CHAPTER 5

OSI Network Layer

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- What is the method described by the network layer for routing packets from a device on one network to a device on a different network?
- How does the Internet Protocol (IP) work at the network layer to provide connectionless, best-effort service to the upper layers of the OSI model?
- How are devices grouped into physical and logical networks?
- How do the hierarchical addresses of devices allow communication between networks?
- How do routers use next-hop addresses to select a path for packets to reach their destination?
- How do routers forward packets?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

route page 136
source IP address page 137
destination IP address page 137
IP header page 137
routing page 138
hop page 138
directly connected network page 138
connection oriented page 140
connectionless page 140
overhead page 140
best-effort page 141
media independent page 141
maximum transmission unit (MTU) page 141
fragmentation page 142
Time to Live (TTL) page 143
subnetwork page 145
subnet page 145
broadcast domain page 149
hierarchical addressing page 151
octets page 152
default gateway page 153
routing table page 156
default route page 158
static route page 163
dynamic routing page 164
routing protocols page 164

Previous chapters explained how application data from an end device traveling to another network is first encapsulated in added bits that indicate presentation, session, and transport layer information and instructions. When the transport layer sends the protocol data unit (PDU) down to the network layer, the PDU needs the essentials of any successful journey: a destination address and directions on how to arrive efficiently and safely.

This chapter describes the process the network layer uses to convert transport layer segments into packets and get them started on their journey down the right path across different networks to the destination network. You learn how the network layer divides networks into groups of hosts to manage the flow of data packets. You also consider how communication between networks is facilitated. This facilitation of communication between networks is called *routing*.

IPv4

The network layer, or Open Systems Interconnection (OSI) Layer 3, provides services to exchange the individual pieces of data over the network between identified end devices. To accomplish this end-to-end transport, Layer 3 uses the processes outlined in the following sections to address the packet to the proper destination, encapsulate the packet with necessary data for delivery, route the packet through the web of connected networks that will deliver the packet to the destination network for delivery, and finally, have the destination host decapsulate the data for processing. The details of these processes are explored further in the next sections.

Network Layer: Communication from Host to Host

The network layer, or OSI Layer 3, receives segments of data, or PDUs, from the transport layer. These bits of data have been processed into a transportable size and numbered for reliability. It is now up to the network layer to use protocols to add addressing and other information to the PDU and send it to the next router along the best path, or ***route***, to the destination network.

Network layer protocols, such as the widely used IP, are rules and instructions that devices use to enable sharing of upper-layer information between hosts. When the hosts are in different networks, additional routing protocols are used to choose routes between networks. Network layer protocols specify the addressing and packaging of a transport layer PDU and describe how the PDU is to be carried with minimum overhead.

The network layer describes four tasks to be performed:

1. Addressing packets with an IP address
2. Encapsulation

3. Routing
4. Decapsulation

The next sections describe each task in more detail and describe popular network layer protocols.

Addressing

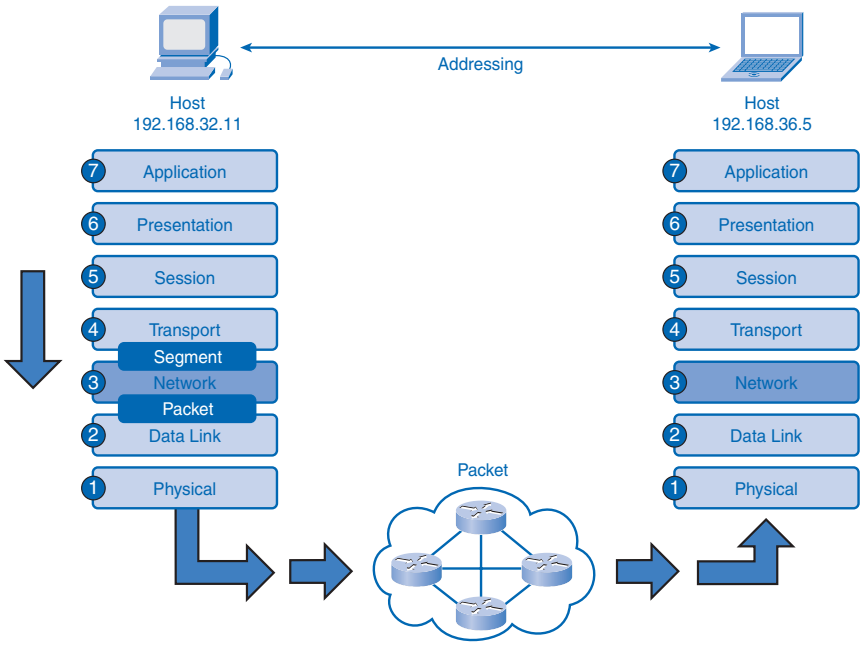
IP requires each sending and receiving device to have a unique IP address. Devices in IP networks that have IP addresses are called *hosts*. The IP address of the sending host is known as the ***source IP address***, and the IP address of the receiving host is referred to as the ***destination IP address***. The conventions of IP addressing will be explored in greater detail in Chapter 6, "Addressing the Network: IPv4."

Encapsulation

Each PDU sent between networks needs to be identified with source and destination IP addresses in an ***IP header***. The IP header contains the address information and some other bits that identify the PDU as a network layer PDU. This process of adding information is called *encapsulation*. When an OSI Layer 4 PDU has been encapsulated at the network layer, it is referred to as a *packet*.

Figure 5-1 displays how segments are encapsulated at the network layer and become IP packets. The process is reversed at the destination.

Figure 5-1 Network Layer Encapsulation



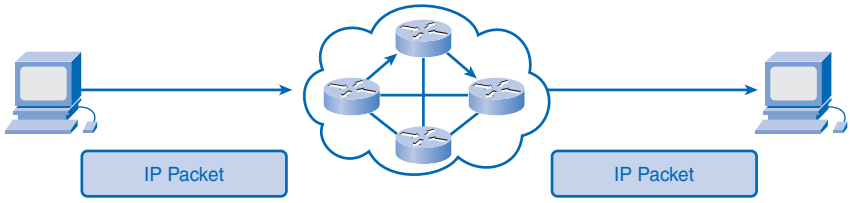
Routing

When a packet is encapsulated at the network layer, it contains all the information necessary to travel to networks near and far. The journey between networks can be very short and relatively simple, or it can be complex and involve many steps between routers connected to different networks.

Routers are devices that connect networks. They specialize in understanding OSI Layer 3 packets and protocols as well as calculating the best path for the packets. ***Routing*** is the process routers perform when receiving packets, analyzing the destination address information, using the address information to select a path for the packet, and then forwarding the packet on to the next router on the selected network. Each route that a packet takes to reach the next device is called a ***hop***. A packet can hop between several different routers en route to the destination. Each router examines the address information in the packet, but neither the IP address information nor the encapsulated transport layer data in the packet is changed or removed until the packet reaches the destination network.

Figure 5-2 shows how there can be several different paths in the internetwork cloud between a source host and a destination host.

Figure 5-2 Multiple Network Paths Between Hosts



At the network layer, the router opens the packet and looks in the packet header for IP address information. The router, depending on how it is configured and what it knows about the destination network, will choose the best network to deliver the packet. The router then forwards the packet out of the interface connected to the chosen network. The last router along the path will realize that the packet belongs to a ***directly connected network*** and will forward it out the correct network interface for final delivery on the local network.

For a network layer packet to travel between hosts, it must be handed down to the data link layer (OSI Layer 2) for another layer of encapsulation called *framing*, and then encoded and put onto the physical layer (OSI layer 1) to be sent to the next router. Details of how these two layers handle the data are the subject of Chapter 7, "OSI Data Link Layer," and Chapter 8, "OSI Physical Layer."

Decapsulation

An IP packet arrives at a router's network interface encapsulated in a Layer 2 frame on the physical OSI layer. The router's network interface card (NIC) accepts the packet, removes the Layer 2 encapsulation data, and sends the packet up to the network layer. The process of removing encapsulation data at different layers is referred to as *decapsulation*.

Encapsulation and decapsulation occur at all layers of the OSI model. As a packet travels from network to network to its destination, there can be several instances in which Layers 1 and 2 are encapsulated and decapsulated by routers. The network layer only decapsulates the IP packet at the final destination after examining the destination addresses and determining that the journey is over. The IP packet is no longer useful, so it is discarded by the destination host.

