

## 12.1.6 IPv4 Addressing Facts

This lesson covers the following topics:

- IPv4 rules and concepts
- IPv4 address structure
- Subnet masks
- Classless Inter-Domain Routing (CIDR)
- Address assignment
- Network Address Translation (NAT) routers

### IPv4 Rules and Concepts

IP addresses and routers are responsible for sorting and delivering packets to and from clients on a network. Each packet contains the IP address of both the sender and the recipient. Routers use the IP address to send the packets to the specified destination. IPv4 addresses allow hosts to participate on IPv4-based networks.

The three most important IPv4 address rules are:

- Each host must have a unique IPv4 address.
- Each host on the same logical network must have the same network address.
- Hosts can only communicate directly with other hosts on the same logical network.

The following table describes IPv4 concepts you should be aware of.

Concept	Description
Host	A host (also known as a network host) is a computer or device (such a router) on a network.
IP address	The IP address is a number assigned to identify hosts and other devices on a network.
Network address	The network address (also referred to as the network ID) is the portion of the IP address that identifies a specific network.
Host address	The host address (also referred to as a host ID) is the remaining portion of the IP address that identifies the specific host or other device on the network.
Subnet mask	A subnet mask identifies the portion of the IP address that defines the network address and the portion of the IP address that defines the specific host.
Address class	IPv4 addresses are divided into classes. The address class identifies the range of IPv4 addresses and a default subnet mask used for the range.

Default subnet mask	<p>A default subnet mask is assigned to classes A - C as follows:</p> <ul style="list-style-type: none"> <li>• <b>255.0.0.0</b> is the default subnet mask for class A networks.</li> <li>• <b>255.255.0.0</b> is the default subnet mask for class B networks.</li> <li>• <b>255.255.255.0</b> is the default subnet mask for class C networks.</li> </ul>
Broadcast address	The broadcast address is the last address in the IP address range and is used to send messages to all hosts on the network.
Default gateway	<p>The default gateway is a device that performs routing and enables a host to communicate with hosts on other networks through the routing process.</p> <ul style="list-style-type: none"> <li>• A default gateway address must be configured on each host to allow internetwork communication. Without the default gateway, hosts can only communicate with devices within the same subnet.</li> <li>• The default gateway address must be on the same subnet as the host computer. <ul style="list-style-type: none"> <li>◦ Routers have multiple network interface cards attached to multiple networks.</li> <li>◦ When configuring the default gateway, choose the address on the local subnet.</li> </ul> </li> </ul>

## IP Address Structure

An IPv4 network address is a grouping of four numbers. Each number in the group is separated by a period (referred to as a dot). IPv4 addresses can be represented in the following ways:

- **Decimal notation:**

In decimal notation, each of the four numbers must be between 0 and 255.

Example: 131.107.2.200 (spoken as 137 dot 107 dot 2 dot 200).

- **Binary notation:**

In binary notation, each of the four numbers is an octet (consisting of 8 bits). Each bit is either a 1 or a 0.

Example: 10000011.01101011.00000010.11001000

On occasion, such as when working with subnet masks, you may need to convert an IP address from a binary value to decimal (or vice versa). Therefore, it is important to understand that each bit position in a binary octet is assigned a decimal value, as shown in the following table:

8-Bit Octet
-------------

Bit Position	7	6	5	4	3	2	1	0
Decimal Value	128	64	32	16	8	4	2	1

To convert from binary to decimal, add the decimal equivalent for each bit position containing the binary value of 1.

For example, the decimal equivalent of 10010101 is  $128 + 16 + 4 + 1 = 149$ . This concept is sometimes easier to see in a table:

Decimal value for each bit	128	64	32	16	8	4	2	1
Binary value for each bit	1	0	0	1	0	1	0	1
Decimal values	128 + 16 + 4 + 1 = 149							

## Subnet Masks

A subnet mask identifies which portion of the IP address represents the network and, consequentially, which portion represents the host address. The structure of a subnet mask is identical to that of an IP address.

- In binary form, the subnet mask is always a series of 1s followed by a series of 0s (1s and 0s are never mixed in sequence in the mask).
- In decimal, each number used to indicate that it is part of the network will be the value of 255. For example, 255.255.255.0 means that the first three numbers (octets) are reserved for the network portion of an IP address.

When using complex subnet masks, the last number of the network portion may be any number as long as that number converted to binary is made of all 1s followed by all 0s. For example, a decimal subnet mask of 255.255.255.240 converted to binary is 11111111.11111111.11111111.11110000. In this address, the first four bits of the last octet are part of the network address.

## Classless Inter-Domain Routing (CIDR)

Classless Inter-Domain Routing (CIDR) is a method by which all of the bits used for the subnet mask are written in a single decimal number. For example, when an IP address is written as 10.10.1.16 /16, the "/16" is the CIDR. The /16 indicates that the first two octets (8-bits + 8-bit = /16) are used for the network address.

CIDR notation is most useful when one of the network octets does not comprise the entire octet. For example, when an IP address is written as 10.10.1.16 /18, the "/18" indicates that part of the third octet is used as part of the network address (8-bits + 8-bit + 2-bit = /18).

The following table shows the default address class for each IPv4 address range with its default subnet mask (also represented in CIDR notation).

