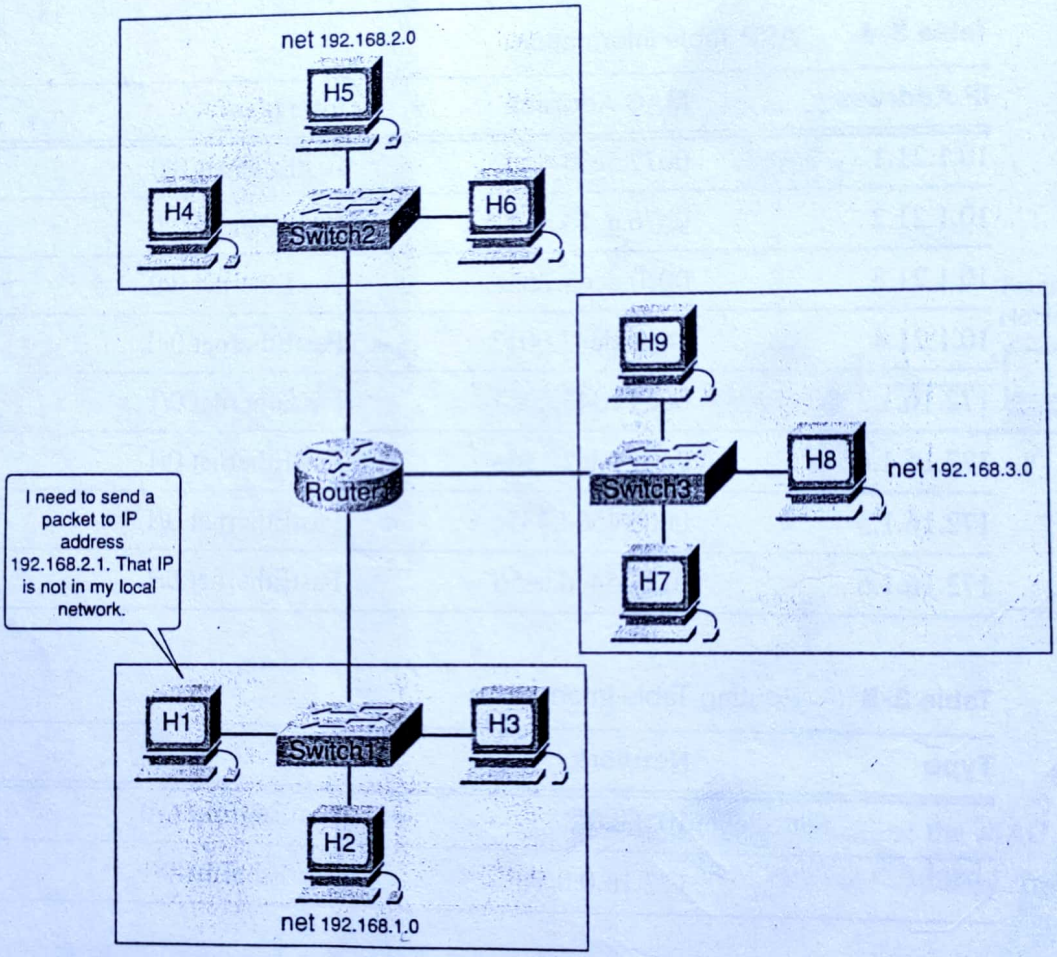
A router forwards a frame to one of two places:

- A directly connected network containing the actual destination host
- Another router on the path to reach the destination host

When a router encapsulates the frame to forward it onto a directly connected Ethernet network, it must include a destination MAC address. This is the MAC address of the actual destination host, if the destination host is part of a network locally connected to the router. Routers obtain these MAC addresses from ARP tables.

In Figure 3-48, host 1 is sending a message to a host that is not on the same network. Because the MAC address of the remote host is not known, the sending host sends the message to the default gateway, as shown in Figure 3-49, for delivery by the router. The default gateway is part of the same local network, so the sending host consults its ARP table for the correct information.

Figure 3-48 Message Destined for a Host on Another Network



After the router has the packet, it must decide what to do with it. The router examines the packet header to gather the IP information. When the router determines the network that the remote host is on, it checks to see whether it has information on how to deliver the message. In Figure 3-50, the remote host is part of a network that is directly connected to the router. Because the host is directly connected, the router consults its ARP table and encapsulates the data with the destination IP and MAC address then forwards the message to the remote host.

Figure 3-49 Sending the Message to the Default Gateway for Delivery

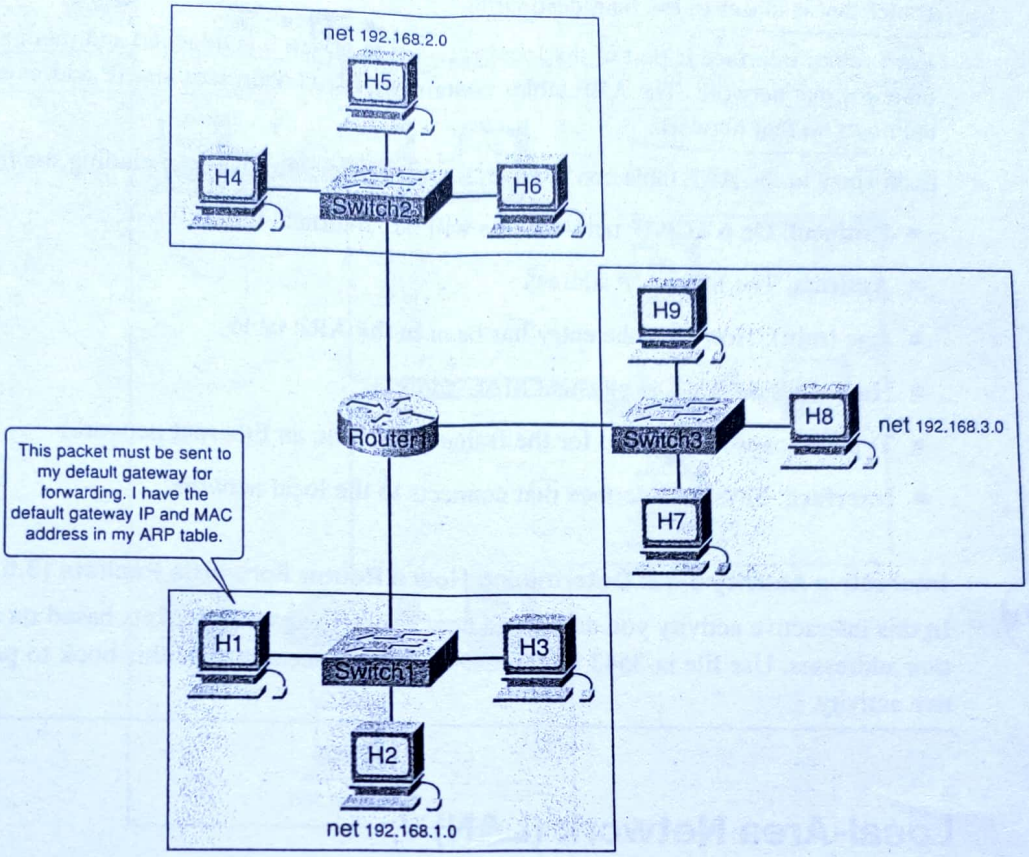
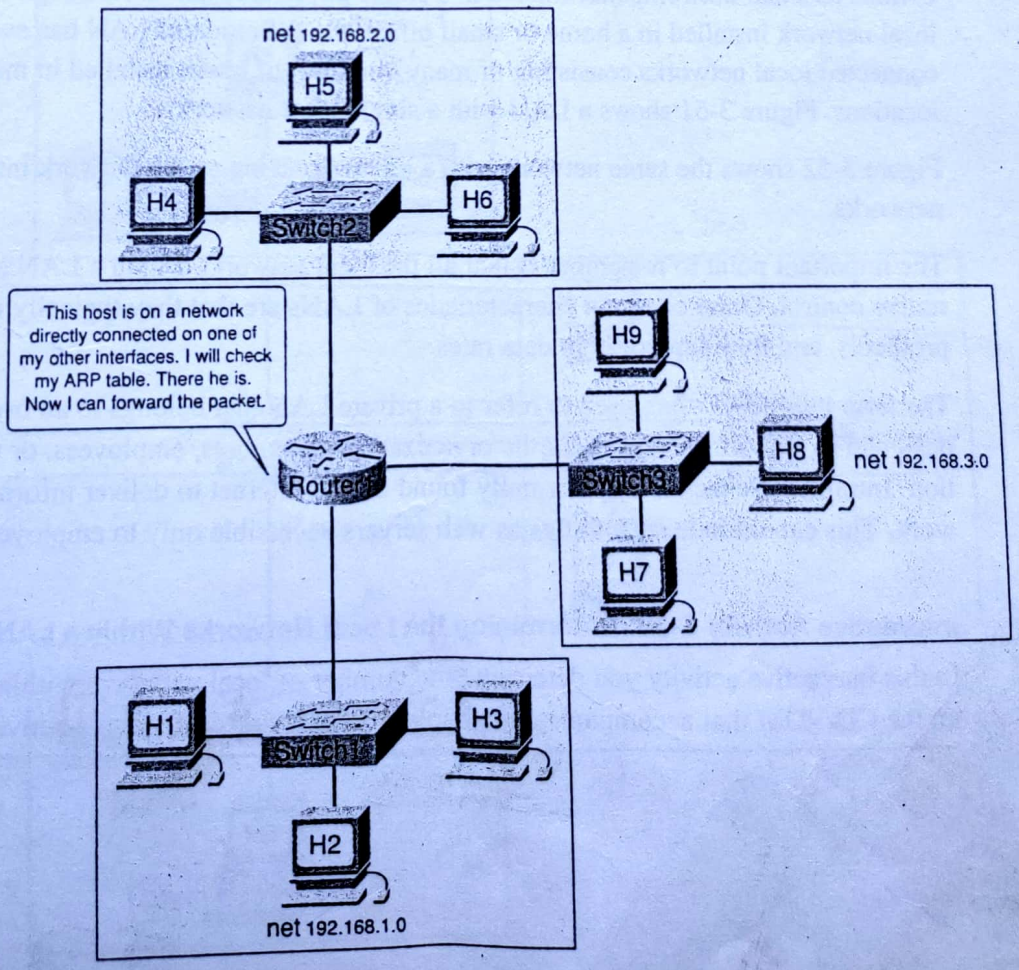


