CCNA 1 v7.0 Curriculum: Module 11 – IPv4 Addressing

April 1, 2020

11.0. Introduction

11.0.1. Why should I take this module?

Welcome to IPv4 Addressing!

Currently, there are still plenty of networks using IPv4 addressing, even as the organizations which use them are making the transition to IPv6. So it is still very important for network administrators to know everything they can about IPv4 addressing. This module covers the fundamental aspects of IPv4 addressing in detail. It includes how to segment a network into subnets and how to create a variable-length subnet mask (VLSM) as part of an overall IPv4 addressing scheme. Subnetting is like cutting a pie into smaller and smaller pieces. Subnetting may seem overwhelming at first, but we show you some tricks to help you along the way. This module includes several videos, activities to help you practice subnetting, Packet Tracers and a lab. Once you get the hang of it, you'll be on your way to network administration!

11.0.2. What will I learn to do in this module?

Module Title: IPv4 Addressing

Module Objective: Calculate an IPv4 subnetting scheme to efficiently segment your network.

Topic Title	Topic Objective
IPv4 Address Structure	Describe the structure of an IPv4 address including the network portion, the host portion, and the subnet mask.
IPv4 Unicast, Broadcast, and Multicast	Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses.
Types of IPv4 Addresses	Explain public, private, and reserved IPv4 addresses.
Network Segmentation	Explain how subnetting segments a network to enable better communication.
Subnet an IPv4 Network	Calculate IPv4 subnets for a /24 prefix.

Topic Title	Topic Objective
Subnet a /16 and a /8 Prefix	Calculate IPv4 subnets for a /16 and /8 prefix.
Subnet To Meet Requirements	Given a set of requirements for subnetting, implement an IPv4 addressing scheme.
Variable Length Subnet Masking	Explain how to create a flexible addressing scheme using variable length subnet masking (VLSM).
Structured Design	Implement a VLSM addressing scheme.

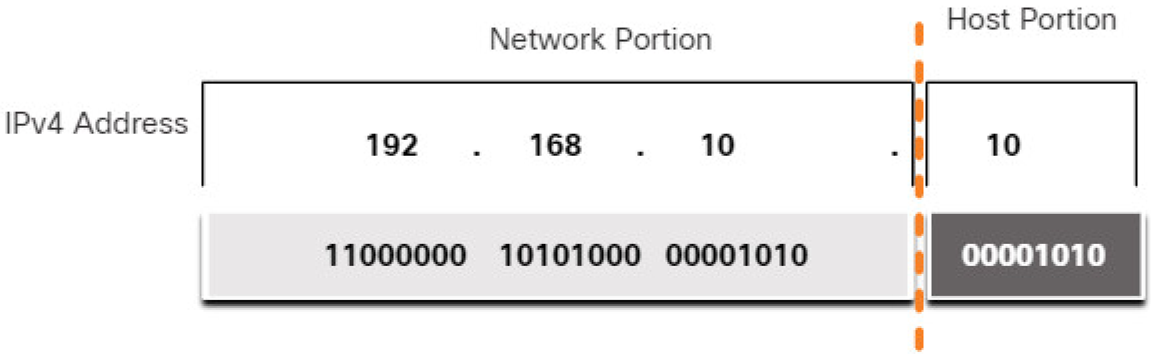
11.1. IPv4 Address Structure

11.1.1. Network and Host Portions

An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion. When determining the network portion versus the host portion, you must look at the 32-bit stream, as shown in the figure.

The diagram shows the breakdown of an IPv4 address into the network and host portions. The IPv4 address is 192.168.10.10. Underneath, the address is converted into 11000000 10101000 00001010 00001010. A dashed line shows the separation between the network and host portions. This occurs after the third octet and the 24th bit.

IPv4 Address



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.

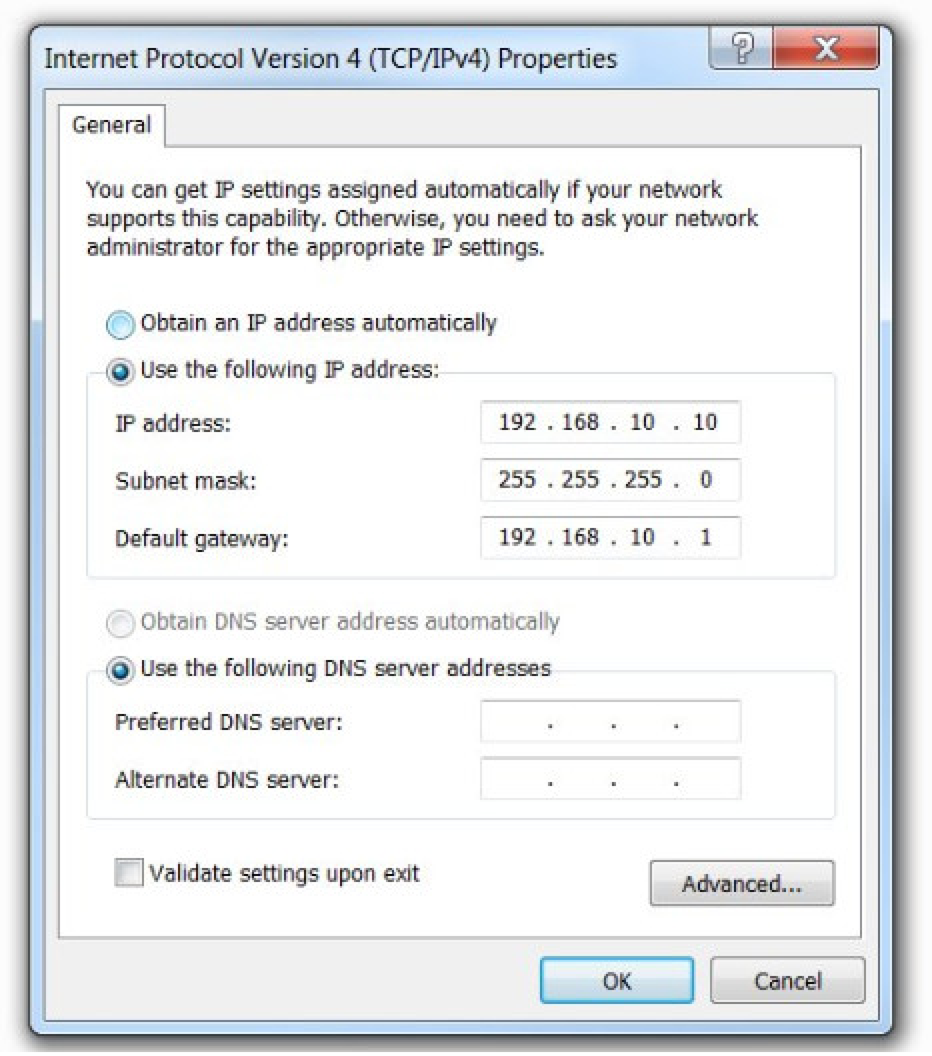
But how do hosts know which portion of the 32-bits identifies the network and which identifies the host? That is the role of the subnet mask.

11.1.2. The Subnet Mask

As shown in the figure, assigning an IPv4 address to a host requires the following:

- **IPv4 address** – This is the unique IPv4 address of the host.
- **Subnet mask**– This is used to identify the network/host portion of the IPv4 address.

IPv4 Configuration on a Windows Computer



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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 . 10 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 10 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

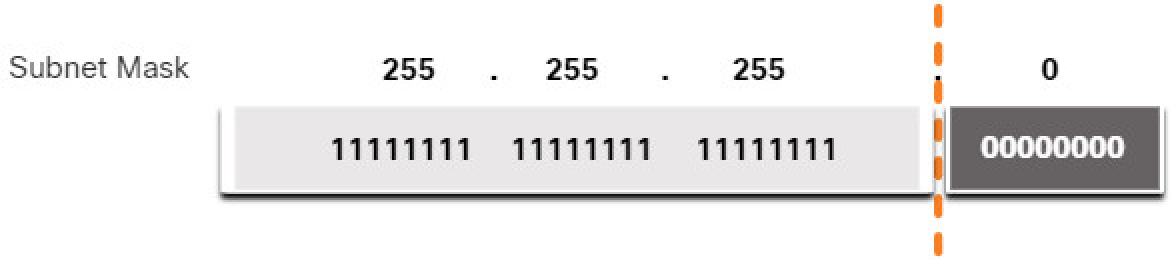
Note: A default gateway IPv4 address is required to reach remote networks and DNS server IPv4 addresses are required to translate domain names to IPv4 addresses.

The IPv4 subnet mask is used to differentiate the network portion from the host portion of an IPv4 address. When an IPv4 address is assigned to a device, the subnet mask is used to determine the network address of the device. The network address represents all the devices on the same network.

The next figure displays the 32-bit subnet mask in dotted decimal and binary formats.

Subnet Mask

subnet mask of 255.255.255.0 on top with the binary representation of 11111111 111111111 11111111 0000000 underneath; a dashed line is drawn after the third octet and the 24th bit

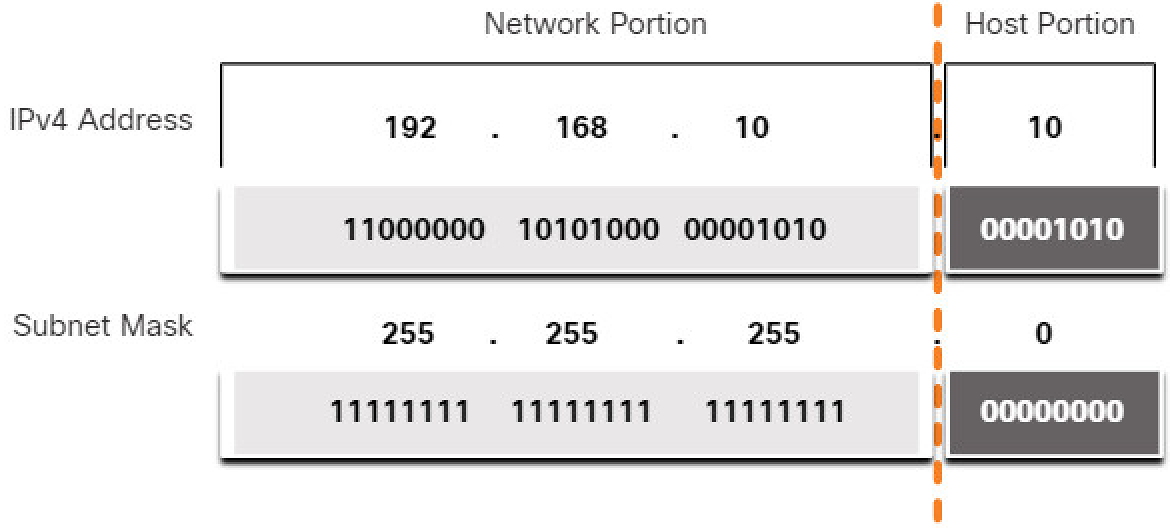


Notice how the subnet mask is a consecutive sequence of 1 bits followed by a consecutive sequence of 0 bits.

To identify the network and host portions of an IPv4 address, the subnet mask is compared to the IPv4 address bit for bit, from left to right as shown in the figure.

Associating an IPv4 Address with its Subnet Mask

The figure shows an IPv4 address, written in both dotted-decimal and binary, with the subnet mask below, also written in dotted-decimal and binary, used to show the division between the network portion and host portion of the address. The IPv4 address is 192.168.10.10 which is converted to 11000000 10101000 00001010 00001010. The subnet mask is 255.255.255.0 which is converted to 11111111 11111111 11111111 00000000. A dashed line shows the separation between the network and host portions. This occurs after the third octet and 24th bit.



Note that 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 the part of the IPv4 address that is the network portion and which part is the host portion.

The actual process used to identify the network portion and host portion is called ANDing.

11.1.3. The Prefix Length

Expressing network addresses and host addresses with the dotted decimal subnet mask address can become cumbersome. Fortunately, there is an alternative method of identifying a subnet mask, a method called the prefix length.

The prefix length is the number of bits set to 1 in the subnet mask. It is written in “slash notation”, which is noted by a forward slash (/) followed by the number of bits set to 1. Therefore, count the number of bits in the subnet mask and prepend it with a slash.

Refer to the table for examples. The first column lists various subnet masks that can be used with a host address. The second column displays the converted 32-bit binary address. The last column displays the resulting prefix length.

Comparing the Subnet Mask and Prefix Length

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	`11111111.00000000.00000000.00000000`	/8
255.255.0.0	`11111111.11111111.00000000.00000000`	/16
255.255.255.0	`11111111.11111111.11111111.00000000`	/24
255.255.255.128	`11111111.11111111.11111111.10000000`	/25
255.255.255.192	`11111111.11111111.11111111.11000000`	/26

Subnet Mask	32-bit Address	Prefix Length
255.255.255.224	`11111111.11111111.11111111.11100000`	/27
255.255.255.240	`11111111.11111111.11111111.11110000`	/28
255.255.255.248	`11111111.11111111.11111111.11111000`	/29
255.255.255.252	`11111111.11111111.11111111.11111100`	/30

Note: A network address is also referred to as a prefix or network prefix. Therefore, the prefix length is the number of 1 bits in the subnet mask.

When representing an IPv4 address using a prefix length, the IPv4 address is written followed by the prefix length with no spaces. For example, 192.168.10.10 255.255.255.0 would be written as 192.168.10.10/24. Using various types of prefix lengths will be discussed later. For now, the focus will be on the /24 (i.e. 255.255.255.0) prefix

11.1.4. Determining the Network: Logical AND

A logical AND is one of three Boolean operations used in Boolean or digital logic. The other two are OR and NOT. The AND operation is used in determining the network address.

Logical AND is the comparison of two bits that produce the results shown below. Note how only a 1 AND 1 produces a 1. Any other combination results in a 0.

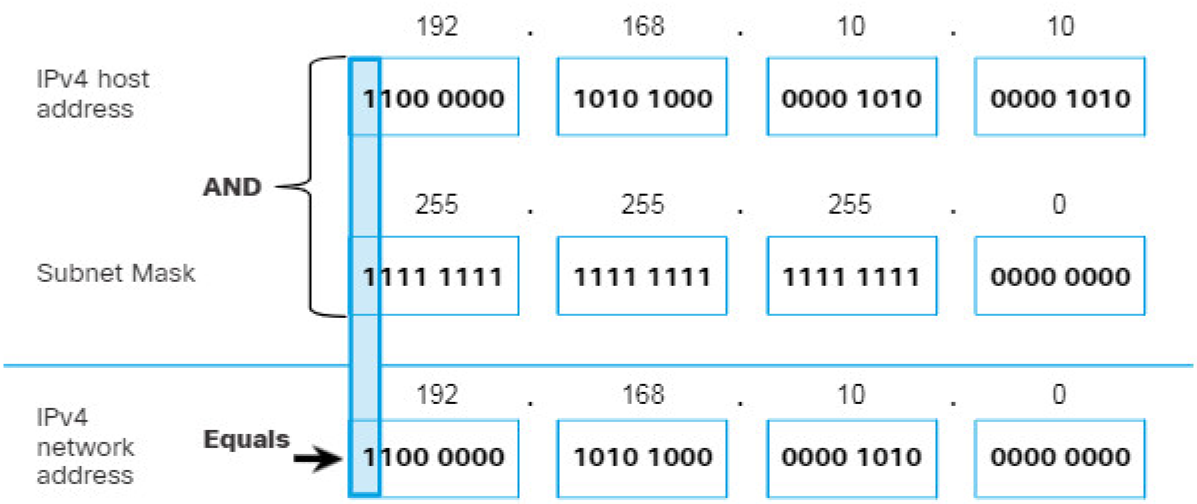
- 1 AND 1 = 1
- 0 AND 1 = 0
- 1 AND 0 = 0
- 0 AND 0 = 0

Note: In digital logic, 1 represents True and 0 represents False. When using an AND operation, both input values must be True (1) for the result to be True (1).

To identify the network address of an IPv4 host, the IPv4 address is logically ANDed, bit by bit, with the subnet mask. ANDing between the address and the subnet mask yields the network address.

To illustrate how AND is used to discover a network address, consider a host with IPv4 address 192.168.10.10 and subnet mask of 255.255.255.0, as shown in the figure:

- **IPv4 host address (192.168.10.10)** – The IPv4 address of the host in dotted decimal and binary formats.
- **Subnet mask (255.255.255.0)** – The subnet mask of the host in dotted decimal and binary formats.
- **Network address (192.168.10.0)** – The logical AND operation between the IPv4 address and subnet mask results in an IPv4 network address shown in dotted decimal and binary formats.



	192	168	10	10
IPv4 host address	1100 0000	1010 1000	0000 1010	0000 1010
	255	255	255	0
Subnet Mask	1111 1111	1111 1111	1111 1111	0000 0000
	192	168	10	0
IPv4 network address	1100 0000	1010 1000	0000 1010	0000 0000

Using the first sequence of bits as an example, notice the AND operation is performed on the 1-bit of the host address with the 1-bit of the subnet mask. This results in a 1 bit for the network address. 1 AND 1 = 1.

The AND operation between an IPv4 host address and subnet mask results in the IPv4 network address for this host. In this example, the AND operation between the host address of 192.168.10.10 and the subnet mask 255.255.255.0 (/24), results in the IPv4 network address of 192.168.10.0/24. This is an important IPv4 operation, as it tells the host what network it belongs to.

11.1.5. Video – Network, Host and Broadcast Addresses

Click Play to view a demonstration of how the network, host, and broadcast addresses are determined for a given IPv4 address and subnet mask.

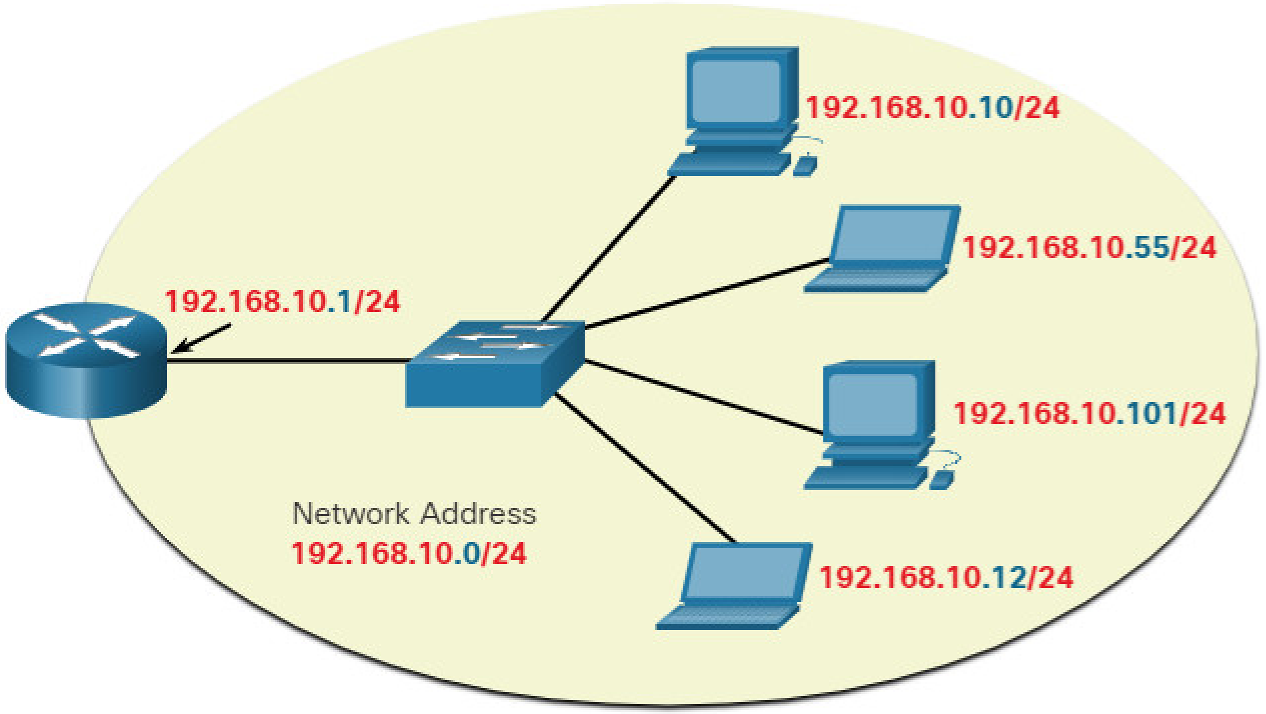
11.1.6. Network, Host, and Broadcast Addresses

Within each network are three types of IP addresses:

- Network address

- Host addresses
- Broadcast address

Using the topology in the figure, these three types of addresses will be examined.



Network address

A network address is an address that represents a specific network. A device belongs to this network if it meets three criteria:

- It has the same subnet mask as the network address.
- It has the same network bits as the network address, as indicated by the subnet mask.
- It is located on the same broadcast domain as other hosts with the same network address.

A host determines its network address by performing an AND operation between its IPv4 address and its subnet mask.

As shown in the table, the network address has all 0 bits in the host portion, as determined by the subnet mask. In this example, the network address is 192.168.10.0/24. A network address cannot be assigned to a device.

Network, Host, and Broadcast Addresses

	Network Portion	Host Portion	Host Bits

	Network Portion	Host Portion	Host Bits

Subnet mask **255.255.255.**0 or **/24**	`255 255 255`
	`11111111 11111111 11111111`
		`0`
		`00000000`	

Network address **192.168.10.**0 or **/24**	`192 168 10`
	`11000000 10100000 00001010`
		`0`
		`00000000`
			All 0s

First address **192.168.10**.1 or **/24**	`192 168 10`
	`11000000 10100000 00001010`
		`1`
		`00000001`
			All 0s and a 1

Last address **192.168.10**.254 or **/24**	`192 168 10`
	`11000000 10100000 00001010`
		`254`
		`11111110`
			All 1s and a 0

Broadcast address **192.168.10**.255 or **/24**	`192 168 10`
	`11000000 10100000 00001010`
		`255`
		`11111111`
			All 1s

Host addresses

Host addresses are addresses that can be assigned to a device such as a host computer, laptop, smart phone, web camera, printer, router, etc. The host portion of the address is the bits indicated by 0 bits in the subnet mask. Host addresses can have any combination of bits in the host portion except for all 0 bits (this would be a network address) or all 1 bits (this would be a broadcast address).

All devices within the same network, must have the same subnet mask and the same network bits. Only the host bits will differ and must be unique.

Notice that in the table, there is a first and last host address:

- **First host address** – This first host within a network has all 0 bits with the last (right-most) bit as a 1 bit. In this example it is 192.168.10.1/24.

- **Last host address** – This last host within a network has all 1 bits with the last (right-most) bit as a 0 bit. In this example it is 192.168.10.254/24.

Any addresses between and including, 192.168.10.1/24 through 192.168.10.254/24 can be assigned to a device on the network.

Broadcast address

A broadcast address is an address that is used when it is required to reach all devices on the IPv4 network. As shown in the table, the network broadcast address has all 1 bits in the host portion, as determined by the subnet mask. In this example, the network address is 192.168.10.255/24. A broadcast address cannot be assigned to a device.

