



SUBNETTING SCENARIO'S

This white paper provides several in-depth scenario's dealing with a very confusing topic, subnetting. Many networking engineers need extra practice to completely understand the intricacies involved. These scenarios address this need by providing you with multiple situations that will require a reasoned approach to solving them. Detailed explanations are provided with the actual formulas and how they were achieved.

Table of Contents

Subnetting Scenario's	1
Introduction to IP Addressing	3
IP Addressing	3
Class "A" Addresses	3
Class "B" Addresses	3
Class "C" Addresses	3
Exponent Review	4
Subnetting Review	4
Subnetting Scenarios & Questions	5
Scenario #1: IP Allocation in a MAN	5
Answer:	6
Explanation:	6
Scenario #2: Subnets & Hosts Availability	8
Answer:	9
Explanation:	9
Scenario #3: Address Allocation	10
Answer:	11
Explanation:	11
Scenario #4: What does a NetMask allow?	12
Answer:	13
Explanation:	13
Scenario #5: Writing a subnet mask	14
Answer:	15
Explanation:	15
Subnetting Review Questions	16
Question 1	16
Question 2	16
Question 3	16
Question 4	16
Access List Subnet Masks	18
Access List Scenarios	19
Scenario #1: Permitting & Denying An Entire Subnet	19
Answer:	19
Explanation:	19
Scenario #2: Blocking a range of subnets	19
Answer:	19
Explanation:	19
Scenario #3: Filtering Specific Subnets	20
Configuration Parameters:	20
Explanation:	20
Advanced Topic:	22
Additional Subnetting Resources	22



Certification Resources For Networkers



INTRODUCTION TO IP ADDRESSING

IP Addressing

N = network

H = host

S = subnet

Class "A" Addresses

A class "A" address can be represented in several different ways using different numbering systems as shown below:

Decimal	N.H.H.H
Hexadecimal	NN.HH.HH.HH
Binary	NNNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

The first network "N" bit from the left must be equal to 0 for a class "A" address. This is represented as follows in binary:

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

Some examples of a Class "A" address are written as follows:

Decimal	50.4.194.10
Hexadecimal	32.04.C2.0A
Binary	00110010.0000010.11000010.00001010

Class "B" Addresses

A Class "B" address can be represented in several different ways using different numbering systems as shown below:

Decimal	N.N.H.H
Hexadecimal	NN.NN.HH.HH
Binary	NNNNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

The first two network "N" bits from the left must be 10 for a Class "B" address. This is represented as follows in binary:

10NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

Some examples of a Class "B" address are written as follows:

Decimal	132.25.5.1
Hexadecimal	84.19.05.01
Binary	10000100.00011001.00000101.00000001

Class "C" Addresses

A class "C" address can be represented in several different ways using different numbering systems as shown below:



Certification Resources For Networkers

Decimal	N.N.N.H
Hexadecimal	NN.NN.NN.HH
Binary	NNNNNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

The first three network "N" bit from the left must be equal to 110 for a class "C" address. This is represented as follows in binary:

110NNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

Some examples of a Class "C" address are written as follows:

Decimal	196.77.42.254
Hexadecimal	C4.4D.2A.FE
Binary	11000100.01001101.00101010.11111110

Exponent Review

A^B = the value "A" is raised to the power as indicated by "B".
Thus $A * A * A \dots$ (Repeated "B" times). Please note that by default $A^0 = 1$.

EXPONENT EXAMPLES

$2^0 = 1$	$5^0 = 1$
$2^1 = 2$	$15^1 = 15$
$2^2 = 2 * 2 = 4$	$8^2 = 8 * 8 = 64$
$2^3 = 2 * 2 * 2 = 8$	$10^5 = 10 * 10 * 10 * 10 * 10 = 100,000$
$2^4 = 2 * 2 * 2 * 2 = 16$	

Subnetting Review

When it comes to networking the use of subnetting is vital in determining the proper allocation of ip addresses.