Figure 3-50 Forwarding the Message to the Remote Host



If the remote host is not on a directly connected network, the router will pass the message to another router that is closer to the final destination.

Each router interface is part of the local network to which it is attached and maintains its own ARP table for that network. The ARP tables contain the MAC addresses and IP addresses of all the individual hosts on that network.

Each entry in the ARP table contains several pieces of information including the following:

- **Protocol**: On a TCP/IP network this will be "Internet" for IP
- **Address**: The logical IP address
- **Age (min)**: How long the entry has been in the ARP table
- **Hardware Addr**: The physical MAC address
- **Type**: Encapsulation used for the frame (ARPA on an Ethernet network)
- **Interface**: Physical interface that connects to the local network

Interactive Activity 3-12: Determining How a Router Forwards Packets (3.5.4.3)

In this interactive activity you determine how a router forwards packets based on source and destination addresses. Use file ia-3543 on the CD-ROM that accompanies this book to perform this interactive activity.

Local-Area Network (LAN)

The term *local-area network (LAN)* refers to a local network or a group of interconnected local networks that are under the same administrative control. In the early days of networking, LANs were defined as small networks that existed in a single physical location. Although LANs can be a single local network installed in a home or small office, the definition of LAN has evolved to include interconnected local networks consisting of many hundreds of hosts, installed in multiple buildings and locations. Figure 3-51 shows a LAN with a single local network.

Figure 3-52 shows the same network with a router breaking up the network into three separate local networks.

The important point to remember is that all the local networks within a LAN are under one administrative control. Other common characteristics of LANs are that they typically use Ethernet or wireless protocols, and they support high data rates.

The term intranet is often used to refer to a private LAN that belongs to an organization and is designed to be accessible by only the organization's members, employees, or others with authorization. Intranets use technology normally found on the Internet to deliver information on a private network. This can include such things as web servers accessible only to employees.

Interactive Activity 3-13: Determining the Local Networks Within a LAN (3.5.5.2)

In this interactive activity you determine the number of local networks within a LAN. Use file ia-3552 on the CD-ROM that accompanies this book to perform this interactive activity.

Figure 3-51 LAN with a Single Local Network

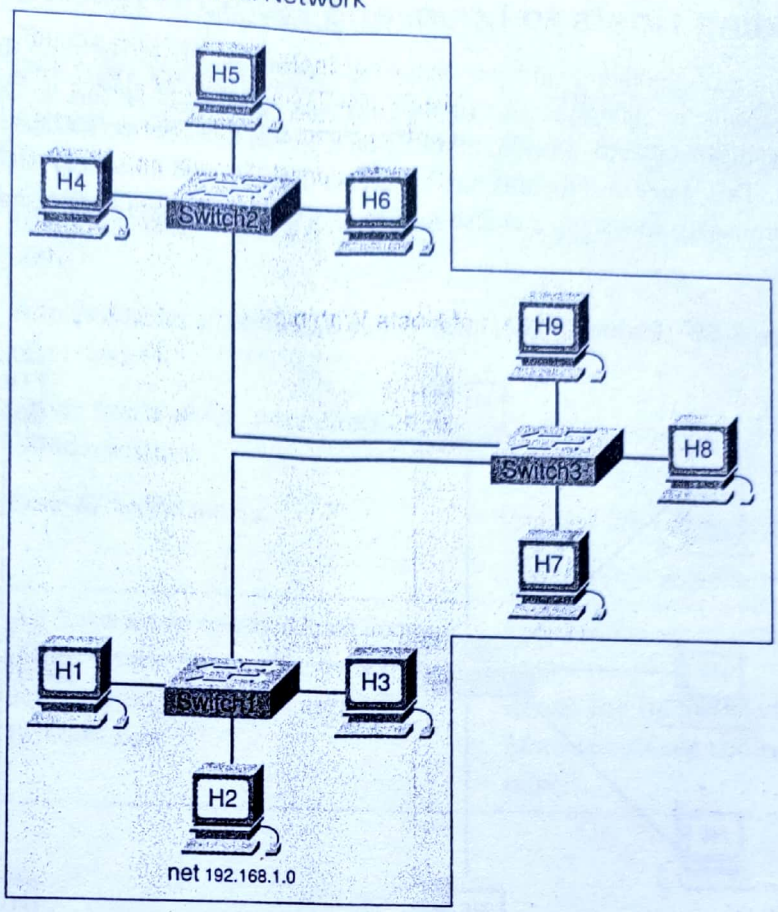
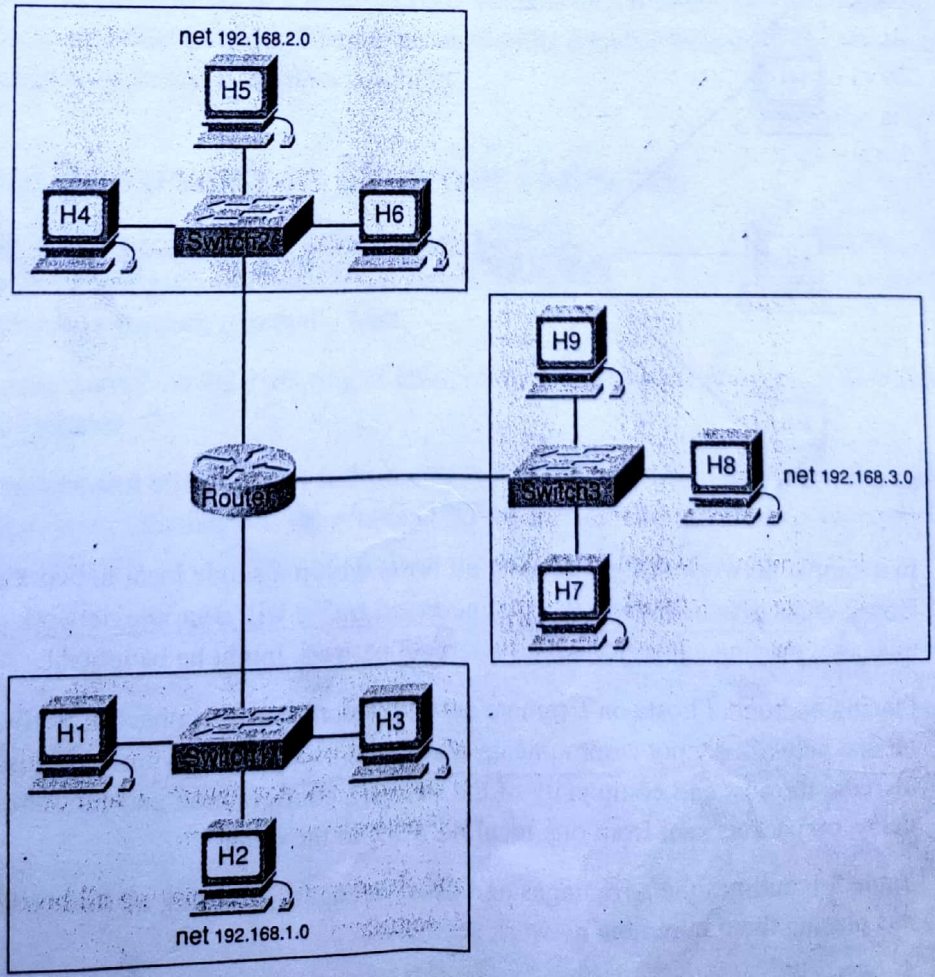


