Topic 8: Network Addressing

IP Addresses and Subnet Masks

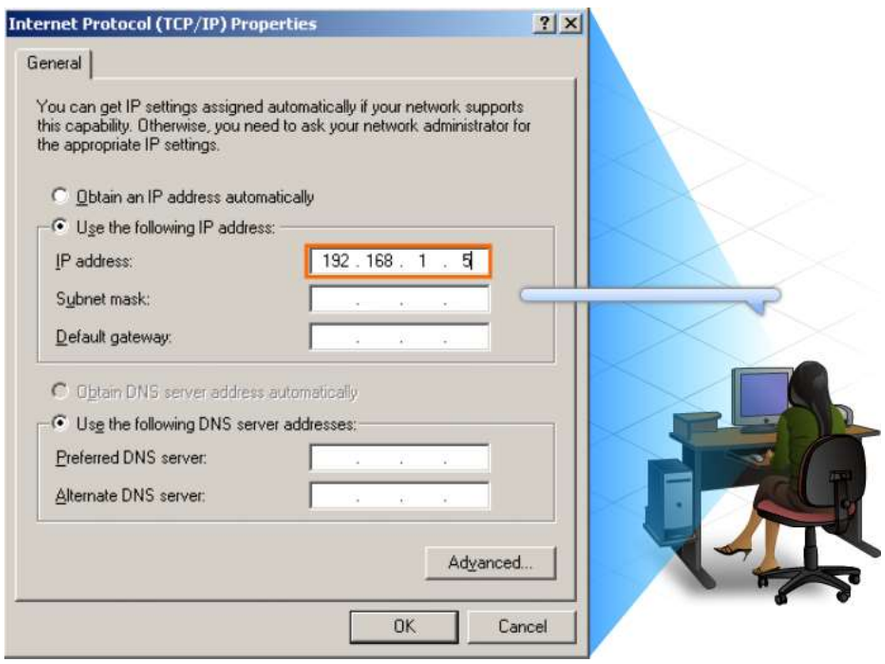
Purpose of the IP Address

host needs an IP address to participate on the Internet. The IP address is a logical network address that identifies a particular host. It must be properly configured and unique in order to communicate with other devices on the Internet.

An IP address is assigned to the Network interface connection for a host. This connection is usually a network interface card (NIC) installed in the device. Examples of end-user devices with network interfaces include workstations, servers, network printers and IP phones. Some servers can have more than one NIC and each of these has its own IP address. Router interfaces that provide connections to an IP network will also have an IP address.

Every packet sent across the Internet has a source and destination IP address. This information is required by networking devices to ensure the information gets to the destination and any replies are returned to the source.

IP Address Structure



An IP address is simply a series of 32 binary bits (ones and zeros). It is very difficult for humans to read a binary IP address. For this reason, the 32 bits are grouped into four 8-bit bytes called octets. An IP address in this format is hard for humans to read, write and remember. To make the IP address easier to understand, each octet is presented as its decimal value, separated by a decimal point or period. This is referred to as dotted-decimal notation.

When a host is configured with an IP address, it is entered as a dotted decimal number such as 192.168.1.5. Imagine if you had to enter the 32-bit binary equivalent of this-11000000101010000000000100000101. If just one bit was mistyped, the address would be different and the host may not be able to communicate on the network.

The 32-bit IP address is defined with IP version 4 (IPv4) and is currently the most common form of IP address on the Internet. There are over 4 billion possible IP addresses using a 32-bit addressing scheme.

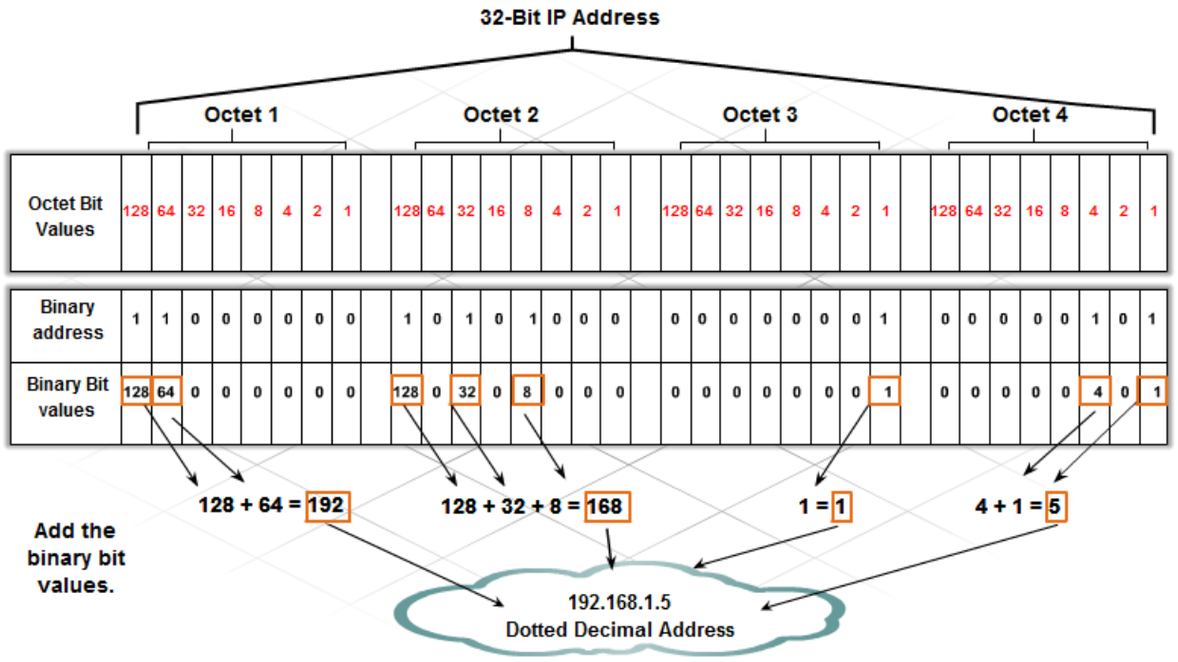
When a host receives an IP address, it looks at all 32 bits as they are received by the NIC. Humans, on the other hand, need to convert those 32 bits into their four-octet decimal equivalent. Each octet is made up of 8 bits and each bit has a value. The four groups of 8 bits

have the same set of values. The rightmost bit in an octet has a value of 1 and the values of the remaining bits, from right to left, are 2, 4, 8, 16, 32, 64 and 128.

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

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

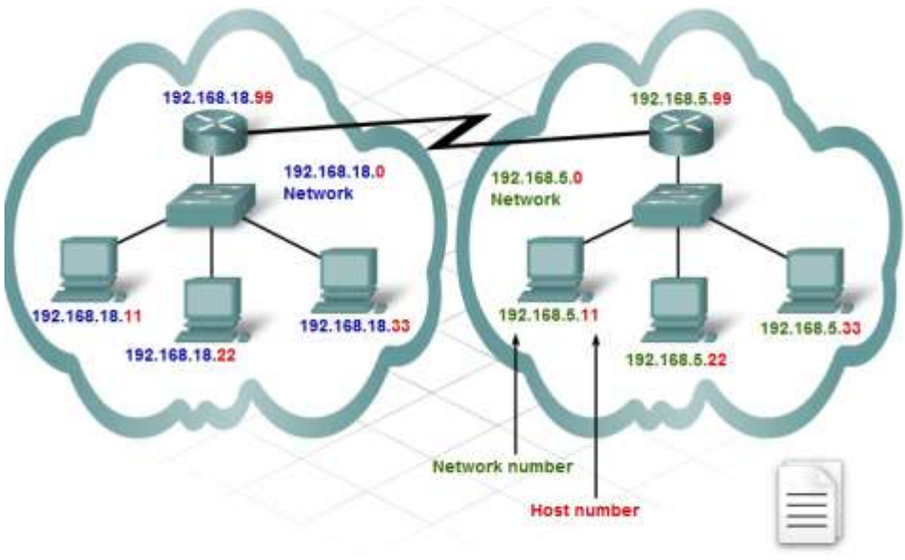
So the value of each of the four octets can range from 0 to a maximum of 255.



Parts of an IP Address

The logical 32-bit IP address is hierarchical and is made up of two parts. The first part identifies the network and the second part identifies a host on that network. Both parts are required in an IP address.

As an example, if a host has IP address 192.168.18.57 the first three octets, (192.168.18), identify the network portion of the address, and the last octet, (57) identifies the host. This is known as hierarchical addressing because the network portion indicates the network on which each unique host address is located. Routers only need to know how to reach each



network, rather than needing to know the location of each individual host.

Another example of a hierarchical network is the telephone system. With a telephone number, the country code, area code and exchange represent the network address and the remaining digits represent a local phone number.

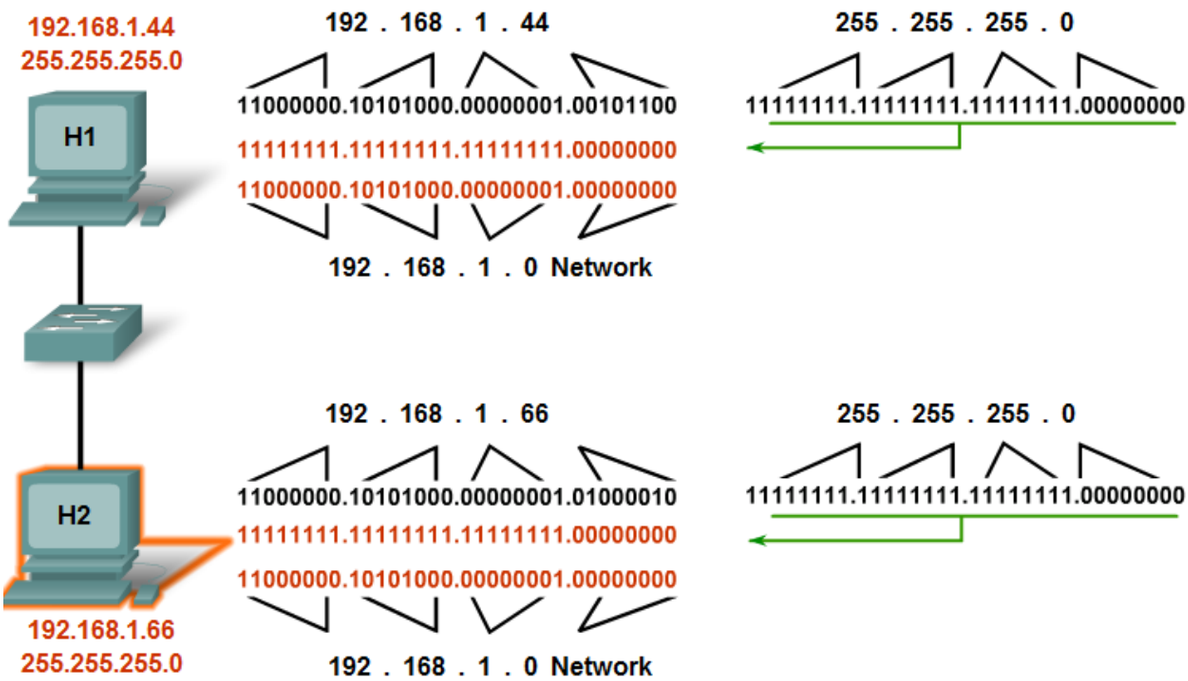
How IP Addresses and Subnet Masks Interact

There are two parts to every IP address. How do hosts know which portion is the network and which is the host? This is the job of the subnet mask.