When the IP packet is decapsulated, the information in the packet is handed up to the upper layers for delivery and processing.

Network Layer Protocols

IP is the most common network layer protocol, but it is important to understand that other protocols are available that offer different features than IP. At one time, network protocols were largely proprietary, and communication was limited to a manufacturer's specific equipment. Internet Protocol version 4 (IPv4), however, is open source and allows devices from various manufacturers to communicate with each other. Table 5-1 lists some of the common network layer protocols.

Table 5-1 Common Network Protocols

Protocol	Description
Internet Protocol version 4 (IPv4)	Most widely used network protocol. Basic protocol of the Internet.
Internet Protocol version 6 (IPv6)	Currently in use in some areas. Will work with IPv4 and likely replace it.
Novell IPX	Part of Novell NetWare, a widely popular internetworking protocol in the 1980s and 1990s.
AppleTalk	Apple Computer's proprietary networking protocol.
Connectionless Network Service (CLNS)	A protocol used in telecommunication networks that does not require established circuits.

The IPv4 protocol describes services and packet structure that are used to encapsulate User Datagram Protocol (UDP) datagrams or TCP segments handed down from the transport layer of the OSI model. Because the Internet Protocol (IPv4 and IPv6) is the most widely used Layer 3 data-carrying protocol, it is the focus of this book. Discussion of the other protocols is minimal.

IPv4: Example Network Layer Protocol

Version 4 of IP (IPv4) is currently the most widely used version of IP. It is the only Layer 3 protocol that is used to carry user data over the Internet and is the focus of the CCNA. Therefore, it will be the example you use for network layer protocols in this course.

IP version 6 (IPv6) is developed and being implemented in some areas. IPv6 will operate alongside IPv4 and might replace it in the future. The services provided by IP, as well as the packet header structure and contents, are specified by either IPv4 or IPv6.

The characteristics of IPv4 and IPv6 are different. Understanding these characteristics will allow you to understand the operation of the services described by this protocol.

IP was designed as a protocol with low overhead. It provides only the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks. The protocol was not designed to track and manage the flow of packets. These functions are performed by other protocols in other layers.

IPv4 basic characteristics include the following:

- **Connectionless:** IPv4 does not establish a connection before sending data packets.
- **Best effort (unreliable):** IPv4 does not use processes that guarantee packet delivery, which reduces processing time on routers and saves the bandwidth that acknowledgment messages would otherwise require.
- **Media independent:** IPv4 operates independently of the medium carrying the data.

The next sections describe these three traits in greater detail.

Connectionless

As you learned in Chapter 4, "OSI Transport Layer," TCP's reliability comes from being ***connection oriented***. TCP uses a connection between the sender and the receiver to exchange control data and ensure reliability of packet delivery.

IP is ***connectionless***, meaning that there is no established connection between the sender and the receiver. IP simply sends packets without informing the receiver. Lacking a connection is not a problem for IP and is part of the "best effort" design. This is why IP and TCP work together so well in a TCP/IP stack: If a packet is lost or late, TCP will correct the problem at Layer 4, and IP can work more efficiently at Layer 3.

Because IP does not have to be accountable for reliability or keep a connection, it does not need as much information in the header as a TCP segment does. Because IP requires less data to perform the required tasks, it uses much less processing power and bandwidth, called ***overhead***, than TCP.

Best Effort

In Chapter 4, you also learned that TCP is reliable. It is reliable because communication is established with the receiver and receipt of the data is confirmed by the receiver. If packets are lost, the receiver communicates with the sender to request a retransmission. The TCP segment contains information that allows reliability to be ensured.

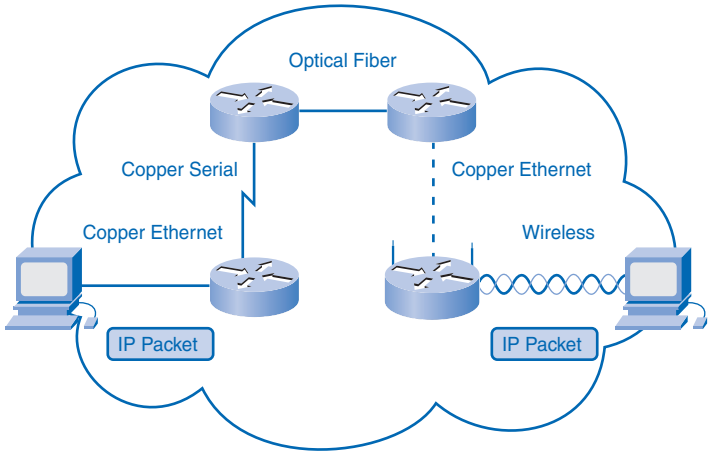
IP is an unreliable, ***best-effort*** protocol in that it is unaware of the quality of job it is performing. IP packets are sent without certainty that they will be received. The IP protocol makes a "best effort" to deliver packets, but it has no way of determining whether the packets are delivered successfully or whether they are lost en route. IP has no way to inform the sender of reliability problems. TCP can be relied on to inform the sender of delivery problems.

Media Independent

IP is ***media independent***, which means it is not concerned with the physical medium that carries the packet. Internetwork communication is likely to be a multimedia journey using a combination of wireless, Ethernet cable, fiber-optic cable, and other OSI Layer 1 media. The arrangement of bits in the IP packet and header will not be changed as the packet transfers from wireless to fiber or any other media.

Figure 5-3 shows how there can be several different physical layer media between the source host and destination host.

Figure 5-3 IP Packets Are Media Independent



One important consideration, however, is the size of the PDU. Some networks have media restrictions and must enforce a ***maximum transmission unit (MTU)***. The MTU is determined by the OSI data link layer, and that requirement is passed to the network layer.

The network layer then builds the packets according to specification. Should the packet come across a network that requires smaller packets, the router connected to the network will fragment the packets before forwarding them on the network's medium. This process is called ***fragmentation***.

The process of sending a packet across the web with the IP protocol is analogous to someone sending a surprise gift to a friend using a package delivery service. The gift, in this example three boxes strapped together, is taken to the delivery office already wrapped. The delivery service does not know (nor does it care) what is in the package. The package is an acceptable size, so the delivery workers add a label with the destination and return address and some of their own routing codes to the package. They place the gift in a standard container used for easy shipping. To keep costs low, the sender chooses simple service, which means nothing is guaranteed and the sender cannot track the package on the web. The container with the package travels by car to the dock terminal and then by boat to its destination terminal. From there it travels by truck to a city delivery office. The final local delivery is by bicycle. The package is too large for the bicycle carrier, so it is broken into three pieces for separate delivery. All pieces arrive at the destination, and the job of the delivery service is complete. Later the sender receives a thank-you note from her friend, and she is assured that the gift was delivered.

In this analogy, the gift was a surprise, so it was sent without notification (connectionless). It was encapsulated in the shipping office by adding source, destination, and control information (header). To reduce cost (overhead), the gift was sent "best effort" without guarantee. The service was media independent (traveled by car, boat, truck, and bicycle), but at one point, the package had to be fragmented into the original three boxes (but the gift itself was not altered). The delivery service did not assure the sender that the package was successfully delivered, but the sender relied on the higher-level protocol of good manners to receive notification that the package was delivered.

IPv4 Packet: Packaging the Transport Layer PDU

IPv4 encapsulates, or packages, the transport layer segment or datagram so that the network can deliver it to the destination host. The IPv4 encapsulation remains in place from the time the packet leaves the network layer of the originating host until it arrives at the network layer of the destination host.

The process of encapsulating data by layer enables the services at the different layers to develop and scale without affecting other layers. This means that transport layer segments can be readily packaged by existing network layer protocols, such as IPv4 and IPv6, or by any new protocol that might be developed in the future.

Routers can implement these different network layer protocols to operate concurrently over a network to and from the same or different hosts. The routing performed by these intermediary devices only considers the contents of the packet header that encapsulates the segment.

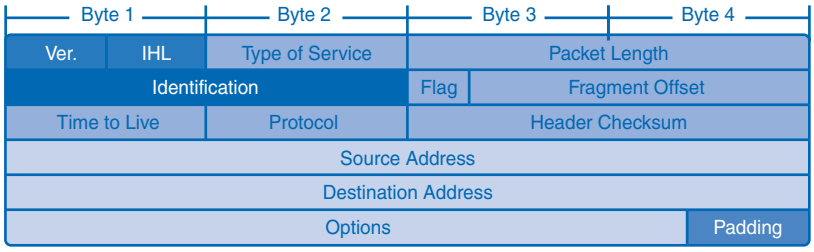
In all cases, the data portion of the packet—that is, the encapsulated transport layer PDU—remains unchanged during the network layer processes.