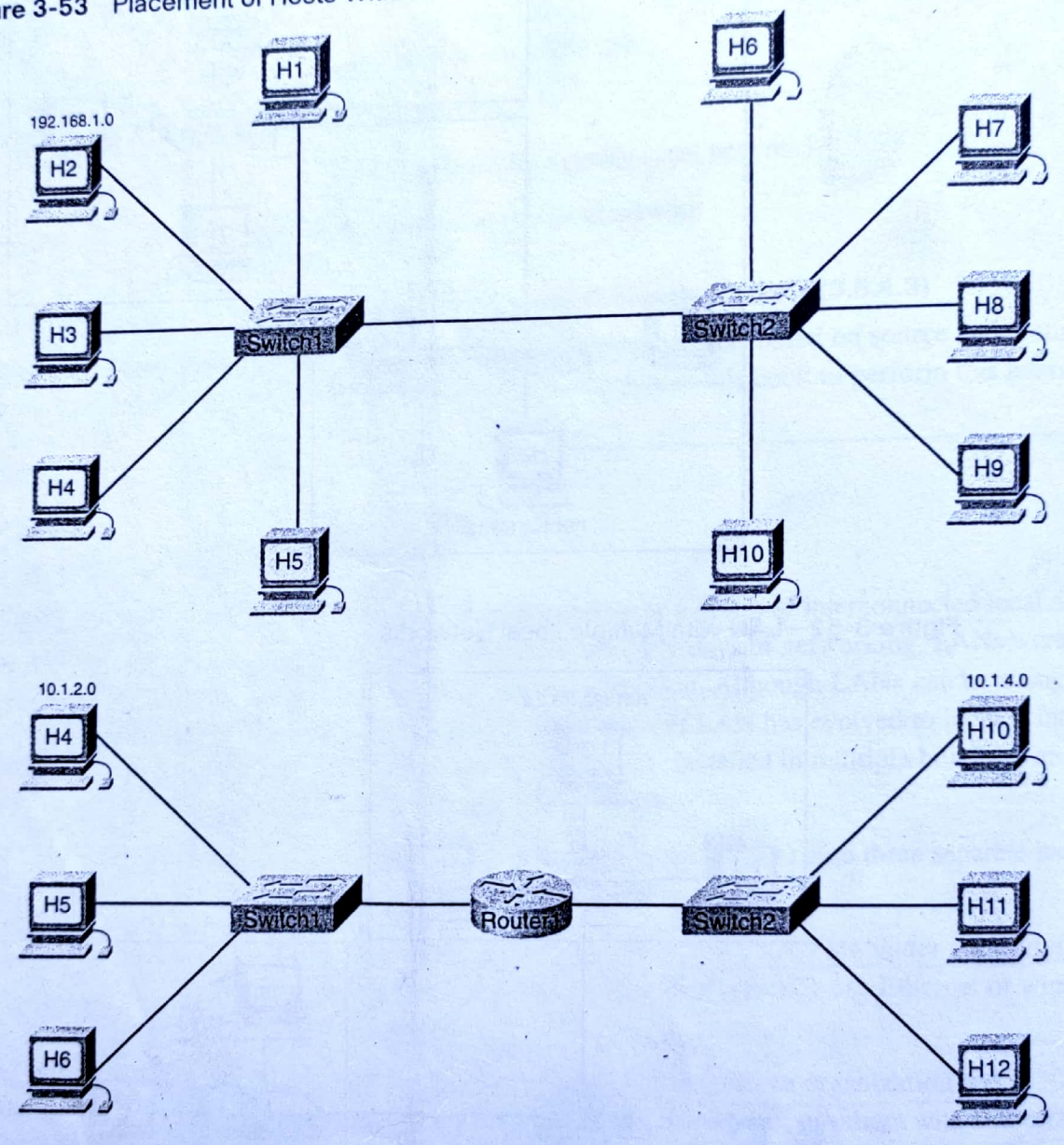
Figure 3-52 LAN with Multiple Local Networks



Adding Hosts to Local and Remote Networks

Within a LAN, placing all hosts on a single local network or dividing them up between multiple networks using a router at the distribution layer is possible, as shown in Figure 3-53. The choice depends on the desired results. Placing all hosts on a single local network allows them to be seen by all other hosts. This is because there is one broadcast domain, and hosts use ARP to find each other. Unfortunately, this setup can also lead to excessive broadcast traffic and degraded network performance.

Figure 3-53 Placement of Hosts Within a LAN



In a simple network design, keeping all hosts within a single local network might be beneficial. However, as networks grow in size, increased traffic will decrease network performance and speed. In this case, moving some hosts onto a remote network might be beneficial.

Placing additional hosts on a remote network decreases the impact of traffic demands. However, hosts on one network cannot communicate with hosts on the other without the use of routing. Routers increase the cost and complexity of the network configuration and can introduce latency, or time delay, on packets sent from one local network to the other.

Table 3-6 outlines the advantages and disadvantages of placing all hosts on a single local network versus placing them in remote network segments.

In order to establish reliable communications channels, a global addressing scheme is required. This addressing scheme must be both flexible and dynamic. IP addresses have become the standard for network communications around the world. This chapter examines IP addresses and how unique IP addresses can be provided to host devices. It also explains the concept of private address space and the role of NAT. Part II of this book includes the corresponding labs for this chapter.

IP Addresses and Subnet Masks

The requirement for a simple, yet effective, global addressing system has been fulfilled by the IP addressing scheme. This system allows each host to be provided with a unique address but also allows these addresses to be grouped together into logical networks.

Purpose of an IP Address

In order to participate in communication on an IP network such as the Internet, a host needs an IP address. The IP address is a ***logical network address*** that identifies a particular host. It must be properly configured and unique in order to allow a device to communicate with other devices on the Internet.

An IP address is assigned to the network interface connection for a host. This connection is usually a network interface card (NIC) installed in the device. These NICs can be designed to participate in either a wired or a wireless network. Examples of end-user devices with network interfaces include workstations, servers, network printers, and IP phones. Some servers can have more than one NIC and each of these has its own IP address. Router interfaces that provide connections to an IP network also have an IP address because they behave as a host on the network.

Every packet sent across the Internet has both a ***source*** and destination IP address. This information is required by networking devices to ensure that the information gets to the destination and any replies can be returned to the source. Figure 5-1 shows this process.

