IP Address Notation - What Is An IP Address?

This tutorial explains the technology behind Internet Protocol (IP) networking. For those not interested in the technical aspects, skip to the following:

IPv4 and IPv6

Internet Protocol (IP) technology was developed in the 1970s to support some of the first research computer networks. Today, IP has become a worldwide standard for home and business networking as well. Our network routers, Web browsers, email programs, instant messaging software - all rely on IP or other network protocols layered on top of IP. Two versions of IP technology exist today.

Essentially all home computer networks use IP version 4 (IPv4), but an increasing number of educational and research institutions have adopted the next generation IP version 6 (IPv6).

IPv4 Addressing Notation

An IPv4 address consists of four bytes (32 bits). These bytes are also known as octets. For readability purposes, humans typically work with IP addresses in a notation called dotted decimal. This notation places periods between each of the four numbers (octets) that comprise an IP address. For example, an IP address that computers see as

00001010 00000000 00000000 00000001

is written in dotted decimal as

10.0.0.1

Because each byte contains 8 bits, each octet in an IP address ranges in value from a minimum of 0 to a maximum of 255. Therefore, the full range of IP addresses is from 0.0.0.0 through 255.255.255.255. That represents a total of 4,294,967,296 possible IP addreses.

IPv6 Addressing Notation

IP addresses change significantly with IPv6. IPv6 addresses are 16 bytes (128 bits) long rather than four bytes (32 bits). This larger size means that IPv6 supports more than

300,000,000,000,000,000,000,000,000,000,000,000,000 possible addresses! In the coming years, as an increasing number of cell phones, PDAs, and other consumer electronics expand their networking capability, the smaller IPv4 address space will likely run out and IPv6 address become necessary.

IPv6 addresses are generally written in the following form:

```
hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh
```

In this full notation, pairs of IPv6 bytes are separated by a colon and each byte in turns is represented as a pair of hexadecimal numbers, like in the following example:

```
E3D7:0000:0000:0000:51F4:9BC8:C0A8:6420
```

As shown above, IPv6 addresses commonly contain many bytes with a zero value.Shorthand notation in IPv6 removes these values from the text representation (though the bytes are still present in the actual network address) as follows:

```
E3D7::51F4:9BC8:C0A8:6420
```

Finally, many IPv6 addresses are extensions of IPv4 addresses. In these cases, the rightmost four bytes of an IPv6 address (the rightmost two byte pairs) may be rewritten in the IPv4 notation. Converting the above example to mixed notation yields

```
E3D7::51F4:9BC8:192.168.100.32
```

IPv6 addresses may be written in any of the full, shorthand or mixed notation illustrated above.

IPv4 Address Classes

The IPv4 address space can be subdivided into 5 **classes** - Class A, B, C, D and E. Each class consists of a contiguous subset of the overall IPv4 address range. With a few special exceptions explained further below, the values of the leftmost four bits of an IPv4 address determine its class as follows:

Class	Leftmost bits	Start address	Finish address
A	0xxx	0.0.0.0	127.255.255.255
B	10xx	128.0.0.0	191.255.255.255
C	110x	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

All Class C addresses, for example, have the leftmost three bits set to '110', but each of the remaining 29 bits may be set to either '0' or '1' independently (as represented by an x in these bit positions):

110xxxxx xxxxxxxx xxxxxxxx xxxxxxxx

Converting the above to dotted decimal notation, it follows that all Class C addresses fall in the range from 192.0.0.0 through 223.255.255.255.

IP Address Class E and Limited Broadcast

The IPv4 networking standard defines Class E addresses as reserved, meaning that they should not be used on IP networks. Some research organizations use Class E addresses for experimental purposes. However, nodes that try to use these addresses on the Internet will be unable to communicate properly.

A special type of IP address is the limited broadcast address 255.255.255.255. A broadcast involves delivering a message from one sender to many recipients. Senders direct an IP broadcast to 255.255.255.255 to indicate all other nodes on the local network (LAN) should pick up that message. This broadcast is 'limited' in that it does not reach every node on the Internet, only nodes on the LAN.

