Chapter 8. IP Addressing

Objectives

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

- What are the parts of an IPv4 address?
- What is the purpose of the subnet address?
- What are the similarities and differences among unicast, broadcast, and multicast IPv4 addresses?
- What are the uses of public and private address space?
- What are the reasons for the development of IPv6 addressing?
- How are IPv6 addresses represented?
- What are the different types of IPv6 addresses?
- How are global unicast addresses configured?
- What are the purpose and uses of multicast addresses?
- How is ICMP used in IPv4 and IPv6 addresses?
- How are the ping and traceroute utilities used to test network connectivity?

Key Terms

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

subnetwork* page *393

American Standard Code for Information Interchange (ASCII)* page *394

octet* page *394

network address* page *402

prefix length* page *402

slash notation* page *402

host address* page *405

broadcast address* page *405

logical AND* page *406

directed broadcast* page *412

limited broadcast* page *412

multicast client* page *414

public address* page *416

private address* page *416

link-local address* page *418

TEST-NET address* page *418

classful addressing page *419*

classless addressing page *421*

Internet Assigned Numbers Authority (IANA) page *422*

Internet service provider (ISP) page *422*

hextet page 429

unspecified address page 433

unique local address page 433

Stateless Address Autoconfiguration (SLAAC) page 439

round-trip time (RTT) page 457

Introduction (8.0.1.1)

This chapter examines in detail the structure of IP addresses and their application to the construction and testing of IP networks and ***subnetworks***.

Addressing as a key function of network layer protocols enables data communication between hosts, regardless of whether the hosts are on the same network or on different networks. Both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) provide hierarchical addressing for packets that carry data.

Designing, implementing, and managing an effective IP addressing plan ensures that networks can operate efficiently.

Class Activity 8.0.1.2: The Internet of Everything (IoE)

If nature, traffic, transportation, networking, and space exploration depend on digital information sharing, how will that information be identified from source to destination?

In this activity, you will begin to think about not only what will be identified in the IoE world but also how everything will be addressed in the same world!

- Read the blog/news source provided by John Chambers regarding the Internet of Everything (IoE): http://blogs.cisco.com/news/internet-of-everything-2. View the video halfway down the page.
- Next, venture to the IoE main page: www.cisco.com/web/tomorrow-starts-here/index.html. Click a category that interests you.
- View the video, blog, or .pdf file that belongs to your IoE category of interest.
- Write five comments or questions about what you saw or read, and share with the class.

IPv4 Network Addresses (8.1)

For communication to take place between hosts, the appropriate addresses must be applied to these devices. Managing the addressing of the devices and understanding the IPv4 address structure and its representation are essential.

IPv4 Address Structure (8.1.1)

This section will present the IPv4 address structure.

Binary Notation (8.1.1.1)

To understand the operation of devices on a network, we need to look at addresses and other data the way devices do—in binary notation. Binary notation is a representation of information using only 1s and 0s. Computers communicate using binary data. Binary data can be used to represent many different forms of data. For example, when typing letters on a keyboard, those letters appear on screen in a form that you can read and understand; however, the computer translates each letter to a series of binary digits for storage and transport. To translate those letters, the computer uses ***American Standard Code for Information Interchange (ASCII)***.

With ASCII, each character is represented by a string of 7 bits. This allows a total of 128 different characters to be represented. Extended ASCII uses 8 bits per character, allowing the representation of 256 different characters. Each byte is used to represent a single character using extended ASCII. For example, the uppercase letter *A* is represented by the bit pattern 0100 0001 while the lowercase letter *a* is represented in bit form as 01100001, the character for the number 9 is represented by the pattern 0011 1001, and the # symbol is represented by 0010 0011.

While it is not generally necessary for people to concern themselves with binary conversion of letters, it is necessary to understand the use of binary for IP addressing. Each device on a network must be uniquely identified using a binary address. In IPv4 networks, this address is represented using a string of 32 bits (1s and 0s). At the network layer, the packets then include this unique identification information for both the source and destination systems. Therefore, in an IPv4 network, each packet includes a 32-bit source address and a 32-bit destination address in the Layer 3 header.

For most individuals, a string of 32 bits is difficult to interpret and even more difficult to remember. Therefore, we represent IPv4 addresses using dotted-decimal format instead of binary. This means that we look at each byte (***octet***) as a decimal number in the range of 0 to 255. To understand how this works, we need to have some skill in binary-to-decimal conversion.

Positional Notation

Learning to convert binary to decimal requires an understanding of the mathematical basis of a numbering system called positional notation. Positional notation means that a digit represents different values depending on the position the digit occupies. In a positional notation system, the number base is called the radix. In the base 10 system, the radix is 10. In the binary system, we use a radix of 2. The terms radix and base can be used interchangeably. More specifically, the value that a digit represents is that value multiplied by the power of the base, or radix, represented by the position the digit occupies. Some examples will help to clarify how this system works.

For the decimal number 192, the value that the 1 represents is $1*10^2$ (1 times 10 to the power of 2). The 1 is in what we commonly refer to as the “100s” position. Positional notation refers to this position as the base 2 position because the base, or radix, is 10 and the power is 2. The 9 represents $9*10^1$ (9 times 10 to the power of 1). The 2 represents $2*10^0$ (2 times 10 to the power of 0)

Using positional notation in the base 10 number system, 192 represents:

$$192 = (1 * 10^2) + (9 * 10^1) + (2 * 10^0)$$

or

192 = (1 * 100) + (9 * 10) + (2 * 1)

Binary Number System (8.1.1.2)

In IPv4, addresses are 32-bit binary numbers. However, for ease of use by people, binary patterns representing IPv4 addresses are expressed as dotted decimals. This representation is first accomplished by separating each byte (8 bits) of the 32-bit binary pattern, called an octet, with a dot. It is called an octet because each decimal number represents 1 byte, or 8 bits.

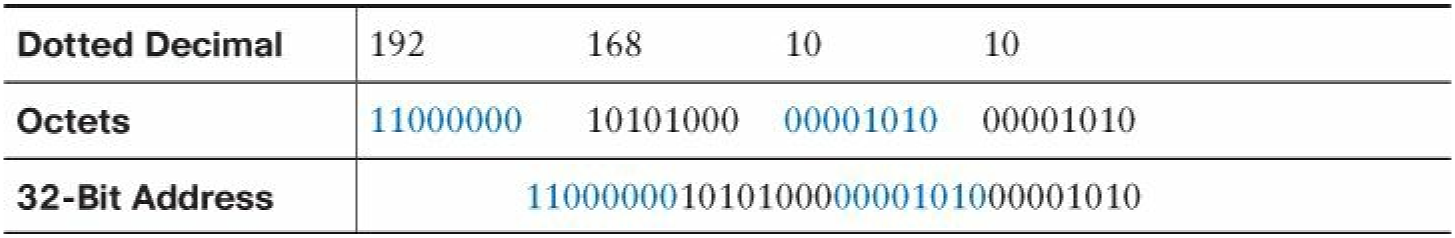
The binary address

11000000 10101000 00001010 00001010

is expressed in dotted decimal as

192.168.10.10

Table 8-1 shows different representations of the IPv4 address of 192.168.10.10. This includes dotted-decimal, binary octets, and the full 32 bit address.



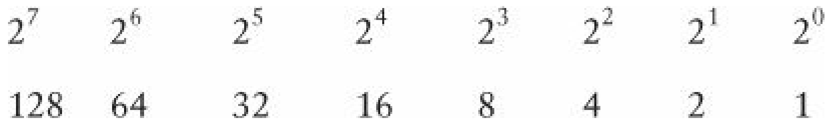
Dotted Decimal	192	168	10	10
Octets	11000000	10101000	00001010	00001010
32-Bit Address	11000000101010000000101000001010			

Table 8-1 IPv4 Address Representation

To understand the dotted-decimal representation, you need to understand how actual decimal equivalents are determined.

Binary Numbering System

In the binary numbering system, the radix is 2. Therefore, each position represents increasing powers of 2. In 8-bit binary numbers, the positions represent these quantities:

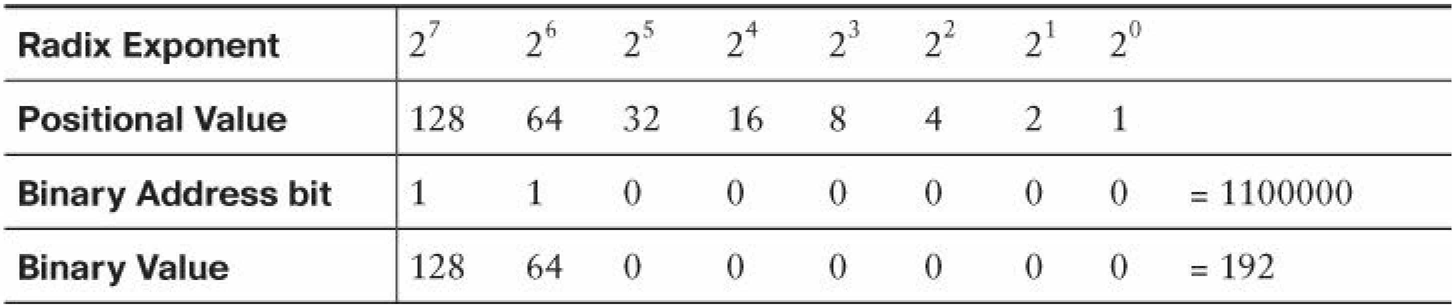


2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

The base 2 numbering system only has two digits: 0 and 1.

When we interpret a byte as a decimal number, we have the quantity that position represents if the digit is a 1 and we do not have that quantity if the digit is a 0.

Table 8-2 illustrates the representation of the decimal number 192 in binary. A 1 in a certain position means that we add that value to the total. A 0 means we do not add that value. The binary number 11000000 has a 1 in the 2^7 position (decimal value 128) and a 1 in the 2^6 position (decimal value 64). The remaining bits are all 0. So, no further corresponding decimal values are added. The result of adding 128+64 is 192, the decimal equivalent of 11000000.

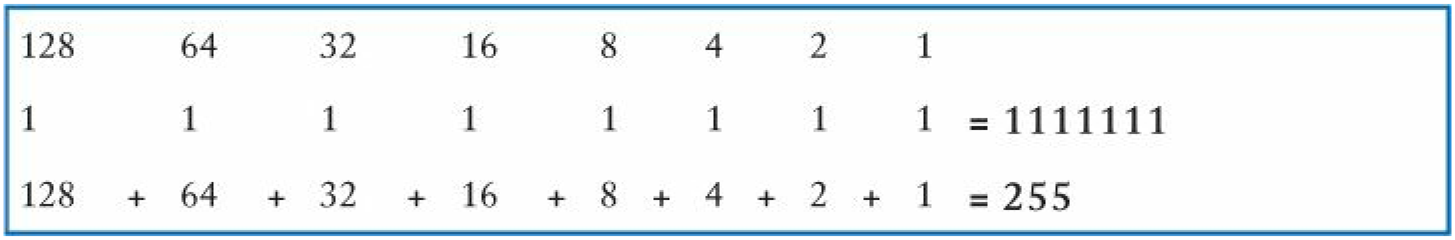


Radix Exponent	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Positional Value	128	64	32	16	8	4	2	1	
Binary Address bit	1	1	0	0	0	0	0	0	= 1100000
Binary Value	128	64	0	0	0	0	0	0	= 192

Table 8-2 Representation of Decimal Number 192

Examples 8-1 and 8-2 show the extreme values of an octet. A 1 in each position means that we add the value for that position to the total. In Example 8-1, all 1s means that the values of every position are included in the total; therefore, the value of all 1s in an octet is 255.

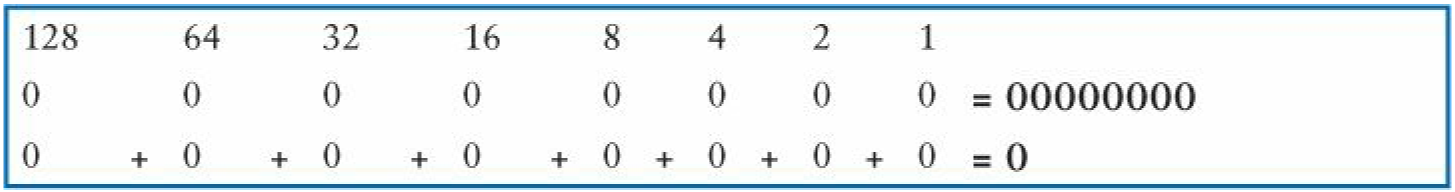
Example 8-1 Octet Containing All 1s: 11111111



128	64	32	16	8	4	2	1	
1	1	1	1	1	1	1	1	= 1111111
128	+ 64	+ 32	+ 16	+ 8	+ 4	+ 2	+ 1	= 255

A 0 in each position indicates that the value for that position is not included in the total. In Example 8-2, a 0 in every position yields a total of 0.

Example 8-2 Octet Containing All 0s: 00000000



128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	= 00000000
0	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0	= 0

Each different combination of 1s and 0s will yield a different decimal value.

Converting a Binary Address to Decimal (8.1.1.3)

Each octet is made up of 8 bits and each bit has a value, either 0 or 1. The four groups of 8 bits have the same set of valid values in the range of 0 to 255 inclusive. The value of each bit placement, from right to left is 1, 2, 4, 8, 16, 32, 64, and 128.

Determine the value of the octet by adding the values of positions wherever there is a binary 1 present:

- If there is a 0 in a position, do not add the value.
- If all 8 bits are 0s, 00000000, the value of the octet is 0.
- If all 8 bits are 1s, 11111111, the value of the octet is 255 (128+64+32+16+8+4+2+1).
- If the 8 bits are mixed, the values are added together. For example, the octet 00100111 has a value of 39 (32+4+2+1).

So the value of each of the four octets can range from 0 to a maximum of 255.

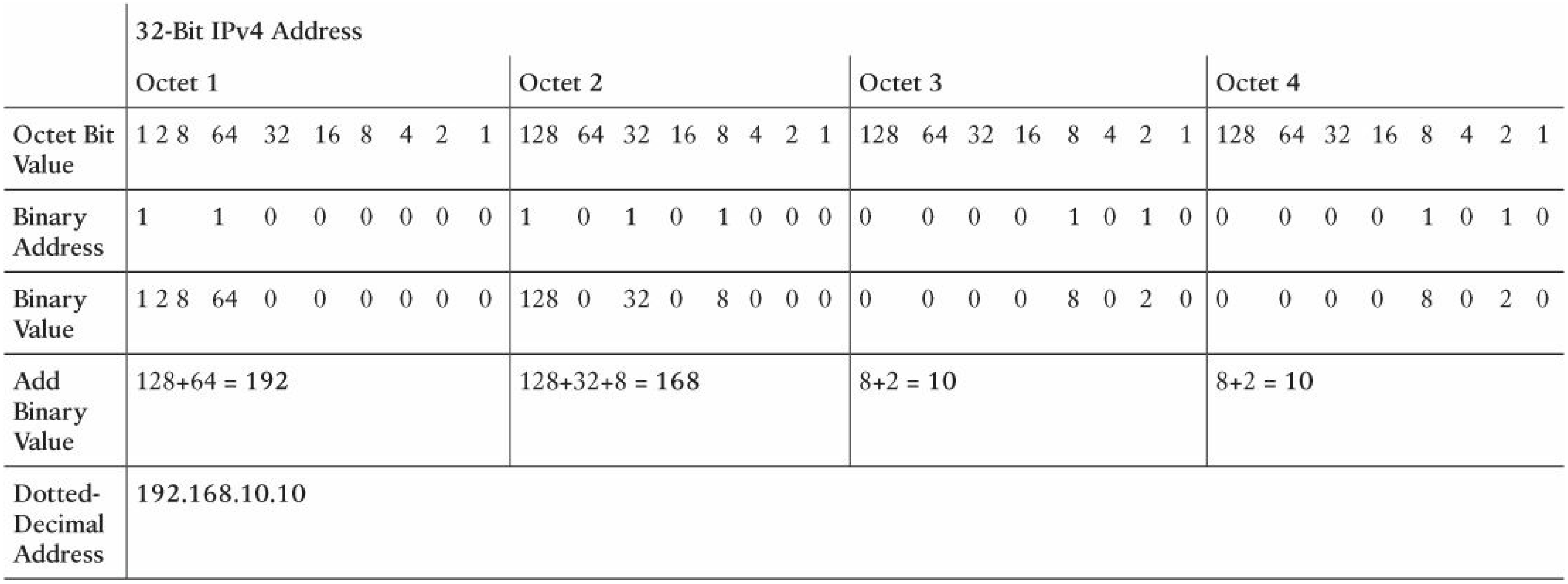
Table 8-3, shows how a binary address is converted to dotted decimal. Using the 32-bit IPv4 address 11000000101010000000101000001010, convert the binary representation to dotted decimal using the following steps:

How To

Step 1. Divide the 32 bits into 4 octets.

Step 2. Convert each octet to decimal.

Step 3. Add a “dot” between each decimal.



	32-Bit IPv4 Address			
	Octet 1	Octet 2	Octet 3	Octet 4
Octet Bit Value	1 2 8 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1
Binary Address	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 1 0 1 0	0 0 0 0 1 0 1 0
Binary Value	1 2 8 64 0 0 0 0 0 0	128 0 32 0 8 0 0 0	0 0 0 0 8 0 2 0	0 0 0 0 8 0 2 0
Add Binary Value	128+64 = 192	128+32+8 = 168	8+2 = 10	8+2 = 10
Dotted-Decimal Address	192.168.10.10			

Table 8-3 Representation of Dotted-Decimal Address

Interactive Graphic

Activity 8.1.1.4: Binary-to-Decimal Conversions

Go to the course online to perform this practice activity.

Converting from Decimal to Binary (8.1.1.5, 8.1.1.6)

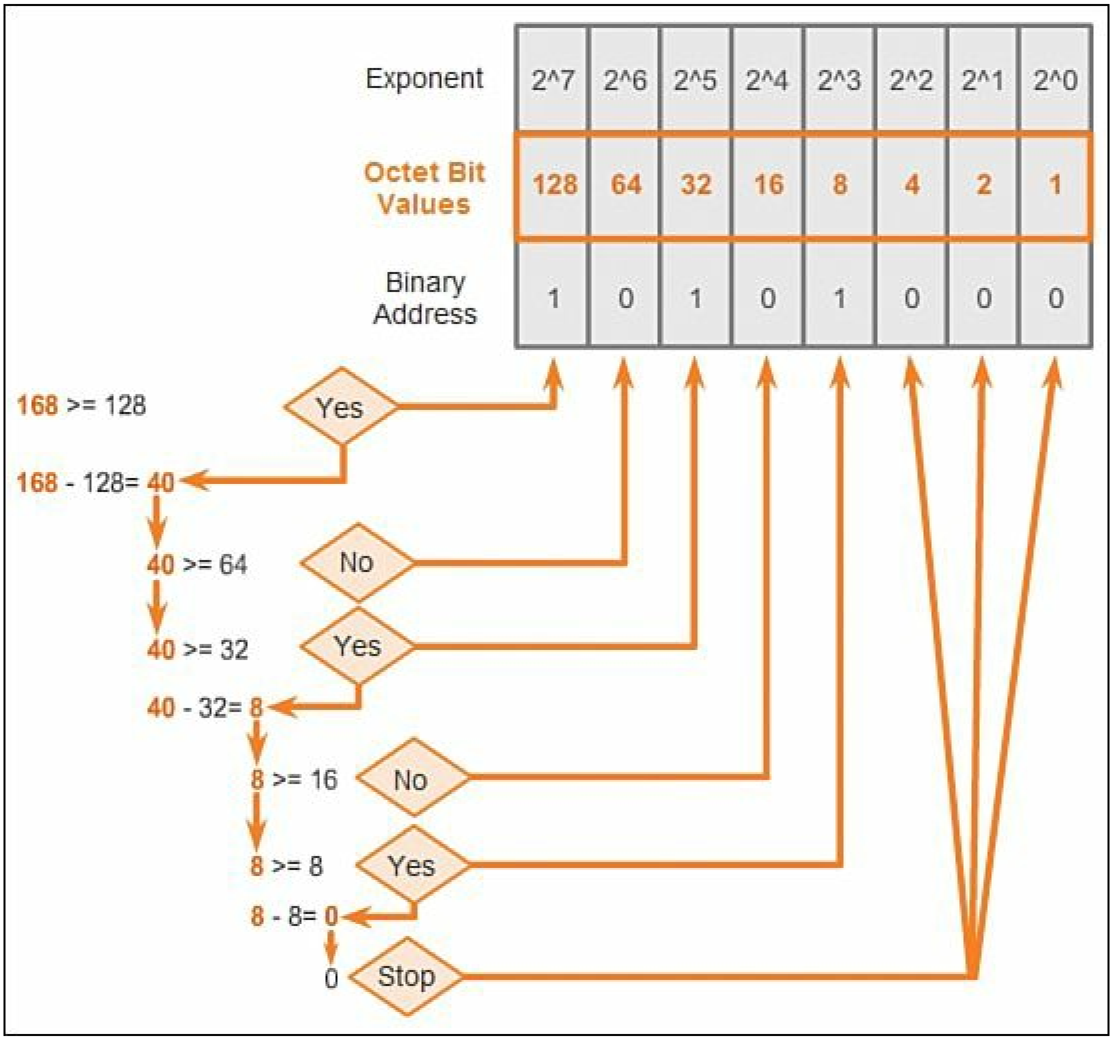
In addition to being able to convert from binary to decimal, it is also necessary to understand how to convert from decimal to binary.

Because we represent IPv4 addresses using dotted-decimal format, it is only necessary that we examine the process of converting 8-bit binary to the decimal values of 0 to 255 for each octet in an IPv4 address.

To begin the conversion process, we start by determining whether the decimal number is equal to or greater than our largest decimal value represented by the most significant bit. In the highest position, we determine whether the octet number is equal to or greater than 128. If the octet number is smaller than 128, we place a 0 in the bit position for decimal value 128 and move to the bit position for decimal value 64.