11.1.7. Activity – ANDing to Determine the Network Address

Instructions:

Use the ANDing process to determine the network address (in binary and decimal formats).

Host Address	172	23	163	220
Subnet Mask	255	255	255	192
Host Address in binary	10101100	00010111	10100011	11011100
Subnet Mask in binary	11111111	11111111	11111111	11000000
Network Address in binary	10101100	00010111	10100011	11000000
Network Address in decimal	172	23	163	192

11.2. IPv4 Unicast, Broadcast, and Multicast

11.2.1. Unicast

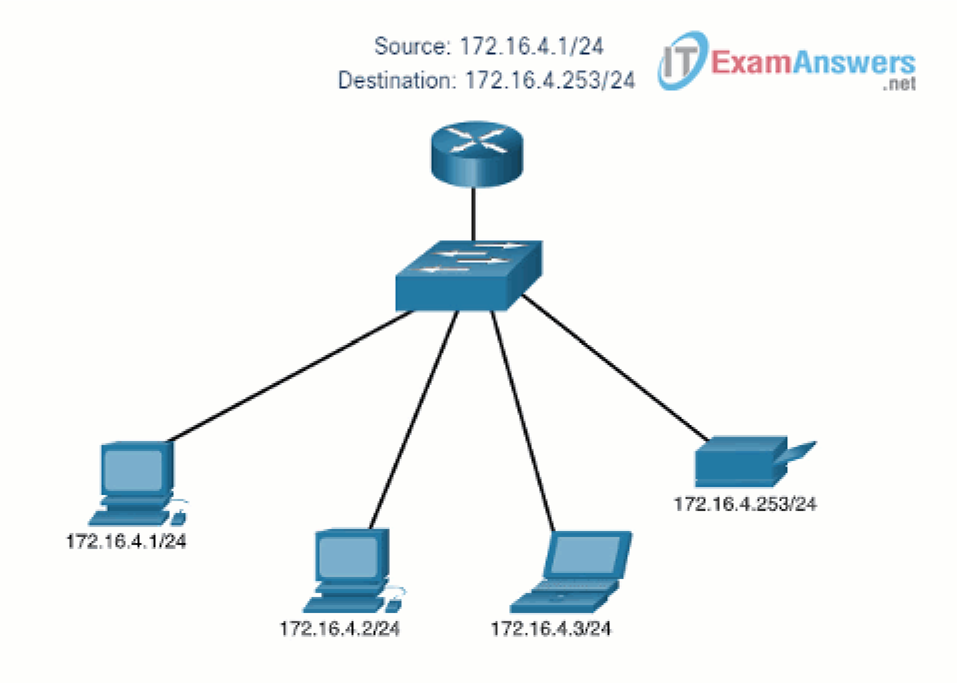
In the previous topic you learned about the structure of an IPv4 address; each has a network portion and a host portion. There are different ways to send a packet from a source device, and these different transmissions affect the destination IPv4 addresses.

Unicast transmission refers to one device sending a message to one other device in one-to-one communications.

A unicast packet has a destination IP address that is a unicast address which goes to a single recipient. A source IP address can only be a unicast address, because the packet can only originate from a single source. This is regardless of whether the destination IP address is a unicast, broadcast or multicast.

The animation to see an example of unicast transmission.

Unicast Transmission



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

IPv4 unicast host addresses are in the address range of 1.1.1.1 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 module.

11.2.2. Broadcast

Broadcast transmission refers to a device sending a message to all the devices on a network in one-to-all communications.

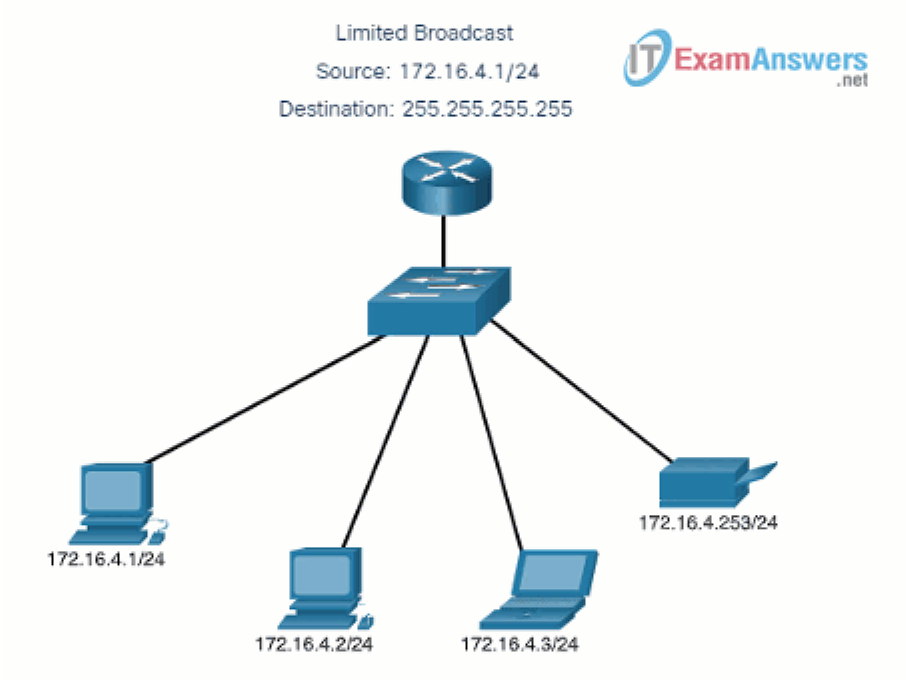
A broadcast packet has a destination IP address with all ones (1s) in the host portion, or 32 one (1) bits.

Note: IPv4 uses broadcast packets. However, there are no broadcast packets with IPv6.

A broadcast packet must be processed by all devices in the same broadcast domain. A broadcast domain identifies all hosts on the same network segment. A broadcast may be directed or limited. A directed broadcast is sent to all hosts on a specific network. For example, a host on the 172.16.4.0/24 network sends a packet to 172.16.4.255. A limited broadcast is sent to 255.255.255.255. By default, routers do not forward broadcasts.

This animation consists of three hosts and a printer connected to a switch and router. The animation illustrates the host with IP address 172.16.4.1 sending a broadcast packet. When the switch receives the broadcast packet, it forwards it out all ports to the other hosts, printer, and router.

Limited Broadcast Transmission



Broadcast packets use resources on the network and make every receiving host on the network process the packet. Therefore, broadcast traffic should be limited so that it does not adversely affect the performance of the network or devices. Because routers separate broadcast domains, subdividing networks can improve network performance by eliminating excessive broadcast traffic.

IP Directed Broadcasts

In addition to the 255.255.255.255 broadcast address, there is a broadcast IPv4 address for each network. Called a directed broadcast, this address uses the highest address in the network, which is the address where all the host bits are 1s. For example, the directed broadcast address for 192.168.1.0/24 is 192.168.1.255. This address allows communication to all the hosts in that network. To send data to all the hosts in a network, a host can send a single packet that is addressed to the broadcast address of the network.

A device that is not directly connected to the destination network forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that network. When a directed broadcast packet reaches a router that is directly connected to the destination network, that packet is broadcast on the destination network.

Note: Because of security concerns and prior abuse from malicious users, directed broadcasts are turned off by default starting with Cisco IOS Release 12.0 with the global configuration command no ip directed-broadcasts.

11.2.3. Multicast

Multicast transmission reduces traffic by allowing a host to send a single packet to a selected set of hosts that subscribe to a multicast group.

A multicast packet is a packet with a destination IP address that is a multicast address. IPv4 has reserved the 224.0.0.0 to 239.255.255.255 addresses as a multicast range.

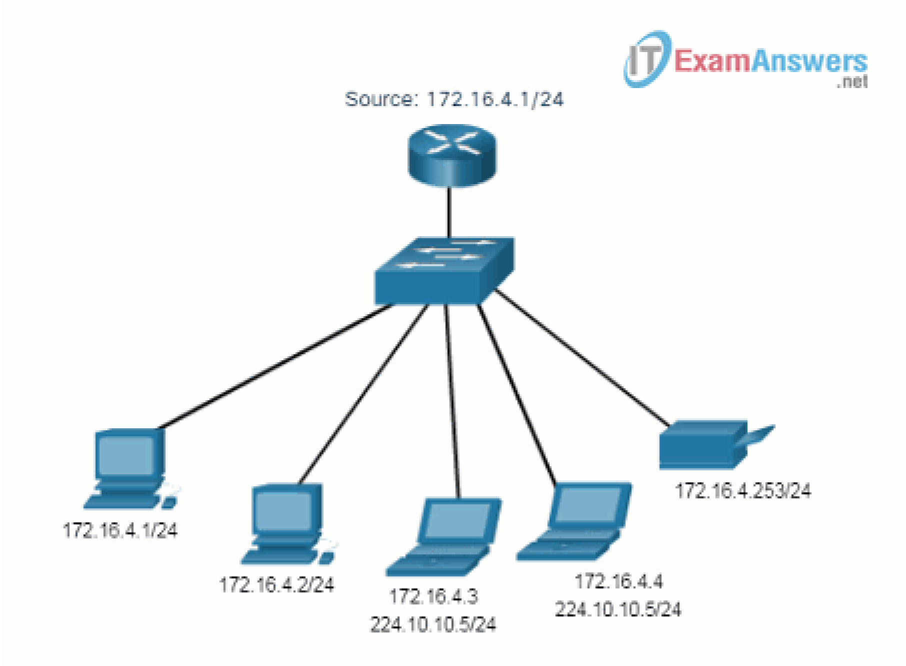
Hosts that receive particular multicast packets are called multicast clients. The multicast clients use services requested by a client program to subscribe to the multicast group.

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, and packets addressed to its uniquely allocated unicast address.

Routing protocols such as OSPF use multicast transmissions. For example, routers enabled with OSPF communicate with each other using the reserved OSPF multicast address 224.0.0.5. Only devices enabled with OSPF will process these packets with 224.0.0.5 as the destination IPv4 address. All other devices will ignore these packets.

The animation demonstrates clients accepting multicast packets.

Multicast Transmission



11.3. Types of IPv4 Addresses

11.3.1. Public and Private IPv4 Addresses

Just as there are different ways to transmit an IPv4 packet, there are also different types of IPv4 addresses. Some IPv4 addresses cannot be used to go out to the internet, and others are specifically allocated for routing to the internet. Some are used to verify a connection and others are self-assigned. As a network administrator, you will eventually become very familiar with the types of IPv4 addresses, but for now, you should at least know what they are and when to use them.

Public IPv4 addresses are addresses which are globally routed between internet service provider (ISP) routers. However, not all available IPv4 addresses can be used on the internet. There are blocks of addresses called private addresses that are used by most organizations to assign IPv4 addresses to internal hosts.

In the mid-1990s, with the introduction of the World Wide Web (WWW), private IPv4 addresses were introduced because of the depletion of IPv4 address space. Private IPv4 addresses are not unique and can be used internally within any network.

Note: The long-term solution to IPv4 address depletion was IPv6.

The Private Address Blocks

Network Address and Prefix	RFC 1918 Private Address Range
10.0.0.0/8	10.0.0.0 – 10.255.255.255
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

Note: Private addresses are defined in RFC 1918 and sometimes referred to as RFC 1918 address space.

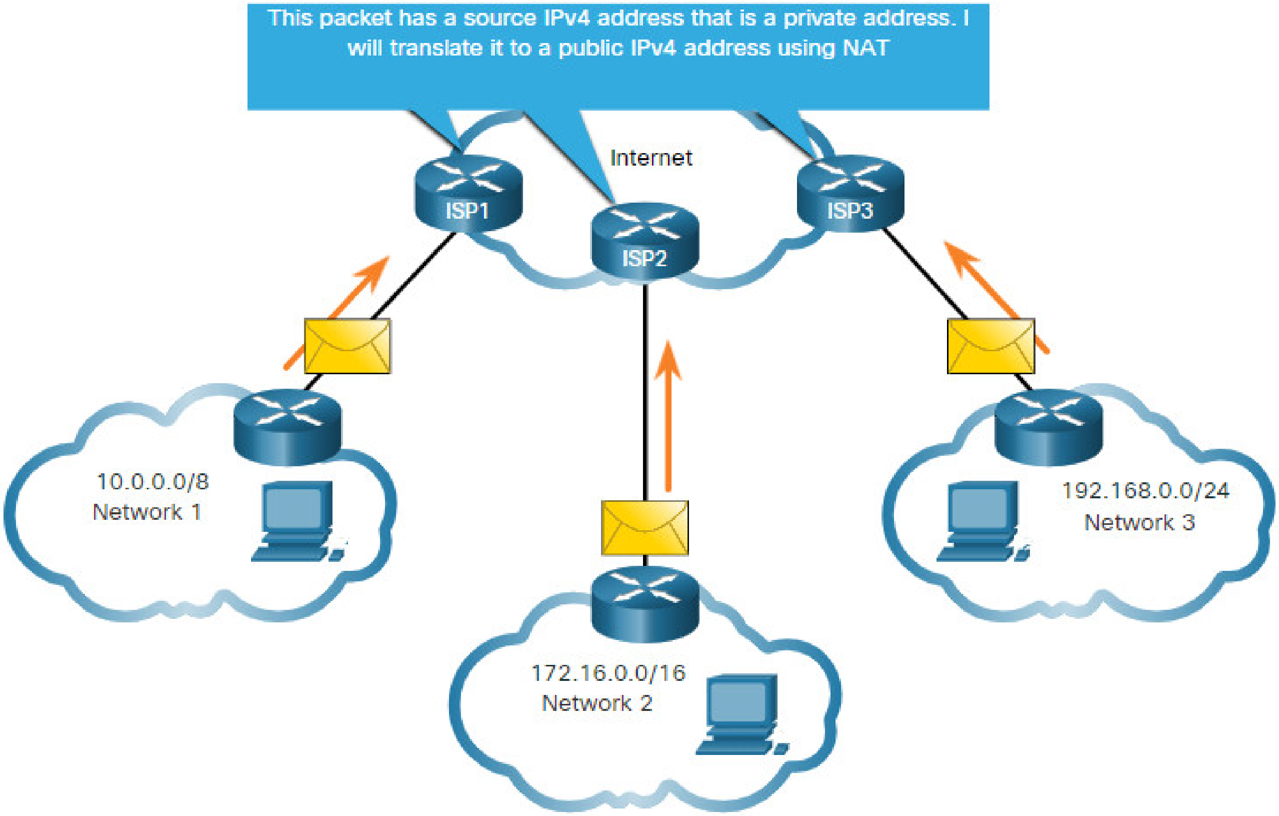
11.3.2. Routing to the Internet

Most internal networks, from large enterprises to home networks, use private IPv4 addresses for addressing all internal devices (intranet) including hosts and routers. However, private addresses are not globally routable.

In the figure, customer networks 1, 2, and 3 are sending packets outside their internal networks. These packets have a source IPv4 address that is a private address and a destination IPv4 address that is public (globally routable). Packets with a private address must be filtered (discarded) or translated to a public address before forwarding the packet to an ISP.

The diagram is a network topology with three networks, each connected to a different ISP router. The ISP routers are performing NAT between each network and the Internet.

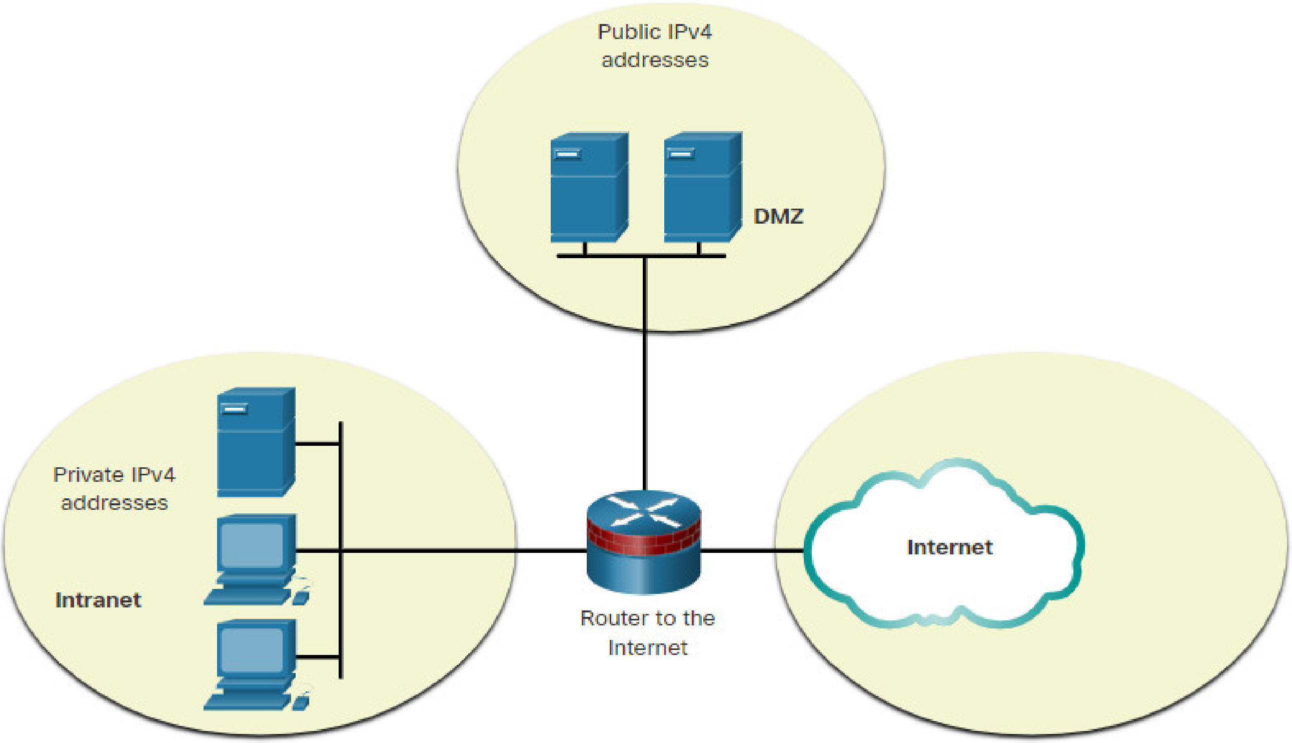
Private IPv4 Addresses and Network Address Translation (NAT)


This packet has a source IPv4 address that is a private address. I will translate it to a public IPv4 address using NAT
Internet
ISP1
ISP2
ISP3
10.0.0.0/8
Network 1
172.16.0.0/16
Network 2
192.168.0.0/24
Network 3

Before the ISP can forward this packet, it must translate the source IPv4 address, which is a private address, to a public IPv4 address using Network Address Translation (NAT). NAT is used to translate between private IPv4 and public IPv4 addresses. This is usually done on the router that connects the internal network to the ISP network. Private IPv4 addresses in the organization's intranet will be translated to public IPv4 addresses before routing to the internet.

Note: Although, a device with a private IPv4 address is not directly accessible from another device across the internet, the IETF does not consider private IPv4 addresses or NAT as effective security measures.

Organizations that have resources available to the internet, such as a web server, will also have devices that have public IPv4 addresses. As shown in the figure, this part of the network is known as the DMZ (demilitarized zone). The router in the figure not only performs routing, it also performs NAT and acts as a firewall for security.



11.3.4. Special Use IPv4 Addresses

There are certain addresses, such as the network address and broadcast address, 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.

Loopback addresses

Loopback addresses (127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254) are more commonly identified as only 127.0.0.1, these are special addresses used by a host to direct traffic to itself. For example, it can be used on a host to test if the TCP/IP configuration is operational, as shown in the figure. Notice how the 127.0.0.1 loopback address replies to the ping command. Also note how any address within this block will loop back to the local host, which is shown with the second ping in the figure.

