IP Addressing

Understating IP addressing

The Internet continues to grow at a phenomenal rate. This is reflected in the tremendous popularity of the World Wide Web (WWW), the opportunities that businesses see in reaching customers from virtual storefronts, and the emergence of new ways of doing business. It is clear that expanding business and public awareness will continue to increase demand for access to resources on the Internet.

Internet Scaling Problems

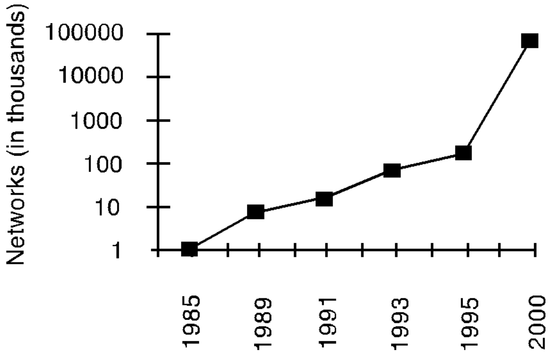
Over the past few years, the Internet has experienced two major scaling issues as it has struggled to provide continuous and uninterrupted growth:

- The eventual exhaustion of IP version 4 (IPv4) address space
- The need to route traffic between the ever increasing number of networks that comprise the Internet

The first problem is concerned with the eventual depletion of the IP address space. IPv4 defines a 32-bit address which means that there are only 232 (4,294,967,296) IPv4 addresses available. As the Internet continues to grow, this finite number of IP addresses will eventually be exhausted.

The address shortage problem is aggravated by the fact that portions of the IP address space have not been efficiently allocated. Also, the traditional model of classful addressing does not allow the address space to be used to its maximum potential. The Address Lifetime Expectancy (ALE) Working Group of the Internet Engineering Task Force (IETF) has expressed concerns that if the current address allocation policies are not modified, the Internet will experience a near to medium term exhaustion of its unallocated address pool. If the Internet’s address supply problem is not solved, new users may be unable to connect to the global Internet. More than half of all possible IPv4 addresses have been assigned to ISPs, corporations, and government agencies, but only an Estimated 69 million addresses are actually in use.

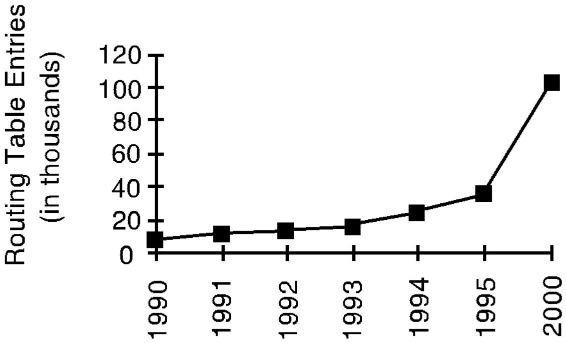
FIGURE 1. Network Number Growth



The second problem is caused by the rapid growth in the size of the

Internet routing tables. Internet backbone routers are required to maintain complete routing information for the Internet. Over recent years, routing tables have experienced exponential growth as increasing numbers of organizations connect to the Internet. In December 1990 there were 2,190 routes, in December 1995 there were more than 30,000 routes, and in December 2000 more than 100,000 routes.

FIGURE 2. Growth of Internet Routing Tables



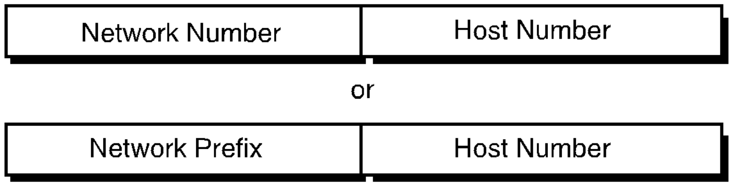
Unfortunately, the routing problem cannot be solved by simply installing more router memory and increasing the size of the routing tables. Other factors related to the capacity problem include the growing demand for CPU horsepower to compute routing table/topology changes, the increasingly dynamic nature of WWW connections and their effect on router forwarding caches, and the sheer volume of information that needs to be managed by people and machines. If the number of entries in the global routing table is allowed to increase without bounds, core routers will be forced to drop routes and portions of the Internet will become unreachable.

The long-term solution to these problems can be found in the widespread deployment of IP Next Generation (IPng or IPv6). Currently, IPv6 is being tested and implemented on the 6Bone network, which is an informal collaborative project covering North America, Europe, and Japan. 6Bone supports the routing of IPv6 packets, since that function has not yet been integrated into many production routers. Until IPv6 can be deployed worldwide, IPv4 patches will need to be used and modified to continue to provide the universal connectivity users have come to expect.

Classful IP Addressing

When IP was first standardized in September 1981, the specification required that each system attached to an IP-based Internet be assigned a unique, 32-bit Internet address value. Systems that have interfaces to more than one network require a unique IP address for each network interface. The first part of an Internet address identifies the network on which the host resides, while the second part identifies the particular host on the given network. This creates the two-level addressing hierarchy that is illustrated in Figure 3.