If the octet number in the bit position for decimal value 128 is larger than or equal to 128, we place a 1 in the bit position for decimal value 128 and subtract 128 from the octet number being converted. We then compare the remainder of this operation to the next smaller value, 64. We continue this process for all the remaining bit positions.

Figure 8-1 shows the process of converting 168 to the binary equivalent of 10101000.



Exponent	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Octet Bit Values	128	64	32	16	8	4	2	1
Binary Address	1	0	1	0	1	0	0	0

Figure 8-1 Decimal-to-Binary Conversion

The conversion steps shown in Figure 8-2 outline the process to convert an IP address to binary. Each octet is converted to binary and then combined. The steps for this example are

How To

Step 1. Convert 192 to binary.

Step 2. Convert 168 to binary.

Step 3. Convert 10 to binary.

Step 4. Convert 10 to binary.

Step 5. Combine the converted octets beginning with the first octet.

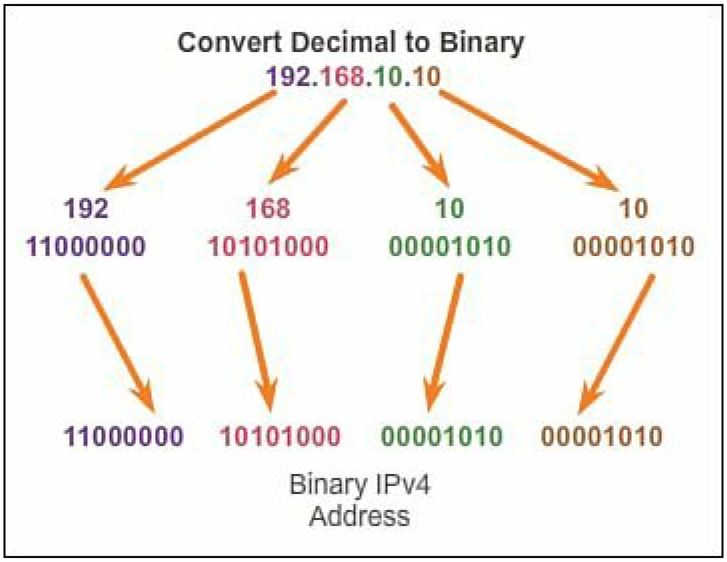


Figure 8-2 Decimal-to-Binary Conversion of IPv4 Address

Interactive Graphic **Activity 8.1.1.7: Decimal-to-Binary Conversion Activity**

Go to the course online to perform this practice activity.

Interactive Graphic **Activity 8.1.1.8: Binary Game**

Go to the course online to perform this practice activity.

IPv4 Subnet Mask (8.1.2)

This section introduces the use and structure of the subnet mask used in IPv4 addressing.

Network Portion and Host Portion of an IPv4 Address (8.1.2.1)

Understanding binary notation is important when determining whether two hosts are in the same network. Recall that an IP address is a hierarchical address that is made up of two parts: a network portion and a host portion. However, when determining the network portion versus the host portion, it is necessary to look, not at the decimal value, but at the 32-bit stream. Within the 32-bit stream, a portion of the bits makes up the IPv4 network and a portion of the bits makes up the host.

The bits within the network portion of the address must be identical for all devices that reside in the same network. The bits within the host portion of the address must be unique to identify a specific host within a network. If two hosts have the same bit pattern in the specified network portion of the 32-bit stream, those two hosts will reside in the same network.

However, how do hosts know which portion of the 32 bits is network and which is host? That is the job of the subnet mask.

When an IP host is configured, a subnet mask is assigned along with an IPv4 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.

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. As shown in Figure 8-3, the subnet mask is created by placing a binary 1 in each bit position that represents the network portion and placing a binary 0 in each bit position that represents the host portion.

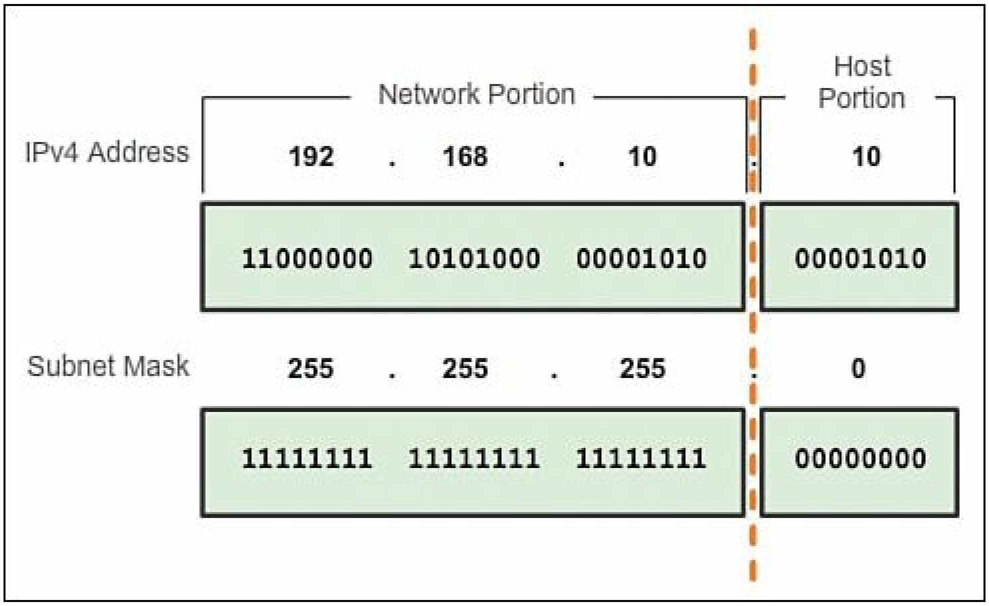


Figure 8-3 Decimal-to-Binary Conversion of IPv4 Address

Note

The subnet mask does not actually contain the network or host portion of an IPv4 address; it just tells the computer where to look for these portions in a given IPv4 address.

Similar to IPv4 addresses, the subnet mask is represented in dotted-decimal format for ease of use. The subnet mask is configured on a host device, in conjunction with the IPv4 address, and is required so that the host can determine to which network it belongs. Table 8-4 displays the valid subnet masks for an IPv4 octet as well as the number of bits used to identify both the ***network address*** and host address within a single octet.

Mask (Decimal)	Mask (Binary)	Network Bits	Host Bits
0	00000000	0	8
128	10000000	1	7
192	11000000	2	6
224	11100000	3	5
240	11110000	4	4
248	11111000	5	3
252	11111100	6	2
254	11111110	7	1
255	11111111	8	0

Table 8-4 Subnet Mask Values Within an Octet

Examining the Prefix Length (8.1.2.2)

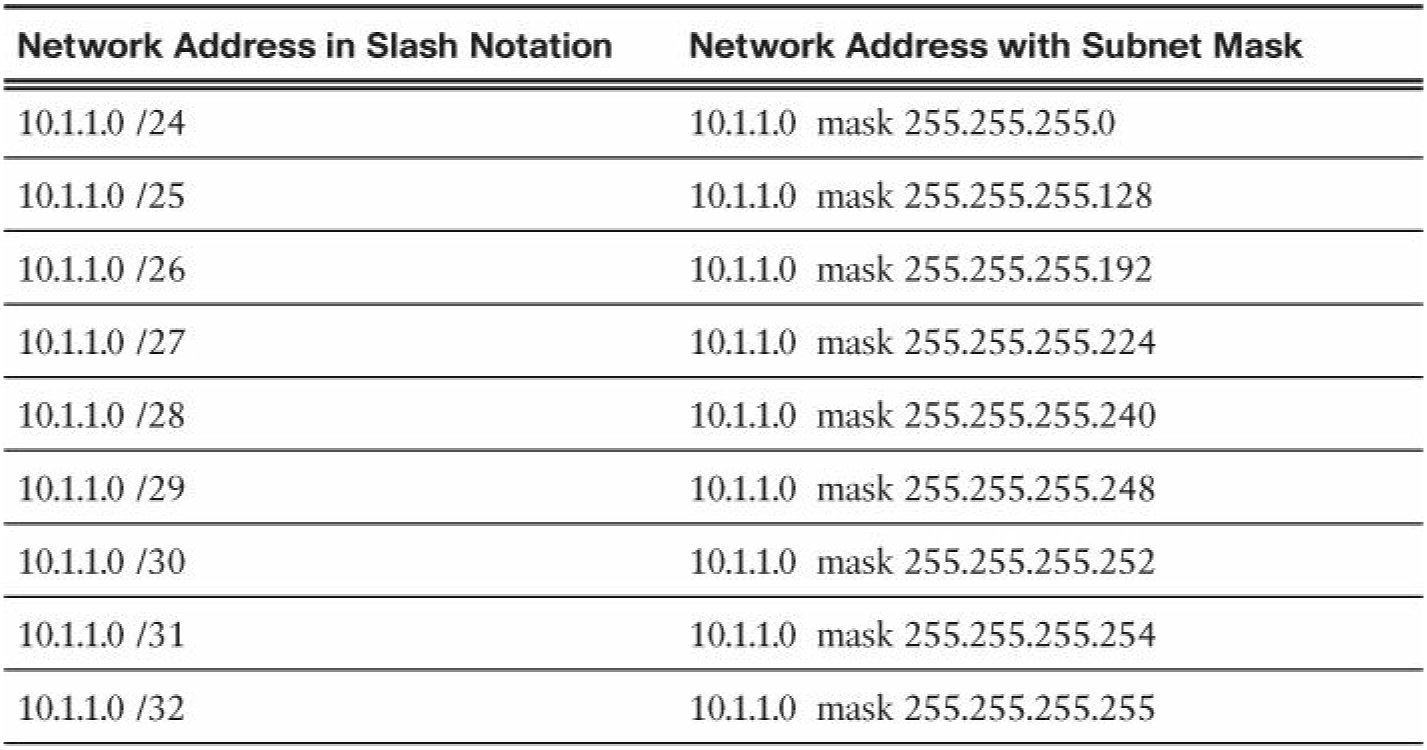
Subnet masks are often a cumbersome way of indicating the network and host portion of an IPv4 address. This section will present the use of an alternative representation.

Network Prefixes

The ***prefix length*** is another way of expressing the subnet mask. The prefix length is the number of bits set to 1 in the subnet mask. It is written in "***slash notation***," a "/" followed by the number of bits set to 1. For example, if the subnet mask is 255.255.255.0, there are 24 bits set to 1 in the binary version of the subnet mask, so the prefix length is 24 bits or /24. The prefix and the subnet mask are different ways of representing the same thing—the network portion of an address.

Networks are not always assigned a /24 prefix. Depending on the number of hosts on the network, the prefix assigned might be different. Having a different prefix number changes the host range and broadcast address for each network.

Table 8-5 illustrates different prefixes using the same 10.1.1.0 address.



Network Address in Slash Notation	Network Address with Subnet Mask
10.1.1.0 /24	10.1.1.0 mask 255.255.255.0
10.1.1.0 /25	10.1.1.0 mask 255.255.255.128
10.1.1.0 /26	10.1.1.0 mask 255.255.255.192
10.1.1.0 /27	10.1.1.0 mask 255.255.255.224
10.1.1.0 /28	10.1.1.0 mask 255.255.255.240
10.1.1.0 /29	10.1.1.0 mask 255.255.255.248
10.1.1.0 /30	10.1.1.0 mask 255.255.255.252
10.1.1.0 /31	10.1.1.0 mask 255.255.255.254
10.1.1.0 /32	10.1.1.0 mask 255.255.255.255

Table 8-5 Subnet Addresses in Slash Notation

Note

Generally, the /31 subnet mask is not used. It is only used in special configurations that are beyond the scope of this book. Additionally, 10.1.1.0 would not be a valid address with /31 or with /24 but is shown here to illustrate the slash notation.

IPv4 Network, Host, and Broadcast Addresses (8.1.2.3)

There are three types of addresses within the address range of each IPv4 network:

- Network address
- Host address

- Broadcast address

Network Address

The network address is a standard way to refer to a network. The subnet mask or the prefix length might also be used when referring to a network address. For example, the network shown in Figure 8-4 could be referred to as the 10.1.1.0 network, the 10.1.1.0 255.255.255.0 network, or the 10.1.1.0/24 network. All hosts in the 10.1.1.0/24 network will have the same network portion bits.

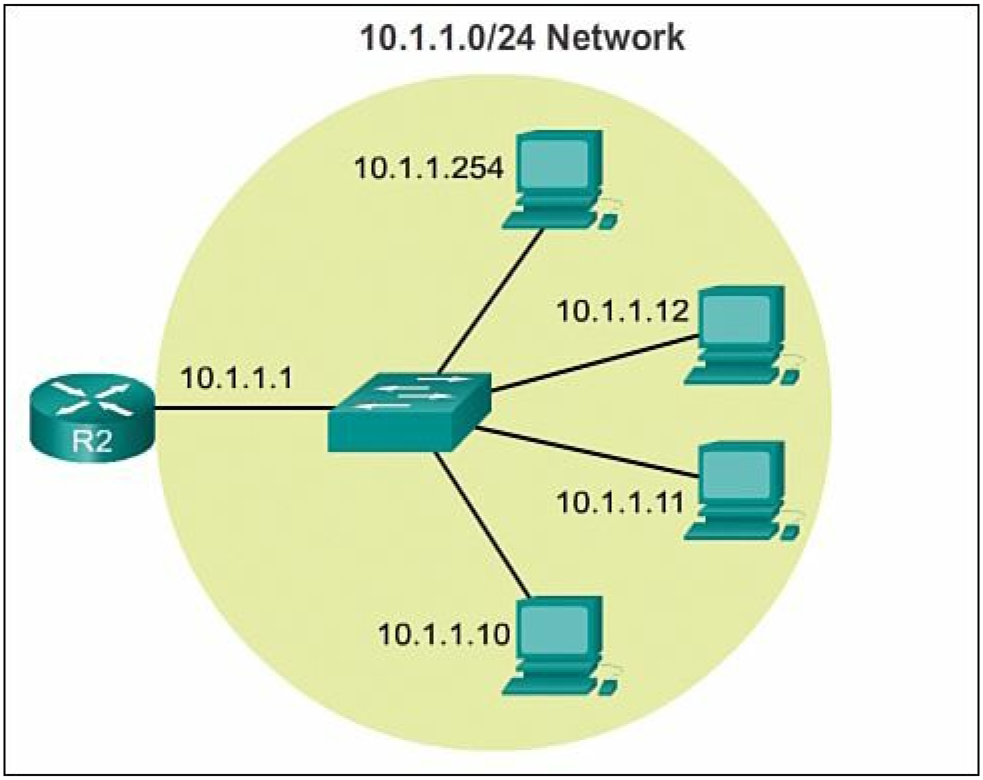


Figure 8-4 Example Network 10.1.1.0 /24

Within the IPv4 address range of a network, the first address (lowest address) is reserved for the network address. This address has a 0 for each host bit in the host portion of the address. All hosts within the network share the same network address. The network is only a reference to the network. This address is not used for communication.

Host Address

Every end device requires a unique address to communicate on the network. In IPv4 addresses, the values between the network address and the broadcast address can be assigned to end devices in a network. A host address has any combination of 0 and 1 bits in the host portion of the address but cannot contain all 0 bits or all 1 bits. In Figure 8-4, each network portion of all the hosts is 10.1.1. Each of the hosts has a unique host portion of the address of 10, 11, 12, 254, and the router interface is 1.

Broadcast Address

The IPv4 broadcast address is a special address for each network that allows communication to all the hosts in that network. To send data to all hosts in a network at once, a host can send a single packet that is addressed to the broadcast address of the network, and each host in the network that receives this packet will process its contents.

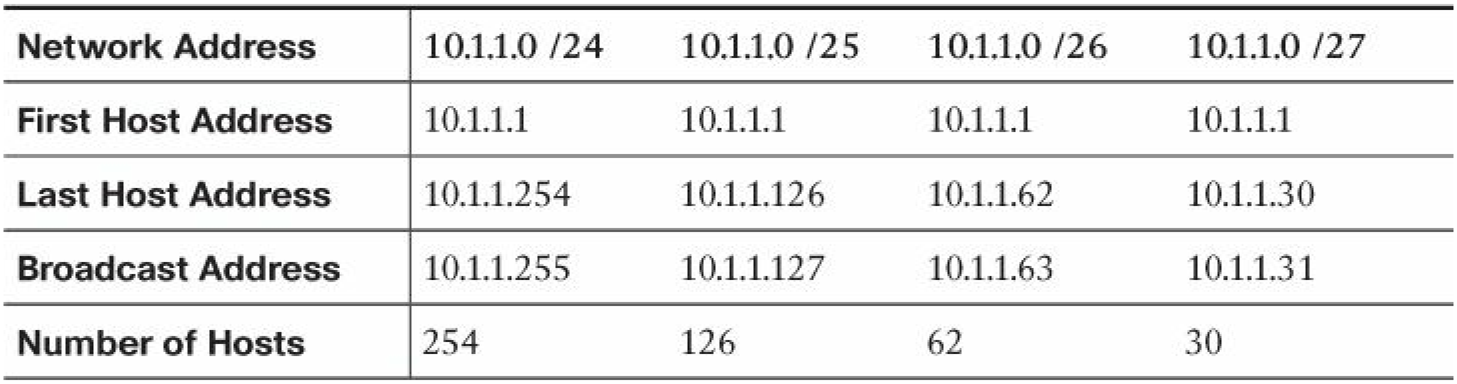
The broadcast address uses the last (highest) address in the network range. This is the address in which the bits in the host portion are all 1s. All 1s in an octet in binary form is equal to the number

255 in decimal form. For the network 10.1.1.0/24, in which the last octet is used for the host portion, the broadcast address would be 10.1.1.255.

Note

The host portion might not always be an entire octet. This address is also referred to as the directed broadcast address.

Table 8-6 shows that the network address could remain the same with different subnets. However, the host range and the broadcast address are different for the different prefix lengths. Also, the number of hosts that can be addressed on the network also changes.



Network Address	10.1.1.0 /24	10.1.1.0 /25	10.1.1.0 /26	10.1.1.0 /27
First Host Address	10.1.1.1	10.1.1.1	10.1.1.1	10.1.1.1
Last Host Address	10.1.1.254	10.1.1.126	10.1.1.62	10.1.1.30
Broadcast Address	10.1.1.255	10.1.1.127	10.1.1.63	10.1.1.31
Number of Hosts	254	126	62	30

Table 8-6 Subnet with Different Masks

First Host and Last Host Addresses (8.1.2.4)

To ensure that all hosts within a network are assigned a unique IP address within that network range, it is important to identify the first ***host address*** and the last host address. Hosts within a network can be assigned IP addresses within this range.

First Host Address

Also seen in Table 8-6, the host portion of the first host address will contain all 0 bits with a 1 bit for the lowest-order or rightmost bit. This address is always 1 greater than the network address. The first host address on the 10.1.1.0/24 network is 10.1.1.1. It is common in many addressing schemes to use the first host address for the router or default gateway address.

Last Host Address

The host portion of the last host address will contain all 1 bits with a 0 bit for the lowest-order or rightmost bit. This address is always 1 less than the ***broadcast address***. As seen in Table 8-6, the last host address on the 10.1.1.0/24 network is 10.1.1.254.

Note

Because the lowest host address in any network has a 1 in the least significant bit, all first host addresses will be odd numbers. In contrast, the last host address will a 0 in the least significant bit, So, last host addresses will be even. Similarly, network addresses are always even numbers and broadcast addresses will be odd.

Bitwise AND Operation (8.1.2.5)

When an IPv4 address is assigned to a device, that device uses the subnet mask to determine to what network address the device belongs. The network address is the address that represents all the devices on the same network.

When sending network data, the device uses this information to determine whether it can send packets locally, or whether it must send the packets to a default gateway for remote delivery. When a host sends a packet, it compares the network portion of its own IP address to the destination IP address, based on the host's subnet mask. The network portion of the addresses of the source and destination IPv4 addresses are determined based on a logical AND of the subnet mask with each of these addresses. If the network bits of the source and destination 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 default gateway to be sent on to the other network.

The AND Operation

ANDing is one of three basic binary operations used in digital logic. The other two are OR and NOT. While all three are used in data networks, AND is used in determining the network address. Therefore, our discussion here will be limited to ***logical AND***. Logical AND is the comparison of two bits that yields the following results:

1 AND 1 = 1

0 AND 1 = 0

0 AND 0 = 0

1 AND 0 = 0

The IPv4 host address is logically ANDed, bit by bit, with its subnet mask to determine the network address to which the host is associated. When this bitwise ANDing between the address and the subnet mask is performed, the result yields the network address.

Importance of ANDing (8.1.2.6)

Any address bit ANDed with a 1 bit value from the subnet mask will yield the original bit value from the address. So, a 0 (from the IPv4 address) AND 1 (from the subnet mask) is 0. 1 (from the IPv4 address) AND 1 (from the subnet mask) is 1. Consequently, anything ANDed with a 0 yields a 0. These properties of ANDing are used with the subnet mask to "mask" the host bits of an IPv4 address. Each bit of the address is ANDed with the corresponding bit of the subnet mask.

Because all the bits of the subnet mask that represent host bits are 0s, the host portion of the resulting network address becomes all 0s. Recall that an IPv4 address with all 0s in the host portion represents the network address.

Likewise, all the bits of the subnet mask that indicate the network portion are 1s. When each of these 1s is ANDed with the corresponding bit of the address, the resulting bits are identical to the original address bits.

As shown in Table 8-7, the 1 bits in the subnet mask will result in the network portion of the network address having the same bits as the network portion of the host. The host portion of the network address will result in all 0s.

	Dotted Decimal				Binary Octets			
Host	192	168	10	10	11000000	10101000	00001010	00001010
Mask	255	255	255	0	11111111	11111111	11111111	00000000
AND								
Network	192	168	10	0	11000000	10101000	00001010	00000000

Table 8-7 Logical AND to Determine Subnet

For a given IP address and its subnet mask, ANDing can be used to determine what subnetwork the address belongs to, as well as what other addresses belong to the same subnet. Remember that if two addresses are in the same network or subnetwork, they are considered to be local to each other and can therefore communicate directly with each other. Addresses that are not in the same network or subnetwork are considered to be remote to each other and must therefore have a Layer 3 device (like a router or Layer 3 switch) between them to communicate.