- 1) Divide the network into smaller pieces called subnetworks
- 2) Use address bits from the host portion of an ip address range in order to address the subnetworks
- 3) Adjust the subnet mask to show many host bits are being "used" to address the subnetwork

```

Binary address = NNNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH
Binary mask with 8 bit subnet = 11111111.11111111.00000000.00000000
-----
Result = NNNNNNNN.SSSSSSSS.HHHHHHHH.HHHHHHHH

```

8 bits are being "stolen" from the host part of the address in order to create subnet addresses

To obtain only the network and subnetwork address, perform a logical "AND" between the address and the subnet mask as follows:

```

Binary address = NNNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

```



Binary mask with 8 bit subnet = 11111111.11111111.00000000.00000000

Result of the logical "AND" = NNNNNNNN.SSSSSSSS.00000000.00000000
Only the network and subnet portion of address
remains

SUBNETTING SCENARIOS & QUESTIONS

This section will provide you a series of subnetting scenarios and questions

Scenario #1: IP Allocation in a MAN

You are tasked by your supervisor with assigning IP addresses for your new MAN (Metropolitan Area Network), which consists of 8 different buildings, each building will have **255** workstations. Your supervisor tells you to only use as much of the 164.10.0.0 network as you need. Your supervisor will assign the IP addresses to the serial interfaces using a different network. You will need to determine the following four items for each of the eight buildings:

- A) Subnet masks
- B) Network addresses
- C) Broadcast address for each subnet
- D) Valid host ranges on each subnet



Answer:

A) 255.255.254.0

B) 164.10.2.0
164.10.4.0
164.10.6.0
164.10.8.0
164.10.10.0
164.10.12.0
164.10.14.0
164.10.16.0

C) 164.10.3.255
164.10.5.255
164.10.7.255
164.10.9.255
164.10.11.255
164.10.13.255
164.10.15.255
164.10.17.255

D) 164.10.2.1 - 164.10.3.254
164.10.4.1 - 164.10.5.254
164.10.6.1 - 164.10.7.254
164.10.8.1 - 164.10.9.254
164.10.10.1 - 164.10.11.254
164.10.12.1 - 164.10.13.254
164.10.14.1 - 164.10.15.254
164.10.16.1 - 164.10.17.254

Explanation:

A) We need to have 255 workstations on each LAN. A 255.255.255.0 netmask will allow us only 254 valid hosts on a LAN, reserving one IP address for the network address and one for the broadcast address. Therefore, we should "borrow" one bit from the previous octet. 164.10.0.0 is a class "B" subnet because the first 2 bits of 164 are written in binary as "10". The default number of subnet bits on a class "B" network is 16. With this mask we are using a total of 23 masked subnet bits ("1"s), with 9 bits unmasked ("0"s). We have 7 additional masked subnet bits ($23 - 16 = 7$). $2^7 - 2 = 126$. We have 126 subnets available. We have a total of 9 unmasked subnet bits. $2^9 - 2 = 510$. We have a total of 512 host IP addresses available for each subnet. To double-check your math, add the default subnet bits with the additional subnet bits and the unmasked subnet bits together to get 32 ($16 + 7 + 9 = 32$).

There is another way to figure this out: We know that we need 255 workstation addresses, and 1 subnet network address and 1 subnet broadcast address. This is a total of 257. What is the lowest power of 2 that gives us a number greater than 257? The answer is 9. Therefore, we need 9 unmasked bits. We know we need 8 subnets. $8 + 2$ (for network and broadcast) gives 10. What is the lowest power of 2 that gives us a number greater than 10? The answer is 5 ($2^5 = 16$). $16 - 5 = 9$. We need 9 additional masked bits. Since we had a default subnet mask of 16 bits, and we know



that the total length of a subnet mask is 32 bits, the two answers we come up with MUST equal 16, which is the difference between 32 and the default subnet mask.

