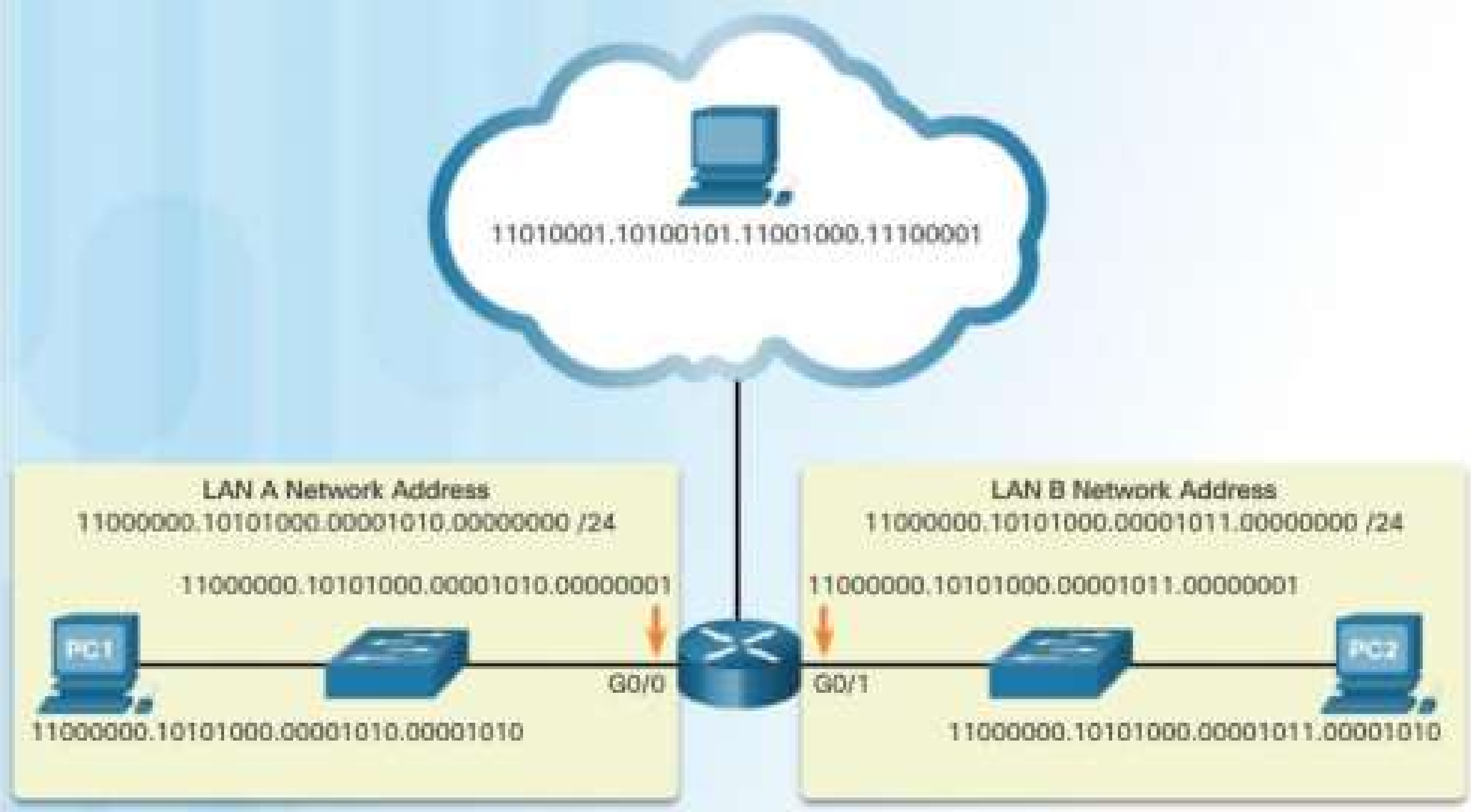
IPv4 Addresses

Binary

- Binary is a numbering system that consists of the numbers 0 and 1 called bits. In contrast, the decimal numbering system consists of 10 digits consisting of the numbers 0 – 9.
- Binary is important to understand because hosts, servers, and network devices use binary addressing. Specifically, they use binary IPv4 addresses to identify each other.
- Each address consists of a string of 32 bits, divided into four sections called octets. Each octet contains 8 bits (or 1 byte) separated with a dot.
- For example, PC1 in the figure is assigned IPv4 address 11000000.10101000.00001010.00001010. Its default gateway address would be that of R1 Gigabit Ethernet interface 11000000.10101000.00001010.00000001.

- IPv4 addresses are commonly expressed in dotted decimal notation as shown in the figure below. PC1 is assigned IPv4 address 192.168.10.10, and its default gateway address is 192.168.10.1.



Binary to Decimal Conversion

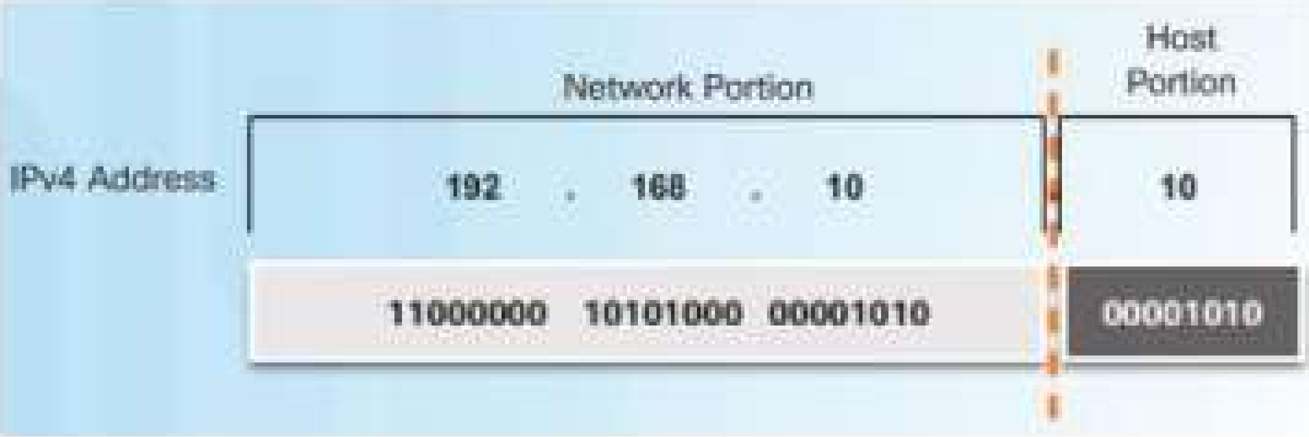
- To convert a binary IPv4 address to its dotted decimal equivalent, divide the IPv4 address into four 8-bit octets.
- Next apply the binary positional value to all octets binary number and calculate accordingly.
- For example, consider that 11000000.10101000.00001011.00001010 is the binary IPv4 address of a host.

