IP Addressing and Subnetting

Requirements

Cisco recommends that you have a basic understanding of binary and decimal numbers.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Additional Information

If definitions are helpful to you, use these vocabulary terms in order to get you started:

- **Address -** The unique number ID assigned to one host or interface in a network.
- **Subnet -** A portion of a network that shares a particular subnet address.
- **Subnet mask -** A 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host.
- **Interface -** A network connection.

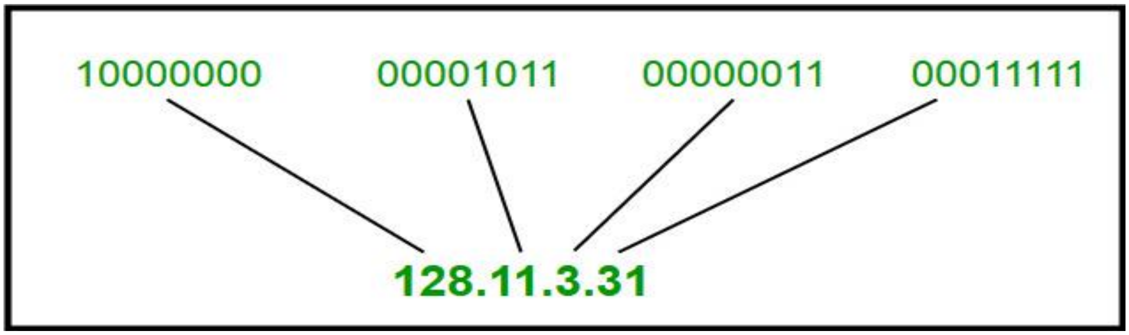
Understand IP Addresses

An IP address is an address used in order to uniquely identify a device on an IP network. The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask.

The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 00000000 - 11111111 binary.

Generally, IP address is written in dotted decimal notation as follows.

Dotted Decimal Notation:



. Some points to be noted about **dotted decimal notation**:

1. The value of any segment (byte) is between 0 and 255 (both included).
2. There are no zeroes preceding the value in any segment (054 is wrong, 54 is correct).

Here is how binary octets convert to decimal: The right most bit, or least significant bit, of an octet holds a value of 20. The bit just to the left of that holds a value of 21. This continues until the left-most bit, or most significant bit, which holds a value of 27. So if all binary bits are a one, the decimal equivalent would be 255 as shown here:

```
  1   1   1   1 1 1 1 1
128  64  32  16 8 4 2 1 (128+64+32+16+8+4+2+1=255)
```

Here is a sample octet conversion when not all of the bits are set to 1.

```
0  1 0 0 0 0 0 1
0 64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65)
```