Pinging the Loopback Interface

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\NetAcad> ping 127.1.1.1
Pinging 127.1.1.1 with 32 bytes of data:
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\NetAcad>
```

Link-Local addresses

Link-local addresses (169.254.0.0 /16 or 169.254.0.1 to 169.254.255.254) are more commonly known as the Automatic Private IP Addressing (APIPA) addresses or self-assigned addresses. They are used by a Windows DHCP client to self-configure in the event that there are no DHCP servers available. Link-local addresses can be used in a peer-to-peer connection but are not commonly used for this purpose.

11.3.5. Legacy Classful Addressing

In 1981, IPv4 addresses were assigned using classful addressing as defined in RFC 790 (https://tools.ietf.org/html/rfc790), Assigned Numbers. Customers were allocated a network address based on one of three classes, A, B, or C. The RFC divided the unicast ranges into specific classes as follows:

- **Class A (0.0.0.0/8 to 127.0.0.0/8)** – Designed to support extremely large networks with more than 16 million host addresses. Class A used a fixed /8 prefix with the first octet to indicate the network address and the remaining three octets for host addresses (more than 16 million host addresses per network).
- **Class B (128.0.0.0 /16 – 191.255.0.0 /16)** – Designed to support the needs of moderate to large size networks with up to approximately 65,000 host addresses. Class B used a fixed /16 prefix with the two high-order octets to indicate the network address and the remaining two octets for host addresses (more than 65,000 host addresses per network).

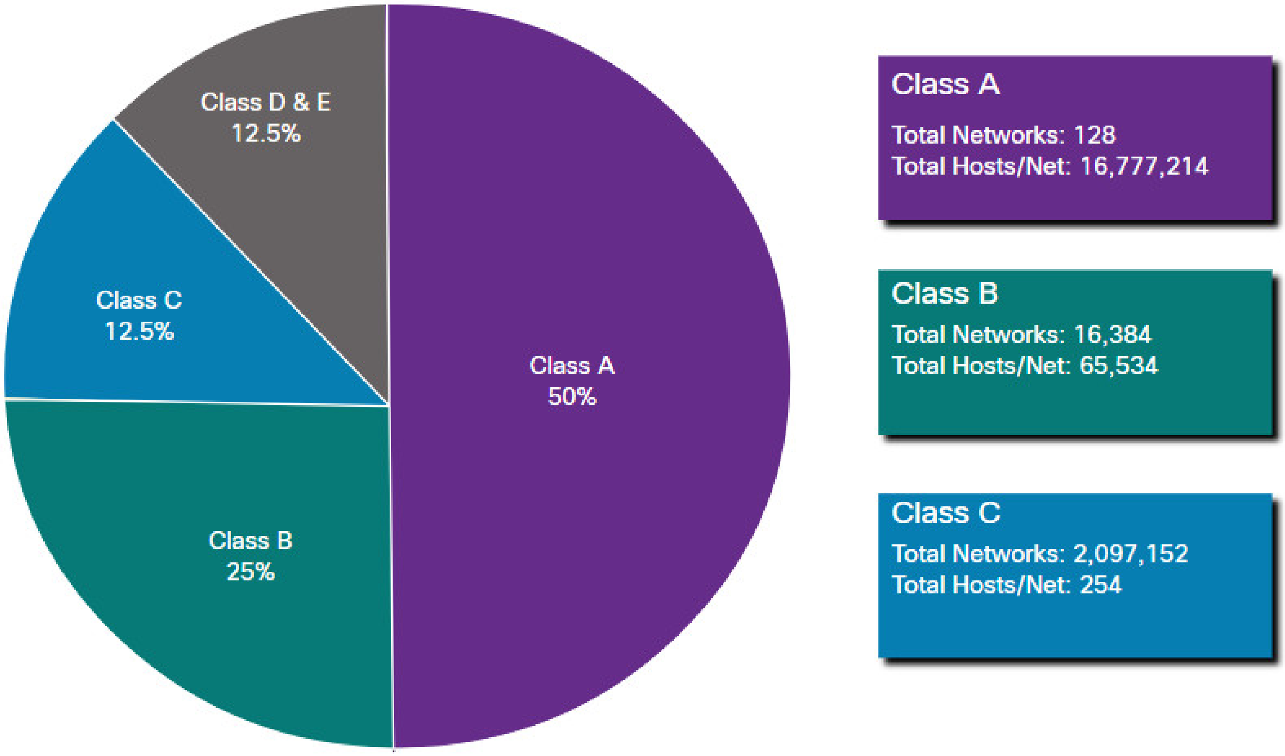
- **Class C (192.0.0.0 /24 – 223.255.255.0 /24)** – Designed to support small networks with a maximum of 254 hosts. Class C used a fixed /24 prefix with the first three octets to indicate the network and the remaining octet for the host addresses (only 254 host addresses per network).

Note: There is also a Class D multicast block consisting of 224.0.0.0 to 239.0.0.0 and a Class E experimental address block consisting of 240.0.0.0 – 255.0.0.0.

At the time, with a limited number of computers using the internet, classful addressing was an effective means to allocate addresses. As shown in the figure, Class A and B networks have a very large number of host addresses and Class C has very few. Class A networks accounted for 50% of the IPv4 networks. This caused most of the available IPv4 addresses to go unused.

Summary of Classful Addressing

The diagram is a pie chart showing the percentage of Class A, B, C, D, & E IPv4 addressing with the total number of networks and hosts per class A, B, and C networks. Percentages are: class A = 50%, class B = 25%, class C = 12.5%, and class D and E = 12.5%. For the total number of networks and total number of hosts per network: class A = 128 networks with 16,777,214 total hosts per network; class B = 16,384 networks with 65,534 total hosts per network; and class C = 2,097,152 networks with 254 total hosts per network.



In the mid-1990s, with the introduction of the World Wide Web (WWW), classful addressing was deprecated to more efficiently allocate the limited IPv4 address space. Classful address allocation was replaced with classless addressing, which is used today. Classless addressing ignores the rules of classes (A, B, C). Public IPv4 network addresses (network addresses and subnet masks) are allocated based on the number of addresses that can be justified.

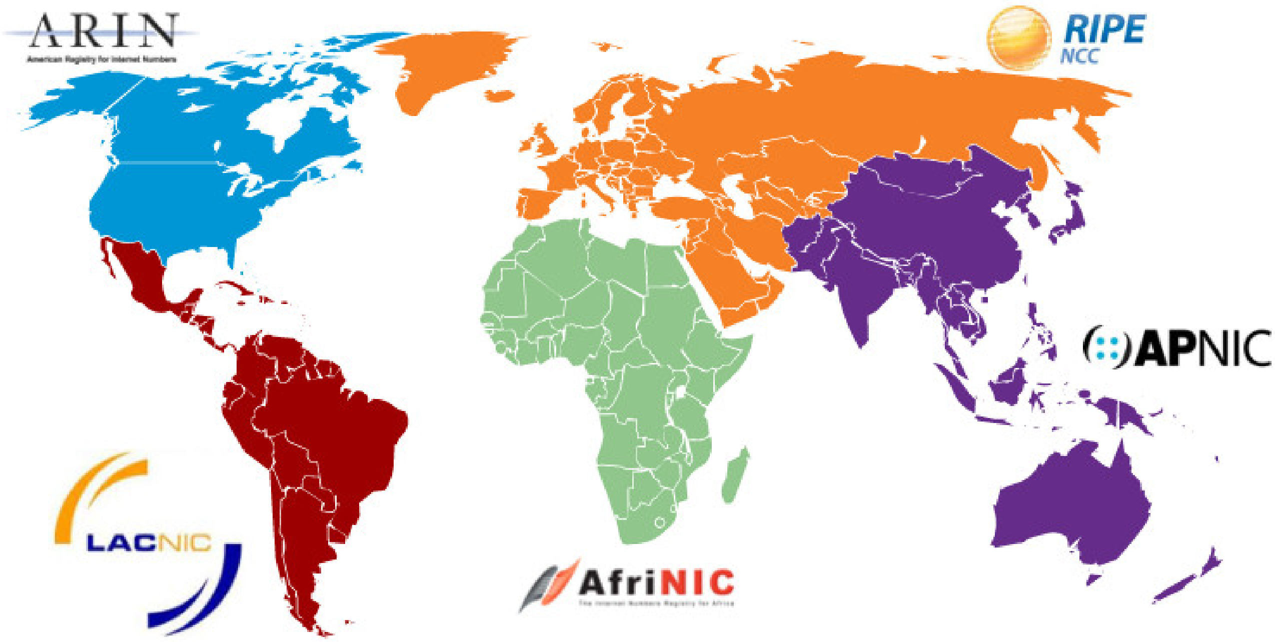
11.3.6. Assignment of IP Addresses

Public IPv4 addresses are addresses which are globally routed over the internet. Public IPv4 addresses must be unique.

Both IPv4 and IPv6 addresses are managed by the Internet Assigned Numbers Authority (IANA). The IANA manages and allocates blocks of IP addresses to the Regional Internet Registries (RIRs). The five RIRs are shown in the figure.

RIRs are responsible for allocating IP addresses to ISPs who provide IPv4 address blocks to organizations and smaller ISPs. Organizations can also get their addresses directly from an RIR (subject to the policies of that RIR).

Regional Internet Registries


ARIN
American Registry for Internet Numbers
RIPE NCC
APNIC
LACNIC
AfriNIC
The Internet Numbers Registry for Africa

- **AfriNIC** (African Network Information Centre) – Africa Region
- **APNIC** (Asia Pacific Network Information Centre) – Asia/Pacific Region
- **ARIN** (American Registry for Internet Numbers) – North America Region
- **LACNIC** (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- **RIPE NCC** (Réseaux IP Européens Network Coordination Centre) – Europe, the Middle East, and Central Asia

11.4. Network Segmentation

11.4.1 Broadcast Domains and Segmentation

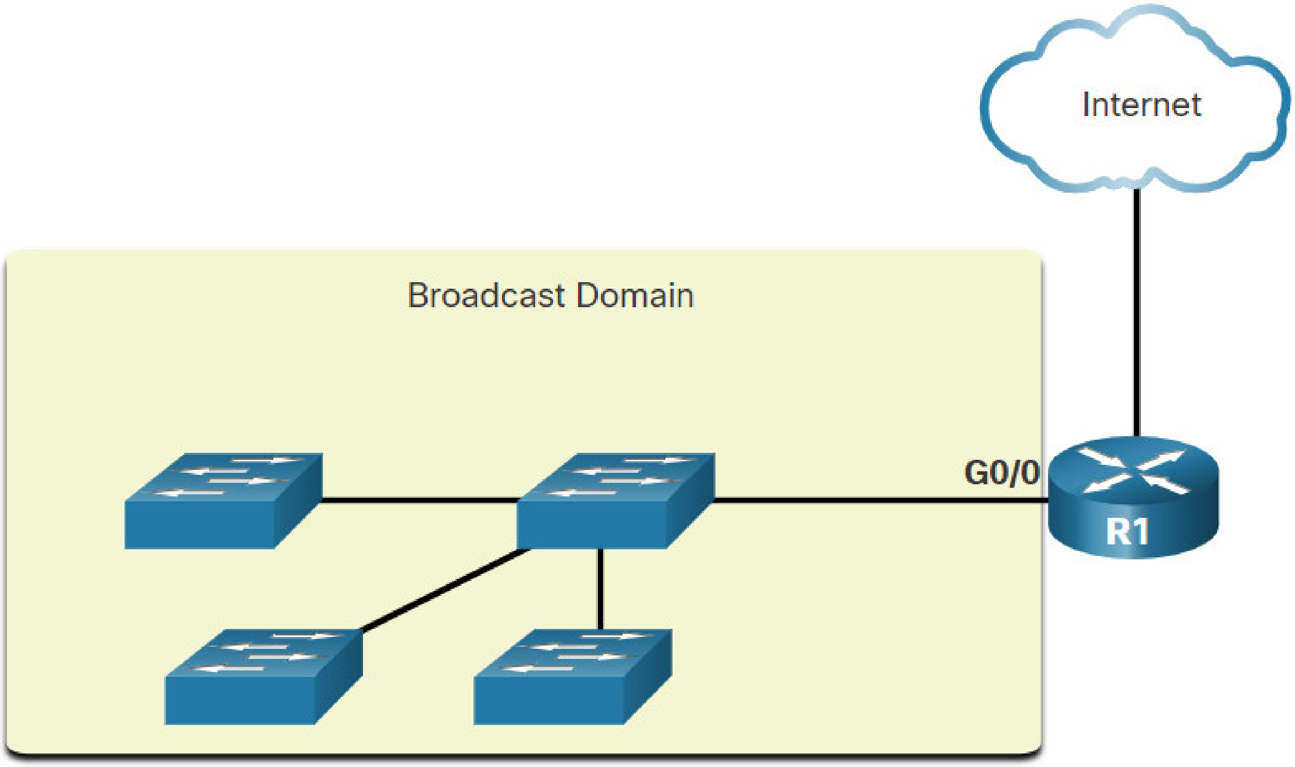
Have you ever received an email that was addressed to every person at your work or school? This was a broadcast email. Hopefully, it contained information that each of you needed to know. But often a broadcast is not really pertinent to everyone in the mailing list. Sometimes, only a segment of the population needs to read that information.

In an Ethernet LAN, devices use broadcasts and the Address Resolution Protocol (ARP) to locate other devices.. ARP sends Layer 2 broadcasts to a known IPv4 address on the local network to discover the associated MAC address. Devices on Ethernet LANs also locate other devices using services. A host typically acquires its IPv4 address configuration using the Dynamic Host Configuration Protocol (DHCP) which sends broadcasts on the local network to locate a DHCP server.

Switches propagate broadcasts out all interfaces except the interface on which it was received. For example, if a switch in the figure were to receive a broadcast, it would forward it to the other switches and other users connected in the network.

Routers Segment Broadcast Domains

A router, R1, is connected to a switch via interface G0/0. The switch has connections to three other switches. The broadcast domain consists of the four switches and the router interface to which they are connected. A connection from the router to the Internet is not within the broadcast domain.



Routers do not propagate broadcasts. When a router receives a broadcast, it does not forward it out other interfaces. For instance, when R1 receives a broadcast on its Gigabit Ethernet 0/0 interface, it does not forward out another interface.

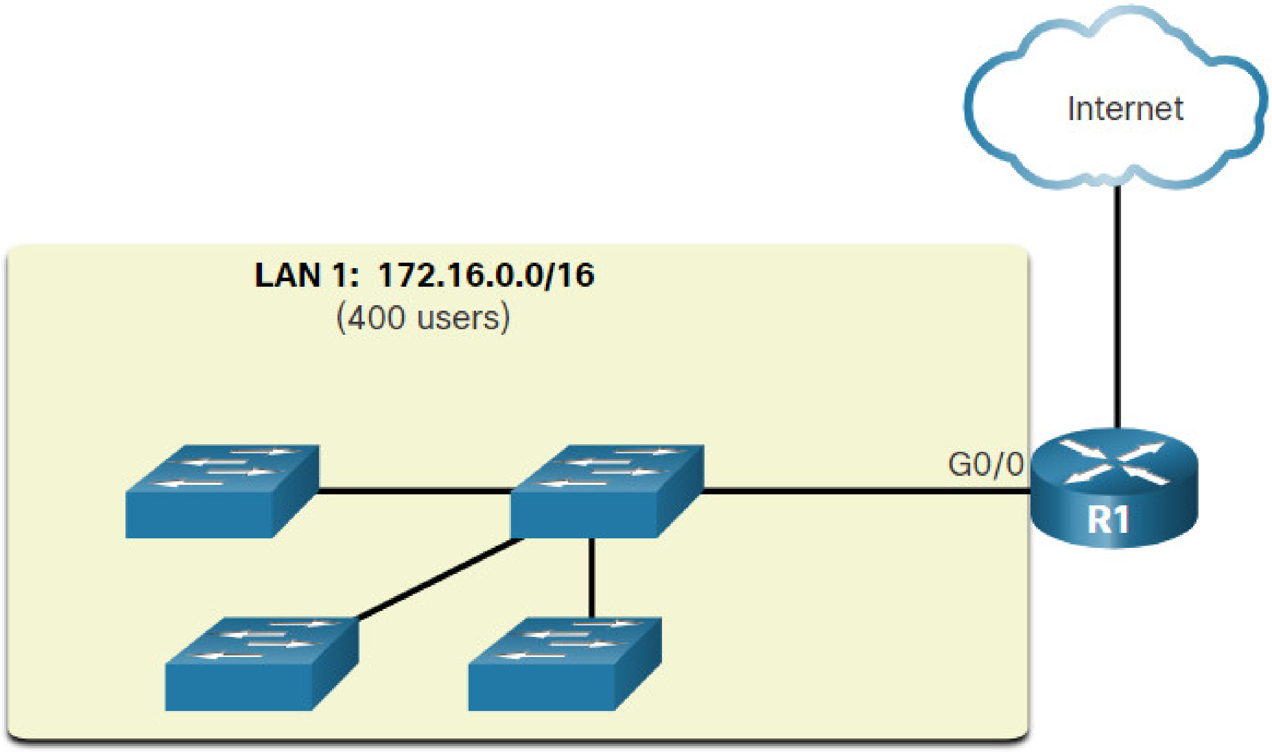
Therefore, each router interface connects to a broadcast domain and broadcasts are only propagated within that specific broadcast domain.

11.4.2. Problems with Large Broadcast Domains

A large broadcast domain is a network that connects many hosts. A problem with a large broadcast domain is that these hosts can generate excessive broadcasts and negatively affect the network. In the figure, LAN 1 connects 400 users that could generate an excess amount of broadcast traffic. This results in slow network operations due to the significant amount of traffic it can cause, and slow device operations because a device must accept and process each broadcast packet.

A Large Broadcast Domain

A router, R1, is connected to a switch via interface G0/0. The switch has connections to three other switches. The broadcast domain consists of the four switches and the router interface to which they are connected. This is identified as LAN1 with an address of 172.16.0.0/16. A connection from the router to the Internet is not within the broadcast domain.

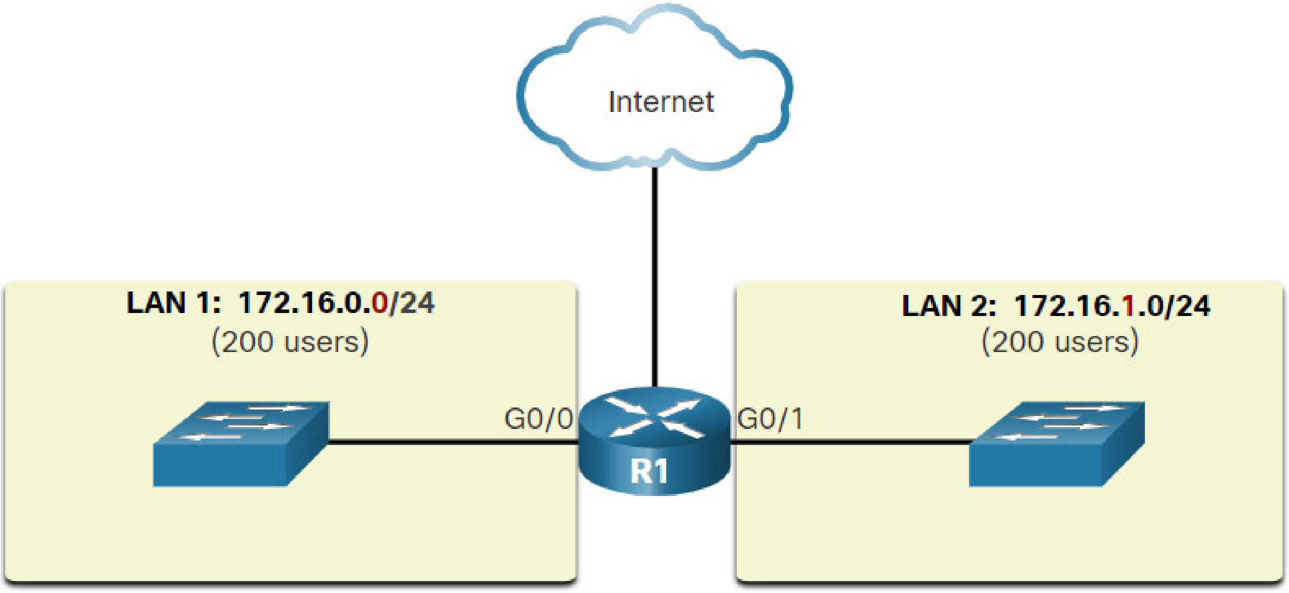


The solution is to reduce the size of the network to create smaller broadcast domains in a process called subnetting. These smaller network spaces are called subnets.

In the figure, the 400 users in LAN 1 with network address 172.16.0.0 /16 have been divided into two subnets of 200 users each: 172.16.0.0 /24 and 172.16.1.0 /24. Broadcasts are only propagated within the smaller broadcast domains. Therefore, a broadcast in LAN 1 would not propagate to LAN 2.

Communicating Between Networks

A router, R1, is connected to two LANs which represent two different broadcast domains. Connected on the left via G0/0 is a switch supporting 200 users in LAN 1 with a network address of 172.16.0.0/24. Connected on the right via G0/1 is a switch supporting 200 users in LAN 2 with a network address of 172.16.1.0/24.



Notice how the prefix length has changed from a single /16 network to two /24 networks. This is the basis of subnetting: using host bits to create additional subnets.

Note: The terms subnet and network are often used interchangeably. Most networks are a subnet of some larger address block.

11.4.3. Reasons for Segmenting Networks

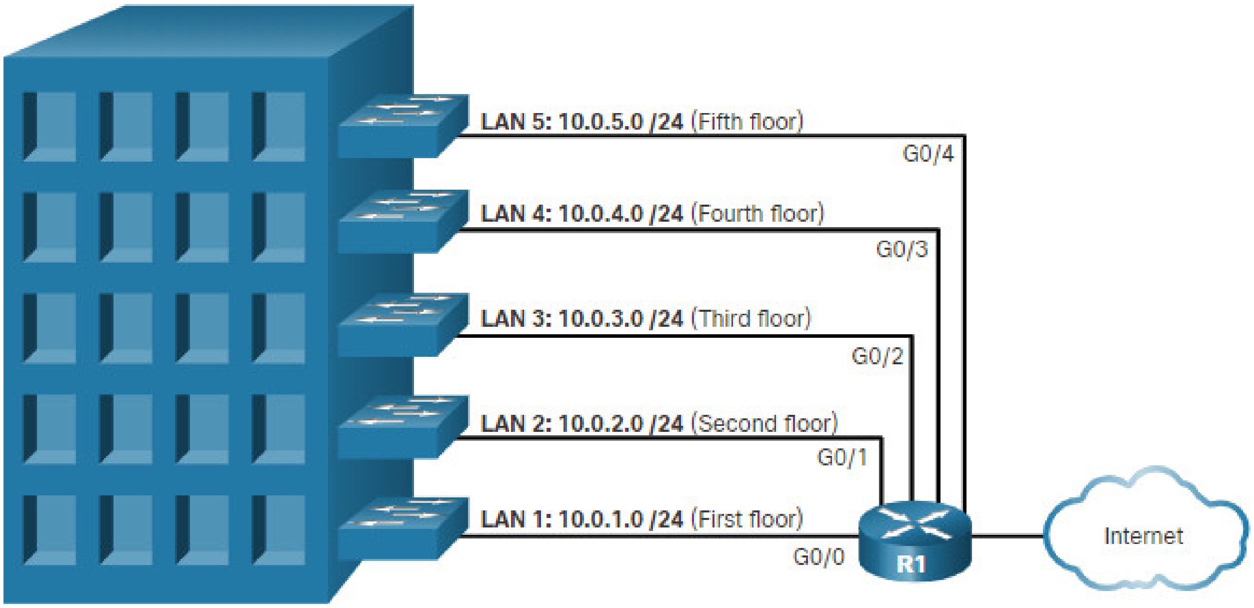
Subnetting reduces overall network traffic and improves network performance. It also enables an administrator to implement security policies such as which subnets are allowed or not allowed to communicate together. Another reason is that it reduces the number of devices affected by abnormal broadcast traffic due to misconfigurations, hardware/software problems, or malicious intent.

There are various ways of using subnets to help manage network devices.

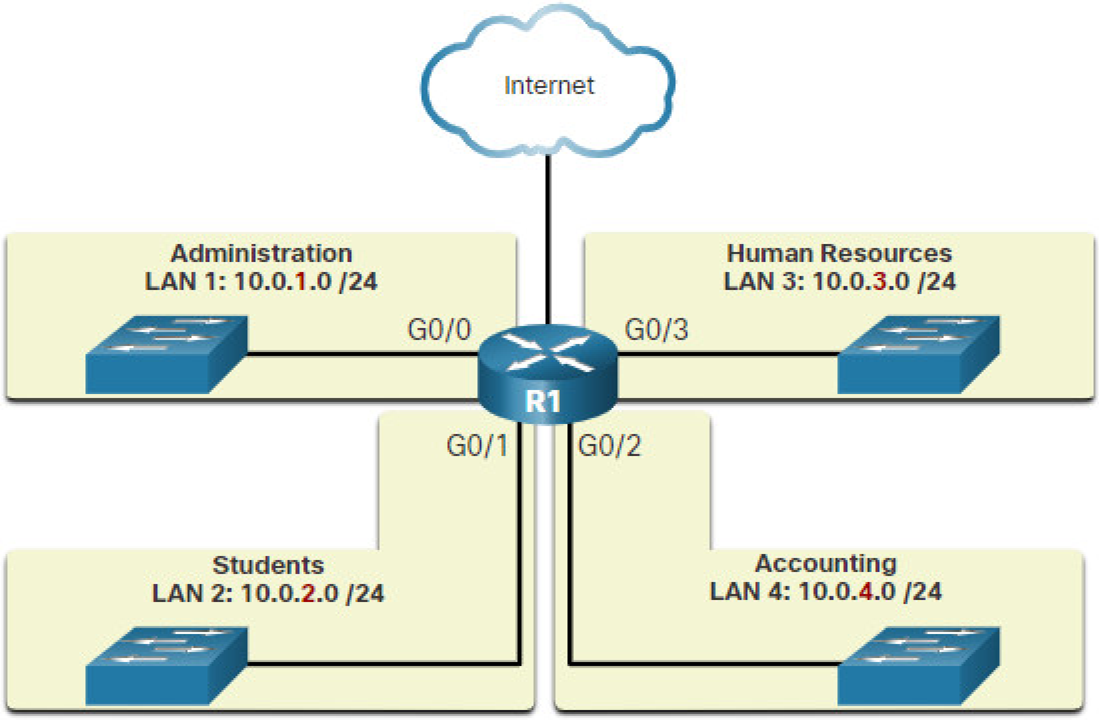
Click each image for an illustration of how network administrators can group devices and services into subnets.

- Location
- Group or Function
- Device Type

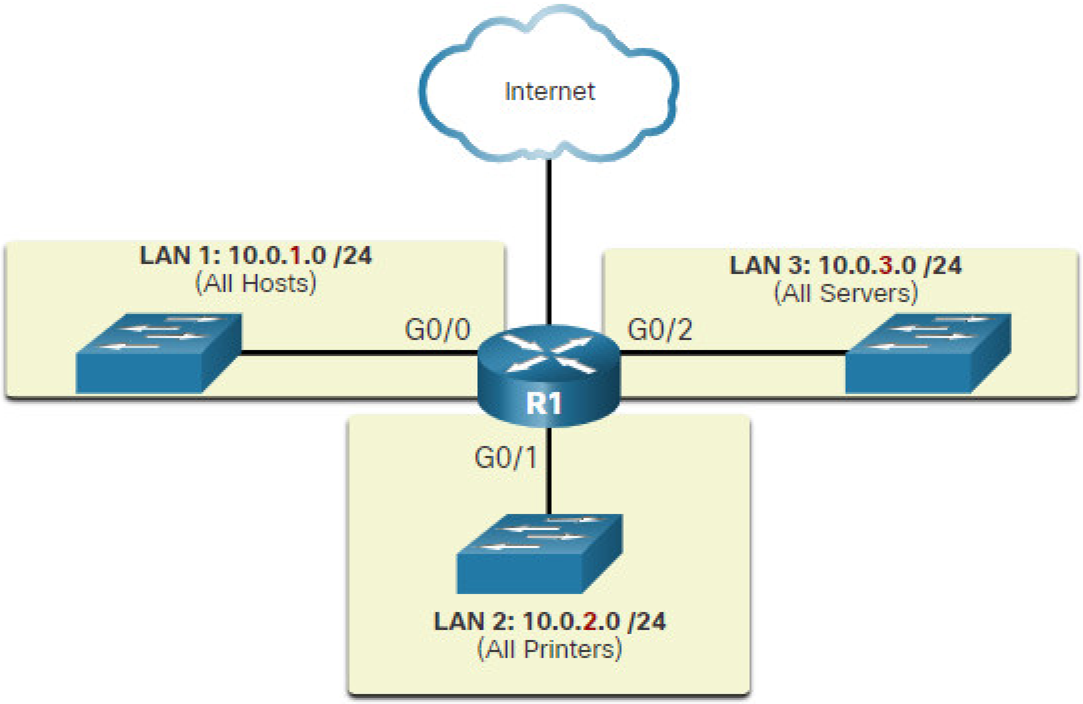
Subnetting by Location


LAN 5: 10.0.5.0 /24 (Fifth floor)
G0/4
LAN 4: 10.0.4.0 /24 (Fourth floor)
G0/3
LAN 3: 10.0.3.0 /24 (Third floor)
G0/2
LAN 2: 10.0.2.0 /24 (Second floor)
G0/1
LAN 1: 10.0.1.0 /24 (First floor)
G0/0
R1
Internet

Subnetting by Group or Function



Subnetting by Device Type



Network administrators can create subnets using any other division that makes sense for the network. Notice in each figure, the subnets use longer prefix lengths to identify networks.

Understanding how to subnet networks is a fundamental skill that all network administrators must develop. Various methods have been created to help understand this process. Although a little overwhelming at first, pay close attention to the detail and, with practice, subnetting will become easier.

11.5. Subnet an IPv4 Network

11.5.1. Subnet on an Octet Boundary

In the previous topic you learned several good reasons for segmenting a network. You also learned that segmenting a network is called subnetting. Subnetting is a critical skill to have when administering an IPv4 network. It is a bit daunting at first, but it gets much easier with practice.

IPv4 subnets are created by using one or more of the host bits as network bits. This is done by extending the subnet mask to borrow some of the bits from the host portion of the address to create additional network bits. The more host bits that are borrowed, the more subnets that can be defined. The more bits that are borrowed to increase the number of subnets reduces the number of hosts per subnet.

Networks are most easily subnetted at the octet boundary of /8, /16, and /24. The table identifies these prefix lengths. Notice that using longer prefix lengths decreases the number of hosts per subnet.

Subnet Masks on Octet Boundaries

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts

/8	**255**.0.0.0	`nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh`
		`11111111.00000000.00000000.00000000`
			16,777,214

/16	**255.255**.0.0	`nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh`
		`11111111.11111111.00000000.00000000`
			65,534

/24	**255.255.255**.0	`nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh`
		`11111111.11111111.11111111.00000000`
			254

To understand how subnetting on the octet boundary can be useful, consider the following example. Assume an enterprise has chosen the private address 10.0.0.0/8 as its internal network address. That network address can connect 16,777,214 hosts in one broadcast domain. Obviously, having more than 16 million hosts on a single subnet is not ideal.