Technically, IP reserves the entire range of addresses from 255.0.0.0 through 255.255.255.255 for broadcast, and this range should not be considered part of the normal Class E range.

IP Address Class D and Multicast

The IPv4 networking standard defines Class D addresses as reserved for multicast. Multicast is a mechanism for defining groups of nodes and sending IP messages to that group rather than to every node on the LAN (broadcast) or just one other node (unicast).

Multicast is mainly used on research networks. As with Class E, Class D addresses should not be used by ordinary nodes on the Internet.

IP Address Class A, Class B, and Class C

Class A, Class B, and Class C are the three classes of addresses used on IP networks in common practice, with three exceptions as explained next.

IP Loopback Address

127.0.0.1 is the loopback address in IP. Loopback is a test mechanism of network adapters. Messages sent to 127.0.0.1 do not get delivered to the network. Instead, the adapter intercepts all loopback messages and returns them to the sending application. IP applications often use this feature to test the behavior of their network interface.

As with broadcast, IP officially reserves the entire range from 127.0.0.0 through 127.255.255.255 for loopback purposes. Nodes should not use this range on the Internet, and it should not be considered part of the normal Class A range.

Zero Addresses

As with the loopback range, the address range from 0.0.0.0 through 0.255.255.255 should not be considered part of the normal Class A range. 0.x.x.x addresses serve no particular function in IP, but nodes attempting to use them will be unable to communicate properly on the Internet.

Private Addresses

The IP standard defines specific address ranges within Class A, Class B, and Class C reserved for use by private networks (intranets). The table below lists these reserved ranges of the IP address space.

Class	**Private start address**	**Private finish address**
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Nodes are effectively free to use addresses in the private ranges if they are not connected to the Internet, or if they reside behind firewalls or other gateways that use Network Address Translation (NAT).

IPv6 Address Types

IPv6 does not use classes. IPv6 supports the following three IP address types:

unicast

multicast

anycast

Unicast and multicast messaging in IPv6 are conceptually the same as in IPv4. IPv6 does not support broadcast, but its multicast mechanism accomplishes essentially the same effect. Multicast addresses in IPv6 start with 'FF' (255) just like IPv4 addresses.

Anycast in IPv6 is a variation on multicast. Whereas multicast delivers messages to all nodes in the multicast group, anycast delivers messages to any one node in the multicast group. Anycast is an advanced networking concept designed to support the failover and load balancing needs of applications.

IPv6 Reserved Addresses

IPv6 reserves just two special addresses: 0:0:0:0:0:0:0:0 and 0:0:0:0:0:0:0:1. IPv6 uses 0:0:0:0:0:0:0:0 internal to the protocol implementation, so nodes cannot use it for their own communication purposes. IPv6 uses 0:0:0:0:0:0:0:1 as its loopback address, equivalent to 127.0.0.1 in IPv4.

IP Network Partioning

Computer networks consist of individual segments of network cable. The electrical properties of cabling limit the useful size of any given segment such that even a modestly-sized local-area network (LAN) will require several of them. Gateway devices like routers and bridges connect these segments together although not in a perfectly seamless way...

Besides partitioning through the use of cable, subdividing of the network can also be done at a higher level. Subnets support virtual network segments that partition traffic flowing through the cable rather than the cables themselves. The subnet configuration often matches the segment layout one-to-one, but subnets can also subdivide a given network segment.

IP Network Numbering

Even without subnetting (explained later), hosts on the Internet or any other IP network are assigned a network number. Network numbering allows a group of hosts (peers) to communicate efficiently with each other. Hosts on the same network may be computers located in the same facility or all computers used by a workgroup, for example. Multi-homed hosts, that contain multiple network adapters, can belong to multiple networks, but each adapter is assigned exactly one network number.

