NETWORK ADMINISTRATION AND SECURITY

IP ADDRESSING

PURPOSE OF AN IP ADDRESS

A 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.

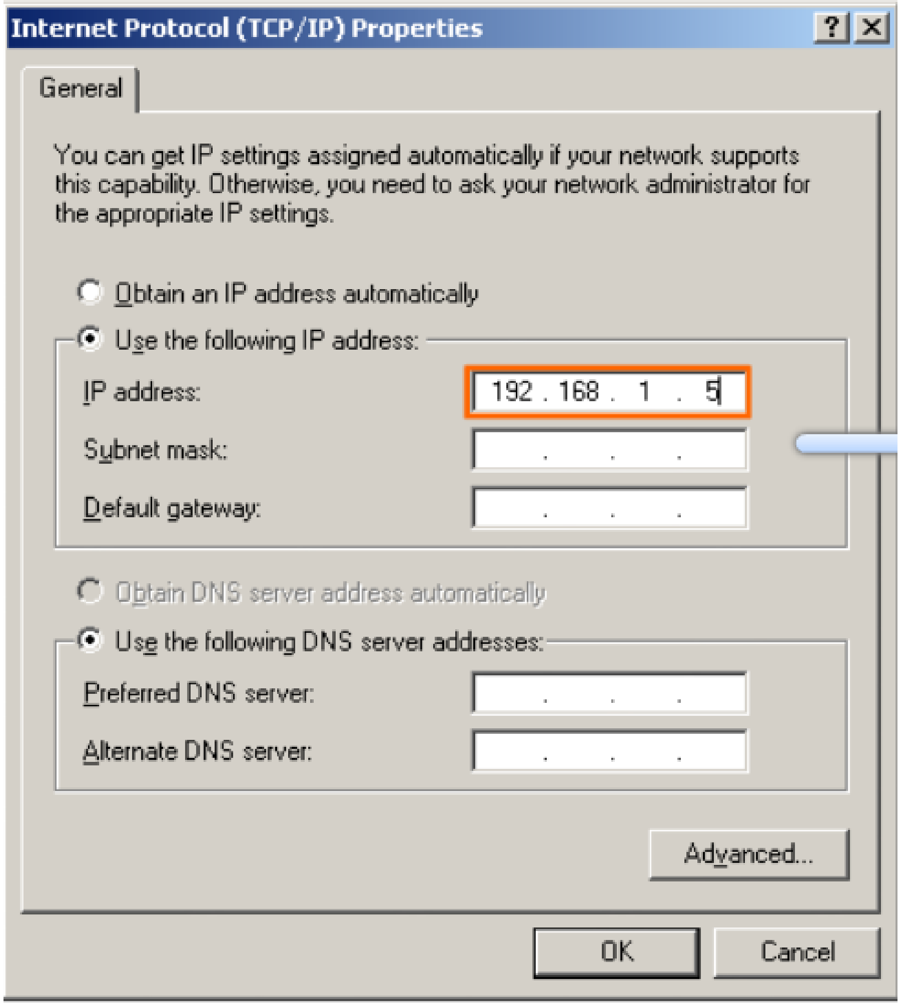
Every packet sent across the Internet has a source and destination IP address. This information is required by networking devices to insure the information gets to the destination and any replies are returned to the source.

THE 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.



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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 5

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

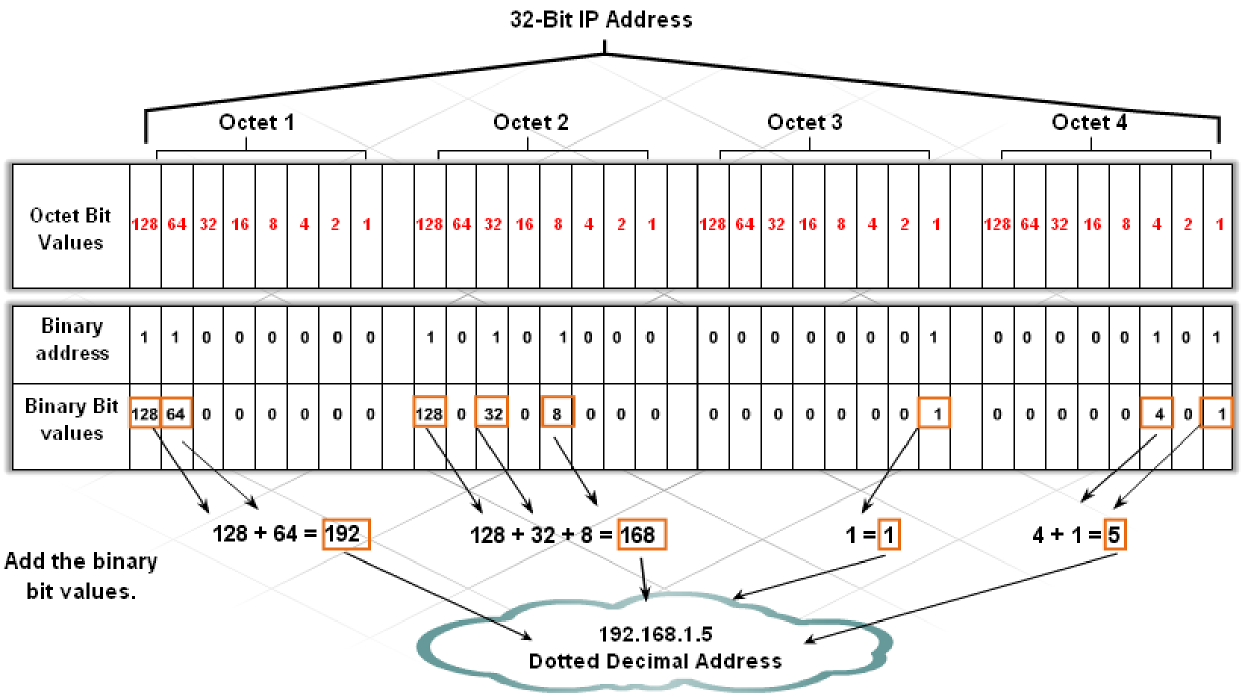
Preferred DNS server: . . .

