IP Addressing and Subnetting

Objectives

Upon completion, you will be able to:

- Discuss the Types of Network Addressing
- Explain the Form of an IP Address
  - Network ID
  - Host ID
- Discuss the Classes of IP Addresses
- Understand the Function of the Mask

Let's Talk About Addressing!

- **Types of Addressing:**
  - Layer 2 – MAC Addresses (Media Access Control)

0134.2345.12AB	A MAC Address
0134.23	Vendor Code
45.12AB	Serial Number

  - Layer 3 – Logical Addresses (IPv4 or IPX)
- **Assignment of IP Addresses:**
  - Static Addresses – assigned by an Administrator
  - Dynamic Addresses – DHCP
  - "Hierarchical" vs. "Flat" Addressing Schemes

Can You Count in Binary?

We are Very Familiar with our Decimal System…

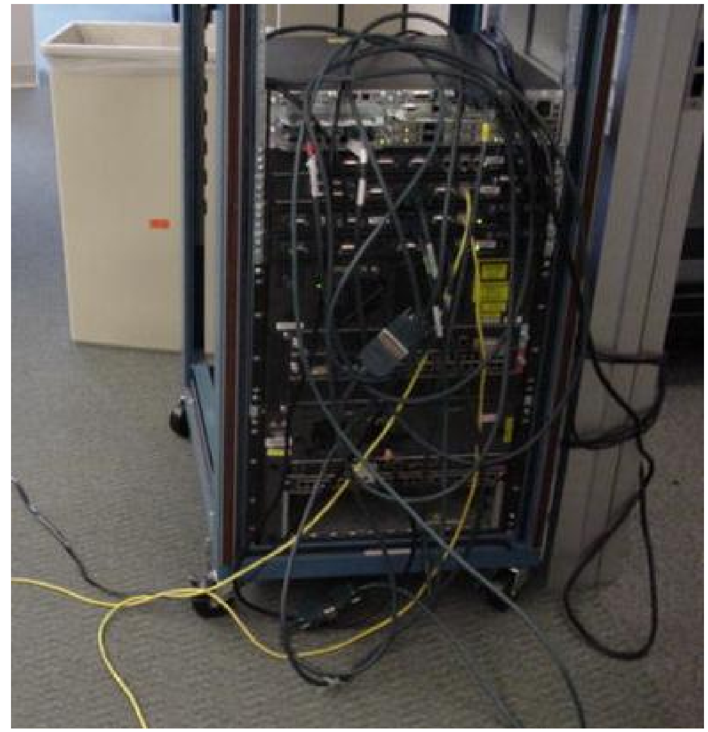
0 1 2 3 4 5 6 7 8 9…10 11 12 13…

But,

We Need to Become Familiar with the Binary System…only 0's and 1's

0000	**1**	**10**	**11**	**100**	**101**	**110**	**111**	**1000**	**1001…**
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**

Basics of An IPv4 Address



- Layer 3 (L3) Logical IP Addresses are comprised of 4 Octets, separated by a .
- The Decimal form looks like this:

176.223.14.127

- The Binary form looks like:

128 64 32 16 8 4 2 1

10110000.11011111.00001110.01111111

Basics of An IPv4 Address

- Each of the 4 Octets has 8 Bits
- Each of these Bits has a “Binary Value”
- Each Bit can only be a One or a Zero
- Let’s Look at One of the Octets – 8 Bits

128 64 32 16 8 4 2 1

Each of these 8 bits has a distinct value, that starts at “1” from the right side and moving to the left, doubles each time to 2, 4, 8, 16, 32, 64, and finally 128, as shown above.