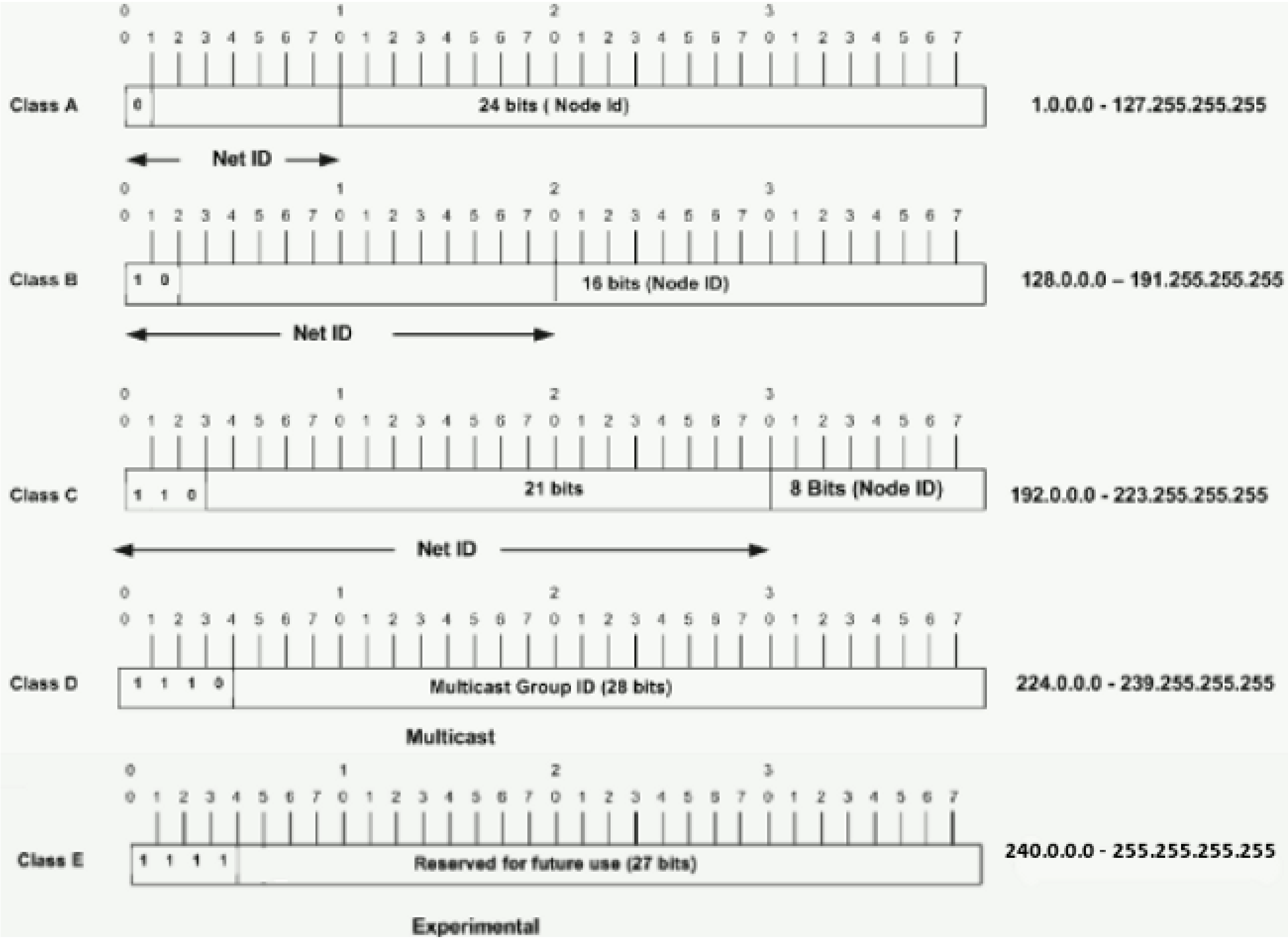
And this sample shows an IP address represented in both binary and decimal.

```
      10.       1.      23.      19 (decimal)
00001010.00000001.00010111.00010011 (binary)
```

These octets are broken down to provide an addressing scheme that can accommodate large and small networks. There are five different classes of networks, A to E. This document focuses on classes A to C, since classes D and E are reserved and discussion of them is beyond the scope of this document.

Given an IP address, its class can be determined from the three high-order bits (the three left-most bits in the first octet). Figure 1 shows the significance in the three high order bits and the range of addresses that fall into each class. For informational purposes, Class D and Class E addresses are also shown.

Figure 1



In a Class A address, the first octet is the network portion, so the Class A example in Figure 1 has a major network address of 1.0.0.0 - 127.255.255.255. Octets 2, 3, and 4 (the next 24 bits) are for the network manager to divide into subnets and hosts as he/she sees fit. Class A addresses are used for networks that have more than 65,536 hosts (actually, up to 16777214 hosts!).

In a Class B address, the first two octets are the network portion, so the Class B example in Figure 1 has a major network address of 128.0.0.0 - 191.255.255.255. Octets 3 and 4 (16 bits) are for local subnets and hosts. Class B addresses are used for networks that have between 256 and 65534 hosts. In a Class C address, the first three octets are the network portion. The Class C example in Figure 1 has a major network address of 192.0.0.0 - 223.255.255.255. Octet 4 (8 bits) is for local subnets and hosts - perfect for networks with less than 254 hosts.

Network Masks

A network mask helps you know which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C networks have default masks, also known as natural masks, as shown here:

```
Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0
```

An IP address on a Class A network that has not been subnetted would have an address/mask pair similar to: 8.20.15.1 255.0.0.0. In order to see how the mask helps you identify the network and node parts of the address, convert the address and mask to binary numbers.

```
8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000
```

Once you have the address and the mask represented in binary, then identification of the network and host ID is easier. Any address bits which have corresponding mask bits set to 1 represent the network ID. Any address bits that have corresponding mask bits set to 0 represent the node ID.

```
8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000
            -----------------------------------
             Net id |      host id

Netid = 00001000 = 8
Hostid = 00010100.00001111.00000001 = 20.15.1
```

Note: Also note that the terms "Class A, Class B" and so on are used in this document in order to help facilitate the understanding of IP addressing and subnetting. These terms are rarely used in the industry anymore because of the introduction of classless interdomain routing (CIDR).