FIGURE 3. Two-Level Internet Address Structure

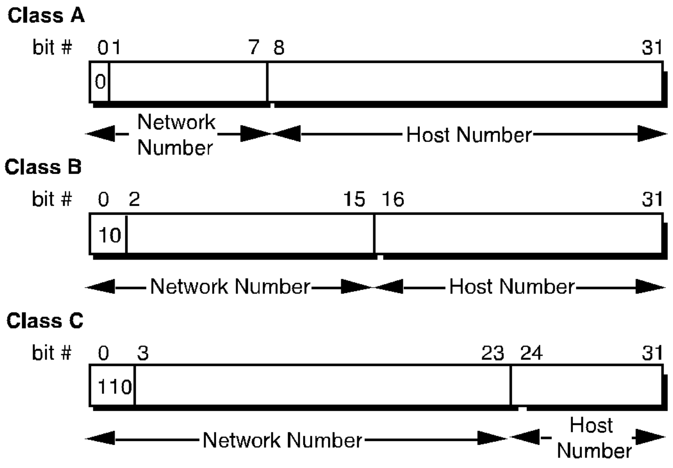


In recent years, the network number field has been referred to as the network prefix because the leading portion of each IP address identifies the network number. All hosts on a given network share the same network prefix but must have a unique host number. Similarly, any two hosts on different networks must have different network prefixes but may have the same host number.

Primary Address Classes

To provide the flexibility required to support networks of varying sizes, the Internet designers decided that the IP address space should be divided into three address classes-Class A, Class B, and Class C. This is often referred to as classful addressing. Each class fixes the boundary between the network prefix and the host number at a different point within the 32-bit address. The formats of the fundamental address classes are illustrated in Figure 4.

FIGURE 4. Principle Classful IP Address Formats



One of the fundamental features of classful IP addressing is that each address contains a self-encoding key that identifies the dividing point between the network prefix and the host number. For example, if the first two bits of an IP address are 1-0, the dividing point falls between the 15th and 16th bits. This simplified the routing system during the early years of the Internet because the original routing protocols did not supply a deciphering key or mask with each route to identify the length of the network prefix.

Class A Networks (/8 Prefixes)

Each Class A network address has an 8-bit network prefix, with the highest order bit set to 0 (zero) and a 7-bit network number, followed by a 24-bit host number. Today, Class A networks are referred to as "/8s" (pronounced "slash eight" or just "eights") since they have an 8-

bit network prefix.

A maximum of 126 (27 -2) /8 networks can be defined. The calculation subtracts two because the /8 network 0.0.0.0 is reserved for use as the default route and the /8 network 127.0.0.0 (also written 127/8 or 127.0.0.0/8) is reserved for the “loopback” function. Each /8 supports a maximum of 224 -2 (16,777,214) hosts per network. The host calculation subtracts two because the all-0s (all zeros or “this network”) and all-1s (all ones or “broadcast”) host numbers may not be assigned to individual hosts.

Since the /8 address block contains 231 (2,147,483,648) individual addresses and the IPv4 address space contains a maximum of 232 (4,294,967,296) addresses, the /8 address space is 50 percent of the total IPv4 unicast address space.

Class B Networks (/16 Prefixes)

Each Class B network address has a 16-bit network prefix, with the two highest order bits set to 1-0 and a 14-bit network number, followed by a 16-bit host number. Class B networks are now referred to as “/16s” since they have a 16-bit network prefix.

A maximum of 16,384 (214) /16 networks can be defined with up to 65,534 (216-2) hosts per network. Since the entire /16 address block contains 230 (1,073,741,824) addresses, it represents 25 percent of the total IPv4 unicast address space.

Class C Networks (/24 Prefixes)

Each Class C network address has a 24-bit network prefix, with the three highest order bits set to 1-1-0 and a 21-bit network number, followed by an 8-bit host number. Class C networks are now referred to as “/24s” since they have a 24-bit network prefix.

A maximum of 2,097,152 (221) /24 networks can be defined with up to 254 (28-2) hosts per network. Since the entire /24 address block contains 229 (536,870,912) addresses, it represents 12.5 percent (or oneeighth) of the total IPv4 unicast address space.

Other Classes

In addition to the three most popular classes, there are two additional classes. Class D addresses have their leading four bits set to 1-1-1-0 and are used to support IP Multicasting. Class E addresses have their leading four bits set to 1-1-1-1 and are reserved for experimental use.

Dotted-Decimal Notation

To make Internet addresses easier for people to read and write, IP addresses are often expressed as four decimal numbers, each separated by a dot. This format is called “dotted-decimal notation.”

Dotted-decimal notation divides the 32-bit Internet address into four 8-bit fields and specifies the value of each field independently as a decimal number with the fields separated by dots. Figure 5 shows how a typical /16 (Class B) Internet address can be expressed in dotted-decimal notation.

FIGURE 5. Dotted Decimal Notation

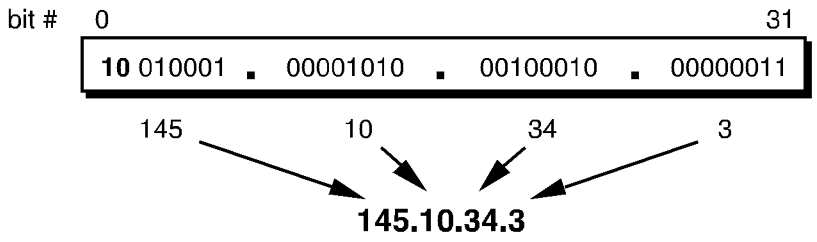


Table 1 displays the range of dotted-decimal values that can be assigned to each of the three principle address classes. The “xxx” represents the host number field of the address that is assigned by the local network Administrator.