In network verification/troubleshooting, we often need to determine whether two hosts are on the same local network. We need to make this determination from the perspective of the network devices. Because of improper configuration, a host might see itself on a network that was not the intended one. This can create an operation that seems erratic unless diagnosed by examining the ANDing processes used by the host.

Lab 8.1.2.7: Using the Windows Calculator with Network Addresses

In this lab, you will complete the following objectives:

- Part 1: Access the Windows Calculator
- Part 2: Convert Between Numbering Systems
- Part 3: Convert Host IPv4 Addresses and Subnet Masks into Binary
- Part 4: Determine the Number of Hosts in a Network Using Powers of 2
- Part 5: Convert MAC Addresses and IPv6 Addresses to Binary

Lab 8.1.2.8: Converting IPv4 Addresses to Binary

In this lab, you will complete the following objectives:

- Part 1: Convert IPv4 Addresses from Dotted Decimal to Binary
- Part 2: Use Bitwise ANDing Operation to Determine Network Addresses
- Part 3: Apply Network Address Calculations

Activity 8.1.2.9: ANDing to Determine the Network Address

Go to the course online to perform this practice activity.

IPv4 Unicast, Broadcast, and Multicast (8.1.3)

In data networks, communication can take place as either unicast, broadcast, or multicast. This section will discuss these three methods of communication in IPv4.

Assigning a Static IPv4 Address to a Host (8.1.3.1)

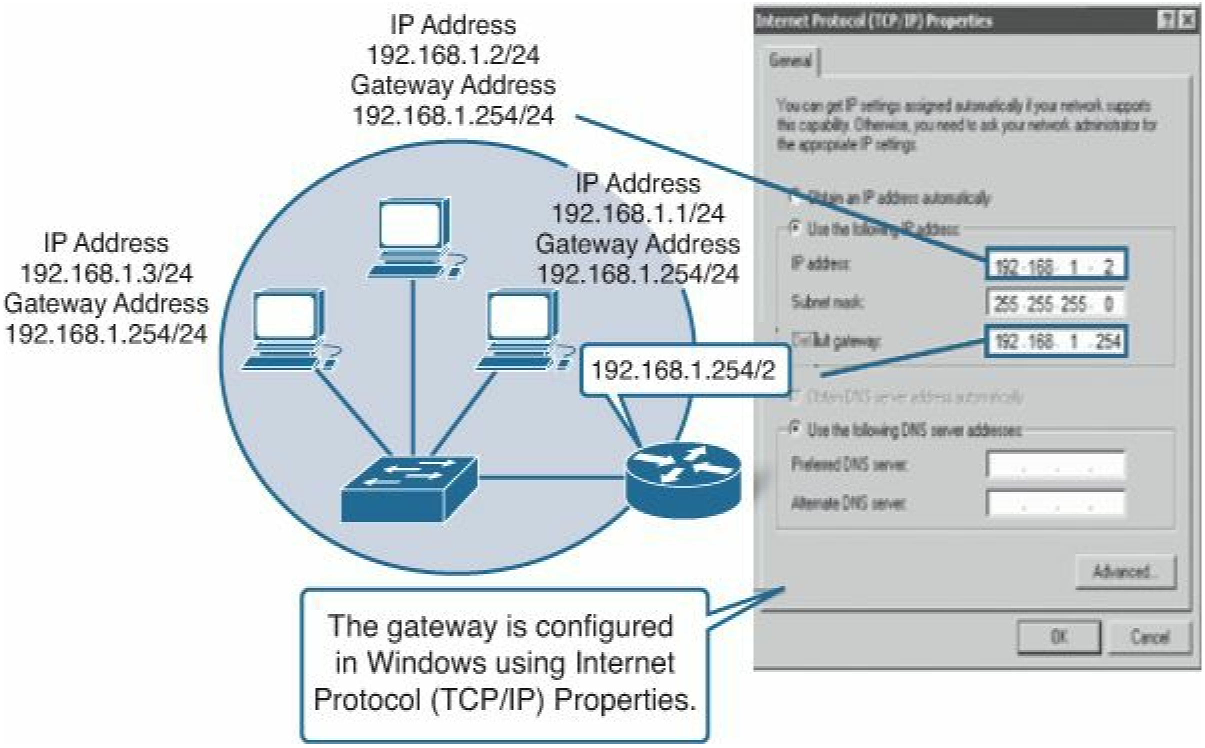
For a host to participate in IPv4 unicast, multicast, or broadcast, the host must first have IPv4 addressing configured. This section will introduce static IPv4 host configuration.

Addresses for User Devices

In most data networks, the largest population of hosts includes the end devices such as PCs, tablets, smartphones, printers, and IP phones. Because this represents the largest number of devices within a network, the largest number of addresses should be allocated to these hosts. These hosts are assigned IP addresses from the range of available addresses in the network. These IP addresses can be assigned either statically or dynamically.

Static Assignment

With a static assignment, the network administrator must manually configure the network information for a host. To configure a static IPv4 address, choose IPv4 on the network adapter screen and then key in the static address, subnet mask, and default gateway. Figure 8-5 shows the minimum static configuration: the host IP address, subnet mask, and default gateway.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 254

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

The gateway is configured in Windows using Internet Protocol (TCP/IP) Properties.

Figure 8-5 Configuring IPv4 Addressing on Windows Host

There are several advantages to static addressing. For example, it is useful for printers, servers, and other networking devices that do not change location often and need to be accessible to clients on the network based on a fixed IP address. If hosts normally access a server at a particular IP address, it would cause problems if that address changed. Additionally, static assignment of addressing information can provide increased control of network resources. For example, it is possible to create access filters based on traffic to and from a specific IP address. However, static addressing can be time-consuming to enter on each host.

When using static IP addressing, it is necessary to maintain an accurate list of the IP address assigned to each device. Assigning duplicate addresses within a network can create communication problems.

Assigning a Dynamic IPv4 Address to a Host (8.1.3.2)

This section will introduce dynamic IPv4 host configuration.

Dynamic Assignment

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 or other network devices, such as smartphones, that need to be connected. Rather than have the network administrator assign IP addresses for each workstation, it is easier to have IP addresses assigned automatically. This is done using a protocol known as Dynamic Host Configuration Protocol (DHCP).

DHCP enables the automatic assignment of addressing information such as IP address, subnet mask, default gateway, and other configuration information. The configuration of the DHCP server requires that a block of addresses, called an address pool, is used for assigning to the DHCP clients on a network. Addresses assigned to this pool should be planned so that they exclude any static addresses used by other devices.

DHCP is generally the preferred method of assigning IPv4 addresses to hosts on large networks because it reduces the burden on network support staff and virtually eliminates entry errors.

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 for mobile users that come and go on a network.

If DCHP is enabled on a host device, the **ipconfig** command can be used to view the IP address information assigned by the DHCP server, as shown in Example 8-3.

Example 8-3 Confirming the IP Address and Gateway Route

Click here to view code image

```
C:\> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . . .: 192.168.254.11
   Subnet Mask . . . . . . .  . . . . . : 255.255.255.0
     Default Gateway  . . . . . . . . . : 192.168.254.1
```

Unicast Transmission (8.1.3.3)

In an IPv4 network, the hosts can communicate one of three ways:

- **Unicast:** The process of sending a packet from one host to an individual host

- **Broadcast:** The process of sending a packet from one host to all hosts in the network
- **Multicast:** The process of sending a packet from one host to a selected group of hosts, possibly in different networks

These three types of communication are used for different purposes in data networks. In all three cases, the IPv4 address of the originating host is placed in the packet header as the source address.

Unicast Traffic

Unicast communication is used for normal host-to-host communication in both a client/server and a peer-to-peer network. Unicast packets use the address of the destination device as the destination address and can be routed through an internetwork. In Figure 8-6, host 172.16.4.1 is communicating with the host (printer) at 172.16.4.253 as a unicast communication.

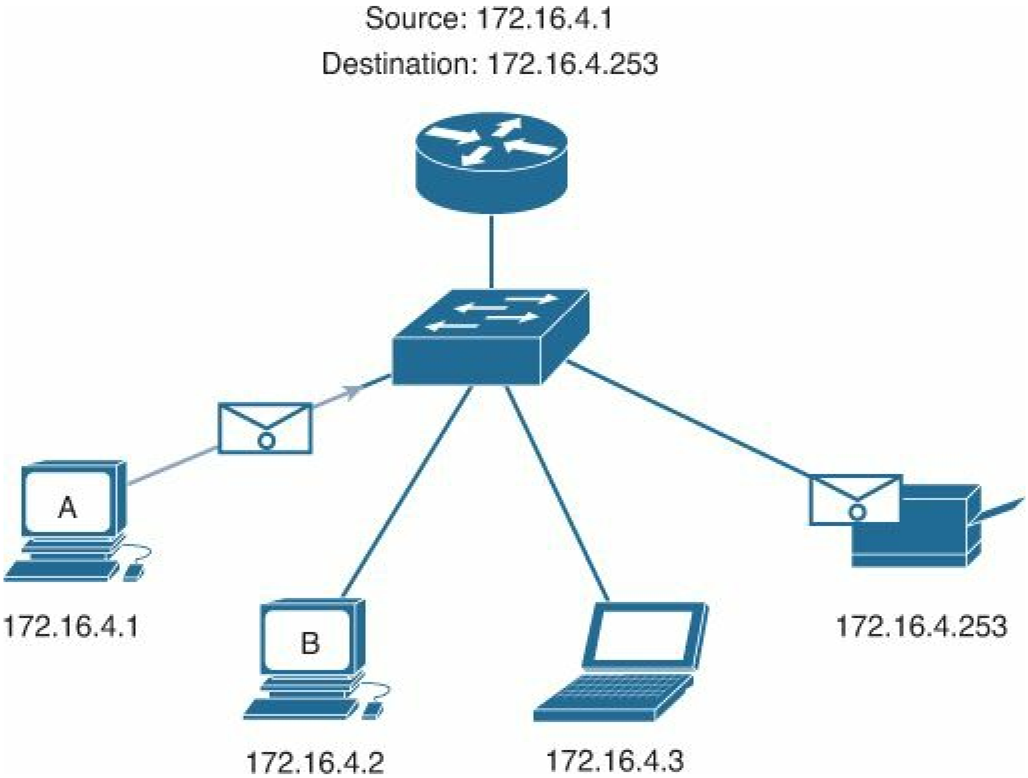


Figure 8-6 Unicast Communication

In an IPv4 network, the unicast address applied to an end device is referred to as the host address. For unicast communication, the addresses assigned to the two end devices are used as the source and destination IPv4 addresses. During the encapsulation process, the source host places its IPv4 address in the unicast packet header as the source address and the IPv4 address of the destination host in the packet header as the destination address. The source address of any packet is always the unicast address of the originating host.

Note

In this course, all communication between devices is unicast communication unless otherwise noted.

IPv4 addresses are unicast addresses and are in the address range of 0.0.0.0 to 223.255.255.255. However, within this range are many addresses that are reserved for special purposes. These special purpose addresses will be discussed later in this chapter.

Broadcast Transmission (8.1.3.4)

This section will introduce different types of IPv4 broadcast.

Broadcast Transmission

Broadcast traffic is used to send packets to all hosts in the network using the broadcast address for the network. With a broadcast, the packet contains a destination IP address with all 1s in the host portion. This means that all hosts on that local network (broadcast domain) will receive and look at the packet. Many network protocols, such as DHCP, use broadcasts. When a host receives a packet sent to the network broadcast address, the host processes the packet as it would a packet addressed to its unicast address.

Some examples for using broadcast transmission are

- Mapping upper-layer addresses to lower-layer addresses.
- Requesting an address.
- Unlike unicast, where the packets can be routed throughout the internetwork, broadcast packets are usually restricted to the local network. This restriction is dependent on the configuration of the gateway router and the type of broadcast. There are two types of broadcasts: ***directed broadcast*** and ***limited broadcast***.

Directed Broadcast

A directed broadcast is sent to all hosts on a specific network. This type of broadcast is useful for sending a broadcast to all hosts on a nonlocal network. For example, for a host outside of the 172.16.4.0/24 network to communicate with all the hosts within that network, the destination address of the packet would be 172.16.4.255. With a default configuration, Cisco does not forward directed broadcasts. However, they can be configured to do so.

Limited Broadcast

These packets always use a destination IPv4 address 255.255.255.255. Routers do not forward a limited broadcast. For this reason, an IPv4 network is also referred to as a broadcast domain. Routers form the boundary for a broadcast domain.

As an example, a host within the 172.16.4.0/24 network would broadcast to all hosts in its network using a packet with a destination address of 255.255.255.255. This type of communication is shown in Figure 8-7, where host 172.16.4.1 is communicating to all the hosts in the network using broadcast.

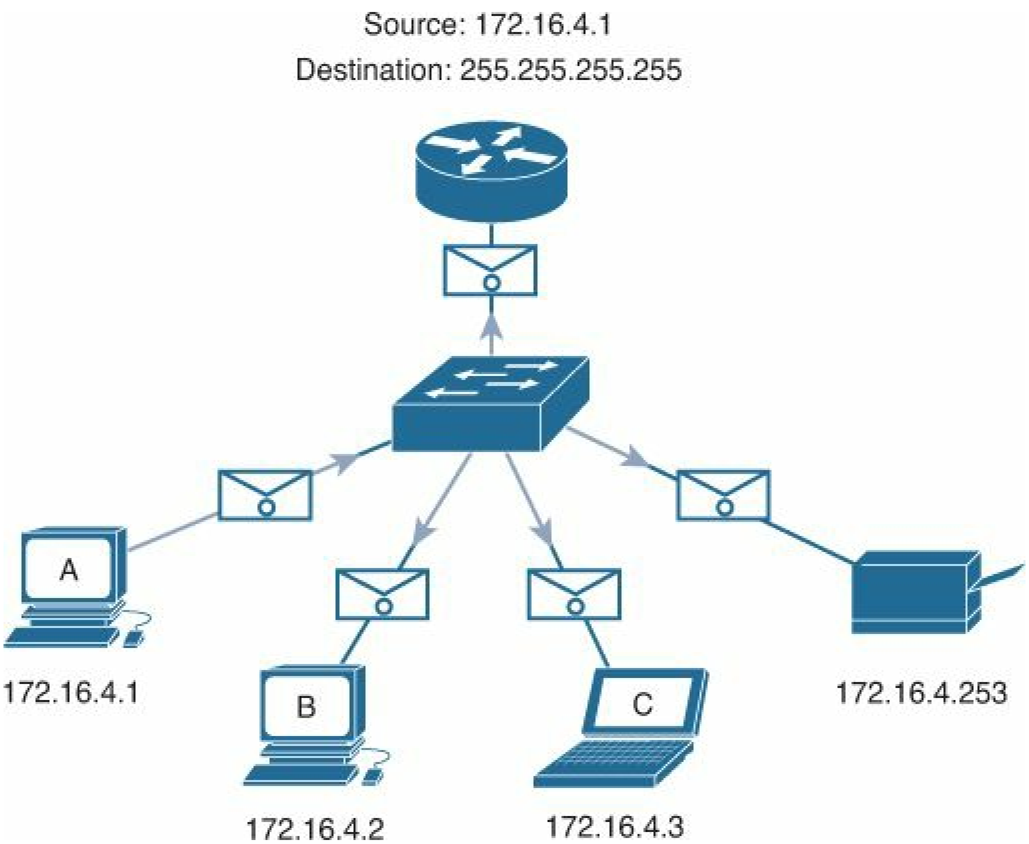


Figure 8-7 Broadcast Communication

When a packet is broadcast, it uses resources on the network and causes every receiving host on the network to process the packet. Therefore, broadcast traffic should be limited so that it does not adversely affect performance of the network or devices. Because routers separate broadcast domains, subdividing networks with excessive broadcast traffic can improve network performance.

Multicast Transmission (8.1.3.5)

This section presents IPv4 multicast addressing and communication.

Multicast Transmission

Multicast transmission is designed to conserve the bandwidth of an IPv4 network. It reduces traffic by allowing a host to send a single packet to a selected set of hosts that are part of a subscribing multicast group. To reach multiple destination hosts using unicast communication, a source host would need to send an individual packet addressed to each host. With multicast, the source host can send a single packet that can reach thousands of destination hosts. The internetwork’s responsibility is to replicate the multicast flows in an efficient manner so that they reach only their intended recipients.

Some examples of multicast transmission are

- Video and audio broadcasts
- Routing information exchange by routing protocols
- Distribution of software
- Remote gaming

Multicast Addresses

IPv4 has a block of addresses reserved for addressing multicast groups. This address range is 224.0.0.0 to 239.255.255.255. The multicast address range is subdivided into different types of addresses: reserved link-local addresses and globally scoped addresses. One additional type of multicast address is the administratively scoped address, also called the limited scope address.

The IPv4 multicast addresses 224.0.0.0 to 224.0.0.255 are reserved link-local addresses. These addresses are to be used for multicast groups on a local network. A router connected to the local network recognizes that these packets are addressed to a link-local multicast group and never forwards them farther. A typical use of reserved link-local addresses is in routing protocols using multicast transmission to exchange routing information.

The globally scoped addresses are 224.0.1.0 to 238.255.255.255. They can be used to multicast data across the Internet. For example, 224.0.1.1 has been reserved for the Network Time Protocol (NTP) to synchronize the time-of-day clocks of network devices.

Multicast Clients

Hosts that receive particular multicast data are called ***multicast clients***. The multicast clients use services requested by a client program to subscribe to the multicast group.

Each multicast group is represented by a single IPv4 multicast destination address. When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address, as well as packets addressed to its uniquely allocated unicast address.

In the multicast communication shown in Figure 8-8, the source host A, with the address 172.16.4.1, creates a single packet addressed to the multicast address 224.10.10.5. In this example, host C and host D have an application or service running that subscribes to this multicast group. When a copy of this packet arrives, these devices will process the packet.

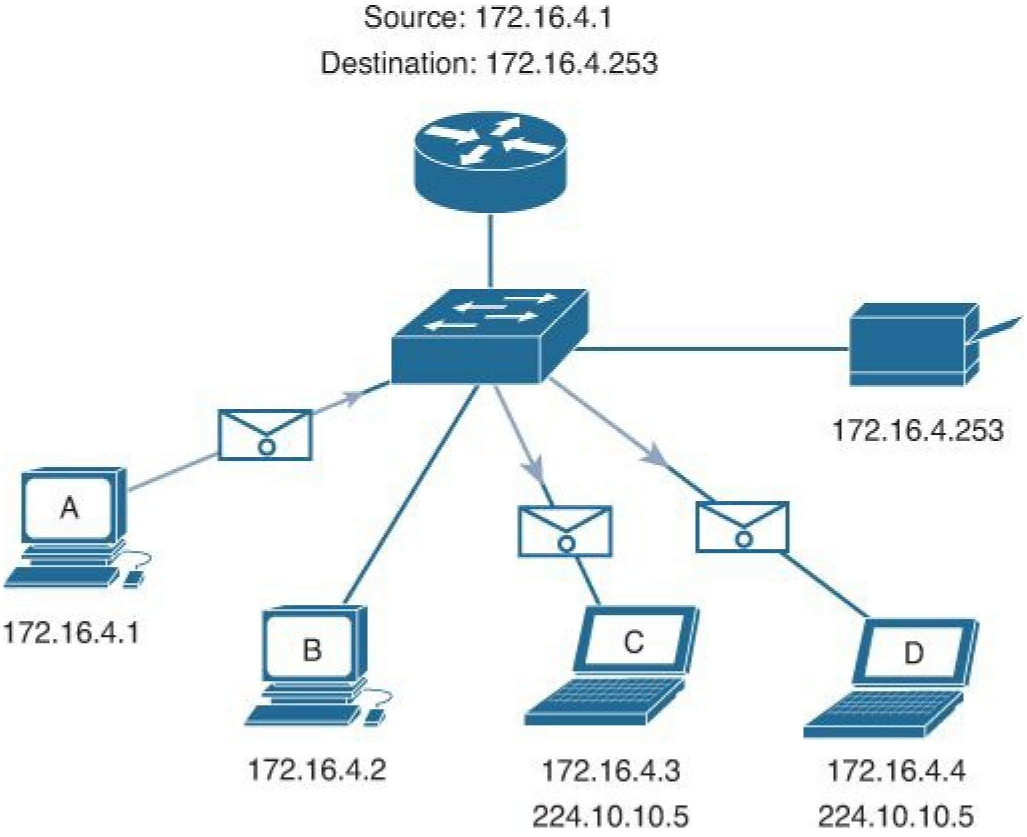


Figure 8-8 Multicast Communication

Interactive Graphic

Activity 8.1.3.6: Unicast, Broadcast, or Multicast

Go to the course online to perform this practice activity.

Interactive Graphic

Activity 8.1.3.7: Calculate the Network, Broadcast, and Host Addresses

Go to the course online to perform this practice activity.

Packet Tracer ☐ Activity

Packet Tracer Activity 8.1.3.8: Investigate Unicast, Broadcast, and Multicast Traffic

This activity will examine unicast, broadcast, and multicast behavior. Most traffic in a network is unicast. When a PC sends an ICMP echo request to a remote router, the source address in the IP packet header is the IP address of the sending PC. The destination address in the IP packet header is the IP address of the interface on the remote router. The packet is sent only to the intended destination.

Using the **ping** command or the Add Complex PDU feature of Packet Tracer, you can directly ping broadcast addresses to view broadcast traffic.

For multicast traffic, you will view Enhanced Interior Gateway Routing Protocol (EIGRP) traffic. EIGRP is used by Cisco routers to exchange routing information between routers. Routers using EIGRP send packets to multicast address 224.0.0.10, which represents the group of EIGRP routers. Although these packets are received by other devices, they are dropped at Layer 3 by all devices except EIGRP routers, with no other processing required.

Types of IPv4 Addresses (8.1.4)

This section will introduce the different types and uses of IPv4 addresses.