IPv4 Packet Header

The IP header holds the delivery and handling instructions for an IP packet. For example, when a packet arrives on a router's interface, the router needs to know whether the packet is IPv4 or IPv6. The router looks to a specific field in the header to see which type is arriving. The header also contains addressing information and other data about how to handle the packet along the way.

Figure 5-4 shows an outline of an IP packet header. There are several fields in the packet, and not every network uses every field. There are highlighted fields that are important to understanding how the IP header helps routers route IP packets successfully.

Figure 5-4 Components of an IP Header



The key fields are as follows:

- **IP Source Address:** Contains a 32-bit binary value that represents the host that will receive the packet. Routers will use this data to forward the packet to the correct network.
- **IP Destination Address:** Contains a 32-bit binary value that represents the host that will receive the packet. Routers will use this data to forward the packet to the correct network.
- ***Time to Live (TTL)*:** The 8-bit TTL field describes the maximum hops the packet can take before it is considered "lost" or undeliverable. Each router that handles the packet decrements the TTL field by at least 1. The packet will be dropped if the TTL value reaches 0. This keeps the Internet from being cluttered with lost packets.

- **Type of Service (ToS):** Each of the 8 bits in this field describes a level of throughput priority a router should use in processing the packet. For example, a packet containing IP voice data gets precedence over a packet containing streaming music. The way a router handles a packet from this data is known as *QoS*, or *quality of service*.
- **Protocol:** This 8-bit field indicates the upper-layer protocol—for example, TCP, UDP, or ICMP—that will receive the packet when it is decapsulated and given to the transport layer.
- **Flag and Fragment Offset:** A router might have to fragment a packet when forwarding it from one medium to another medium that has a smaller MTU. When fragmentation occurs, the IPv4 packet uses the Fragment Offset field and the MF flag in the IP header to reconstruct the packet when it arrives at the destination host. The Fragment Offset field identifies the order in which to place the packet fragment in the reconstruction.

Other fields are as follows:

- **Version:** Indicates IP version 4 or 6.
- **Internet Header Length (IHL):** Tells the router how long the header is. The length is not always the same because of variable data in the Options field.
- **Packet Length:** This is the total length of the datagram, including the header. The minimum length of a packet is 20 bytes (header with no data), and the maximum length with data is 65,535 bytes.
- **Identification:** Sent by the source to help reassemble any fragments.
- **Header Checksum:** This data is used to indicate the length of the header and is checked by each router along the way. An algorithm is run by each router, and if the checksum is invalid, the packet is assumed to be corrupted and is dropped. Because the TTL value is changed by each router that handles the packet, the header checksum is recalculated at each hop.
- **Options:** A rarely used field that can provide special routing services.
- **Padding:** Padding is used to fill in bits when header data does not end on a 32-bit boundary.

Networks: Dividing Hosts into Groups

Networks are communities of computers and other hosts, but in many ways, they are like human communities. When people live in a small town, it is usually easy for community members to find and communicate with each other. A small town does not need large roads and expensive traffic signals, and in general does not require as many services as a large

community. In a small town, many members also know and trust each other, and many consider smaller communities to be safer than big cities. As a town grows, however, it needs to scale its services to the needs of the increasing number of citizens. As the number of streets grows and the number of dwellings increases, a system for citizens to find each other easily must be designed and implemented. Finding other members gets more complex as a town becomes a city, and at some point, the city divides into more manageable neighborhoods, often connected by major roads, to better govern, serve, and secure the community members.

Computer communities are similar to human communities in that as they grow, they become more complex, and at some point, dividing the large networks into smaller, more manageable groups can make sense. As networks grow and divide, hosts still need to find each other to communicate. One of the major roles of the network layer is to provide a mechanism for addressing hosts in a way that allows all member hosts to find each other. As the number of hosts on the network grows, more planning is required to address the network so that it can be managed efficiently.

Creating Common Groups

Just as cities can be divided into geographic neighborhoods, large computer networks can be separated into internetworks. Departments and groups that share computers and servers are good candidates for dividing into groups from the large network into a common ***subnetwork***, or ***subnet***. Membership in a subnet requires following the rules of communication provided by the TCP/IP protocols.

Historically, large computer networks were divided geographically, like city neighborhoods, because workers with common tasks tended to be clustered into workgroups. The early technology for computer network communication was designed for workgroups that were close together. As networking technology evolved, the nature of the workgroups began to change. Now network members can be grouped not just by physical attributes, but by abstract attributes such as purpose and ownership.

Grouping Hosts Geographically

Grouping network hosts geographically is an economical way to improve communications by reducing overhead for the users, especially if most of their communication stays in the neighborhood. When communication leaves the subnet, it can be subject to external bandwidth issues. Figure 5-5 shows an example of grouping by office locations.

Figure 5-5 Grouping by Physical Location

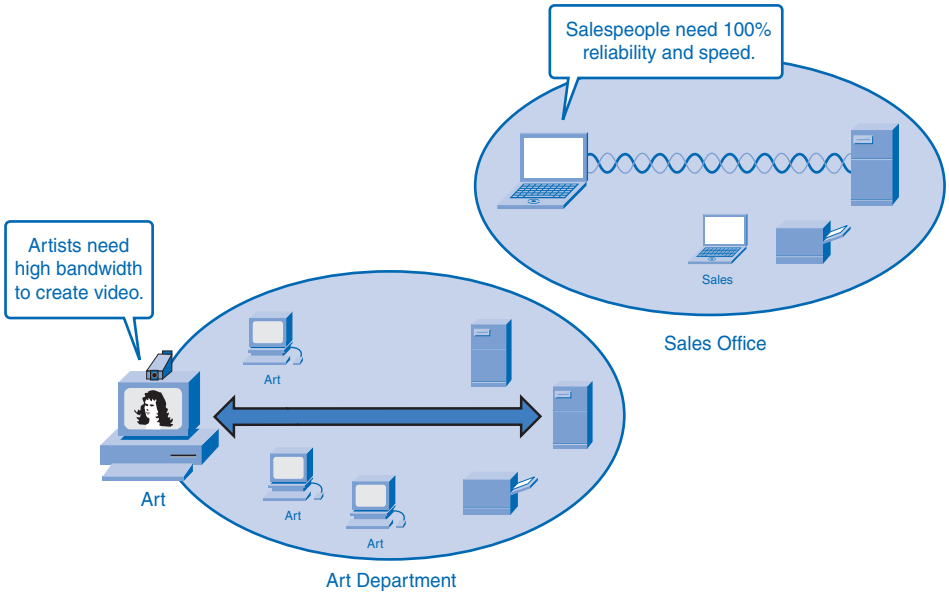
The simple fact of wiring together the physical network can make geographic location a logical place to start when segmenting a network.

Grouping Hosts for a Specific Purpose

People on a large network will likely use computers for many different reasons. The tools people use for work are increasingly software based and are requiring ever-increasing amounts of computing power to perform work tasks. The purpose of these tasks can be clerical, design, education, government administration, or e-commerce. Each purpose can have specialized software that can consume substantial resources. Whatever the purpose, a network must provide sufficient resources to allow people to work. It can make sense for a network manager to divide a network by purpose instead of geography so that people sharing a common purpose are also sharing common resources.

In Figure 5-6, the business employs salespersons who can only log in once a day to record their sales transactions, which generates minimal network traffic. The art department has very different functions and requires different computing resources. In this scenario, the best use of network resources would be to create a network for artists to access and another one for the salespeople to use.