When an IP host is configured, a subnet mask is assigned along with an IP address. Like the IP address, the subnet mask is 32 bits long. The subnet mask signifies which part of the IP address is network and which part is host.

The subnet mask is compared to the IP address from left to right, bit for bit. The 1s in the subnet mask represent the network portion; the 0s represent the host portion. In the example shown, the first three octets are network, and the last octet represents the host.

When a host sends a packet, it compares its subnet mask to its own IP address and the destination IP address. If the network bits match, both the source and destination host are on the same network and the packet can be delivered locally. If they do not match, the sending host forwards the packet to the local router interface to be sent on to the other network.



the subnet masks we see most often with home and small business networking are: 255.0.0.0 (8-bits), 255.255.0.0 (16 bits) and 255.255.255.0 (24 bits). A subnet mask of 255.255.255.0 (decimal) or 11111111.11111111.1111111.00000000 (binary) uses 24 bits to identify the network number which leaves 8 bits to number the hosts on that network.

To calculate the number of hosts that can be on that network, take the number 2 to the power of the number of host bits (2 ^ 8 = 256). From this number, we must subtract 2 (256-2). The reason we subtract 2 is because all 1s within the host portion of an IP address is a broadcast address for that network and cannot be assigned to a specific host. All 0s within the host portion indicates the network ID and again, cannot be assigned to a specific host. Powers of 2 can be calculated easily with the calculator that comes with any Windows operating system.

Another way to determine the number of hosts available is to add up the values of the available host bits (128+64+32+16+8+4+2+1 = 255). From this number, subtract 1 (255-1 = 254), because the host bits cannot be all 1s. It is not necessary to subtract 2 because the value of all 0s is 0 and is not included in the addition.

With a 16-bit mask, there are 16 bits (two octets) for host addresses and a host address could have all 1s (255) in one of the octets. This might appear to be a broadcast but as long as the other octet is not all 1s, it is a valid host address. Remember that the host looks at all host bits together, not at octet values.

Types of IP Addresses

IP Address Classes and Default Subnet Masks

The IP address and subnet mask work together to determine which portion of the IP address represents the network address and which portion represents the host address.

IP addresses are grouped into 5 classes. Classes A, B and C are commercial addresses and are assigned to hosts. Class D is reserved for multicast use and Class E is for experimental use.

1. Class C addresses have three octets for the network portion and one for the hosts. The default subnet mask is 24 bits (255.255.255.0). Class C addresses are usually assigned to small networks.

2. Class B addresses have two octets to represent the network portion and two for the hosts. The default subnet mask is 16 bits (255.255.0.0). These addresses are typically used for medium-sized networks.

3. Class A addresses have only one octet to represent the network portion and three to represent the hosts. The default subnet mask is 8 bits (255.0.0.0). These addresses are typically assigned to large organizations.

The class of an address can be determined by the value of the first octet. For instance, if the first octet of an IP address has a value in the range 192-223, it is classified as a Class C address. As an example, 200.14.193.67 is a Class C address.

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits don't change)	Network (N) and Host (H) parts of an address	Default subnet mask (decimal and binary)	Numbers of possible networks and hosts per network
A	1 - 127	00000000 - 01111111	N.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	126 nets (2^7-2) 16,777,214 hosts per net (2^24-2)
B	128 - 191	10000000 - 10111111	N.N.H.H	255.255.0.0 11111111.11111111.00000000.00000000	16,382 nets (2^14-2) 65,534 hosts per net (2^16-2)
C	192 - 223	11000000 - 11011111	N.N.N.H	255.255.255.0 11111111.11111111.11111111.00000000	2,097.150 nets (2^21-2) 254 hosts per net (2^8-2)
D	224 - 239	11100000 - 11101111	Not for commercial use as a host		
E	240 - 255	11110000 - 11111111	Not for commercial use as a host		

^^ All zeros (0) and all ones (1) are invalid host addresses.

Public and Private IP Addresses

All hosts that connect directly to the Internet require a unique public IP address. Because of the finite number of 32-bit addresses available, there is a risk of running out of IP addresses. One solution to this problem was to reserve some private addresses for use exclusively inside an organization. This allows hosts within an organization to communicate with one another without the need of a unique public IP address.

RFC 1918 is a standard that reserves several ranges of addresses within each of the classes A, B and C. As shown in the table, these private address ranges consist of a single Class A network, 16 Class B networks and 256 Class C networks. This gives a network administrator considerable flexibility in assigning internal addresses.

A very large network can use the Class A private network, which allows for over 16 million private addresses.

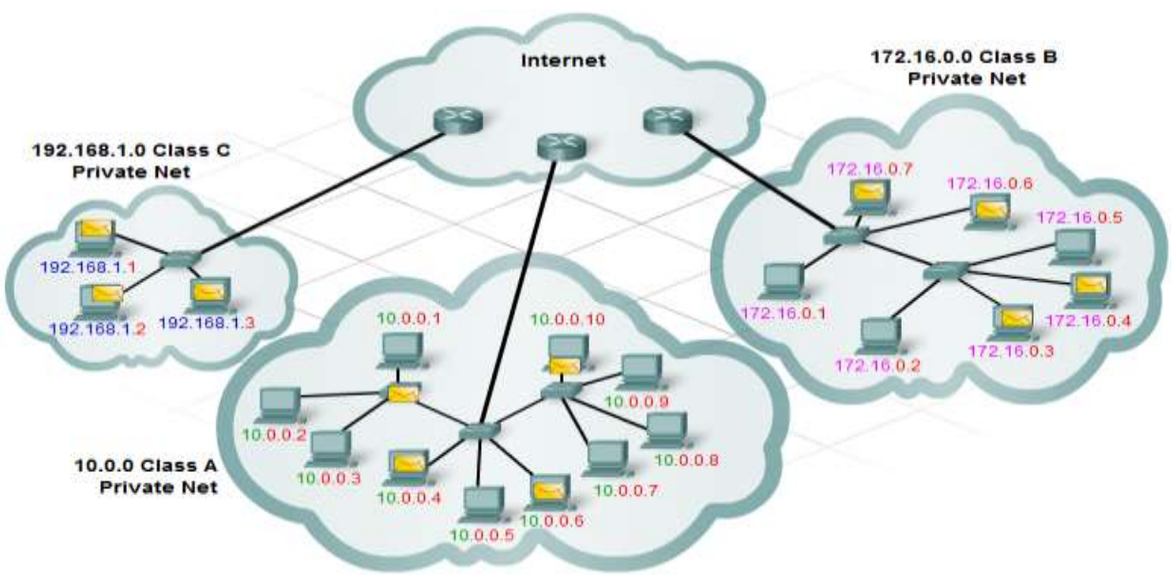
On medium size networks, a Class B private network could be used, which provides over 65,000 addresses.

Home and small business networks typically use a single class C private address, which allows up to 254 hosts.

The Class A network, the 16 Class B networks, or the 256 Class C networks can be used within any size organization. Typically many organizations use the Class A private network.

Address Class	Number of Network Numbers Reserved	Network Addresses
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0

Private addresses can be used internally by hosts in an organization as long as the hosts do not connect directly to the Internet. Therefore, the same set of private addresses can be used by multiple organizations. Private addresses are not routed on the Internet and will be quickly blocked by an ISP router.



The use of private addresses can provide a measure of security since they are only visible on the local network, and outsiders cannot gain direct access to the private IP addresses.

There are also private addresses that can be used for the diagnostic testing of devices. This type of private address is known as a loopback address. The class A, 127.0.0.0 network, is reserved for loopback addresses.