TABLE 1. Dotted Decimal Ranges for Each Address Class

Address Class	Dotted-Decimal Notation Ranges
A (/8 prefixes)	1.xxx.xxx.xxx through 126.xxx.xxx.xxx
B (/16 prefixes)	128.0.xxx.xxx through 191.255.xxx.xxx
C (/24 prefixes)	192.0.0.xxx through 223.255.255.xxx

Unforeseen Limitations to Classful Addressing

The original Internet designers never envisioned that the Internet would grow into what it has become today. Many of the problems that the Internet is facing today can be traced back to the early decisions That were made during its formative years.

• During the early days of the Internet, the seemingly unlimited address space allowed IP addresses to be allocated to an organization based on its request rather than its actual need. As a result, addresses were freely assigned to those who asked for them without concerns about the eventual depletion of the IP address space.

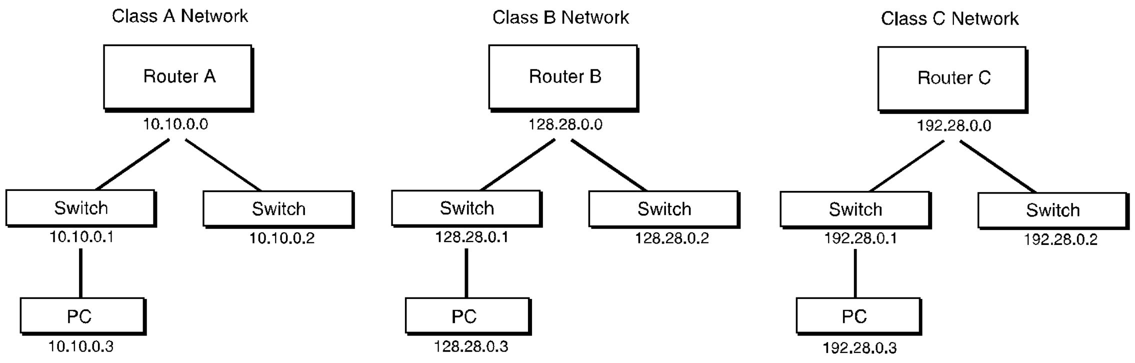
• The decision to standardize on a 32-bit address space meant that there were only 232 (4,294,967,296) IPv4 addresses available. A decision to support a slightly larger address space would have exponentially increased the number of addresses thus eliminating the current address shortage problem.

• The classful A, B, and C octet boundaries were easy to understand and implement, but they did not foster the efficient allocation of a finite address space. Problems resulted from the lack of a network class that was designed to support medium-sized organizations. For example, a /24, which supports 254 hosts, is too small while a /16, which supports 65,534 hosts, is too large. In the past, sites with several hundred hosts were assigned a single /16 address instead of two /24 addresses. This resulted in a premature depletion of the /16 network address space. Now the only readily available addresses for

medium-sized organizations are /24s, which have the potentially negative impact of increasing the size of the global Internet's routing table.
Figure 6 shows basic class A, B, and C networks.

The subsequent history of Internet addressing involved a series of steps that overcame these addressing issues and supported the growth of the global Internet

FIGURE 6. Basic Class A, B, and C Networks

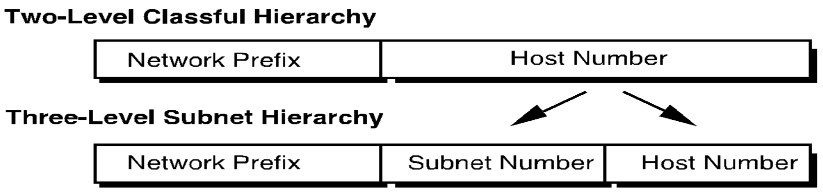


Subnetting

In 1985, RFC 950 defined a standard procedure to support the subnetting, or division, of a single Class A, B, or C network number into smaller pieces. Subnetting was introduced to overcome some of the problems that parts of the Internet were beginning to experience with the classful two-level addressing hierarchy, such as:
- Internet routing tables were beginning to grow.
- Local administrators had to request another network number from the Internet before a new network could be installed at their site.

Both of these problems were attacked by adding another level of hierarchy to the IP addressing structure. Instead of the classful two-level hierarchy, subnetting supports a three-level hierarchy. Figure 7 illustrates the basic idea of subnetting, which is to divide the standard classful host number field into two parts-the subnet number and the host number on that subnet.