Figure 5-6 Grouping by Purpose

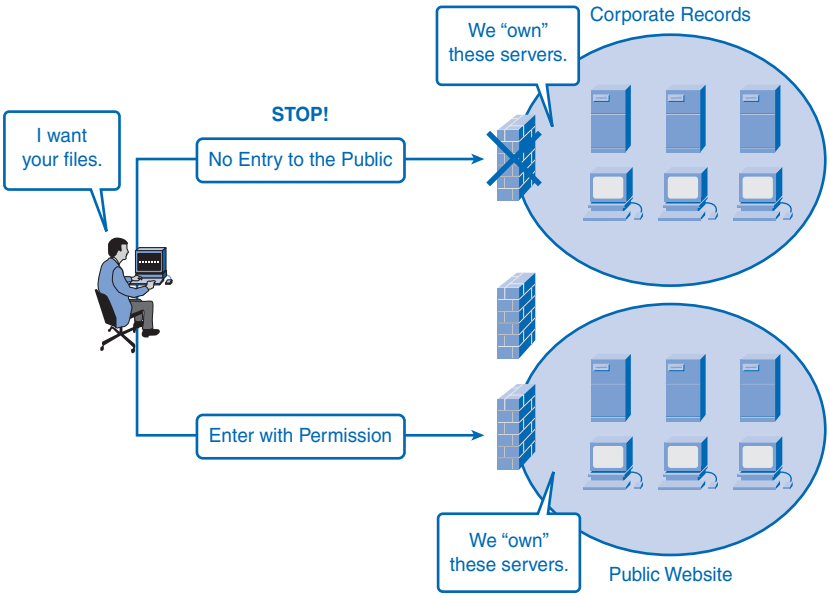


Grouping Hosts for Ownership

Ownership of (and access to) information is another way to group users. Grouping by purpose and geography is concerned with efficient resources and reduced network overhead. In an ownership group, the main concern is security. In a large network, it is much more difficult to define and limit the responsibility and access for the network personnel. Dividing hosts into separate networks provides a boundary for security enforcement and management of each network.

In the previous example, networks were grouped by their differing functions. In Figure 5-7, corporate records and the public website are kept separate, because it was determined that their need for security is more important than their physical location or group function.

Figure 5-7 Grouping by Ownership



Why Separate Hosts into Networks?

As communities and networks grow larger, they present problems that can be alleviated by dividing the network into smaller, interconnected networks. In growing computer networks, some common issues arise, such as the following:

- Performance degradation
- Security issues
- Address management

Performance

Hosts on a network can be chatty devices. They are designed to broadcast news about themselves to all other users on the network. A *broadcast* is a message sent from one host to all other hosts on the network, and the purpose is usually to share its own information and to request information about other hosts. Broadcasts are a necessary and useful tool used by protocols as part of the communication process. When a group of computers is networked, they generate broadcasts to each other, and the more users on a network, the more broadcasting consumes bandwidth. As users are added, performance quality decreases because the broadcast traffic takes up valuable bandwidth that can otherwise be carrying productive

data. Because broadcasts do not travel beyond the network boundary, the network is known as a ***broadcast domain***. Isolating groups of users into smaller networks reduces the size of broadcast domains and restores performance.

Packet Tracer Activity

Routers Segment Broadcast Domains (5.2.2.2)

In this activity, the replacement of a switch with a router breaks one large broadcast domain into two more manageable ones. Use file e1-5222.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Security

As more of the world's businesses and consumers shift their trade onto the Internet, so too are thieves and cyber-pirates finding new ways to exploit the web for criminal gain. Policing a large community like the Internet can be a daunting task, but tending to a small neighborhood's security needs is much more manageable.

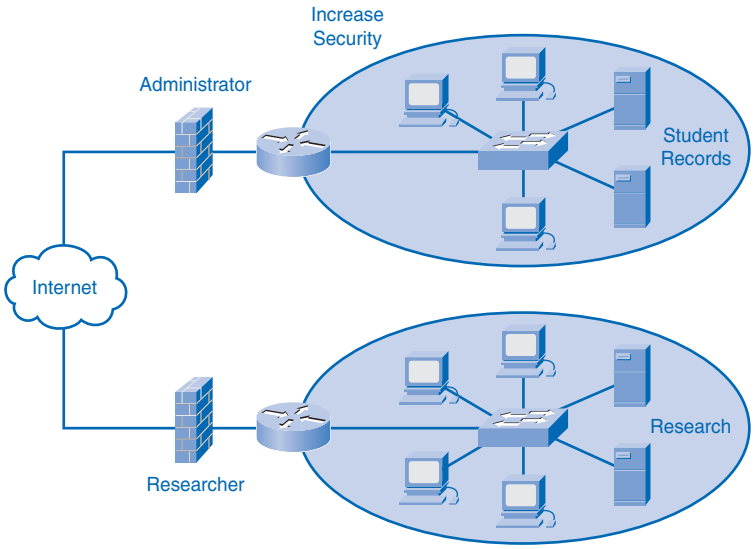
The original IP-based network that has now become the Internet once consisted of a small number of trusted users in government agencies and research organizations. In such a small community of known users, security was a fairly simple issue.

Since then, the Internet has grown beyond recognition, and now individuals, businesses, and organizations have developed their own IP networks that can link to the Internet. The hosts, network equipment, and data are the property of those network owners. By isolating themselves from the larger networks and shielding their devices from public access, companies and organizations can better protect themselves from spies and thieves. A local network manager can more easily control outside access to the smaller network.

Internetwork access within a company or organization can be similarly secured. For example, a college network can be divided into administrative, research, and student subnetworks. Dividing a network based on user access is an effective way to protect the organization's interests and employee privacy. Such access restrictions can protect an organization from both unauthorized internal access and malicious external attacks.

Security between networks is controlled in an intermediary device (a router or firewall appliance) at the perimeter of the network. The firewall function can be configured to allow only known, trusted data and users to access the network. Figure 5-8 displays a network with firewalls protecting information while allowing access to the Internet.

Figure 5-8 Firewalls



Address Management and Hierarchical Addressing

A group of hosts in a network can be compared to a small neighborhood in a town with a helpful local post office. The postal worker knows all the residents and their streets and street addresses, but he does not share that information with anyone outside the neighborhood.

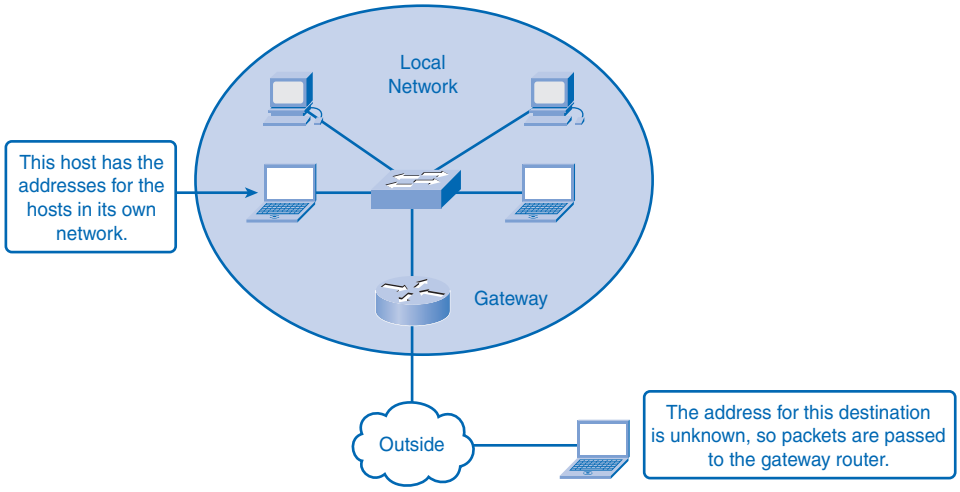
Just as the neighborhood post office has a postal code that identifies the physical location of the neighborhood, a network has a network address that identifies the logical location of the network on a router. (Because computer networks are not restricted to physical locations, IPv4 provides a logical system of keeping track of networks.) An IPv4 address contains both network bits that identify a logical network address and host bits that contain a local "inside the neighborhood" address of the end device.

In the neighborhood analogy, residents (hosts) can communicate with others in their neighborhood quite easily. They know each other's street addresses and trust each other, and they are constantly chatting and checking up on each other. If they need to send messages somewhere outside the neighborhood, however, they give the message to the postal worker, who figures out how to forward the message to another post office in the neighborhood of the destination. This frees the residents on the inside of the neighborhood from having to know how to communicate with all the possible addresses outside their known neighborhood. The post office serves as a community gateway to communication with the world outside the neighborhood.

When messages arrive from the outside, they are addressed with information containing the address of both the neighborhood post office (the postal code) and the street address (the local address). The helpful postal worker takes all the messages addressed to the neighborhood, sorts them by address, and delivers the message inside the neighborhood to the proper recipient.