Packet Tracer Activity

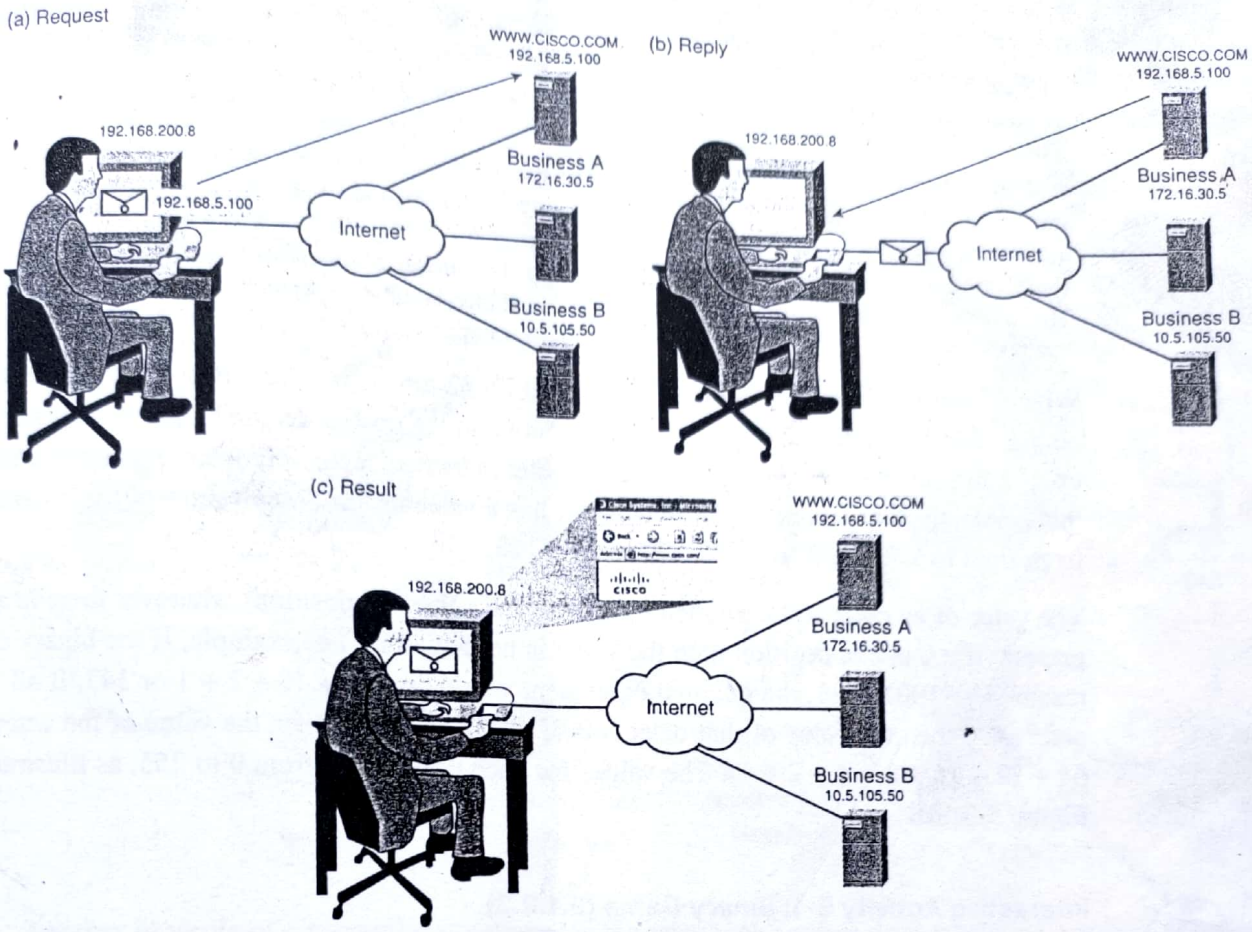
Connecting to a Web Server Using IP (5.1.1.2)

In this Packet Tracer activity you observe how packets are sent across the Internet using IP addresses. Use file d1-5112.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

IP Address Structure

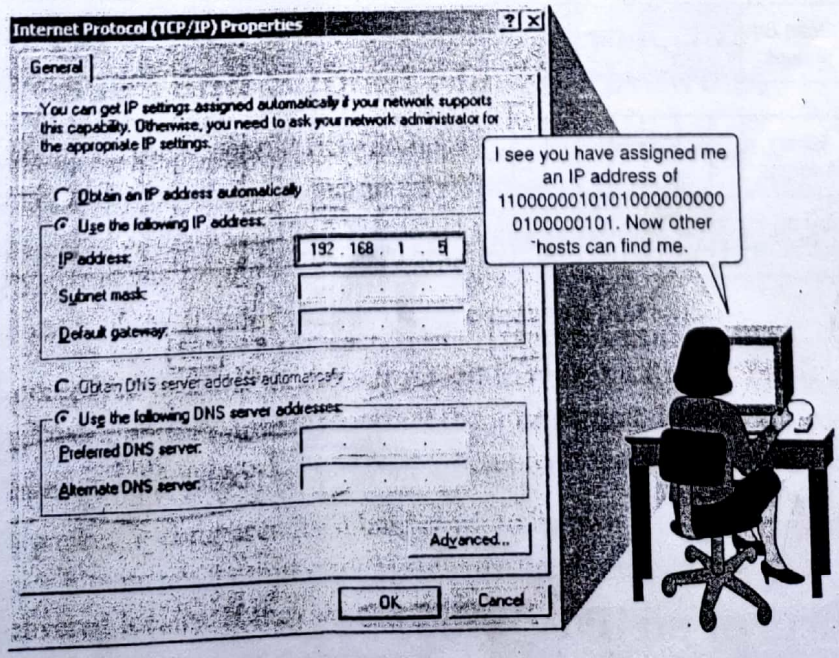
An IP address is simply a series of 32 ***binary digits***. Although machines have no difficulty accurately reading these longs strings of ones and zeros, reading an IP address in binary IP form is very difficult for humans. For this reason, the 32 bits are grouped into four 8-bit bytes called ***octets***. Even with this grouping, it is still hard for humans to read, write, and remember these addresses. To make the addresses easier to understand, each octet is presented as its decimal value, separated by a decimal point or period. This is referred to as ***dotted-decimal notation*** and is the usual way that humans work with IP addresses.

Figure 5-1 Purpose of a Host IP Address



When a host is configured with an IP address, as shown in Figure 5-2, it is entered as a dotted-decimal number such as 192.168.1.5. Imagine if you had to enter the 32-bit binary equivalent of this: 11000000101010000000000100000101. If you mistyped just one bit, the address would be different and the host would not be able to communicate on the network.

Figure 5-2 Configuring an IP Address on a Host



The 32-bit IP address is defined with *IP version 4 (IPv4)* and is currently the most common form of IP address on the Internet. More than 4 billion IP addresses are possible using a 32-bit addressing scheme.

TIP

Although IPv4 is still the most common addressing scheme in common use, these addresses are quickly becoming exhausted due to the increasing number of devices that require them. For this reason a newer version of IP addressing has been developed, known as *IP version 6 (IPv6)*. IPv6 uses 128 bits to represent hosts instead of the 32 used by IPv4. This feature greatly increases the number of available hosts (2^{128} addresses or roughly 5×10^{28} addresses for every person alive today) and will alleviate the problem of scarce addresses.

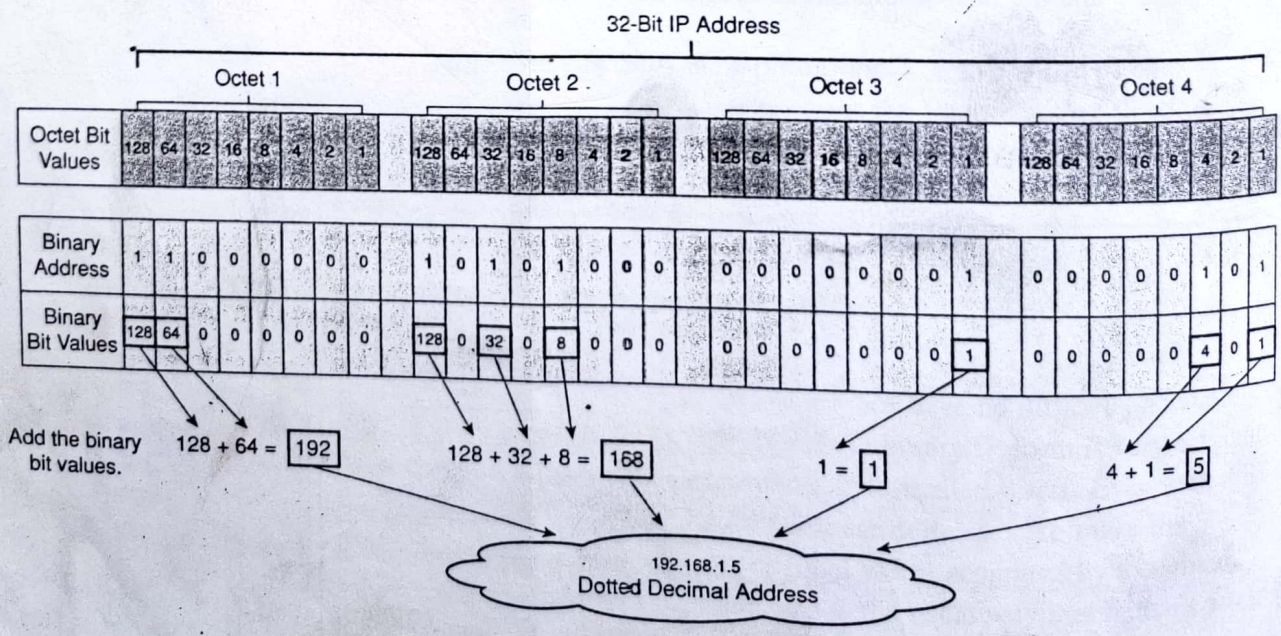
When a host receives an IP address, it looks at all 32 bits as they are received by the NIC. Humans, on the other hand, need to convert those 32 bits into the dotted-decimal equivalent. Each octet is made up of 8 bits and each bit has a value. Each octet is treated separately from the others and is converted independently. The rightmost bit in an octet has a value of 1 and the values of the remaining bits, from right to left, are 2, 4, 8, 16, 32, 64, and 128.