 *The trick to either method is knowing what the default network mask is.*

- B) What happened to 164.10.0.0? While this may work on some routers, this is not a "standard" configuration. We are able to do this on a Cisco router with the addition of the "ip subnet-zero" command, but it is still not a standard usage. Therefore, the first standard subnet is 164.10.2.0. Since each subnet contains a total of 514 addresses ($2^9 = 512$), the subnet must increment in sets of 512. If the first subnet is 164.10.2.0, the next must be 168.10.4.0. Let's work it out the long way: $164.10.2.0 + 255 = 164.10.2.255$. Also, $164.10.2.255 + 1 = 164.10.3.0$. Next, $164.10.3.0 + 255 = 164.10.3.255$, and $164.10.3.255 + 1 = 164.10.4.0$. Finally, $255+1+255+1 = 512$. Therefore, $164.10.2.0 + 512 = 164.10.4.0$.
- C) Broadcast addresses are so simple to figure out it will amaze you. Simply take the address of the next subnet and subtract 1. This equates to all "1"s in the area of the subnet mask that contain the unmasked bits:

164.10.3.255 =	10100100.00001010.00000011.11111111
255.255.254.0 =	11111111.11111111.11111110.00000000

In the 3rd octet of the subnet mask, notice where the masked bits change to unmasked bits. If all of the bits of the IP address that are over unmasked bits are "1"s, this is a broadcast address. A network address would have all "0"s over the unmasked bits.

- D) To find the valid IP hosts, simply use the network address and add 1. This is the first valid host address. Take the broadcast address and subtract 1. This is the last valid host address.



Scenario #2: Subnets & Hosts Availability

You have subnetted the 172.30.10.0 network with a mask of 255.255.255.192. How many usable subnets will you have and how many hosts are available on each subnet? (pick two)

- A) 64 hosts
- B) 62 hosts
- C) 192 hosts
- D) 2 subnets
- E) 3 subnets
- F) 4 subnets



Answer:

B and D – 62 Hosts & 2 Subnets

Explanation:

Why do we have 62 hosts per subnet? A subnet mask of 192 has two additional bits masked and six bits unmasked.

The formula for calculating available hosts is $(2^{\text{number of unmasked bits}}) - 2$ thus for answer B we would calculate the following:

$$\text{Thus for answer B: } (2^6) - 2 = (64) - 2 = 62$$

The formula for calculating the number of available subnets is $(2^{\text{number of additionally masked bits}}) - 2$

$$\text{Thus for answer D: } (2^2) - 2 = (4) - 2 = 2$$

But, what happened to the two hosts we subtracted from each subnet? The first available address is reserved for the network and the last is reserved for broadcast. In the same way, the first subnet (172.30.10.0 – 172.30.10.63) is reserved for the network, and the last subnet (172.30.10.192 – 172.30.10.255) is reserved for the broadcast. While it is possible to use the 172.30.10.0 – 172.30.10.63 subnet on some routers, the RFCs covering subnetting do not recommend doing this.



Scenario #3: Address Allocation

You are asked to figure out how many host addresses you need for your network. Which item(s) do you need to take into account?

- A) The subnet broadcast address
- B) The subnet network address
- C) Each computer in the building
- D) Each WAN connection
- E) Each network interface connection



Answer:

A, B, and E.

Explanation:

You will need both a network and broadcast address as well as one address for each network interface connection. Remember that the total number of connections includes the Ethernet interface on each router and switch connected to this Local Area Network. In order for the router to forward packets from the Ethernet interface to a remote location, the Ethernet interface MUST have a valid IP address on the Local Area Network. We will need to count all of the devices connected to the network and add one host for the network address and another host for the broadcast address for the network.



Scenario #4: What does a NetMask allow?

You are told that your client has a subnet mask of 255.255.255.248. How many hosts and subnets does this client have available?