IPv4 addresses 32 bit binary addresses (divided into 4 octets) used by the Internet Protocol (OSI Layer 3) for delivering packet to a device located in same or remote network. MAC address (Hardware address) is a globally unique address which represents the network card and cannot be changed. IPv4 address refers to a logical address, which is a configurable address used to identify which network this host belongs to and also a network specific host number. In other words, an IPv4 address consists of two parts; a network part and a host part.

This can be compared to your home address. A letter addressed to your home address will be delivered to your house because of this logical address. If you move to another house, your address will change, and letters addressed to you will be sent to your new address. But the person who the letter is being delivered to, that is “you”, is still the same.

IPv4 addresses are stored internally as binary numbers but they are represented in decimal numbers because of simplicity.

An example of IPv4 address is 192.168.10.100, which is actually:
11000000.10101000.00001010.01100100.

For Each network, one address is used to represent the network and one address is used for broadcast. Network address is an IPv4 address with all host bits are "0". Broadcast address is an IPv4 address with all host bits are "1".

That means, for a network, the first IPv4 address is the network address and the last IPv4 address is the broadcast address. You cannot configure these addresses for your devices. All the usable IPv4 addresses in any IP network are between network address and broadcast address.

We can use the following equation for find the number of usable IPv4 addresses in a network (We have to use two IPv4 addresses in each network to represent the network id and the broadcast id.)

Number of usable IPv4 addresses = (2^n-2). Where "n" is the number of bits in host part. Many IPv4 addresses are reserved and we cannot use those IPv4 address. There are five IPv4 address Classes and certain special addresses.

Class A IPv4 addresses

"Class A" IPv4 addresses are for very large networks. The left most bit of the left most octet of a "Class A" network is reserved as "0". The first octet of a "Class A" IPv4 address is used to identify the Network and the three remaining octets are used to identify the host in that particular network (**Network**.**Host.Host.Host**).

The 32 bits of a "Class A" IPv4 address can be represented as 0xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx.

The minimum possible value for the leftmost octet in binaries is 00000000 (decimal equivalent is 0) and the maximum possible value for the leftmost octet is 01111111 (decimal equivalent is 127). Therefore for a "Class A" IPv4 address, leftmost octet must have a value between 0-127 (0.X.X.X to 127.X.X.X).

The network 127.0.0.0 is known as loopback network. The IPv4 address 127.0.0.1 is used by the host computer to send a message back to itself. It is commonly used for troubleshooting and network testing.

Computers not connected directly to the Internet need not have globally-unique IPv4 addresses. They need an IPv4 addresses unique to that network only. 10.0.0.0 Network belongs to "Class A" is reserved for private use and can be used inside any organization.

Class B IPv4 addresses

"Class B" IPv4 addresses are used for medium-sized networks. Two left most bits of the left most octet of a "Class B" network is reserved as "10". The first two octets of a "Class B" IPv4 address is used to identify the Network and the remaining two octets are used to identify the host in that particular network (**Network.Network.Host**.**Host**).

The 32 bits of a "Class B" IPv4 address can be represented as
10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx.

The minimum possible value for the leftmost octet in binaries is 10000000 (decimal equivalent is 128) and the maximum possible value for the leftmost octet is 10111111 (decimal equivalent is 191). Therefore for a "Class B" IPv4 address, leftmost octet must have a value between **128-191 (128.X.X.X to 191.X.X.X).**

Network 169.254.0.0 is known as APIPA (Automatic Private IPv4 addresses). APIPA range of IPv4 addresses are used when a client is configured to automatically obtain an IPv4 address from the DHCP server was unable to contact the DHCP server for dynamic IPv4 address. Networks starting from 172.16.0.0 to 172.31.0.0 are reserved for private use.

Class C IPv4 addresses

"Class C" IPv4 addresses are commonly used for small to mid-size businesses. Three left most bits of the left most octet of a "Class C" network is reserved as "110". The first three octets of a "Class C" IPv4 address is used to identify the Network and the remaining one octet is used to identify the host in that particular network (**Network.Network.Networkt**.**Host**).