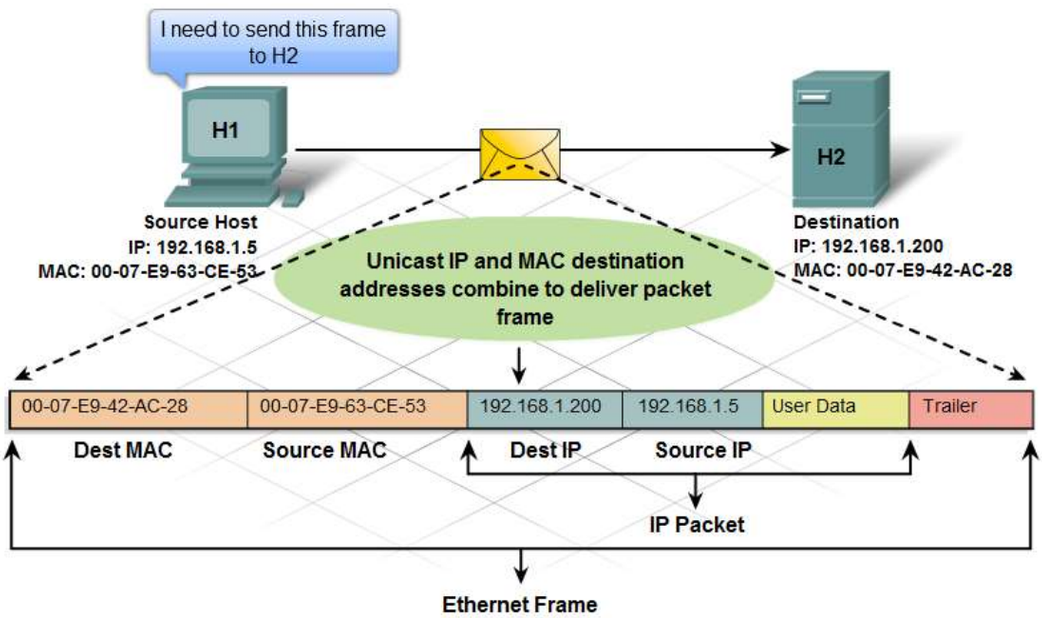
Unicast, Broadcast, and Multicast Addresses

In addition to address classes, we also categorize IP addresses as unicast, broadcast, or multicast. Hosts can use IP addresses to communicate one-to-one (unicast), one-to-many (multicast) or one-to-all (broadcast).

Unicast

A unicast address is the most common type on an IP network. A packet with a unicast destination address is intended for a specific host. An example is a host with IP address 192.168.1.5 (source) requesting a web page from a server at IP address 192.168.1.200 (destination).

For a unicast packet to be sent and received, a destination IP address must be in the IP packet header. A corresponding destination MAC address must also be present in the Ethernet frame header. The IP address and MAC address combine to deliver data to one specific destination host.



Broadcast

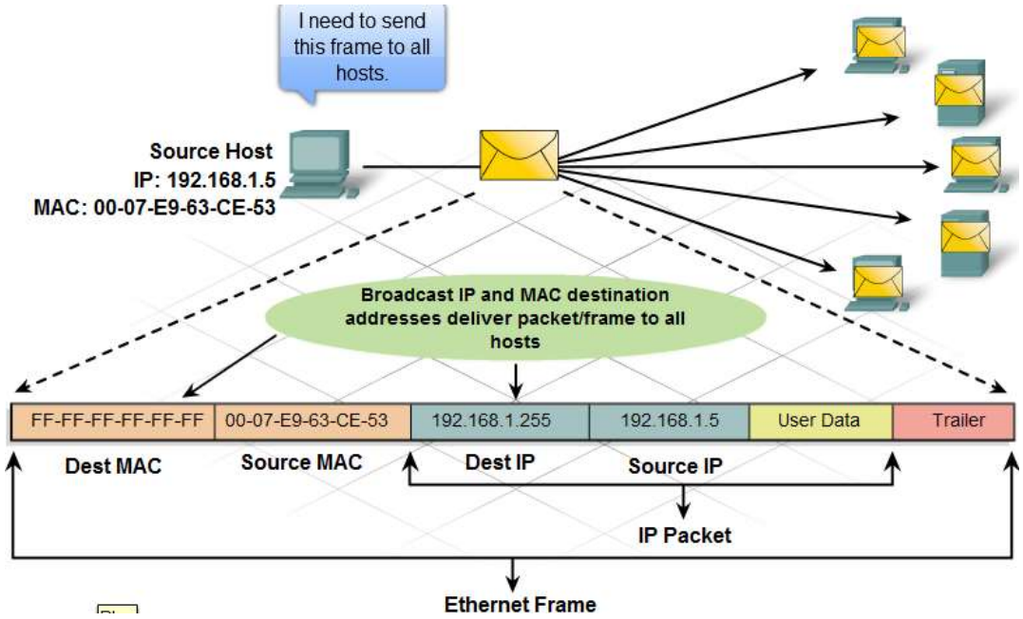
With a broadcast, the packet contains a destination IP address with all ones (1s) in the host portion. This means that all hosts on that local network (broadcast domain) will receive and look at the packet. Many network protocols, such as ARP and DHCP use broadcasts.

A Class C network 192.168.1.0 with a default subnet mask of 255.255.255.0 has a broadcast address of 192.168.1.255. The host portion is decimal 255 or binary 11111111 (all 1s).

A Class B network of 172.16.0.0, with a default mask of 255.255.0.0, has a broadcast of 172.16.255.255.

A Class A network of 10.0.0.0, with a default mask of 255.0.0.0, has a broadcast of 10.255.255.255.

A broadcast IP address for a network needs a corresponding broadcast MAC address in the Ethernet frame. On Ethernet networks, the broadcast MAC address is 48 ones displayed as Hexadecimal FF-FF-FF-FF-FF-FF.

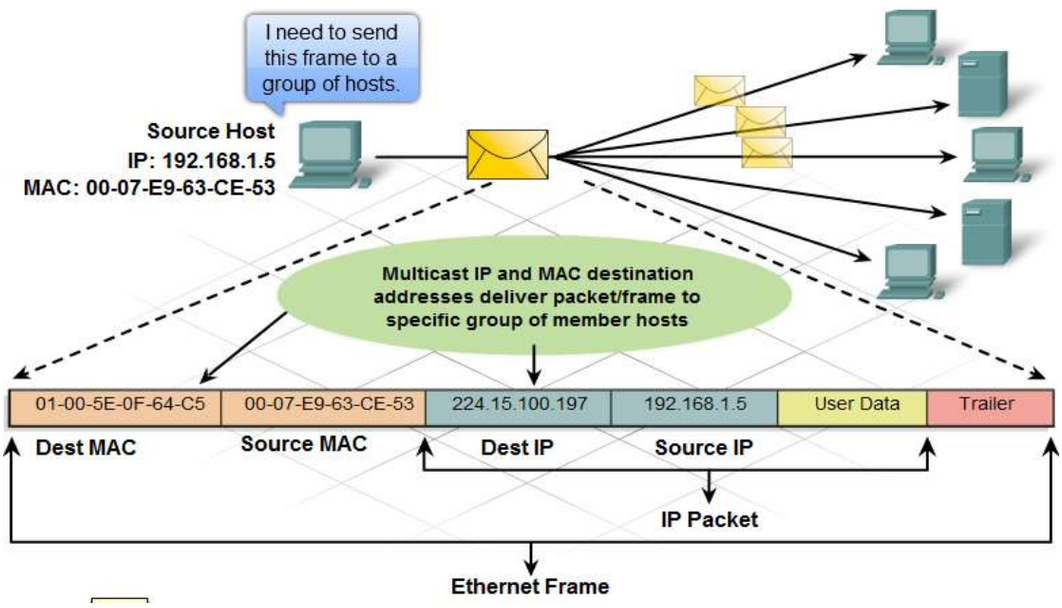


Multicast

Multicast addresses allow a source device to send a packet to a group of devices.

Devices that belong to a multicast group are assigned a multicast group IP address. The range of multicast addresses is from 224.0.0.0 to 239.255.255.255. Since multicast addresses represent a group of addresses (sometimes called a host group), they can only be used as the destination of a packet. The source will always have a unicast address.

Examples of where multicast addresses would be used are in remote gaming, where many players are connected remotely but playing the same game. Another example would be distance learning through video conferencing, where many students are connected to the same class. As with a unicast or broadcast address, multicast IP addresses need a corresponding multicast MAC address to actually deliver frames on a local network. The multicast MAC address is a special value that begins with 01-00-5E in hexadecimal. The value ends by converting the lower 23 bits of the IP multicast group address into the remaining 6 hexadecimal characters of the Ethernet address. An example, as shown in the graphic, is hexadecimal 01-00-5E-0F-64-C5. Each hexadecimal character is 4 binary bits.

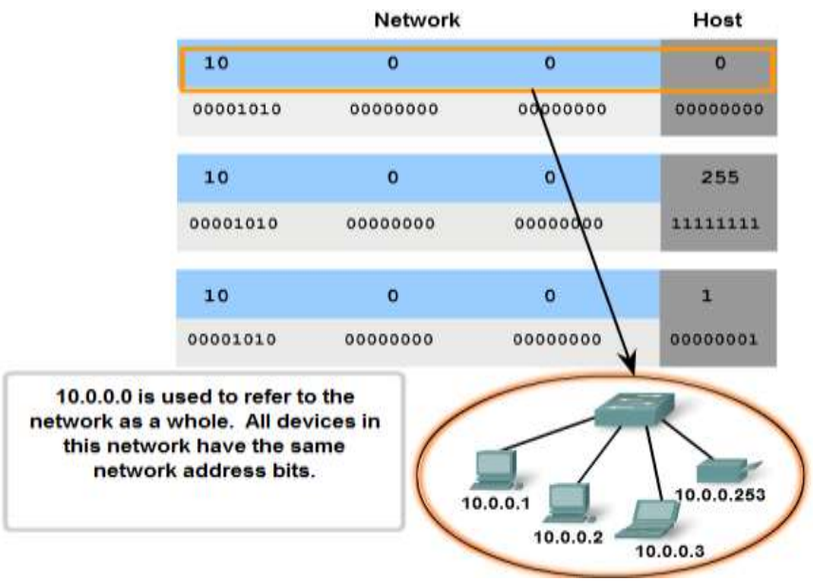


Types of addresses in an IPv4 Network

Within the address range of each IPv4 network, we have three types of addresses:

1. Network address - The address by which we refer to the network
2. Broadcast address - A special address used to send data to all hosts in the network
3. Host addresses - The addresses assigned to the end devices in the network

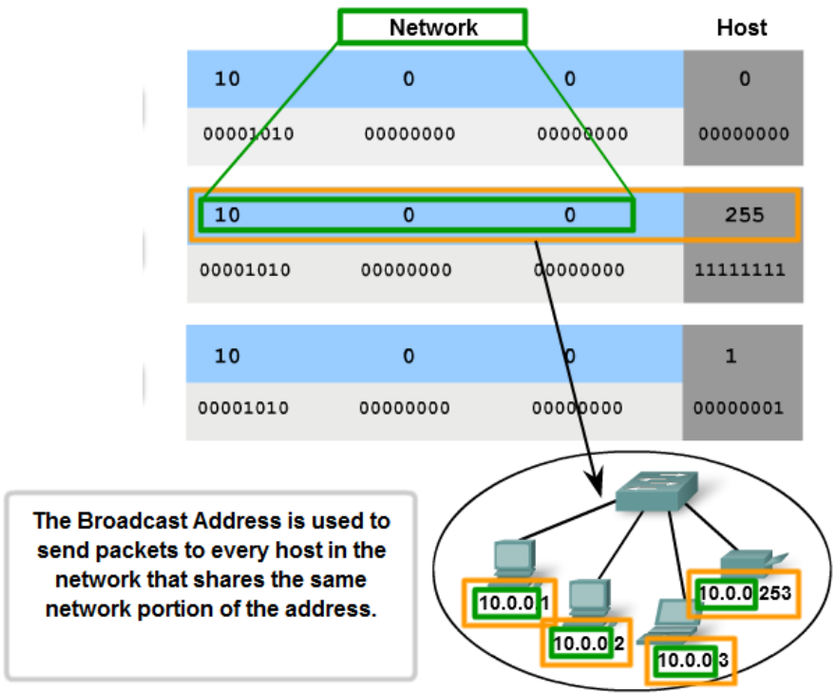
Network Address



The network address is a standard way to refer to a network. For example, we could refer to the network shown in the figure as "the 10.0.0.0 network." This is a much more convenient and descriptive way to refer to the network than using a term like "the first network." All hosts in the 10.0.0.0 network will have the same network bits.