Public and Private IPv4 Addresses (8.1.4.1)

Although most IPv4 host addresses are ***public addresses*** designated for use in networks that are accessible on the Internet, there are blocks of addresses that are used in networks that require limited or no Internet access. These addresses are called ***private addresses***.

Private Addresses

The private address blocks are

10.0.0.0 to 10.255.255.255 (10.0.0.0/8)

172.16.0.0 to 172.31.255.255 (172.16.0.0/12)

192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

Private addresses are defined in RFC 1918, Address Allocation for Private Internets, and are sometimes referred to as RFC 1918 addresses. Private space address blocks are used in private networks. Hosts that do not require access to the Internet can use private addresses. However, within the private network, hosts still require unique IP addresses within the private space.

Hosts in different networks can use the same private space addresses. Packets using these addresses as the source or destination should not appear on the public Internet. The router or firewall device at the perimeter of these private networks must block or translate these addresses. Even if these packets were to make their way to the Internet, the routers would not have routes to forward them to the appropriate private network.

In RFC 6598, the Internet Assigned Numbers Authority (IANA) reserved another group of addresses known as shared address space. Similar to RFC 1918 private address space, shared address space addresses are not globally routable. However, these addresses are intended only for use in service provider networks. The shared address block is 100.64.0.0/10.

Public Addresses

The vast majority of the addresses in the IPv4 unicast host range are public addresses. These addresses are designed to be used in the hosts that are publicly accessible from the Internet. Even within these IPv4 address blocks, there are many addresses that are designated for other special purposes.

Interactive Graphic

Activity 8.1.4.2: Pass or Block IPv4 Addresses

Go to the course online to perform this practice activity.

Special-Use IPv4 Addresses (8.1.4.3)

There are certain addresses that cannot be assigned to hosts. There are also special addresses that can be assigned to hosts, but with restrictions on how those hosts can interact within the network.

Network and Broadcast Addresses

As explained earlier, within each network, the first and last addresses cannot be assigned to hosts. These are the network address and the broadcast address, respectively.

Loopback

One such reserved address is the IPv4 loopback address 127.0.0.1. The loopback is a special address that hosts use to direct traffic to themselves. The loopback address creates a shortcut method for TCP/IP applications and services that run on the same device to communicate with one another. By using the loopback address instead of the assigned IPv4 host address, two services on the same host can bypass the lower layers of the TCP/IP stack. You can also ping the loopback address to test the configuration of TCP/IP on the local host.

Although only the single 127.0.0.1 address is used, addresses 127.0.0.0 to 127.255.255.255 are reserved. Any address within this block will loop back to the local host. No address within this block should ever appear on any network.

Link-Local Addresses

IPv4 addresses in the address block 169.254.0.0 to 169.254.255.255 (169.254.0.0/16) are designated as ***link-local addresses***. These addresses can be automatically assigned to the local host by the operating system in environments where no IP configuration is available. These might be used in a small peer-to-peer network or for a host that could not automatically obtain an address from a DHCP server.

Communication using IPv4 link-local addresses is only suitable for communication with other devices connected to the same network. A host must not send a packet with an IPv4 link-local destination address to any router for forwarding and should set the IPv4 time to live (TTL) for these packets to 1.

Link-local addresses do not provide services outside of the local network. However, many client/server and peer-to-peer applications will work properly with IPv4 link-local addresses.

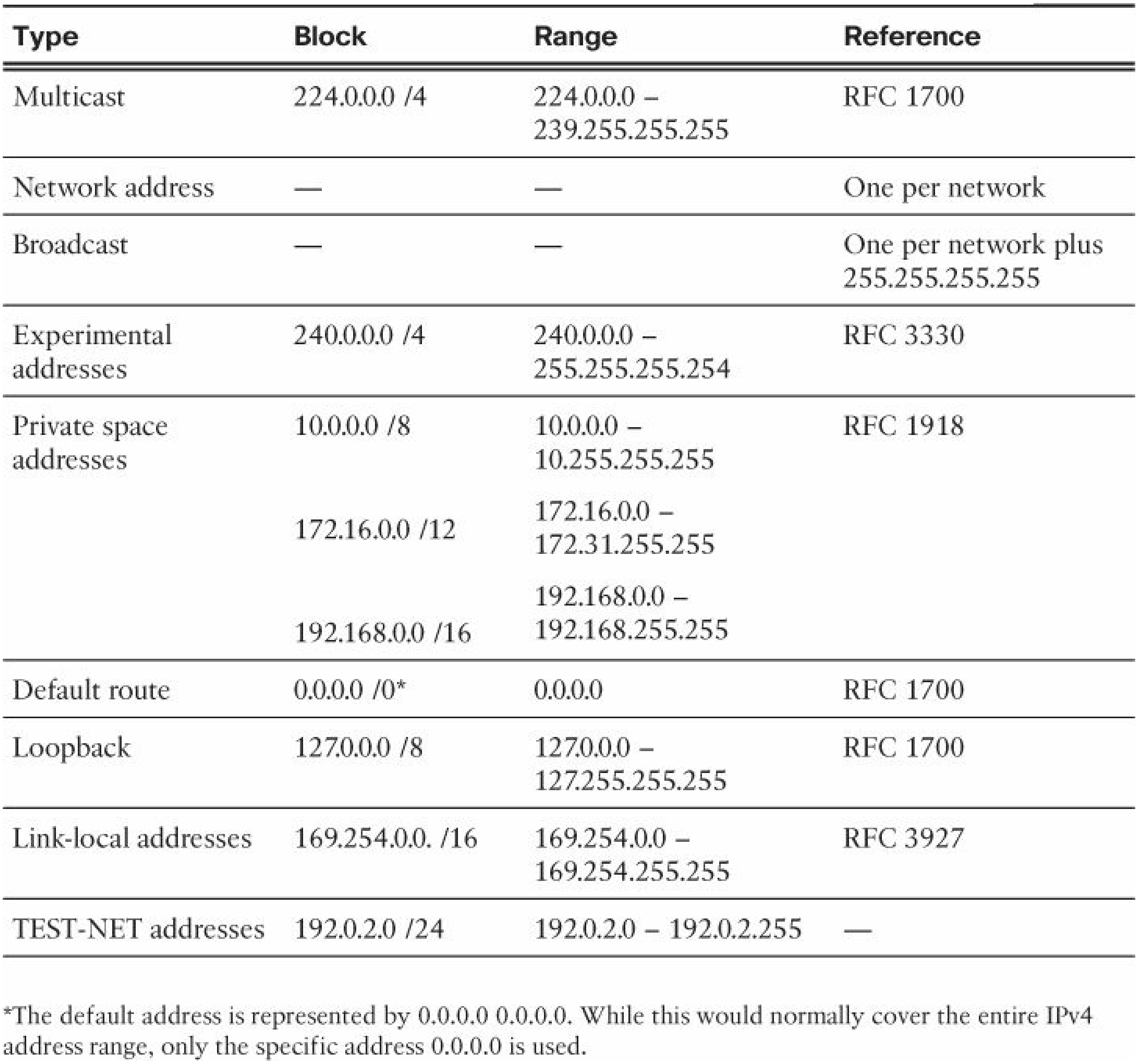
TEST-NET Addresses

The address block 192.0.2.0 to 192.0.2.255 (192.0.2.0/24) is set aside for teaching and learning purposes. These ***TEST-NET addresses*** can be used in documentation and network examples. Unlike the experimental addresses, network devices will accept these addresses in their configurations. You can often find these addresses used with the domain names example.com or example.net in RFCs and vendor and protocol documentation. Addresses within this block should not appear on the Internet.

Experimental Addresses

The addresses in the block 240.0.0.0 to 255.255.255.254 are listed as reserved for future use (RFC 3330). Currently, these addresses can only be used for research or experimentation purposes, but cannot be used in an IPv4 network. Though, according to RFC 3330, they could, technically, be converted to usable addresses in the future.

Table 8-8 is a summary of the reserved and special-purpose IPv4 addresses presented in this section. These do not represent all the special address blocks used in IPv4 networks. Additionally, the status of these blocks can be changed. You should consult the RFCs for any changes.



Type	Block	Range	Reference
Multicast	224.0.0.0 /4	224.0.0.0 – 239.255.255.255	RFC 1700
Network address	—	—	One per network
Broadcast	—	—	One per network plus 255.255.255.255
Experimental addresses	240.0.0.0 /4	240.0.0.0 – 255.255.255.254	RFC 3330
Private space addresses	10.0.0.0 /8	10.0.0.0 – 10.255.255.255	RFC 1918
	172.16.0.0 /12	172.16.0.0 – 172.31.255.255	
	192.168.0.0 /16	192.168.0.0 – 192.168.255.255	
Default route	0.0.0.0 /0*	0.0.0.0	RFC 1700
Loopback	127.0.0.0 /8	127.0.0.0 – 127.255.255.255	RFC 1700
Link-local addresses	169.254.0.0. /16	169.254.0.0 – 169.254.255.255	RFC 3927
TEST-NET addresses	192.0.2.0 /24	192.0.2.0 – 192.0.2.255	—

*The default address is represented by 0.0.0.0 0.0.0.0. While this would normally cover the entire IPv4 address range, only the specific address 0.0.0.0 is used.

Table 8-8 Major Reserved and Special-Purpose IPv4 Addresses

Legacy Classful Addressing (8.1.4.4)

Historically, RFC 1700, Assigned Numbers, grouped the unicast ranges into specific sizes called class A, class B, and class C addresses. It also defined class D (multicast) and class E (experimental) addresses, as previously presented. The unicast address classes A, B, and C defined specifically sized networks and specific address blocks for these networks. A company or organization was assigned an entire network from a class A, class B, or class C address block. This use of address space is referred to as ***classful addressing***.

Class A Blocks

A class A address block was designed to support extremely large networks with more than 16 million host addresses. Class A IPv4 addresses used a fixed /8 prefix with the first octet to indicate the network address. The remaining three octets were used for host addresses. All class A addresses required that the most significant bit of the high-order octet be a 0. This meant that there were only 128 possible class A networks, 0.0.0.0/8 to 127.0.0.0/8. Even though the class A addresses reserved one-half of the address space, because of their limit of 128 networks, they could only be allocated to approximately 120 companies or organizations.

Class B Blocks

Class B address space was designed to support the needs of moderate- to large-size networks with up to approximately 65,000 hosts. A class B IP address used the two high-order octets to indicate the network address. The other two octets specified host addresses. As with class A, address space for the remaining address classes needed to be reserved. For class B addresses, the most significant 2 bits of the high-order octet were 10. This restricted the address block for class B to 128.0.0.0/16 to 191.255.0.0/16. Class B had slightly more efficient allocation of addresses than class A because it equally divided 25 percent of the total IPv4 address space among approximately 16,000 networks.

Class C Blocks

The class C address space was the most commonly available of the historic address classes. This address space was intended to provide addresses for small networks with a maximum of 254 hosts. Class C address blocks used a /24 prefix. This meant that a class C network used only the last octet as host addresses with the three high-order octets used to indicate the network address. Class C address blocks set aside address space by using a fixed value of 110 for the 3 most significant bits of the high-order octet. This restricted the address block for class C from 192.0.0.0/24 to 223.255.255.0/24. Although it occupied only 12.5 percent of the total IPv4 address space, it could provide addresses to 2 million networks.

Limits to the Class-Based System

Not all organizations' requirements fit well into one of these three classes. Classful allocation of address space often wasted many addresses, which exhausted the availability of IPv4 addresses. For example, a company that had a network with 260 hosts would need to be given a class B address with more than 65,000 addresses.

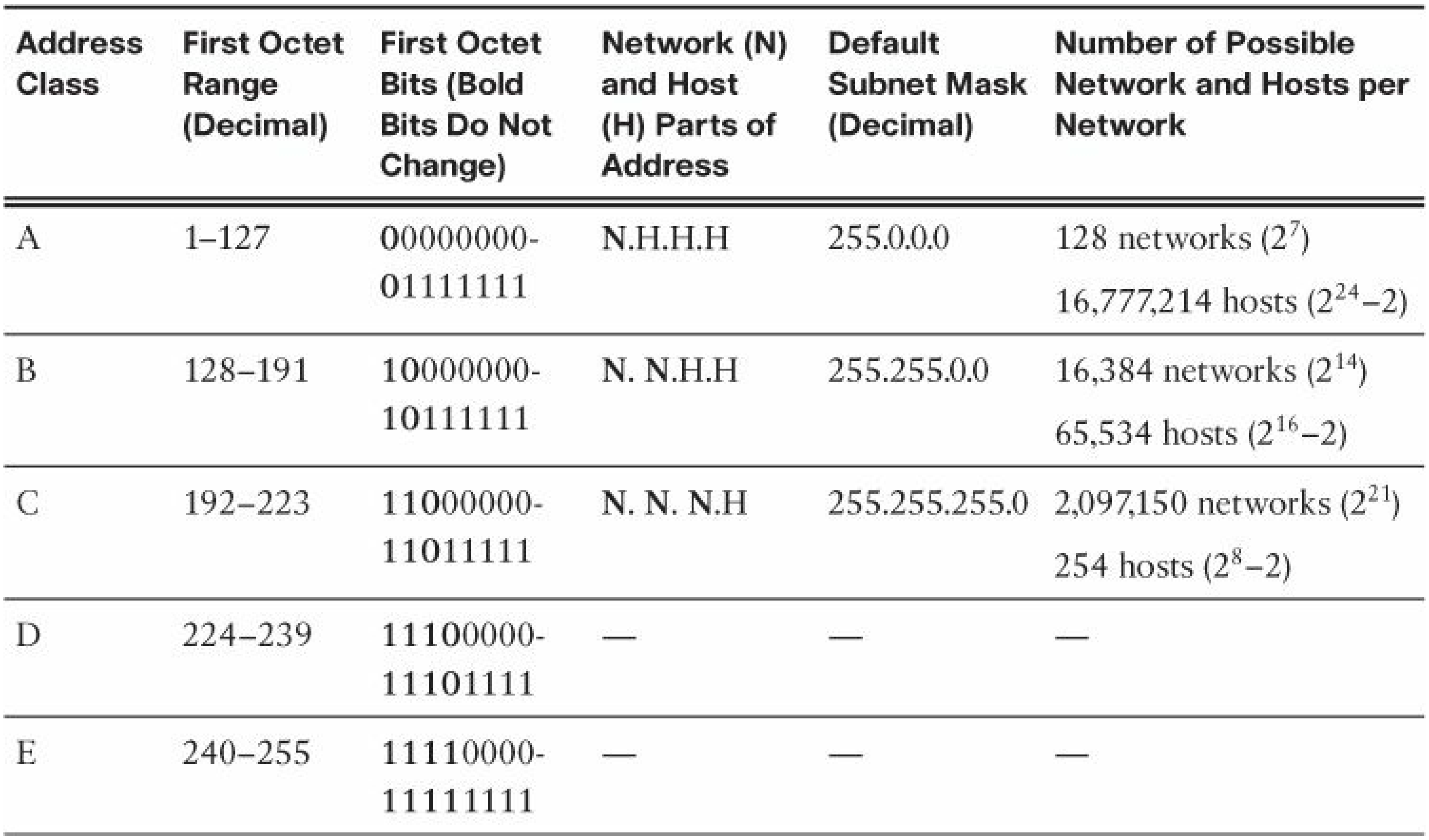
Even though this classful system was all but abandoned in the late 1990s, you will see remnants of it in networks today. For example, when you assign an IPv4 address to a computer, the operating system examines the address being assigned to determine whether this address is a class A, class B, or class C. The operating system then assumes the prefix used by that class and makes the default subnet mask assignment.

Classless Addressing

The system in use today is referred to as ***classless addressing***. The formal name is Classless Inter-Domain Routing (CIDR, pronounced "cider"). The classful allocation of IPv4 addresses was very inefficient, allowing only /8, /16, or /24 prefix lengths, each from a separate address space. In 1993, the Internet Engineering Task Force (IETF) created a new set of standards that allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B, or C address.

The IETF knew that CIDR was only a temporary solution and that a new IP protocol would have to be developed to accommodate the rapid growth in the number of Internet users. In 1994, the IETF began its work to find a successor to IPv4, which eventually became IPv6.

Table 8-9 illustrates the classful address ranges.



Address Class	First Octet Range (Decimal)	First Octet Bits (Bold Bits Do Not Change)	Network (N) and Host (H) Parts of Address	Default Subnet Mask (Decimal)	Number of Possible Network and Hosts per Network
A	1–127	00000000- 01111111	N.H.H.H	255.0.0.0	128 networks (2^7) 16,777,214 hosts (2^{24}–2)
B	128–191	10000000- 10111111	N. N.H.H	255.255.0.0	16,384 networks (2^{14}) 65,534 hosts (2^{16}–2)
C	192–223	11000000- 11011111	N. N. N.H	255.255.255.0	2,097,150 networks (2^{21}) 254 hosts (2^8–2)
D	224–239	11100000- 11101111	—	—	—
E	240–255	11110000- 11111111	—	—	—

Note: All 0s and all 1s are invalid host addresses.

Table 8-9 Legacy IPv4 Address Classes

Assignment of IP Addresses (8.1.4.5, 8.1.4.6)

For a company or organization to have network hosts, such as web servers, accessible from the Internet, that organization must have a block of public addresses assigned. Remember that public addresses must be unique, and use of these public addresses is regulated and allocated to each organization separately. This is true for IPv4 and IPv6 addresses.

IANA and RIRs

The ***Internet Assigned Numbers Authority (IANA)*** (www.iana.org) manages the allocation of IPv4 and IPv6 addresses. Until the mid-1990s, all IPv4 address space was managed directly by the IANA. At that time, the remaining IPv4 address space was allocated to various other registries to manage for particular purposes or for regional areas. These registration companies are called Regional Internet Registries (RIR).

The major registries are

- AfriNIC (African Network Information Centre) - Africa Region, www.afrinic.net
- APNIC (Asia Pacific Network Information Centre) - Asia/Pacific Region, www.apnic.net
- ARIN (American Registry for Internet Numbers) - North America Region, www.arin.net
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Latin America and

some Caribbean Islands, www.lacnic.net

- RIPE NCC (Réseaux IP Européens) - Europe, the Middle East, and Central Asia, www.ripe.net

ISPs

RIRs are responsible for allocating IP addresses to the ***Internet service providers (ISP)***. Most companies or organizations obtain their IPv4 address blocks from an ISP. An ISP will generally supply a small number of usable IPv4 addresses (for example, 6 or 14) to their customers as a part of their services. Larger blocks of addresses can be obtained based on justification of needs and for additional service costs.

In a sense, the ISP loans or rents these addresses to the organization. If we choose to move our Internet connectivity to another ISP, the new ISP will provide us with addresses from the address blocks that have been provided to it, and our previous ISP returns the blocks loaned to us to its allocation to be loaned to another customer.

IPv6 addresses can be obtained from the ISP or in some cases directly from the RIR. IPv6 addresses and typical address block sizes will be discussed later in this chapter.

ISP Services

To get access to the services of the Internet, we have to connect our data network to the Internet using an Internet service provider (ISP).

ISPs have their own set of internal data networks to manage Internet connectivity and to provide related services. Among the other services that an ISP generally provides to its customers are Domain Name System (DNS) services, email services, and a website. Depending on the level of service required and available, customers use different tiers of an ISP.

ISP Tiers

ISPs are designated by a hierarchy based on their level of connectivity to the Internet backbone. Each lower tier obtains connectivity to the backbone through a connection to a higher-tier ISP.

Tier 1

At the top of the ISP hierarchy are Tier 1 ISPs. These ISPs are large national or international ISPs that are directly connected to the Internet backbone. The customers of Tier 1 ISPs are either lower-tiered ISPs or large companies and organizations. Because they are at the top of Internet connectivity, they engineer highly reliable connections and services. Among the technologies used to support this reliability are multiple connections to the Internet backbone.

The primary advantages for customers of Tier 1 ISPs are reliability and speed. Because these customers are only one connection away from the Internet, there are fewer opportunities for failures or traffic bottlenecks. The drawback for Tier 1 ISP customers is its high cost.

Tier 2

Tier 2 ISPs acquire their Internet service from Tier 1 ISPs. Tier 2 ISPs generally focus on business customers. Tier 2 ISPs usually offer more services than the other two tiers of ISPs. These Tier 2 ISPs tend to have the IT resources to operate their own services such as DNS, email servers, and web servers. Other services that Tier 2 ISPs might offer include website development and maintenance, e-commerce/e-business, and VoIP.

The primary disadvantage of Tier 2 ISPs, as compared to Tier 1 ISPs, is slower Internet access. Because Tier 2 ISPs are at least one more connection away from the Internet backbone, they also tend to have lower reliability than Tier 1 ISPs.

Tier 3

Tier 3 ISPs purchase their Internet service from Tier 2 ISPs. The focus of these ISPs is the retail and home markets in a specific locale. Tier 3 customers typically do not need many of the services required by Tier 2 customers. Their primary need is connectivity and support.

These customers often have little or no computer or network expertise. Tier 3 ISPs often bundle Internet connectivity as a part of network and computer service contracts for their customers. While they might have reduced bandwidth and less reliability than Tier 1 and Tier 2 providers, they are often good choices for small- to medium-size companies.

Interactive Graphic

Activity 8.1.4.7: Public or Private IPv4 Addresses

Go to the course online to perform this practice activity.

Lab 8.1.4.8: Identifying IPv4 Addresses

In this lab, you will complete the following objectives:

- Part 1: Identify IPv4 Addresses
- Part 2: Classify IPv4 Addresses

IPv6 Network Addresses (8.2)

This section will introduce IPv6.

IPv4 Issues (8.2.1)

The useful life of IPv4 has almost been reached. This section will examine the reasons for the migration to IPv6.