Network numbers look very much like IP addresses, but the two should not be confused. Consider for example the host IP address 10.0.0.1, an address commonly used on private networks. Because it is a Class A address, with no subnetting employed, its leftmost byte (eight bits) by default refer to the network address and all other bits remain set at zero. Thus, 10.0.0.0 is the network number corresponding to IP address 10.0.0.1.

The portion of the IP address that does not refer to the network refers instead to the host address - literally, the unique identifier of the host on that network. In the above example, the host address becomes '0.0.0.1' or simply '1'. Also note that a network address becomes a reserved address that should not be assigned to any actual host. Configuring a live host at 10.0.0.0 in the example above could impact communications for all hosts on that network.

The table below illustrates the default numbering scheme for Class A, B, and C networks.

Class	**Host address range**	**Network address**	**Default mask**
A	0.0.0.0 - 127.255.255.255	x.0.0.0	255.0.0.0
B	128.0.0.0 - 191.255.255.255	x.x.0.0	255.255.0.0
C	192.0.0.0 - 223.255.255.255	x.x.x.0	255.255.255.0

In general, a network address uses the leftmost byte of its hosts' addressing if the hosts fall within the Class A range, the leftmost two bytes for hosts in Class B, and the leftmost three bytes for hosts in Class C. This algorithm is applied in practice through the use of a network mask. The above table shows the decimal representation of the default network masks that is commonly used by network operating systems. Note that the decimal value '255' corresponds to one byte that has all bits set to one (11111111).

Benefit of Network Addressing

Network addressing fundamentally organizes hosts into groups. This can improve security (by isolating critical nodes) and can reduce network traffic (by preventing transmissions between nodes that do not need to communicate with each other). Overall, network addressing becomes even more powerful when introducing subnetting and/or supernetting.

Subnet Masks and Subnetting

A subnet allows the flow of network traffic between hosts to be segregated based on a network configuration. By organizing hosts into logical groups, subnetting can improve network security and performance.

Subnet Mask

Perhaps the most recognizable aspect of subnetting is the subnet mask. Like IP addresses, a subnet mask contains four bytes (32 bits) and is often written using the same "dotted-decimal" notation. For example, a very common subnet mask in its binary representation

11111111 11111111 11111111 00000000

is typically shown in the equivalent, more readable form

255.255.255.0

Applying a Subnet Mask

A subnet mask neither works like an IP address, nor does it exist independently from them. Instead, subnet masks accompany an IP address and the two values work together.

Applying the subnet mask to an IP address splits the address into two parts, an "extended network address" and a host address.

For a subnet mask to be valid, its leftmost bits must be set to '1'. For example, 00000000 00000000 00000000 00000000

is an invalid subnet mask because the leftmost bit is set to '0'.

Conversely, the rightmost bits in a valid subnet mask must be set to '0', not '1'. Therefore,

11111111 11111111 11111111 11111111

is invalid.

All valid subnet masks contain two parts: the left side with all mask bits set to '1' (the extended network portion) and the right side with all bits set to '0' (the host portion), such as the first example above.

Subnetting in Practice

Subnetting works by applying the concept of extended network addresses to individual computer (and other network device) addresses.

An extended network address includes both a network address and additional bits that represent the subnet number...

Together, these two data elements support a two-level addressing scheme recognized by standard implementations of IP. The network address and subnet number, when combined with the host address, therefore support a three-level scheme.

Consider the following real-world example. A small business plans to use the 192.168.1.0 network for its internal (intranet) hosts. The human resources department wants their computers to be on a restricted part of this network because they store payroll information and other sensitive employee data. But because this is a Class C network, the default subnet mask of 255.255.255.0 allows all computers on the network to be peers (to send messages directly to each other) by default.

The first four bits of 192.168.1.0 -

1100

place this network in the Class C range and also fix the length of the network address at 24 bits. To subnet this network, more than 24 bits must be set to '1' on the left side of the subnet mask. For instance, the 25-bit mask 255.255.255.128 creates a two-subnet network as follows.