Within the IPv4 address range of a network, the lowest address is reserved for the network address. This address has a 0 for each host bit in the host portion of the address.

Broadcast Address

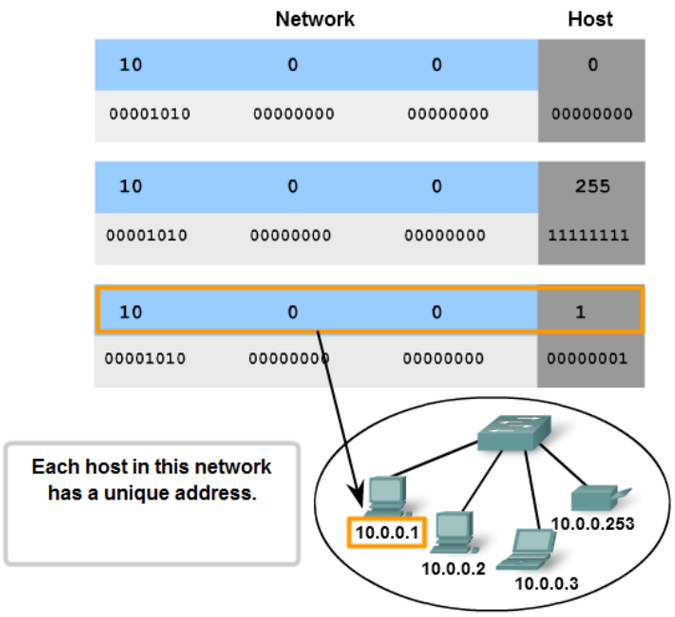


The IPv4 broadcast address is a special address for each network that allows communication to all the hosts in that network. To send data to all hosts in a network, a host can send a single packet that is addressed to the broadcast address of the network.

The broadcast address uses the highest address in the network range. This is the address in which the bits in the host portion are all 1s. For the network 10.0.0.0 with 24 network bits, the broadcast address would be 10.0.0.255. This address is also referred to as the directed broadcast.

Host Addresses

As described previously, every end device requires a unique address to deliver a packet to that host. In IPv4 addresses, we assign the values between the network address and the broadcast address to the devices in that network.



Network Prefixes

An important question is: How do we know how many bits represent the network portion and how many bits represent the host portion? When we express an IPv4 network address, we add a prefix length to the network address. The prefix length is the number of bits in the address that gives us the network portion. For example, in 172.16.4.0 /24, the /24 is the prefix length - it tells us that the first 24 bits are the network address. This leaves the remaining 8 bits, the last octet, as the host portion. Later in this chapter, we will learn more about another entity that is used to specify the network portion of an IPv4 address to the network devices. It is called the subnet mask. The subnet mask consists of 32 bits, just as the address does, and uses 1s and 0s to indicate which bits of the address are network bits and which bits are hosts bits.

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

Network	Network address All Hosts Bits (Red) = 0	Host range Represents all combinations of host bits except where host bits are all zeros or all ones	Broadcast address All Host Bits (in Red) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
Binary Representation 24 Network Bits	10101100.00010000.00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011 10101100.00010000.00000100.11111110	10101100.00010000.00000100.1111111
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

SAME NETWORK ADDRESS ALL PREFIXES

DIFFERENT BROADCAST ADDRESS EACH PREFIX

254 Hosts

DIFFERENT NUMBER OF HOSTS EACH PREFIX

Notice that the network address could remain the same, but the host range and the broadcast address are different for the different prefix lengths. In this figure you can also see that the number of hosts that can be addressed on the network changes as well.

Calculating Network, Hosts, and Broadcast Addresses

At this point, you may be wondering: How do we calculate these addresses? This calculation process requires us to look at these addresses in binary.

In the example network divisions, we need to look at the octet of the address where the prefix divides the network portion from the host portion. In all of these examples, it is the last octet. While this is common, the prefix can also divide any of the octets.

To get started understanding this process of determining the address assignments, let's break some examples down into binary.

See the figure for an example of the address assignment for the 172.16.20.0 /25 network.

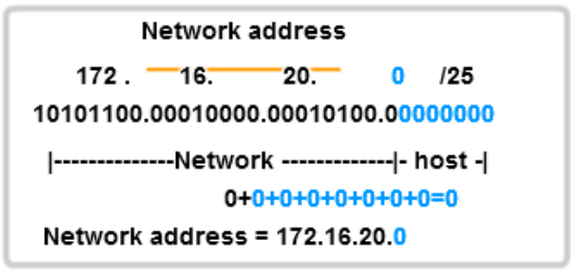
In the first box, we see the representation of the network address. With a 25-bit prefix, the last 7 bits are host bits. To represent the network address, all of these host bits are (0). This makes the last octet of the address 0. This makes the network address 172.16.20.0 /25.

In the second box, we see the calculation of the lowest host address. This is always one greater than the network address. In this case, the last of the seven host bits becomes a (1). With the lowest bit of host address set to a 1, the lowest host address is 172.16.20.1.

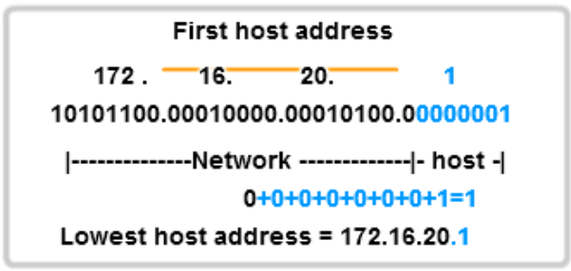
The third box shows the calculation of the broadcast address of the network. Therefore, all seven host bits used in this network are all '1s'. From the calculation, we get 127 in the last octet. This gives us a broadcast address of 172.16.20.127.

The fourth box presents the calculation of the highest host address. The highest host address for a network is always one less than the broadcast. This means the lowest host bit is a '0 and all other host bits as (1s). As seen, this makes the highest host address in this network 172.16.20.126.

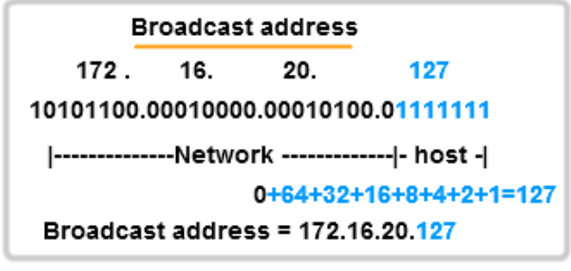
Although for this example we expanded all of the octets, we only need to examine the content of the divided octet.



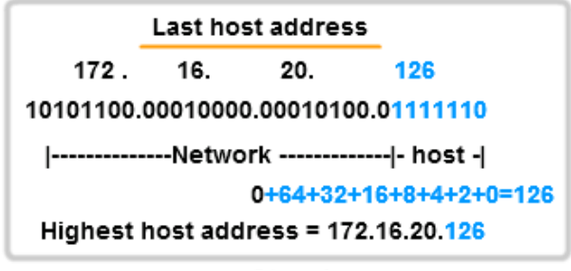
Step 1



Step 2



Step 3

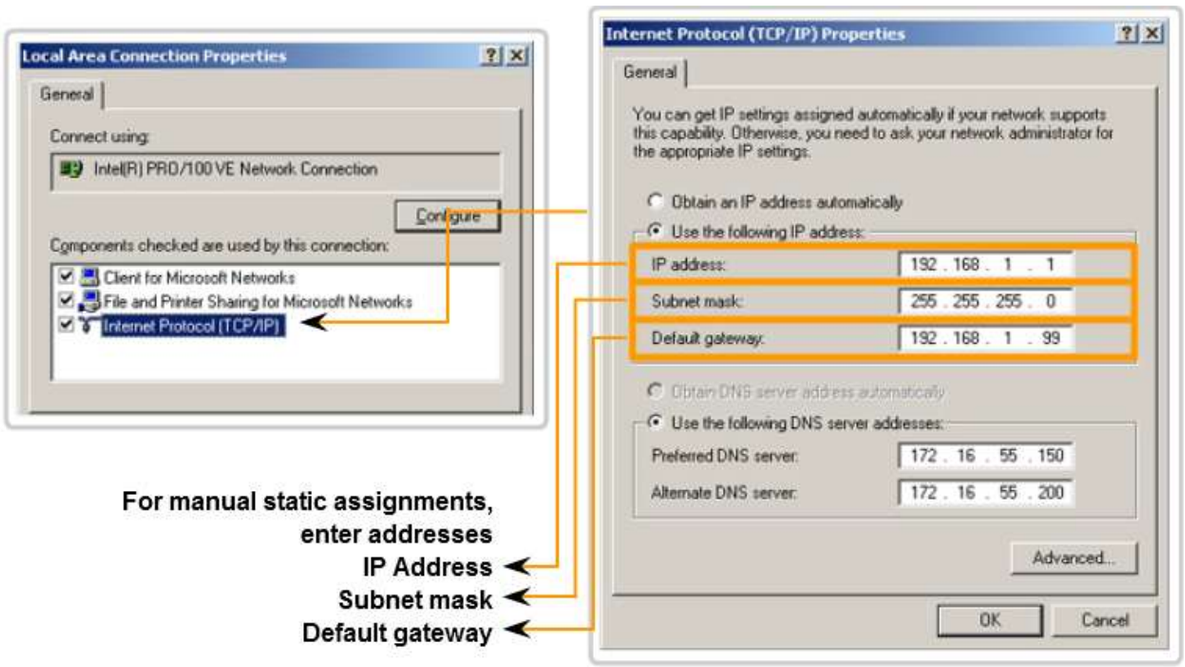


Step 4

How IP addresses are Obtained

Static and Dynamic Address Assignment
IP addresses can be assigned either statically or dynamically.

