IP Addressing Overview

An IP address uniquely identifies a device on an IP network.

Allocating, recycling, and documenting IP addresses and subnets in a network can get confusing very quickly if you have not laid out an IP addressing plan. A sound plan will help you prepare the network foundation to support additional services such as unified communications, wireless access, and enhanced network security.

IP addressing is a Network Foundation service, which makes it core to the network design. It provides the base for all other network and user services. Without the foundation, it would not be possible to interact with network and user services, from picking up the phone using the phone service to reading email using the email service.

By following recommended IP address management standards, you can avoid:

- Overlapping or duplicate subnets
- Nonsummarization in the network
- Duplicate IP address device assignments
- Wasted IP address space
- Unnecessary complexity

Notes

IP Addressing Basics

IP version 4 (IPv4) addresses, which uniquely identify a device on an IP network, are 32 bits in length and are typically communicated in a format known as dotted decimal.

The 32 binary bits are:

- Divided into a network portion and host portion
- Broken into four octets (1 octet = 8 bits)
- Each octet can be converted to binary.

Consider this IP address, which is presented in dotted decimal: **192.168.15.1**. The address breaks down into the following octets:

- 192
- 168
- 15
- 1

The value in each octet ranges from 0 to 255 decimal, or 00000000–11111111 binary. In binary, the same address is represented as: **11000000.10101000.00001111.00000001**.

IP Address Classes

IP addresses are split up into several different categories, including Class A, B, C, D (Multicast), and E (Reserved).

Address classes are defined, in part, based on the number of bits that make up the network portion of the address, and in turn, on how many are left for the definition of individual host addresses.

- In Class A addresses, the first octet is the network portion.
- In Class B, the first two octets are the network portion.
- In Class C, the first 3 octets are the network portion.

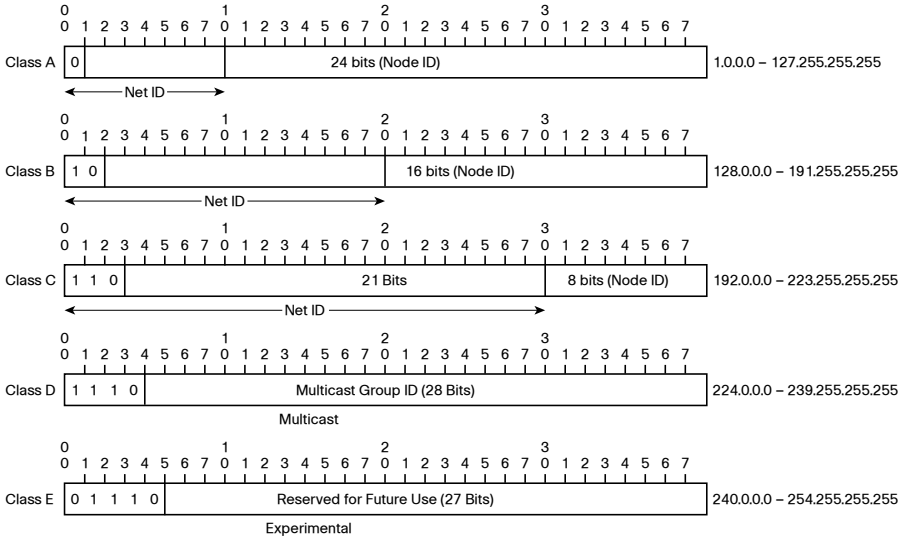
Figure 1 shows how the network and host IDs are different for each class of IP addresses.

Class A has 3 octets for the host portion of the address. Deployed as is, a Class A address represents a very inefficient use of address space, since available Layer 2 technologies cannot easily support this many hosts on a single subnet. Subnetting is utilized to use this address space efficiently.

Tech Tip

IP version 6 (IPv6) is the next generation of IP addressing. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, which provides enough globally unique IP addresses for every networked device on the planet. IPv6 is an important protocol for the future of IP networking. More information can be found at www.cisco.com/go/ipv6.

Figure 1. Classful Addresses



Private IP Addressing

The Internet Assigned Numbers Authority (IANA) has reserved a number of IPv4 network ranges as private. These network addresses are routed in the public Internet as defined in RFC 1918.

These network ranges, known as RFC 1918 spaces, are reserved for organizations that want to build an internal network infrastructure based on TCP/IP without using public IP space.

RFC 1918 space includes the following three blocks of IP address space:

- 10.0.0.0 – 10.255.255.255 (10.0.0.0/8), which allows the greatest flexibility with the equivalent of 255 Class B address spaces to be used as needed.
- 172.16.0.0 – 172.31.255.255 (172.16.0.0/12), which allows for 16 Class B address spaces.
- 192.168.0.0 – 192.168.255.255 (192.168.0.0/16), which allows for one Class B address space.