Alternate DNS server: . . .

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. If there is a 0 in a position, do not add the value.

If all 8 bits are 0s. 00000000 the value of the octet is 0.
If all 8 bits are 1s, 11111111 the value of the octet is 255 (128+64+32+16+8+4+2+1)
If the 8 bits are mixed, 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.



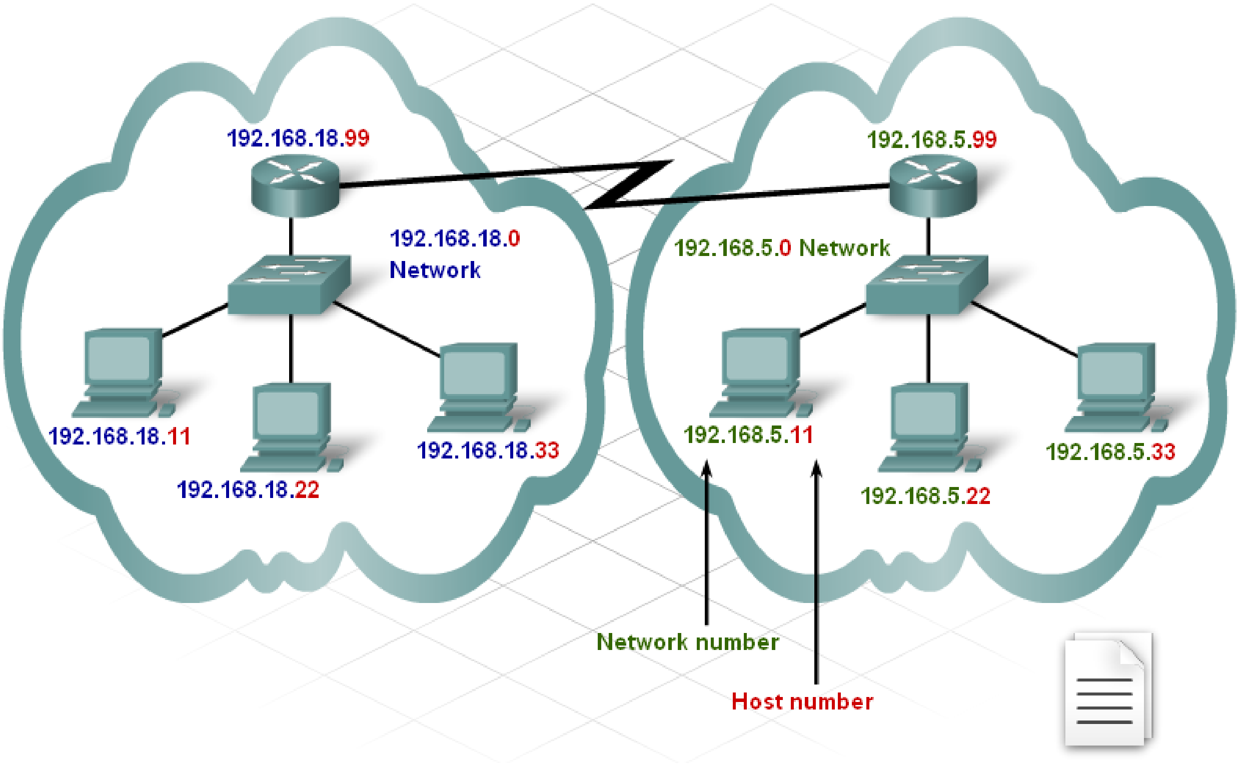
Octet Bit Values	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
Binary address	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1
Binary Bit values	128	64	0	0	0	0	0	0	128	0	32	0	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	4	0	1

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.



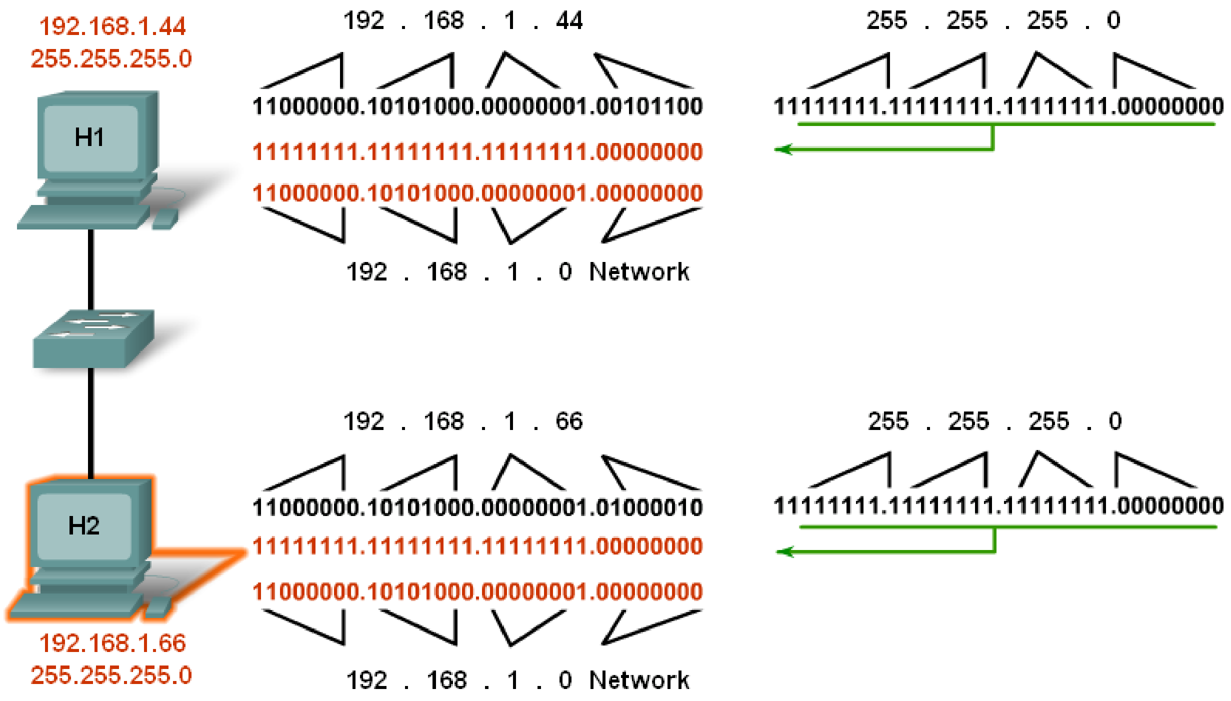
How an IP Address and the Subnet Mask Interact