Static



With a static assignment, the network administrator must manually configure the network information for a host. At a minimum, this includes the host IP address, subnet mask and default gateway.

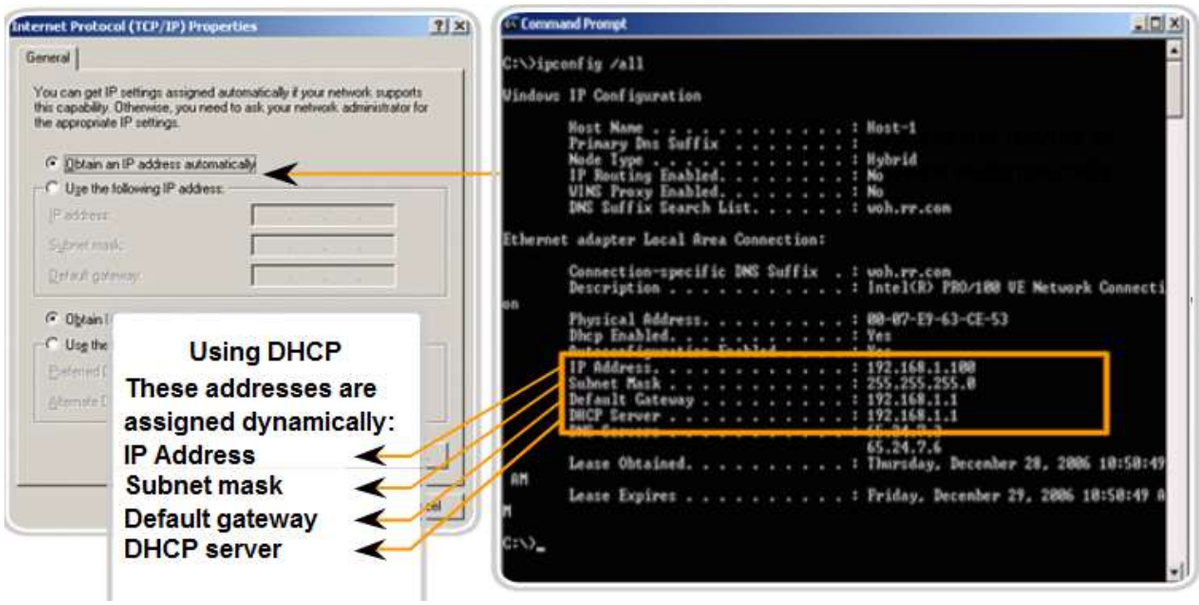
Static addresses have some advantages. For instance, they are useful for printers, servers and other networking devices that need to be accessible to clients on the network. If hosts normally access a server at a particular IP address, it would not be good if that address changed.

Static assignment of addressing information can provide increased control of network resources, but it can be time consuming to enter the information on each host. When entering IP addresses statically, the host only performs basic error checks on the IP address. Therefore, errors are more likely to occur.

When using static IP addressing, it is important to maintain an accurate list of which IP addresses are assigned to which devices. Additionally, these are permanent addresses and are not normally reused.

Dynamic
On local networks it is often the case that the user population changes frequently. New users arrive with laptops and need a connection. Others have new workstations that need to be connected. Rather than have the network administrator assign IP addresses for each workstation, it is easier to have IP addresses assigned automatically. This is done using a protocol known as Dynamic Host Configuration Protocol (DHCP).

DHCP provides a mechanism for the automatic assignment of addressing information such as IP address, subnet mask, default gateway, and other configuration information. DHCP is generally the preferred method of assigning IP addresses to hosts on large networks since it reduces the burden on network support staff and virtually eliminates entry errors.



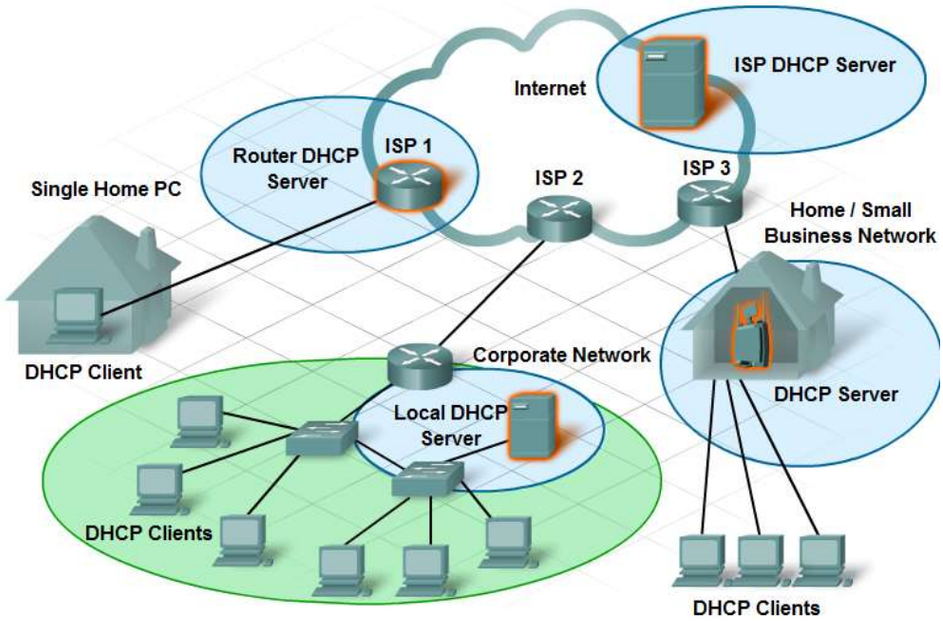
Another benefit of DHCP is that an address is not permanently assigned to a host but is only leased for a period of time. If the host is powered down or taken off the network, the address is returned to the pool for reuse. This is especially helpful with mobile users that come and go on a network.

DHCP Servers

If you enter a wireless hotspot at an airport or coffee shop, DHCP makes it possible for you to access the Internet. As you enter the area, your laptop DHCP client contacts the local DHCP server via a wireless connection. The DHCP server assigns an IP address to your laptop.

Various types of devices can be DHCP servers as long as they are running DHCP service software. With most medium to large networks, the DHCP server is usually a local dedicated PC-based server.

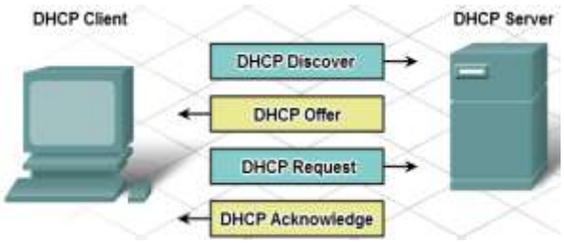
With home networks the DHCP server is usually located at the ISP and a host on the home network receives its IP configuration directly from the ISP.



Many home networks and small businesses use an integrated router to connect to the ISP modem. In this case, the integrated router is both a DHCP client and a server. The integrated router acts as a client to receive its IP configuration from the ISP and then acts a DHCP server for internal hosts on the local network.

In addition to PC-based servers and integrated routers, other types of networking devices such as dedicated routers can provide DHCP services to clients, although this is not as common.

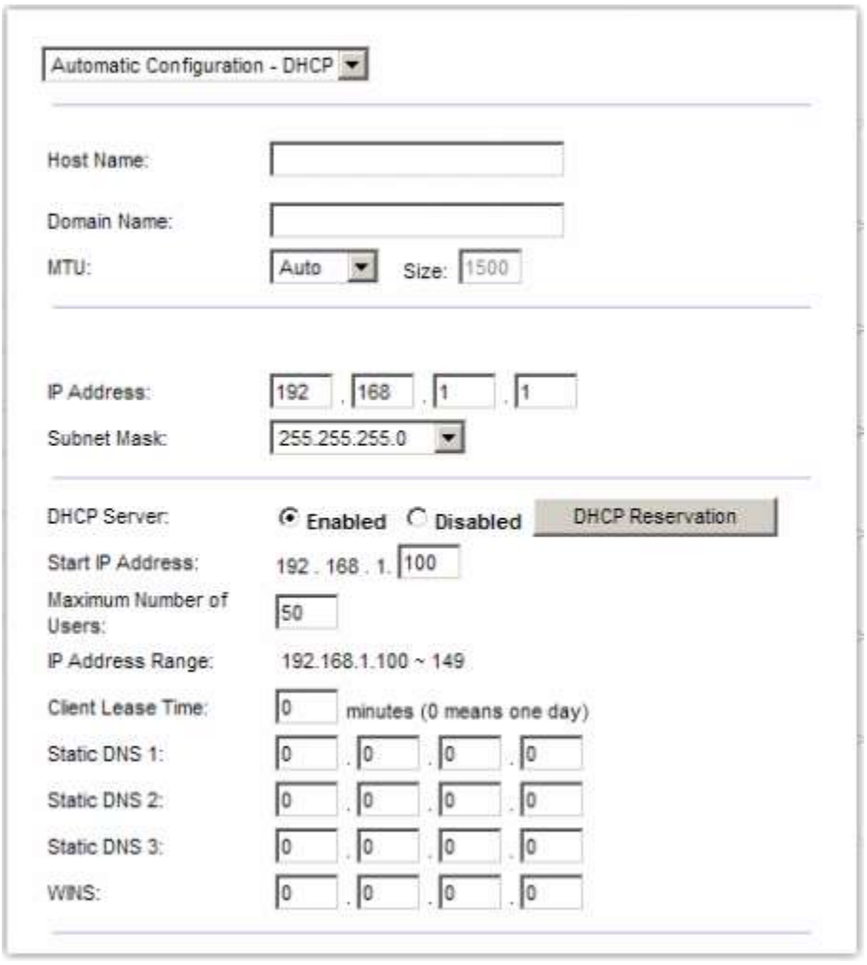
Configuring DHCP



When a host is first configured as a DHCP client, it does not have an IP address, subnet mask or default gateway. It obtains this information from a DHCP server, either on the local network or one located at the ISP. The DHCP server is configured with a range, or pool, of IP addresses that can be assigned to DHCP clients.