By universally recognizing these ranges as private and non-routable in the Internet, multiple organizations can use these ranges internally without causing a conflict with public Internet addresses. If an organization attempts to route these networks externally, the traffic is filtered and dropped by the Internet Service Provider.

Since RFC 1918 space is completely private it allows an incredible amount of flexibility when designing a network.

Tech Tip

To allow traffic from hosts that are using private addresses to access Internet hosts using a public address, Network Address Translation (NAT) is required. NAT allows internal hosts to use a few public addresses for Internet access. Public address space is difficult to get and can be expensive so the small pool of public addresses that an ISP allocates must be used sparingly.(Please see NAT in the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide*). Public addresses are also needed if a Demilitarized zone is required

Subnetting

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you can only use one network from your Class A, B, or C network, which is simply unrealistic.

Each data link on a network must have a unique network address, with every host on that link being a member of the same network. If you break a major network (Class A, B, or C) into smaller subnetworks, you can create a network of interconnecting subnetworks. Each data link on this network would then have a unique network/subnetwork ID.

To subnet a network, extend the mask using some of the bits from the host ID portion of the address to create a subnetwork ID. For example: given a network of 192.168.5.0/24, which has a mask of 255.255.255.0, you can create subnets in this manner:

```
192.168.5.0     - 11000000.10101000.00000101.00000000
255.255.255.224 - 11111111.11111111.11111111.11100000
-----------------------------------------[sub]------
```

The address on the left is in dotted decimal notation and the binary representation is on the right. When planning IP subnetting, sometimes it is easier to visualize the different portions of the network address when looking at the binary format. The subnet mask is also represented in dotted decimal and binary. Any address bits that have corresponding mask bits set to 1 represent the network ID. Any address bits that have corresponding mask bits set to 0 represent the host ID.

By extending the mask to be 255.255.255.224, you've taken three bits (indicated by sub) from the original host portion of the address and used them to make subnets. With these three bits, you can create eight subnets. With the remaining five host ID bits, each subnet can have up to 32 host addresses. A single subnet can be split up into eight 32-host subnets. Eight 32-host subnets, however, may not be flexible enough. For example:

```
192.168.5.0 255.255.255.224 address range 0 to 31
192.168.5.32 255.255.255.224 address range 32 to 63
…
192.168.5.224 255.255.255.224 address range 224 to 255
```

Tech Tip

There are two ways to denote subnet masks:

- Since you are using three bits more than the originally specified 255.255.255.0 mask, the mask is now 255.255.255.224.
- The mask can also be denoted as /27 as there are 27 bits that are set in the mask and is denoted with the notation prefix/length. For example: 192.168.5.32/27 denotes the network 192.168.5.32 with a mask of 255.255.255.224.

When appropriate, the prefix/length notation is used to denote the mask throughout the rest of this document.

Variable Length Subnet Masks (VLSMs)

Variable Length Subnet Masks (VLSMs) allow you to use different masks for each subnet, and thereby use address space efficiently. With private address space, it is rarely necessary to shrink below a /24 subnet mask as space is plentiful. Use VLSM to:

- Create a larger subnet of more than 255 host addresses
- Create very small subnets for WAN links
- Configure loopback addresses

VLSM Example

Given the 192.168.5.0/24 network and requirements below, develop a subnetting scheme with the use of VLSM:

- netA: must support 330 hosts
- netB: must support 6 hosts for a point-to-point WAN link supporting Hot Standby Router Protocol (HSRP)
- netC: must support 2 hosts for a T1 circuit to a remote site
- netD: must support a single address for a router loopback

The first step is to determine what mask allows the required number of hosts.

- netA: requires a /23 (255.255.254.0) mask to support 510 hosts
- netB: requires a /29 (255.255.255.248) mask to support 6 hosts
- netC: requires a /30 (255.255.255.252) mask to support 2 hosts
- netD*: requires a /32 (255.255.255.255) mask to support 1 address

*Note: This is a special configuration reserved for loopback addresses.

The easiest way to assign the subnets is to assign the largest first. For example: You can assign in this manner:

- netA: 192.168.5.0/23 address range 5.0 to 6.255
- netB: 192.168.7.0/28 address range 0 to 7
- netC: 192.168.7.8/28 address range 8 to 11
- netD:192.168.7.12/32 address of 12

Reader Tip

For specific information on IP addressing and variable length subnet masks, please reference "IP Addressing and Subnetting for New Users," Document ID: 13788, http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800a67f5.shtml.