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.

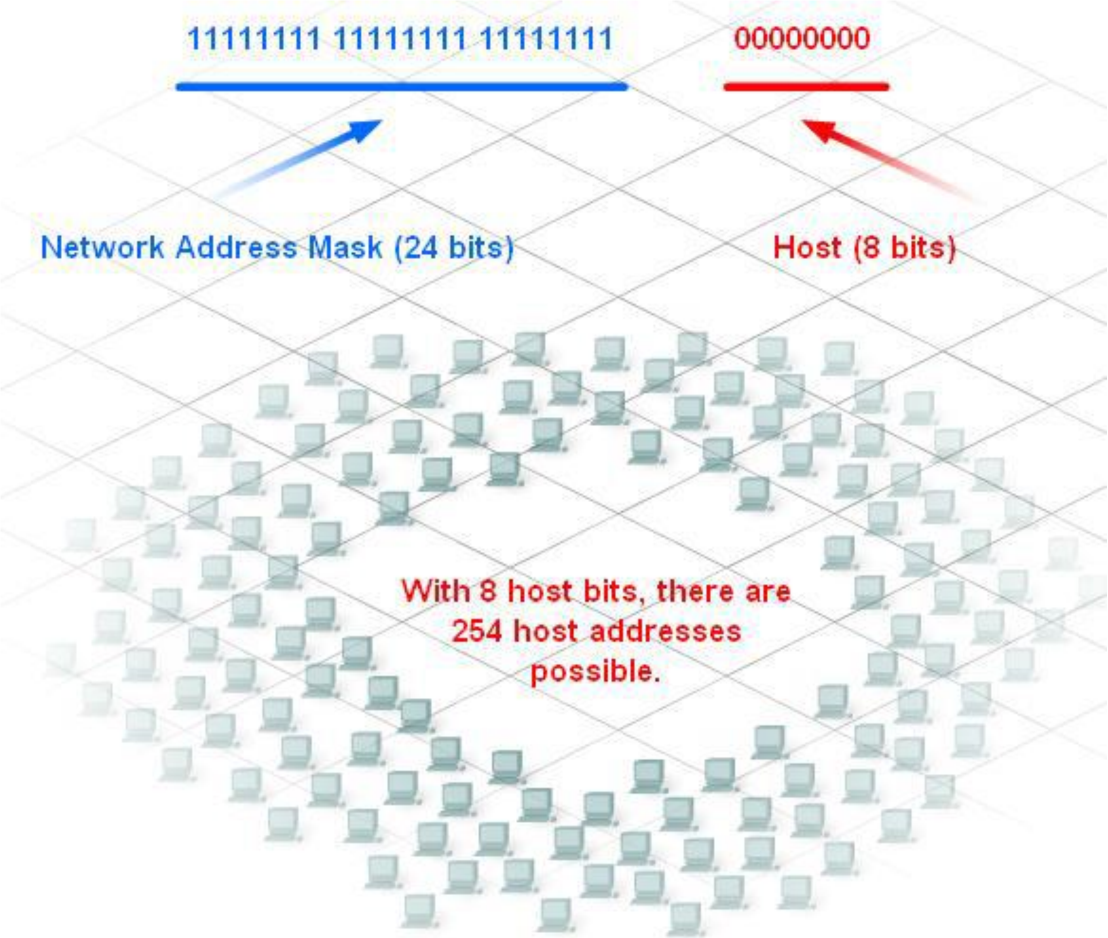


The subnet masks we see most often with home and small business networking are: 255.0.0.0 (8-bits), 255.255.0.0 (16 bits) and 255.255.255.0 (24 bits). A subnet mask of 255.255.255.0 (decimal) or 11111111.11111111.1111111.00000000 (binary) uses 24 bits to identify the network number which leaves 8 bits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


11111111 11111111 11111111
00000000
Network Address Mask (24 bits)
Host (8 bits)
With 8 host bits, there are 254 host addresses possible.

IP Address Classes and their Default Network 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.