Network address (24 bits)	Subnet number (1 bit)	Extended network	Host address range
11000000 10101000 00000001	0	192.168.1.0	192.168.1.1 - 192.168.1.127
11000000 10101000 00000001	1	192.168.1.128	192.168.1.129 - 192.168.1.255

For every additional bit set to '1' in the mask, another bit becomes available in the subnet number to index additional subnets. A two-bit subnet number can support up to four subnets, a three-bit number supports up to eight subnets, and so on.

Private Networks and Subnets

As mentioned earlier in this tutorial, the governing bodies that administer Internet Protocol have reserved certain networks for internal uses. In general, intranets utilizing these networks gain more control over managing their IP configuration and Internet access. The default subnet masks associated with these private networks are listed below.

Network address range	Default mask
10.0.0.0 - 10.255.255.255	255.0.0.0
172.16.0.0 - 172.31.255.255	255.240.0.0
192.168.0.0 - 192.168.255.255	255.255.0.0

Consult RFC 1918 for more details about these special networks.

Subnetting Review

Subnetting allows network administrators some flexibility in defining relationships among network hosts. Hosts on different subnets can only "talk" to each other through specialized network gateway devices like routers. The ability to filter traffic between subnets can make more bandwidth available to applications and can limit access in desirable ways.

CIDR Notation and IP Tutorial

CIDR stands for Classless Inter-Domain Routing. CIDR was developed in the 1990s as a standard scheme for routing network traffic across the Internet.

Why Use CIDR?

Before CIDR technology was developed, Internet routers managed network traffic based on the class of IP addresses. In this system, the value of an IP address determines its subnetwork for the purposes of routing.

CIDR is an alternative to traditional IP subnetting that organizes IP addresses into subnetworks independent of the value of the addresses themselves. CIDR is also known as supernetting as it effectively allows multiple subnets to be grouped together for network routing.

CIDR Notation

CIDR specifies an IP address range using a combination of an IP address and its associated network mask.

CIDR notation uses the following format -

xxx.xxx.xxx.xxx/n

where n is the number of (leftmost) '1' bits in the mask. For example,

192.168.12.0/23

applies the network mask 255.255.254.0 to the 192.168 network, starting at 192.168.12.0. This notation represents the address range 192.168.12.0 - 192.168.13.255. Compared to traditional class-based networking, 192.168.12.0/23 represents an aggregation of the two Class C subnets 192.168.12.0 and 192.168.13.0 each having a subnet mask of 255.255.255.0. In other words,

192.168.12.0/23 = 192.168.12.0/24 + 192.168.13.0/24

Additionally, CIDR supports Internet address allocation and message routing independent of the traditional class of a given IP address range. For example,

10.4.12.0/22

represents the address range 10.4.12.0 - 10.4.15.255 (network mask 255.255.252.0). This allocates the equivalent of four Class C networks within the much larger Class A space.

You will sometimes see CIDR notation used even for non-CIDR networks. In non-CIDR IP subnetting, however, the value of n is restricted to either 8 (Class A), 16 (Class B) or 24 (Class C). Examples:

10.0.0.0/8

172.16.0.0/16

192.168.3.0/24

How CIDR Works

CIDR implementations require certain support be embedded within the network routing protocols. When first implemented on the Internet, the core routing protocols like BGP (Border Gateway Protocol) and OSPF (Open Shortest Path First) were updated to support CIDR. Obsolete or less popular routing protocols may not support CIDR.

CIDR aggregation requires the network segments involved to be contiguous (numerically adjacent) in the address space. CIDR cannot, for example, aggregate 192.168.12.0 and 192.168.15.0 into a single route unless the intermediate .13 and .14 address ranges are included (i.e., the 192.168.12/22 network).

Internet WAN or backbone routers (those that manage traffic between Internet Service Providers) all generally support CIDR to achieve the goal of conserving IP address space. Mainstream consumer routers often do not support CIDR, therefore private networks (including home networks) and even small public networks (LANs) often do not employ it.

CIDR and IPv6

IPv6 utilizes CIDR routing technology and CIDR notation in the same way as IPv4. IPv6 was designed for fully classless addressing.