The enterprise could further subnet the 10.0.0.0/8 address at the octet boundary of /16 as shown in the table. This would provide the enterprise the ability to define up to 256 subnets (i.e., 10.0.0.0/16 – 10.255.0.0/16) with each subnet capable of connecting 65,534 hosts. Notice how the first two octets identify the network portion of the address whereas the last two octets are for host IP addresses.

Subnetting Network 10.0.0.0/8 using a /16

Subnet Address **(256 Possible Subnets)**	**Host Range** **(65,534 possible hosts per subnet)**	**Broadcast**
10.0.0.0/**16**	**10.0**.0.1 – **10.0**.255.254	**10.0**.255.255
10.1.0.0/**16**	**10.1**.0.1 – **10.1**.255.254	**10.1**.255.255
10.2.0.0/**16**	**10.2**.0.1 – **10.2**.255.254	**10.2**.255.255
10.3.0.0/**16**	**10.3**.0.1 – **10.3**.255.254	**10.3**.255.255
10.4.0.0/**16**	**10.4**.0.1 – **10.4**.255.254	**10.4**.255.255
10.5.0.0/**16**	**10.5**.0.1 – **10.5**.255.254	**10.5**.255.255
10.6.0.0/**16**	**10.6**.0.1 – **10.6**.255.254	**10.6**.255.255
10.7.0.0/**16**	**10.7**.0.1 – **10.7**.255.254	**10.7**.255.255
…	…	…
10.255.0.0/**16**	**10.255**.0.1 – **10.255**.255.254	**10.255**.255.255

Alternatively, the enterprise could choose to subnet the 10.0.0.0/8 network at the /24 octet boundary, as shown in the table. This would enable the enterprise to define 65,536 subnets each capable of connecting 254 hosts. The /24 boundary is very popular in subnetting because it accommodates a reasonable number of hosts and conveniently subnets at the octet boundary.

Subnetting Network 10.0.0.0/8 using a /24 Prefix

Subnet Address **(65,536 Possible Subnets)**	**Host Range** **(254 possible hosts per subnet)**	**Broadcast**
10.0.0.0/**24**	**10.0.0**.1 – **10.0.0**.254	**10.0.0**.255

Subnet Address (65,536 Possible Subnets)	Host Range (254 possible hosts per subnet)	Broadcast
10.0.1.0/**24**	**10.0.1**.1 – **10.0.1**.254	**10.0.1**.255
10.0.2.0/**24**	**10.0.2**.1 – **10.0.2**.254	**10.0.2**.255
…	…	…
10.0.255.0/**24**	**10.0.255**.1 – **10.0.255**.254	**10.0.255**.255
10.1.0.0/**24**	**10.1.0**.1 – **10.1.0**.254	**10.1.0**.255
10.1.1.0/**24**	**10.1.1**.1 – **10.1.1**.254	**10.1.1**.255
10.1.2.0/**24**	**10.1.2**.1 – **10.1.2**.254	**10.1.2**.255
…	…	…
10.100.0.0/**24**	**10.100.0**.1 – **10.100.0**.254	**10.100.0**.255
…	…	…
10.255.255.0/**24**	**10.255.255**.1 – **10.2255.255**.254	**10.255.255**.255

11.5.2. Subnet within an Octet Boundary

The examples shown thus far borrowed host bits from the common /8, /16, and /24 network prefixes. However, subnets can borrow bits from any host bit position to create other masks.

For instance, a /24 network address is commonly subnetted using longer prefix lengths by borrowing bits from the fourth octet. This provides the administrator with additional flexibility when assigning network addresses to a smaller number of end devices.

Refer to the table to see six ways to subnet a /24 network.

Subnet a /24 Network

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

For each bit borrowed in the fourth octet, the number of subnetworks available is doubled, while reducing the number of host addresses per subnet:

/25 row – Borrowing 1 bit from the fourth octet creates 2 subnets supporting 126 hosts each.
/26 row – Borrowing 2 bits creates 4 subnets supporting 62 hosts each.
/27 row – Borrowing 3 bits creates 8 subnets supporting 30 hosts each.
/28 row – Borrowing 4 bits creates 16 subnets supporting 14 hosts each.
/29 row – Borrowing 5 bits creates 32 subnets supporting 6 hosts each.
/30 row – Borrowing 6 bits creates 64 subnets supporting 2 hosts each.

11.5.3. Video – The Subnet Mask

11.5.4. Video – Subnet with the Magic Number

11.5.5. Packet Tracer – Subnet an IPv4 Network

In this activity, starting from a single network address and network mask, you will subnet the Customer network into multiple subnets. The subnet scheme should be based on the number of host computers required in each subnet, as well as other network considerations, like future network host expansion.

After you have created a subnetting scheme and completed the table by filling in the missing host and interface IP addresses, you will configure the host PCs, switches and router interfaces.

After the network devices and host PCs have been configured, you will use the ping command to test for network connectivity.

11.5.5 Packet Tracer – Subnet an IPv4 Network

11.6. Subnet a Slash 16 and a Slash 8 Prefix

11.6.1. Create Subnets with a Slash 16 prefix

Some subnetting is easier than other subnetting. This topic explains how to create subnets that each have the same number of hosts.

In a situation requiring a larger number of subnets, an IPv4 network is required that has more hosts bits available to borrow. For example, the network address 172.16.0.0 has a default mask of 255.255.0.0, or /16. This address has 16 bits in the network portion and 16 bits in the host portion. The 16 bits in the host portion are available to borrow for creating subnets. The table highlights all the possible scenarios for subnetting a /16 prefix.

Subnet a /16 Network

Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.**n**hhhhhhh.hhhhhhhh 11111111.11111111.**1**0000000.00000000	**2**	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.**nn**hhhhhh.hhhhhhhh 11111111.11111111.**11**000000.00000000	**4**	16382

Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts

/19	255.255.224.0	`nnnnnnnn.nnnnnnnn.`**`nnn`**`hhhhh.hhhhhhhh`
		`11111111.11111111.`**`111`**`00000.00000000`
			8	8190

/20	255.255.240.0	`nnnnnnnn.nnnnnnnn.`**`nnnn`**`hhhh.hhhhhhhh`
		`11111111.11111111.`**`1111`**`0000.00000000`
			16	4094

/21	255.255.248.0	`nnnnnnnn.nnnnnnnn.`**`nnnnn`**`hhh.hhhhhhhh`
		`11111111.11111111.`**`11111`**`000.00000000`
			32	2046

/22	255.255.252.0	`nnnnnnnn.nnnnnnnn.`**`nnnnnn`**`hh.hhhhhhhh`
		`11111111.11111111.`**`111111`**`00.00000000`
			64	1022

/23	255.255.254.0	`nnnnnnnn.nnnnnnnn.`**`nnnnnnn`**`h.hhhhhhhh`
		`11111111.11111111.`**`1111111`**`0.00000000`
			128	510

/24	255.255.255.0	`nnnnnnnn.nnnnnnnn.`**`nnnnnnnn`**`.hhhhhhhh`
		`11111111.11111111.`**`11111111`**`.00000000`
			256	254

/25	255.255.255.128	`nnnnnnnn.nnnnnnnn.`**`nnnnnnnn.n`**`hhhhhhh`
		`11111111.11111111.`**`11111111.1`**`0000000`
			512	126

/26	255.255.255.192	`nnnnnnnn.nnnnnnnn.`**`nnnnnnnn.nn`**`hhhhhh`
		`11111111.11111111.`**`11111111.11`**`000000`
			1024	62

Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts

/27	255.255.255.224	`nnnnnnnn.nnnnnnnn.`**`nnnnnnnn.nnn`**`hhhhh`
		`11111111.11111111.`**`11111111.111`**`00000`
			2048	30

/28	255.255.255.240	`nnnnnnnn.nnnnnnnn.`**`nnnnnnnn.nnnn`**`hhhh`
		`11111111.11111111.`**`11111111.1111`**`0000`
			4096	14

/29	255.255.255.248	`nnnnnnnn.nnnnnnnn.`**`nnnnnnnn.nnnnn`**`hhh`
		`11111111.11111111.`**`11111111.11111`**`000`
			8192	6

/30	255.255.255.252	`nnnnnnnn.nnnnnnnn.`**`nnnnnnnn.nnnnnn`**`hh`
		`11111111.11111111.`**`11111111.111111`**`00`
			16384	2

Although you do not need to memorize this table, you still need a good understanding of how each value in the table is generated. Do not let the size of the table intimidate you. The reason it is big is that it has 8 additional bits that can be borrowed, and, therefore, the numbers of subnets and hosts are simply larger.

11.6.2. Create 100 Subnets with a Slash 16 prefix

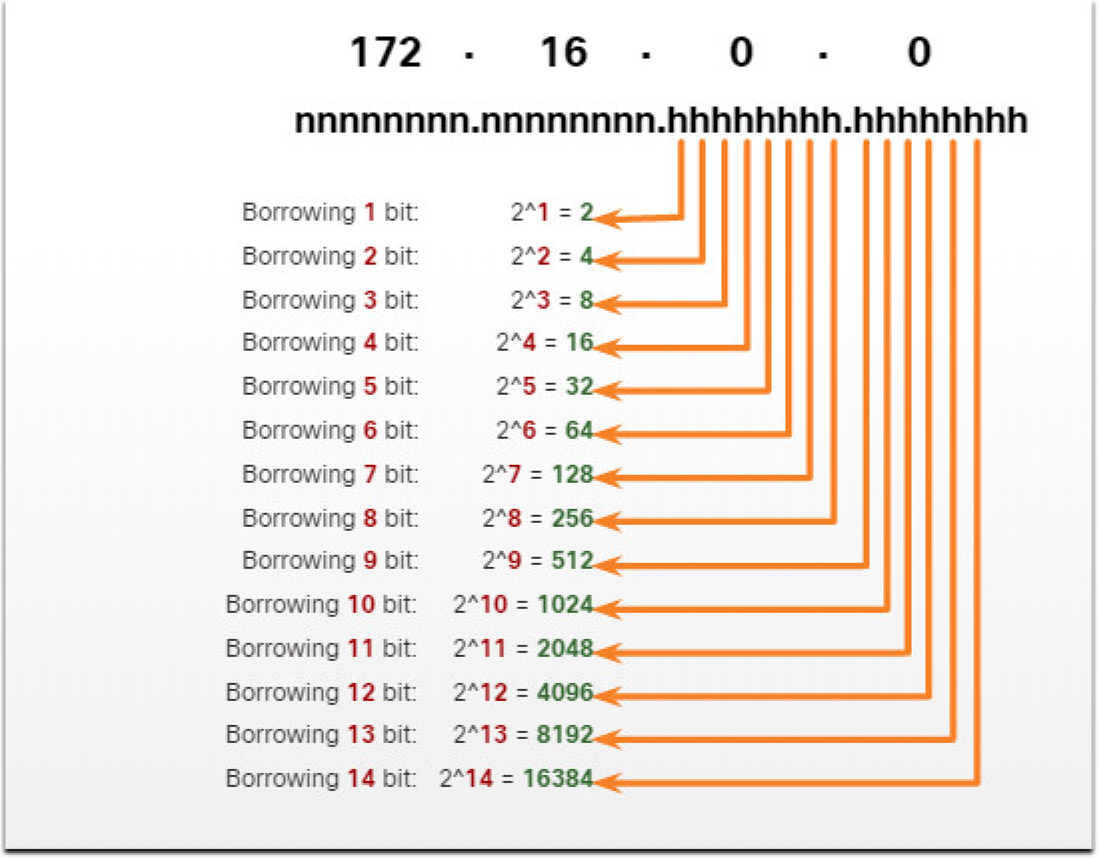
Consider a large enterprise that requires at least 100 subnets and has chosen the private address 172.16.0.0/16 as its internal network address.

When borrowing bits from a /16 address, start borrowing bits in the third octet, going from left to right. Borrow a single bit at a time until the number of bits necessary to create 100 subnets is reached.

The figure displays the number of subnets that can be created when borrowing bits from the third octet and the fourth octet. Notice there are now up to 14 host bits that can be borrowed.

Number of Subnets Created

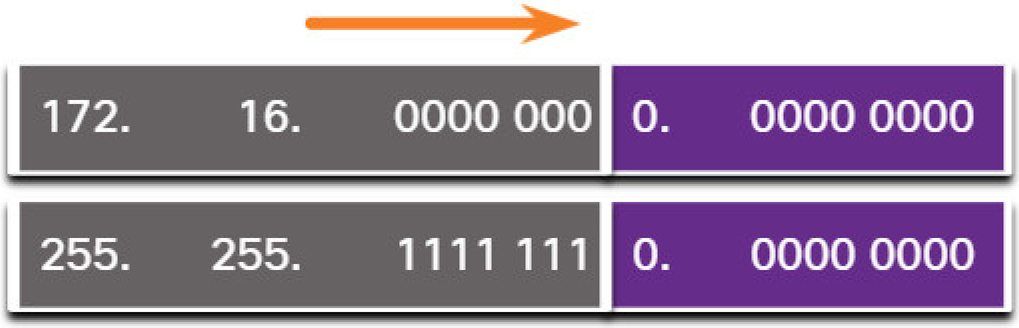
The graphic shows how to compute the number of subnets created when borrowing bits from the third and fourth octets of an IPv4 network address. The formula to determine the number of subnets created is 2 to the power of the number of bits borrowed. The graphic shows an address of 172.16.0.0. Underneath, are the letters nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh. It starts by borrowing the first h bit in the third octet which results in 2 to the power of 1 = 2 subnets. When the first two h bits in the third octet are borrowed, the formula is 2 to the power of 2 = 4. This continues until the first 14 h bits are borrowed from the third and fourth octets resulting in 2 to the power of 14 = 16384. The last two h bits in the fourth octet remain the same.


172 . 16 . 0 . 0
nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh
Borrowing 1 bit: 2^1 = 2
Borrowing 2 bit: 2^2 = 4
Borrowing 3 bit: 2^3 = 8
Borrowing 4 bit: 2^4 = 16
Borrowing 5 bit: 2^5 = 32
Borrowing 6 bit: 2^6 = 64
Borrowing 7 bit: 2^7 = 128
Borrowing 8 bit: 2^8 = 256
Borrowing 9 bit: 2^9 = 512
Borrowing 10 bit: 2^10 = 1024
Borrowing 11 bit: 2^11 = 2048
Borrowing 12 bit: 2^12 = 4096
Borrowing 13 bit: 2^13 = 8192
Borrowing 14 bit: 2^14 = 16384

To satisfy the requirement of 100 subnets for the enterprise, 7 bits (i.e., 27 = 128 subnets) would need to be borrowed (for a total of 128 subnets), as shown in the figure.

172.16.0.0/23 Network

The graphic shows the decimal and bit representation of a network address, and below it a subnet mask, when seven bits are borrowed in the third octet to create subnets. The first two octets are shown in decimal and the last two octets are shown in binary. The network address is 172.16.0000 0000.0000 0000. The subnet mask is 255.255.1111 1110.0000 0000.

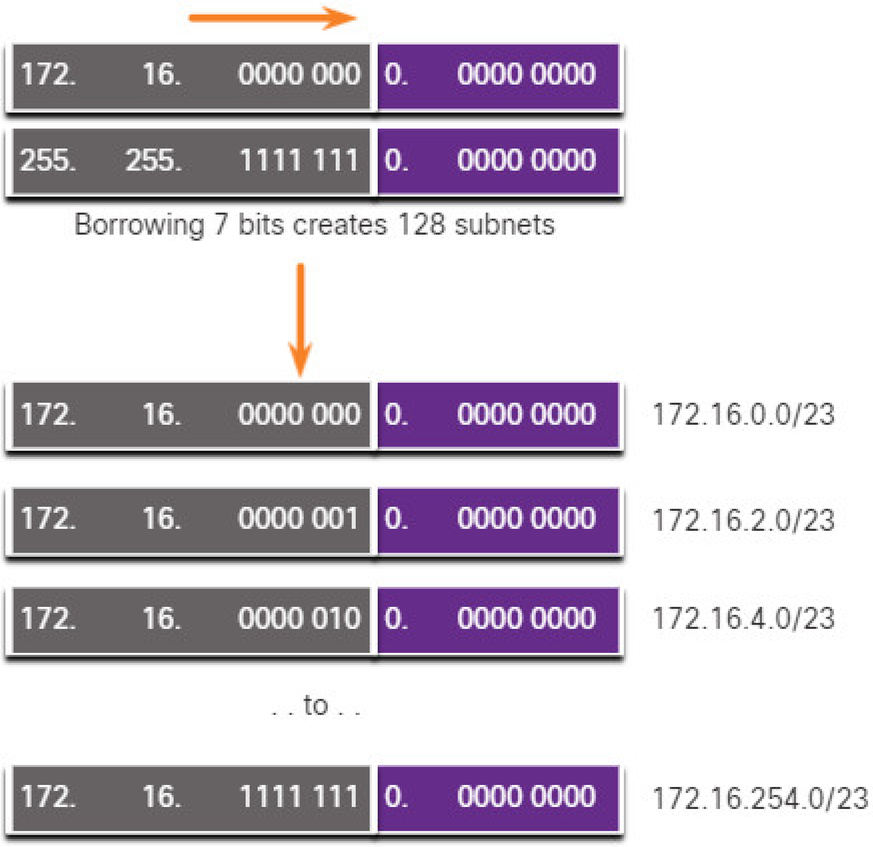


Recall that the subnet mask must change to reflect the borrowed bits. In this example, when 7 bits are borrowed, the mask is extended 7 bits into the third octet. In decimal, the mask is represented as 255.255.254.0, or a /23 prefix, because the third octet is 11111110 in binary and the fourth octet is 00000000 in binary.

The figure displays the resulting subnets from 172.16.0.0 /23 up to 172.16.254.0 /23.

Resulting /23 Subnets

The graphic shows the subnets created when using a /23 subnet mask with the address 172.16.0.0. First, it shows the decimal and bit representation of the network address, and below it the subnet mask. The first two octets are shown in decimal and the last two octets are shown in binary. The network address is 172.16.0000 0000.0000 0000. The subnet mask is 255.255.1111 1110.0000 0000. The first two octets and the first seven bits in the third octet are shaded gray and the last bit in the third octet and the entire fourth octet are shaded purple. Below, the text reads: borrowing 7 bits creates 128 subnets. Below that, it shows the first three subnets and the last subnet created. Again, the first two octets are shown in decimal and the last two octets are shown in binary. The first subnet is 172.16.0000 0000.0000 0000 or 172.16.0.0/23. The second subnet is 172.16.0000 0010.0000 0000 or 172.16.2.0/23. The third subnet is 172.16.0000 0100.0000 0000 or 172.16.4.0/23. The text ..to.. is used to show that this process continues until you reach the last subnet created which is 172.16.1111 1110.0000 0000 or 172.16.254.0/23.

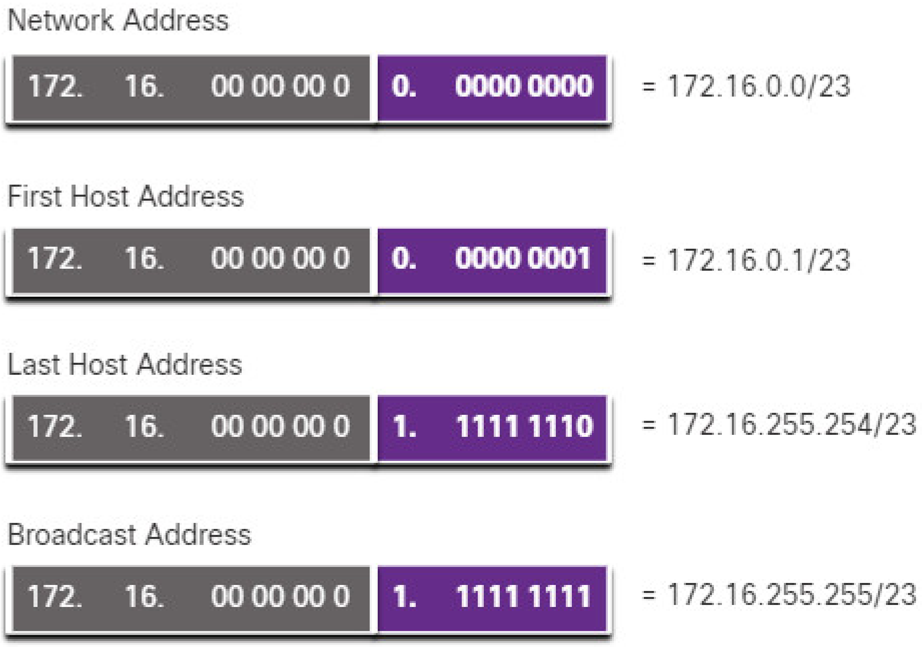


After borrowing 7 bits for the subnet, there is one host bit remaining in the third octet, and 8 host bits remaining in the fourth octet, for a total of 9 bits that were not borrowed. 29 results in 512 total host addresses. The first address is reserved for the network address and the last address is reserved for the broadcast address, so subtracting for these two addresses (29 – 2) equals 510 available host addresses for each /23 subnet.

As shown in the figure, the first host address for the first subnet is 172.16.0.1, and the last host address is 172.16.1.254.

Address Range for 172.16.0.0/23 Subnet