A client that needs an IP address will send a DHCP Discover message which is a broadcast with a destination IP address of 255.255.255.255 (32 ones) and a destination MAC address of FF-FF-FF-FF-FF-FF (48 ones). All hosts on the network will receive this broadcast DHCP frame, but only a DHCP server will reply. The server will respond with a DHCP Offer, suggesting an IP address for the client. The host then sends a DHCP Request to that server asking to use the suggested IP address. The server responds with a DHCP Acknowledgment.

For most home and small business networks, a multi-function device provides DHCP services to the local network clients. To configure a Linksys wireless router, access its graphical web interface by opening the browser and entering the in the Address area the router default IP address: 192.168.1.1. Navigate to the screen that shows the DHCP configuration.



The IP address of 192.168.1.1 and subnet mask of 255.255.255.0 are the defaults for the internal router interface. This is the default gateway for all hosts on the local network and also the internal DHCP server IP address. Most Linksys wireless routers and other home integrated routers have DHCP Server enabled by default.

On the DHCP configuration screen a default DHCP range is available or you can specify a starting address for the DHCP range (do not use 192.168.1.1) and the number of addresses to be assigned. The lease time can also be modified (default is 24 hours). The DHCP configuration feature on most ISRs gives information about connected hosts and IP addresses, their associated MAC address, and lease times.

The DHCP Client Table also shows the client name and whether it is connected via the Ethernet LAN or wireless (Interface).

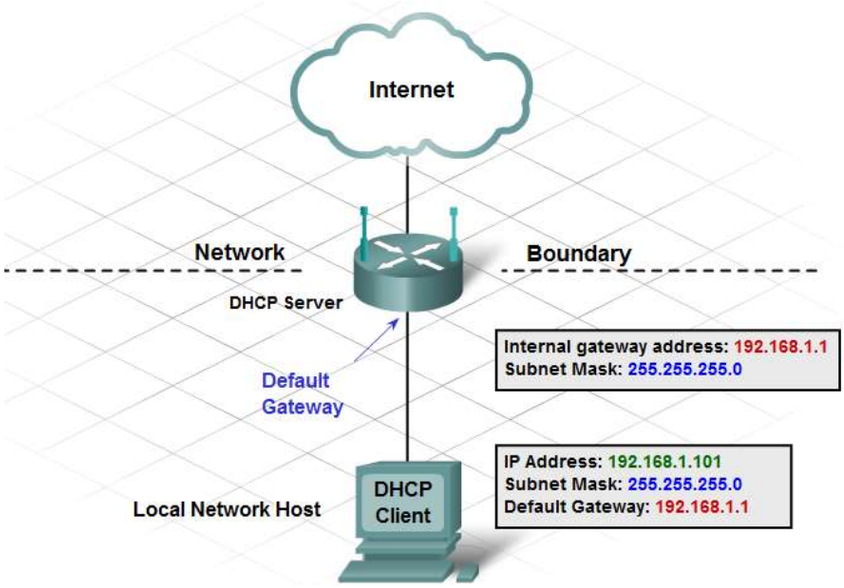
Address Management

Network Boundaries and Address Space

The router provides a gateway through which hosts on one network can communicate with hosts on different networks. Each interface on a router is connected to a separate network.

The IP address assigned to the interface identifies which local network is connected directly to it.

Every host on a network must use the router as a gateway to other networks. Therefore, each host must know the IP address of the router interface connected to the network where the host is attached. This address is known as the default gateway address. It can be either statically configured on the host, or received dynamically by DHCP.



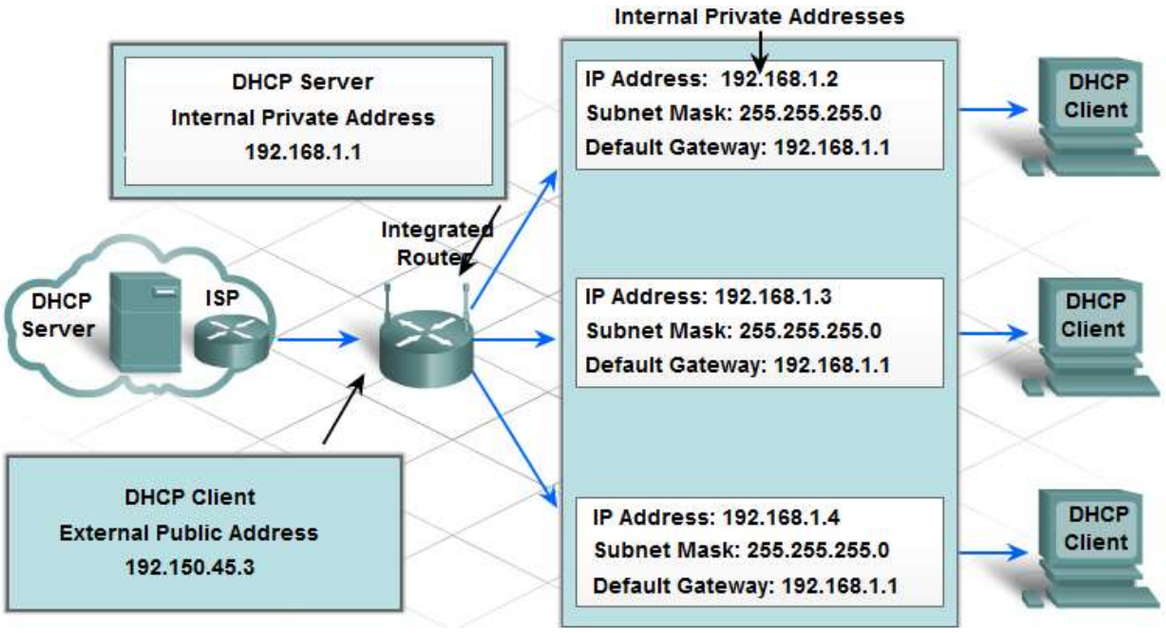
When an integrated router is configured to be a DHCP server for the local network, it automatically sends the correct interface IP address to the hosts as the default gateway address. In this manner, all hosts on the network can use that IP address to forward messages to hosts located at the ISP and get access to hosts on the Internet. Integrated routers are usually set to be DHCP servers by default.

The IP address of that local router interface becomes the default gateway address for the host configuration. The default gateway is provided, either statically or by DHCP.

When an integrated router is configured as a DHCP server, it provides its own internal IP address as the default gateway to DHCP clients. It also provides them with their respective IP address and subnet mask.

Address Assignment

The integrated router acts as a DHCP server for all local hosts attached to it, either by Ethernet cable or wirelessly. These local hosts are referred to as being located on an internal, or inside, network. Most DHCP servers are configured to assign private addresses to the hosts on the internal network, rather than Internet routable public addresses. This ensures that, by default, the internal network is not directly accessible from the Internet.



The default IP address configured on the local integrated router interface is usually a private Class C address. Internal hosts must be assigned addresses within the same network as the integrated router, either statically configured, or through DHCP. When configured as a DHCP server, the integrated router provides addresses in this range. It also provides the subnet mask information and its own interface IP address as the default gateway. Many ISPs also use DHCP servers to provide IP addresses to the Internet side of the integrated router installed at their customer sites. The network assigned to the Internet side of the integrated router is referred to as the external, or outside, network.

When an integrated router is connected to the ISP, it acts like a DHCP client to receive the correct external network IP address for the Internet interface. ISPs usually provide an Internet-routable address, which enables hosts connected to the integrated router to have access to the Internet. The integrated router serves as the boundary between the local internal network and the external Internet. There are several ways hosts can be connected to an ISP and the Internet. Whether or not an individual host is assigned a public or private address depends on how it is connected.