The value of an octet is determined by adding the values of positions wherever there is a binary 1 present. If a 0 is in a position then the value is not added in. For example, if the binary octet was represented by 1001 0011, the decimal equivalent would be 128 + 16 + 2 + 1 or 147. If all 8 bits in an octet are 0 then the value of that octet is 0. If all the bits are 1 then the value of the octet is 255 (128 + 64 + 32 + 16 + 8 + 4 + 2 + 1). The values for each octet range from 0 to 255, as illustrated in Figure 5-3.

Interactive Activity 5-1: Binary Game (5.1.2.3)

In this interactive activity you practice your binary-to-decimal conversion skills. Use file ia-5123 on the CD-ROM that accompanies this book to perform this interactive activity.

Figure 5-3 Decimal Equivalent of a Binary IP Address

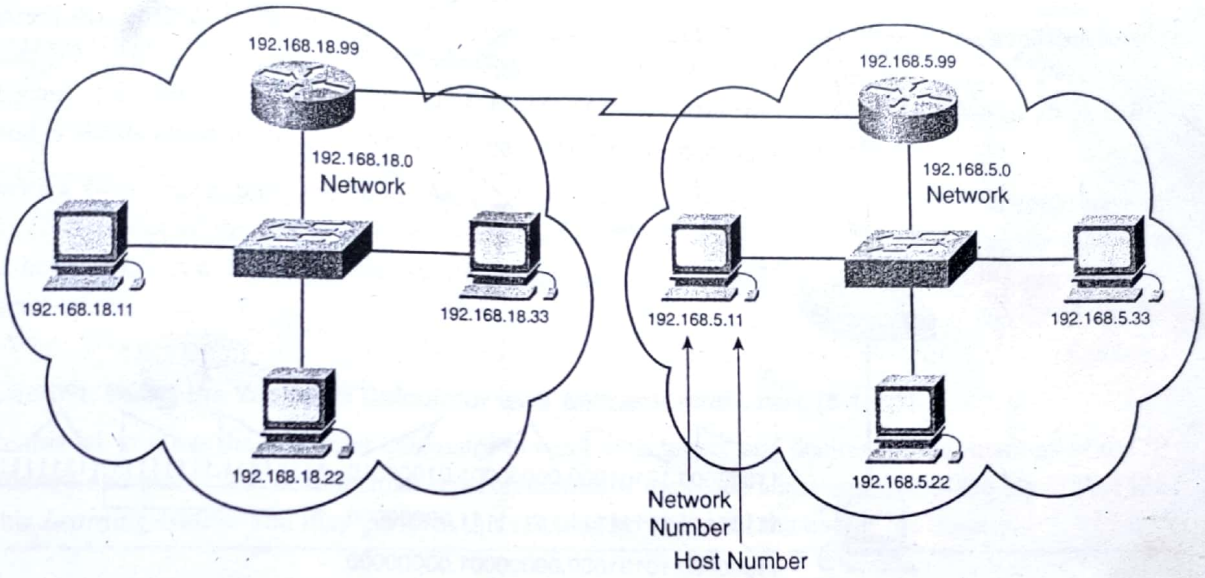


Parts of an IP Address

The logical 32-bit IP address is ***hierarchical*** and is made up of two parts, as shown in Figure 5-4. The first part identifies the network and the second part identifies a host on that network. Both parts are required in an IP address.

As an example, if a host has IP address 192.168.18.57, the first three octets, 192.168.18, identify the network portion of the address, and the last octet, 57 identifies the host. This is known as hierarchical addressing because the network portion indicates the network on which each unique host address is located. Routers only need to know how to reach each network, rather than needing to know the location of each individual host.

Figure 5-4 Parts of an IP Address



Another example of a hierarchical network is the telephone system. In a telephone number, the country code, area code, and exchange or prefix represent the network address, and the remaining digits represent a local phone number.

Interactive Activity 5-2: Identifying the Network Portion of an IP Address (5.1.3.2)

In this interactive activity you sort specific host IP addresses into the correct network containers. Use file ia-5132 on the CD-ROM that accompanies this book to perform this interactive activity.

How IP Addresses and Subnet Masks Interact

Every IP address is made up of two parts. How do hosts know which portion is the network and which is the host? This is the job of the subnet mask. When an IP host is configured, a ***subnet mask*** is assigned along with an IP address. Like the IP address, the subnet mask is 32 bits long. The subnet mask signifies which part of the IP address is network and which part is host. It acts like a filter to block out the host portion of the IP address to reveal the network portion.

The subnet mask is compared to the IP address from left to right, bit for bit. The 1s in the subnet mask represent the network portion; the 0s represent the host portion. In the example shown in Figure 5-5, the first three octets are the network, and the last octet represents the host.

When a host sends a packet, it compares its subnet mask to its own IP address and the destination IP address. If the network bits match, both the source and destination host are on the same network and the packet can be delivered locally. If they do not match, the sending host forwards the packet to the local router interface to be sent on to the other network. The local router interface is known as the default gateway to the host machine.

The subnet masks we see most often with home and small business networking are 255.0.0.0 (8 bits), 255.255.0.0 (16 bits), and 255.255.255.0 (24 bits). A subnet mask of 255.255.255.0 (decimal) or 11111111.11111111.11111111.00000000 (binary) uses 24 bits to identify the network number, which leaves 8 bits to number the hosts on that network, as shown in Figure 5-6.

Figure 5-5 Determining Whether Hosts Are on the Same Network

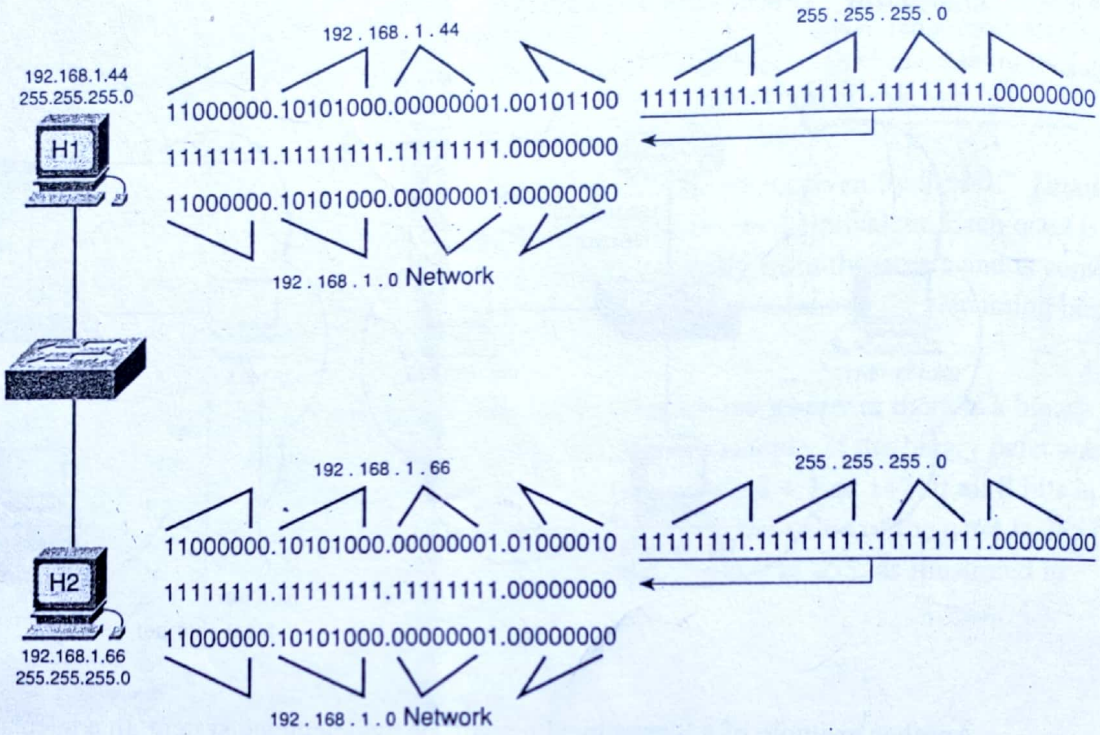
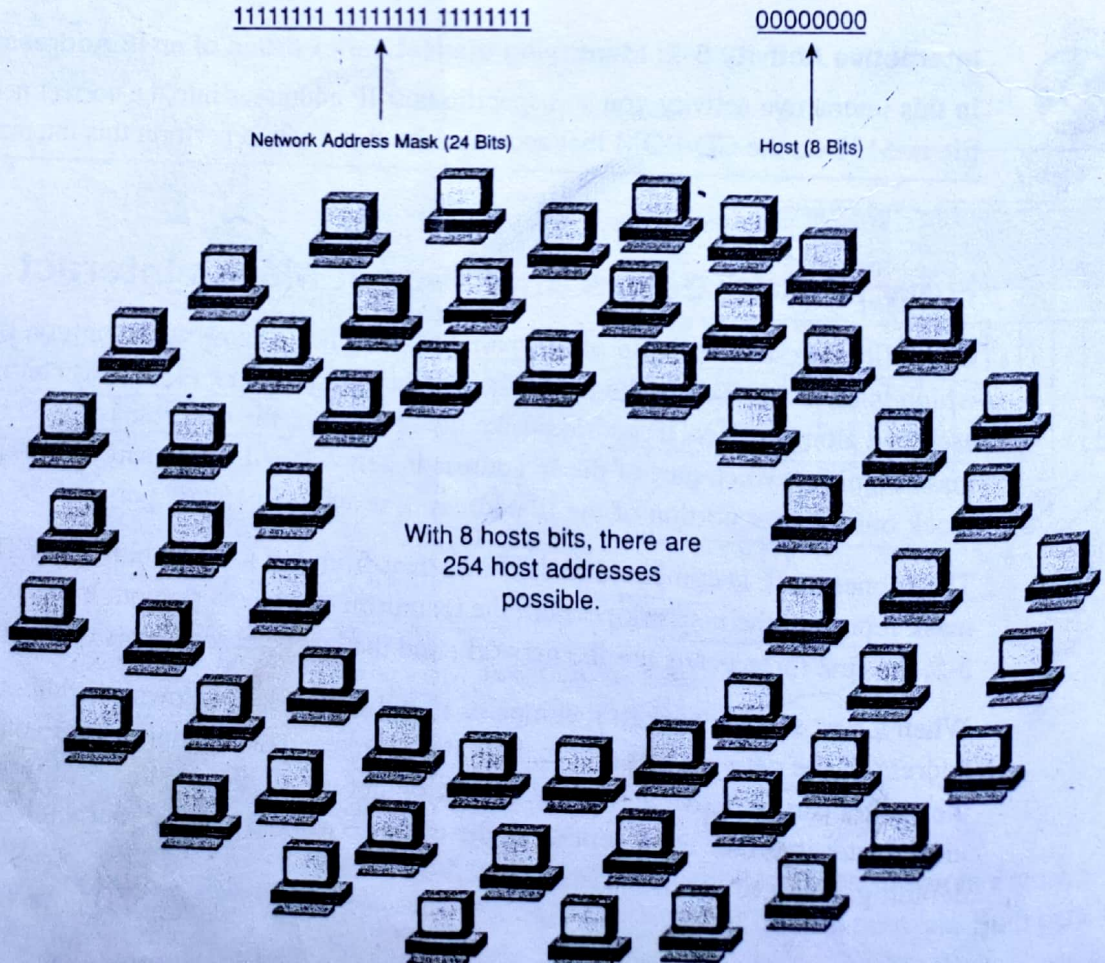