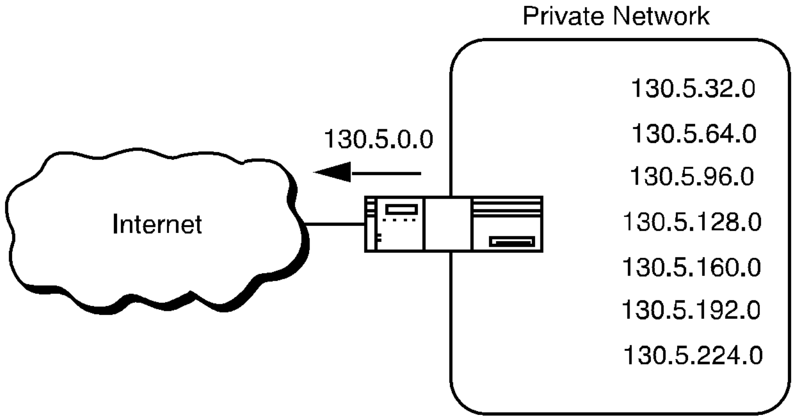
FIGURE 7. Subnet Address Hierarchy



Subnetting attacked the expanding routing table problem by ensuring that the subnet structure of a network is never visible outside of the organization's private network. The route from the Internet to any subnet of a given IP address is the same, no matter which subnet the destination host is on. This is because all subnets of a given network number use the same network prefix but different subnet numbers. The routers within the private organization need to differentiate between the individual subnets, but as far as the Internet routers are concerned, all of the subnets in the organization are collected into a single routing table entry. This allows the local administrator to introduce arbitrary complexity into the private network without affecting the size of the Internet's routing tables.

Subnetting overcame the registered number issue by assigning each organization one (or at most a few) network numbers from the IPv4 address space. The organization was then free to assign a distinct subnetwork number for each of its internal networks. This allowed the organization to deploy additional subnets without obtaining a new network number from the Internet.

FIGURE 8. Subnetting the Routing Requirements of the Internet



In Figure 8, a site with several logical networks uses subnet addressing with a single /16 (Class B) network address. The router accepts all traffic from the Internet addressed to network 130.5.0.0, and forwards traffic to the interior subnetworks based on the third octet of the classful address. The deployment of subnetting within the private network provides several benefits:

- The size of the global Internet routing table does not grow because the site administrator does not need to obtain additional address space and the routing advertisements for all of the subnets are combined into a single routing table entry.

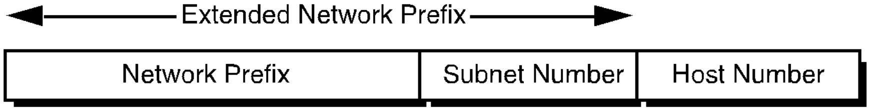
- The local administrator has the flexibility to deploy additional subnets without obtaining a new network number from the Internet.

- Route flapping (that is, the rapid changing of routes) within the private network does not affect the Internet routing table since Internet routers do not know about the reachability of the individual subnetsthey just know about the reachability of the parent network number.

Extended Network Prefix

Internet routers use only the network prefix of the destination address to route traffic to a subnetted environment. Routers within the subnetted environment use the extended network prefix to route traffic between the individual subnets. The extended network prefix is composed of the classful network prefix and the subnet number.

FIGURE 9. Extended Network Prefix



The extended network prefix has traditionally been identified by the subnet mask. For example, if an administrator has the /16 address of 130.5.0.0 and wants to use the entire third octet to represent the subnet number, the administrator must specify a subnet mask of 255.255.255.0. The bits in the subnet mask and the Internet address have a one to one correspondence. The bits of the subnet mask are set to 1 (one) if the system examining the address should treat the corresponding bit in the IP address as part of the extended network prefix. The bits in the mask are set to 0 (zero) if the system should treat the bit as part of the host number. This numbering is illustrated in Figure 10.

FIGURE 10. Subnet Mask

```
                                             ¦  Subnet   ¦   Host
                              Network Prefix ¦  Number   ¦  Number
IP Address:   130.5.5.25      10000010.00000101.00000101.00011001
Subnet Mask:  255.255.255.0   11111111.11111111.11111111.00000000
                              ◄──── Extended Network ────►
                                        Prefix
```

The standards describing modern routing protocols often refer to the extended network prefix length rather than the subnet mask. The prefix length is equal to the number of contiguous one-bits in the traditional subnet mask. This means that specifying the network address 130.5.5.25 with a subnet mask of 255.255.255.0 can also be expressed as 130.5.5.25/24. The /<prefix length> notation is more compact and easier to understand than writing out the mask in its traditional dotteddecimal format. This is illustrated in Figure 11.

FIGURE 11. Extended Network Prefix Length

```
130.5.5.25       10000010.00000101.00000101.00011001
255.255.255.0    11111111.11111111.11111111.00000000

                               or

130.5.5.25/24    10000010.00000101.00000101.00011001
                ◄──── 24 bit Extended ────►
                       Network Prefix
```

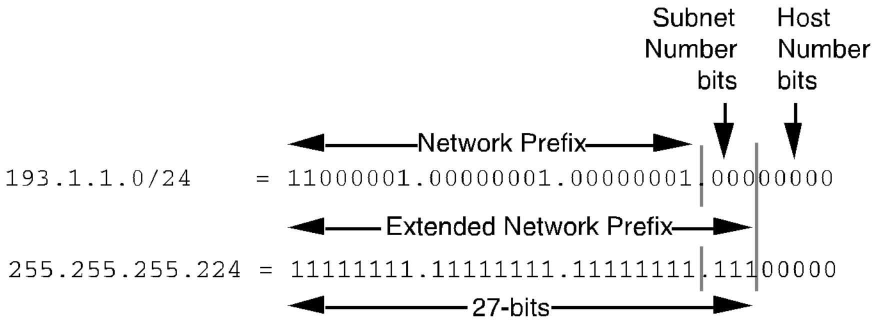
Note that modern routing protocols still carry the subnet mask. None of the Internet standard routing protocols have a 1-byte field in the header that contains the number of bits in the extended network prefix. Each routing protocol is still required to carry the complete four-octet subnet mask.