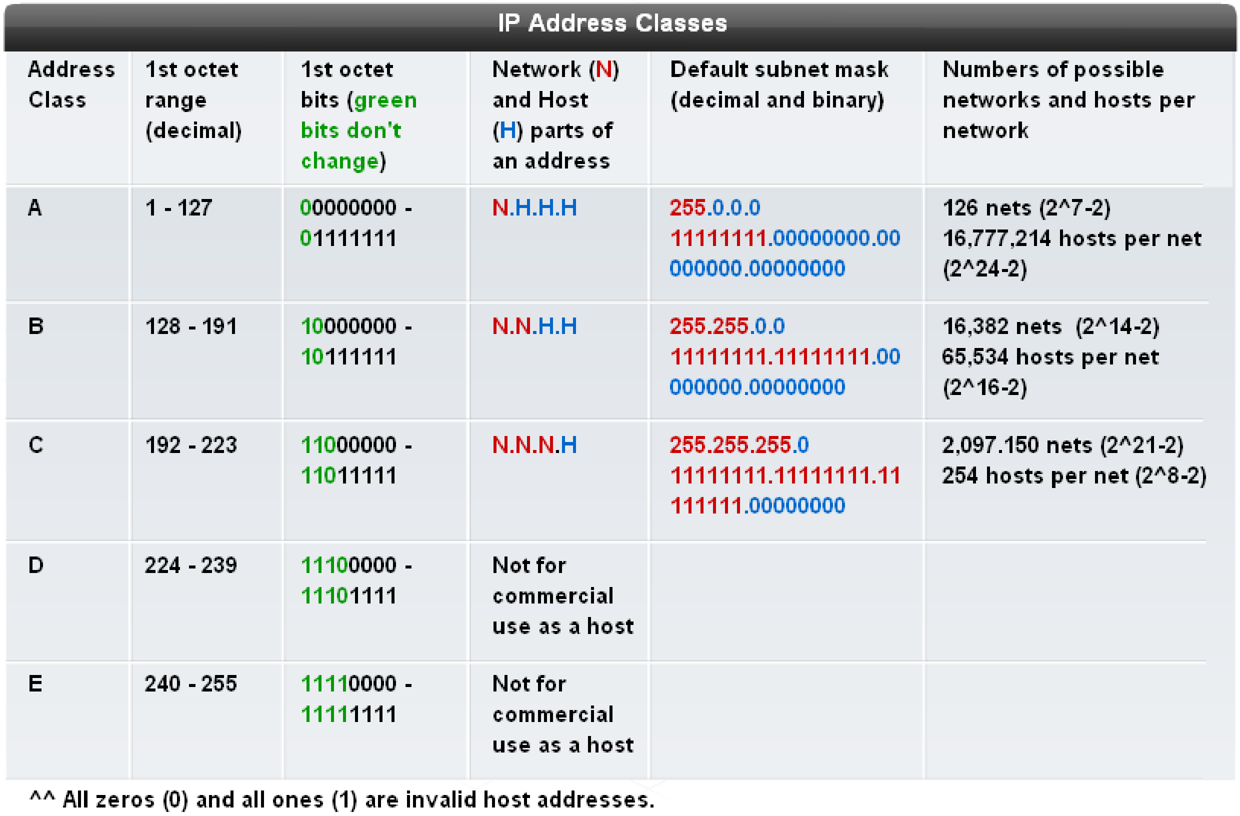
IP addresses are grouped into 5 classes. Classes A, B and C are commercial addresses and are assigned to hosts. Class D is reserved for multicast use and Class E is for experimental use.

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.

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.

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.

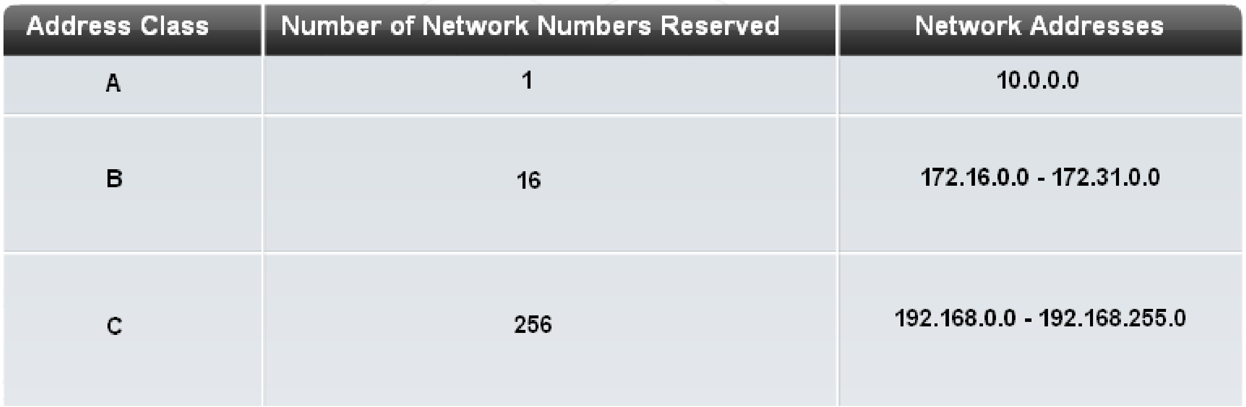
RFC 1918 is a standard that reserves several ranges of addresses within each of the classes A, B and C. As shown in the table, these private address ranges consist of a single Class A network, 16 Class B networks and 256 Class C networks. This gives a network administrator considerable flexibility in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