The Need for IPv6 (8.2.1.1)

IPv6 is designed to be the successor to IPv4. IPv6 has a larger 128-bit address space, providing for 340 undecillion addresses (that is the number 340, followed by 36 zeroes). However, IPv6 is much more than just larger addresses. When the IETF began its development of a successor to IPv4, it used this opportunity to fix the limitations of IPv4 and include additional enhancements. One example is Internet Control Message Protocol version 6 (ICMPv6), which includes address resolution and address autoconfiguration not found in ICMP for IPv4 (ICMPv4). ICMPv4 and ICMPv6 will be discussed later in this chapter.

Need for IPv6

The depletion of IPv4 address space has been the motivating factor for moving to IPv6. As Africa, Asia, and other areas of the world become more connected to the Internet, there are not enough IPv4 addresses to accommodate this growth. On Monday, January 31, 2011, the IANA allocated the last two /8 IPv4 address blocks to the Regional Internet Registries (RIR). Various projections show that all five RIRs will have run out of IPv4 addresses between 2013 and 2020. At that point, the remaining IPv4 addresses will have been allocated to ISPs.

IPv4 has a theoretical maximum of 4.3 billion addresses. RFC 1918 private addresses in combination with Network Address Translation (NAT) have been instrumental in slowing the depletion of IPv4 address space. NAT has limitations that severely impede peer-to-peer communications.

Internet of Things

The Internet of today is significantly different than the Internet of past decades. The Internet of today is more than email, web pages, and file transfer between computers. The evolving Internet is becoming an Internet of things. No longer will the only devices accessing the Internet be computers, tablets and smartphones. The sensor-equipped, Internet-ready devices of tomorrow will include everything from automobiles and biomedical devices to household appliances and natural ecosystems. Imagine a meeting at a customer site that is automatically scheduled on your calendar application to begin an hour before you normally start work. This could be a significant problem, especially if you forget to check the calendar or adjust the alarm clock accordingly. Now imagine that the calendar application communicates this information directly to your alarm clock for you and to your automobile. Your car automatically warms up to melt the ice on the windshield before you enter the car and reroutes you to your meeting.

With an increasing Internet population, a limited IPv4 address space, issues with NAT and an Internet of things, the time has come to begin the transition to IPv6.

IPv4 and IPv6 Coexistence (8.2.1.2)

There is not a single date to move to IPv6. For the foreseeable future, both IPv4 and IPv6 will coexist. The transition is expected to take years. The IETF has created various protocols and tools to help network administrators migrate their networks to IPv6. The migration techniques can be divided into three categories:

- **Dual-stack:** As shown in Figure 8-9a, dual-stack allows IPv4 and IPv6 to coexist on the same network. Dual-stack devices run both IPv4 and IPv6 protocol stacks simultaneously.

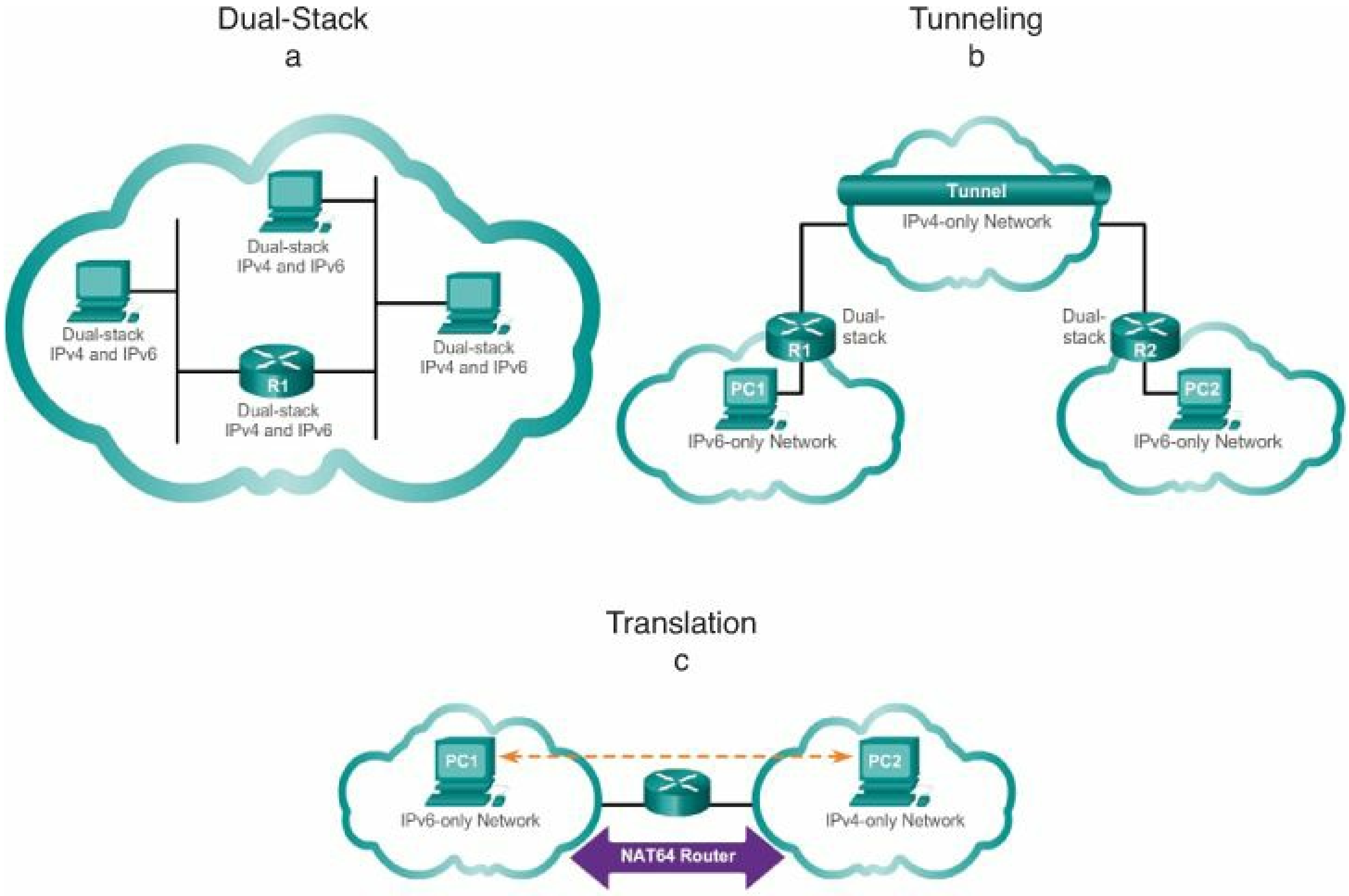


Figure 8-9 IPv4 and IPv6 Coexistence Methods

- **Tunneling:** As shown in Figure 8-9b, tunneling is a method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet, similar to other types of data.
- **Translation:** As shown in Figure 8-9c, Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet and vice versa.

Interactive Graphic **Activity 8.2.1.3: IPv4 Issues and Solutions**

Go to the course online to perform this practice activity.

IPv6 Addressing (8.2.2)

At their core, both IPv4 and IPv6 are binary. However, to make it easier to work with the expanded address range of IPv6, these addresses are represented differently. This section will present the representation of IPv6 addresses.

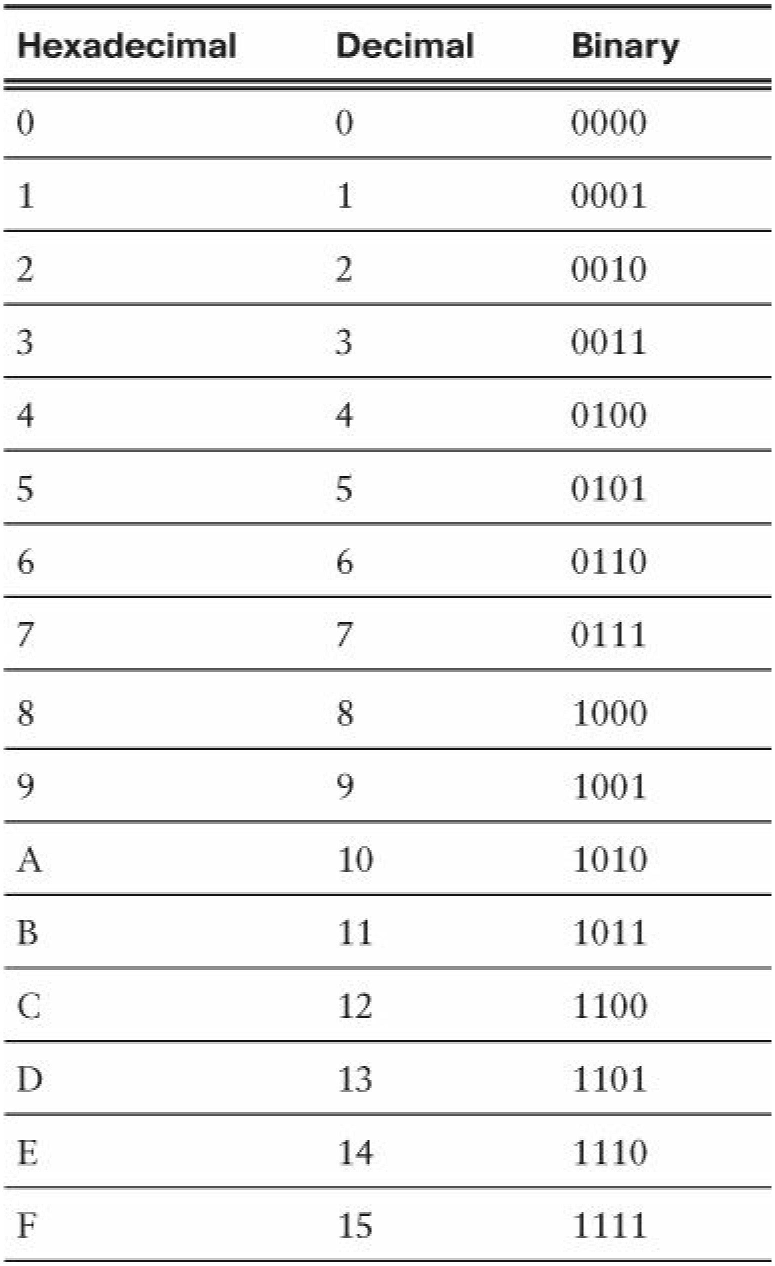
Hexadecimal Number System (8.2.2.1)

Unlike IPv4 addresses that are expressed in dotted-decimal notation, IPv6 addresses are represented using hexadecimal values. You have seen hexadecimal used in the Packets Byte pane of Wireshark. In Wireshark, hexadecimal is used to represent the binary values within frames and packets. Hexadecimal is also used to represent Ethernet Media Access Control (MAC) addresses.

Hexadecimal Numbering

Hexadecimal ("hex") is a convenient way to represent binary values. Just as decimal is a base 10 numbering system and binary is base 2, hexadecimal is a base 16 system.

The base 16 numbering system uses the numbers 0 to 9 and the letters A to F. Table 8-10 shows the equivalent decimal, binary, and hexadecimal values. There are 16 unique combinations of 4 bits, from 0000 to 1111. The 16-digit hexadecimal is the perfect number system to use, because any 4 bits can be represented with a single hexadecimal value.



Hexadecimal	Decimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Table 8-10 Hexadecimal Numbers

Understanding Bytes

Given that 8 bits (a byte) is a common binary grouping, binary 00000000 to 11111111 can be represented in hexadecimal as the range from 00 to FF. Leading 0s can be displayed to complete the 8-bit representation. For example, the binary value 0000 1010 is shown in hexadecimal as 0A.

Representing Hexadecimal Values

Note

It is important to distinguish hexadecimal values from decimal values regarding the characters 0 to 9.

Hexadecimal is usually represented in text by the value preceded by 0x (for example 0x73) or a subscript 16. Less commonly, it can be followed by an H, for example 73H. However, because subscript text is not recognized in command-line or programming environments, the technical representation of hexadecimal is preceded with “0x” (zero X). Therefore, the previous examples would be shown as 0x0A and 0x73, respectively.

Hexadecimal Conversions

Number conversions between decimal and hexadecimal values are straightforward, but quickly dividing or multiplying by 16 is not always convenient. With practice, it is possible to recognize the binary bit patterns that match the decimal and hexadecimal values.

IPv6 Address Representation (8.2.2.2)

IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every 4 bits is represented by a single hexadecimal digit, for a total of 32 hexadecimal values. IPv6 addresses are not case sensitive and can be written in either lowercase or uppercase.

Preferred Format

As shown in Figure 8-10, the preferred format for writing an IPv6 address is x:x:x:x:x:x:x:x, with each “x” consisting of four hexadecimal values. When referring to 8 bits of an IPv4 address, we use the term *octet*. In IPv6, a ***hextet*** is the unofficial term used to refer to a segment of 16 bits or four hexadecimal values. Each “x” is a single hextet, 16 bits, or four hexadecimal digits.

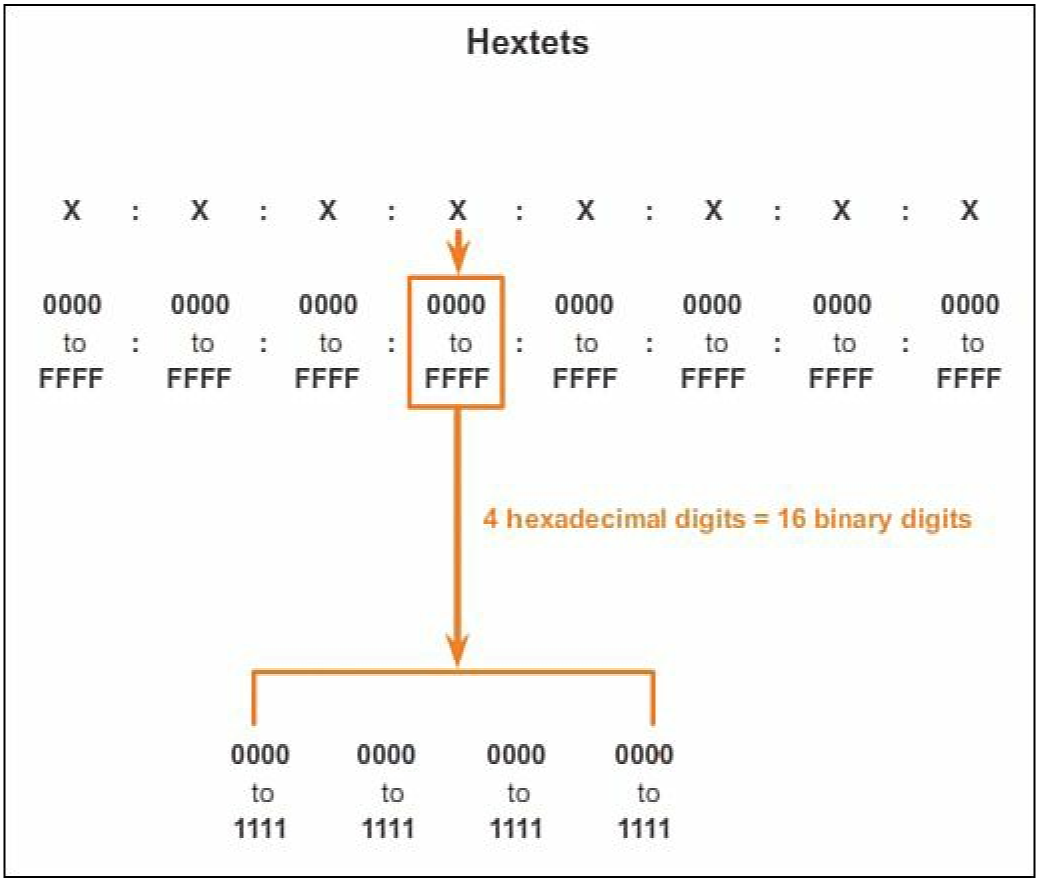

Hextets
X : X : X : X : X : X : X : X
0000 to FFFF : 0000 to FFFF : 0000 to FFFF : 0000 to FFFF : 0000 to FFFF : 0000 to FFFF : 0000 to FFFF : 0000 to FFFF
4 hexadecimal digits = 16 binary digits
0000 to 1111
0000 to 1111
0000 to 1111
0000 to 1111

Figure 8-10 IPv6 Preferred Format

Preferred format means that the IPv6 address is written using all 32 hexadecimal digits. It does not necessarily mean that it is the ideal method for representing the IPv6 address. In the following pages, we will see two rules to help reduce the number of digits needed to represent an IPv6 address.

Some examples of IPv6 addresses in the preferred format are

Click here to view code image

```
2001:0DB8:0000:1111:0000:0000:0000:0200
FE80:0000:0000:0000:0123:4567:89AB:CDEF
FF02:0000:0000:0000:0000:0001:FF00:0200
0000:0000:0000:0000:0000:0000:0000:0001
```

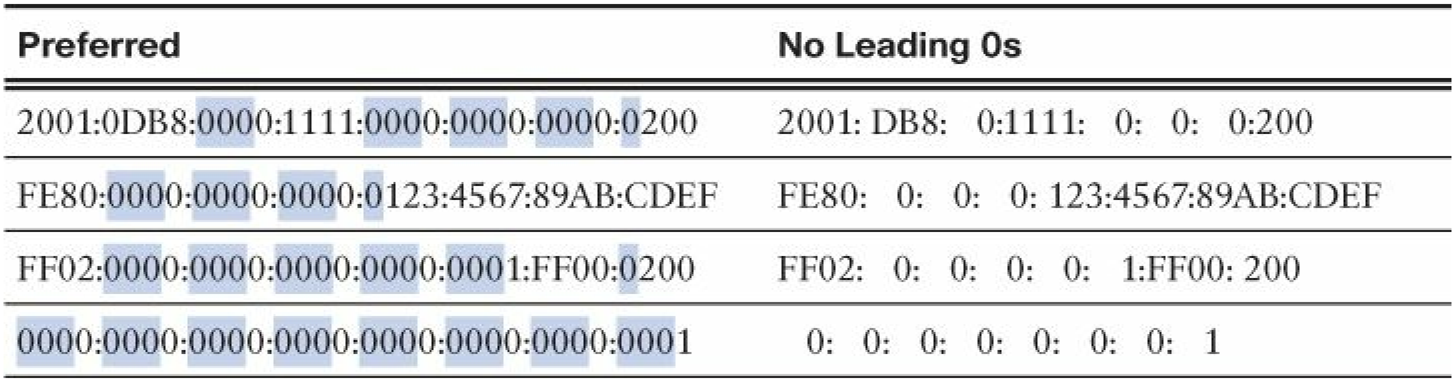
Rule 1: Omit Leading 0s (8.2.2.3)

The first rule to help reduce the notation of IPv6 addresses is that any leading 0s in any 16-bit section or hextet can be omitted. For example:

- 01AB can be represented as 1AB.
- 09F0 can be represented as 9F0.
- 0A00 can be represented as A00.
- 00AB can be represented as AB.

This rule only applies to leading 0s, *not* to trailing 0s; otherwise, the address would be ambiguous. For example, the hextet “ABC” could be either “0ABC” or “ABC0.”

Table 8-11 shows several examples of how omitting leading 0s can be used to reduce the size of an IPv6 address. For each example, the preferred format is shown. Notice how omitting the leading 0s in most examples results in a smaller address representation.



Preferred	No Leading 0s
2001:0DB8:0000:1111:0000:0000:0000:0200	2001: DB8: 0:1111: 0: 0: 0:200
FE80:0000:0000:0000:0123:4567:89AB:CDEF	FE80: 0: 0: 0: 123:4567:89AB:CDEF
FF02:0000:0000:0000:0000:0001:FF00:0200	FF02: 0: 0: 0: 0: 1:FF00: 200
0000:0000:0000:0000:0000:0000:0000:0001	0: 0: 0: 0: 0: 0: 0: 1

Table 8-11 IPv6 Addresses Omitting Leading 0s

Rule 2: Omit All 0 Segments (8.2.2.4)

The second rule to help reduce the notation of IPv6 addresses is that a double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0s.

The double colon (::) can only be used once within an address; otherwise, there would be more than one possible resulting address. When used with the omitting leading 0s technique, the notation of IPv6 address can often be greatly reduced. This is commonly known as the compressed format.

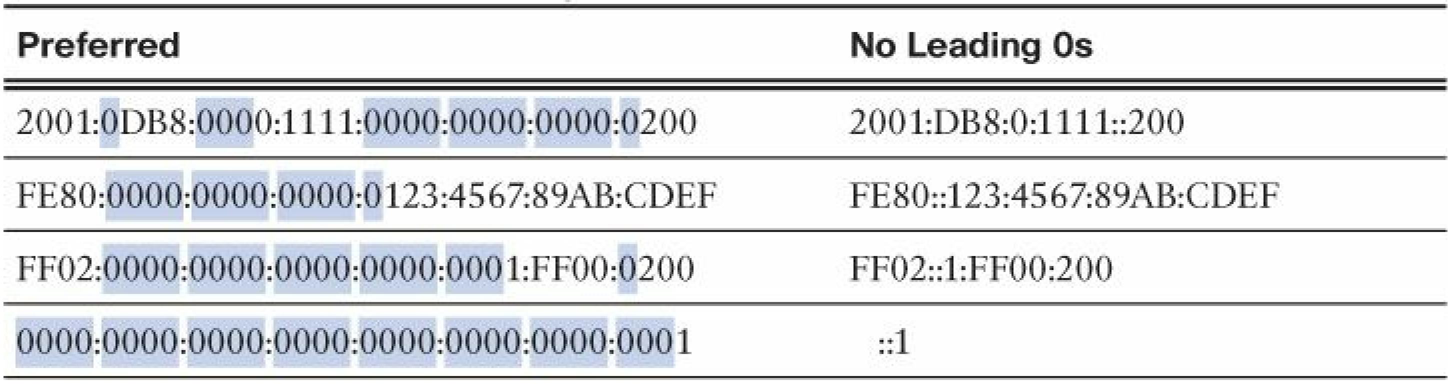
Here is an incorrect address:

- 2001:0DB8::ABCD::1234

Possible expansions of the ambiguous compressed address are

- 2001:0DB8::ABCD:0000:0000:1234
- 2001:0DB8::ABCD:0000:0000:0000:1234
- 2001:0DB8:0000:ABCD::1234
- 2001:0DB8:0000:0000:ABCD::1234

Table 8-12 shows several examples of how using the double colon (::) and omitting leading 0s can reduce the size of an IPv6 address.