Decimal to Binary Conversion

Examples Consider the IP address 192.168.11.10.

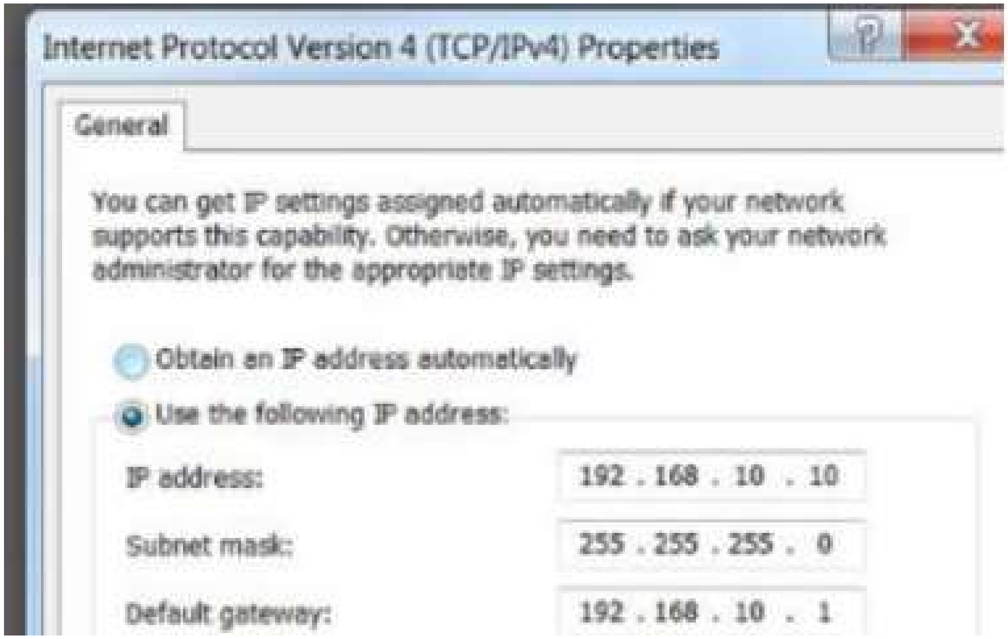
Network and Host Portions

- An IPv4 address is a hierarchical address that is made up of a network portion and a host portion. Within the 32-bit stream, a portion of the bits identify the network, and a portion of the bits identify the host as shown in the figure.
- 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 job of the subnet mask.


Network Portion
Host Portion
IPv4 Address
192 . 168 . 10
10
11000000 10101000 00001010
00001010

Subnet Mask

- Three dotted decimal IPv4 addresses must be configured when assigning an IPv4 configuration to host:
  - IPv4 address – Unique IPv4 address of the host
  - Subnet mask- Used to identify the network/host portion of the IPv4 address
  - Default gateway – Identifies the local gateway (i.e. local router interface IPv4 address) to reach remote networks



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

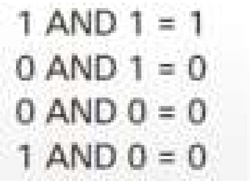
Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 10 . 1

- When an IPv4 address is assigned to a device, the subnet mask is used to determine the network address where the device belongs. The network address represents all the devices on the same network.
- 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 below. The 1s in the subnet mask identify the network portion while the 0s identify the host portion.
- 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 these portions in a given IPv4 address.
- The actual process used to identify the network portion and host portion is called ANDing

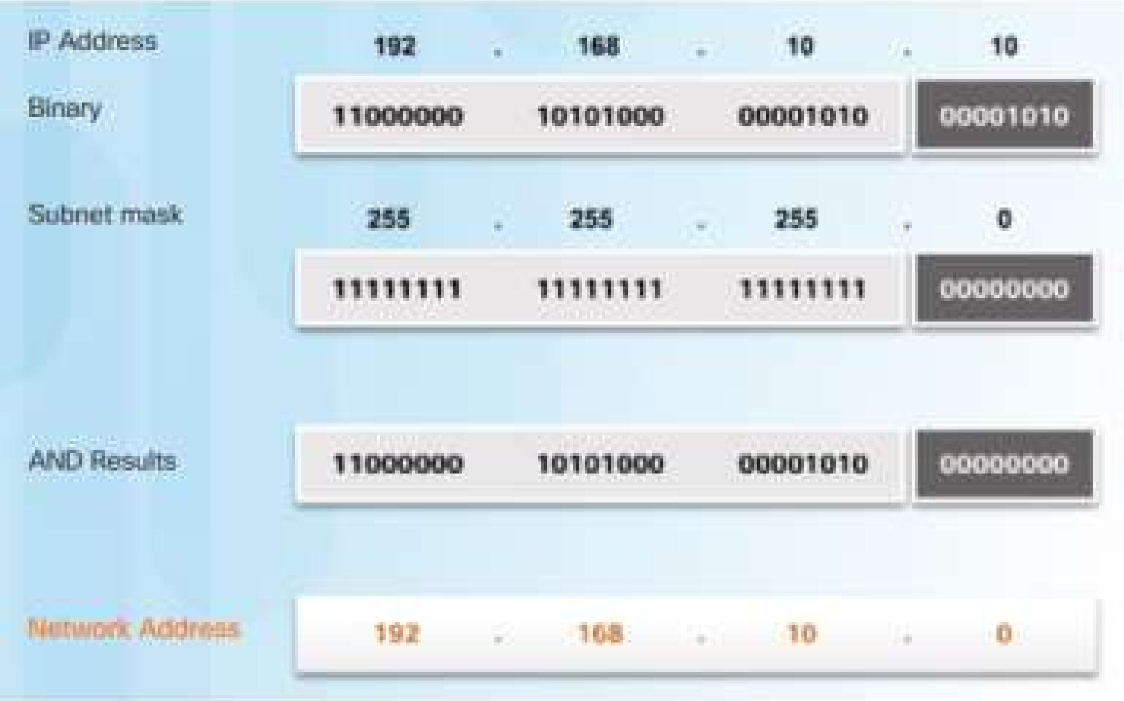
Logical AND

- A logical AND is one of three basic binary operations used in digital logic. The other two are OR and NOT. While all three are used in data networks, only AND is used in determining the network address. Logical AND is the comparison of two bits that produce the results below.