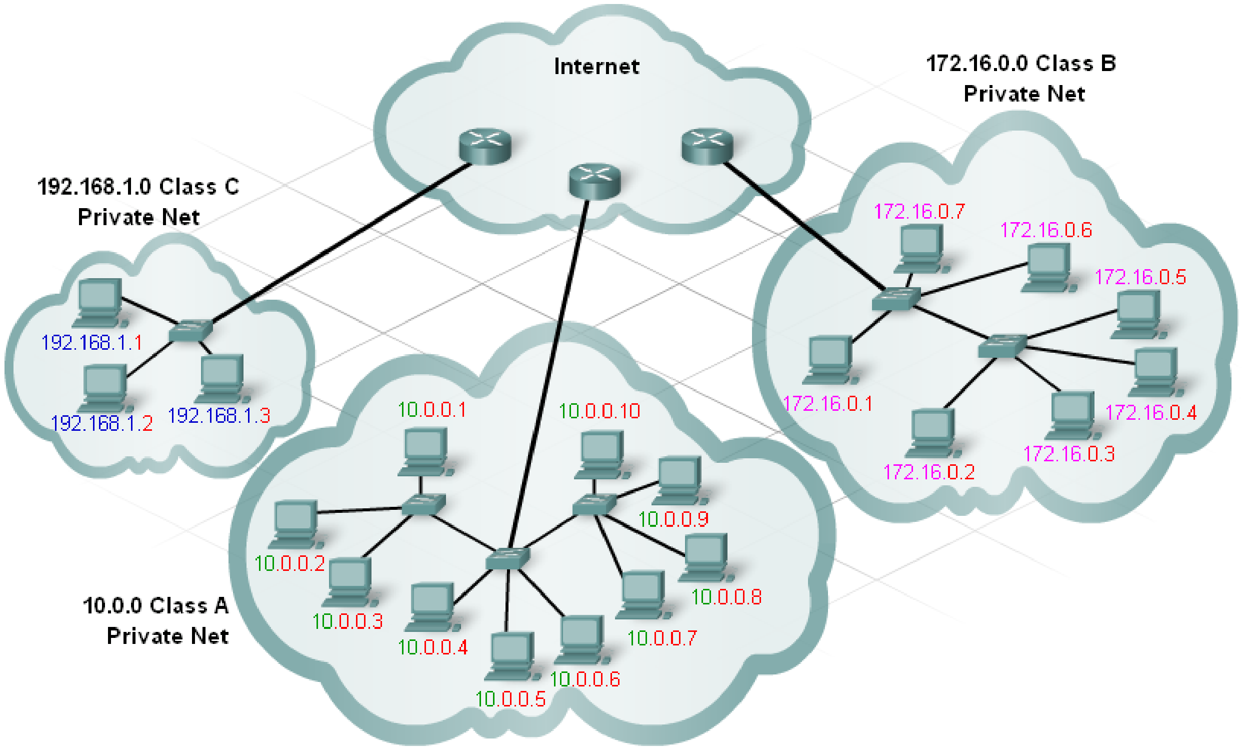


Address Class	Number of Network Numbers Reserved	Network Addresses
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0

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.



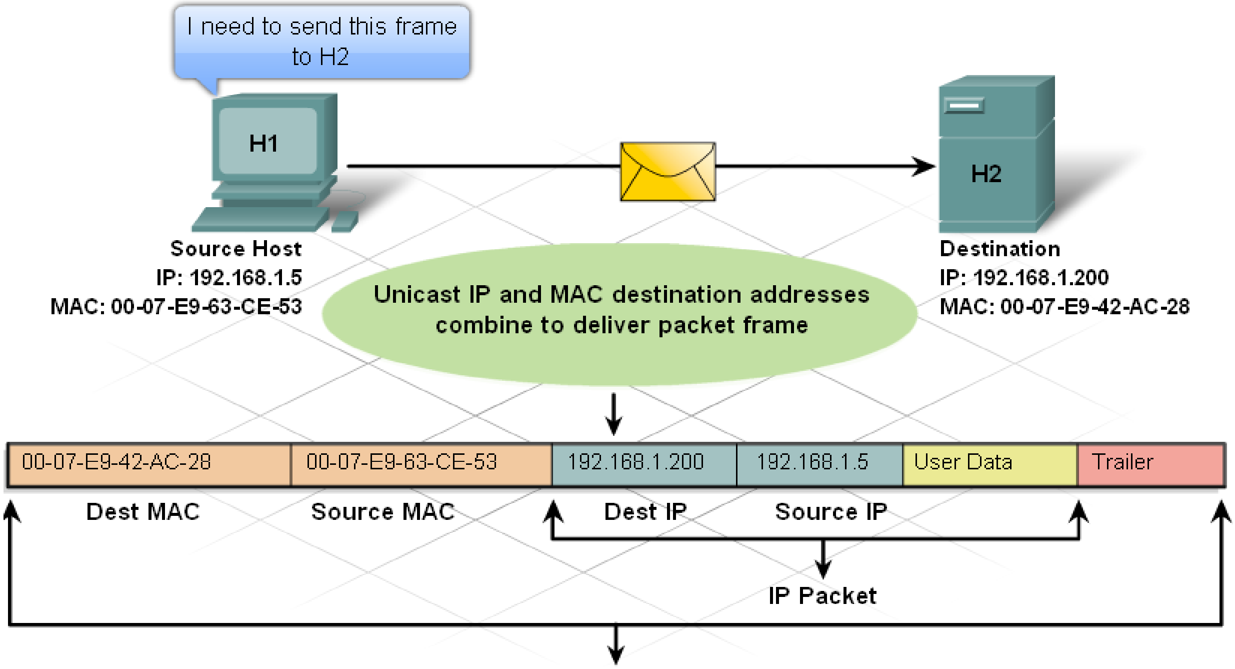
Types of IP Addresses

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.