- A) 16 subnets and 14 hosts
- B) 30 subnets and 16 hosts
- C) 8190 subnets and 8 hosts
- D) 8190 subnets and 6 hosts

**Answer:**

D is the correct answer. How do we know the correct answer is letter D?

Explanation:

Remember our powers of two: 2, 4, 8, 16, 32, 64, 128, 256, 1024, 2048, 4096, and 8192. Let's look at the hosts first. Our choices are 14, 16, 8, and 6. The first step in explaining this is to determine which of these numbers is two less than a power of two? Answers A and D fulfill this requirement. Our subnets from answers A and D are 16 and 8190. Again, we ask which of these numbers is two less than a power of two? Answer D fulfills this requirement. Notice that we didn't even need to know the IP address of the network, we simply worked off of the formulas previously given.



Scenario #5: Writing a subnet mask

On a Class B network with a 10 bit subnet mask, how would you write the subnet mask?

- A) 255.255.255.192
- B) 255.192.0.0
- C) 255.255.192.0
- D) 255.255.255.255



Answer:

A is the correct answer for this scenario.

Explanation:

When you are told what class the network is, assume that the question means ADDITIONAL subnet bits beyond what is the default based upon the class of the network unless you are told that this is the total number of subnet bits. A Class A network has a default subnet mask of 255.0.0.0, or 8 bits. A class B network's default subnet mask is 255.255.0.0, or 16 bits. A Class C network has a default subnet mask of 255.255.255.0, or 24 bits. The question stated that you had a Class B network. Therefore, you have a default subnet mask of 255.255.0.0, or 16 bits. Adding ten bits will give you 255.255.255.192, or 26 bits. Subnets masks are also represented by a decimal number indicating how many bits are used in the mask. Example, the notation 131.108.1.0/24 is equivalent to a mask of 255.255.255.0. Cisco routers can be modified to display the subnets mask in three ways:

R1#term ip netmask-format ?

bit-count	Display netmask as number of significant bits example 131.108.1.1/24 (default)
decimal	Display netmask in dotted decimal example 131.108.1.1 255.255.255.0
hexadecimal	Display netmask in hexadecimal example 131.108.1.1 0xFFFFF00



Subnetting Review Questions

Lets take a minute to do some questions as a review to what you have learned so far.

Question 1

How many hosts/networks are available in using a netmask of 255.255.254.0?

- A. 255
- B. 254
- C. 510
- D. 2048
- E. 512

Answer: C

The numbers of bits available for hosts are 9. Hence $2^9 - 2 = 510$ host addresses. Two addresses are reserved for broadcasts.

Question 2

What mask will allow at most 14 hosts?

- A. /30
- B. /24
- C. /20
- D. /28
- E. /29

Answer: D

The slash donation simply states how many bits are used in the subnet mask. For example /28 means 255.255.255.240 (28 consecutive 1's followed by 4 bits for host address). This mask allows at most 14 hosts as $2^4 - 2 = 14$ hosts.

Question 3

Having been assigned a Class C network block, what would be the extended network prefix to allow 22 host on each subnet?

- A. /28
- B. /24
- C. /27
- D. /32

Answer: C

To accommodate 22 hosts per subnet, a minimum of 5 bits are required and hence the extended network prefix of /27 i.e. 255.255.255.224. The maximum number of hosts on a subnet would be $2^5 - 2 = 30$ hosts and hence meeting our requirements.

Question 4

Having been assigned 172.16.0.0/16 network block. You are asked to establish 12 subnets. What would be the mask that allows the creation of 12 subnets?

- A. /16
- B. /18



- C. /24
- D. /20

Answer: D

The number of subnets can be in blocks of powers of two i.e. 2 (2^1), 4 (2^2), etc. Hence to have 12 subnets, we define a block of 16 (2^4). Four bits are required and hence the mask of /20.