Defining the Subnet Mask / Extended Prefix Length

The first step in defining the subnet mask is to determine the number of bits required to define the six subnets. Since a network address can only be subnetted along binary boundaries, subnets must be created in blocks of powers of two [2 (21), 4 (22), 8 (23), 16 (24), and so on]. Thus, it is impossible to define an IP address block such that it contains exactly six subnets. For this example, the network administrator must define a block of 8 (23) and have two unused subnets that can be reserved for future growth.

Since 8 = 23, three bits are required to enumerate the eight subnets in the block. In this example, the organization is subnetting a /24 so it will need three more bits, or a /27, as the extended network prefix. A 27-bit extended network prefix can be expressed in dotted-decimal notation as 255.255.255.224. This notation is illustrated in Figure 12.

FIGURE 12. Example #1-Defining the Subnet Mask/Extended Prefix Length



A 27-bit extended network prefix leaves 5 bits to define host addresses on each subnet. This means that each subnetwork with a 27-bit prefix represents a contiguous block of 25 (32) individual IP addresses. However, since the all-0s and all-1s host addresses cannot be allocated, there are 30 (25-2) assignable host addresses on each subnet.

Defining the Subnet Numbers

The eight subnets will be numbered 0 through 7. Throughout the remainder of this paper, the XXX notation indicates the binary representation Of the number. The 3-bit binary representation of the decimal values 0 through 7 are: 0 (000), 1 (001), 2 (010), 3 (011), 4 (100), 5 (101), 6 (110), and 7 (111).

In general, to define Subnet #N, the network administrator places the binary representation of N into the bits of the subnet number field. For example, to define Subnet #6, the network administrator simply places the binary representation of 6 (110) into the 3 bits of the subnet number field.

The eight subnet numbers for this example are listed in the following code sample. The underlined portion of each address identifies the extended network prefix, while the bold digits identify the 3 bits representing the subnet number field:

Base Net: 11000001.00000001.00000001 .00000000 = 193.1.1.0/24

Subnet #0: 11000001.00000001.00000001.**000** 00000 = 193.1.1.0/27

Subnet #1: 11000001.00000001.00000001.**001** 00000 = 193.1.1.32/27

Subnet #2: 11000001.00000001.00000001.**010** 00000 = 193.1.1.64/27

Subnet #3: 11000001.00000001.00000001.**011** 00000 = 193.1.1.96/27

Subnet #4: 11000001.00000001.00000001.**100** 00000 = 193.1.1.128/27

Subnet #5: 11000001.00000001.00000001.**101** 00000 = 193.1.1.160/27

Subnet #6: 11000001.00000001.00000001.**110** 00000 = 193.1.1.192/27

Subnet #7: 11000001.00000001.00000001.**111** 00000 = 193.1.1.224/27

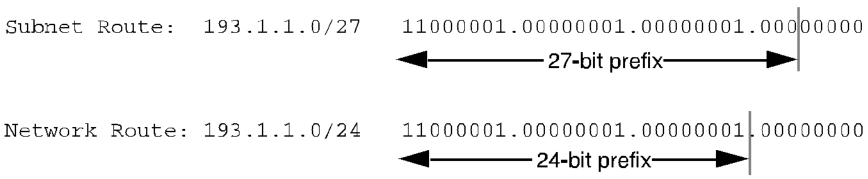
An easy way to verify that the subnets are correct is to ensure that they are all multiples of the Subnet #1 addresses. In this example, all subnets are multiples of 32: 0, 32, 64, 96, and so on.

The All-0s Subnet and All-1s Subnet

When subnetting was first defined in RFC 950, it prohibited the use of the all-0s and the all-1s subnets. The reason for this restriction was to eliminate situations that could potentially confuse a classful router. Today a router can be both classless and classful at the same time-it could be running RIP-1 (classful protocol) and BGP-4 (Border Gateway Protocol Version 4-a classless protocol) at the same time.

With respect to the all-0s subnet, a router requires that each routing table update include the route/<prefix length> pair to differentiate between a route to the all-0s subnet and a route to the entire network. For example, when using RIP-1which does not supply a mask or prefix length with each route, the routing advertisements for subnet 193.1.1.0/27 and for network 193.1.1.0/24 are identical-193.1.1.0. Without somehow knowing the prefix length or mask, a router cannot tell the difference between a route to the all-0s subnet and the route to the entire network. This example is illustrated in Figure 13.

FIGURE 13. Differentiating Between a Route to the All-0s Subnet and the Entire Network



IP Address

An **IP address** (**Internet Protocol address**) is a unique address that certain electronic devices currently use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (**IP**)—in simpler terms, a computer address. Any participating network device—including routers, switches, computers, infrastructure servers (e.g., NTP, DNS, DHCP, SNMP, etc.), printers, Internet fax machines, and some telephones—can have its own address that is unique within the scope of the specific network. Some IP addresses are intended to be unique within the scope of the global Internet, while others need to be unique only within the scope of an enterprise.