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

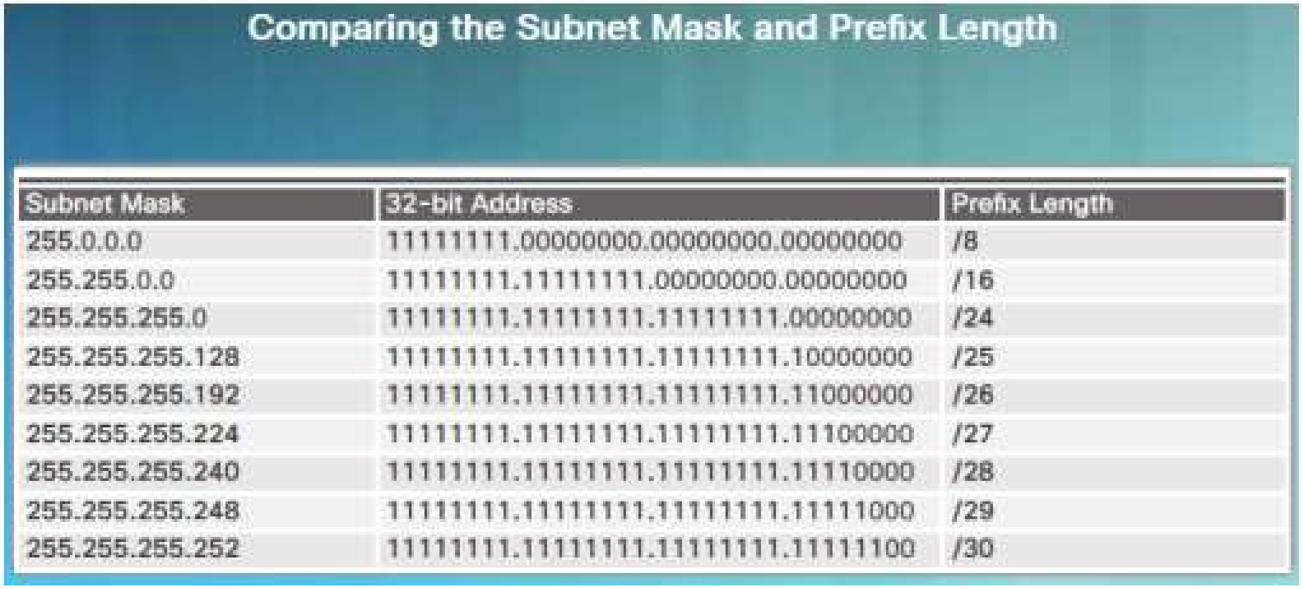
- To identify the network address of an IPv4 host, the IPv4 address is logically ANDed, bit by bit, with the subnet mask. ANDing between the address and the subnet mask yields the network address. For example, consider a host with IPv4 address 192.168.10.10 and subnet mask of 255.255.255.0.



IP Address	192	.	168	.	10	.	10
Binary	11000000		10101000		00001010		00001010
Subnet mask	255	.	255	.	255	.	0
	11111111		11111111		11111111		00000000
AND Results	11000000		10101000		00001010		00000000
Network Address	192	.	168	.	10	.	0

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 a “/” 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. For example, refer to the table in the figure. 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.

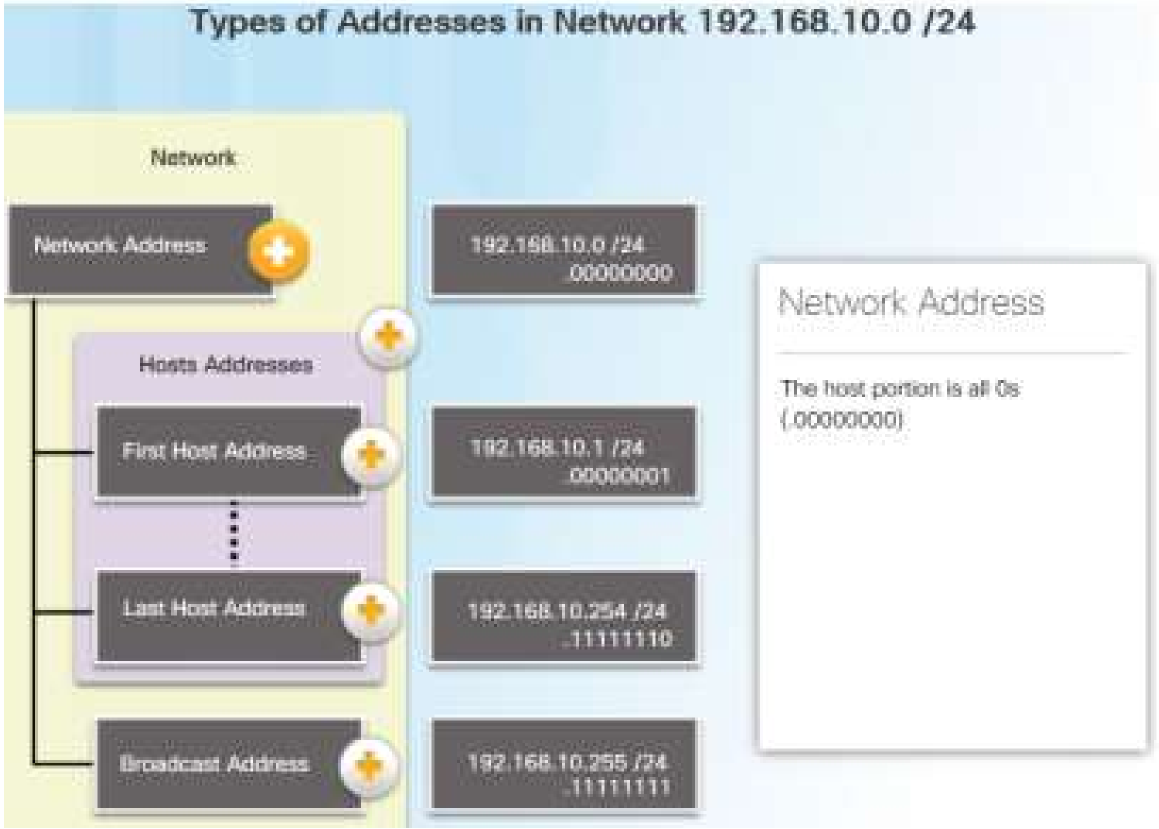


Comparing the Subnet Mask and Prefix Length

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
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