Preferred	No Leading 0s
2001:0DB8:0000:1111:0000:0000:0000:0200	2001:DB8:0:1111::200
FE80:0000:0000:0000:0123:4567:89AB:CDEF	FE80::123:4567:89AB:CDEF
FF02:0000:0000:0000:0000:0001:FF00:0200	FF02::1:FF00:200
0000:0000:0000:0000:0000:0000:0000:0001	::1

Table 8-12 IPv6 Addresses Using Double Colons

Interactive Graphic **Activity 8.2.2.5: Practicing IPv6 Address Representations**

Go to the course online to perform this practice activity.

Types of IPv6 Addresses (8.2.3)

This section will introduce the different types and uses of IPv6 addresses.

IPv6 Address Types (8.2.3.1)

There are three types of IPv6 addresses:

- **Unicast:** An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device. A source IPv6 address must be a unicast address.
- **Multicast:** An IPv6 multicast address is used to send a single IPv6 packet to multiple destinations.
- **Anycast:** An IPv6 anycast address is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address. Anycast addresses are beyond the scope of this course.

Unlike IPv4, IPv6 does not have a broadcast address. However, there is an IPv6 all-nodes multicast address that essentially gives the same result.

IPv6 Prefix Length (8.2.3.2)

Recall that the prefix, or network, portion of an IPv4 address can be identified by a dotted-decimal subnet mask or prefix length (slash notation). For example, an IP address of 192.168.1.10 with dotted-decimal subnet mask 255.255.255.0 is equivalent to 192.168.1.10/24.

IPv6 uses the prefix length to represent the prefix portion of the address. IPv6 does not use the dotted-decimal subnet mask notation. The prefix length is used to indicate the network portion of an IPv6 address using the IPv6 address/prefix length.

The prefix length can range from 0 to 128. A typical IPv6 prefix length for LANs and most other types of networks is /64. This means that the prefix or network portion of the address is 64 bits in length, leaving another 64 bits for the interface ID (host portion) of the address.

IPv6 Unicast Addresses (8.2.3.3)

An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device. A packet sent to a unicast address is received by the interface that is assigned that address. Similar to IPv4, a source IPv6 address must be a unicast address. The destination IPv6 address can be either a unicast or a multicast address.

There are six types of IPv6 unicast addresses, described in the following sections.

Global Unicast

A global unicast address is similar to a public IPv4 address. These are globally unique, Internet routable addresses. Global unicast addresses can be configured statically or assigned dynamically. There are some important differences in how a device receives its IPv6 address dynamically compared to DHCP for IPv4.

Link-Local

Link-local addresses are used to communicate with other devices on the same local link. With IPv6, the term *link* refers to a subnet. Link-local addresses are confined to a single link. Their uniqueness must only be confirmed on that link because they are not routable beyond the link. In other words, routers will not forward packets with a link-local source or destination address.

Loopback

The loopback address is used by a host to send a packet to itself and cannot be assigned to a physical interface. Similar to an IPv4 loopback address, you can ping an IPv6 loopback address to test the configuration of TCP/IP on the local host. The IPv6 loopback address is all-0s except for the last bit, represented as ::1/128, or just ::1 in the compressed format.

Unspecified Address

An ***unspecified address*** is an all-0s address represented in the compressed format as ::/128, or just :: in the compressed format. It cannot be assigned to an interface and is only to be used as a source address in an IPv6 packet. An unspecified address is used as a source address when the device does not yet have a permanent IPv6 address or when the source of the packet is irrelevant to the destination.

Unique Local

IPv6 unique local addresses have some similarity to RFC 1918 private addresses for IPv4, but there are significant differences as well. ***Unique local addresses*** are used for local addressing within a site or between a limited number of sites. These addresses should not be routable in the global IPv6. Unique local addresses are in the range of FC00::/7 to FDFF::/7.

With IPv4, private addresses are combined with NAT/PAT to provide a many-toone translation of private to public addresses. This is done because of the limited availability of IPv4 address space. Many sites also use the private nature of RFC 1918 addresses to help secure or hide their network from potential security risks. However, this was never the intended use of these technologies, and the IETF has always recommended that sites take the proper security precautions on their Internet-facing router. Although IPv6 does provide site-specific addressing, it is not intended to be used to help hide internal IPv6-enabled devices from the IPv6 Internet. IETF recommends that limiting access to devices should be accomplished using proper, best-practice security measures.

Note

The original IPv6 specification defined site-local addresses for a similar purpose, using the prefix range FEC0::/10. There were several ambiguities in the specification, and site-local addresses were deprecated by the IETF in favor of unique local addresses.

IPv4 embedded

The last type of unicast address type is the IPv4 embedded address. These addresses are used to help transition from IPv4 to IPv6. IPv4 embedded addresses are beyond the scope of this course.

IPv6 Link-Local Unicast Addresses (8.2.3.4)

An IPv6 link-local address enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet). Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated.

Unlike IPv4 link-local addresses, IPv6 link-local addresses have a significant role in various aspects of the network. The global unicast address is not a requirement; however, every IPv6-enabled network interface is required to have a link-local address.

If a link-local address is not configured manually on an interface, the device will automatically create its own without communicating with a DHCP server. IPv6-enabled hosts create an IPv6 link-local address even if the device has not been assigned a global unicast IPv6 address. This allows IPv6-enabled devices to communicate with other IPv6-enabled devices on the same subnet. This includes communication with the default gateway (router).

IPv6 link-local addresses are in the FE80::/10 range. The /10 indicates that the first 10 bits are 1111 1110 10xx xxxx. The first hextet has a range of 1111 1110 10**00 0000** (FE80) to 1111 1110 10**11 1111** (FEBF).

Figure 8-11 shows the format of an IPv6 link-local address.

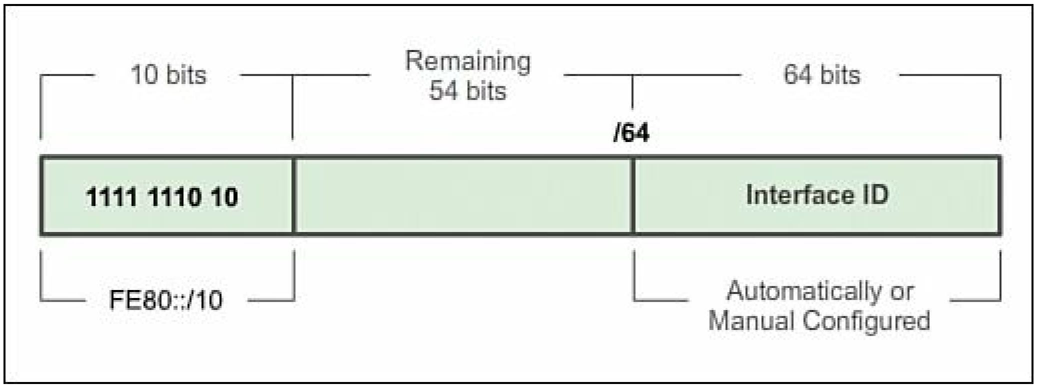


Figure 8-11 IPv6 Link-Local Address

IPv6 link-local addresses are also used by IPv6 routing protocols to exchange messages and as the next-hop address in the IPv6 routing table. Link-local addresses are discussed in more detail in a later course.

Note

Typically, it is the link-local address of the router and not the global unicast address that is used as the default gateway for other devices on the link.

Activity 8.2.3.5: Identify Types of IPv6 Addresses

Go to the course online to perform this practice activity.

IPv6 Unicast Addresses (8.2.4)

This section will introduce IPv6 unicast addressing.

Structure of an IPv6 Global Unicast Address (8.2.4.1)

IPv6 global unicast addresses are globally unique and routable on the IPv6 Internet. These addresses are equivalent to public IPv4 addresses. The Internet Committee for Assigned Names and Numbers (ICANN), the operator for the Internet Assigned Numbers Authority (IANA), allocates IPv6 address blocks to the five RIRs. Currently, only global unicast addresses with the first three bits of 001 or 2000::/3 are being assigned. This is only 1/8th of the total available IPv6 address space, excluding only a very small portion for other types of unicast and multicast addresses.

Note

The 2001:0DB8::/32 address has been reserved for documentation purposes, including use in examples.

Figure 8-12 shows the structure and range of a global unicast address.

A global unicast address has three parts:

- Global routing prefix
- Subnet ID
- Interface ID

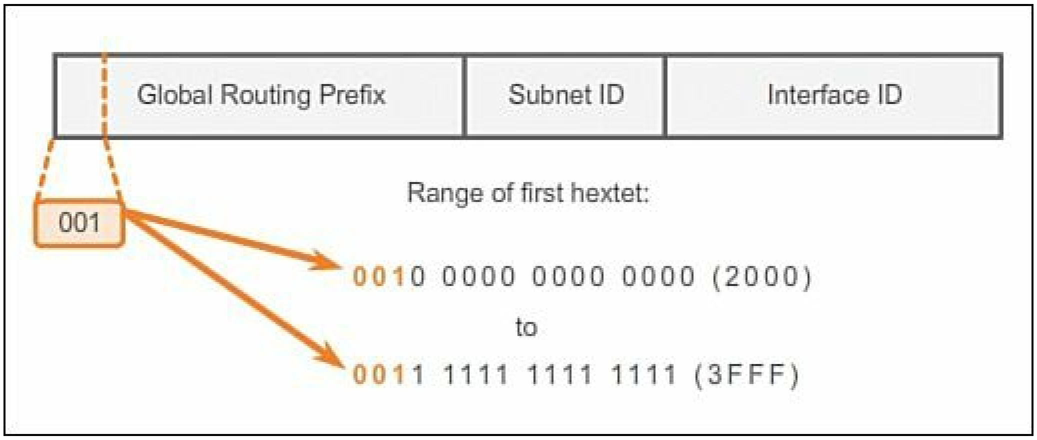


Figure 8-12 Parts of a IPv6 Global Unicast Address

Global Routing Prefix

The global routing prefix is the prefix, or network, portion of the address that is assigned by the provider, such as an ISP, to a customer or site. Currently, RIRs assign a /48 global routing prefix to customers. This includes everyone from enterprise business networks to individual households. This is more than enough address space for most customers.

Figure 8-13 shows the structure of a global unicast address using a /48 global routing prefix. /48 prefixes are the most common global routing prefixes assigned and will be used in most of the examples throughout this course.

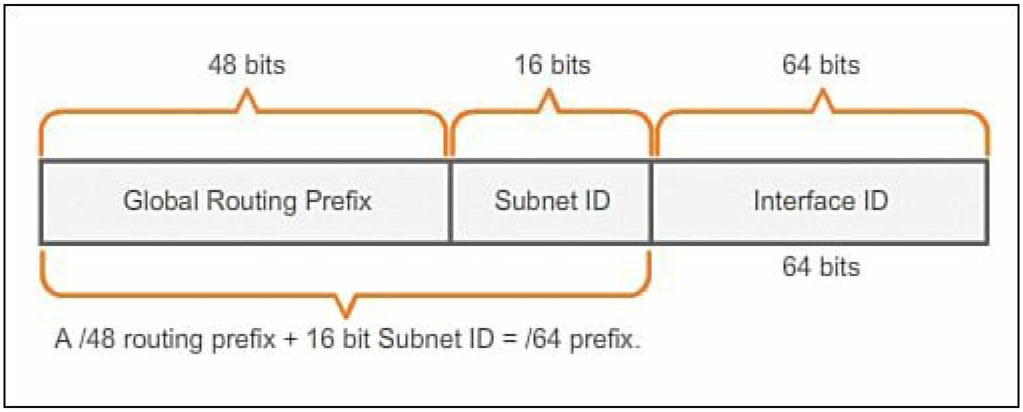


Figure 8-13 Division of an IPv6 Global Unicast Address

For example, the IPv6 address 2001:0DB8:ACAD::/48 has a prefix that indicates that the first 48 bits (3 hextets) (2001:0DB8:ACAD) is the prefix or network portion of the address. The double colon (::) prior to the /48 prefix length means that the rest of the address contains all 0s.

Subnet ID

The subnet ID is used by an organization to identify subnets within its site.

Interface ID

The IPv6 interface ID is equivalent to the host portion of an IPv4 address. The term *interface ID* is used because a single host can have multiple interfaces, each having one or more IPv6 addresses.

Note

Unlike IPv4, in IPv6, the all-0s address can be assigned to a device. However, the all-0s address is reserved as a Subnet-Router anycast address, and should be assigned only to routers.

An easy way to read most IPv6 addresses is to count the number of hextets. As shown in Figure 8-14, in a /64 global unicast address, the first four hextets are for the network portion of the address, with the fourth hextet indicating the subnet ID. The remaining four hextets are for the interface ID.

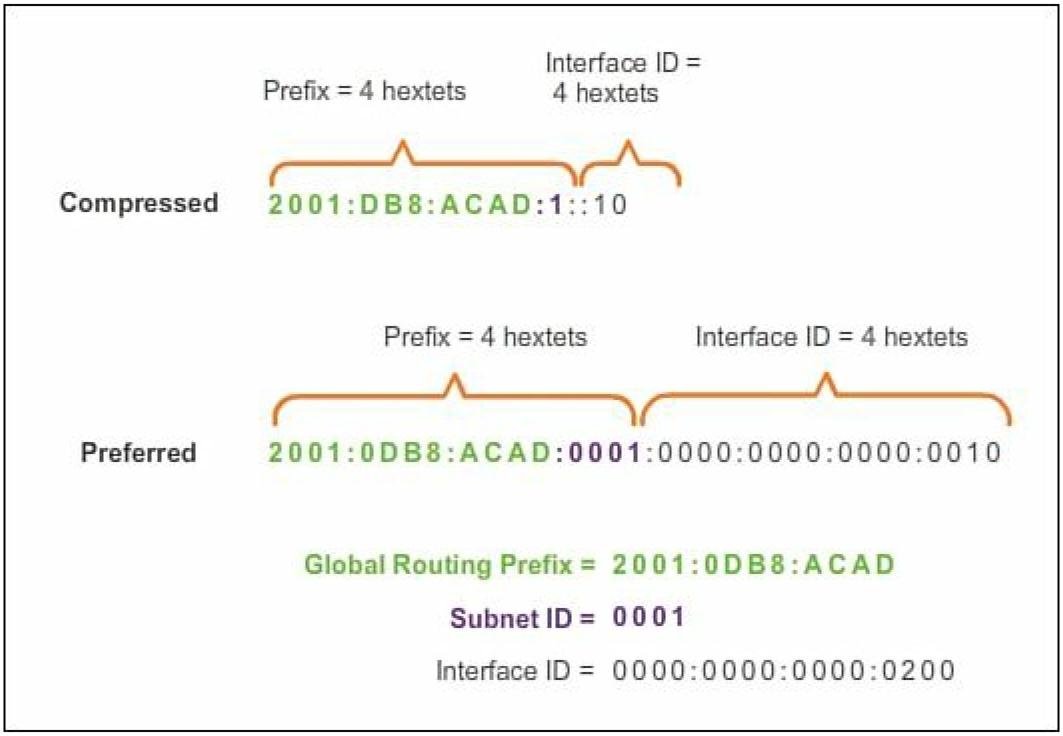


Figure 8-14 Interpreting an IPv6 Global Unicast Address

Static Configuration of a Global Unicast Address (8.2.4.2)

This section will introduce the configuration of IPv6 global unicast addresses.

Router Configuration

Most IPv6 configuration and verification commands in the Cisco IOS are similar to their IPv4 counterparts. In many cases, the only difference is the use of **ipv6** in place of **ip** within the commands.

The **interface** command to configure an IPv6 global unicast address on an interface is **ipv6 address** *ipv6-address/prefix-length*.

Notice that there is not a space between *ipv6-address* and *prefix-length*.

The example configuration will use the topology shown in Figure 8-15 and these IPv6 subnets:

- 2001:0DB8:ACAD:0001:/64 (*or* 2001:DB8:ACAD:1::/64)
- 2001:0DB8:ACAD:0002:/64 (*or* 2001:DB8:ACAD:2::/64)

- 2001:0DB8:ACAD:0003:/64 (*or* 2001:DB8:ACAD:3::/64)

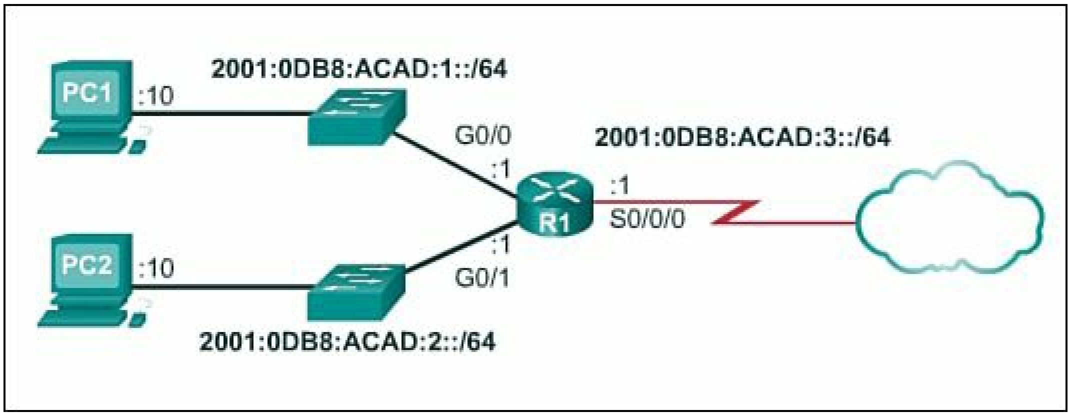


Figure 8-15 Example IPv6 Topology

Manually configuring the IPv6 address on a host is similar to configuring an IPv4 address. Example 8-4 shows the IPv6 configuration of the router in Figure 8-15.

Example 8-4 Configuration of IPv6 on a Router

Click here to view code image

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 0/0
Router(config-if)# ipv6 address 2001:db8:acad:1::1/64
Router(config-if)# no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
  changed state to up


Router(config-if)#
Router(config-if)# interface gigabitethernet 0/1
Router(config-if)# ipv6 address 2001:db8:acad:2::2/64
Router(config-if)# no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
  changed state to up

Router(config-if)#
Router(config-if)# interface serial 0/0/0
Router(config-if)# ipv6 address 2001:db8:acad:3::1/64
Router(config-if)# no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINKPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Router(config-if)# exit

Router(config)# ipv6 unicast-routing
Router(config)# end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router# copy running-config startup-config
```

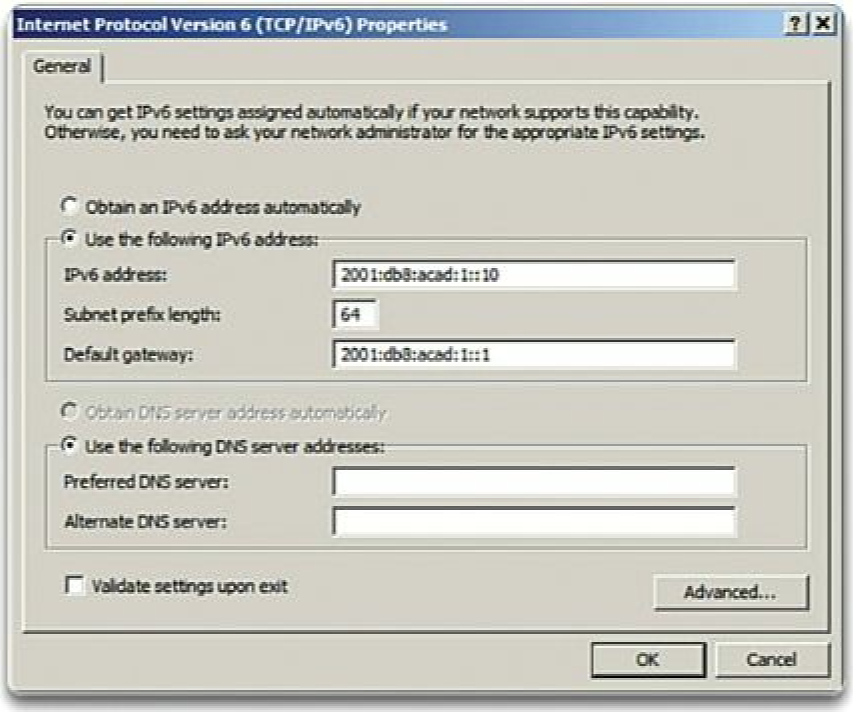
```
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

IPv6 routing is not enabled by default. To enable a router as an IPv6 router, the **ipv6 unicast-routing** global configuration command must be used.

Note

Cisco routers are enabled as IPv4 routers by default.

Figure 8-16 shows the IPv6 configuration of PC1 shown in Figure 8-15. In this configuration, the default gateway address configured for PC1 is 2001:DB8:ACAD:1::1, the global unicast address of the R1 Gigabit Ethernet interface on the same network.



You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

○ Obtain an IPv6 address automatically

● Use the following IPv6 address:

IPv6 address: 2001:db8:acad:1::10

Subnet prefix length: 64

Default gateway: 2001:db8:acad:1::1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

Figure 8-16 IPv6 Configuration of PC1

Just as with IPv4, configuring static addresses on clients does not scale to larger environments. For this reason, most network administrators in an IPv6 network will enable dynamic assignment of IPv6 addresses.

A device can obtain an IPv6 global unicast address automatically in two ways:

- ***Stateless Address Autoconfiguration (SLAAC)***
- DHCPv6

Dynamic Configuration of a Global Unicast Address Using SLAAC (8.2.4.3)

This section will introduce the dynamic assignment of IPv6 addresses with Stateless Address Autoconfiguration.

Stateless Address Autoconfiguration

Stateless Address Autoconfiguration (SLAAC) is a method that allows a device to obtain its prefix, prefix length, and default gateway address information from an *IPv6 router* without the use of a DHCPv6 server. Using SLAAC, devices rely on the local router's ICMPv6 Router Advertisement (RA) messages to obtain the necessary information.