This example also describes the basic function of network addressing. Routers act as postal workers at post offices for small networks by taking care of messages going out and serving as a general destination and sorting station for messages coming in. The router a network uses to send and receive messages beyond the network is called a *gateway router*. Figure 5-9 depicts a gateway router providing local hosts with access to an outside host whose address is unknown inside the network.

Figure 5-9 Gateway Routers Provide Outside Network Access



The address is divided into two parts: the network address and the host address. The network portion of the address tells routers where to find the general network, and the host portion is used by the last router for delivery inside the network. The structure of the IP address will be explored in greater detail in Chapter 6.

The type of addressing in the analogy is considered hierarchical. ***Hierarchical addressing*** is read from the most general information to the most specific. When a letter or package is sent through the postal service, there is an addressing protocol. Figure 5-10 shows an example of a properly addressed letter for the Canadian postal system.

Figure 5-10 Hierarchical Postal Address

The address in Figure 5-10 will be read by postal workers from the most general information (the country and postal code) to the most specific (the name of the addressee). When the letter is in the hands of the Canadian postal service, the postal code will be used to route the letter to the neighborhood of its destination. (In reality, the first few characters of the postal code include province and city information, so the city and province information in the letter address is redundant.) When the letter is in the neighborhood, the postal worker uses the street address to get to the house, and then the name identifies the person in the house who gets the letter. Postal codes in most countries use the same hierarchical organization.

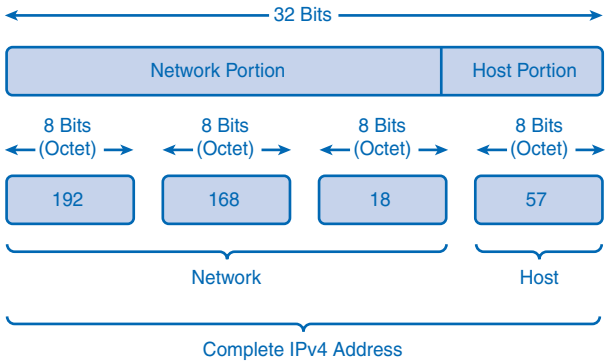
Dividing Networks from Networks

The IPv4 address is composed of 32 bits divided into two parts: the network address and the host address. The network portion of the address acts like a postal code and tells routers where to find the general neighborhood of a network. Routers forward packets between networks by referring only to the network portion. When the packet arrives at the last router, like a letter arriving at the last postal station, the local portion of the address identifies the destination host.

The IPv4 addressing system is flexible. If a large network needs to be divided into smaller subnets, additional network codes can be created using some of the bits designated for the host in a process called *subnetting*. Network managers use this flexibility to customize their private networks. IPv4's ability to scale to the ever-growing demands of the Internet has contributed to its wide use.

Figure 5-11 shows the basic structure of an IPv4 address. In this address, the three ***octets*** to the left are the general network address, and the last octet is used by the destination router to identify the local host.

Figure 5-11 Hierarchical IPv4 Address



The portion of the address that is network and the portion that is host can vary. The structure of the IP addressing will be explored in greater detail in Chapter 6.

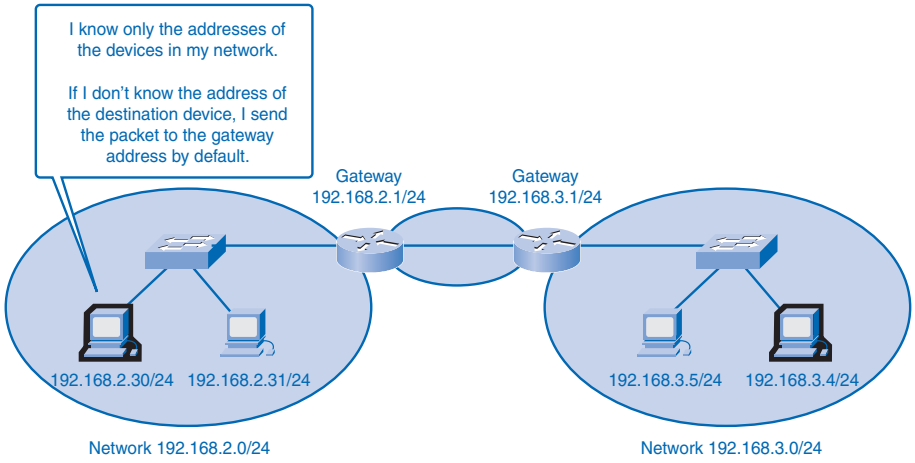
Routing: How Data Packets Are Handled

Communication within a network, or subnet, happens without a network layer device. When a host communicates outside the local network, a router acts as a gateway and performs the network layer function of choosing a path for the packet.

Device Parameters: Supporting Communication Outside the Network

As a part of its configuration, a host has a ***default gateway*** address defined. As shown in Figure 5-12, this gateway address is the address of a router interface that is connected to the same network as the host. The router interface is actually a host on the local network, so the host IP address and the default gateway address must be on the same network. Figure 5-12 shows that default gateways are members of their own local networks.

Figure 5-12 Gateways Enable Communications Between Networks



The default gateway is configured on a host. On a Windows computer, the Internet Protocol (TCP/IP) Properties tools are used to enter the default gateway IPv4 address. Both the host IPv4 address and the gateway address must have the same network (and subnet, if used) portion of their respective addresses.

IP Packets: Carrying Data End to End

The role of the network layer is to transfer data from the host that originates the data to the host that uses it. During encapsulation at the source host, an IP packet is constructed at Layer 3 to transport the Layer 4 PDU. If the destination host is in the same network as the source host, the packet is delivered between the two hosts on the local media without the need for a router.

However, if the destination host and source host are not in the same network, the packet can be carrying a transport layer PDU across many networks and through many routers. As it does, the information contained within is not altered by any routers when forwarding decisions are made.

At each hop, the forwarding decisions are based on the information in the IP packet header. The packet with its network layer encapsulation also is basically intact throughout the complete process, from the source host to the destination host.

If communication is between hosts in different networks, the local network delivers the packet from the source to its gateway router. The router examines the network portion of the packet destination address and forwards the packet to the appropriate interface. If the destination network is directly connected to this router, the packet is forwarded directly to that host. If the destination network is not directly connected, the packet is forwarded to a second router that is the next-hop router.

The packet forwarding then becomes the responsibility of this second router. Many routers or hops along the way can process the packet before reaching the destination.

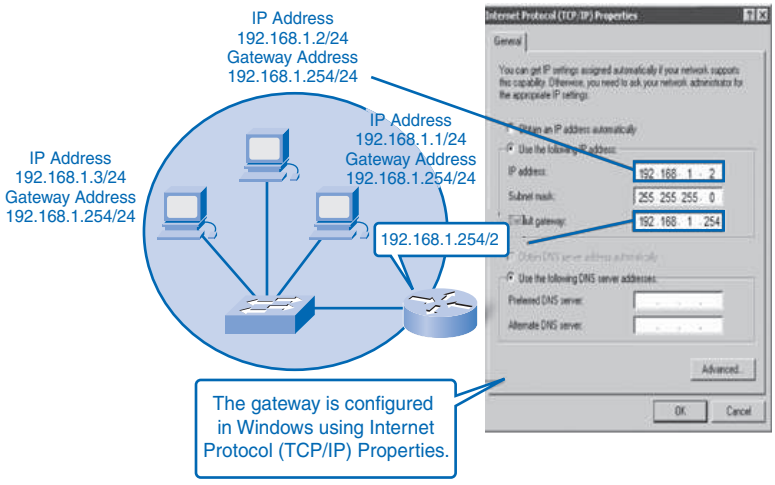
Gateway: The Way Out of the Network

The gateway, also known as the default gateway, is needed to send a packet out of the local network. If the network portion of the destination address of the packet is different from the network of the originating host, the packet has to be routed outside the original network. To do this, the packet is sent to the gateway. This gateway is a router interface connected to the local network. The gateway interface has a network layer address that matches the network address of the hosts. The hosts are configured to recognize that address as the gateway.

Default Gateway

The default gateway is configured on a host. On a Windows computer, the Internet Protocol (TCP/IP) Properties tools are used to enter the default gateway IPv4 address. Both the host IPv4 address and the gateway address must have the same network (and subnet, if used) portion of their respective addresses. Figure 5-13 depicts the Windows TCP/IP Properties configuration.