The 32 bits of a "Class C" IPv4 address can be represented as:
110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx.

The minimum possible value for the leftmost octet in binaries is 11000000 (decimal equivalent is 192) and the maximum possible value for the leftmost octet is 11011111 (decimal equivalent is 223). Therefore for a "Class C" IPv4 address, leftmost octet must have a value between **192-223 (192.X.X.X to 223.X.X.X).**

Networks starting from 192.168.0.0 to 192.168.255.0 are reserved for private use.

Class D IPv4 addresses

Class D IPv4 addresses are known as multicast IPv4 addresses. Multicasting is a technique developed to send packets from one device to many other devices, without any unnecessary packet duplication. In multicasting, one packet is sent from a source and is replicated as needed in the network to reach as many end-users as necessary. You cannot assign these IPv4 addresses to your devices.

Four left most bits of the left most octet of a "Class D" network is reserved as "1110". The other 28 bits are used to identify the group of computers the multicast message is intended for.

The minimum possible value for the left most octet in binaries is 11100000 (decimal equivalent is 224) and the maximum possible value for the leftmost octet is 11101111 (decimal equivalent is 239). Therefore for a "Class D" IPv4 address, leftmost octet must have a value between **224-239 (224.X.X.X to 239.X.X.X).**

Class E IPv4 addresses

Class E is used for experimental purposes only and you cannot assign these IPv4 addresses to your devices. Four left most bits of the left most octet of a "Class E" network is reserved as "1111".

The minimum possible value for the left most octet in binaries is 11110000 (decimal equivalent is 240) and the maximum possible value for the leftmost octet is 11111111 (decimal equivalent is 255). Therefore for a "Class E" IPv4 address, leftmost octet must have a value between **240-255 (240.X.X.X to 255.X.X.X).**

What is Subnet Mask?

An IPv4 address has two components, a "Network" part and a "Host" part. To identify which part of an IPv4 address is the "Network" part and which part of the IPv4 address is "Host" part, we need another identifier, which is known as "Subnet Mask". IPv4 address is a combination of IPv4 address and Subnet mask and the purpose of subnet mask is to identify which part of an IPv4 address is the network part and which part is the host part. Subnet mask is also a 32 bit number where all the bits of the network part are represented as "1" and all the bits of the host part are represented as "0". If we take an example for a Class C network, 192.168.10.0, the address part and the subnet mask can be represented as below.

What is a Network Address?

A network address is used to identify the subnet that a host may be placed on and is used to represent that network. Network Address is the very first address of an IPv4 address block.

For Example, 10.0.0.0 is the network address of all IPv4 addresses starting from 10.0.0.1 to 10.255.255.254, having a subnet mask of 255.0.0.0

What is Limited Broadcast?

IPv4 Address 255.255.255.255 is used to send messages to all devices in the LAN and this IPv4 address is known as limited broadcast IPv4 address. A limited broadcast IPv4 Address can never be a source IPv4 address in an IPv4 datagram.

What is Directed Broadcast?

The host id value containing all 1's in the bit pattern indicates a directed broadcast address. A directed broadcast address can never be a source IPv4 address in an IPv4 datagram. A directed broadcast address will be seen by all nodes on that network. For example, the broadcast id for the network 192.168.10.0 with a subnet mask of 255.255.255.0 will be 192.168.10.255.

What is Default Network?

The IPv4 address of 0.0.0.0 is used for the default network. When a program sends a packet to an address that is not added in the on the computer's routing table, the packet is forwarded to the gateway for 0.0.0.0, which may able to route it to the correct address.

What are Loopback IPv4 Addresses?

IPv4 has a special reserved range of addresses known as IPv4 loopback addresses. Loopback range of IPv4 addresses ranges from 127.0.0.1 to 127.255.255.254. IP datagrams sent by a device to IPv4 loopback addresses not passed down to the data link layer for transmission to other devices. The IP datagrams sent to any address ranging from 127.0.0.1 to 127.255.255.254 are looped back to the source device at network layer.

If the TCP/IP protocol stack is working properly in your device, whenever you ping to any IPv4 loopback addresses, you will get a reply. Most of the operating systems map the IPv4 loopback address 127.0.0.1 with a name "localhost" by adding an entry in "hosts" file.

Understand 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 are only able to use one network from your Class A, B, or C network, which is unrealistic.

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

Any device, or gateway, that connects n networks/subnetworks has n distinct IP addresses, one for each network / subnetwork that it interconnects.