The graphic shows the address range for the 172.16.0.0/23 subnet. The first two octets are shown in decimal and the last two octets are shown in binary, then the address is shown in its dotted decimal format. The network address is 172.16.0000 0000.0000 0000 = 172.16.0.0/23. The first host address is 172.16.0000 0000.0000 0001 = 172.16.0.1/23. The last host address is 172.16.0000 0001.1111 1110 = 172.16.255.254/23 (change to 172.16.1.254 when fixed). The broadcast address is 172.16.0000 0001.1111 1111 = 172.16.255.255/23 (change to 172.16.1.255 when fixed).



Network Address

172. 16. 00 00 00 0 0. 0000 0000 = 172.16.0.0/23

First Host Address

172. 16. 00 00 00 0 0. 0000 0001 = 172.16.0.1/23

Last Host Address

172. 16. 00 00 00 0 1. 1111 1110 = 172.16.255.254/23

Broadcast Address

172. 16. 00 00 00 0 1. 1111 1111 = 172.16.255.255/23

11.6.3. Create 1000 Subnets with a Slash 8 prefix

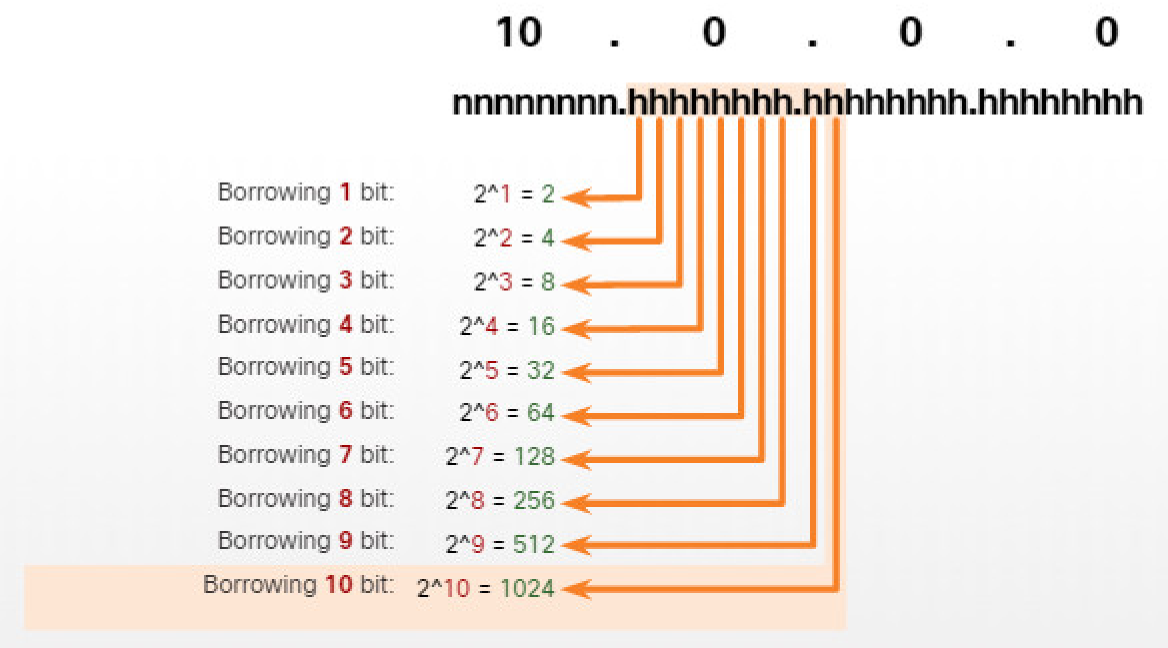
Some organizations, such as small service providers or large enterprises, may need even more subnets. For example, take a small ISP that requires 1000 subnets for its clients. Each client will need plenty of space in the host portion to create its own subnets.

The ISP has a network address 10.0.0.0 255.0.0.0 or 10.0.0.0/8. This means there are 8 bits in the network portion and 24 host bits available to borrow toward subnetting. Therefore, the small ISP will subnet the 10.0.0.0/8 network.

To create subnets, you must borrow bits from the host portion of the IPv4 address of the existing internetwork. Starting from the left to the right with the first available host bit, borrow a single bit at a time until you reach the number of bits necessary to create 1000 subnets. As shown in the figure, you need to borrow 10 bits to create 1024 subnets (2^{10} = 1024). This includes 8 bits in the second octet and 2 additional bits from the third octet.

Number of Subnets Created

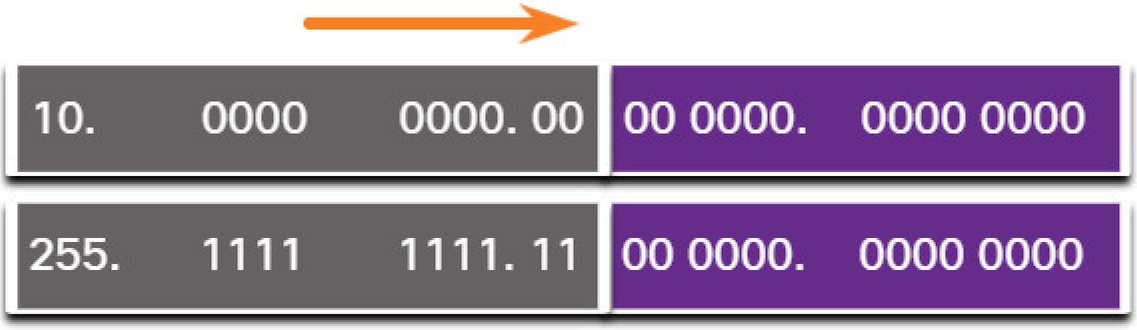
The graphic shows how to compute the number of subnets created when borrowing bits from the second and third octets of an IPv4 network address. The formula to determine the number of subnets created is 2 to the power of the number of bits borrowed. The graphic shows an address of 10.0.0.0. Underneath, are the letters nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh. It starts by borrowing the first h bit in the second octet which results in 2 to the power of 1 = 2 subnets. When the first two h bits in the second octet are borrowed, the formula is 2 to the power of 2 = 4. This continues until the first 10 h bits are borrowed from the second and third octets resulting in 2 to the power of 10 = 1024.


10 . 0 . 0 . 0
nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh
Borrowing 1 bit: 2^1 = 2
Borrowing 2 bit: 2^2 = 4
Borrowing 3 bit: 2^3 = 8
Borrowing 4 bit: 2^4 = 16
Borrowing 5 bit: 2^5 = 32
Borrowing 6 bit: 2^6 = 64
Borrowing 7 bit: 2^7 = 128
Borrowing 8 bit: 2^8 = 256
Borrowing 9 bit: 2^9 = 512
Borrowing 10 bit: 2^10 = 1024

This figure displays the network address and the resulting subnet mask, which converts to 255.255.192.0 or 10.0.0.0/18.

10.0.0.0/18 Network

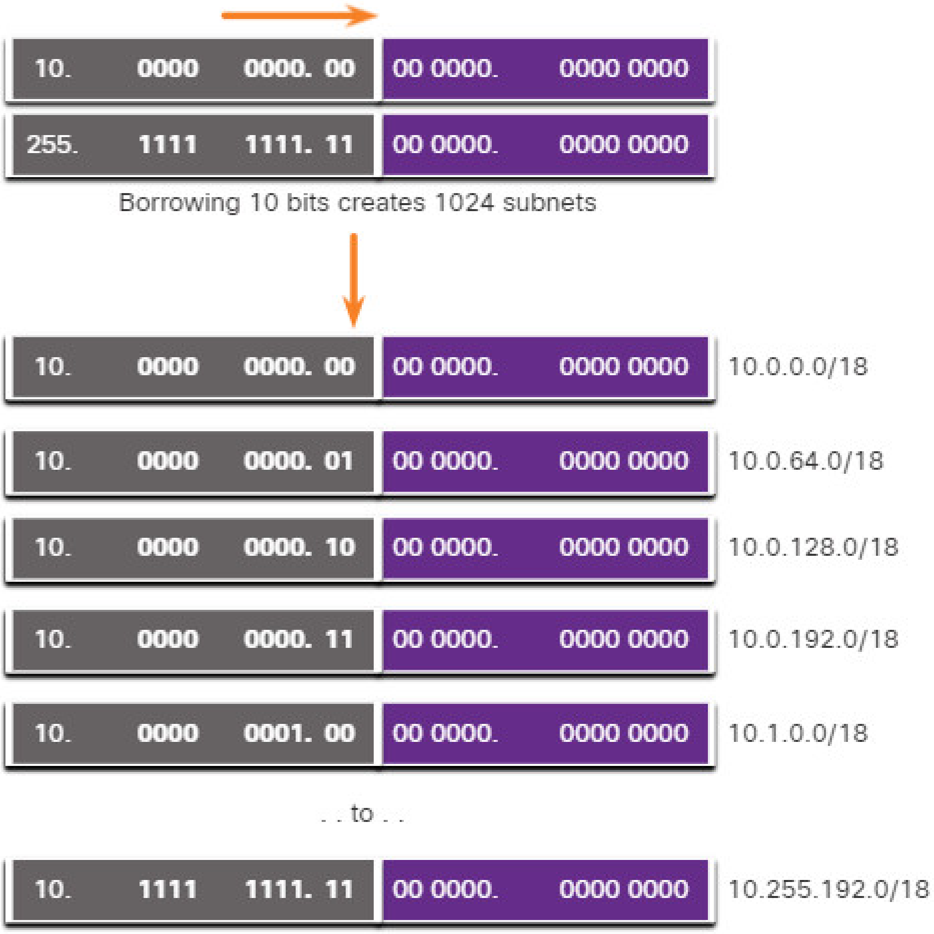
The graphic shows the decimal and bit representation of a network address, and below it a subnet mask, when 10 bits are borrowed in the second and third octets to create subnets. The first octet is shown in decimal and the last three octets are shown in binary. The network address is 10.1111 1111.1100 0000.0000 0000 (should be 10.0000 0000.0000 0000.0000 0000 when fixed). The subnet mask is 255.255.1111 1110.0000 0000.



This figure displays the subnets resulting from borrowing 10 bits, creating subnets from 10.0.0.0/18 to 10.255.128.0/18.

Resulting /18 Subnets

The graphic shows the subnets created when using a /18 subnet mask with the address 10.0.0.0. First, it shows the decimal and bit representation of the network address, and below it the subnet mask. The first octet is shown in decimal and the last three octets are shown in binary. The network address is 10.0000 0000.0000 0000.0000 0000. The subnet mask is 255.1111 1111.1100 0000.0000 0000. The first octet and the next 10 bits are shaded gray and the remaining bits are shaded purple. Below, the text reads: borrowing 10 bits creates 1024 subnets. Below that, it shows the first five subnets and the last subnet created. Again, the first octet is shown in decimal and the last three octets are shown in binary. The first subnet is 10.0000 0000.0000 0000.0000 0000 or 10.0.0.0/18. The second subnet is 10.0000 0000.0100 0000.0000 0000 or 10.0.64.0/18. The third subnet is 10.0000 0000.1000 0000.0000 0000 or 10.0.128.0/18. The fourth subnet is 10.0000 0000.1100 0000.0000 0000 or 10.0.192.0/18. The fifth subnet is 10.0000 0001.0000 0000.0000 0000 or 10.1.0.0/18. The text ..to.. is used to show that this process continues until you reach the last subnet created which is 10.1111 1111.1100 0000.0000 0000 or 10.255.192.0/18.



10. 0000 0000. 00 00 0000. 0000 0000

255. 1111 1111. 11 00 0000. 0000 0000

Borrowing 10 bits creates 1024 subnets

10. 0000 0000. 00 00 0000. 0000 0000 10.0.0.0/18

10. 0000 0000. 01 00 0000. 0000 0000 10.0.64.0/18

10. 0000 0000. 10 00 0000. 0000 0000 10.0.128.0/18

10. 0000 0000. 11 00 0000. 0000 0000 10.0.192.0/18

10. 0000 0001. 00 00 0000. 0000 0000 10.1.0.0/18

. . to . .

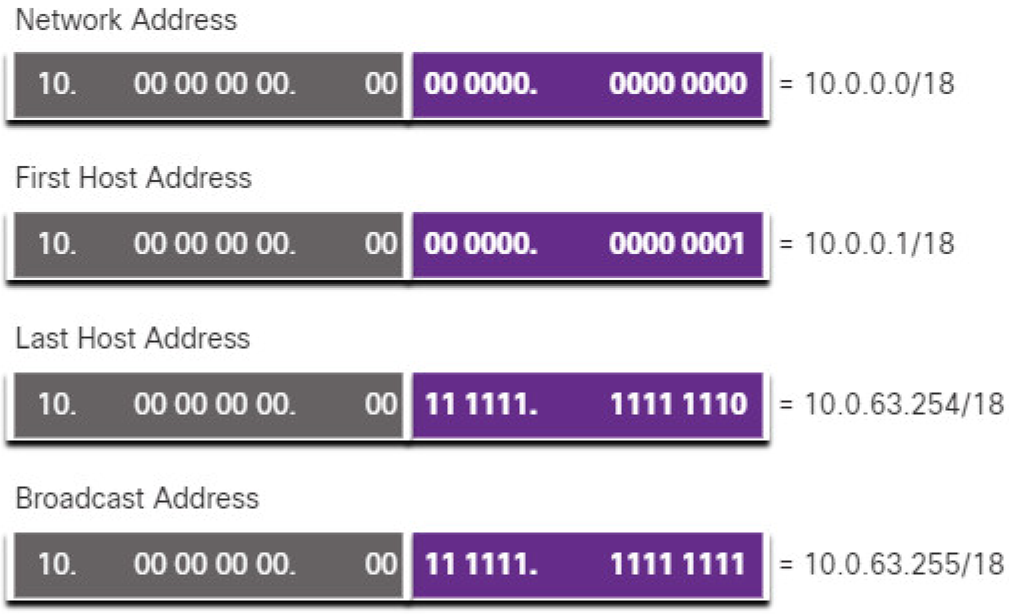
10. 1111 1111. 11 00 0000. 0000 0000 10.255.192.0/18

Borrowing 10 bits to create the subnets, leaves 14 host bits for each subnet. Subtracting two hosts per subnet (one for the network address and one for the broadcast address) equates to 214 – 2 = 16382 hosts per subnet. This means that each of the 1000 subnets can support up to 16,382 hosts.

This figure displays the specifics of the first subnet.

Address Range for 10.0.0.0/18 Subnet

The graphic shows the address range for the 10.0.0.0/18 subnet. The first octet is shown in decimal and the last three octets are shown in binary, then the address is shown in its dotted decimal format. The network address is 10.0000 0000.0000 0000.0000 0000 = 10.0.0.0/18. The first host address is 10.0000 0000.0000 0000.0000 0001 = 10.0.0.1/18. The last host address is 10.0000 0000.0011 1111.1111 1110 = 10.0.63.254/18. The broadcast address is 10.0000 0000.0011 1111. 1111 1111 = 10.0.63.255/18.



Network Address

10. 00 00 00 00. 00 00 0000. 0000 0000 = 10.0.0.0/18

First Host Address

10. 00 00 00 00. 00 00 0000. 0000 0001 = 10.0.0.1/18

Last Host Address

10. 00 00 00 00. 00 11 1111. 1111 1110 = 10.0.63.254/18

Broadcast Address

10. 00 00 00 00. 00 11 1111. 1111 1111 = 10.0.63.255/18

11.6.4. Video – Subnet Across Multiple Octets

11.6.6. Lab – Calculate IPv4 Subnets

In this lab, you will complete the following objectives:

Part 1: Determine IPv4 Address Subnetting
Part 2: Calculate IPv4 Address Subnetting

11.6.6 Lab – Calculate IPv4 Subnets

11.7. Subnet to Meet Requirements

11.7.1. Subnet Private versus Public IPv4 Address Space

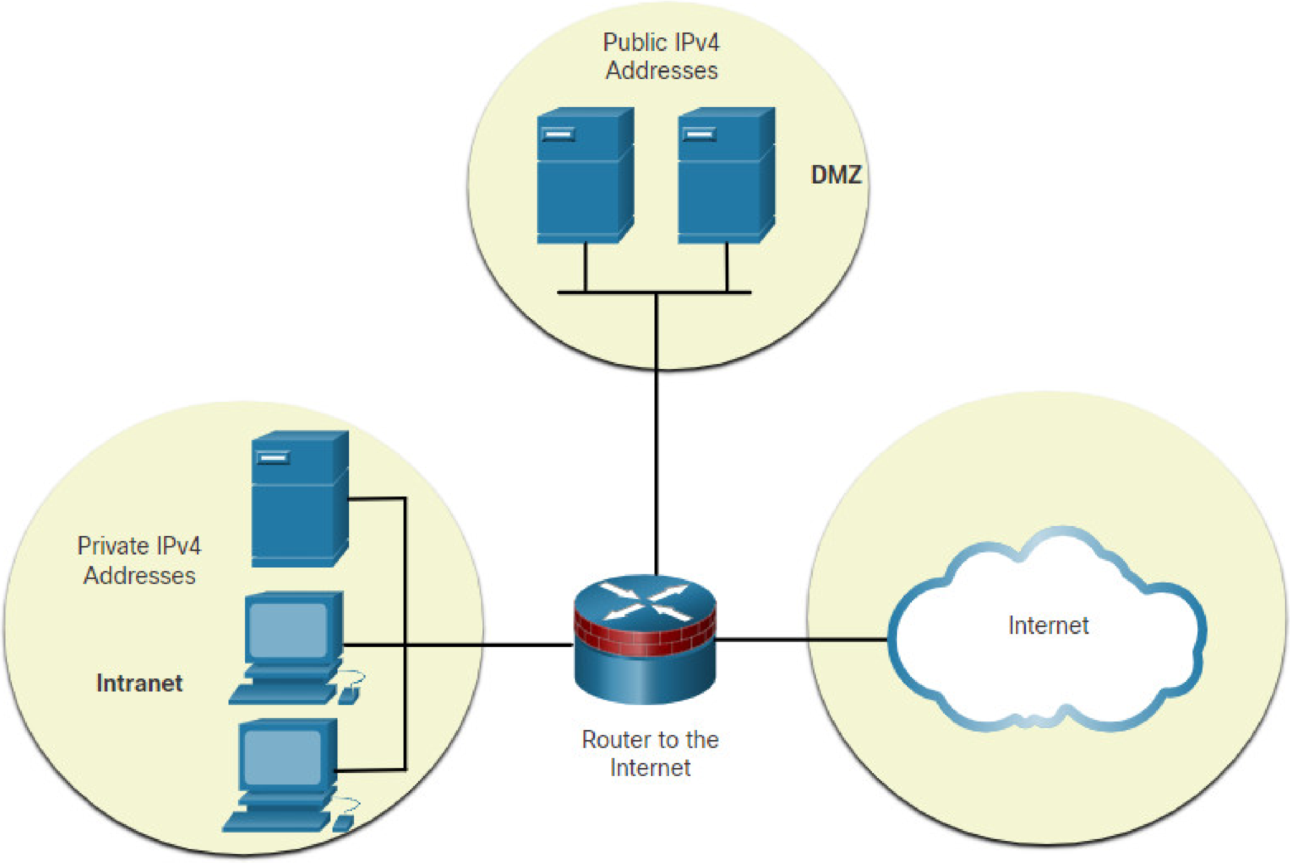
While it is nice to quickly segment a network into subnets, your organization’s network may use both public and private IPv4 addresses. This affects how you will subnet your network.

The figure shows a typical enterprise network:

- **Intranet** – This is the internal part of a company's network, accessible only within the organization. Devices in the intranet use private IPv4 addresses.
- **DMZ** – This is part of the company's network containing resources available to the internet such as a web server. Devices in the DMZ use public IPv4 addresses.

Public and Private IPv4 Address Space

The diagram is a network topology showing a router in the center with three connections; one to the company Intranet, one to a DMZ, and one to the Internet. On the left is the Intranet with devices using private IPv4 addresses. At the top, is the DMZ with two servers using public IPv4 addresses. The router is labeled router to the Internet and has a connection to the Internet cloud.



Both the intranet and the DMZ have their own subnetting requirements and challenges.

The intranet uses private IPv4 addressing space. This allows an organization to use any of the private IPv4 network addresses including the 10.0.0.0/8 prefix with 24 host bits and over 16 million hosts. Using a network address with 24 host bits makes subnetting easier and more flexible. This includes subnetting on an octet boundary using a /16 or /24.

For example, the private IPv4 network address 10.0.0.0/8 can be subnetted using a /16 mask. As shown in the table, this results in 256 subnets, with 65,534 hosts per subnet. If an organization has a need for fewer than 200 subnets, allowing for some growth, this gives each subnet more than enough host addresses.

Subnetting Network 10.0.0.0/8 using a /16

Subnet Address (256 Possible Subnets)	**Host Range (65,534 possible hosts per subnet)**	**Broadcast**
10.0.0.0/**16**	**10.0**.0.1 – **10.0**.255.254	**10.0**.255.255
10.1.0.0/**16**	**10.1**.0.1 – **10.1**.255.254	**10.1**.255.255
10.2.0.0/16	**10.2**.0.1 – **10.2**.255.254	**10.2**.255.255
10.3.0.0/**16**	**10.3**.0.1 – **10.3**.255.254	**10.3**.255.255
10.4.0.0/**16**	**10.4**.0.1 – **10.4**.255.254	**10.4**.255.255
10.5.0.0/**16**	**10.5**.0.1 – **10.5**.255.254	**10.5**.255.255
10.6.0.0/**16**	**10.6**.0.1 – **10.6.**255.254	**10.6**.255.255
10.7.0.0/**16**	**10.7**.0.1 – **10.7**.255.254	**10.7**.255.255
…	…	…
10.255.0.0/**16**	**10.255**.0.1 – **10.255**.255.254	**10.255**.255.255

Another option using the 10.0.0.0/8 private IPv4 network address is to subnet using a /24 mask. As shown in the table, this results in 65,536 subnets, with 254 hosts per subnet. If an organization needs more than 256 subnets, then using a /24 can be used with 254 hosts per subnet.

Subnetting Network 10.0.0.0/8 using a /24

Subnet Address (65,536 Possible Subnets)	**Host Range (254 possible hosts per subnet)**	**Broadcast**
10.0.0.0/**24**	**10.0.0**.1 – **10.0.0**.254	**10.0.0**.255
10.0.1.0/**24**	**10.0.1**.1 – **10.0.1**.254	**10.0.1**.255
10.0.2.0/**24**	**10.0.2**.1 – **10.0.2**.254	**10.0.2**.255
…	…	…
10.0.255.0/**24**	**10.0.255**.1 – **10.0.255**.254	**10.0.255**.255

Subnet Address **(65,536 Possible Subnets)**	**Host Range** **(254 possible hosts per subnet)**	**Broadcast**
10.1.0.0/**24**	**10.1.0**.1 – **10.1.0**.254	**10.1.0**.255
10.1.1.0/**24**	**10.1.1**.1 – **10.1.1**.254	**10.1.1**.255
10.1.2.0/**24**	**10.1.2**.1 – **10.1.2**.254	**10.1.2**.255
…	…	…
10.100.0.0/**24**	**10.100.0**.1 – **10.100.0**.254	**10.100.0**.255
…	…	…
10.255.255.0/**24**	**10.255.255**.1 – **10.2255.255**.254	**10.255.255**.255

The 10.0.0.0/8 can also be subnetted using any other number of prefix lengths, such as /12, /18, /20, etc. This would give the network administrator a wide variety of options. Using a 10.0.0.0/8 private IPv4 network address makes subnet planning and implementation easy.

What about the DMZ?

Because these devices need to be publicly accessible from the internet, the devices in the DMZ require public IPv4 addresses. The depletion of public IPv4 address space became an issue beginning in the mid-1990s. Since 2011, IANA and four out of five RIRs have run out of IPv4 address space. Although organizations are making the transition to IPv6, the remaining IPv4 address space remains severely limited. This means an organization must maximize its own limited number of public IPv4 addresses. This requires the network administrator to subnet their public address space into subnets with different subnet masks, in order to minimize the number of unused host addresses per subnet. This is known as Variable Subnet Length Masking (VLSM).

11.7.2. Minimize Unused Host IPv4 Addresses and Maximize Subnets

To minimize the number of unused host IPv4 addresses and maximize the number of available subnets, there are two considerations when planning subnets: the number of host addresses required for each network and the number of individual subnets needed.