Network, Host and Broadcast Addresses

- Each network address contains (or identifies) host addresses and a broadcast address as described in the figure below.



Types of Addresses in Network 192.168.10.0 /24

Network

Network Address

192.168.10.0 /24
.00000000

Hosts Addresses

First Host Address

192.168.10.1 /24
.00000001

Last Host Address

192.168.10.254 /24
.11111110

Broadcast Address

192.168.10.255 /24
.11111111

Network Address

The host portion is all 0s
(.00000000)

Static IPv4 Address

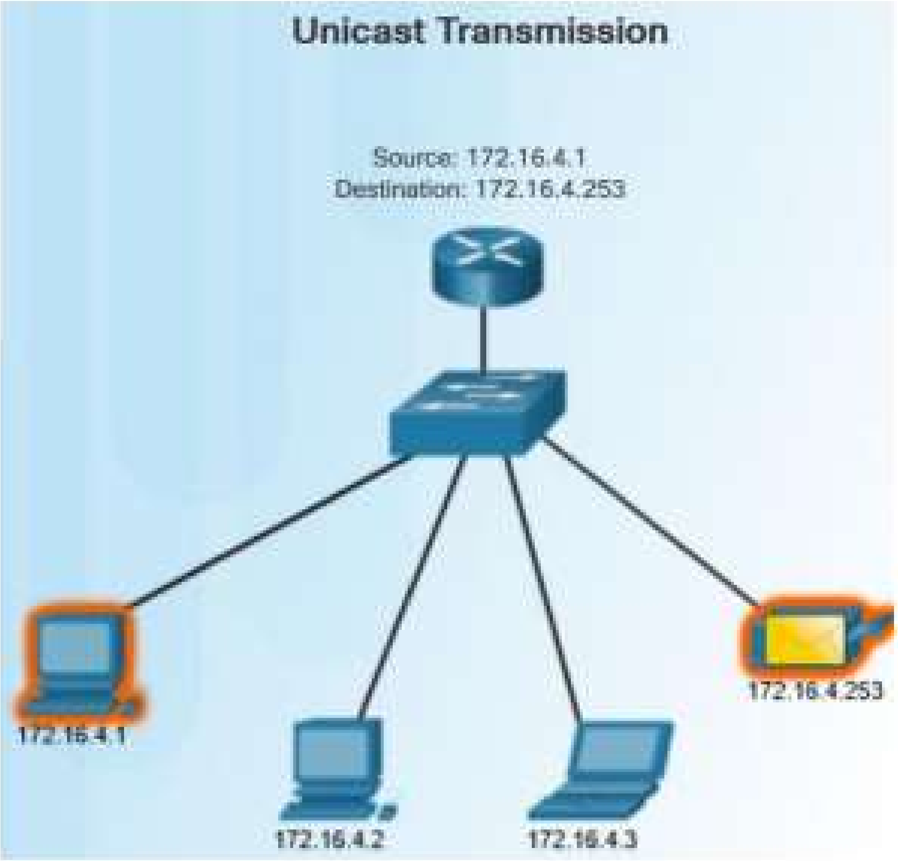
- Assignment to a host devices can be assigned an IP address either statically or dynamically.
- In networks, some devices require a fixed IP address. For instance, printers, servers, and networking devices need an IP address that does not change. For this reason, these devices are typically assigned static IP addresses.
- A host can also be configured with a static IPv4 address such as shown in the figure. Assigning hosts static IP addresses is acceptable in small networks. However, it would be time-consuming to enter static addresses on each host in a large network. It is important to maintain an accurate list of static IP addresses assigned to each device.

Dynamic IPv4 Address

- Host devices are assigned IPv4 addresses dynamically using the Dynamic Host Configuration Protocol (DHCP).
- A host can obtain IPv4 addressing information automatically. The host is a DHCP client and requests IPv4 address information from a DHCP server. The DHCP server provides an IPv4 address, subnet mask, default gateway, and other configuration information.
- DHCP is generally the preferred method of assigning IPv4 addresses to hosts on large networks. An additional benefit of DHCP is the address is not permanently assigned to a host but is only "leased" for a period of time. If the host is powered down or taken off the network, the address is returned to the pool for reuse. This feature is especially helpful for mobile users that come and go on a network