In order to subnet a network, extend the natural mask with some of the bits from the host ID portion of the address in order to create a subnetwork ID. For example, given a Class C network of 204.17.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:

```
204.17.5.0 -      11001100.00010001.00000101.00000000
255.255.255.224 - 11111111.11111111.11111111.11100000
                  --------------------------|sub|----
```

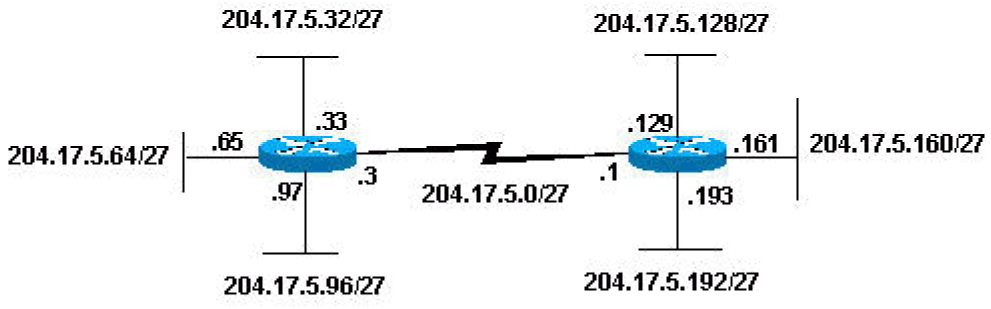
By extending the mask to be 255.255.255.224, you have taken three bits (indicated by "sub") from the original host portion of the address and used them to make subnets. With these three bits, it is possible to create eight subnets. With the remaining five host ID bits, each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device since host ids of all zeros or all ones are not allowed (it is very important to remember this). So, with this in mind, these subnets have been created.

```
204.17.5.0 255.255.255.224      host address range 1 to 30
204.17.5.32 255.255.255.224     host address range 33 to 62
204.17.5.64 255.255.255.224     host address range 65 to 94
204.17.5.96 255.255.255.224     host address range 97 to 126
204.17.5.128 255.255.255.224    host address range 129 to 158
204.17.5.160 255.255.255.224    host address range 161 to 190
204.17.5.192 255.255.255.224    host address range 193 to 222
204.17.5.224 255.255.255.224    host address range 225 to 254
```

Note: There are two ways to denote these masks. First, since you use three bits more than the "natural" Class C mask, you can denote these addresses as having a 3-bit subnet mask. Or, secondly, the mask of 255.255.255.224 can also be denoted as /27 as there are 27 bits that are set in the mask. This second method is used with CIDR. With this method, one of these networks can be described with the notation prefix/length. For example, 204.17.5.32/27 denotes the network 204.17.5.32 255.255.255.224. When appropriate, the prefix/length notation is used to denote the mask throughout the rest of this document.

The network subnetting scheme in this section allows for eight subnets, and the network might appear as:

Figure 2



Notice that each of the routers in Figure 2 is attached to four subnetworks, one subnetwork is common to both routers. Also, each router has an IP address for each subnetwork to which it is attached. Each subnetwork could potentially support up to 30 host addresses.

This brings up an interesting point. The more host bits you use for a subnet mask, the more subnets you have available. However, the more subnets available, the less host addresses available per subnet. For example, a Class C network of 204.17.5.0 and a mask of 255.255.255.224 (/27) allows you to have eight subnets, each with 32 host addresses (30 of which could be assigned to devices). If you use a mask of 255.255.255.240 (/28), the break down is:

```
204.17.5.0 -      11001100.00010001.00000101.00000000
255.255.255.240 - 11111111.11111111.11111111.11110000
                  -------------------------|sub |---
```

Since you now have four bits to make subnets with, you only have four bits left for host addresses. So in this case you can have up to 16 subnets, each of which can have up to 16 host addresses (14 of which can be assigned to devices).

Take a look at how a Class B network might be subnetted. If you have network 172.16.0.0 ,then you know that its natural mask is 255.255.0.0 or 172.16.0.0/16. Extending the mask to anything beyond 255.255.0.0 means you are subnetting. You can quickly see that you have the ability to create a lot more subnets than with the Class C network. If you use a mask of 255.255.248.0 (/21), how many subnets and hosts per subnet does this allow for?

```
172.16.0.0  -   10101100.00010000.00000000.00000000
255.255.248.0 - 11111111.11111111.11111000.00000000
                -----------------| sub |-----------
```

You use five bits from the original host bits for subnets. This allows you to have 32 subnets (2^5). After using the five bits for subnetting, you are left with 11 bits for host addresses. This allows each subnet so have 2048 host addresses (2^{11}), 2046 of which could be assigned to devices.