The table displays the specifics for subnetting a /24 network. Notice how there is an inverse relationship between the number of subnets and the number of hosts. The more bits that are borrowed to create subnets, the fewer host bits remain available. If more host addresses are needed, more host bits are required, resulting in fewer subnets.

The number of host addresses required in the largest subnet will determine how many bits must be left in the host portion. Recall that two of the addresses cannot be used, so the usable number of addresses can be calculated as 2n-2.

Subnetting a /24 Network

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts per subnet

/25	255.255.255.128	`nnnnnnnn.nnnnnnnn.nnnnnnnn.`**`n`**`hhhhhhh`
		`11111111.11111111.11111111.`**`1`**`0000000`
			2	126

/26	255.255.255.192	`nnnnnnnn.nnnnnnnn.nnnnnnnn.`**`nn`**`hhhhhh`
		`11111111.11111111.11111111.`**`11`**`000000`
			4	62

/27	255.255.255.224	`nnnnnnnn.nnnnnnnn.nnnnnnnn.`**`nnn`**`hhhhh`
		`11111111.11111111.11111111.`**`111`**`00000`
			8	30

/28	255.255.255.240	`nnnnnnnn.nnnnnnnn.nnnnnnnn.`**`nnnn`**`hhhh`
		`11111111.11111111.11111111.`**`1111`**`0000`
			16	14

/29	255.255.255.248	`nnnnnnnn.nnnnnnnn.nnnnnnnn.`**`nnnnn`**`hhh`
		`11111111.11111111.11111111.`**`11111`**`000`
			32	6

/30	255.255.255.252	`nnnnnnnn.nnnnnnnn.nnnnnnnn.`**`nnnnnn`**`hh`
		`11111111.11111111.11111111.`**`111111`**`00`
			64	2

Network administrators must devise the network addressing scheme to accommodate the maximum number of hosts for each network and the number of subnets. The addressing scheme should allow for growth in both the number of host addresses per subnet and the total number of subnets.

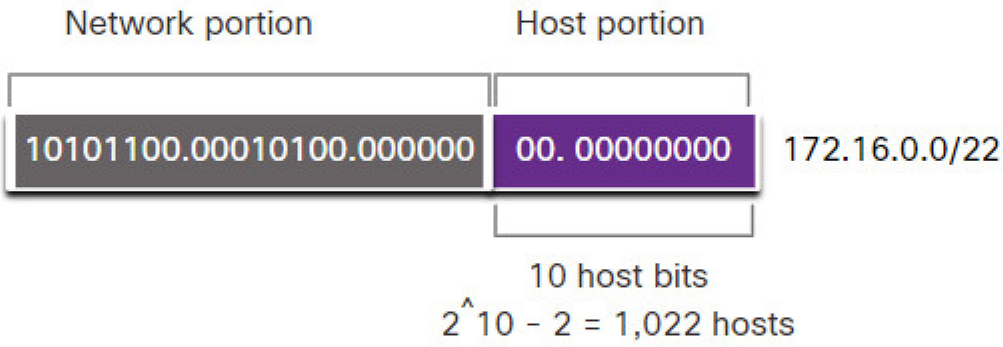
11.7.3. Example: Efficient IPv4 Subnetting

In this example, corporate headquarters has been allocated a public network address of 172.16.0.0/22 (10 host bits) by its ISP. As shown in the figure, this will provide 1,022 host addresses.

Note: 172.16.0.0/22 is part of the IPv4 private address space. We are using this address instead of an actual public IPv4 address.

The graphic shows the number of hosts provided when using a 172.16.0.0/22 network. The network portion of the address in binary is: 10101100.00010100.000000. The host portion in binary is: 00.00000000. The host portion consists of 10 host bits therefore 2 to the power of 10 – 2 = 1,022 hosts.

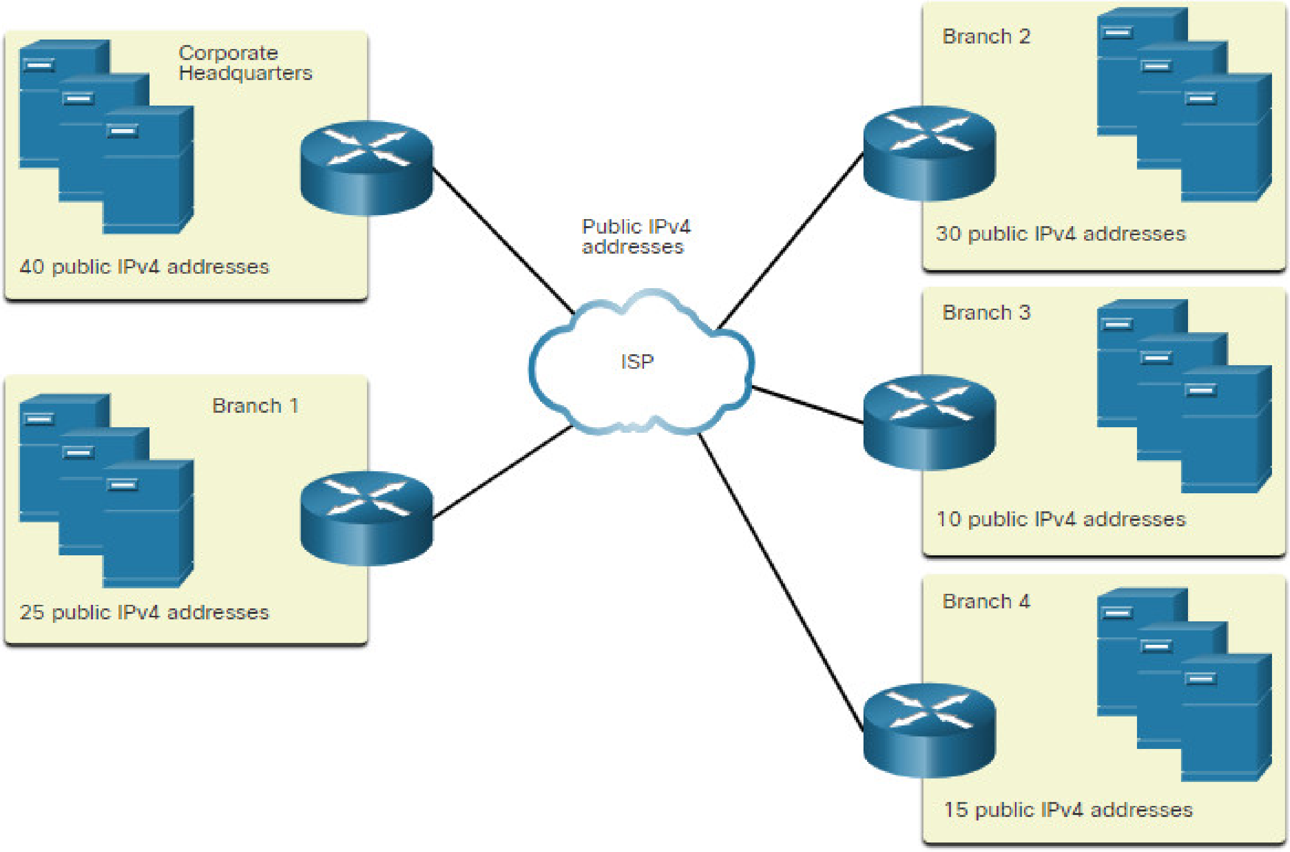
Network Address



The corporate headquarters has a DMZ and four branch offices, each needing its own public IPv4 address space. Corporate headquarters needs to make best use of its limited IPv4 address space.

The topology shown in the figure consists of five sites; a corporate office and four branch sites. Each site requires internet connectivity and therefore, five internet connections. This means that the organization requires 10 subnets from the company’s 172.16.0.0/22 public address. The largest subnet requires 40 addresses.

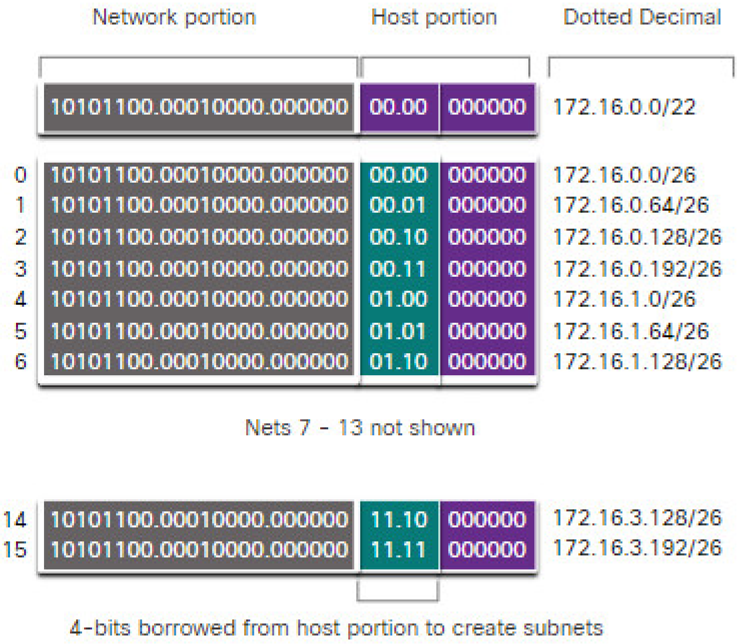
Corporate Topology with Five Sites



The 172.16.0.0/22 network address has 10 host bits, as shown in the figure. Because the largest subnet requires 40 hosts, a minimum of 6 host bits are needed to provide addressing for 40 hosts. This is determined by using this formula: $2^6 - 2 = 62$ hosts.

Subnet Scheme

The diagram shows the subnet scheme for the given address 172.16.0.0/22 with 4 bits borrowed from the host portion to create subnets. All four octets are shown in binary followed by the dotted decimal format for the given network address and for several subnets created. The given network address in binary is 10101100.00010000.000000 (network portion highlighted in gray) 00.00000000 (host portion highlighted in purple) = 172.16.0.0/22. For the subnets listed below, the first 22 bits are highlighted in gray (network portion), the next 4 bits are shaded in blue, and the last 6 bits are the remaining host portion shaded in purple. Subnet 0 is 10101100.00010000.00000000.00000000 = 172.16.0.0/26. Subnet 1 is 10101100.00010000.0000000.01000000 = 172.16.0.64/26. Subnet 2 is 10101100.00010000.00000000.10000000 = 172.16.0.128/26. Subnet 3 is 10101100.00010000.00000000.11000000 = 172.16.0.192/26. Subnet 4 is 10101100.00010000.00000001.00000000 = 172.16.1.0/26. Subnet 5 is 10101100.00010000.00000001.01000000 = 172.16.1.64/26. Subnet 6 is 10101100.00010000.00000001.10000000 = 172.16.1.128/26. Subnet 7 – 13 are not shown. Subnet 14 is 10101100.00010000.00000011.10000000 = 172.16.3.128/26. Subnet 15 is 10101100.00010000.00000011.11000000 = 172.16.3.192/26.



	Network portion	Host portion		Dotted Decimal
	10101100.00010000.000000	00.00	000000	172.16.0.0/22
0	10101100.00010000.000000	00.00	000000	172.16.0.0/26
1	10101100.00010000.000000	00.01	000000	172.16.0.64/26
2	10101100.00010000.000000	00.10	000000	172.16.0.128/26
3	10101100.00010000.000000	00.11	000000	172.16.0.192/26
4	10101100.00010000.000000	01.00	000000	172.16.1.0/26
5	10101100.00010000.000000	01.01	000000	172.16.1.64/26
6	10101100.00010000.000000	01.10	000000	172.16.1.128/26
14	10101100.00010000.000000	11.10	000000	172.16.3.128/26
15	10101100.00010000.000000	11.11	000000	172.16.3.192/26

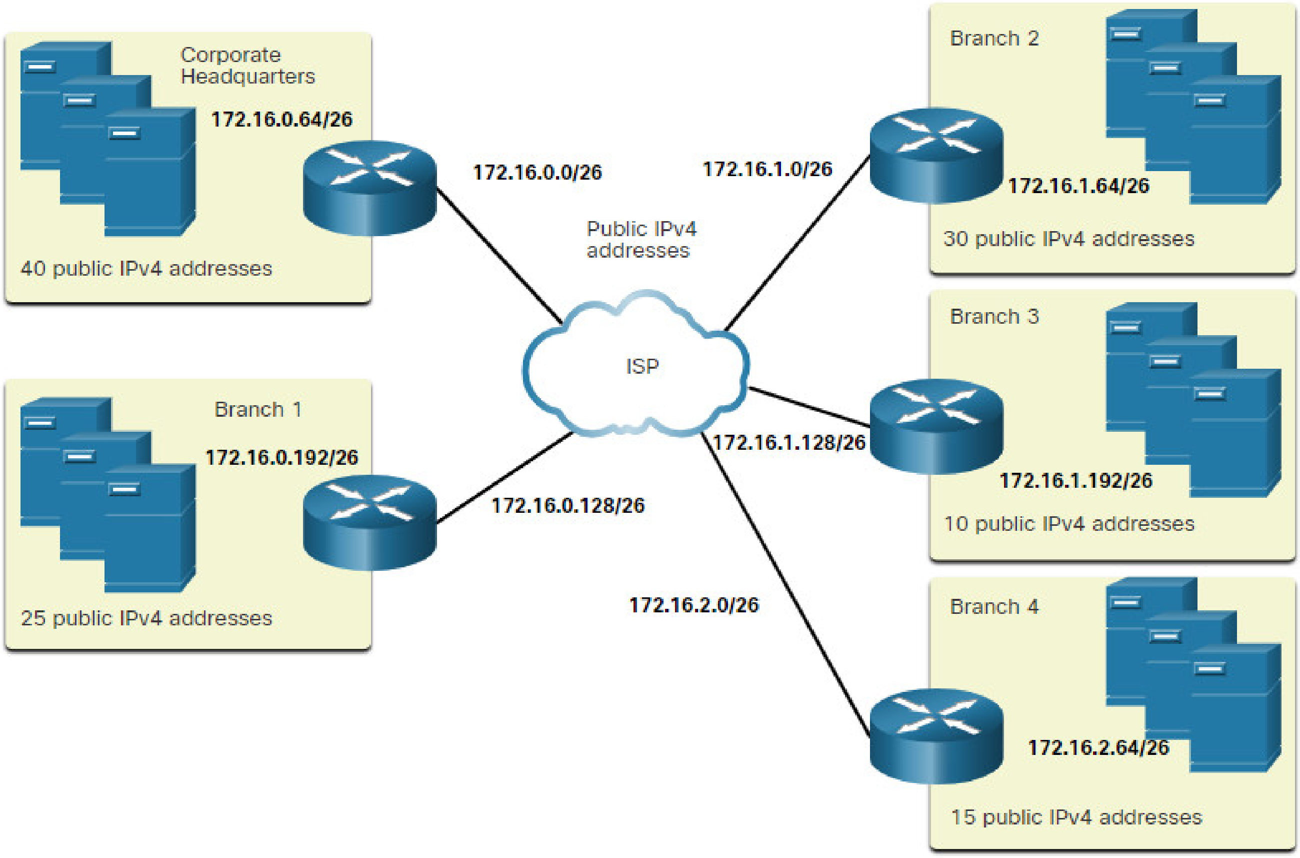
Using the formula for determining subnets results in 16 subnets: $2^4 = 16$. Because the example internetwork requires 10 subnets, this will meet the requirement and allow for some additional growth.

Therefore, the first 4 host bits can be used to allocate subnets. This means two bits from the 3rd octet and two bits from the 4th octet will be borrowed. When 4 bits are borrowed from the 172.16.0.0/22 network, the new prefix length is /26 with a subnet mask of 255.255.255.192.

As shown in this figure, the subnets can be assigned to each location and router-to-ISP connections.

Subnet Assignments to each Site and ISP

The diagram shows the subnet assignments for a corporate topology with five sites connected to an ISP cloud. Each site shows a router connected to the ISP, several servers, the public IPv4 addressing requirements, and the assigned subnet address. Each router-to-ISP connection has also been assigned a subnet address. The Corporate headquarters connection is assigned subnet 172.16.0.0/26 and the site with 40 addresses is assigned subnet 172.16.0.64/26. The Branch 1 connection is assigned subnet 172.16.0.128/26 and the site with 25 addresses is assigned 172.16.0.192/26. The Branch 2 connection is assigned subnet 172.16.1.0/26 and the site with 30 addresses is assigned subnet 172.16.1.64/26. The Branch 3 connection is assigned subnet 172.16.1.128/26 and the site with 10 addresses is assigned subnet 172.16.1.192/26. The Branch 4 connection is assigned subnet 172.16.2.0/26 and the site with 15 addresses is assigned subnet 172.16.2.64/26.



11.7.5. Packet Tracer – Subnetting Scenario

In this activity, you are given the network address of 192.168.100.0/24 to subnet and provide the IP addressing for the network shown in the topology. Each LAN in the network requires enough space for at least 25 addresses, which includes end devices as well as the switch and the router. The connection between R1 to R2 will require an IP address for each end of the link.

11.7.5 Packet Tracer – Subnetting Scenario

11.8. VLSM

11.8.1. Video – VLSM Basics

As mentioned in the previous topic, public and private addresses affect the way you would subnet your network. There are also other issues that affect subnetting schemes. A standard /16 subnetting scheme creates subnets that each have the same number of hosts. Not every subnet you create will need this many hosts, leaving many IPv4 addresses unused. Perhaps you will need one subnet that contains many more hosts. This is why the variable-length subnet mask (VLSM) was developed.

Click Play to view a demonstration of basic VLSM techniques.

11.8.2. Video – VLSM Example

Click Play to view a demonstration of VLSM subnetting.

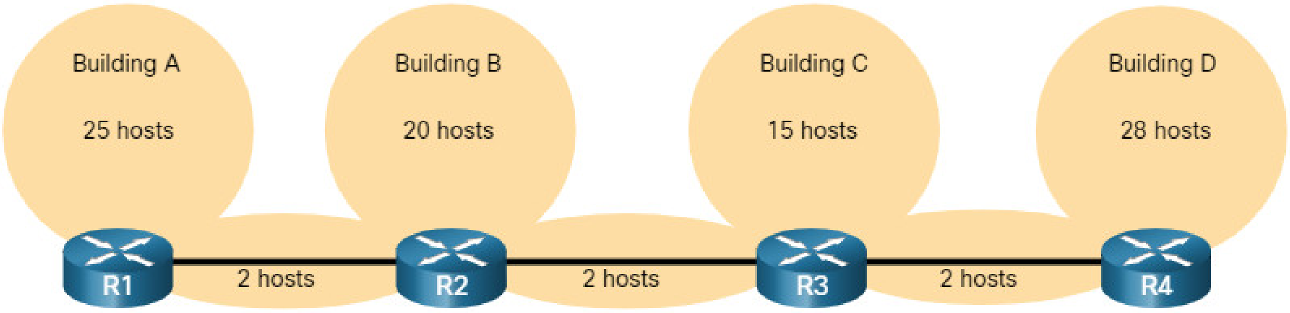
11.8.3. IPv4 Address Conservation

Because of the depletion of public IPv4 address space, making the most out of the available host addresses is a primary concern when subnetting IPv4 networks.

Note: The larger IPv6 address allows for much easier address planning and allocation than IPv4 allows. Conserving IPv6 addresses is not an issue. This is one of the driving forces for transitioning to IPv6.

Using traditional subnetting, the same number of addresses is allocated for each subnet. If all the subnets have the same requirements for the number of hosts, or if conserving IPv4 address space is not an issue, these fixed-size address blocks would be efficient. Typically, with public IPv4 addresses, that is not the case.

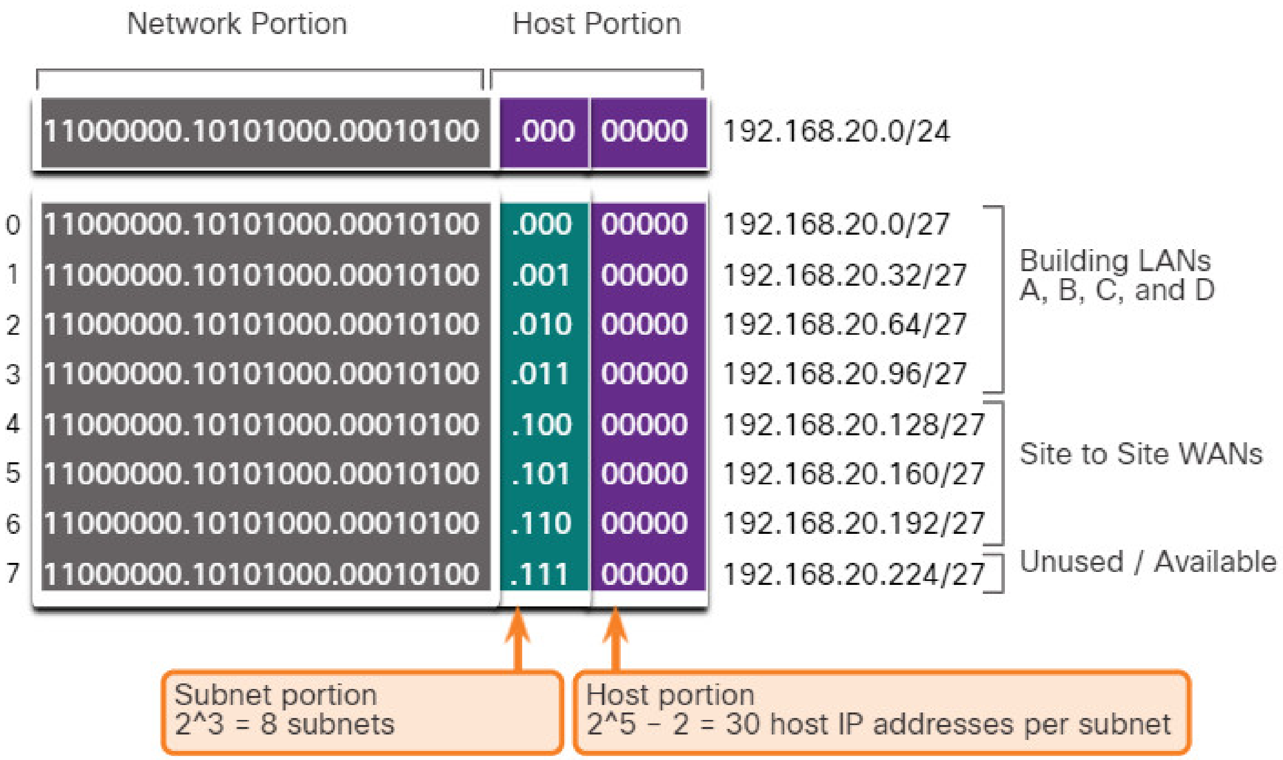
For example, the topology shown in the figure requires seven subnets, one for each of the four LANs, and one for each of the three connections between the routers.



Using traditional subnetting with the given address of 192.168.20.0/24, three bits can be borrowed from the host portion in the last octet to meet the subnet requirement of seven subnets. As shown in the figure, borrowing 3 bits creates 8 subnets and leaves 5 host bits with 30 usable hosts per subnet. This scheme creates the needed subnets and meets the host requirement of the largest LAN.

Basic Subnet Scheme

The diagram shows the basic subnet scheme for a given address of 192.168.20.0/24 with three bits borrowed for subnetting. Having 3 bits for subnetting results in 2 to the power of 3 = 8 subnets. Having 5 bits for hosts results in 2 to the power of 5 – 2 = 30 host IP addresses per subnet. All four octets are shown in binary followed by the dotted decimal format for the given address and for all the subnets created. The given network address in binary is 11000000.10101000.00010100 (network portion highlighted in gray) .00000000 (host portion highlighted in purple) = 192.168.20.0/24. For the subnets listed below, the first 24 bits are highlighted in gray (network portion), the next three bits are highlighted in blue (subnet portion), and the last five bits are the remaining host bits highlighted in purple. Subnet 0 is 11000000.10101000.00010100.00000000 = 192.168.20.0/27. Subnet 1 is 11000000.10101000.00010100.00100000 = 192.168.20.32/27. Subnet 2 is 11000000.10101000.00010100.01000000 = 192.168.20.64/27. Subnet 3 is 11000000.10101000.00010100.01100000 = 192.168.20.96/27. Subnets 0 – 3 are assigned to building LANs A, B, C, and D. Subnet 4 is 11000000.10101000.00010100.10000000 = 192.168.20.128/27. Subnet 5 is 11000000.10101000.00010100.10100000 = 192.168.20.160/27. Subnet 6 is 11000000.10101000.00010100.11000000 = 192.168.20.192/27. Subnets 4, 5, and 6 are assigned to the site to site WANs. Subnet 7 is 11000000.10101000.00010100.11100000 = 192.168.20.224/27. Subnet 7 is unused/available.

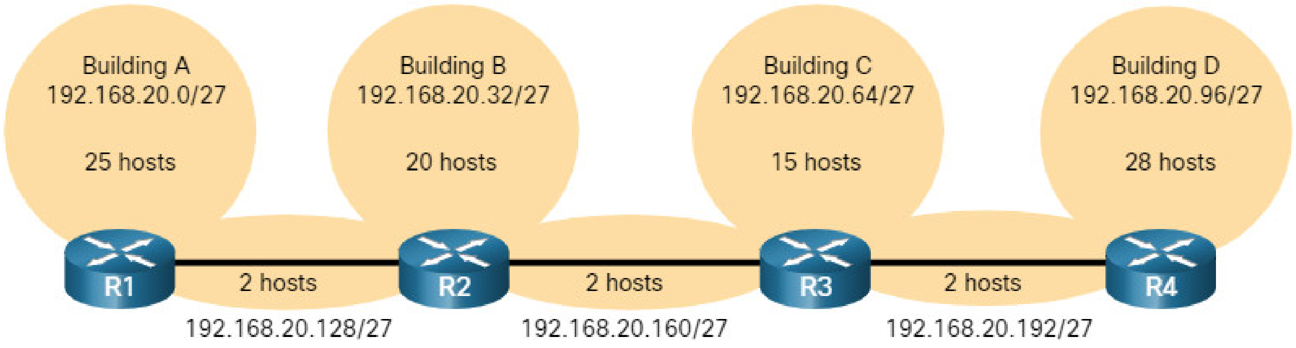


	Network Portion	Host Portion			
	11000000.10101000.00010100	.000	00000	192.168.20.0/24	
0	11000000.10101000.00010100	.000	00000	192.168.20.0/27	Building LANs A, B, C, and D
1	11000000.10101000.00010100	.001	00000	192.168.20.32/27	
2	11000000.10101000.00010100	.010	00000	192.168.20.64/27	
3	11000000.10101000.00010100	.011	00000	192.168.20.96/27	
4	11000000.10101000.00010100	.100	00000	192.168.20.128/27	Site to Site WANs
5	11000000.10101000.00010100	.101	00000	192.168.20.160/27	
6	11000000.10101000.00010100	.110	00000	192.168.20.192/27	
7	11000000.10101000.00010100	.111	00000	192.168.20.224/27	Unused / Available

Subnet portion
2^3 = 8 subnets

Host portion
2^5 – 2 = 30 host IP addresses per subnet

These seven subnets could be assigned to the LAN and WAN networks, as shown in the figure.

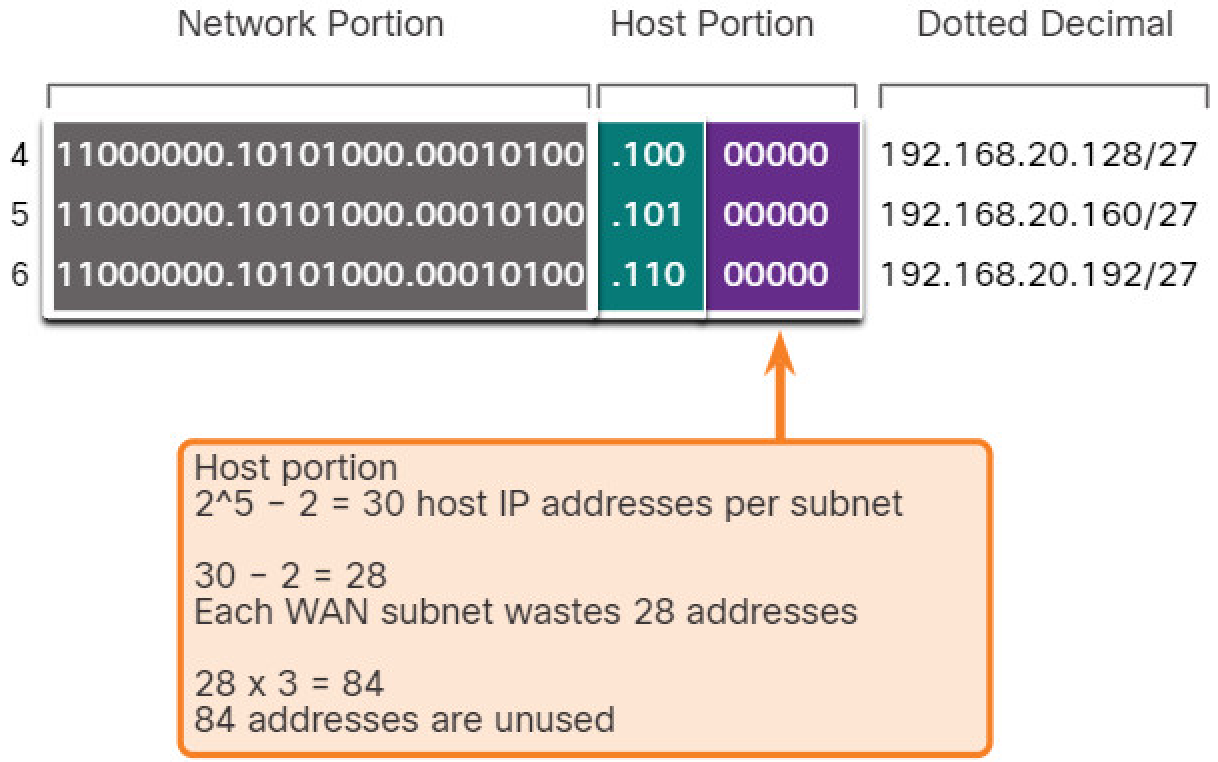


Although this traditional subnetting meets the needs of the largest LAN and divides the address space into an adequate number of subnets, it results in significant waste of unused addresses.

For example, only two addresses are needed in each subnet for the three WAN links. Because each subnet has 30 usable addresses, there are 28 unused addresses in each of these subnets. As shown in the figure, this results in 84 unused addresses (28×3).