ACCESS LIST SUBNET MASKS

Access Control Lists are meant to provide filtering capabilities. As the packets pass through the router they are analyzed and filtered by help of Access Control Lists (ACLs). ACLs can be configured for all routed protocols (IP, AppleTalk, DecNet, etc.). By help of this filtering mechanism of ACLs, traffic to and from a particular network can be prevented or allowed. The router examines each and every packet and based upon the ACLs, the packet is either forwarded or blocked.

Although ACLs are used for many reasons the prime reason is to provide basic level security to the network. ACLs are generally used on gateway routers to act as a "wall" between the Internal and the External network. One can use access lists on a router connecting two parts of the same network. For e.g: The management would not like anybody and everybody in the company to access the finance network.

Below are the types of access lists:

- ⇒ Standard Access Lists
- ⇒ Static Extended Access Lists
- ⇒ Lock and Key Security (Dynamic Access Lists)
- ⇒ Reflexive Access Lists (This allows IP packets to be filtered based on upper-layer session information)

Access Lists should be defined for every protocol that one wants to filter. Every Access List is assigned a unique number or name and the packet filtering criteria is defined. The single access list can have multiple filtering criteria. For e.g: Access to only mail server is allowed from the outside network and that too for port 25 of the server.

By default there is an implicit deny ALL at end of every Access List. Hence, any packet that does not matches the criteria specified, the packet will be dropped. One has to be careful while defining the criteria of ACLs. The packet is matched against each criteria statement in the order the statements were created and is processed. Because of this it is quite possible a particular kind of traffic that should have been allowed to pass through the router is blocked.

The access lists can be defined either on the inbound or the outbound interface of the router. The access lists criteria must be logged and a continuous check on the logs must be kept.



ACCESS LIST SCENARIOS

The following information is provided to assist you in understanding Access Lists and their design as well as implementation.

Scenario #1: Permitting & Denying An Entire Subnet

Your supervisor has given you two subnets i.e. 10.10.10.0 with subnet mask 255.255.255.0 and 172.21.10.0 with subnet mask 255.255.255.248. You have been asked to permit traffic from the 10.10.10.0 network and to deny access to your internal network from the 172.21.10.0 network. No other traffic needs to be permitted. Define the access list to do the above said.

Answer:

```
Access-list 100 permit 10.10.10.0 0.0.0.255
```

Explanation:

Access List masks are inverse of the normal mask. The way we calculate the wildcard mask is as follows:

```
255.255.255.255  
- 255.255.255.0  
0.0.0.255
```

If you are still wondering that we have not denied access to the 172.21.10.0 then remember that there is a implicit deny at the end of every access list and hence the 172.21.10.0 network will not be able to access our network. We have used an extended access list. The better option would be to specify that everything is being denied access by using the command "access-list 100 deny any any log". This will deny any traffic and log the denials to the system logging server.

Scenario #2: Blocking a range of subnets

You have been asked by your supervisor to permit the 172.20.16.0 - 172.20.31.255 range which has a subnet mask of 255.255.240.0. Define an access list to do the above said.

Answer:

```
Access-list 101 permit 172.20.16.0 0.0.15.255
```

Explanation:

To find the wildcard mask, take the higher minus the lower i.e.

```
172.20.31.255  
- 172.20.16.0  
0.0.15.255
```



To further explain how it works.

0 = Check (C)
1 = Don't Care (D)

0.0.15.255
CCCCCCCC.CCCCCCCC.CCCDDDD.DDDDDDD

This means that the first 20 bits will be checked and the last 12 will be ignored. You'll notice that any network from 172.20.16.0 - 172.20.31.0 will match Network 0 for the first 20 bits, after the first 20 bits, we don't care if they match or not.

```
11111111.11111111.1111|0000.00000000 255.255.240.0
10101100.00010100.0001|0000.00000000 172.20.16.0
10101100.00010100.0001|0001.00000000 172.20.17.0
10101100.00010100.0001|0010.00000000 172.20.18.0
...
10101100.00010100.00011111.00000000 172.20.31.0
10101100.00010100.00100000.00000000 172.20.32.0
```

Notice how this network does not match 172.20.16.0 for the first 20 bits? Therefore this network doesn't match and does not satisfy the access list.