Note: In the past, there were limitations to the use of a subnet 0 (all subnet bits are set to zero) and all ones subnet (all subnet bits set to one). Some devices would not allow the use of these subnets.

Cisco Systems devices allow the use of these subnets when the **ip subnet zero**command is configured.

Examples

Sample Exercise 1

Now that you have an understanding of subnetting, put this knowledge to use. In this example, you are given two address / mask combinations, written with the prefix/length notation, which have been assigned to two devices. Your task is to determine if these devices are on the same subnet or different subnets. You can use the address and mask of each device in order to determine to which subnet each address belongs.

```
DeviceA: 172.16.17.30/20

DeviceB: 172.16.28.15/20
```

Determine the Subnet for DeviceA:

```
172.16.17.30  -   10101100.00010000.00010001.00011110

255.255.240.0 -   11111111.11111111.11110000.00000000

                  -----------------| sub|------------

Subnet = 10101100.00010000.00010000.00000000 = 172.16.16.0
```

Looking at the address bits that have a corresponding mask bit set to one, and setting all the other address bits to zero (this is equivalent to performing a logical "AND" between the mask and address), shows you to which subnet this address belongs. In this case, DeviceA belongs to subnet 172.16.16.0.

Determine the Subnet for DeviceB:

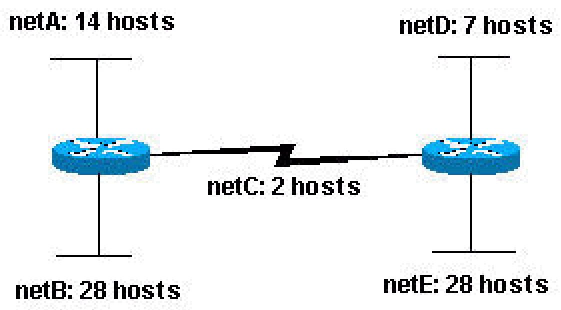
```
172.16.28.15  -   10101100.00010000.00011100.00001111

255.255.240.0 -   11111111.11111111.11110000.00000000

                  -----------------| sub|------------

subnet =          10101100.00010000.00010000.00000000 = 172.16.16.0
```

From these determinations, DeviceA and DeviceB have addresses that are part of the same subnet.

Sample Exercise 2

Given the Class C network of 204.15.5.0/24, subnet the network in order to create the network in Figure 3 with the host requirements shown.

Figure 3



Looking at the network shown in Figure 3, you can see that you are required to create five subnets. The largest subnet must support 28 host addresses. Is this possible with a Class C network? and if so, then how?

You can start by looking at the subnet requirement. In order to create the five needed subnets you would need to use three bits from the Class C host bits. Two bits would only allow you four subnets (2^2).

Since you need three subnet bits, that leaves you with five bits for the host portion of the address. How many hosts does this support? $2^5 = 32$ (30 usable). This meets the requirement.

Therefore you have determined that it is possible to create this network with a Class C network. An example of how you might assign the subnetworks is:

```
netA: 204.15.5.0/27      host address range 1 to 30
netB: 204.15.5.32/27     host address range 33 to 62
netC: 204.15.5.64/27     host address range 65 to 94
netD: 204.15.5.96/27     host address range 97 to 126
netE: 204.15.5.128/27    host address range 129 to 158
```

VLSM Example

In all of the previous examples of subnetting, notice that the same subnet mask was applied for all the subnets. This means that each subnet has the same number of available host addresses. You can need this in some cases, but, in most cases, having the same subnet mask for all subnets ends up wasting address space. For example, in the Sample Exercise 2 section, a class C network was split into eight equal-size subnets; however, each subnet did not utilize all available host addresses, which results in wasted address space. Figure 4 illustrates this wasted address space.