Figure 5-13 IP Address and Gateway Configuration in Windows



No packet can be forwarded without a route. Whether the packet is originating in a host or being forwarded by an intermediary device, the device must have a route to identify where to forward the packet.

A host must either forward a packet to the host on the local network or to the gateway, as appropriate. To forward the packets, the host must have routes that represent these destinations.

A router makes a forwarding decision for each packet that arrives at the gateway interface. This forwarding process is referred to as *routing*. To forward a packet to a destination network, the router requires a route to that network. If a route to a destination network does not exist, the packet cannot be forwarded.

The destination network can be a number of routers or hops away from the gateway. The route to that network would only indicate the next-hop router to which the packet is to be forwarded, not the final router. The routing process uses a route to map the destination network address to the next hop and then forwards the packet to this next-hop address.

Confirming the Gateway and Route

An easy way to check the host IP address and default gateway is by issuing the **ipconfig** command at the command-line prompt of a Windows XP computer:

Step 1. Open the command-prompt window by clicking the Windows Start button in the lower-left corner of the desktop.

Step 2. Choose the Run icon.

Step 3. In the text box, type **cmd** and press **Enter**.

Step 4. The c:\Windows\system32\cmd.exe program is running. At the prompt, type **ipconfig** and press Enter. The Windows IP configuration will display with the IP address, subnet mask, and default gateway addresses.

Example 5-1 shows a sample of the **ipconfig** output with the host's IP address information.

Example 5-1 Confirming the IP Address and Gateway Route

```
C:\> ipconfig

Windows IP Configuration
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  .  :
        IP Address.....................: 192.168.1.2
        Subnet Mask....................: 255.255.255.0
        Default Gateway................: 192.168.1.254
```

Route: A Path to a Network

A route for packets for remote destinations is added using the default gateway address as the next hop. Although it is not usually done, a host can also have routes manually added through configurations.

Like end devices, routers also add routes for the connected networks to their ***routing table***. When a router interface is configured with an IP address and subnet mask, the interface becomes part of that network. The routing table now includes that network as a directly

connected network. All other routes, however, must be configured or acquired through a routing protocol. To forward a packet, the router must know where to send it. This information is available as routes in a routing table.

The routing table stores information about connected and remote networks. Connected networks are directly attached to one of the router interfaces. These interfaces are the gateways for the hosts on different local networks. Remote networks are networks that are not directly connected to the router. Routes to these networks can be manually configured on the router by the network administrator or learned automatically using dynamic routing protocols.

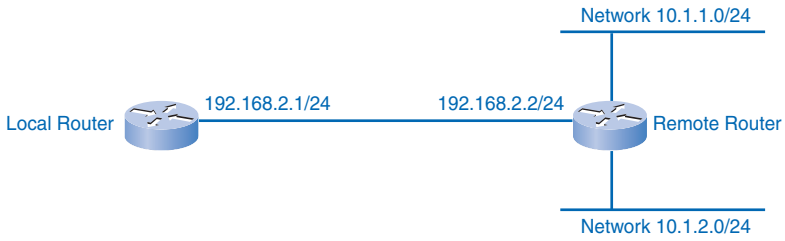
Routes in a routing table have three main features:

- Destination network
- Next-hop
- Metric

The router matches the destination address in the packet header with the destination network of a route in the routing table and forwards the packet to the next-hop router specified by that route. If there are two or more possible routes to the same destination, the metric is used to decide which route appears on the routing table.

Figure 5-14 shows a sample network with a local router and a remote router. Example 5-2 displays the routing table in the local router, which you can examine with the **show ip route** command from a router's console. From left to right, the output contains the destination network, the metric of [120/1], and the next hop through 192.168.2.2.

Figure 5-14 Confirming the Gateway and Route



Example 5-2 Router's Routing Table

```
Local_Router# show ip route

10.0.0.0/24 is subnetted, 2 subnets
R    10.1.1.0  [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R    10.1.1.0  [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

Note

The routing process and the role of metrics are the subject of a later course and companion book.

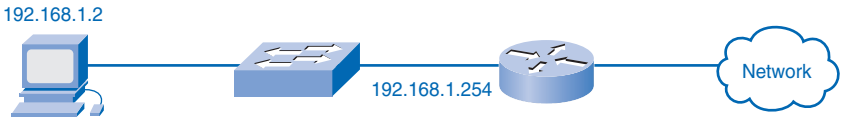
As you know, packets cannot be forwarded by the router without a route. If a route representing the destination network is not on the routing table, the packet will be dropped (that is, not forwarded). The matching route could be either a connected route or a route to a remote network. The router can also use a default route to forward the packet. The ***default route*** is used when the destination network is not represented by any other route in the routing table.

Host Routing Table

Hosts require a local routing table to ensure that network layer packets are directed to the correct destination network. Unlike the routing table in a router, which contains both local and remote routes, the local table of the host typically contains its direct connection or connections (hosts can belong to more than one local network) and its own default route to the gateway. Configuring the default gateway address on the host creates the local default route. Without a default gateway or route, packets destined outside the network will be dropped.

Figure 5-15 shows a simple network for the host routing table example that follows. The routing table of a computer host can be examined at the Windows command line by issuing the **netstat –r** or the **route print** command. Note that the host (192.168.1.2) serves as its own gateway to its own network (192.168.1.0) and has a default gateway for destinations outside the network pointing to the router interface (192.168.1.254).

Figure 5-15 Simple Network for Example 5-3



How To

Follow these steps to display a local routing table on a host:

Step 1. Open the command-prompt window by clicking the Windows Start button in the lower-left corner of the desktop.

Step 2. Choose the Run icon.

Step 3. In the text box, type **cmd** and click the OK button or press **Enter**.

Step 4. The c:\Windows\system32\cmd.exe program is running. At the prompt, type **route print** or **netstat -r** and press Enter. The route table listing all known routes on the host will display.

Example 5-3 shows the host routing table.

Example 5-3 Host IP Routing Table Commands

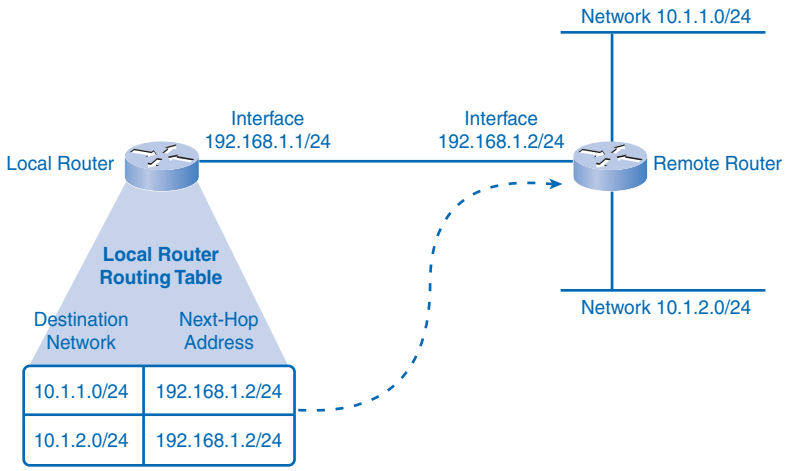
```
C:\> netstat -r