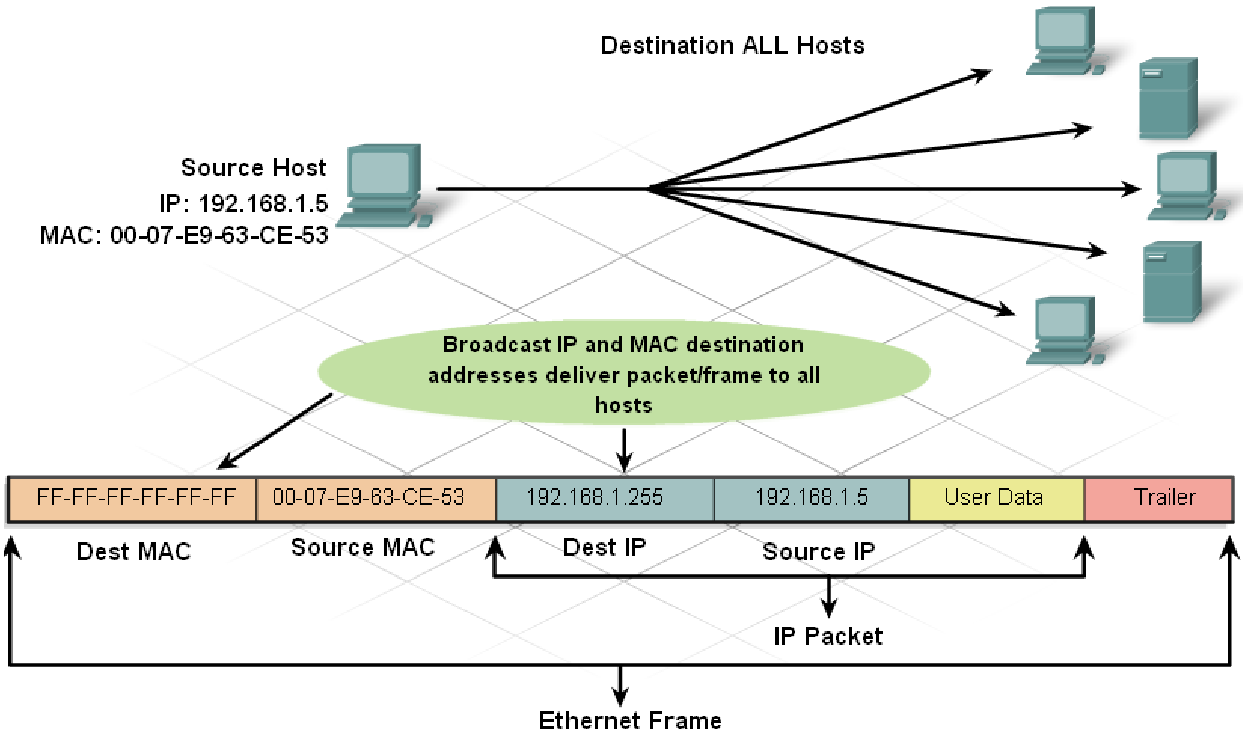


Broadcast

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.



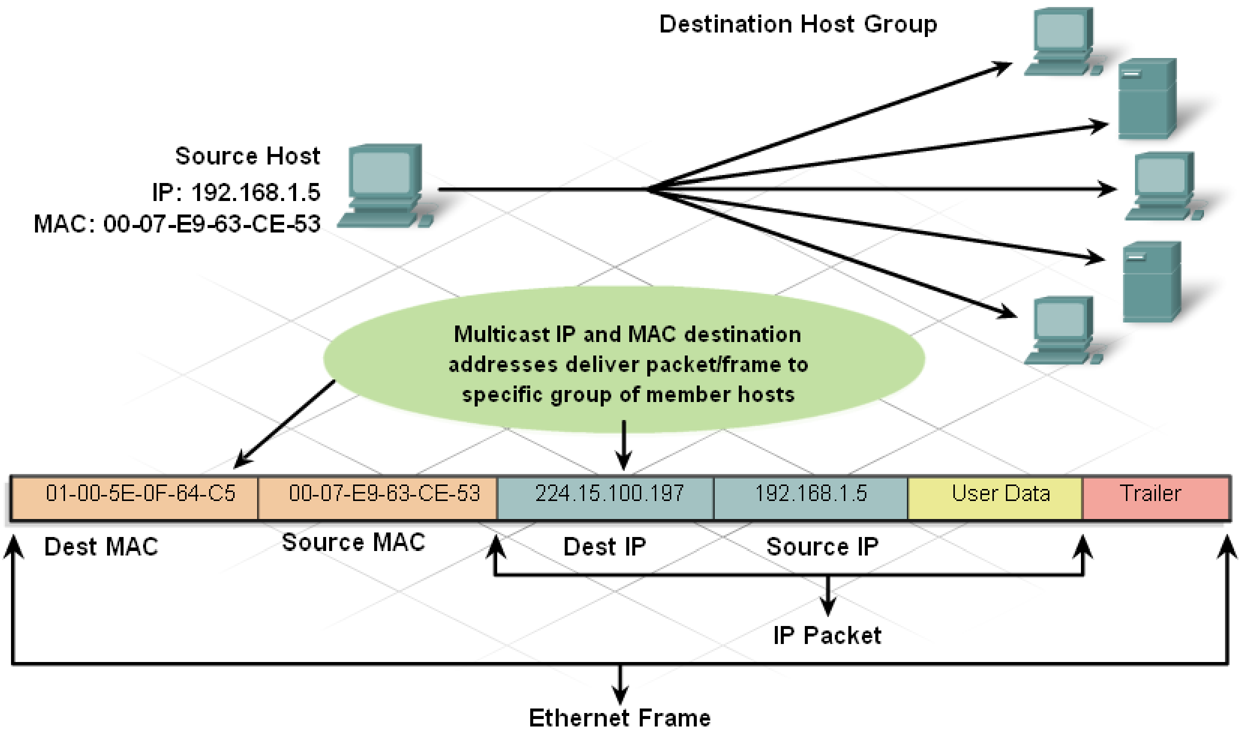
Multicast

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.



STATIC AND DYNAMIC ADDRESSING

IP addresses can be assigned either statically or dynamically.