IPv4 Addressing

32 bits

Dotted Decimal	Network		Host	
Maximum	255	255	255	255
	1 8	9 16	17 24	25 32
Binary	11111111	11111111	11111111	11111111
	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1
Example Decimal	172	16	122	204
Example Binary	10101100	00010000	01111010	11001100

IPv4 Address Classes

	8 bits	8 bits	8 bits	8 bits
• Class A:	Network	Host	Host	Host
• Class B:	Network	Network	Host	Host
• Class C:	Network	Network	Network	Host

- Class D: Multicast
- Class E: Research

IPv4 Address Classes

Class A:

Bits:	1 … 8	9 … 16	17 … 24	25 … 32
	0NNNNNNN	Host	Host	Host

Range (1-127) – 16,777,214 hosts

Class B:

Bits:	1 … 8	9 … 16	17 … 24	25 … 32
	10NNNNNN	Network	Host	Host

Range (128-191) – 65,534 hosts

Class C:

Bits:	1 … 8	9 … 16	17 … 24	25 … 32
	110NNNNN	Network	Network	Host

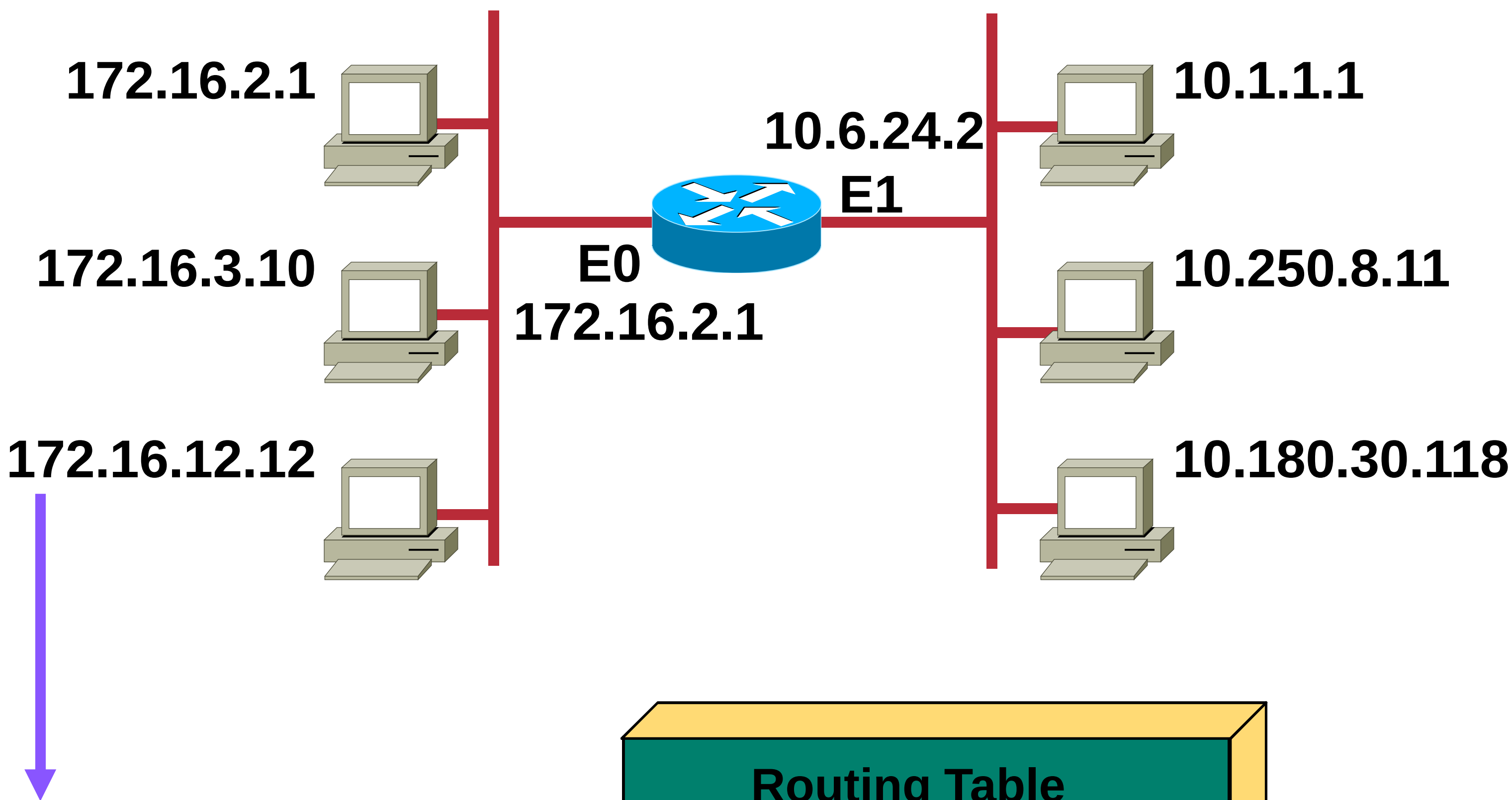
Range (192-223) – 254 hosts

Class D:

Bits:	1 … 8	9 … 16	17 … 24	25 … 32
	1110MMMM	Multicast Group	Multicast Group	Multicast Group

Range (224-239)

Host Addresses



172.16 . 12 . 12

Network Host

Routing Table Network	Interface
172.16.0.0	E0
10.0.0.0	E1

Determining Available Host Addresses

Cisco.com

Network		Host	
172	16	0	0

16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 N

10101100	00010000	00000000	00000000	1
		00000000	00000001	2
		00000000	00000011	3
		⋮	⋮	⋮
		11111111	11111101	65534
		11111111	11111110	65535
		11111111	11111111	65536

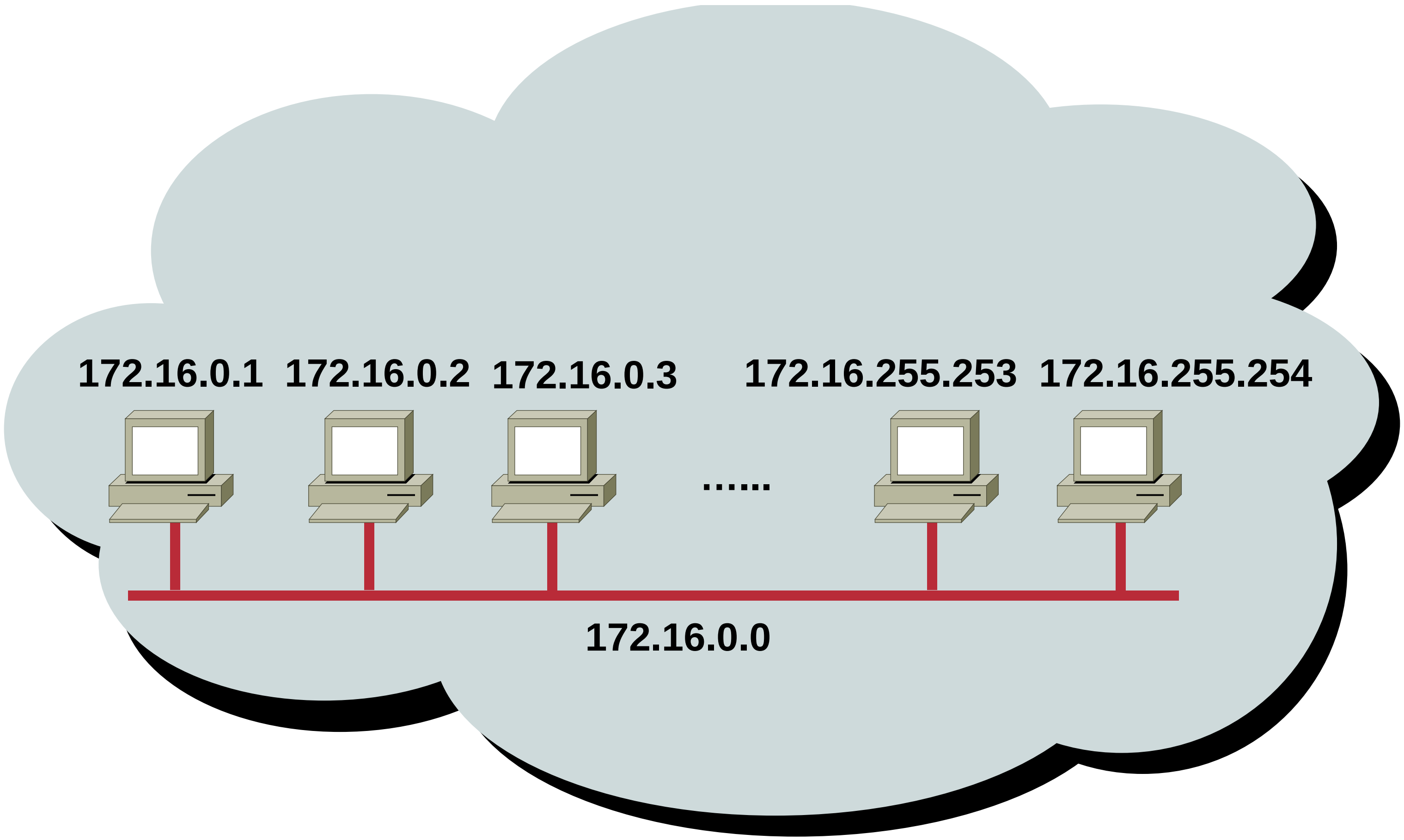
Remember 2^N-2 (where N is the number of host bits)