Unicast Transmission

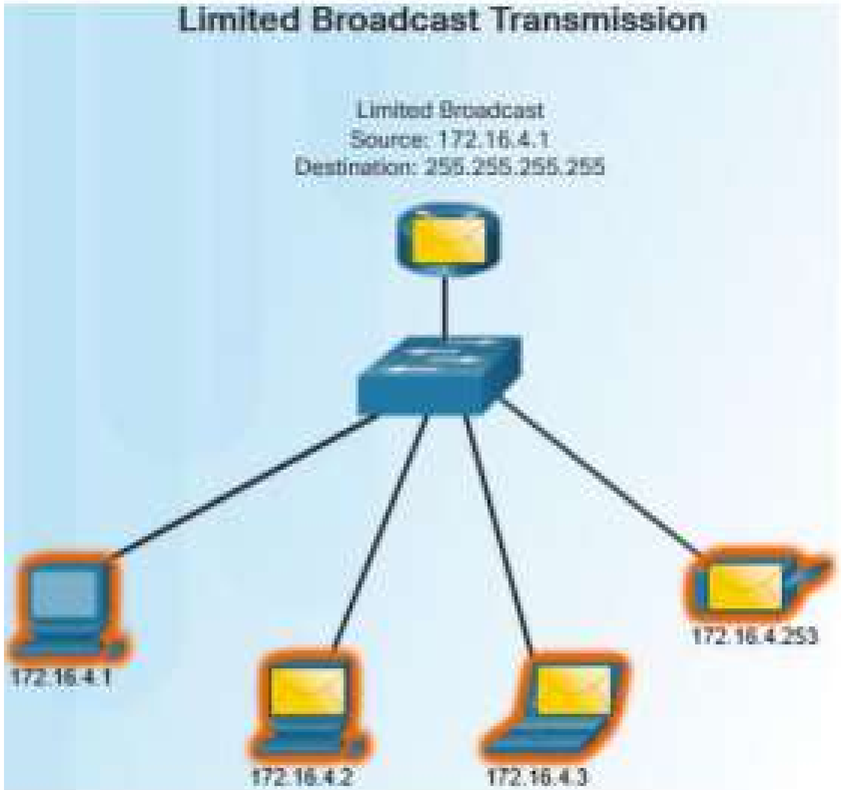
- Unicast communication is used for normal host-to-host communication in both a client/server and a peer-to-peer network. Unicast packets use the address of the destination device as the destination address and can be routed through an internetwork.
- In an IPv4 network, the unicast address applied to an end device is referred to as the host address. For unicast communication, the addresses assigned to the two end devices are used as the source and destination IPv4 addresses. During the encapsulation process, the source host uses its IPv4 address as the source address and the IPv4 address of the destination host as the destination address. Regardless of whether the destination specified a packet as a unicast, broadcast or multicast; the source address of any packet is always the unicast address of the originating host.
- IPv4 unicast host addresses are in the address range of 0.0.0.0 to 223.255.255.255. However, within this range are many addresses that are reserved for special purposes.


Unicast Transmission
Source: 172.16.4.1
Destination: 172.16.4.253
172.16.4.1
172.16.4.2
172.16.4.3
172.16.4.253

Broadcast Transmission

- Broadcast traffic is used to send packets to all hosts in the network using the broadcast address for the network.
- With a broadcast, the packet contains a destination IPv4 address with all ones (1s) in the host portion. This means that all hosts on that local network (broadcast domain) will receive and look at the packet. Many network protocols, such as DHCP, use broadcasts. When a host receives a packet sent to the network broadcast address, the host processes the packet as it would a packet addressed to its unicast address.
- 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.

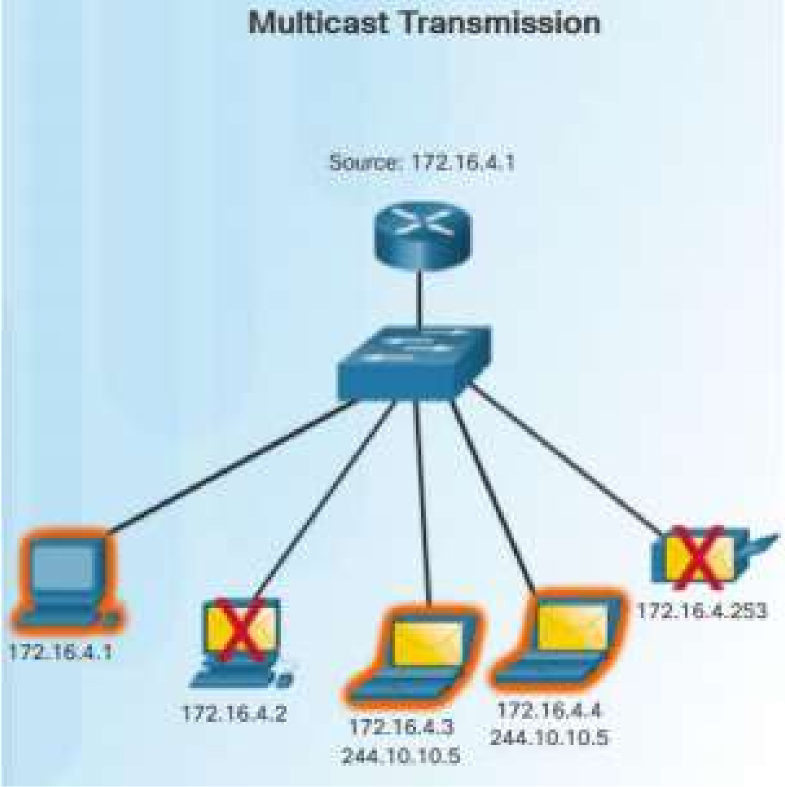
- As an example, a host within the 172.16.4.0/24 network would broadcast to all hosts in its network using a packet with a destination address of 255.255.255.255.
- When a packet is broadcast, it uses resources on the network and causes every receiving host on the network to process the packet. Therefore, broadcast traffic should be limited so that it does not adversely affect the performance of the network or devices. Because routers separate broadcast domains, subdividing networks can improve network performance by eliminating excessive broadcast traffic.


Limited Broadcast Transmission
Limited Broadcast
Source: 172.16.4.1
Destination: 255.255.255.255
172.16.4.1
172.16.4.2
172.16.4.3
172.16.4.253

Multicast Transmission

- 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.
- IPv4 has reserved the 224.0.0.0 to 239.255.255.255 addresses as a multicast range. The IPv4 multicast addresses 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network only. These addresses are to be used for multicast groups on a local network.
- A router connected to the local network recognizes that these packets are addressed to a local network multicast group and never forwards them further.

- Hosts that receive particular multicast data are called multicast clients. The multicast clients use services requested by a client program to subscribe to the multicast group.
- Each multicast group is represented by a single IPv4 multicast destination address. When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address, and packets addressed to its uniquely allocated unicast address.



Multicast Transmission

Private Addresses

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

Private Addresses

- The private address blocks are:
- 10.0.0.0 to 10.255.255.255 (10.0.0.0 /8)
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255 (192.168.0.0 /24)

- Private space address blocks are set aside for use in private networks. The use of these addresses need not be unique among outside networks. Hosts that do not require access to the Internet at large may make unrestricted use of private addresses. However, the internal networks still must design network address schemes to ensure that the hosts in the private networks use IP addresses that are unique within their networking environment.
- Many hosts in different networks may use the same private space addresses. Packets using these addresses as the source or destination should not appear on the public Internet. The router or firewall device at the perimeter of these private networks must block or translate these addresses. Even if these packets were to make their way to the Internet, the routers would not have routes to forward them to the appropriate private network.