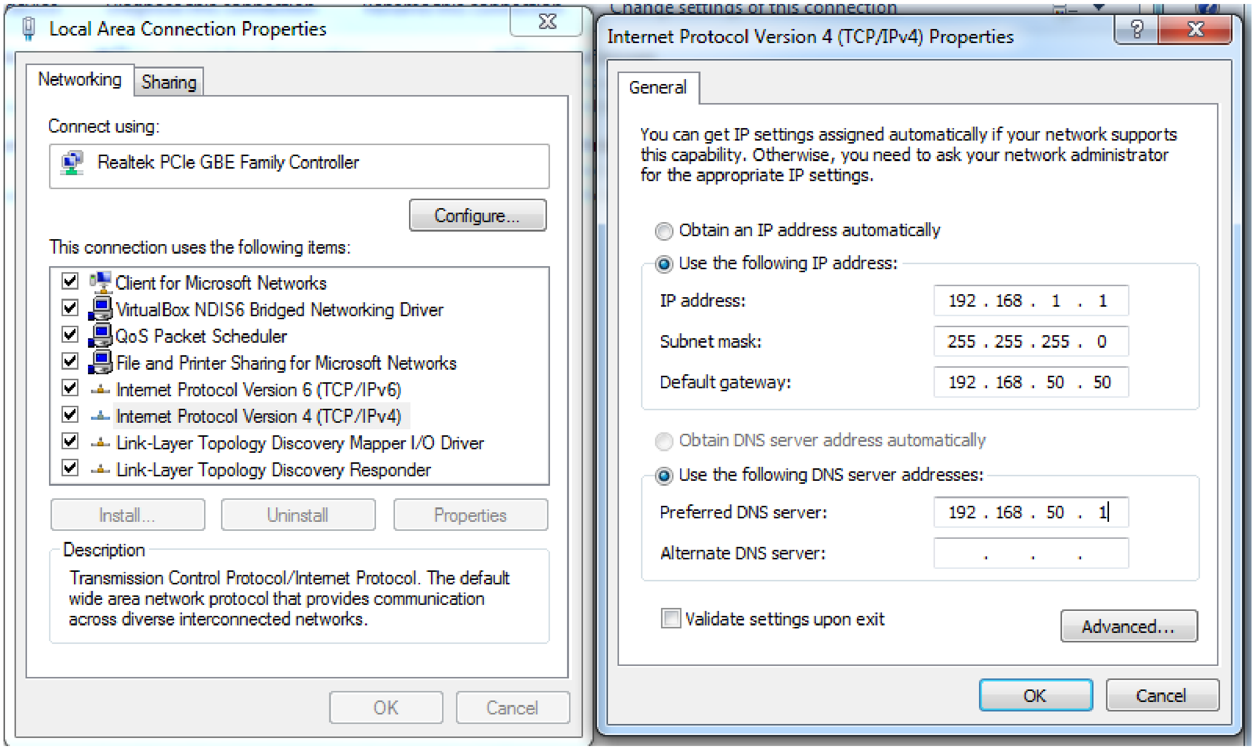
Static Addressing

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.



Local Area Connection Properties

Networking | Sharing

Connect using:

Realtek PCIe GBE Family Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ VirtualBox NDIS6 Bridged Networking Driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 50 . 50

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 50 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

Dynamic Addressing

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.

SUBNETTING

It is a technique that enables a network administrator to divide a single private Internet Protocol (IP) network into multiple smaller logical subnetworks by subdividing the host address into a subnetwork address and host address.

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. For each bit borrowed, we double the number of subnetworks available. For example, if we borrow 1 bit, we can define 2 subnets. If we borrow 2 bits, we can have 4 subnets. However, with each bit we borrow, fewer host addresses are available per subnet.

Router A 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".

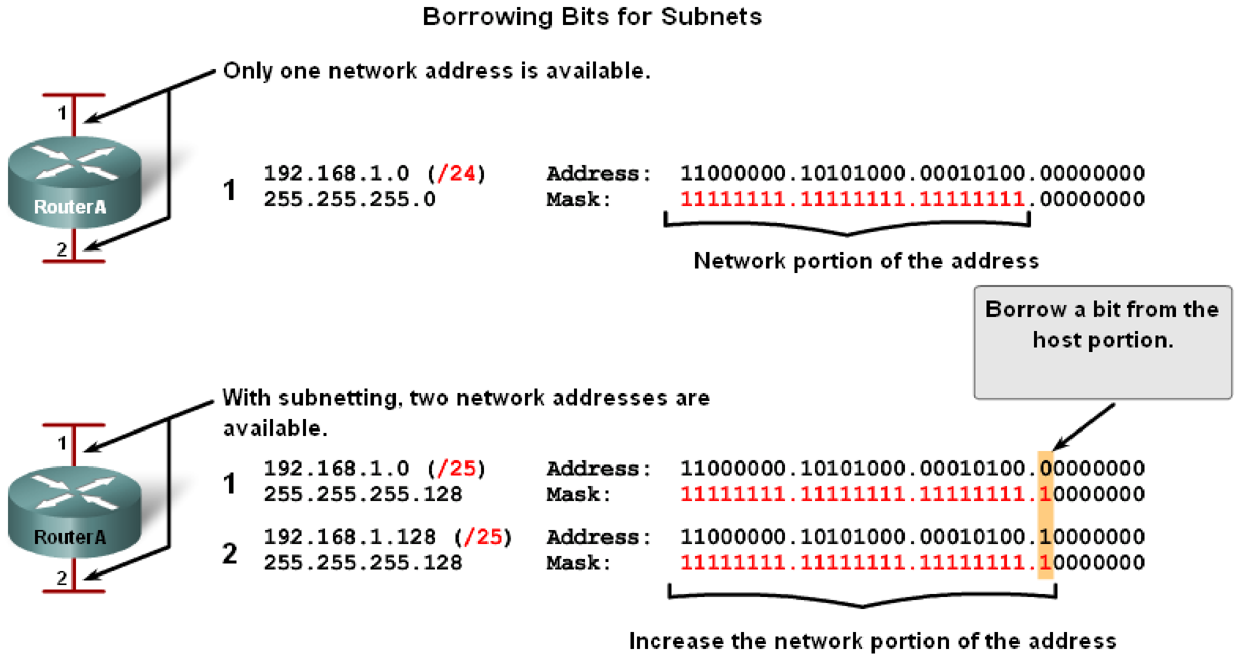
Formula for calculating subnets

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


Borrowing Bits for Subnets
Only one network address is available.
1
Router A
2
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
Router A
2
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

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.