Figure 4

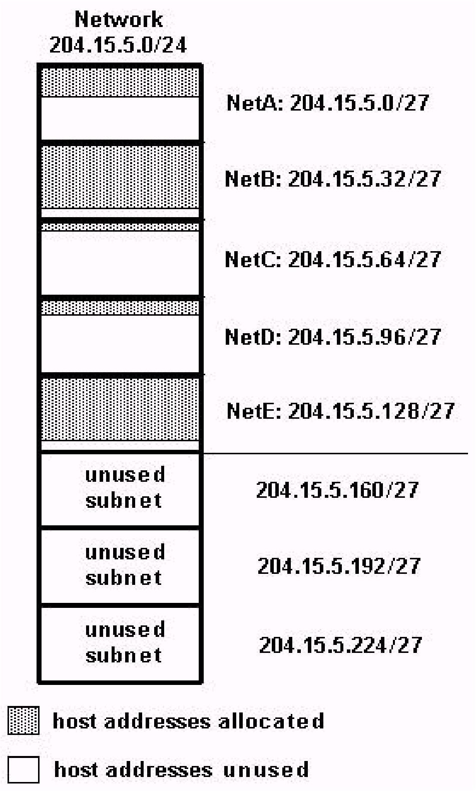


Figure 4 illustrates that of the subnets that are being used, NetA, NetC, and NetD have a lot of unused host address space. It is possible that this was a deliberate design accounting for future growth, but in many cases this is just wasted address space due to the fact that the same subnet mask is used for all the subnets.

Variable Length Subnet Masks (VLSM) allows you to use different masks for each subnet, thereby using address space efficiently.

VLSM Example

Given the same network and requirements as in Sample Exercise 2 develop a subnetting scheme with the use of VLSM, given:

netA: must support 14 hosts

netB: must support 28 hosts

netC: must support 2 hosts

netD: must support 7 hosts

netE: must support 28 host

Determine what mask allows the required number of hosts.

netA: requires a /28 (255.255.255.240) mask to support 14 hosts

netB: requires a /27 (255.255.255.224) mask to support 28 hosts

netC: requires a /30 (255.255.255.252) mask to support 2 hosts

netD*: requires a /28 (255.255.255.240) mask to support 7 hosts

netE: requires a /27 (255.255.255.224) mask to support 28 hosts

* a /29 (255.255.255.248) would only allow 6 usable host addresses

Therefore netD requires a /28 mask.

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

netB: 204.15.5.0/27 host address range 1 to 30

netE: 204.15.5.32/27 host address range 33 to 62

netA: 204.15.5.64/28 host address range 65 to 78

netD: 204.15.5.80/28 host address range 81 to 94

netC: 204.15.5.96/30 host address range 97 to 98

This can be graphically represented as shown in Figure 5:

Figure 5

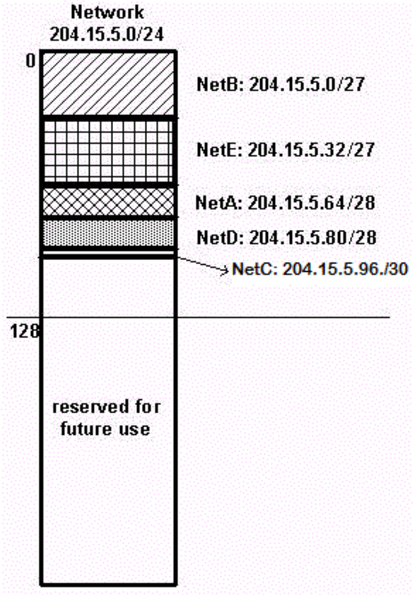


Figure 5 illustrates how using VLSM helped save more than half of the address space.

CIDR

Classless Interdomain Routing (CIDR) was introduced in order to improve both address space utilization and routing scalability in the Internet. It was needed because of the rapid growth of the Internet and growth of the IP routing tables held in the Internet routers.

CIDR moves way from the traditional IP classes (Class A, Class B, Class C, and so on). In CIDR, an IP network is represented by a prefix, which is an IP address and some indication of the length of the mask. Length means the number of left-most contiguous mask bits that are set to one. So network 172.16.0.0 255.255.0.0 can be represented as 172.16.0.0/16. CIDR also depicts a more hierarchical Internet architecture, where each domain takes its IP addresses from a higher level. This allows for the summarization of the domains to be done at the higher level. For example, if an ISP owns network 172.16.0.0/16, then the ISP can offer 172.16.1.0/24, 172.16.2.0/24, and so on to customers. Yet, when advertising to other providers, the ISP only needs to advertise 172.16.0.0/16.

Reference:

https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html#cidr