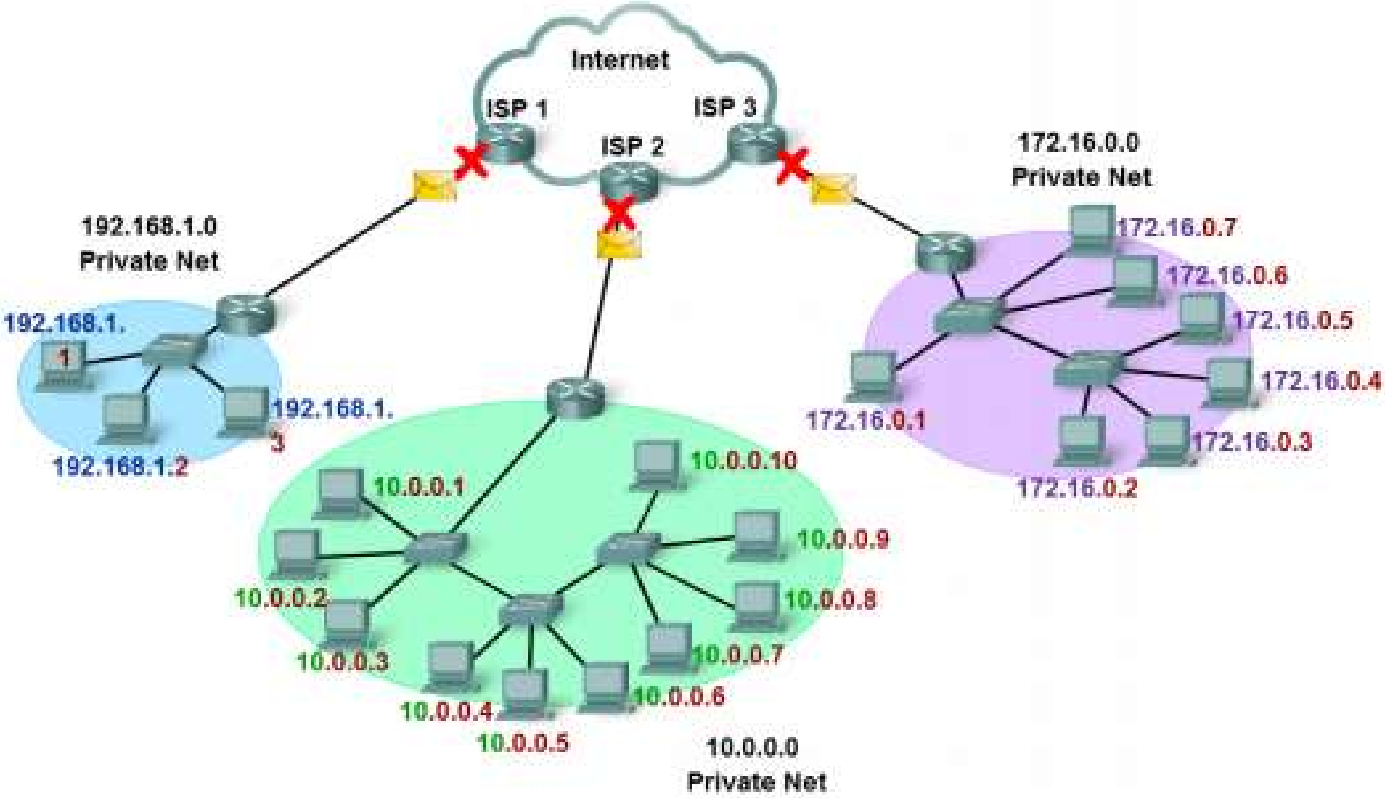
Network Address Translation

- With services to translate private addresses to public addresses, hosts on a privately addressed network can have access to resources across the Internet. These services, called Network Address Translation (NAT), can be implemented on a device at the edge of the private network.
- NAT allows the hosts in the network to "borrow" a public address for communicating to outside networks. While there are some limitations and performance issues with NAT, clients for most applications can access services over the Internet without noticeable problems.

Public Addresses

- The vast majority of the addresses in the IPv4 unicast host range are public addresses.
- These addresses are designed to be used in the hosts that are publicly accessible from the Internet. Even within these address blocks, there are many addresses that are designated for other special purposes.
- Class A 1.0.0.0 - 9.255.255.255, 11.0.0.0 – 126.255.255.255
- Class B 128.0.0.0 – 172.15.255.255, 172.32.0.0 – 191.255.255.255
- Class C 192.0.0.0 – 192.167.255.255, 192.169.0.0 – 223.255.255.255

Private Addresses Used in Networks without NAT



Special IP Addresses

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

Default Route

- Also presented earlier, we represent the IPv4 default route as 0.0.0.0. The default route is used as a "catch all" route when a more specific route is not available.
- The use of this address also reserves all addresses in the 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8) address block.

Loopback

- One such reserved address is the IPv4 loopback address 127.0.0.1. The loopback is a special address that hosts use to direct traffic to themselves. The loopback address creates a shortcut method for TCP/IP applications and services that run on the same device to communicate with one another.
- Although only the single 127.0.0.1 address is used, addresses 127.0.0.0 to 127.255.255.255 are reserved. Any address within this block will loop back within the local host. No address within this block should ever appear on any network.

Link-Local Addresses

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

TEST_NET Addresses

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

Legacy IPv4 Addressing

- Historically, RFC1700 grouped the unicast ranges into specific sizes called class A, class B, and class C addresses. It also defined class D (multicast) and class E (experimental) addresses, as previously presented.
- The unicast address classes A, B, and C defined specifically-sized networks as well as specific address blocks for these networks. A company or organization was assigned an entire class A, class B, or class C address block. This use of address space is referred to as classful addressing.