Figure 5-6 Number of Possible Hosts with Eight Host Bits



To calculate the number of hosts that can be on that network, take the number 2 to the power of the number of host bits ($2^8 = 256$). We do this because each bit can have one of two values, either a zero or a one. From this number, we must subtract 2 (256 – 2 = 254). The reason we subtract 2 is because we cannot assign an IP address that has either all 0s or all 1s in the host portion. An IP address with all 1s within the host portion is a broadcast address for that network and an address with all 0s within the host portion indicates the ***network number***. Powers of 2 can be calculated easily with the calculator that comes with any Windows operating system.

Another way to determine the number of hosts available is to add up the values of the available host bits (128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255). From this number, subtract 1 (255 – 1 = 254), because the host bits cannot be all 1s. Subtracting 2 is not necessary because the value of all 0s is 0 and is not included in the addition.

With a 16-bit mask, there are 16 bits (two octets) for host addresses, and a host address could have all 1s (255) in one of the octets. This address might appear to be a broadcast but as long as the other octet is not all 1s, it is a valid host address. Remember that the host looks at all host bits together, not at octet values.

Lab 5-1: Using the Windows Calculator with Network Addresses (5.1.4.3)

In this lab you use the Windows calculator to work with binary and decimal representations of the IP address and binary and hexadecimal representations of the MAC address. Refer to the lab in Part II of this *Learning Guide*. You may perform this lab now or wait until the end of the chapter.

Types of IP Addresses

Many different types of IP addresses are available. Some addresses indicate a special form of communication should occur whereas others are designed to provide adequate address space for use inside a company or organization. Some are routable on the Internet whereas others are not. The pattern of bits within the IP address tells the network devices how the packet should be treated.

IP Address Classes and Default Subnet Masks

The IP address and subnet mask work together to determine which portion of the IP address represents the network address and which portion represents the host address. IP addresses are grouped into five classes. ***Class A***, ***Class B***, and ***Class C*** are commercial addresses and are assigned to hosts. ***Class D*** is reserved for multicast use and ***Class E*** is for experimental use. These last two classes of addresses are not normally assigned to any one organization.

NOTE

The ***classful*** system of IP addressing breaks up the available address space into five distinct classes. Another system that exists, the ***classless*** system, does not rely on class boundaries but instead treats all address space as being equal. Any number of bits can be assigned to represent the network portion of an address leaving the rest to represent hosts. This also introduces a new nomenclature for specifying the subnet mask. Subnet masks in the classless system are represented by a slash followed by the number of bits used by the network portion. For example, the network address 192.168.1.2 with a subnet mask of 255.255.255.0 would be written as 192.168.1.2/24. This notation is referred to as ***classless interdomain routing (CIDR)***.

Class C address:

- Addresses have three octets for the network portion and one for the hosts
- Default subnet mask is 24 bits (255.255.255.0)
- Usually assigned to small networks

Class B address:

- Addresses have two octets to represent the network portion and two for the hosts
- Default subnet mask is 16 bits (255.255.0.0)
- Typically used for medium-sized networks

Class A address:

- Addresses have only one octet to represent the network portion and three to represent the hosts
- Default subnet mask is 8 bits (255.0.0.0)
- Typically assigned to large organizations

The class of an address can be determined by the value of the first octet. For example, if the first octet of an IP address has a value in the range 192 to 223, it is classified as a Class C address. As an example, 200.14.193.67 is a Class C address. Table 5-1 shows the ranges for the three assignable classes.

Table 5-1 IP Address Classes

Address Class	First Octet Range (Decimal)	First Octet Bits (Highlighted Bits Do Not Change)	Network (N) and Host (H) Portions of an Address	Default Subnet Mask (Decimal and Binary)	Number of Possible Networks and Hosts Per Network
A	1 – 127	00000000 – 01111111	N.H.H.H	11111111.00000000. 00000000.00000000 255.0.0.0	254 nets ($2^8 - 2$) 16.777.214 hosts per net ($2^{24} - 2$)
B	128 – 191	10000000 – 10111111	N.N.H.H	11111111.11111111. 00000000.00000000 255.255.0.0	65,534 nets ($2^{16} - 2$) 65,534 hosts per net ($2^{16} - 2$)
C	192 – 223	11000000 – 11011111	N.N.N.H	11111111.11111111. 11111111.00000000 255.255.255.0	16,777,214 nets ($2^{24} - 2$) 254 hosts per net ($2^8 - 2$)
D	224 – 239	11100000 – 11101111	Not for commercial use as a host		
E	240 – 255	11110000 – 11111111	Not for commercial use as a host		

TIP

The router reads the bits from the most significant bit (leftmost)to the least significant (rightmost). The values of the first several bits can tell the router what class address it is dealing with. For a Class A address the bit pattern starts as "0," for a class B it is "10," for a class C it is "110," and for a class D the pattern is "1110." Class E addresses are the remainder of the available values.

Interactive Activity 5-3: Subnet Mask Game (5.2.1.2)

In this interactive activity you must select the proper default subnet mask for an IP address. Use file ia-5212 on the CD-ROM that accompanies this book to perform this interactive activity.

Public and Private IP Addresses

All hosts that connect directly to the Internet require a unique ***public IP address***. Because of the finite number of 32-bit addresses available, there is a risk of running out of IP addresses. One solution to this problem was to reserve some private addresses for use exclusively inside an organization. This allows hosts within an organization to communicate with one another without the need of a unique public IP address.

RFC 1918 is a standard that reserves several ranges of ***private IP addresses*** within each of the classes A, B, and C. As shown in Table 5-2, these private address ranges consist of a single Class A network, 16 Class B networks, and 256 Class C networks, which gives a network administrator considerable flexibility in assigning internal addresses.