Direct Connection

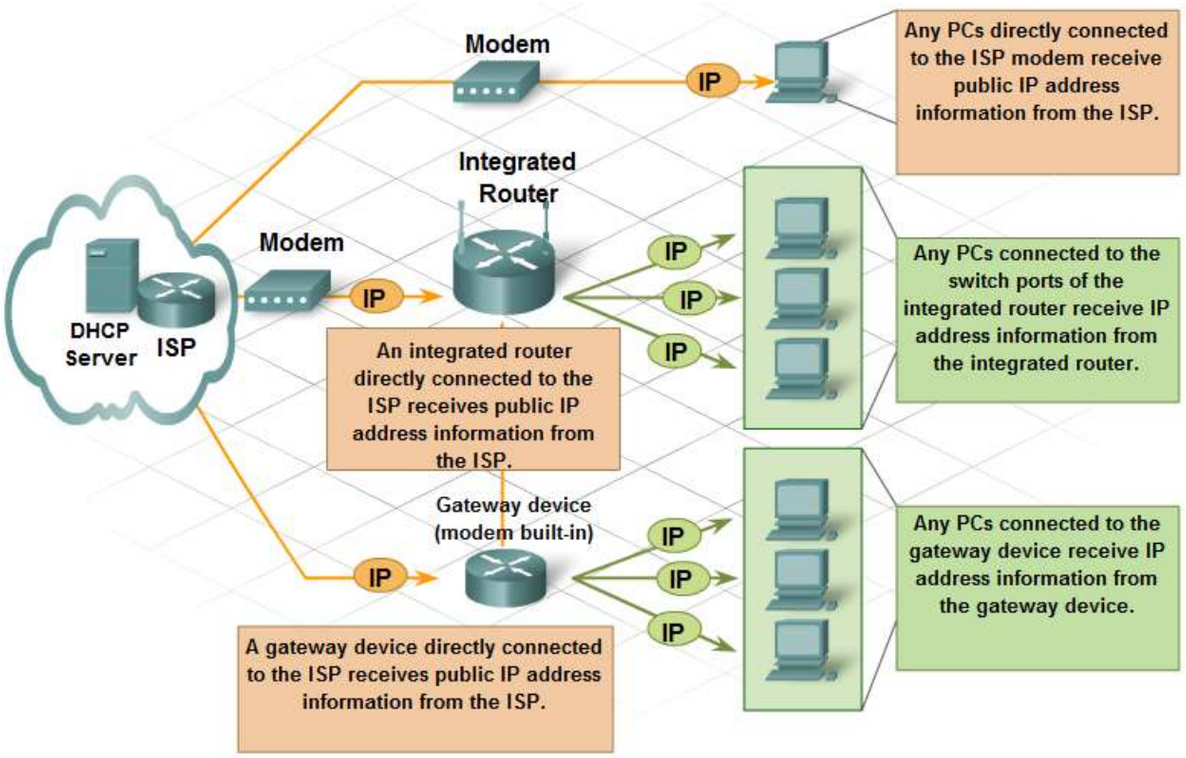
Some customers have just a single computer with a direct connection from the ISP through a modem. In this case, the public address from the ISP DHCP server is assigned to the single host.

Connection Through an Integrated Router

When there is more than one host that needs access to the Internet, the ISP modem can be attached directly to an integrated router instead of directly to a single computer. This enables the creation of a home or small business network. The integrated router receives the public address from the ISP. Internal hosts receive private addresses from the integrated router.

Connection Through a Gateway Device

Gateway devices combine an integrated router and a modem in one unit, and connect directly to the ISP service. As with integrated routers, the gateway device receives a public address from the ISP and internal PCs will receive private addresses from the gateway device.



Network Address Translation

The integrated router receives a public address from the ISP, which allows it to send and receive packets on the Internet. It, in turn, provides private addresses to local network clients. Since private addresses are not allowed on the Internet, a process is needed for translating private addresses into unique public addresses to allow local clients to communicate on the Internet.

The process used to convert private addresses to Internet-routable addresses is called Network Address Translation (NAT). With NAT, a private (local) source IP address is translated to a public (global) address. The process is reversed for incoming packets. The integrated router is able to translate many internal IP addresses to the same public address, by using NAT.

Only packets destined for other networks need to be translated. These packets must pass through the gateway, where the integrated router replaces the source host's private IP address with its own public IP address.

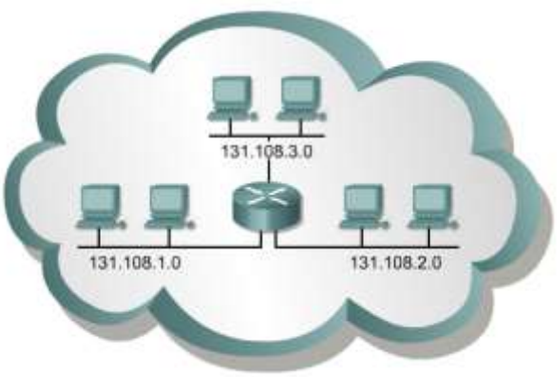
Although each host on the internal network has a unique private IP address assigned to it, the hosts must share the single Internet routable addressed assigned to the integrated router.

Subnetting

Introduction to subnetting

Subnetting is another method of managing IP addresses.

Internally, networks may be divided into smaller networks called subnetworks, or simply subnets. By providing a third level of addres subnets provide extra flexibility for the network administrator. For e Class B network address provided by the American Registry for Int Numbers (ARIN), can be broken up into many subnetworks. In this example, 131.108.1.0, 131.108.2.0, and 131.108.3.0 are all subnet the network 131.108.0.0.



This method of dividing full network address classes into smaller pieces has prevented complete IP address exhaustion. It is impossible to cover TCP/IP without mentioning subnetting. As a system administrator it is important to understand subnetting as a means of dividing and identifying separate networks throughout the LAN. It is not always necessary to subnet a small network. However, for large or extremely large networks, subnetting is required.

Subnetting a network means to use the subnet mask to divide the network and break a large network up into smaller, more efficient and manageable segments, or subnets. An example would be the U.S. telephone system which is broken into area codes, exchange codes, and local numbers. The system administrator must resolve these issues when adding and expanding the network. It is important to know how many subnets or networks are needed and how many hosts will be needed on each network. With subnetting, the network is not limited to the default Class A, B, or C network masks and there is more flexibility in the network design.

Decimal Notation for First Host Octet	Number of Subnets	Number of Class A Hosts per Subnet	Number of Class B Hosts per Subnet	Number of Class C Hosts per Subnet
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

Subnet addresses include the network portion, plus a subnet field and a host field. The subnet field and the host field are created from the original host portion for the entire network. The ability to decide how to divide the original host portion into the new subnet and host fields provides addressing flexibility for the network administrator. To create a subnet address, a network administrator borrows bits from the host field and designates them as the subnet field. The minimum number of bits that can be borrowed is two. When creating a subnet, where only one bit was borrowed the network number would be the .0 network. The broadcast number would then be the .255 network. The maximum number of bits that can be borrowed can be any number that leaves at least two bits remaining, for the host number.

The Mechanics of Subnetting

Classes of network IP addresses

To efficiently manage a limited supply of IP addresses, all classes can be subdivided into smaller subnetworks. Figure provides an overview of the division between networks and hosts.

IP Address Bit Patterns

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

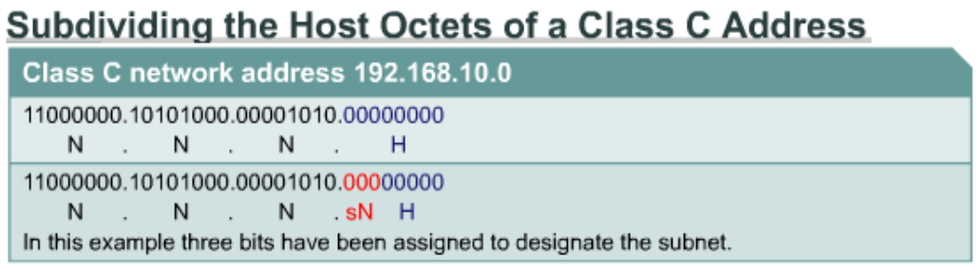
Class D	Host			
Octet	1	2	3	4

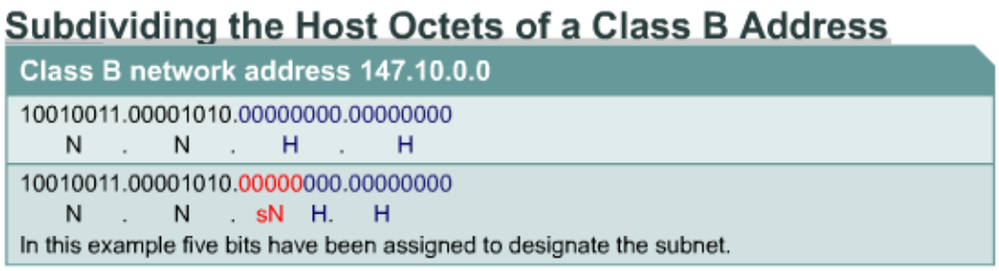
Class D addresses are used for multicast groups. There is no need to allocate octets or bits to separate network and host addresses. Class E addresses are reserved for research use only.

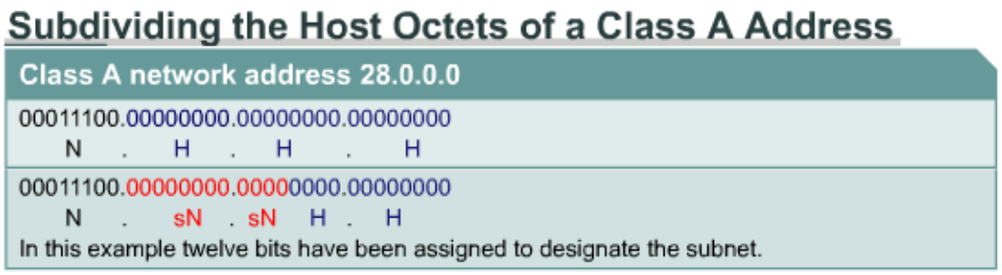
Reason for subnetting

To create the subnetwork structure, host bits must be reassigned as network bits. This is often referred to as 'borrowing' bits. However, a more accurate term would be lending bits. The starting point for this process is always the leftmost host bit, the one closest to the last network octet.

Subnet addresses include the Class A, Class B, and Class C network portion, plus a subnet field and a host field. The subnet field and the host field are created from the original host portion of the major IP address. This is done by re-assigning bits from the host portion to the original network portion of the address. The ability to divide the original host portion of the address into the new subnet and host fields provides addressing flexibility for the network administrator.







In addition to the need for manageability, subnetting enables the network administrator to provide broadcast containment and low-level security on the LAN. Subnetting provides some security since access to other subnets is only available through the services of a router. Further, access security may be provided through the use of access lists. These lists can permit or deny access to a subnet, based on a variety of criteria, thereby providing more security. Access lists will be studied later in the curriculum. Some owners of Class A and B networks have also discovered that subnetting creates a revenue source for the organization through the leasing or sale of previously unused IP addresses. Subnetting is an internal function of a network. From the outside, a LAN is seen as a single network with no details of the internal network structure. This view of the network keeps the routing tables small and efficient. Given a local node address of 147.10.43.14 on subnet 147.10.43.0, the world outside the LAN sees only the advertised major network number of 147.10.0.0. The reason for this is that the local subnet address of 147.10.43.0 is only valid within the LAN where subnetting is applied.