Route Table
———————————————————————————————————————————
Interface List
0x2….00 0f fe 26 f7 7b …Gigabit Ethernet – Packet Scheduler Miniport
———————————————————————————————————————————
Active Routes:
Network Destination    Netmask           Gateway           Interface        Metric
0.0.0.0                0.0.0.0           192.168.1.254     192.168.1.2      20
192.168.1.0            255.255.255.0     192.168.1.2       192.168.1.2      20
Default Gateway:       192.168.1.254
// output omitted //
———————————————————————————————————————————
```

When a host creates packets, it uses the routes it knows to forward them to the locally connected destination. These local network packets are delivered on the local route within the network without using a router. No packet is forwarded without a route. Whether the packet is originating in a host or being forwarded by an intermediary router, the device must have a route to identify which interface will be used to forward the packet. A host must either forward a packet to the host on the local network or to the gateway, as appropriate.

Routing

Routing is the process a router performs when making forwarding decisions for each packet arriving at the gateway interface. To forward a packet to a destination network, the router requires a route to that network. If a route to a destination network does not exist on the router, the packet will be forwarded to a default gateway. If no default gateway is configured, the packet cannot be forwarded. The destination network can be a number of routers or hops away from the gateway. If the router has an entry for the network in its routing table, it would only indicate the next-hop router to which the packet is to be forwarded, not the exact route to the final router. The routing process uses a routing table to map the destination network address to the next hop and then forwards the packet to this next-hop address. Figure 5-16 depicts a portion of a local router's routing table.

Figure 5-16 Local Router's Routing Table



Destination Network

For a router to route a packet to a destination network efficiently, it needs information about the route in its routing table. With millions of routes on the Internet, however, it is not reasonable to expect every route to be known to the router. The following sections describe how routers use information in routing tables and how packets can be forwarded when no information about routes can be found.

Routing Table Entries

The route, or destination network, in a routing table entry represents a range of host addresses and sometimes a range of network and host addresses.

The hierarchical nature of Layer 3 addressing means that one route entry can refer to a large general network and another entry can refer to a subnet of that same network. When forwarding a packet, the router will select the most specific route that it knows. If a specific subnet is not in the routing table but the larger network that holds the subnet is known, the router will send it to the larger network, trusting that another router will find the subnet.

Consider Example 5-4. If a packet arrives at the router with the destination address of 10.1.1.55, the router forwards the packet to a next-hop router associated with a route to network 10.1.1.0. If a route to 10.1.1.0 is not listed in the routing table but a route to 10.1.0.0 is available, the packet is forwarded to the next-hop router for that network.

Example 5-4 Routes in a Routing Table

```
10.0.0.0/24 is subnetted, 2 subnets
R    10.1.1.0  [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R    10.1.1.0  [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

The precedence the router uses for route selection for the packet going to 10.1.1.55 is as follows:

1. 10.1.1.0
2. 10.1.0.0
3. 10.0.0.0
4. 0.0.0.0 (default route if configured)
5. Dropped

In this case, the 10.1.1.0 network is known through 192.168.2.2, which is out the FastEthernet 0/0 interface.

Default Route

Remember that a default route is the route used if no specific route is available to be selected for delivery. In IPv4 networks, the address 0.0.0.0 is used for this purpose. Packets with a destination network address that does not match a more specific route in the routing table are forwarded to the next-hop router associated with the default route. The default route is also known as the *gateway of last resort*. When a default route is configured in a router, you can see it in the output, as noted in the first line of Example 5-5.

Example 5-5 Gateway of Last Resort

```
Gateway of Last Resort is 192.168.2.2 to Network 0.0.0.0
10.0.0.0/24 is subnetted, 2 subnets
R    10.1.1.0  [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R    10.1.1.0  [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 [1/0] via 192.168.2.2
```

Next Hop: Where the Packet Goes Next

The *next hop* is the address of the device that will process the packet next. For a host on a network, the address of the default gateway (router interface) is the next hop for all packets destined for another network.

As each packet arrives at a router, the destination network address is examined and compared to the routes in the routing table. The routing table lists an IP address for the next-hop router for the routes it knows. If a matching route is determined, the router then forwards

the packet out the interface to which the next-hop router is connected. Example 5-6 outlines the association of routes with next hops and router interfaces.