Table 5-2 RFC 1918 Private Address Space

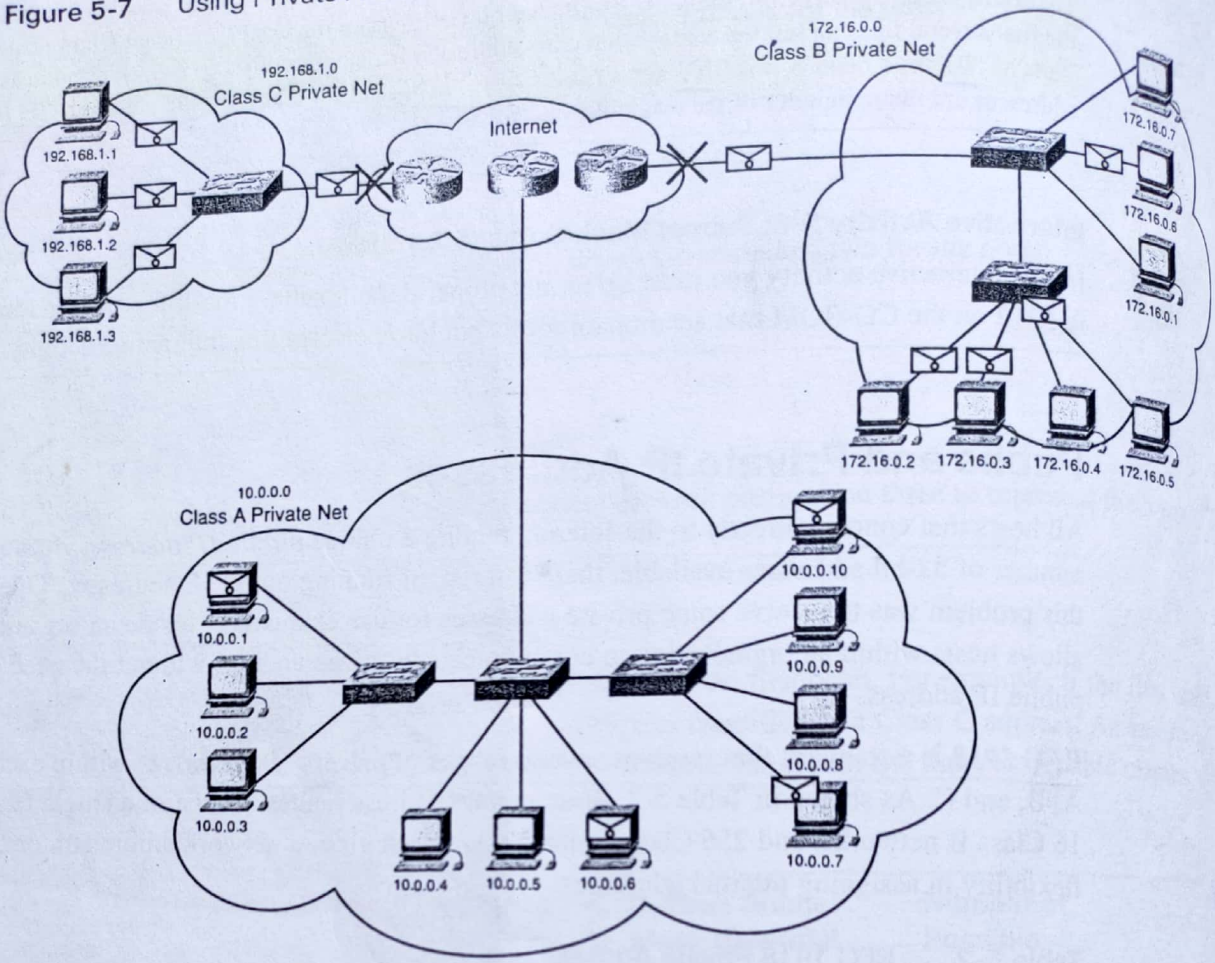
Address Class	Number of Network Numbers Reserved	Network Addresses
A	1	10.0.0.0
B	16	172.16.0.0 – 172.31.0.0
C	256	192.168.0.0 – 192.168.255.0

A very large network can use the Class A private network, which allows for more than 16 million private addresses. On medium-size networks, a Class B private network could be used, which provides more than 65,000 addresses. Home and small business networks typically use a single Class C private address, which allows up to 254 hosts.

The Class A network, the 16 Class B networks, or the 256 Class C networks, as defined by RFC 1918, can be used within any size organization. Typically many organizations use the Class A private network because it provides enough addresses to allow for easy organization of the internal hosts.

Hosts can use private addresses internally in an organization as long as they do not connect directly to the Internet. Therefore, the same set of private addresses can be used by multiple organizations. Private addresses are not routed on the Internet and will be quickly blocked by an ISP router, as shown in Figure 5-7.

Figure 5-7 Using Private Address Space on a Network



The use of private addresses can provide a measure of security because they are only visible on the local network, and outsiders cannot gain direct access to the private IP addresses.

There are also private addresses that can be used for the diagnostic testing of devices. One such private address is known as a ***loopback address***. The Class A 127.0.0.0 network is reserved for loopback addresses. Another address range has been reserved by Microsoft for use with ***Automatic Private IP Addressing (APIPA)***. With APIPA, a DHCP client automatically self-configures an IP address and subnet mask when a DHCP server is not available. The IP address range used for APIPA is 169.254.0.1 through 169.254.255.254. The client configures itself with an address from this range and a default Class B subnet mask of 255.255.0.0. A client uses the self-configured IP address until a DHCP server becomes available.

Interactive Activity 5-4: Address Blocker Game (5.2.2.3)

In this interactive activity you must decide to permit or deny an IP packet access to the Internet based on whether it is a private or public source IP address. Use file ia-5223 on the CD-ROM that accompanies this book to perform this interactive activity.

Unicast, Broadcast, and Multicast Addresses

In addition to address classes, we also categorize IP addresses as unicast, broadcast, or multicast depending on the nature of the message they carry. Hosts can use IP addresses to communicate one-to-one (unicast), one-to-many (multicast), or one-to-all (broadcast).

How IP Addresses Are Obtained

Because each host must be assigned a unique IP address, the management of IP addresses on a large network can be quite time-consuming if done manually. Luckily more automated methods of assigning IP addresses to hosts are available that relieve the network administrator from some of the burden.

Static and Dynamic Address Assignment

IP addresses can be assigned either statically or dynamically. Dynamic allocation allows the reuse of IP addresses and allows hosts to be configured without administrator intervention. Static assignment of host IP addresses is more labor intensive but also provides the network administrator with much more control over the flow of information on the network.

Static

With a static assignment, the network administrator must manually configure the network information for a host. At a minimum, this includes the host IP address, subnet mask, and default gateway.

Static addresses have some advantages. For example, they are useful for printers, servers, and other networking devices that need to be accessible to clients on the network. If hosts normally access a server at a particular IP address, it would not be good if that address changed.

Static assignment of addressing information can provide increased control of network resources, but entering the information on each host can be time-consuming. When you enter IP addresses statically, the host only performs basic error checks on the IP address. Therefore, errors are more likely to occur.

When using static IP addressing, maintaining an accurate list of which IP addresses are assigned to which devices is important. Additionally, these addresses are permanent and are not normally reused. Figure 5-11 shows the static assignment of IP information to a Windows machine.

Dynamic

On local networks it is often the case that the user population changes frequently. New users arrive with laptops and need a connection. Others have new workstations that need to be connected. Rather than have the network administrator assign IP addresses for each workstation, having IP addresses assigned automatically is easier. This is done using a protocol known as ***Dynamic Host Configuration Protocol (DHCP)***.

DHCP provides a mechanism for the automatic assignment of addressing information such as IP address, subnet mask, default gateway, and other configuration information. DHCP is generally the preferred method of assigning IP addresses to hosts on large networks because it reduces the burden on network support staff and virtually eliminates entry errors. It is also the preferred method for many home and small business users who may lack the knowledge necessary to properly configure the IP settings manually. Figure 5-12 shows how to configure a Windows machine to obtain an address automatically from a DHCP server.