Scenario #3: Filtering Specific Subnets

Configure the appropriate Access Control List (ACL) to permit or deny the following networks on the inbound interface of a Cisco 2520's first low speed interface.

```
Deny network 204.199.104.X
Deny network 164.199.104.X
Permit network 204.199.108.X
Permit network 164.199.108.X
```

Configuration Parameters:

- ⇒ Permit all other networks that are in the range 140.140.X.Y where X is the even numbered subnets only.
- ⇒ Permit all other IP subnets.
- ⇒ You must also minimize the configuration as much as possible!

Explanation:

You are asked to configure simple access-lists. This appears to be easy until we get the last requirement:

"Minimize the configurations as much as possible."

How do we minimize networks with Access lists? We first need to look at the networks and look at them in binary format to see any differences or similarities. Let's first look at the first two networks:

204.199.104.X

164.199.104.X

At first glance the only similarities appears to be the second and third octet until we look at the first 8 bits in binary.

 In the CCIE lab you have access to the windows calculator

Thus the first octet appears as follows when viewed in binary:

204 = 11001100
164 = 10001100

Looking at these we see that only the second bit position is different hence we can apply our wildcard mask to make sure the other 7 bits match and we do not care about the second bit as it could be 0 or 1.

We will calculate the mask as follows:

```
11001100
10001100
-----
01000000 ---> 64
```

The do care (match) bits are set to 0 and the don't care (ignore) bits are set to 1. Hence the mask in decimal is 64. We can now apply the required configuration in one line to block the networks 204.199.104.X and 164.199.104.X as follows:

```
Access-list 1 deny ip 140.199.104.0 64.0.0.0
```

You must now apply the same technique to the second pair of networks, 204.199.108.X and 160.199.108.X differ by one bit in the first byte hence the mask is once again 64.0.0.0.

To permit all networks that are 140.140.X.Y where X is even requires a little more mathematical knowledge than you would normally use in the real world. But remember that even numbers are always divisible by 2 or in binary this means that the last bit is always set to zero. This sample table will demonstrate what we mean.

Decimal	Binary	
1	00000001	Odd
2	00000010	Even
3	00000011	Odd
4	00000100	Even, etc...

So what wildcard mask will deny all networks unless they are even? Well any mask that must match the last bit as being 0. That is we don't care what the first seven bits are but the last bit must be set to zero which is the case with all even numbers. Hence the mask is 11111110 or 254.

So to complete the third part of the question our configuration is:



Access 1 permit ip 140.140.2.0 0.0.254.255

To permit all other IP traffic we need to add the line:

Access 1 permit ip any

By default all other networks are denied. Lastly we need to apply the access-list to the inbound interface on a Cisco 2520 first low speed interface as instructed. A Cisco 2520 has four serial ports of which the first two are high speed and the last two are low speed so we need to apply it to interface Serial2.

```
R1(config)#int s 2
R1(config-if)#ip access-group 1 in
R1(config-if)#exit
```

Advanced Topic:

Verify networks statements match and denies as instructed. Could you of used an extended IP access list. How would you deny all odd networks? How could you view logs against this access list?


Additional Subnetting Resources

IP Subnet Calculation & Design Online Documentation

http://www.cisco.com/techtools/ip_addr_help.html

This is a great tutorial to get you started called "Understanding IP Addressing".

<http://www.3com.com/nsc/501302s.html>

 As always NetCerts welcomes your feedback regarding this white paper and encourage our fellow virtual community members to contribute to our site so all can benefit. If you are interested please contact us at: webmaster@netcerts.com