IPv6 routers periodically send out ICMPv6 RA messages to all IPv6-enabled devices on the network. By default, Cisco routers send out RA messages every 200 seconds to the IPv6 all-nodes multicast group address. An IPv6 device on the network does not have to wait for these periodic RA messages. A device can send a Router Solicitation (RS) message to the router, using the IPv6 all-routers multicast group address. When an IPv6 router receives an RS message, it will immediately respond with a Router Advertisement.

As previously mentioned, even though an interface on a Cisco router can be configured with an IPv6 address, this does not make it an "IPv6 router." When the **ipv6 unicast-routing** global configuration command is used, the router becomes an IPv6 router and can

- Forward IPv6 packets between networks
- Be configured with static IPv6 routes or a dynamic IPv6 routing protocol
- Send ICMPv6 RA messages

The ICMPv6 RA message contains the prefix, prefix length, and other information for the IPv6 device. The RA message also informs the IPv6 device how to obtain its addressing information. The RA message can contain one of the following three options:

- **Option 1 – SLAAC only:** The device should use the prefix, prefix length, and default gateway address information contained in the RA message. No other information is available from a DHCPv6 server.
- **Option 2 – SLAAC and DHCPv6:** The device should use the prefix, prefix length, and default gateway address information in the RA message. There is other information available from a DHCPv6 server, such as the DNS server address. The device will, through the normal process of discovering and querying a DHCPv6 server, obtain this additional information. This is known as stateless DHCPv6 because the DHCPv6 server does not need to allocate or keep track of any IPv6 address assignments, but only provide additional information such as the DNS server address.
- **Option 3 – DHCPv6 only:** The device should not use the information in this RA message for its addressing information. Instead, the device will use the normal process of discovering and querying a DHCPv6 server to obtain all its addressing information. This includes an IPv6 global unicast address, a prefix length, a default gateway address, and the addresses of DNS servers. In this case, the DHCPv6 server is acting as a stateful DHCP server similar to DHCP for IPv4. The DHCPv6 server allocates and keeps track of IPv6 addresses so that it does not assign the same IPv6 address to multiple devices.

Routers send ICMPv6 RA messages using the link-local address as the source IPv6 address. Devices using SLAAC use the router's link-local address as their default gateway address.

Dynamic Configuration of a Global Unicast Address Using DHCPv6 (8.2.4.4)

This section will introduce the dynamic assignment of IPv6 addresses with Dynamic Host Configuration Protocol for IPv6.

DHCPv6

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is similar to DHCP for IPv4. A device can automatically receive its addressing information, including a global unicast address, prefix length, default gateway address, and the addresses of DNS servers using the services of a DHCPv6 server.

A device can receive all or some of its IPv6 addressing information from a DHCPv6 server depending upon whether Option 2 (SLAAC and DHCPv6) or Option 3 (DHCPv6 only) is specified in the ICMPv6 RA message. Additionally, the host OS can choose to ignore whatever is in the router's RA message and obtain its IPv6 address and other information directly from a DHCPv6 server.

For Option 2 (SLAAC and DHCPv6), the steps are

Step 1. The client sends a Router Solicitation (RS) message to all IPv6 routers requesting addressing information.

Step 2. One or more IPv6 routers send a Router Advertisement (RA) to all IPv6 nodes containing prefix, prefix length, and gateway information.

Step 3. The node requires more IPv6 configuration. Therefore, the node contacts a DHCPv6 server for the remaining configuration.

Before deploying IPv6 devices in a network, it is a good idea to first verify whether the host observes the options within the router's ICMPv6 RA message.

A device can obtain its IPv6 global unicast address dynamically and can also be configured with multiple static IPv6 addresses on the same interface. IPv6 allows multiple IPv6 addresses, belonging to the same IPv6 network, to be configured on the same interface.

A device can also be configured with more than one default gateway IPv6 address. For further information about how the decision is made regarding which address is used as a source IPv6 address or which default gateway address is used, refer to RFC 6724, Default Address Selection for IPv6.

The Interface ID

If the client does not use the information contained within the RA message and relies solely on DHCPv6, the DHCPv6 server will provide the entire IPv6 global unicast address, including the prefix and the interface ID.

However, if Option 1 (SLAAC only) or Option 2 (SLAAC with DHCPv6) is used, the client does not obtain the actual interface ID portion of the address from this process. The client device must determine its own 64-bit interface ID, either by using the EUI-64 process or by generating a random 64-bit number.

EUI-64 Process or Randomly Generated (8.2.4.5)

This section shows how the EUI-64 process uses the MAC address to generate an IPv6 interface ID.

EUI-64 Process

IEEE defined the Extended Unique Identifier (EUI) or modified EUI-64 process. This process uses a client's 48-bit Ethernet MAC address and inserts another 16 bits in the middle of the 48-bit MAC address to create a 64-bit interface ID.

Ethernet MAC addresses are usually represented in hexadecimal and are made up of two parts:

- **Organizationally Unique Identifier (OUI):** The OUI is a 24-bit (6 hexadecimal digits) vendor code assigned by the IEEE.

- **Device identifier:** The device identifier is a unique 24-bit (6 hexadecimal digits) value within a common OUI.

An EUI-64 interface ID is represented in binary and is made up of three parts:

- 24-bit OUI from the client MAC address, but the seventh bit (the Universally/Locally [U/L] bit) is reversed. This means that if the seventh bit is a 0, it becomes a 1 and vice versa.
- The inserted 16-bit value FFFE (in hexadecimal).
- 24-bit device identifier from the client MAC address.

The EUI-64 process is illustrated in Figure 8-17, using R1's Gigabit Ethernet MAC address of FC99:4775:CEE0.

Step 1. Divide the MAC address between the OUI and device identifier.

Step 2. Insert the hexadecimal value FFFE, which in binary is 1111 1111 1111 1110.

Step 3. Convert the first two hexadecimal values of the OUI to binary and flip the U/L bit (bit 7). In this example, the 0 in bit 7 is changed to a 1.

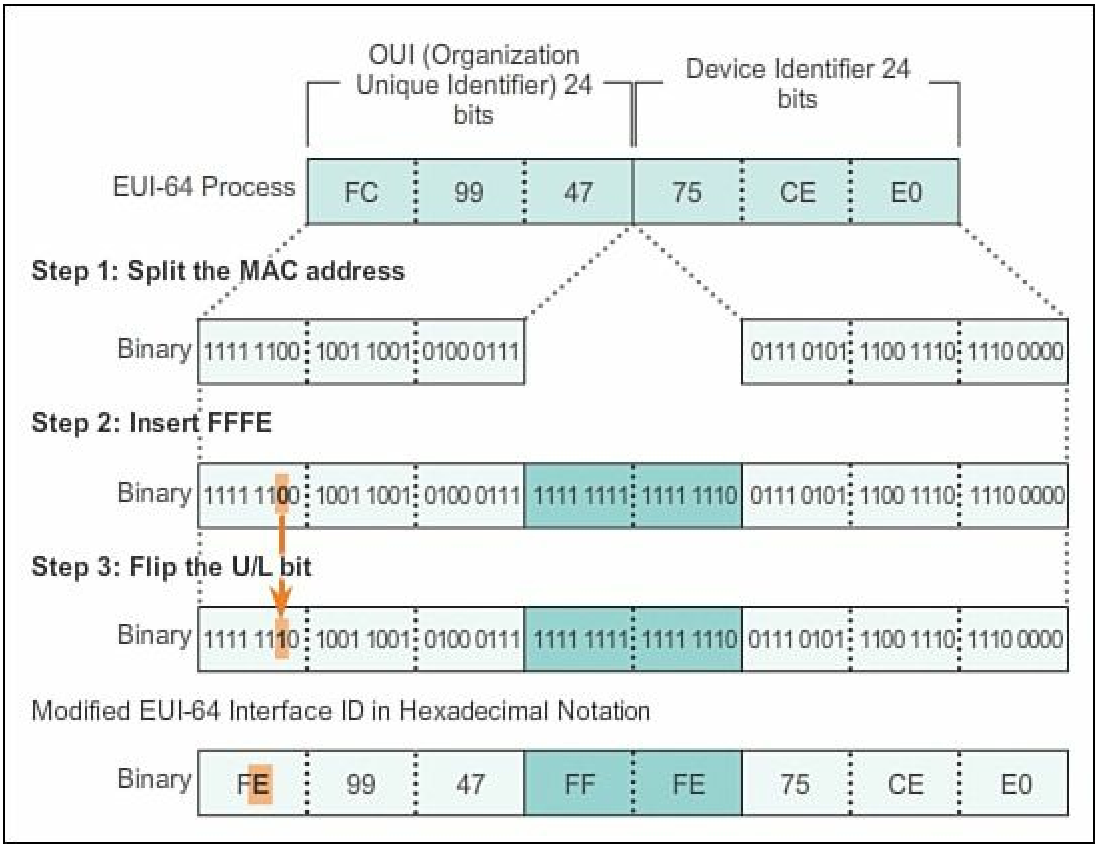


Figure 8-17 EUI-64 Process

The result is an EUI-64 generated interface ID of FE99:47FF:FE75:CEE0.

Note

The use of the U/L bit and the reasons for reversing its value are discussed in RFC 5342.

The advantage of EUI-64 is that the Ethernet MAC address can be used to determine the interface ID. It also allows network administrators to easily track an IPv6 address to an end device using the unique MAC address. However, this has caused privacy concerns among many users. They are concerned that their packets can be traced to the actual physical computer. Because of these concerns, a randomly generated interface ID can be used instead.

Randomly Generated Interface IDs

Depending upon the operating system, a device might use a randomly generated interface ID instead of using the MAC address and the EUI-64 process. For example, beginning with Windows Vista, Windows uses a randomly generated interface ID instead of one created with EUI-64. Windows XP and previous Windows operating systems used EUI-64.

An easy way to identify that an address was more than likely created using EUI-64 is the FFFE located in the middle of the interface ID, as shown in Example 8-5.

Example 8-5 Configuration of IPv6 on a Router

Click here to view code image

```
Router# show ipv6 interface brief
GigabitEthernet0/0          [up/up]
    FE80::2D0:58FF:FE75:C3E0
    2001:DB8:1::1
GigabitEthernet0/1          [up/up]
    FE80::2D0:58FF:FE75:C3E1
    2001:DB8:ACAD:2::2
Serial0/0/0                 [up/up]
    FE80::240:BFF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1                 [administratively down/down]
Vlan1                       [administratively down/down]
  Router#
```

Note

With EUI-64 for interfaces that do not have MAC addresses, such as serial and loopback, the router uses the first MAC address in the device. In Example 8-5, interface Serial 0/0/0 is using the MAC identifier of interface Gigabit Ethernet 0/0.

After the interface ID is established, either through the EUI-64 process or through random generation, it can be combined with an IPv6 prefix to create a global unicast address or a link-local address:

- **Global unicast address:** When using SLAAC, the device receives its prefix from the ICMPv6 RA and combines it with the interface ID.
- **Link-local address:** A link-local prefix begins with FE80::/10. A device typically uses FE80::/64 as the prefix/prefix length, followed by the interface ID.

Dynamic Link-Local Addresses (8.2.4.6)

When using SLAAC (SLAAC only or SLAAC with DHCPV6), a device receives its prefix and prefix length from the ICMPv6 RA. Because the prefix of the address has been designated by the RA message, the device must provide only the interface ID portion of its address. As stated previously, the interface ID can be automatically generated using the EUI-64 process or, depending on the OS, be randomly generated. Using the information from the RA message and the interface ID, the device can establish its global unicast address.

After a global unicast address is assigned to an interface, the IPv6-enabled device will automatically generate its link-local address. IPv6-enabled devices must have, at a minimum, the link-local address. Recall that an IPv6 link-local address enables a device to communicate with other IPv6-enabled devices on the same subnet.

IPv6 link-local addresses are used for a variety of purposes including

- A host uses the link-local address of the local router for its default gateway IPv6 address.
- Routers exchange dynamic routing protocol messages using link-local addresses.
- Routers' routing tables use the link-local address to identify the next-hop router when forwarding IPv6 packets.

A link-local address can be established dynamically or configured manually as a static link-local address.

Dynamically Assigned Link-Local Address

The link-local address is dynamically created using the FE80::/10 prefix and the interface ID.

By default, Cisco IOS routers use EUI-64 to generate the interface ID for all link-local addresses on IPv6 interfaces. For serial interfaces, the router will use the MAC address of an Ethernet interface. Recall that a link-local address must be unique only on that link or network. However, a drawback to using the dynamically assigned link-local address is its length, which makes it challenging to identify and remember assigned addresses.

Static Link-Local Addresses (8.2.4.7)

This section introduces manually configuring the IPv6 link-local addressing.

Static Link-Local Address

Configuring the link-local address manually provides the ability to create an address that is recognizable and easier to remember.

Link-local addresses can be configured manually using the same interface command used to create IPv6 global unicast addresses but with an additional parameter:

Click here to view code image

```
Router(config-if)# ipv6 address link-local-address link-local
```

Example 8-6 shows that a link-local address has a prefix within the range of FE80 to FEBF. When an address begins with this hextet (16-bit segment), the link-local parameter must follow the address. Also, shown in Example 8-6 is the configuration of a link-local address using the **ipv6 address interface** command. The link-local address FE80::1 is used to make it easily recognizable as belonging to Router R1. The same IPv6 link-local address is configured on all of R1's interfaces. FE80::1 can be configured on each link because it only has to be unique on that link.

Example 8-6 Configuration and Verification of IPv6 Link-Local Address

Click here to view code image

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 address FE80::1 ?
  link-local  Use link-local address
```

```
R1(config-if)# ipv6 address FE80::1 link-local
R1(config-if)# no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
R1(config-if)# exit

R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 address FE80::1 link-local
R1(config-if)# no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
R1(config-if)# exit

R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 address FE80::1 link-local
R1(config-if)# no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)# end

R1(config-if)# exit

R1(config)# ipv6 unicast-routing
R1(config)# end
R1#

R1# show ipv6 interface brief
GigabitEthernet0/0          [up/up]
    FE80::1
GigabitEthernet0/1          [up/up]
    FE80::1
Serial0/0/0                 [up/up]
    FE80::1
Serial0/0/1                 [administratively down/down]
Vlan1                       [administratively down/down]
  R1#
```

Verifying IPv6 Address Configuration (8.2.4.8)

As shown in Example 8-6, the commands to verify the IPv6 interface configuration, IPv6 routes, and IPv6 connectivity are similar to the commands used for IPv4.

The **show ipv6 interface brief** command displays abbreviated output for each of the interfaces. The [up/up] output on the same line as the interface indicates the Layer 1/Layer 2 interface state. This is the same as the Status and Protocol columns in the equivalent IPv4 command.

Notice that each interface has two IPv6 addresses. The second address for each interface is the global unicast address that was configured. The first address, the one that begins with FE80, is the link-local unicast address for the interface. Recall that the link-local address is automatically added to the interface when a global unicast address is assigned.

Also, notice that R1’s Serial 0/0/0 link-local address is the same as its Gigabit Ethernet 0/0 interface. Serial interfaces do not have an Ethernet MAC address, so Cisco IOS uses the MAC address of the first available Ethernet interface. This is possible because link-local interfaces only have to be unique on that link.

The link-local address of the router interface is typically the default gateway address for devices on that link or network.

As shown in Example 8-7, the **show ipv6 route** command can be used to verify that IPv6 networks and specific IPv6 interface addresses have been installed in the IPv6 routing table. The **show ipv6 route** command will only display IPv6 networks, not IPv4 networks.

Within the route table, a C next to a route indicates that this is a directly connected network. When the router interface is configured with a global unicast address and is in the “up/up” state, the IPv6 prefix and prefix length are added to the IPv6 routing table as a connected route.

The IPv6 global unicast address configured on the interface is also installed in the routing table as a local route. The local route has a /128 prefix. Local routes are used by the routing table to efficiently process packets with a destination address of the router’s interface address.

The **ping** command for IPv6 is identical to the command used with IPv4, except that an IPv6 address is used. Also shown in Example 8-7, the command is used to verify Layer 3 connectivity between R1 and a host. When pinging a link-local address from a router, Cisco IOS will prompt the user for the exit interface. Because the destination link-local address can be on one or more of its links or networks, the router needs to know on which interface to send the ping.

Example 8-7 Configuration and Verification of IPv6 Link-Local Address

Click here to view code image

```
R1#
R1# show ipv6 interface brief
GigabitEthernet0/0          [up/up]
    FE80::1
    2001:DB8:ACAD:1::
GigabitEthernet0/1          [up/up]
    FE80::1
    2001:DB8:ACAD:2::
Serial0/0/0                 [up/up]
    FE80::1
    2001:DB8:ACAD:3::
Serial0/0/1                 [administratively down/down]
Vlan1                       [administratively down/down]

R1# show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:DB8:ACAD:1::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2001:DB8:ACAD:1::/128 [0/0]
     via ::, GigabitEthernet0/0
C   2001:DB8:ACAD:2::/64 [0/0]
     via ::, GigabitEthernet0/1
L   2001:DB8:ACAD:2::/128 [0/0]
     via ::, GigabitEthernet0/1
C   2001:DB8:ACAD:3::/64 [0/0]
     via ::, Serial0/0/0
L   2001:DB8:ACAD:3::/128 [0/0]
     via ::, Serial0/0/0
```