Example 5-6 Routing Table Output with Next Hops

```
10.0.0.0/24 is subnetted, 2 subnets
R    10.1.1.0  [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R    10.1.1.0  [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

As you can see in Example 5-6, some routes can have multiple next hops. This indicates that there are multiple paths to the same destination network. These are parallel routes that the router can use to select paths and forward packets.

Packet Forwarding: Moving the Packet Toward Its Destination

Routing is performed packet by packet and hop by hop. Each packet is treated independently by each router along the path. At each hop, the router examines the destination IP address for each packet and then checks the routing table for forwarding information. The router will then do one of the following with the packet:

- Forward it to the next-hop router
- Forward it to the destination host
- Drop it

A router takes the following steps to determine the appropriate action:

1. As an intermediary device, a router processes the packet at the network layer. However, packets that arrive at a router's interfaces are encapsulated as a data link layer (Layer 2) PDU. The router first discards the Layer 2 encapsulation so that the IP packet can be examined.
2. The router examines the IP address.
3. The router checks the routing table for a match.
4. The router selects the next hop. In the router, the destination address in a packet header is examined. If a matching route in the routing table shows that the destination network is directly connected to the router, the packet is forwarded to the interface to which that network is connected.
5. The router then does one of the following:
    - **Scenario A: The router forwards the packet.** If the route matching the destination network of the packet is a remote network, the packet is forwarded to the indicated interface, encapsulated by the Layer 2 protocol, and sent to the next-hop address. If the destination network is on a directly connected network, the

packet has to be first reencapsulated by the Layer 2 protocol and then forwarded out the proper interface to the local network.

- **Scenario B: The router uses the default route.** If the routing table does not contain a more specific route entry for an arriving packet, the packet is forwarded to the interface indicated by a default route, if one exists. At this interface, the packet is encapsulated by the Layer 2 protocol and sent to the next-hop router. The default route is also known as the *gateway of last resort*.
- **Scenario C: The router drops the packet.** If a packet is dropped, IP, by design, has no provision to return a packet to the sender or previous router. Such a function would detract from the protocol's efficiency and low overhead. Other protocols are used to report such errors.

Packet Tracer Activity

Router Packet Forwarding (5.3.7.4)

In this activity, the rules (algorithms) that routers use to make decisions on how to process packets, depending on the state of their routing tables when the packet arrives, are examined. Use file e1-5374.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Routing Processes: How Routes Are Learned

Routers need information about other networks to build a reliable routing table. Networks and routes are constantly changing, with new networks coming on and routes going down. If a router has bad information about routes, it is likely it will forward packets incorrectly, causing packets to be delayed or dropped. It is vital that routers have current information about neighboring routers to reliably forward packets. The two ways in which a router can learn information about routes is through static routing and dynamic routing. The following sections also introduce common routing protocols used by routers to dynamically share information.

Static Routing

The route information can be manually configured on the router, creating what is known as a ***static route***. An example of a static route is a default route. Static routing requires a network administrator for initial setup and for any changes to routes. Static routes are considered very reliable, and the router does not use much overhead to process packets. On the other hand, static routes do not update automatically and have higher continuing administrative costs.

If the router is connected to a number of other routers, knowledge of the internetworking structure is required. To ensure that the packets are routed to use the best possible next

hops, each known destination network needs to either have a route or a default route configured. Because packets are forwarded at every hop, every router must be configured with static routes to next hops that reflect its location in the internetwork.

Furthermore, if the internetwork structure changes or if new networks become available, these changes have to be manually updated on every router. If updating is not done in a timely fashion, the routing information can be incomplete or inaccurate, resulting in packet delays and possible packet loss.

Dynamic Routing

Routers can also learn about routes automatically from other routers in the same internetwork, which is known as ***dynamic routing***. Dynamic routing updates arrive from other routers and are used by the receiving router without administrative configuration. Dynamic routing has higher router processing overhead but little administrative cost after initial setup.

If dynamic routing is not enabled and configured on a router, static routes to the next hops must be in place for the router to know where to forward packets.

Routing Protocols

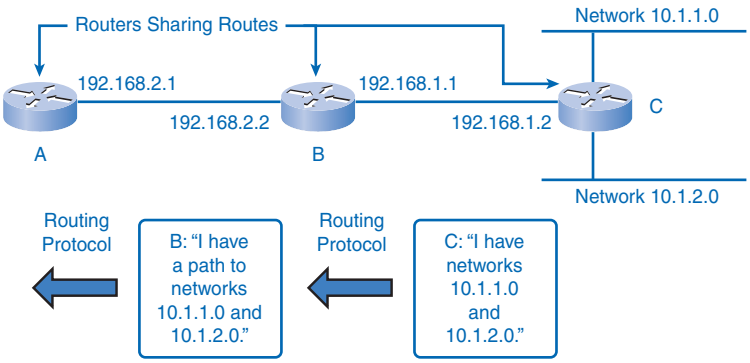
It is imperative that all routers in an internetwork have up-to-date and extensive route knowledge. Maintaining the routing table by manual static configuration is not always feasible. Configuring one of several available dynamic routing protocols on network routers is a much more efficient way to keep the routers updated.

Routing protocols are the set of rules by which routers dynamically share their routing information. As routers become aware of changes to the networks for which they act as the gateway, or changes to links between other routers, the information is passed on to other routers. When a router receives information about new or changed routes, it updates its own routing table and, in turn, passes the information to other routers. In this way, all routers have accurate routing tables that are updated dynamically and can learn about routes to remote networks that are many hops away. An example of routers sharing routes is shown in Figure 5-17.

The most common routing protocols used in this book are

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Protocol (EIGRP)
- Open Shortest Path First (OSPF)

Figure 5-17 Dynamic Route Sharing



Router B learns about Router C's networks dynamically.
Router B's next hop to 10.1.1.0 and 10.1.2.0 is 192.168.1.2 (Router C).
Router A learns about Router C's networks dynamically from Router B.
Router A's next hop to 10.1.1.0 and 10.1.2.0 is 192.168.2.2 (Router B).

The advantage of routing protocols providing routers with up-to-date routing tables is tempered by added overhead costs. The exchange of route information adds overhead by consuming network bandwidth. This overhead can be an issue with low-bandwidth links between routers. Another cost is the router's processing overhead. Not only does each packet need to be processed and routed, but updates from routing protocols also require complicated algorithmic calculations before the route information can be used in a routing table. This means that routers employing these protocols must have sufficient processing capacity to both implement the protocol's algorithms and to perform timely packet routing and forwarding, which can add to initial network setup costs.

Static routing does not produce network overhead and places entries directly into the routing table with no route processing required by the router. The cost for static routing, as mentioned earlier, is administrative time taken to manually configure and maintain routing tables in a manner that ensures efficient routing.

In most internetworks, a combination of static (including default) and dynamic routes is used to provide efficient routing. The configuration of routing protocols on routers is an integral component of the CCNA and will be covered extensively by *Routing Protocols and Concepts, CCNA Exploration Companion Guide*.

Packet Tracer Activity

Observing Dynamic Routing Protocol Updates (5.4.3.2)

In this activity, you will examine a simple visualization of a dynamic routing protocol in "action." Use file e1-5432.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Summary

The most significant network layer (OSI Layer 3) protocol is the IP. IP version 4 (IPv4) is the network layer protocol that will be used as an example throughout this book, although IPv6 is available and operational in many areas.

Layer 3 IP routing does not guarantee reliable delivery or establish a connection before data is transmitted. This connectionless and unreliable communication is fast and efficient, but upper layers must provide mechanisms to guarantee delivery of data if it is needed.

The role of the network layer is to encapsulate upper-level data into a packet and route it from one host to another, regardless of the type of data. The data is encapsulated in a packet. The packet header has fields that include the source and destination addresses of the packet.

Hierarchical network layer addressing, called an IP address, with network and host portions, allows the division of networks into subnets. The network portion of the IP address is used for forwarding packets between routers toward the destination. Only the last router connected to the destination network uses the host portion of the IP address.

If a host creates a packet with a destination address outside the local network, the packet is sent to the default gateway for forwarding to the destination network. The default gateway is an interface of a router that is on the local network. The gateway router examines the destination address and, if the gateway router has knowledge of a route to the destination network in its routing table, forwards the packet either to a connected network or to the next-hop router. If no routing entry exists, the router can forward the packet on to a default route or, lacking a default route, drop the packet.

Routing table entries are configured either statically on each router to provide static routing and default routes, or dynamically to collect and share route information with other routers automatically by using one or more routing protocols.

The network layer encapsulates data from the transport layer and sends it down to the data link layer (OSI Layer 2). Chapter 6 explores the communication process at the data link layer of the OSI model.

Labs

The labs available in the companion *Network Fundamentals, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-203-6) provide hands-on practice with the following topics introduced in this chapter:

Lab 5-1: Examining a Device's Gateway (5.5.1)

In this lab, you will examine the purpose of a gateway address, configure network parameters on a Windows computer, and then troubleshoot a hidden gateway address problem.

Lab 5-2: Examining a Route (5.5.2)

In this lab, you will use the **route** command to modify a Windows computer route table, use a Windows Telnet client to connect to a Cisco router, and then examine the router's routing table using basic Cisco IOS commands.

Many of the hands-on labs include Packet Tracer companion activities, where you can use Packet Tracer to complete a simulation of the lab. Look for this icon in *Network Fundamentals, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-203-6) for hands-on labs that have Packet Tracer companion activities.

Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix, "Check Your Understanding and Challenge Questions Answer Key," lists the answers.

1. Which protocol provides connectionless network layer services?

   A. IP
   B. TCP
   C. UDB
   D. OSI

2. What two commands can be used to view a host's routing table?

3. Select three pieces of information about a route that a routing table contains.

   A. Next-hop
   B. Source address
   C. Metric
   D. Destination network address
   E. Last hop
   F. Default gateway

4. What kinds of problems are caused by excessive broadcast traffic on a network segment? (Choose three.)

   A. Consumes network bandwidth
   B. Increases overhead on network
   C. Requires complex address schemes
   D. Interrupts other host functions
   E. Divides networks based on ownership
   F. Advanced hardware required

5. What are three key factors to consider when grouping hosts into a common network?

6. Which of the following are not functions of the network layer? (Choose two.)

   A. Routing
   B. Addressing packets with an IP address
   C. Delivery reliability
   D. Application data analysis
   E. Encapsulation
   F. Decapsulation

7. Which of the following are true about IP? (Choose two.)

   A. IP stands for International Protocol.
   B. It is the most common network layer protocol.
   C. It analyzes presentation layer data.
   D. It operates at OSI Layer 2.
   E. It encapsulates transport layer segments.

8. What is the name of the process of removing the OSI Layer 2 information from an IP packet?

9. Which of the following is true about IP?

   A. It is connection oriented.
   B. It uses application data to determine the best path.
   C. It is used by both routers and hosts.
   D. It is reliable.

10. Which of the following are true about network layer encapsulation? (Choose two.)

   A. It adds a header to a segment.
   B. It can happen many times on the path to the destination host.
   C. It is performed by the last router on the path.
   D. Both source and destination IP addresses are added.
   E. It converts transport layer information into a frame.

11. Which of the following are true about TCP and IP? (Choose two.)

   A. TCP is connectionless and IP is connection oriented.
   B. TCP is reliable and IP is unreliable.
   C. IP is connectionless and TCP is connection oriented.
   D. TCP is unreliable and IP is reliable.
   E. IP operates at the transport layer.

12. Why is IP "media independent"?

   A. It encapsulates Layer 1 instructions.
   B. It works the same on all Layer 1 media.
   C. It carries both video and voice data.
   D. It works without Layer 1 media.

13. TCP is a _____ layer protocol.

14. How many bits are in an IPv4 address?

15. Which of the following are true about static and dynamic routing? (Choose two.)

   A. Static routing requires a routing protocol such as RIP.
   B. A default route is a dynamic route.
   C. Dynamic routing adds packet-processing overhead.
   D. Administrative overhead is reduced with static routing.
   E. Routers can use static and dynamic routing simultaneously.

Challenge Questions and Activities

These questions require a deeper application of the concepts covered in this chapter. You can find the answers in the appendix.

1. What can happen when the TTL is 1? (Choose two.)

   A. The packet can be successfully delivered if it is destined for a directly connected network.

   B. TCP controls in the packet will add hops to the TTL.

   C. The packet will be dropped by the next router unless that router has an interface on the destination network.

   D. The packet will be returned to the source host.

   E. The packet will be returned to the previous router.

2. IP is connectionless and will occasionally drop a packet en route to a destination IP address. If packets are dropped, how will messages be completed?

   A. Only the IP portion of the packet is dropped, but the TCP portion continues to the last router.

   B. The routing protocols will carry the TCP information to the previous-hop router, which sends a reverse notification to the source.

   C. The routing protocols, such as RIP, are connection oriented and will contact the source host.

   D. The destination host is expecting the packet and will send a request if it does not arrive.

   E. The IP header contains the source address so that the packet can be returned by the router that receives the packet when the TTL is 0.

Packet Tracer Challenge

Look for this icon in *Network Fundamentals, CCNA Exploration Labs and Study Guide* (ISBN 1-58713-203-6) for instructions on how to perform the Packet Tracer Skills Integration Challenge for this chapter.

To Learn More

The following questions encourage you to reflect on the topics discussed in this chapter. Your instructor might ask you to research the questions and discuss your findings in class.

1. How can lost data be re-sent when the network layer uses unreliable and connectionless means of packet forwarding?

2. In what network circumstances would it be more advantageous to use static routing instead of dynamic routing protocols?