Class A Blocks

- A class A address block was designed to support extremely large networks with more than 16 million host addresses.
- Class A IPv4 addresses used a fixed /8 prefix with the first octet to indicate the network address. The remaining three octets were used for host addresses.
- To reserve address space for the remaining address classes, all class A addresses required that the most significant bit of the high-order octet be a zero. This meant that there were only 128 possible class A networks, 0.0.0.0 /8 to 127.0.0.0 /8, before taking out the reserved address 4 blocks.
- Even though the class A addresses reserved one-half of the address space, because of their limit of 128 networks, they could only be allocated to approximately 120 companies or organizations.

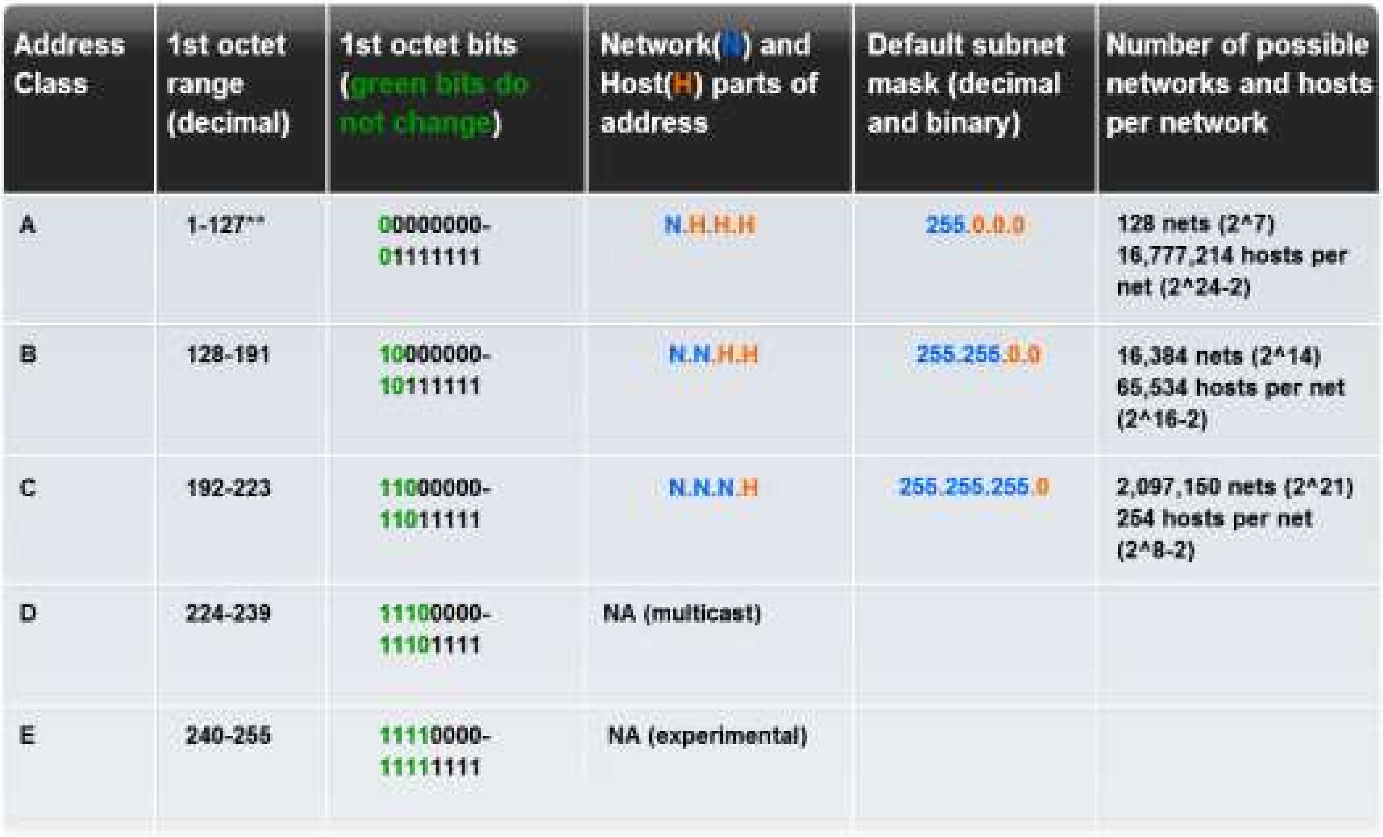
Class B Blocks

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

Class C Blocks

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

IP Address Classes



Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000- 01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000- 10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000- 11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000- 11101111	NA (multicast)		
E	240-255	11110000- 11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

Subnetting

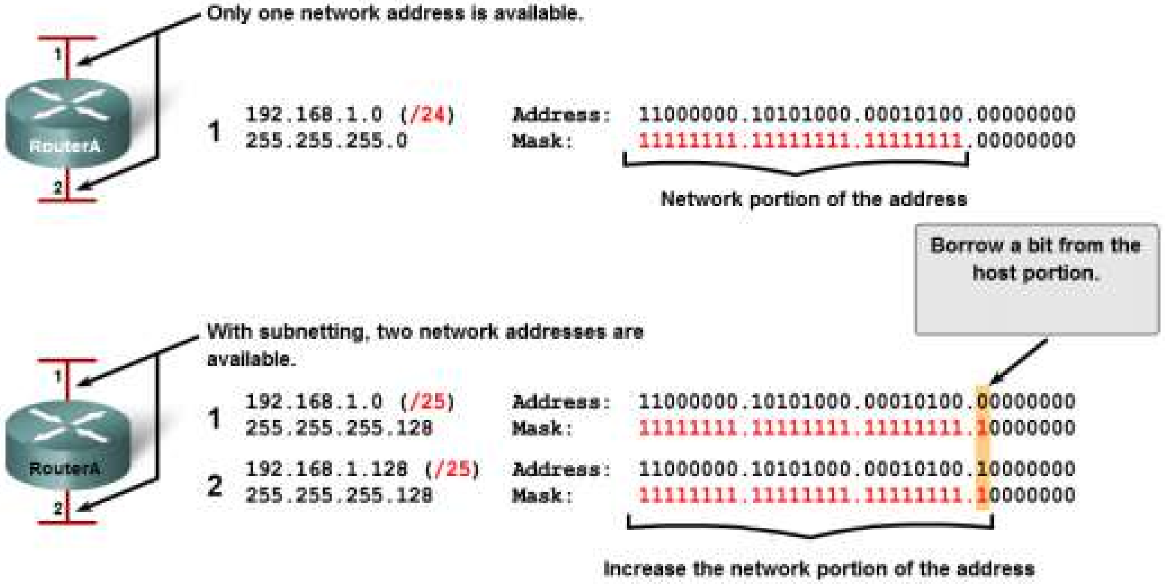
- Subnetting allows for creating multiple logical networks from a single address block.
- Since we use a router to connect these networks together, each interface on a router must have a unique network ID. Every node on that link is on the same network.
- We create the subnets by using one or more of the host bits as network bits. This is done by extending the mask to borrow some of the bits from the host portion of the address to create additional network bits.
- The more host bits used, the more subnets that can be defined. However, with each bit we borrow, fewer host addresses are available per subnet.