```
L    FF00::/8 [0/0]
      via ::, Null0
R1#

R1# ping ipv6 2001:gb8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:gb8:acad:1::10 timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5)
R1#
```

IPv6 Multicast Addresses (8.2.5)

This section will present IPv6 multicast addressing.

Assigned IPv6 Multicast Addresses (8.2.5.1)

IPv6 multicast addresses are similar to IPv4 multicast addresses. Recall that a multicast address is used to send a single packet to one or more destinations (multicast group). IPv6 multicast addresses have the prefix FF00::/8.

> **Note**
>
> Multicast addresses can only be destination addresses and not source addresses.

There are two types of IPv6 multicast addresses:

- Assigned multicast
- Solicited-node multicast

Assigned Multicast

Assigned multicast addresses are reserved multicast addresses for predefined groups of devices. An assigned multicast address is a single address used to reach a group of devices running a common protocol or service. Assigned multicast addresses are used in context with specific protocols such as DHCPv6.

Two common IPv6 assigned multicast groups include

- **FF02::1 All-nodes multicast group:** This is a multicast group that all IPv6-enabled devices join. A packet sent to this group is received and processed by all IPv6 interfaces on the link or network. This has the same effect as a broadcast address in IPv4. An IPv6 router sends Internet Control Message Protocol version 6 (ICMPv6) RA messages to the all-node multicast group. The RA message informs all IPv6-enabled devices on the network about addressing information, such as the prefix, prefix length, and default gateway.
- **FF02::2 All-routers multicast group:** This is a multicast group that all IPv6 routers join. A router becomes a member of this group when it is enabled as an IPv6 router with the **ipv6 unicast-routing** global configuration command. A packet sent to this group is received and processed by all IPv6 routers on the link or network.

IPv6-enabled devices send ICMPv6 Router Solicitation (RS) messages to the all- routers multicast address. The RS message requests an RA message from the IPv6 router to assist the device in its address configuration.

Solicited-Node IPv6 Multicast Addresses (8.2.5.2)

A solicited-node multicast is similar to the all-nodes multicast address. Recall that the all-nodes multicast address is essentially the same thing as an IPv4 broadcast. All devices on the network must process traffic sent to the all-nodes address. To reduce the number of devices that must process traffic, use a solicited-node multicast address.

A solicited-node multicast address is an address that matches only the last 24 bits of the IPv6 global unicast address of a device. The only devices that need to process these packets are those devices that have these same 24 bits in the least significant, far right portion of their interface ID.

An IPv6 solicited-node multicast address is automatically created when the global unicast or link-local unicast addresses are assigned. The IPv6 solicited-node multicast address is created by combining a special FF02:0:0:0:0:FF00::/104 prefix with the far right 24 bits of its unicast address.

The solicited-node multicast address consists of two parts:

- **FF02:0:0:0:0:FF00::/104 multicast prefix:** This is the first 104 bits of the solicited-node multicast address.
- **Least significant 24 bits:** These are the last or far right 24 bits of the solicited-node multicast address. These bits are copied from the far right 24 bits of the global unicast or link-local unicast address of the device.

It is possible that multiple devices will have the same solicited-node multicast address. Although rare, this can occur when devices have the same far right 24 bits in their interface IDs. This does not create any problems because the device will still process the encapsulated message, which will include the complete IPv6 address of the device in question.

Packet Tracer □ Activity

Packet Tracer Activity 8.2.5.3: Configuring IPv6 Addressing

In this activity, you will practice configuring IPv6 addresses on a router, servers, and clients. You will also practice verifying your IPv6 addressing implementation.

Lab 8.2.5.4: Identifying IPv6 Addresses

In this lab, you will complete the following objectives:

- Part 1: Identify the Different Types of IPv6 Addresses
- Part 2: Examine a Host IPv6 Network Interface and Address
- Part 3: Practice IPv6 Address Abbreviation
- Part 4: Identify the Hierarchy of the IPv6 Global Unicast Address Network Prefix

Lab 8.2.5.5: Configuring IPv6 Addresses on Network Devices

In this lab, you will complete the following objectives:

- Part 1: Set Up Topology and Configure Basic Router and Switch Settings
- Part 2: Configure IPv6 Addresses Manually
- Part 3: Verify End-to-End Connectivity

Connectivity Verification (8.3)

This section will introduce verifying IPv6 connectivity.

ICMP (8.3.1)

Both IPv4 and IPv6 use an ICMP protocol as the principal means to verify connectivity. This section will introduce the use of ICMP in IPv4 and IPv6.

ICMPv4 and ICMPv6 Messages (8.3.1.1)

Although IP is not a reliable protocol, the TCP/IP suite does provide for messages to be sent in the event of certain errors. These messages are sent using the services of ICMP. The purpose of these messages is to provide feedback about issues related to the processing of IP packets under certain conditions, not to make IP reliable. ICMP messages are not required and are often not allowed within a network for security reasons.

ICMP is available for both IPv4 and IPv6. ICMPv4 is the messaging protocol for IPv4. ICMPv6 provides these same services for IPv6 but includes additional functionality. In this course, the term ICMP will be used when referring to both ICMPv4 and ICMPv6.

The types of ICMP messages, and the reasons why they are sent, are extensive. We will discuss some of the more common messages.

ICMP messages common to both ICMPv4 and ICMPv6 include

- Host confirmation
- Destination or Service Unreachable
- Time Exceeded
- Route redirection

Host Confirmation

An ICMP Echo message can be used to determine whether a host is operational. The local host sends an ICMP Echo Request to a host. If the host is available, the destination host responds with an Echo Reply. In Figure 8-18, an ICMP Echo Request is sent from H1 to H2. When H2 receives the ICMP packet, it responds with an ICMP Echo Reply. This use of the ICMP Echo messages is the basis of the ping utility.

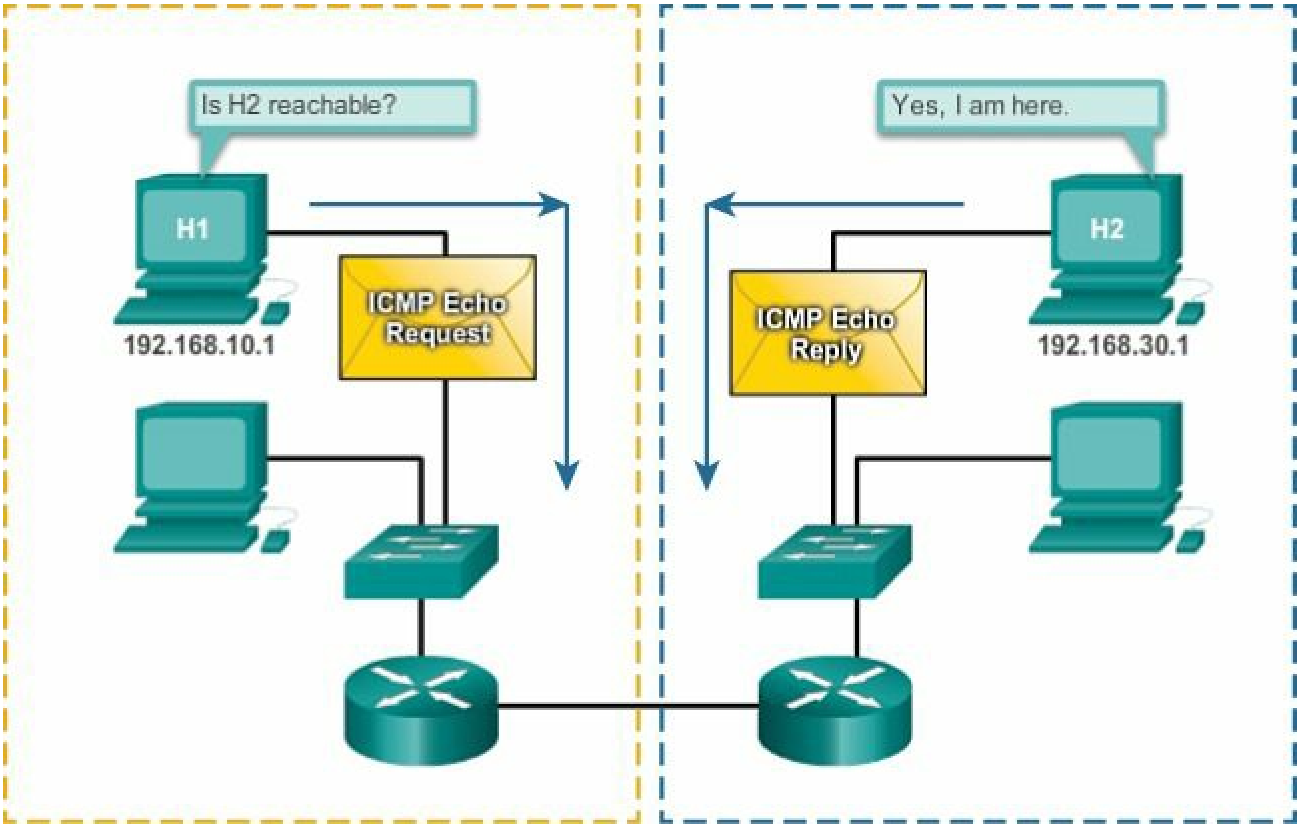


Figure 8-18 ICMP Echo Request and Reply

Destination or Service Unreachable

When a host or gateway receives a packet that it cannot deliver, it can use an ICMP Destination Unreachable message to notify the source that the destination or service is unreachable. The message will include a code that indicates why the packet could not be delivered.

Some of the Destination Unreachable codes for ICMPv4 are

- 0: Net unreachable
- 1: Host unreachable
- 2: Protocol unreachable
- 3: Port unreachable

Note

ICMPv6 has similar but slightly different codes for Destination Unreachable messages.

Time Exceeded

An ICMPv4 Time Exceeded message is used by a router to indicate that a packet cannot be forwarded because the Time to Live (TTL) field of the packet was decremented to 0. If a router receives a packet and decrements the TTL field in the IPv4 packet to 0, it discards the packet and sends a Time Exceeded message to the source host.

ICMPv6 also sends a Time Exceeded message if the router cannot forward an IPv6 packet because the packet has expired. IPv6 does not have a TTL field; it uses the hop limit field to determine whether the packet has expired.

Route Redirection

A router can use the ICMP Redirect message to notify the hosts on a network that a better route is available for a particular destination. This message can only be used when the source host is on the same physical network as both gateways.

Both ICMPv4 and ICMPv6 use route redirection messages.

ICMPv6 Router Solicitation and Router Advertisement Messages (8.3.1.2)

The informational and error messages found in ICMPv6 are very similar to the control and error messages implemented by ICMPv4. However, ICMPv6 has new features and improved functionality not found in ICMPv4.

ICMPv6 includes four new protocols as part of the Neighbor Discovery Protocol (ND or NDP):

- Router Solicitation message
- Router Advertisement message
- Neighbor Solicitation message
- Neighbor Advertisement message

Router Solicitation and Router Advertisement Messages

IPv6-enabled devices can be divided into two categories: routers and hosts. Router Solicitation and Router Advertisement messages are sent between hosts and routers:

- **Router Solicitation (RS) message:** When a host is configured to obtain its addressing information automatically using Stateless Address Autoconfiguration (SLAAC), the host will send an RS message to the router. The RS message is sent as an IPv6 all-routers multicast message.
- **Router Advertisement (RA) message:** RA messages are sent by routers to provide addressing information to hosts using SLAAC. The RA message can include addressing information for the host such as the prefix and prefix length. A router will send an RA message periodically or in response to an RS message. By default, Cisco routers send RA messages every 200 seconds. RA messages are sent to the IPv6 all-nodes multicast address. A host using SLAAC will set its default gateway to the link-local address of the router that sent the RA.

ICMPv6 Neighbor Solicitation and Neighbor Advertisement Messages (8.3.1.3)

ICMPv6 Neighbor Discovery Protocol includes two additional message types, Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages.

Neighbor Solicitation and Neighbor Advertisement messages are used for

- Address resolution
- Duplicate Address Detection (DAD)

Address Resolution

Address resolution is used when a device on the LAN knows the IPv6 unicast address of a destination but does not know its Ethernet MAC address. To determine the MAC address for the destination, the device will send an NS message to the solicited-node address. The message will include the known (targeted) IPv6 address. The device that has the targeted IPv6 address will respond with an NA message containing its Ethernet MAC address.

Duplicate Address Detection

When a device is assigned a global unicast or link-local unicast address, it is recommended that DAD is performed on the address to ensure that it is unique. To check the uniqueness of an address, the device will send an NS message with its own IPv6 address as the targeted IPv6 address. If another device on the network has this address, it will respond with an NA message. This NA message will notify the sending device that the address is in use. If a corresponding NA message is not returned within a certain period of time, the unicast address is unique and acceptable for use.

Note

DAD is not required, but RFC 4861 recommends that DAD be performed on unicast addresses.

Testing and Verification (8.3.2)

This section will introduce the use of the ping and traceroute utilities for testing networks.

Ping: Testing the Local Stack (8.3.2.1)

Ping is a testing utility that uses ICMP Echo Request and Echo Reply messages to test connectivity between hosts. Ping works with both IPv4 and IPv6 hosts.

To test connectivity to another host on a network, an Echo Request is sent to the host address using the **ping** command. If the host at the specified address receives the Echo Request, it responds with an Echo Reply. As each Echo Reply is received, ping provides feedback on the time between when the request was sent and when the reply was received. This can be a measure of network performance.

Ping has a timeout value for the reply. If a reply is not received within the timeout, ping provides a message indicating that a response was not received. This usually indicates that there is a problem, but could also indicate that security features blocking ping messages have been enabled on the network.

After all the requests are sent, the ping utility provides a summary that includes the success rate and average round-trip time to the destination.

Pinging the Local Loopback

There are some special testing and verification cases for which we can use ping. One case is for testing the internal configuration of IPv4 or IPv6 on the local host. To perform this test, we ping the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6).

A response from 127.0.0.1 for IPv4, or ::1 for IPv6, indicates that IP is properly installed on the host. This response comes from the network layer. This response is not, however, an indication that the addresses, masks, or gateways are properly configured. Nor does it indicate anything about the status of the lower layer of the network stack. This simply tests IP down through the network layer of IP. If we get an error message, it is an indication that TCP/IP is not operational on the host.

Ping: Testing Connectivity to the Local LAN (8.3.2.2)

You can also use ping to test the ability of a host to communicate on the local network. This is generally done by pinging the IP address of the gateway of the host. A ping to the gateway indicates that the host and the router interface serving as the gateway are both operational on the local network.

For this test, the gateway address is most often used, because the router is normally always operational. If the gateway address does not respond, a ping can be sent to the IP address of another host on the local network that is known to be operational.

If either the gateway or another host responds, the local host can successfully communicate over the local network. If the gateway does not respond but another host does, this could indicate a problem with the router interface serving as the gateway.

One possibility is that the wrong gateway address has been configured on the host. Another possibility is that the router interface might be fully operational but has security applied to it that prevents it from processing or responding to ping requests.

Ping: Testing Connectivity to Remote (8.3.2.3)

Ping can also be used to test the ability of a local host to communicate across an internetwork. The local host can ping an operational IPv4 host of a remote network.

If this ping is successful, the operation of a large piece of the internetwork can be verified. A successful ping across the internetwork confirms communication on the local network, the operation of the router serving as our gateway, and the operation of all other routers that might be in the path between the local network and the network of the remote host.

Additionally, functionality of the remote host can be verified. If the remote host could not communicate outside of its local network, it would not have responded.

Note

Many network administrators limit or prohibit the entry of ICMP messages into the corporate network; therefore, the lack of a ping response could be due to security restrictions.

Traceroute: Testing the Path (8.3.2.4)

Ping is used to test connectivity between two hosts, but does not provide information about the details of devices between the hosts. Traceroute (tracert) is a utility that generates a list of hops that were successfully reached along the path. This list can provide important verification and troubleshooting information. If the data reaches the destination, the trace lists the interface of every router in the path between the hosts. If the data fails at some hop along the way, the address of the last router that responded to the trace can provide an indication of where the problem or security restrictions are found.

Round-Trip Time (RTT)

Using traceroute provides ***round-trip time (RTT)*** for each hop along the path and indicates whether a hop fails to respond. The round-trip time is the time a packet takes to reach the remote host and for the response from the host to return. An asterisk (*) is used to indicate a lost or unreplied packet.

This information can be used to locate a problematic router in the path. If the display shows high response times or data losses from a particular hop, this is an indication that the resources of the router or its connections might be stressed.

IPv4 Time-to-Live (TTL) and IPv6 Hop Limit

Traceroute makes use of a function of the TTL field in IPv4 and the Hop Limit field in IPv6 in the Layer 3 headers, along with the ICMP Time Exceeded message.

Figure 8-19 and Example 8-8 show how traceroute takes advantage of TTL.

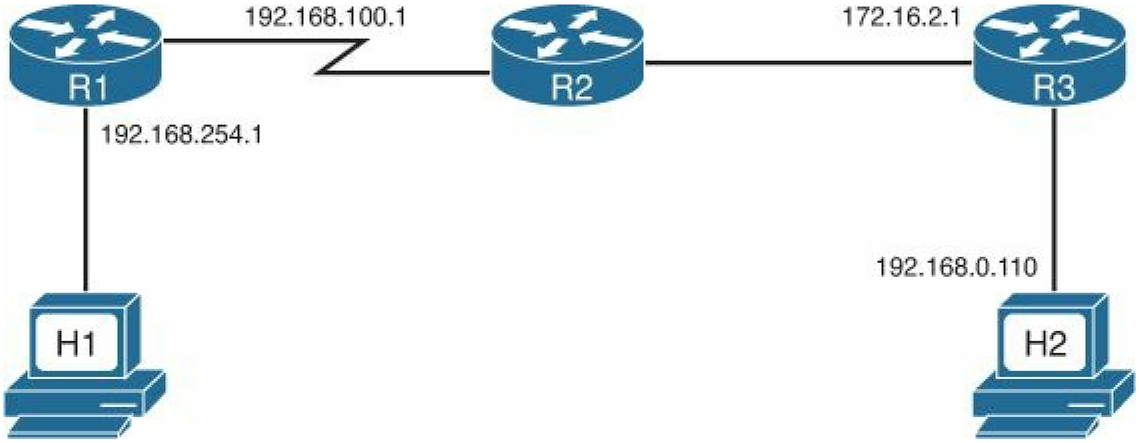


Figure 8-19 Example Network for Traceroute

The first sequence of three messages sent from traceroute on H1 to H2 will have a TTL field value of 1. When this packet reaches R1, the TTL is decremented to 0. This causes the TTL to time-out the IPv4 packet at this first router. This router then responds with an ICMPv4 Time Exceeded message. The ICMPv4 message contains the address of the inbound interface of the first router. Traceroute now has the address of the first hop, 192.168.254.1, as well as the amount of time for the round trips (2 msec, 2 msec, 2 msec).

Traceroute then increments the TTL field to 2 and sends another sequence of three messages. As the message passes through R1, it will be decremented to 1. This allows the message to be forwarded by R1 to reach the next router, R2, before expiring. This provides the trace with the address of the next hop, R2, as well at the round-trip time (99 msec, 95 msec, 94 msec).

Traceroute on H1 then increments the TTL field to 3 to allow the packet to get one hop farther down the path toward H2. This sequence of messages reaches R3 before the timeout of the TTL. The ICMP Time Exceeded reply from R3 provides information about R3.

With the TTL now incremented to 4, the traceroute packets reach the destination of 192.168.0.110 (H2). H2 then responds with either an ICMP Port Unreachable message or an ICMP Echo Reply message instead of the ICMP Time Exceeded message.

Example 8-8 Traceroute Example Output

Click here to view code image

```
C:\H1\Users> tracert 192.168.0.110

Tracing route to 192.168.0.110 over a maximum of 30 hops

 1      2 ms      2 ms      2 ms  192.168.254.1
 2     99 ms     95 ms     94 ms  192.168.100.1
 3     98 ms     93 ms     94 ms  172.16.2.1
 4     98 ms     93 ms     94 ms  192.168.0.110
Trace complete.
```

Packet Tracer ☐ Activity **Packet Tracer Activity 8.3.2.5: Verifying IPv4 and IPv6 Addressing**

IPv4 and IPv6 can coexist on the same network. From the command prompt of a PC, there are some differences in the way that commands are issued and in the way that output is displayed.

Packet Tracer Activity 8.3.2.6: Pinging and Tracing to Test the Path

There are connectivity issues in this activity. In addition to gathering and documenting information about the network, you will locate the problems and implement acceptable solutions to restore connectivity.

Lab 8.3.2.7: Testing Network Connectivity with Ping and Traceroute

In this lab, you will complete the following objectives:

- Part 1: Build and Configure the Network
- Part 2: Use the Ping Command for Basic Network Testing
- Part 3: Use the Tracert and Traceroute Commands for Basic Network Testing
- Part 4: Troubleshoot the Topology

Packet Tracer Activity 8.3.2.8: Troubleshooting IPv4 and IPv6 Addressing

You are a network technician working for a company that has decided to migrate from IPv4 to IPv6. In the interim, the company must support both protocols (dual-stack). Three coworkers have called the help desk with problems and have received limited assistance. The help desk has escalated the matter to you, a Level 2 support technician.

Summary (8.4)

Class Activity 8.4.1.1: The Internet of Everything . . . Naturally!

In this chapter, you learned about how small- to medium-sized businesses are connected to networks in groups. The Internet of Everything was also introduced in the beginning modeling activity.

For this activity, choose one of the following:

- Online banking
- World news
- Weather forecasting/climate
- Traffic conditions

Devise an IPv6 addressing scheme for the area you chose. Include in your addressing scheme how you would plan for

- Subnetting
- Unicasts
- Multicasts
- Broadcasts

Keep a copy of your scheme to share with the class or learning community. Be prepared to explain

- How subnetting, unicasts, multicasts and broadcasts would be incorporated
- Where your addressing scheme could be used
- How small- to medium-sized businesses would be impacted by using your plan

Packet Tracer Activity

Packet Tracer Activity 8.4.1.2: Skills Integration Challenge

Your company has won a contract to set up a small network for a restaurant owner. There are two restaurants near each other, and they all share one connection. The equipment and cabling are installed, and the network administrator has designed the implementation plan. You job is to implement the rest of the addressing scheme according to the abbreviated addressing table and verify connectivity.

IP addresses are hierarchical, with network, subnetwork, and host portions. An IP address can represent a complete network, a specific host, or the broadcast address of the network.

Understanding binary notation is important when determining whether two hosts are in the same network. The bits within the network portion of the IP address must be identical for all devices that reside in the same network. The subnet mask or prefix is used to determine the network portion of an IP address. IP addresses can be assigned either statically or dynamically. DHCP enables the automatic assignment of addressing information such as IP address, subnet mask, default gateway, and other configuration information.

IPv4 hosts can communicate in one of three different ways: unicast, broadcast, and multicast. Also, blocks of addresses that are used in networks that require limited or no Internet access are called private addresses. The private IPv4 address blocks are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.

The depletion of IPv4 address space is the motivating factor for moving to IPv6. Each IPv6 address has 128 bits versus the 32 bits in an IPv4 address. IPv6 does not use the dotted-decimal subnet mask notation. The prefix length is used to indicate the network portion of an IPv6 address using the following format: IPv6 address/prefix length.

There are three types of IPv6 addresses: unicast, multicast, and anycast. An IPv6 link-local address enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet). Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated. IPv6 link-local addresses are in the FE80::/10 range.

ICMP is available for both IPv4 and IPv6. ICMPv4 is the messaging protocol for IPv4. ICMPv6 provides the same services for IPv6 but includes additional functionality.

After it is implemented, an IP network needs to be tested to verify its connectivity and operational performance.

Practice

The following activities provide practice with the topics introduced in this chapter. The labs and class activities are available in the companion *Introduction to Networks Lab Manual* (ISBN 978-1-58713-312-1). The Packet Tracer Activities PKA files are found in the online course.

Class Activities

- Class Activity 8.0.1.2: The Internet of Everything (IoE)
- Class Activity 8.4.1.2: The Internet of Everything . . . Naturally!

Labs

- Lab 8.1.2.7: Using the Windows Calculator with Network Addresses
- Lab 8.1.2.8: Converting IPv4 Addresses to Binary
- Lab 8.1.4.8: Identifying IPv4 Addresses
- Lab 8.2.5.4: Identifying IPv6 Addresses
- Lab 8.2.5.5: Configuring IPv6 Addresses on Network Devices
- Lab 8.3.2.7: Testing Network Connectivity with Ping and Traceroute

Packet Tracer Activities

Packet Tracer ☐ Activity

- Packet Tracer Activity 8.1.3.8: Investigate Unicast, Broadcast, and Multicast Traffic
- Packet Tracer Activity 8.2.5.3: Configuring IPv6 Addressing
- Packet Tracer Activity 8.3.2.5: Verifying IPv4 and IPv6 Addressing
- Packet Tracer Activity 8.3.2.6: Pinging and Tracing to Test the Path
- Packet Tracer Activity 8.3.2.8: Troubleshooting IPv4 and IPv6 Addressing
- Packet Tracer Activity 8.4.1.2: Skills Integration Challenge

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 Answer Key,” lists the answers.

1. What are the parts of an IPv4 address? (Choose two.)

   A. Host

   B. Network

   C. Next hop

   D. Broadcast

   E. Subnet mask

2. What is the purpose of the network address?

   A. To support communication to all hosts within a subnet

   B. To refer to a network

   C. To provide a gate for hosts in the network

   D. To allow multicast

3. What are characteristics in common among unicast, broadcast, and multicast IPv4 communication? (Choose two.)

   A. The source address is always a unicast address.

   B. There is only one host that receives the packet.

   C. There are never multiple destination addresses in the header.

   D. There are equal numbers of addresses used for each.

   E. All are used for the same purpose.

4. Which of the following addresses IPv4 would be used in a private network?

   A. 240.23.56.12

   B. 192.0.1.12

   C. 127.27.20.10

   D. 192.168.1.1

E. 169.254.72.6

5. What is the principal reason for the development of IPv6?

____

6. How are IPv6 addresses represented?

A. 4 octets separated by periods

B. 64 binary bits with no division

C. 8 hextets separated by colons

D. As an octal number

7. What type of IPv6 address should be used for communication that is limited to a single network segment?

A. Global unicast

B. Link-local

C. Unspecified

D. Unique local

8. What methods automatically provide global unicast addresses? (Choose two.)

A. SLAAC

B. DHCPv6

C. ICMP

D. DAD

E. ANDing

9. Which type of IPv4 address allows a host to send a message to a group of hosts?

A. Unicast

B. Multicast

C. Broadcast

10. What protocol is used in IP networks to verify connectivity?

____

11. What utility is used to identify network path between hosts?

A. DHCP

B. Ping

C. Multicast

D. Traceroute