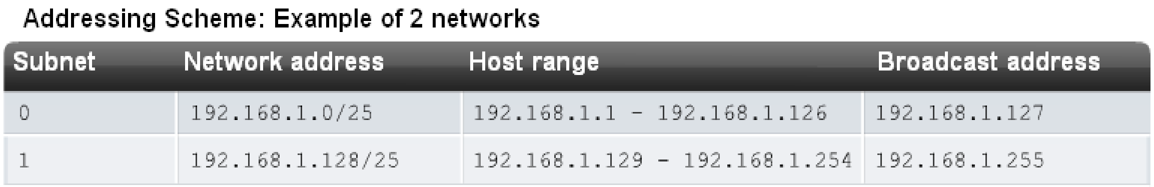
Applying this formula, (2^7 - 2 = 126) shows that each of these subnets can have 126 hosts.

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

See the figure for the addressing scheme for these networks.



Addressing Scheme: Example of 2 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

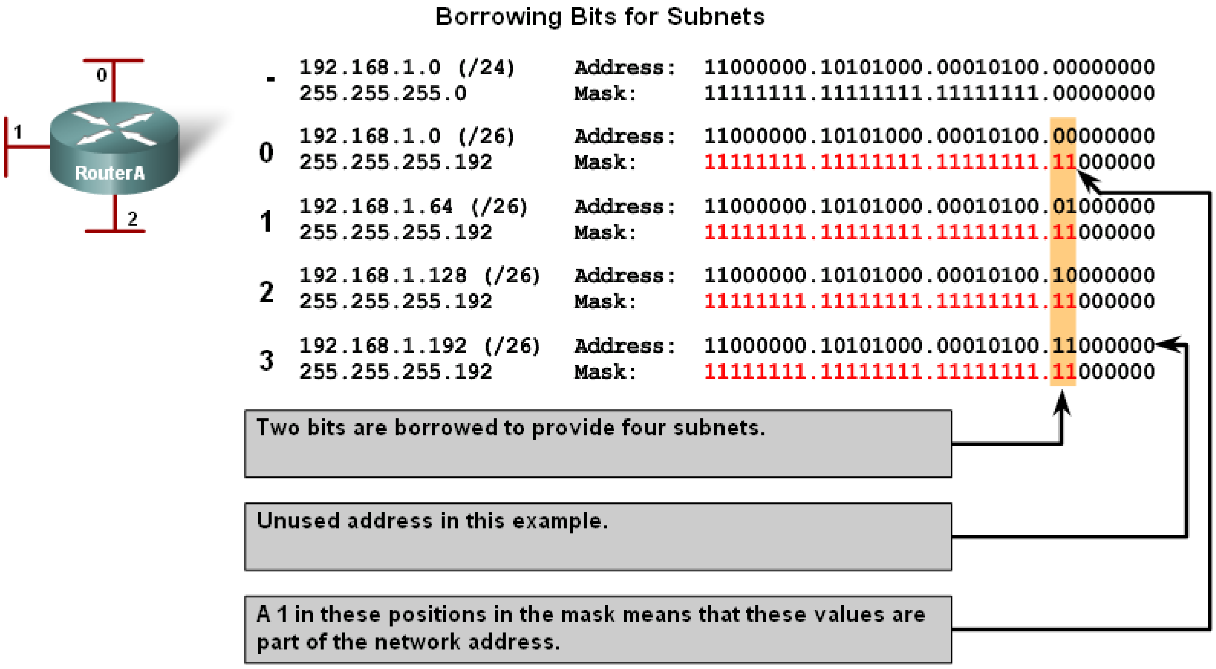
Example with 3 subnets

Next, consider an internetwork that requires three subnets. See the figure.

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



Borrowing Bits for Subnets

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

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

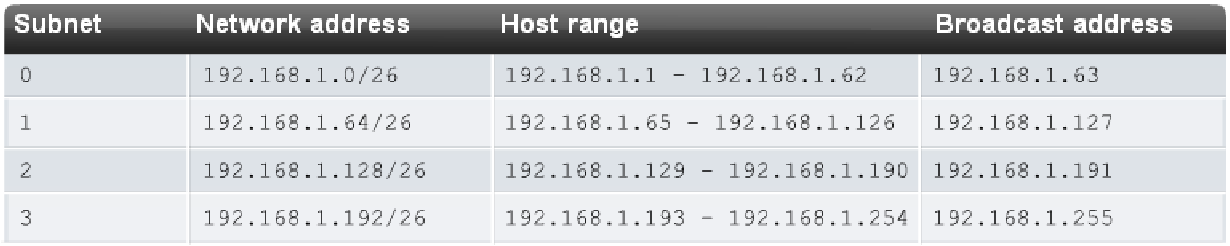
Subnet 3: 192 = 11000000

Apply the host calculation formula.

2^6 - 2 = 62 hosts per subnet

See the figure for the addressing scheme for these networks.

Addressing Scheme: Example of 4 networks



Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255