Class	Address range	First octet range	Default subnet mask	CIDR notation
A	1.0.0.0 to 126.255.255.255	1-126 (00000001--01111110 binary)	255.0.0.0	/8
B	128.0.0.0 to 191.255.255.255	128-191 (10000000--10111111 binary)	255.255.0.0	/16
C	192.0.0.0 to 223.255.255.255	192-223 (11000000--11011111 binary)	255.255.255.0	/24
D	224.0.0.0 to 239.255.255.255	224-239 (11100000--11101111 binary)	n/a	n/a
E	240.0.0.0 to 255.255.255.255	240-255 (11110000--11111111 binary)	n/a	n/a

When using CIDR notation, you must know how to find your subnet mask. When you find the subnet mask, you will know what bits are available for the network address. To convert a CIDR to a subnet mask, use the following steps:

1. If the CIDR is greater than or equal to 8, write 255 in the first available octet (on the left) and then subtract 8 from the CIDR.
2. Repeat step 1 until the number is less than 8. The octets found using these first two steps will be the first part of your subnet mask.
3. Convert the remaining number (which will be less than eight) to 1s and pad the remaining bits (up to 8) with 0. This will be the last octet in your subnet mask.

Examples: If the remaining number is:

- 3 the converted number is written as 11100000
- 5 the converted number is written as 11111000
- 7 the converted number is written as 11111110

4. Convert the 1s in the last (interesting) octet to a decimal number. This number is the subnet mask for this octet.

Examples:

- 11100000 = 224
- 11111000 = 248
- 11111110 = 254

5. Any unused octets are represented with a 0.



CIDR conversion example: IP address /CIDR = 196.200.45.5 /20

1. Find simple subnet mask octets:
  - a.  $12 - 8 = 4$ . 4 is less than 8. Therefore, move to the next step.
2. The number 4 is changed to four 1s with the remaining bits for this octet padded with 0s:  
11110000
3. As a result, the full subnet mask is 255.255.240.0..

## Address Assignment

The following table describes options for assigning IPv4 addresses and other IPv4 configuration values.

Method	
Dynamic Host Configuration Protocol (DHCP)	<p>DHCP is a method used to automatically assign IPv4 addresses and other TCP/IPv4 configuration parameters to hosts. Client computers contact a DHCP server to receive TCP/IPv4 configuration information.</p> <p>Use DHCP:</p> <ul style="list-style-type: none"> <li>• For small, medium, or large networks.</li> <li>• For automatic host configuration.</li> <li>• To automatically deliver additional configuration parameters such as default gateway and DNS servers.</li> </ul> <p>By default, all Windows computers try to use DHCP for TCP/IPv4 configuration information.</p>
Automatic Private IPv4 Addressing (APIPA)	<p>APIPA is an automatic configuration method where hosts automatically select their own IPv4 address within a specific range.</p> <p>When using APIPA:</p> <ul style="list-style-type: none"> <li>• Windows computers will use APIPA if a DHCP server cannot be contacted.</li> <li>• Hosts select an IPv4 address in the 169.254.0.1 to 169.254.255.255 range with a mask of 255.255.0.0. After choosing the address, the host verifies that no other host on the network is using the selected address.</li> <li>• APIPA sets only the IPv4 address and mask. Because it does not assign a default gateway, APIPA can be used on a single subnet, but cannot be used if communication with other subnets is required.</li> </ul>

	Use APIPA for small single-subnet networks that do not use DNS servers or do not have internet or connectivity outside of the local subnet.
Static (manual) assignment	<p>Static/manual IPv4 address assignment means that you manually enter in the required IPv4 address and associated IP information for a host.</p> <ul style="list-style-type: none"> <li>• When you configure a static IPv4 address, you must also configure the subnet mask and default gateway.</li> <li>• When you configure a static IPv4 address, you disable DHCP and APIPA.</li> <li>• If you use DHCP, you can also assign DNS server addresses manually.</li> </ul> <p>Use static addressing:</p> <ul style="list-style-type: none"> <li>• For small networks that do not often change or grow.</li> <li>• If your network does not have a DHCP server or if you want to eliminate DHCP traffic from your network.</li> <li>• For specific hosts that must have the same address each time (such as servers). You can use DHCP on the rest of the network and use static addressing for only a few hosts. However, before you use static addressing, explore the possibility of using a DHCP server to assign the same IPv4 address to specific hosts each time an address is requested.</li> <li>• For non-DHCP hosts (hosts that cannot accept an IPv4 address from DHCP).</li> </ul> <div>  Ensure that duplicate addresses are not assigned to hosts on the same network.         </div>
Alternate IPv4 configuration	<p>When an alternate IPv4 configuration is enabled, the host attempts to use DHCP for TCP/IPv4 configuration information. If a DHCP server cannot be contacted, the alternate IPv4 values are used.</p> <p>Use an alternate configuration:</p> <ul style="list-style-type: none"> <li>• For computers (such as a laptop) that connect to two networks; one with a DHCP server and another without a DHCP server.</li> <li>• To provide values to properly configure the computer in the event that the DHCP server is unavailable.</li> </ul> <div>  When you configure an alternate IPv4 address, APIPA will never be used.         </div>

## Network Address Translation (NAT) Routers

A Network Address Translation (NAT) router translates multiple private addresses into the single registered IP address.

- The internet is classified as a public network. All devices on the public network must have a unique registered IP address. This address is assigned by the ISP. No two hosts on a public network can have the same IP address.
- The internal network is classified as a private network. All devices on the private network use private IP addresses internally, but share the public IP address when accessing the internet.
- A NAT router associates a port number with each private IP address. Port assignments are made automatically by the NAT router. Communications from the internet are sent to the public IP address. The NAT router translates the public IP address into the private IP address of the host.
- A private network can use addresses in the following ranges that have been reserved for private use by IANA:
  - 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 to 192.168.255.255



By default, internet routers are configured not to route private IP addresses.

---

**Copyright © 2022 TestOut Corporation All rights reserved.**