- RouterA in the figure has two interfaces to interconnect two networks. Given an address block of 192.168.1.0 /24, we will create two subnets. We borrow one bit from the host portion by using a subnet mask of 255.255.255.128, instead of the original 255.255.255.0 mask. The most significant bit in the last octet is used to distinguish between the two subnets. For one of the subnets, this bit is a "0" and for the other subnet this bit is a "1

Formula for calculating subnets

- Use this formula to calculate the number of subnets:
- 2^n where n = the number of bits borrowed
- In this example, the calculation looks like this: 2^1 = 2 subnets
- The number of hosts
- To calculate the number of hosts per network, we use the formula of 2^n - 2 where n = the number of bits left for hosts.
- Applying this formula, (2^7 - 2 = 126) shows that each of these subnets can have 126 hosts.
- For each subnet, examine the last octet in binary. The values in these octets for the two networks are: Subnet 1: 00000000 = 0 Subnet 2: 10000000 = 128

Borrowing Bits for Subnets



Only one network address is available.

1 192.168.1.0 (/24)
255.255.255.0

Address: 11000000.10101000.00010100.00000000
Mask: 11111111.11111111.11111111.00000000

Network portion of the address

Borrow a bit from the host portion.

With subnetting, two network addresses are available.

1 192.168.1.0 (/25)
255.255.255.128

Address: 11000000.10101000.00010100.00000000
Mask: 11111111.11111111.11111111.10000000

2 192.168.1.128 (/25)
255.255.255.128

Address: 11000000.10101000.00010100.10000000
Mask: 11111111.11111111.11111111.10000000

Increase the network portion of the address

Example with 3 subnets

- Next, consider an internetwork that requires three subnets.
- Again we start with the same 192.168.1.0 /24 address block. Borrowing a single bit would only provide two subnets. To provide more networks, we change the subnet mask to 255.255.255.192 and borrow two bits. This will provide four subnets.
- Calculate the subnet with this formula:
- 2^2 = 4 subnets
- The number of hosts
- To calculate the number of hosts, begin by examining the last octet. Notice these subnets.
- Subnet 0: 0 = 00000000
- Subnet 1: 64 = 01000000
- Subnet 2: 128 = 10000000
- Subnet 3: 192 = 11000000
- Apply the host calculation formula.
- 2^6 - 2 = 62 hosts per subnet

Borrowing Bits for Subnets

-	192.168.1.0 (/24) 255.255.255.0	Address: Mask:	11000000.10101000.00010100.00000000 11111111.11111111.11111111.00000000
0	192.168.1.0 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.00000000 11111111.11111111.11111111.11000000
1	192.168.1.64 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.01000000 11111111.11111111.11111111.11000000
2	192.168.1.128 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.10000000 11111111.11111111.11111111.11000000
3	192.168.1.192 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.11000000 11111111.11111111.11111111.11000000

Two bits are borrowed to provide four subnets.

Unused address in this example.

A 1 in these positions in the mask means that these values are part of the network address.

More subnets are available, but fewer addresses are available per subnet.

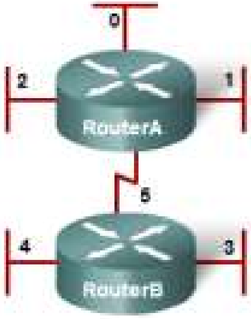
Example with 6 subnets

- Consider this example with five LANs and a WAN for a total of 6 networks. See the figure.
- To accommodate 6 networks, subnet 192.168.1.0 /24 into address blocks using the formula: 2^3 = 8
- To get at least 6 subnets, borrow three host bits.
- A subnet mask of 255.255.255.224 provides the three additional network bits.
- The number of hosts To calculate the number of hosts, begin by examining the last octet.

- Notice these subnets. 0 = 00000000
- 32 = 00100000
- 64 = 01000000
- 96 = 01100000
- 128 = 10000000
- 160 = 10100000
- 192 = 11000000
- 224 = 11100000
- Apply the host calculation formula: 2^5 - 2 = 30 hosts per subnet

Borrowing Bits for Subnets

Start with this address	-	192.168.1.0 (/24)	Address:	11000000.10101000.00010100.00000000
		255.255.255.0	Mask:	11111111.11111111.11111111.00000000
Make 8 subnets	0	192.168.1.0 (/27)	Address:	11000000.10101000.00010100.00000000
		255.255.255.224	Mask:	11111111.11111111.11111111.11100000
	1	192.168.1.32 (/27)	Address:	11000000.10101000.00010100.00100000
		255.255.255.224	Mask:	11111111.11111111.11111111.11100000
	2	192.168.1.64 (/27)	Address:	11000000.10101000.00010100.01000000
		255.255.255.224	Mask:	11111111.11111111.11111111.11100000
	3	192.168.1.96 (/27)	Address:	11000000.10101000.00010100.01100000
		255.255.255.224	Mask:	11111111.11111111.11111111.11100000
	4	192.168.1.128 (/27)	Address:	11000000.10101000.00010100.10000000
		255.255.255.224	Mask:	11111111.11111111.11111111.11100000
	5	192.168.1.160 (/27)	Address:	11000000.10101000.00010100.10100000
		255.255.255.224	Mask:	11111111.11111111.11111111.11100000
	6	192.168.1.192 (/27)	Address:	11000000.10101000.00010100.11000000
		255.255.255.224	Mask:	11111111.11111111.11111111.11100000
	7	192.168.1.224 (/27)	Address:	11000000.10101000.00010100.11100000
		255.255.255.224	Mask:	11111111.11111111.11111111.11100000



Three bits are borrowed to provide eight subnets.