The IP address acts as a **locator** for one IP device to find another and interact with it. It is not intended, however, to act as an **identifier** that always uniquely identifies a particular device. In current practice, an IP address is not always a unique identifier, due to technologies such as **dynamic assignment** and network address translation.

IP addresses are managed and created by the Internet Assigned Numbers Authority (IANA). The IANA generally allocates super-blocks to Regional Internet Registries, who in turn allocate smaller blocks to Internet service providers and enterprises.

IP versions

The Internet Protocol (IP) has two versions currently in use (see IP version history for details). Each version has its own definition of an IP address. Because of its prevalence, "IP address" typically refers to those defined by IPv4.

IPv4 Address Classes

Class Address Ranges

Class A - 1.0.0.0 to 126.0.0.0
Class B - 128.0.0.0 to 191.255.0.0
Class C - 192.0.1.0 to 223.255.255.0

Class D* - 224.0.0.0 to 239.255.255.255
Class E* - 240.0.0.0 to 255.255.255.255

Class A, Class B, and Class C are the three classes of addresses used on IP networks in common practice. Class D addresses are reserved for multicast. Class E addresses are simply reserved, meaning they should not be used on IP networks (used on a limited basis by some research organizations for experimental purposes).

Reserved Address Ranges

Address ranges below are reserved by IANA for private intranets, and not routable to the Internet. For additional information, see RFC 1918.

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

IPv4 only uses 32-bit (4-byte) addresses, which limits the address space to 4,294,967,296 (232) possible unique addresses. However, many are reserved for special purposes, such as private networks (~18 million addresses) or multicast addresses (~270 million addresses). This reduces the number of addresses that can be allocated as public Internet addresses, and as the number of addresses available is consumed, an IPv4 address shortage appears to be inevitable in the long run. This limitation has helped stimulate the push towards IPv6, which is currently in the early stages of deployment and is currently the only contender to replace IPv4.

IPv4 addresses are usually represented in dotted-decimal notation (four numbers, each ranging from 0 to 255, separated by dots, e.g. 147.132.42.18). Each range from 0 to 255 can be represented by 8 bits, and is therefore called an octet. It is possible, although less common, to write IPv4 addresses in binary or hexadecimal. When converting, each octet is treated as a separate number. (So 255.255.0.0 in dot-decimal would be FF.FF.00.00 in hexadecimal.)

Class	Range of first octet	Network ID	Host ID	Possible number of networks	Possible number of hosts
A	1 - 126	a	b.c.d	126 = (2^7 - 2)	16,777,214 = (2^{24} - 2)
B	128 - 191	a.b	c.d	16,384 = (2^{14})	65,534 = (2^{16} - 2)
C	192 - 223	a.b.c	d	2,097,151 = (2^{21} - 1)	254 = (2^8 - 2)

Some first-octet values have special meanings:

- First octet 127 represents the local computer, regardless of what network it is really in. This is useful when testing internal operations.
- First octet 224 and above are reserved for special purposes such as multicasting.

Octets 0 and 255 are not acceptable values in some situations, but 0 can be used as the second and/or third octet (e.g. 10.2.0.100).

A class A network does not necessarily consist of 16 million machines on a single network, which would excessively burden most network technologies and their administrators. Instead, a large company is assigned a class A network, and segregates it further into smaller sub-nets using Classless Inter-Domain Routing. However, the class labels are still commonly used as broad descriptors

IPv4 private addresses

Machines not connected to the outside world (e.g. factory machines that communicate with each other via TCP/IP) need not have globally-unique IP addresses. Three ranges of IPv4 addresses for private networks, one per class, were standardized by RFC 1918; these addresses will not be routed, and thus need not be coordinated with any IP address registrars.

IANA Reserved Private Network Ranges	Class	Start of range	End of range

The 24-bit Block	A	10.0.0.0	10.255.255.255
The 20-bit Block	B	172.16.0.0	172.31.255.255
The 16-bit Block	C	192.168.0.0	192.168.255.255

Each block is not necessarily one single network, although it is possible. Typically the network administrator will divide a block into subnets; for example, many home routers automatically use a default address range of 192.168.0.0 - 192.168.0.255 (192.168.0.0/24).

IP version 6 addresses

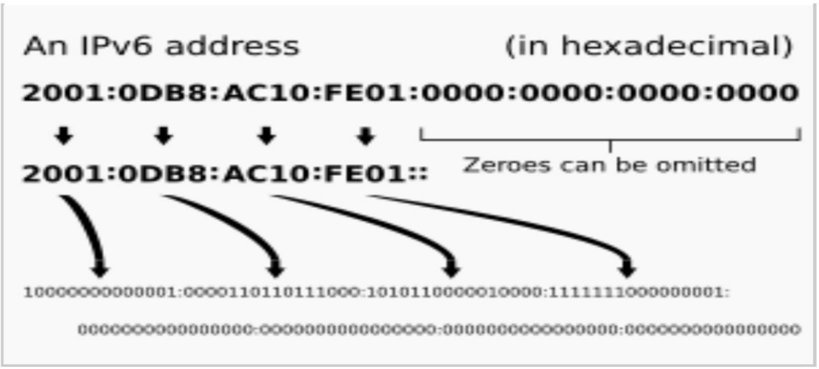
IPv6 is a new standard protocol intended to replace IPv4 for the Internet. Addresses are 128 bits (16 bytes) wide, which, even with a generous assignment of netblocks, will more than suffice for the foreseeable future. In theory, there would be exactly 2^{128}, or about 3.403×10^{38} unique host interface addresses. Further, this large address space will be sparsely populated, which makes it possible to again encode more routing information into the addresses themselves.