Unused Addresses on WAN Subnets

The graphic shows the unused addresses of four WAN subnets using a /27 subnet mask. All four octets are shown in binary followed by the dotted decimal format for the subnet. The first 24 bits are highlighted in gray (network portion), the next three bits are highlighted in blue, and the last five bits are the remaining host bits highlighted in purple. Subnet 4 is 11000000.10101000.00010100.10000000 = 192.168.20.128/27. Subnet 5 is 11000000.10101000.00010100.10100000 = 192.168.20.160/27. Subnet 6 is 11000000.10101000.00010100.11000000 = 192.168.20.192/27. Having 5 bits for hosts results in 2 to the power of 5 – 2 = 30 host IP addresses per subnet. 30 – 2 = 28; each WAN subnet wastes 28 addresses. 28 x 3 = 84; 84 addresses are unused.



	Network Portion	Host Portion		Dotted Decimal
4	11000000.10101000.00010100	.100	00000	192.168.20.128/27
5	11000000.10101000.00010100	.101	00000	192.168.20.160/27
6	11000000.10101000.00010100	.110	00000	192.168.20.192/27

Host portion
2^5 - 2 = 30 host IP addresses per subnet

30 - 2 = 28
Each WAN subnet wastes 28 addresses

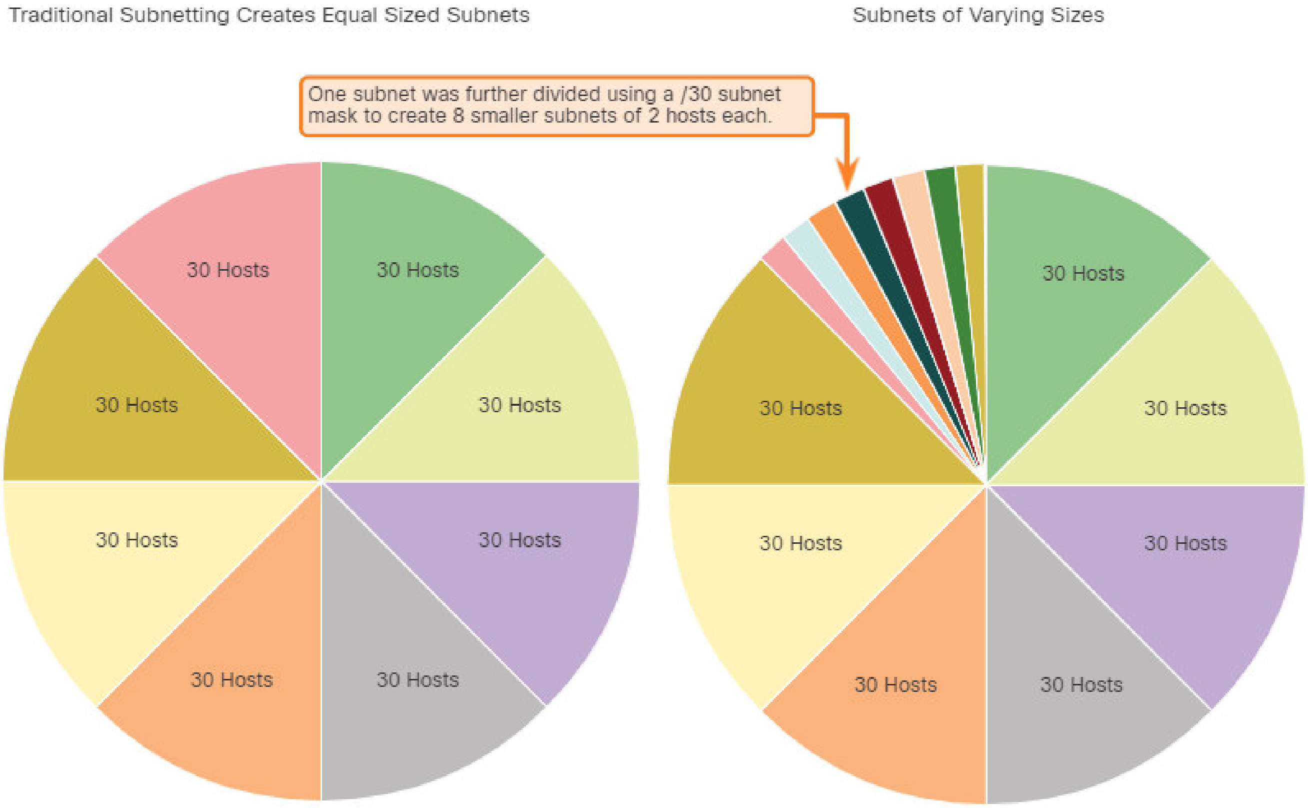
28 x 3 = 84
84 addresses are unused

Further, this limits future growth by reducing the total number of subnets available. This inefficient use of addresses is characteristic of traditional subnetting. Applying a traditional subnetting scheme to this scenario is not very efficient and is wasteful.

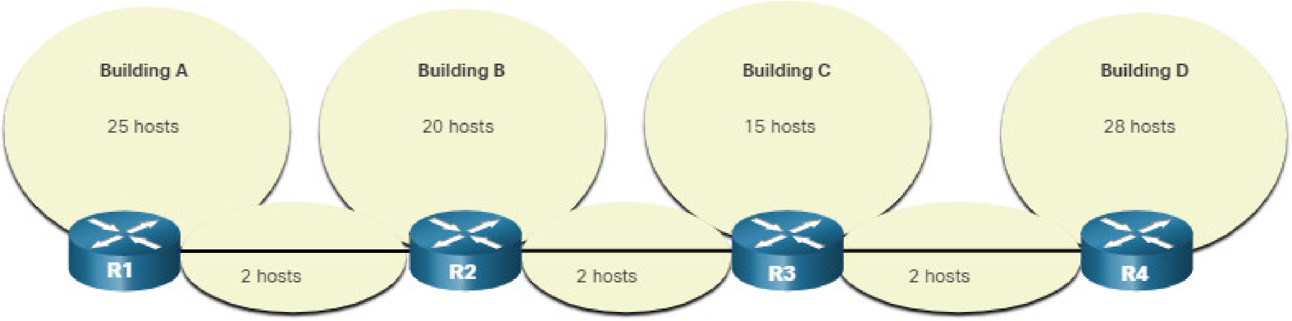
The variable-length subnet mask (VLSM) was developed to avoid wasting addresses by enabling us to subnet a subnet.

11.8.4. VLSM

In all of the previous subnetting examples, the same subnet mask was applied for all the subnets. This means that each subnet has the same number of available host addresses. As illustrated in the left side of the figure, traditional subnetting creates subnets of equal size. Each subnet in a traditional scheme uses the same subnet mask. As shown in the right side of the figure, VLSM allows a network space to be divided into unequal parts. With VLSM, the subnet mask will vary depending on how many bits have been borrowed for a particular subnet, thus the “variable” part of the VLSM.



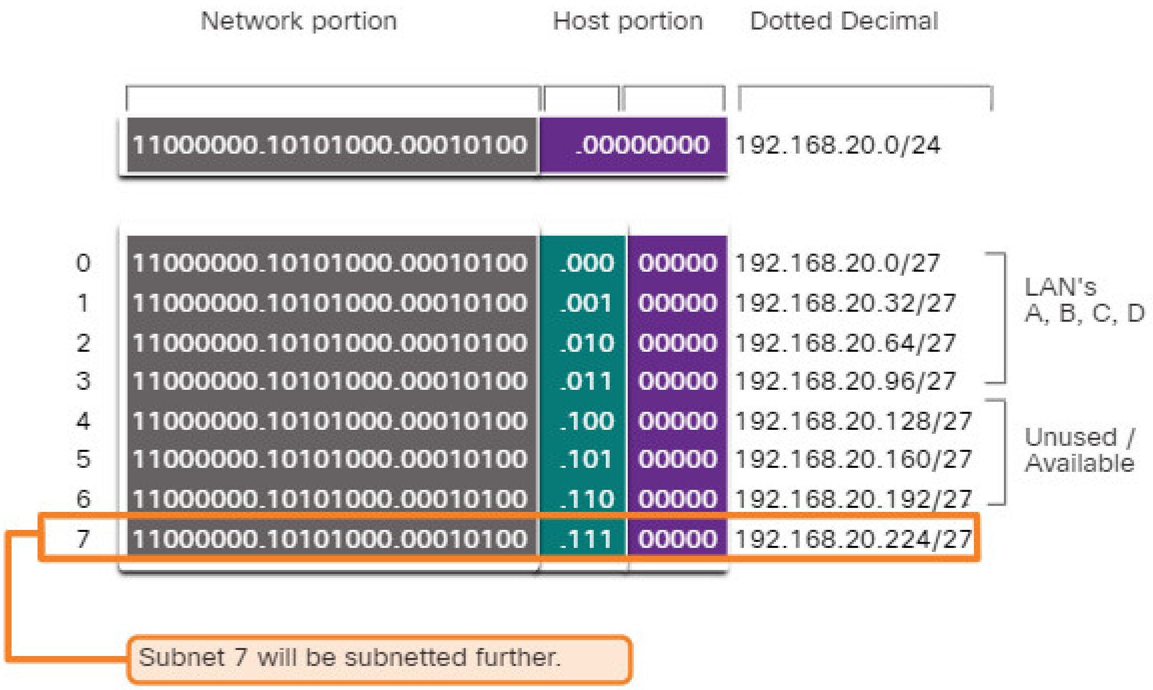
VLSM is just subnetting a subnet. The same topology used previously is shown in the figure. Again, we will use the 192.168.20.0/24 network and subnet it for seven subnets, one for each of the four LANs, and one for each of the three connections between the routers.



The figure shows how network 192.168.20.0/24 subnetted into eight equal-sized subnets with 30 usable host addresses per subnet. Four subnets are used for the LANs and three subnets could be used for the connections between the routers.

Basic Subnetting Scheme

The diagram shows the basic subnet scheme for a given address of 192.168.20.0/24 with three bits borrowed for subnetting. All four octets are shown in binary followed by the dotted decimal format for the given address and for all the subnets created. The given network address in binary is 11000000.10101000.00010100 (network portion highlighted in gray) .00000000 (host portion highlighted in purple) = 192.168.20.0/24. For the subnets listed below, the first 24 bits are highlighted in gray (network portion), the next three bits are highlighted in blue (subnet portion), and the last five bits are the remaining host bits highlighted in purple. Subnet 0 is 11000000.10101000.00010100.00000000 = 192.168.20.0/27. Subnet 1 is 11000000.10101000.00010100.00100000 = 192.168.20.32/27. Subnet 2 is 11000000.10101000.00010100.01000000 = 192.168.20.64/27. Subnet 3 is 11000000.10101000.00010100.01100000 = 192.168.20.96/27. Subnets 0 – 3 are assigned to building LANs A, B, C, and D. Subnet 4 is 11000000.10101000.00010100.10000000 = 192.168.20.128/27. Subnet 5 is 11000000.10101000.00010100.10100000 = 192.168.20.160/27. Subnet 6 is 11000000.10101000.00010100.11000000 = 192.168.20.192/27. Subnets 4, 5, and 6 are unused/available. Subnet 7 is 11000000.10101000.00010100.11100000 = 192.168.20.224/27. Subnet 7 will be subnetted further.



Network portion	Host portion		Dotted Decimal
11000000.10101000.00010100	.00000000		192.168.20.0/24

0	11000000.10101000.00010100	.000	00000	192.168.20.0/27	LAN's A, B, C, D
1	11000000.10101000.00010100	.001	00000	192.168.20.32/27	
2	11000000.10101000.00010100	.010	00000	192.168.20.64/27	
3	11000000.10101000.00010100	.011	00000	192.168.20.96/27	
4	11000000.10101000.00010100	.100	00000	192.168.20.128/27	Unused / Available
5	11000000.10101000.00010100	.101	00000	192.168.20.160/27	
6	11000000.10101000.00010100	.110	00000	192.168.20.192/27	
7	11000000.10101000.00010100	.111	00000	192.168.20.224/27	

Subnet 7 will be subnetted further.

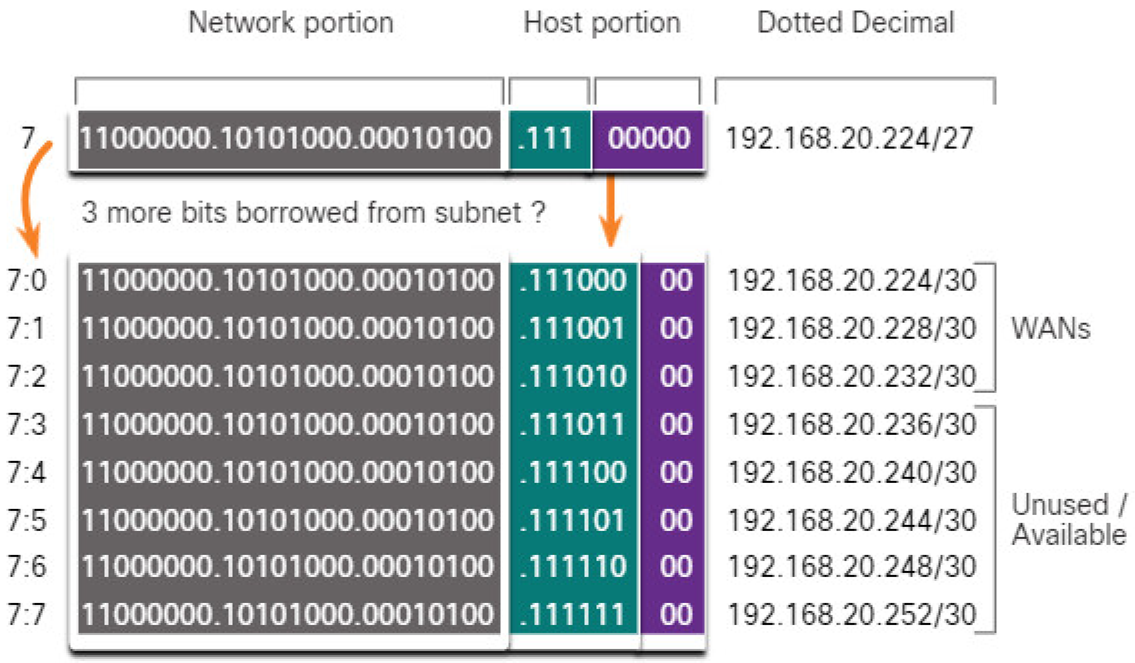
However, the connections between the routers require only two host addresses per subnet (one host address for each router interface). Currently all subnets have 30 usable host addresses per subnet. To avoid wasting 28 addresses per subnet, VLSM can be used to create smaller subnets for the inter-router connections.

To create smaller subnets for the inter-router links, one of the subnets will be divided. In this example, the last subnet, 192.168.20.224/27, will be further subnetted. The figure shows the last subnet has been subnetted further by using the subnet mask 255.255.255.252 or /30.

VLSM Subnetting Scheme

The diagram show the VLSM subnetting scheme when the subnet 192.168.20.224/27 is further subnetted by borrowing 3 more bits. For the original subnet, the first 24 bits represent the network portion and are 11000000.10101000.00010100. The next three bits represent the subnet portion and are 111. The last five bits represent the host portion and are 00000. The address in dotted decimal is 192.168.20.224/27. Borrowing 3 additional bits, subnetting a subnet, results in dividing the original subnet into 8 smaller subnets. For the smaller subnets, the first 24 bits are the network portion, the next six bits are the subnet portion, and the last two bits are the remaining host portion. Subnet 7:0 is 11000000.10101000.00010100.11100000 = 192.168.20.224/30. Subnet 7:1 is 11000000.10101000.00010100.11100100 = 192.168.20.228/30. Subnet 7:2 is 11000000.10101000.00010100.11101000 = 192.168.20.232/30. Subnet 7:3 is 11000000.10101000.00010100.11101100 = 192.168.20.236/30. Subnet 7:4 is 11000000.10101000.00010100.11110000 = 192.168.20.240/30. Subnet 7:5 is 11000000.10101000.00010100.11110100 = 192.168.20.244/30. Subnet 7:6 is

11000000.10101000.00010100.11111000 = 192.168.20.248/30. Subnet 7:7 is 11000000.10101000.00010100.11111100 = 192.168.20.252/30. Subnets 7:0, 7:1, and 7:2 are assigned to the WANs and the remaining subnets are unused/available.



	Network portion	Host portion		Dotted Decimal	
7	11000000.10101000.00010100	.111	00000	192.168.20.224/27	

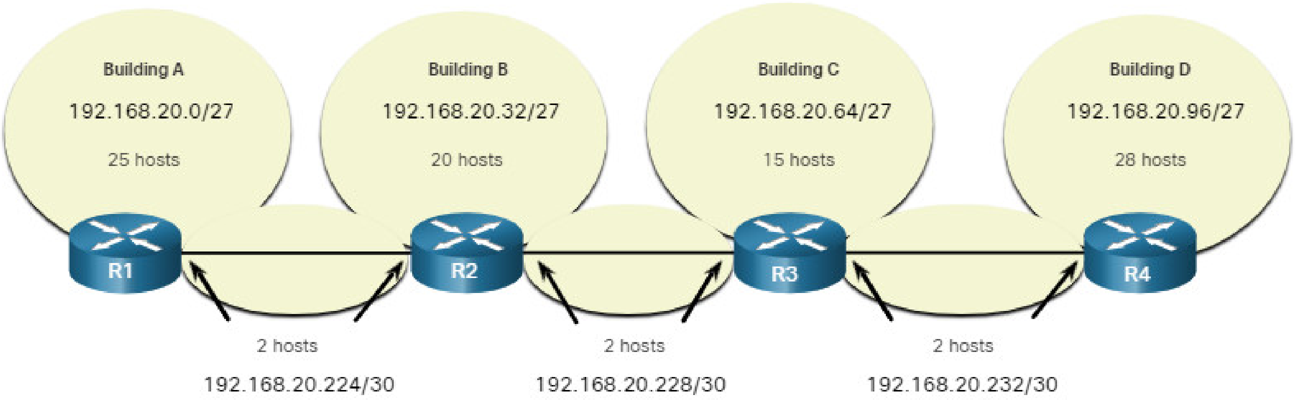
3 more bits borrowed from subnet ?

	Network portion	Host portion		Dotted Decimal	
7:0	11000000.10101000.00010100	.111000	00	192.168.20.224/30	WANs
7:1	11000000.10101000.00010100	.111001	00	192.168.20.228/30	
7:2	11000000.10101000.00010100	.111010	00	192.168.20.232/30	
7:3	11000000.10101000.00010100	.111011	00	192.168.20.236/30	Unused / Available
7:4	11000000.10101000.00010100	.111100	00	192.168.20.240/30	
7:5	11000000.10101000.00010100	.111101	00	192.168.20.244/30	
7:6	11000000.10101000.00010100	.111110	00	192.168.20.248/30	
7:7	11000000.10101000.00010100	.111111	00	192.168.20.252/30	

Subnetting a subnet

Why /30? Recall that when the number of needed host addresses is known, the formula 2n-2 (where n equals the number of host bits remaining) can be used. To provide two usable addresses, two host bits must be left in the host portion.

Because there are five host bits in the subnetted 192.168.20.224/27 address space, three more bits can be borrowed, leaving two bits in the host portion. The calculations at this point are exactly the same as those used for traditional subnetting. The bits are borrowed, and the subnet ranges are determined. The figure shows how the four /27 subnets have been assigned to the LANs and three of the /30 subnets have been assigned to the inter-router links.



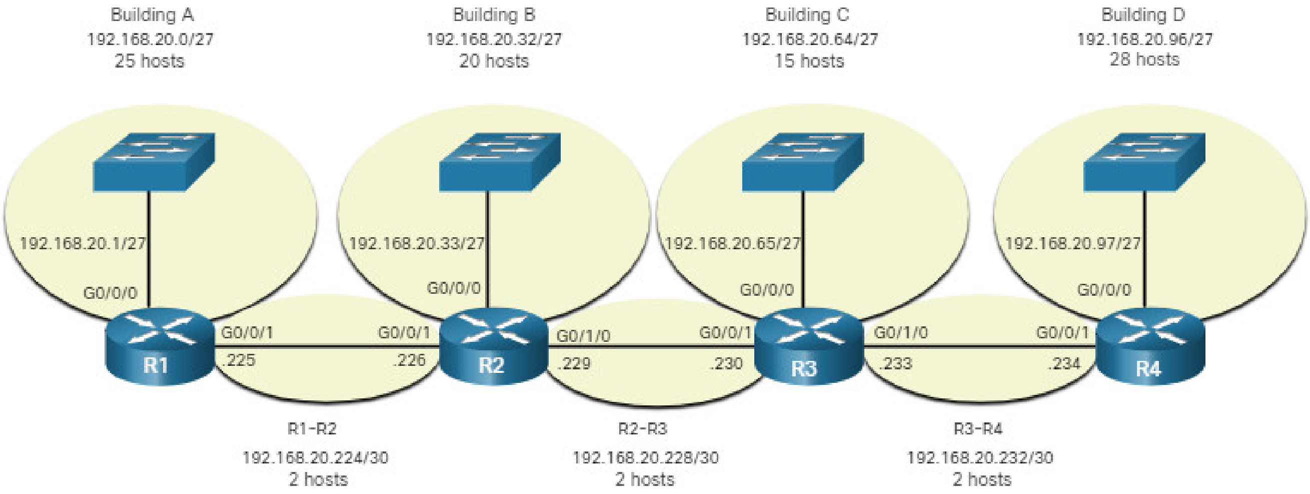
This VLSM subnetting scheme reduces the number of addresses per subnet to a size appropriate for the networks that require fewer subnets. Subnetting subnet 7 for inter-router links, allows subnets 4, 5, and 6 to be available for future networks, as well as five additional subnets available for inter-router connections.

Note: When using VLSM, always begin by satisfying the host requirements of the largest subnet. Continue subnetting until the host requirements of the smallest subnet are satisfied.

11.8.5. VLSM Topology Address Assignment

Using the VLSM subnets, the LAN and inter-router networks can be addressed without unnecessary waste.

The figure shows the network address assignments and the IPv4 addresses assigned to each router interface.



Using a common addressing scheme, the first host IPv4 address for each subnet is assigned to the LAN interface of the router. Hosts on each subnet will have a host IPv4 address from the range of host addresses for that subnet and an appropriate mask. Hosts will use the address of the attached router LAN interface as the default gateway address.

The table shows the network addresses and range of host addresses for each network. The default gateway address is displayed for the four LANs.

	Network Address	Range of Host Addresses	Default Gateway Address
Building A	192.168.20.0/27	192.168.20.1/27 to 192.168.20.30/27	192.168.20.1/27
Building B	192.168.20.32/27	192.168.20.33/27 to 192.168.20.62/27	192.168.20.33/27

	Network Address	Range of Host Addresses	Default Gateway Address
Building C	192.168.20.64/27	192.168.20.65/27 to 192.168.20.94/27	192.168.20.65/27
Building D	192.168.20.96/27	192.168.20.97/27 to 192.168.20.126/27	192.168.20.97/27
R1-R2	192.168.20.224/30	192.168.20.225/30 to 192.168.20.226/30	
R2-R3	192.168.20.228/30	192.168.20.229/30 to 192.168.20.230/30	
R3-R4	192.168.20.232/30	192.168.20.233/30 to 192.168.20.234/30	

11.9. Structured Design

11.9.1. IPv4 Network Address Planning

Before you start subnetting, you should develop an IPv4 addressing scheme for your entire network. You will need to know how many subnets you need, how many hosts a particular subnet requires, what devices are part of the subnet, which parts of your network use private addresses, and which use public, and many other determining factors. A good addressing scheme allows for growth. A good addressing scheme is also the sign of a good network administrator.

Planning IPv4 network subnets requires you to examine both the needs of an organization's network usage, and how the subnets will be structured. Performing a network requirement study is the starting point. This means looking at the entire network, both the intranet and the DMZ, and determining how each area will be segmented. The address plan includes determining where address conservation is needed (usually within the DMZ), and where there is more flexibility (usually within the intranet).

Where address conservation is required, the plan should determine how many subnets are needed and how many hosts per subnet. As discussed earlier, this is usually required for public IPv4 address space within the DMZ. This will most likely include using VLSM.

Within the corporate intranet, address conservation is usually less of an issue This is largely due to using private IPv4 addressing, including 10.0.0.0/8, with over 16 million host IPv4 addresses.

For most organizations, private IPv4 addresses allow for more than enough internal (intranet) addresses. For many larger organizations and ISPs, even private IPv4 address space is not large enough to accommodate their internal needs. This is another reason why organizations are transitioning to IPv6.