Establishing the subnet mask address

Selecting the number of bits to use in the subnet process will depend on the maximum number of hosts required per subnet. An understanding of basic binary math and the position value of the bits in each octet is necessary when calculating the number of subnetworks and hosts created when bits were borrowed.

Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1

The last two bits in the last octet, regardless of the IP address class, may never be assigned to the subnetwork. These bits are referred to as the last two significant bits. Use of all the available bits to create subnets, except these last two, will result in subnets with only two usable hosts. This is a practical address conservation method for addressing serial router links. However, for a working LAN this would result in prohibitive equipment costs.

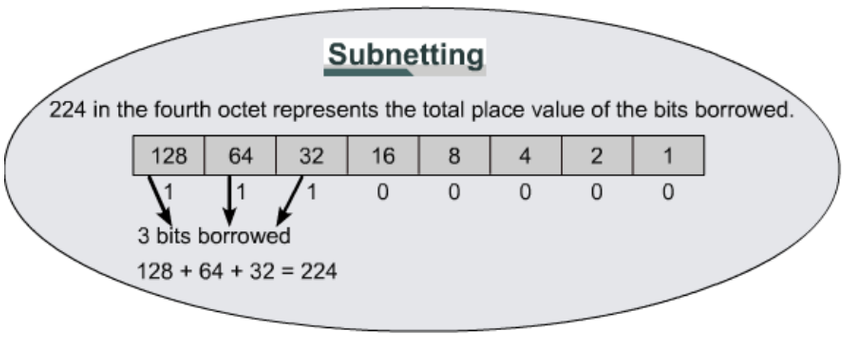
The subnet mask gives the router the information required to determine in which network and subnet a particular host resides.

Subnetting Chart (Subnet Mask Identifier)

Slash format	/25	/26	/27	/28	/29	/30	N/A	N/A
Mask	128	192	224	240	248	252	254	255
Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1

A Class C address with a /25 mask only borrows one bit as shown in the chart above. However, a Class B address with a /25 mask borrows nine bits.

The subnet mask is created by using binary ones in the network bit positions. The subnet bits are determined by adding the position value of the bits that were borrowed. If three bits were borrowed, the mask for a Class C address would be 255.255.255.224. This mask may also be represented, in the slash format, as /27. The number following the slash is the total number of bits that were used for the network and subnetwork portion.



To determine the number of bits to be used, the network designer needs to calculate how many hosts the largest subnetwork requires and the number of subnetworks needed. As an example, the network requires 30 hosts and five subnetworks. A shortcut to determine how many bits to reassign is by using the subnetting chart.

Subnetting Chart

Slash format	/25	/26	/27	/28	/29	/30	N/A	N/A
Mask	128	192	224	240	248	252	254	255
Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1
Total Subnets		4	8	16	32	64		
Usable Subnets		2	6	14	30	62		
Total Hosts		64	32	16	8	4		
Usable Hosts		62	30	14	6	2		

A Class C address with a /25 mask only borrows one bit as shown in the chart above. However, a Class B address with a /25 mask borrows nine bits.

By consulting the row titled (Usable Hosts), the chart indicates that for 30 usable hosts three bits are required. The chart also shows that this creates six usable subnetworks, which will satisfy the requirements of this scheme. The difference between usable hosts and total hosts is a result of using the first available address as the ID and the last available address as the broadcast for each subnetwork. Borrowing the appropriate number of bits to accommodate required subnetworks and hosts per subnetwork can be a balancing act and may result in unused host addresses in multiple subnetworks. The ability to use these addresses is not provided with classful routing. However, classless routing, which will be covered later in the course can recover many of these lost addresses.

The method that was used to create the subnet chart can be used to solve all subnetting problems. This method uses the following formula:

Number of usable subnets = two to the power of the assigned subnet bits or borrowed bits, minus two. The minus two is for the reserved addresses of network ID and network broadcast.

$$(2^{\text{power of borrowed bits}}) - 2 = \text{usable subnets}$$
$$(2^3) - 2 = 6$$

Number of usable hosts = two to the power of the bits remaining, minus two (reserved addresses for subnet id and subnet broadcast).

$$(2^{\text{power of remaining host bits}}) - 2 = \text{usable hosts}$$
$$(2^5) - 2 = 30$$

Applying the subnet mask

Once the subnet mask has been established it then can be used to create the subnet scheme. The chart in Figure is an example of the subnets and addresses created by assigning three bits to the subnet field. This will create eight subnets with 32 hosts per subnet. Start with zero (0) when numbering subnets. The first subnet is always referenced as the zero subnet.

Subnet Scheme

Subnetwork #	Subnetwork ID	Host Range	Broadcast ID
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

When filling in the subnet chart three of the fields are automatic, others require some calculation. The subnetwork ID of subnet zero is the same as the major network number, in this case 192.168.10.0. The broadcast ID for the whole network is the largest number possible, in this case 192.168.10.255. The third number that is given is the subnetwork ID for subnet number seven. This number is the three network octets with the subnet mask number inserted in the fourth octet position. Three bits were assigned to the subnet field with a cumulative value of 224. The ID for subnet seven is 192.168.10.224. By inserting these numbers, checkpoints have been established that will verify the accuracy when the chart is completed.

When consulting the subnetting chart or using the formula, the three bits assigned to the subnet field will result in 32 total hosts assigned to each subnet. This information provides the step count for each subnetwork ID. Adding 32 to each preceding number, starting with subnet zero, the ID for each subnet is established. Notice that the subnet ID has all binary 0s in the host portion.

Subnetting Chart

Slash format	/25	/26	/27	/28	/29	/30	N/A	N/A
Mask	128	192	224	240	248	252	254	255
Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1
Total Subnets		4	8	16	32	64		
Usable Subnets		2	6	14	30	62		
Total Hosts		64	32	16	8	4		
Usable Hosts		62	30	14	6	2		

A Class C address with a /25 mask only borrows one bit as shown in the chart above. However, a Class B address with a /25 mask borrows nine bits.

The broadcast field is the last number in each subnetwork, and has all binary ones in the host portion. This address has the ability to broadcast only to the members of a single subnet. Since the subnetwork ID for subnet zero is 192.168.10.0 and there are 32 total hosts the broadcast ID would be 192.168.10.31. Starting at zero the 32nd sequential number is 31. It is important to remember that zero (0) is a real number in the world of networking.

The balance of the broadcast ID column can be filled in using the same process that was used in the subnetwork ID column. Simply add 32 to the preceding broadcast ID of the subnet. Another option is to start at the bottom of this column and work up to the top by subtracting one from the preceding subnetwork ID.

Subnetting Class A and B Networks

The Class A and B subnetting procedure is identical to the process for Class C, except there may be significantly more bits involved. The available bits for assignment to the subnet field in a Class A address is 22 bits while a Class B address has 14 bits.

Subdividing the Host Octets of a Class B Network

Class B network address 147.10.0.0 (14 bits available)
11001011.00001010.00000000.00000000 N . N . H . H
10010011.00001010.00000000.00000000 N . N . sN . sN H In this example 12 bits have been assigned to designate the subnet.

Subdividing the Host Octets of a Class A Network

Class A network adress 28.0.0.0 (22 bits available)
00011100.00000000.00000000.00000000 N . H . H . H
00011100.00000000.00000000.00000000 N . sN . sN . sN H In this example 20 bits have been assigned to designate the subnet.

Assigning 12 bits of a Class B address to the subnet field creates a subnet mask of 255.255.255.240 or /28. All eight bits were assigned in the third octet resulting in 255, the total value of all eight bits. Four bits were assigned in the fourth octet resulting in 240. Recall that the slash mask is the sum total of all bits assigned to the subnet field plus the fixed network bits.

Subnetting

Mask	128	192	224	240	248	252	254	255
Bits Borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1
Subnets	2	4	8	16	32	64	128	256

A Class C address with a /25 mask only borrows one bit as shown in the chart above. However, a Class B address with a /25 mask borrows nine bits.

Assigning 20 bits of a Class A address to the subnet field creates a subnet mask of 255.255.255.240 or /28. All eight bits of the second and third octets were assigned to the subnet field and four bits from the fourth octet. In this situation, it is apparent that the subnet mask for the Class A and Class B addresses appear identical. Unless the mask is related to a network address it is not possible to decipher how many bits were assigned to the subnet field.

Enter the subnet mask value into the subnet mask box based on the information provided in the other boxes. Click the check answer button to verify the answer.

Network Address	49.0.0.0
Number of Usable Subnets	47
Number of Hosts Per Subnet	10
Subnet Mask	

Whichever class of address needs to be sub netted, the following rules are the same:

Total subnets = 2 to the power of the bits borrowed

Total hosts = 2 to the power of the bits remaining

Usable subnets = 2 to the power of the bits borrowed **minus 2**

Usable hosts = 2 to the power of the bits remaining **minus 2**

Calculating the resident subnetwork through ANDing

Routers use subnet masks to determine the home subnetwork for individual nodes. This process is referred to as logical ANDing. ANDing is a binary process by which the router calculates the subnetwork ID for an incoming packet. ANDing is similar to multiplication.

The Logical ANDing Process

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

This process is handled at the binary level. Therefore, it is necessary to view the IP address and mask in binary. The IP address and the subnetwork address are ANDed with the result being the subnetwork ID. The router then uses that information to forward the packet across the correct interface.

Calculating the Subnet ID

Packet address	201.10.11.65	11001001.00001010.00001011.01000001
AND		
Mask	255.255.255.224	11111111.11111111.11111111.11100000
Subnetwork ID	201.10.11.64	11001001.00001010.00001011.01000000

Subnetting is a learned skill. It will take many hours performing practice exercises to gain a development of flexible and workable schemes.

Adapted and compiled from:

CCNA IT Essential, PC Hardware and Software version 4.0, Cisco Networking Academy
CCNA Discovery 1, Networking for Home and Small Businesses, Cisco Networking Academy
CCNA Discovery 2, Working at a Small-to-Medium Business of ISP, Cisco Networking Academy
CCNA Exploration 1, Network Fundamentals, Cisco Networking Academy
Cisco Networking Academy Program, CCNA 1 and 2 Companion Guide, Cisco Press