Example: 2001:0db8:85a3:08d3:1319:8a2e:0370:7334

Writing for *Technology Review* in 2004, Simson Garfinkel wrote notes that there will exist "roughly 5,000 addresses for every square micrometer of the Earth's surface".[1] This enormous magnitude of available IP addresses will be sufficiently large for the indefinite future, even though mobile phones, cars and all types of personal devices are coming to rely on the Internet for everyday purposes.

The above source, however, involves a common misperception about the IPv6 architecture. Its large address space is not intended to provide unique addresses for every possible point. Rather, the addressing architecture is such that it allows large blocks to be assigned for specific purposes and, where appropriate, aggregated for providing routing. With a large address space, there is not the need to have complex address conservation methods as used in classless inter-domain routing (CIDR).

Windows Vista, Apple Computer's Mac OS X, and an increasing range of Linux distributions include native support for the protocol, but it is not yet widely deployed elsewhere.



An illustration of an IP address (version 6), in hexadecimal and binary.

IP version 6 private addresses

Just as there are addresses for private, or internal networks in IPv4 (one example being the 192.168.0.0 - 192.168.255.255 range), there are blocks of addresses set aside in IPv6 for private addresses. Addresses starting with FE80: are called link-local addresses and are routable only on your local link area. This means that if several hosts connect to each other through a hub or switch then they would communicate through their link-local IPv6 address.

Early designs specified an address range used for "private" addressing, with prefix FEC0. These are called site-local addresses (SLA) and are routable within a particular site, analogously to IPv4 private addresses. Site-local addresses, however, have been deprecated by the IETF, since they create the same problem that does the existing IPv4 private address space With that private address space, when two sites need to communicate, they may have duplicate addresses that "combine". In the IPv6 architecture, the preferred method is to have unique addresses, in a range not routable on the Internet, issued to organizations (e.g., enterprises).

The preferred alternatives to site-local addresses are centrally assigned unique local unicast addresses (ULA). In current proposals, they will start with the prefix FC00.

Neither ULA nor SLA nor link-local address ranges are routable over the internet.

IP address subnetting

Both IPv4 and IPv6 addresses utilize subnetting, or dividing the IP address into two parts: the *network address* and the *host address*. By using a subnet mask, the computer can determine where to split the IP address

Static and dynamic IP addresses

When a computer uses the same IP address every time it connects to the network, it is known as a *Static IP address*. In contrast, in situations when the computer's IP address changes frequently (such as when a user logs on to a network through dialup or through shared residential cable) it is called a *Dynamic IP address*

Method of assignation

Static IP addresses are manually assigned to a computer by an administrator. The exact procedure varies according to platform. This contrasts with dynamic IP addresses, which is assigned either randomly (by the computer itself, as in Zeroconf), or arbitrarily assigned by a server using Dynamic Host Configuration Protocol (DHCP). Even though IP addresses assigned using DHCP may stay the same for long periods of time, they can generally change. In some cases, a network administrator may implement dynamically assigned static IP addresses. In this case, a DHCP server is used, but it is specifically configured to always assign the same IP address to a particular computer, and never to assign that IP address to another computer. This allows static IP addresses to be configured in one place, without having to specifically configure each computer on the network in a different way.

In the absence of both an administrator (to assign a static IP address) and a DHCP server, the operating system may still assign itself a dynamic IP address using Zeroconf. These IP addresses are known as link-local addresses. For IPv4, link-local addresses are in the 169.254.0.0/16 address range.

Uses of dynamic addressing

Dynamic IP Addresses are most frequently assigned on LANs and broadband networks by Dynamic Host Configuration Protocol (DHCP) servers. They are used because it avoids the administrative burden of assigning specific static addresses to each device on a network. It also allows many devices to share limited address space on a network if only some of them will be online at a particular time. In most current desktop operating systems, dynamic IP configuration is enabled by default so that a user does not need to manually enter any settings to connect to a network with a DHCP server. DHCP is not the only technology used to assigning dynamic IP addresses. Dialup and some broadband networks use dynamic address features of the Point-to-Point Protocol.

Uses of static addressing

Static addressing is essential in some infrastructure situations, such as finding the Domain Name Service directory host that will translate domain names to numbers (IP addresses). Static addresses are also convenient, but not absolutely necessary, to locate servers inside an enterprise. An address obtained from a DNS server comes with a time to live, or caching time, after which it should be looked up to confirm that it has not changed. Even static IP addresses do change as a result of network administration,

Modifications to IP addressing

IP blocking and firewalls

Firewalls are common on today's Internet. For increased network security, they allow or deny access to their private network based on the public IP of the client. Whether using a blacklist or a whitelist, the IP address that is blocked is the perceived public IP address of the client, meaning that if the client is using a proxy server or NAT, blocking one IP address might block many individual people.