Figure 5-11 Static Assignment of IP Address Information

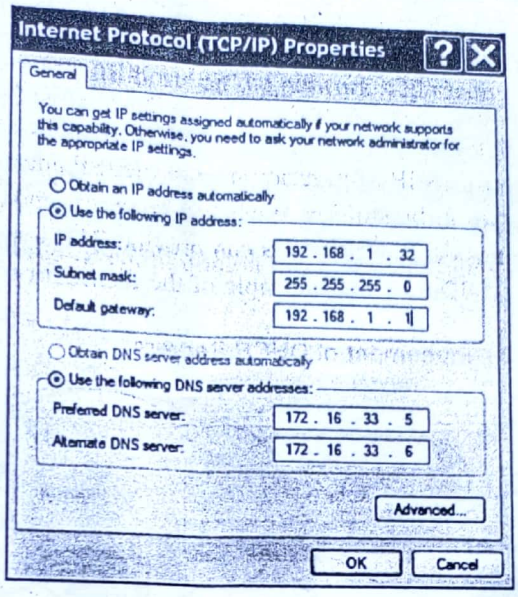
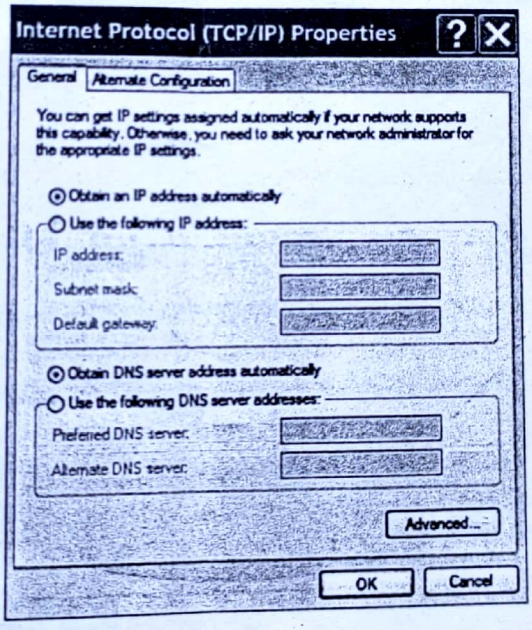


Figure 5-12 Dynamic Assignment of IP Address Information



Another benefit of DHCP is that an address is not permanently assigned to a host but is only leased for a period of time. If the host is powered down or taken off the network, the address is returned to the pool for reuse. This feature is especially helpful with mobile users that come and go on a network.

DHCP Servers

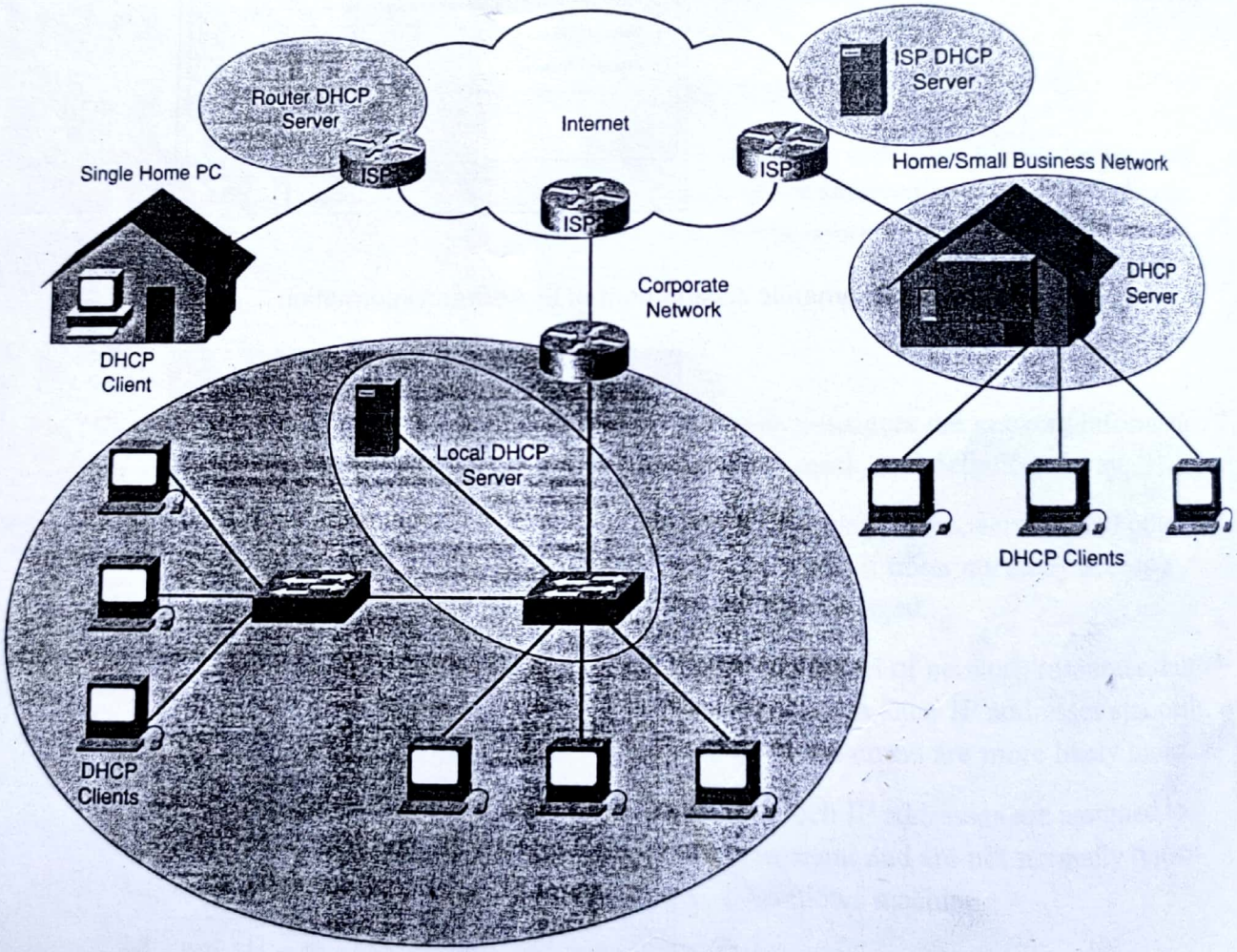
If you enter a wireless hotspot at an airport or coffee shop, DHCP makes accessing the Internet possible for you. As you enter the area, your laptop ***DHCP client*** contacts the local ***DHCP server*** via a wireless connection. The DHCP server assigns an IP address to your laptop.

If hosts are going to obtain IP addresses dynamically, a DHCP server needs to be configured on the network. Various types of devices can be DHCP servers as long as they are running DHCP service

software. With most medium to large networks, the DHCP server is usually a local dedicated PC-based server. With home networks, the DHCP server is usually located at the ISP, and a host on the home network receives its IP configuration directly from the ISP.

Many home networks and small businesses use an integrated router to connect to the ISP modem. In this case, the integrated router is both a DHCP client and a server. The integrated router acts as a client to receive its IP configuration from the ISP and then acts as a DHCP server for internal hosts on the local network. In addition to PC-based servers and integrated routers, other types of networking devices such as dedicated routers can provide DHCP services to clients, although this is not as common. Figure 5-13 shows an example of the distribution of DHCP servers.

Figure 5-13 Placement of DHCP Servers



Configuring DHCP

When a host is first configured as a DHCP client, it does not have an IP address, subnet mask, or default gateway. It obtains this information from a DHCP server, either on the local network or one located at the ISP. The DHCP server is configured with a range, or pool, of IP addresses that can be assigned to DHCP clients.

A client that needs an IP address will send a DHCP Discover message to try and locate a DHCP server that is capable of providing it with the required information. The *DHCP Discover* is a broadcast message with a destination IP address of 255.255.255.255 (32 ones) and a destination MAC address of FF-FF-FF-FF-FF-FF (48 ones). All hosts on the network will receive this broadcast DHCP frame, but only a DHCP server will reply. These DHCP messages are sent to port 67. Only DHCP servers are configured to listen on port 67. The server will respond with a *DHCP Offer*, suggesting an IP address for the client. The host then sends a *DHCP Request* to that server asking to use the suggested IP address. The server responds with a *DHCP Acknowledgment* that informs the client that it has permission to start using the offered IP configuration information. Figure 5-14 shows this process.

Figure 5-14 DHCP Process

For most home and small business networks, a multi-function device provides DHCP services to the local network clients. Most of these home devices are configured through a graphical interface that is accessed using a web browser. For example, to connect to the Linksys multi-function device, open a web browser and enter the default IP address of 192.168.1.1 in the Address area. After you are connected, you can navigate to the screen that shows the DHCP server configuration.

The IP address of 192.168.1.1 and subnet mask of 255.255.255.0 are the defaults for the internal router interface on the Linksys device. This is the default gateway for all hosts on the local network and also the internal DHCP server IP address. Most Linksys wireless routers and other home integrated routers have DHCP Server enabled by default.

On the DHCP configuration screen, a default ***DHCP range*** is available or you can specify a starting address for the DHCP range and the number of addresses to be assigned. You can also modify the ***lease time*** (default is 24 hours). The DHCP configuration feature on most multi-function devices gives information about connected hosts and IP addresses, their associated MAC address, and lease times, as shown in Figure 5-15.

Figure 5-15 DHCP Server Configuration on a Multi-Function Device