For intranets that use private IPv4 addresses and DMZs that use public IPv4 addresses, address planning and assignment is important.

Where required, the address plan includes determining the needs of each subnet in terms of size. How many hosts there will be per subnet? The address plan also needs to include how host addresses will be assigned, which hosts will require static IPv4 addresses, and which hosts can use DHCP for obtaining their addressing information. This will also help prevent the duplication of addresses, while allowing for monitoring and managing of addresses for performance and security reasons.

Knowing your IPv4 address requirements will determine the range, or ranges, of host addresses that you implement and help ensure that there are enough addresses to cover your network needs.

11.9.2. Device Address Assignment

Within a network, there are different types of devices that require addresses:

- **End user clients** – Most networks allocate IPv4 addresses to client devices dynamically, using Dynamic Host Configuration Protocol (DHCP). This reduces the burden on network support staff and virtually eliminates entry errors. With DHCP, addresses are only leased for a period of time, and can be reused when the lease expires. This is an important feature for networks that support transient users and wireless devices. Changing the subnetting scheme means that the DHCP server needs to be reconfigured, and the clients must renew their IPv4 addresses. IPv6 clients can obtain address information using DHCPv6 or SLAAC.
- **Servers and peripherals** – These should have a predictable static IP address. Use a consistent numbering system for these devices.
- **Servers that are accessible from the internet** – Servers that need to be publicly available on the internet must have a public IPv4 address, most often accessed using NAT. In some organizations, internal servers (not publicly available) must be made available to the remote users. In most cases, these servers are assigned private addresses internally, and the user is required to create a virtual private network (VPN) connection to access the server. This has the same effect as if the user is accessing the server from a host within the intranet.
- **Intermediary devices** – These devices are assigned addresses for network management, monitoring, and security. Because we must know how to communicate with intermediary devices, they should have predictable, statically assigned addresses.

- **Gateway** – Routers and firewall devices have an IP address assigned to each interface which serves as the gateway for the hosts in that network. Typically, the router interface uses either the lowest or highest address in the network.

When developing an IP addressing scheme, it is generally recommended that you have a set pattern of how addresses are allocated to each type of device. This benefits administrators when adding and removing devices, filtering traffic based on IP, as well as simplifying documentation.

11.9.3. Packet Tracer – VLSM Design and Implementation Practice

In this activity, you are given a /24 network address to use to design a VLSM addressing scheme. Based on a set of requirements, you will assign subnets and addressing, configure devices, and verify connectivity.

11.9.3 Packet Tracer – VLSM Design and Implementation Practice

11.10. Module Practice and Quiz

11.10.1. Packet Tracer – Design and Implement a VLSM Addressing Scheme

In this lab you will design a VLSM addressing scheme given a network address and host requirements. You will configure addressing on routers, switches, and network hosts.

- Design a VLSM IP addressing scheme given requirements.
- Configure addressing on network devices and hosts.
- Verify IP connectivity.
- Troubleshoot connectivity issues as required.

11.10.1 Packet Tracer – Design and Implement a VLSM Addressing Scheme

11.10.2. Lab – Design and Implement a VLSM Addressing Scheme

Skills Practice Opportunity
You have the opportunity to practice the following skills:

Part 1: Examine Network Requirements
Part 2: Design the VLSM Address Scheme
Part 3: Cable and Configure the IPv4 Network

You can practice these skills using the Packet Tracer or lab equipment, if available.

Packet Tracer – Physical Mode (PTPM)

11.10.2 Packet Tracer – Design and Implement a VLSM Addressing Scheme – Physical Mode

Lab Equipment

11.10.2 Lab – Design and Implement a VLSM Addressing Scheme

11.10.3. What did I learn in this module?

IPv4 Addressing Structure

An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion. 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. A host requires a unique IPv4 address and a subnet mask to show the network/host portions of the address. The prefix length is the number of bits set to 1 in the subnet mask. It is written in "slash notation", which is a "/" followed by the number of bits set to 1. Logical AND is the comparison of two bits. Only a 1 AND 1 produces a 1 and all other combination results in a 0. Any other combination results in a 0. Within each network there are network addresses, host addresses, and a broadcast address.

IPv4 Unicast, Broadcast, and Multicast

Unicast transmission refers to a device sending a message to one other device in one-to-one communications. A unicast packet is a packet with a destination IP address that is a unicast address which is the address of a single recipient. Broadcast transmission refers to a device sending a message to all the devices on a network in one-to-all communications. A broadcast packet has a destination IP address with all ones (1s) in the host portion, or 32 one (1) bits. Multicast transmission reduces traffic by allowing a host to send a single packet to a selected set of hosts that subscribe to a multicast group. A multicast packet is a packet with a destination IP address that is a multicast address. IPv4 has reserved the 224.0.0.0 to 239.255.255.255 addresses as a multicast range.

Types of IPv4 Addresses

Public IPv4 addresses are globally routed between ISP routers. Not all available IPv4 addresses can be used on the internet. There are blocks of addresses called private addresses that are used by most organizations to assign IPv4 addresses to internal hosts. Most internal networks use private IPv4 addresses for addressing all internal devices (intranet); however, these private addresses are not globally routable. Loopback addresses used by a host to direct traffic back to itself. Link-local addresses are more commonly known as APIPA addresses, or self-assigned addresses. In 1981, IPv4 addresses were assigned using classful addressing: A, B, or C. Public IPv4 addresses must be unique, and are globally routed over the internet. Both IPv4 and IPv6 addresses are managed by the IANA, which allocates blocks of IP addresses to the RIRs.

Network Segmentation

In an Ethernet LAN, devices broadcast to locate other devices using ARP. Switches propagate broadcasts out all interfaces except the interface on which it was received. Routers do not propagate broadcasts, instead each router interface connects a broadcast domain and broadcasts are only propagated within that specific domain. A large broadcast domain is a network that connects many hosts. A problem with a large broadcast domain is that these hosts can generate excessive broadcasts and negatively affect the network. The solution is to reduce the size of the network to create smaller broadcast domains in a process called subnetting. These smaller network spaces are called subnets. Subnetting reduces overall network traffic and improves network performance. An administrator may subnet by location, between networks, or by device type.

Subnet an IPv4 Network

IPv4 subnets are created by using one or more of the host bits as network bits. This is done by extending the subnet mask to borrow some of the bits from the host portion of the address to create additional network bits. The more host bits that are borrowed, the more subnets that can be defined. The more bits that are borrowed to increase the number of subnets also reduces the number of hosts per subnet. Networks are most easily subnetted at the octet boundary of /8, /16, and /24. Subnets can borrow bits from any host bit position to create other masks.

Subnet a /16 and a /8 Prefix

In a situation requiring a larger number of subnets, an IPv4 network is required that has more hosts bits available to borrow. To create subnets, you must borrow bits from the host portion of the IPv4 address of the existing internetwork. Starting from the left to the right with the first available host bit, borrow a single bit at a time until you reach the number of bits necessary to create the number of subnets required. When borrowing bits from a /16 address, start borrowing bits in the third octet, going from left to right. The first address is reserved for the network address and the last address is reserved for the broadcast address.

Subnet to Meet Requirements

A typical enterprise network contains an intranet and a DMZ. Both have subnetting requirements and challenges. The intranet uses private IPv4 addressing space. The 10.0.0.0/8 can also be subnetted using any other number of prefix lengths, such as /12, /18, /20, etc., giving the network administrator many options. Because these devices need to be publicly accessible from the internet, the devices in the DMZ require public IPv4 addresses.

Organizations must maximize their own limited number of public IPv4 addresses. To reduce the number of unused host addresses per subnet, the network administrator must subnet their public address space into subnets with different subnet masks. This is known as Variable Subnet Length Masking (VLSM). Administrators must consider how many host addresses are required for each network, and how many subnets are needed.

Variable Length Subnet Masking

Traditional subnetting might meet an organization’s needs for its largest LAN and divide the address space into an adequate number of subnets. But it likely also results in significant waste of unused addresses. VLSM allows a network space to be divided into unequal parts. With VLSM, the subnet mask will vary depending on how many bits have been borrowed for a particular subnet (this is the “variable” part of the VLSM). VLSM is just subnetting a subnet. When using VLSM, always begin by satisfying the host requirements of the largest subnet. Continue subnetting until the host requirements of the smallest subnet are satisfied. Subnets always need to be started on an appropriate bit boundary.

Structured Design

A network administrator should study the network requirements to better plan how the IPv4 network subnets will be structured. This means looking at the entire network, both the intranet and the DMZ, and determining how each area will be segmented. The address plan includes determining where address conservation is needed (usually within the DMZ), and where there is more flexibility (usually within the intranet). Where address conservation is required the plan should determine how many subnets are needed and how many hosts per subnet. This is usually required for public IPv4 address space within the DMZ. This will most likely include using VLSM. The address plan includes how host addresses will be assigned, which hosts will require static IPv4 addresses, and which hosts can use DHCP for obtaining their addressing information. Within a network, there are different types of devices that require addresses: end user clients, servers and peripherals, servers that are accessible from the internet, intermediary devices, and gateways. When developing an IP addressing scheme, have a set pattern of how addresses are allocated to each type of device. This helps when adding and removing devices, filtering traffic based on IP, as well as simplifying documentation.

11.10.4 Module Quiz – IPv4 Addressing

Download Slide Powerpoint (PPT)

PPT

CCNA 1 v7.0 Curriculum: Module 11 - IPv4 Addressing.pptx

1 file(s) 2.41 MB

Download

Tags:ccna 1 v7 modules