IP address translation

IP addresses can appear to be shared by multiple client devices either because they are part of a shared hosting web server environment or because an IPv4 network address translator (NAT) or proxy server acts as an intermediary agent on behalf of its customers, in which case the real originating IP addresses might be hidden from the server receiving a request. A common practice is to have a NAT hide a large number of IP addresses in a private network. Only the "outside" interface(s) of the NAT need to have Internet-routable addresses

Most commonly, the NAT device maps TCP or UDP port numbers on the outside to individual private addresses on the inside. Just as there may be site-specific extensions on a telephone number, the port numbers are site-specific extensions to an IP address.

In small home networks, NAT functions are usually performed by a residential gateway device, typically one marketed as a "router". In this scenario, the computers connected to the router would have 'private' IP addresses and the router would have a 'public' address to communicate with the Internet. This type of router allows several computers to share one public IP address.

MAC address

In computer networking a **Media Access Control address** (**MAC address**) or **Ethernet Hardware Address** (**EHA**) or **hardware address** or **adapter address** is a quasi-unique identifier attached to most network adapters (NICs). It is a number that acts like a name for a particular network adapter, so, for example, the network cards (or built-in network adapters) in two different computers will have different names, or MAC addresses, as would an Ethernet adapter and a wireless adapter in the same computer, and as would multiple network cards in a router. However, it is possible to change the MAC address on most of today's hardware, often referred to as MAC spoofing.

Most layer 2 network protocols use one of three numbering spaces managed by the IEEE: **MAC-48**, **EUI-48**, and **EUI-64**, which are designed to be globally unique. Not all communications protocols use MAC addresses, and not all protocols require globally unique identifiers. The IEEE claims trademarks on the names "EUI-48" and "EUI-64" ("EUI" stands for **Extended Unique Identifier**).

MAC addresses, unlike IP addresses and IPX addresses, are not divided into "host" and "network" portions. Therefore, a host cannot determine from the MAC address of another host whether that host is on the same layer 2 network segment as the sending host or a network segment bridged to that network segment.

ARP is commonly used to convert from addresses in a layer 3 protocol such as Internet Protocol (IP) to the layer 2 MAC address. On broadcast networks, such as Ethernet, the MAC address allows each host to be uniquely identified and allows frames to be marked for specific hosts. It thus forms the basis of most of the layer 2 networking upon which higher OSI Layer protocols are built to produce complex, functioning networks.

Notational conventions

The standard (IEEE 802) format for printing MAC-48 addresses in human-readable media is six groups of two hexadecimal digits, separated by hyphens (-) in transmission order, e.g. 01-23-45-67-89-ab. This form is also commonly used for EUI-64. Other conventions include six groups of two separated by colons (:), e.g. 01:23:45:67:89:ab; or three groups of four hexadecimal digits separated by dots (.), e.g. 0123.4567.89ab; again in transmission order

Address details

The original IEEE 802 **MAC address** comes from the original Xerox Ethernet addressing scheme.[1] This 48-bit address space contains potentially 2or 281,474,976,710,656 possible MAC addresses.

All three numbering systems use the same format and differ only in the length of the identifier. Addresses can either be "universally administered addresses" or "locally administered addresses."

A **universally administered address** is uniquely assigned to a device by its manufacturer; these are sometimes called "burned-in addresses" (BIA). The first three octets (in transmission order) identify the organization that issued the identifier and are known as the Organizationally Unique Identifier (OUI). The following three (MAC-48 and EUI-48) or five (EUI-64) octets are assigned by that organization in nearly any manner they please, subject to the constraint of uniqueness. The IEEE expects the MAC-48 space to be exhausted no sooner than the year 2100; EUI-64s are not expected to run out in the foreseeable future.

A **locally administered address** is assigned to a device by a network administrator, overriding the burned-in address. Locally administered addresses do not contain OUIs.

Universally administered and locally administered addresses are distinguished by setting the second least significant bit of the most significant byte of the address. If the bit is 0, the address is universally administered. If it is 1, the address is locally administered. The bit is 0 in all OUIs. For example, 02-00-00-00-00-01. The most significant byte is 02h. The binary is 000000**1**0 and the second least significant bit is 1. Therefore, it is a locally administered address.[2]

If the least significant bit of the most significant byte is set to a 0, the packet is meant to reach only one receiving NIC. This is called unicast. If the least significant bit of the most significant byte is set to a 1, the packet is meant to be sent only once but still reach several NICs. This is called multicast.

MAC-48 and EUI-48 addresses are usually shown in hexadecimal format, with each octet separated by a dash or colon. An example of a MAC-48 address would be "00-08-74-4C-7F-1D". If you cross-reference the first three octets with IEEE's OUI assignments, you can see that this MAC address came from Dell Computer Corp. The last three octets represent the serial number assigned to the adapter by the manufacturer.

The following technologies use the MAC-48 identifier format:

- Ethernet
- 802.11 wireless networks
- Bluetooth

- IEEE 802.5 token ring
- most other IEEE 802 networks
- FDDI
- ATM (switched virtual connections only, as part of an NSAP address)
- Fibre Channel and Serial Attached SCSI (as part of a World Wide Name)