Voice Overlay Subnets

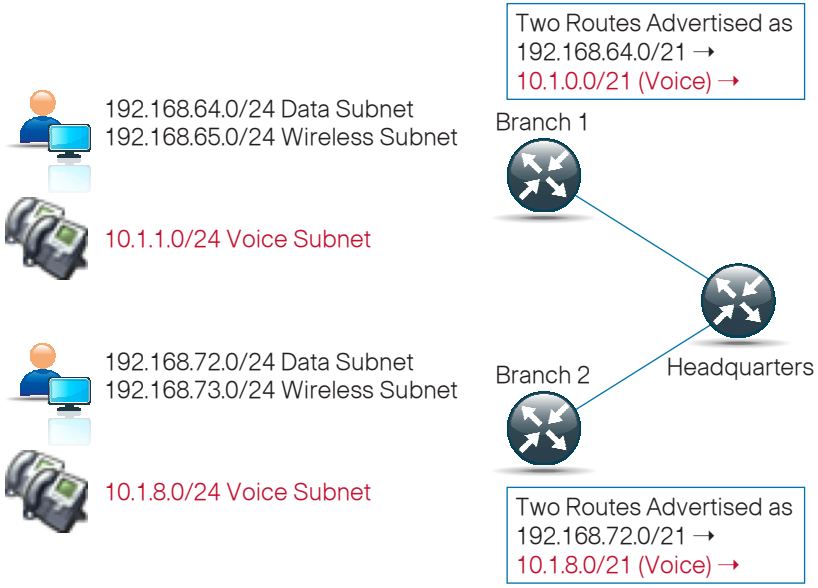
When adding a new service such as unified communications or quality of service, it is very helpful to overlay different private IP addressing on an existing IP addressing scheme. For example:

- All voice could be on its own subnet range from 10.0.0.0 or 172.16.0.0.
- A simple mask covering all 172.16 and 10.0.0.0 addresses could be used to classify voice traffic across all sites.

Such an approach can also help solve scalability issues with an addressing plan that was not designed to accommodate enough subnets and end hosts for each site to support the new service.

For example: Two existing branches have wired and wireless access and would like to add voice. They have reserved all of their 192.168 subnet space. The voice subnet is overlaid in a 10.X.X.X address range highlighted in red in Figure 2.

Figure 2. Voice Overlay Subnets



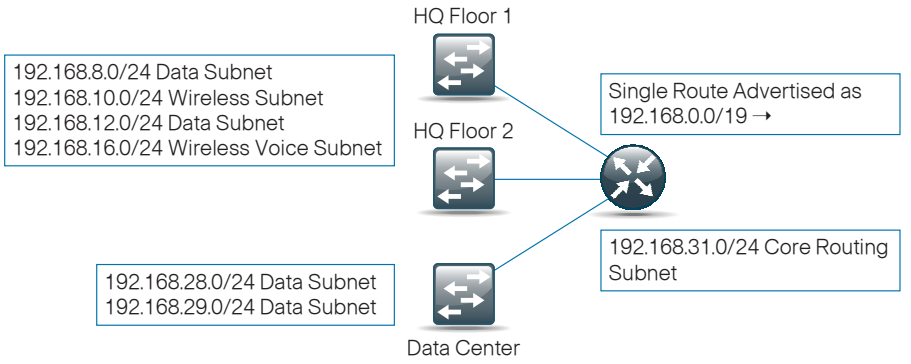
Summarization

Summarizing IP addresses ensures that there are no entries for child routes, which are routes that are created for any combination of the individual IP addresses contained within a summary address, in the routing table. This summarization reduces the size of the table and allows the router to handle more routes.

In a small network, summarization is often not necessary at first. However, as soon as the network starts to expand, it needs to scale. Summarization provides the ability to scale IP address space from a single-site headquarters to an additional remote site location and then include hundreds of remote sites.

An example of summarization from the network headquarters out to the remote site locations is shown in Figure 3. Normal IP routing advertisement would have sent out seven routes in the routing table. With summarization, all seven routes are summarized back to the headquarters as a single route.

Figure 3. IP Summarization at Headquarters



Summarization can be used on all spaces if the addressing is contiguous or specific to a location. If existing IP addressing does not allow for summarization, document it and leave it be while you deploy future IP space that can be summarized.

Tech Tip

Be sure to turn off auto-summarization in the Enhanced Interior Gateway Routing Protocol (EIGRP) if there are noncontiguous IP spaces.

IP Multicast

IP Multicast is a bandwidth conservation technology that reduces traffic and server loads by allowing a single stream of information on the network to be received by thousands of users.

Applications that take advantage of multicast technologies include:

- Video conferencing
- Corporate communications
- Music on hold
- Distance learning
- Distribution of software, stock quotes, and news

IANA has reserved the range of 239.0.0.0/8 as Administratively Scoped addresses for use in private multicast domains. These addresses are similar in nature to the reserved IP unicast ranges (such as 10.0.0.0/8) defined in RFC 1918 and will not be assigned by the IANA to any other group or protocol.

An agency multicast IP addressing plan, just like a unicast addressing plan, needs to be provisioned for the entire network.

Reader Tip

For more information on IP Multicast, please visit www.cisco.com/go/multicast.

Notes