$2^N-2 = 2^{16}-2 = 65534$

$$\begin{array}{r} 65536 \\ -\quad 2 \\ \hline 65534 \end{array}$$

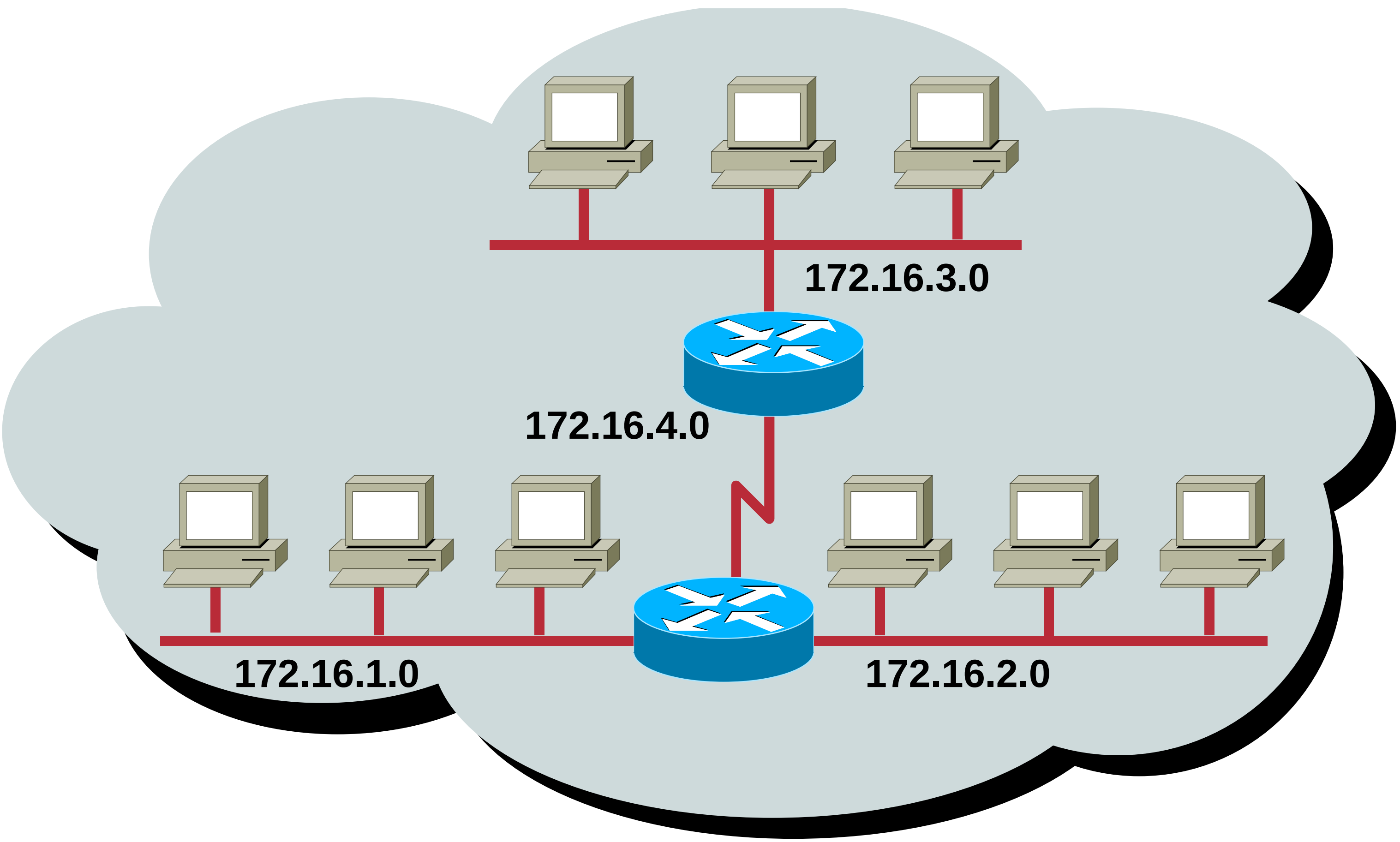
Addressing without Subnets

Cisco.com



- **Network 172.16.0.0**

Addressing with Subnets



- Network 172.16.0.0

Subnet Mask

	Network		Host	
IP Address	172	16	0	0

	Network		Host	
Default Subnet Mask	255 11111111	255 11111111	0 00000000	0 00000000

Also written as "/16" where 16 represents the number of 1s in the mask.

	Network		Subnet	Host
8-bit Subnet Mask	255	255	255	0

Also written as "/24" where 24 represents the number of 1s in the mask.

Decimal Equivalents of Bit Patterns

128	64	32	16	8	4	2	1		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

Know your two's

- $2^1 = 2$
- $2^2 = 4$
- $2^3 = 8$
- $2^4 = 16$
- $2^5 = 32$
- $2^6 = 64$
- $2^7 = 128$
- $2^8 = 256$
- $2^9 = 512$
- $2^{10} = 1024$
- $2^{11} = 2048$
- $2^{12} = 4096$
- $2^{13} = 8192$
- $2^{14} = 16384$
- $2^{15} = 32768$
- $2^{16} = 65536$

Know Your CIDR Values

Cisco.com

- 255.0.0.0 /8
- 255.128.0.0 /9
- 255.192.0.0 /10
- 255.224.0.0 /11
- 255.240.0.0 /12
- 255.248.0.0 /13
- 255.252.0.0 /14
- 255.254.0.0 /15
- 255.255.0.0 /16
- 255.255.128.0 /17
- 255.255.192.0 /18
- 255.255.224.0 /19
- 255.255.240.0 /20
- 255.255.248.0 /21
- 255.255.252.0 /22
- 255.255.254.0 /23
- 255.255.255.0 /24
- 255.255.255.128 /25
- 255.255.255.192 /26
- 255.255.255.224 /27
- 255.255.255.240 /28
- 255.255.255.248 /29
- 255.255.255.252 /30

Subnet Mask with Subnets

	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.0	11111111	11111111	11111111	00000000
	10101100	00010000	00000010	00000000
			128 192 224 240 248 252 254 255	
Network Number	172	16	2	0

- Network number extended by eight bits
- Without a subnet mask you cannot tell the host address nor the network it resides on!

Subnet Mask with Subnets (cont.)

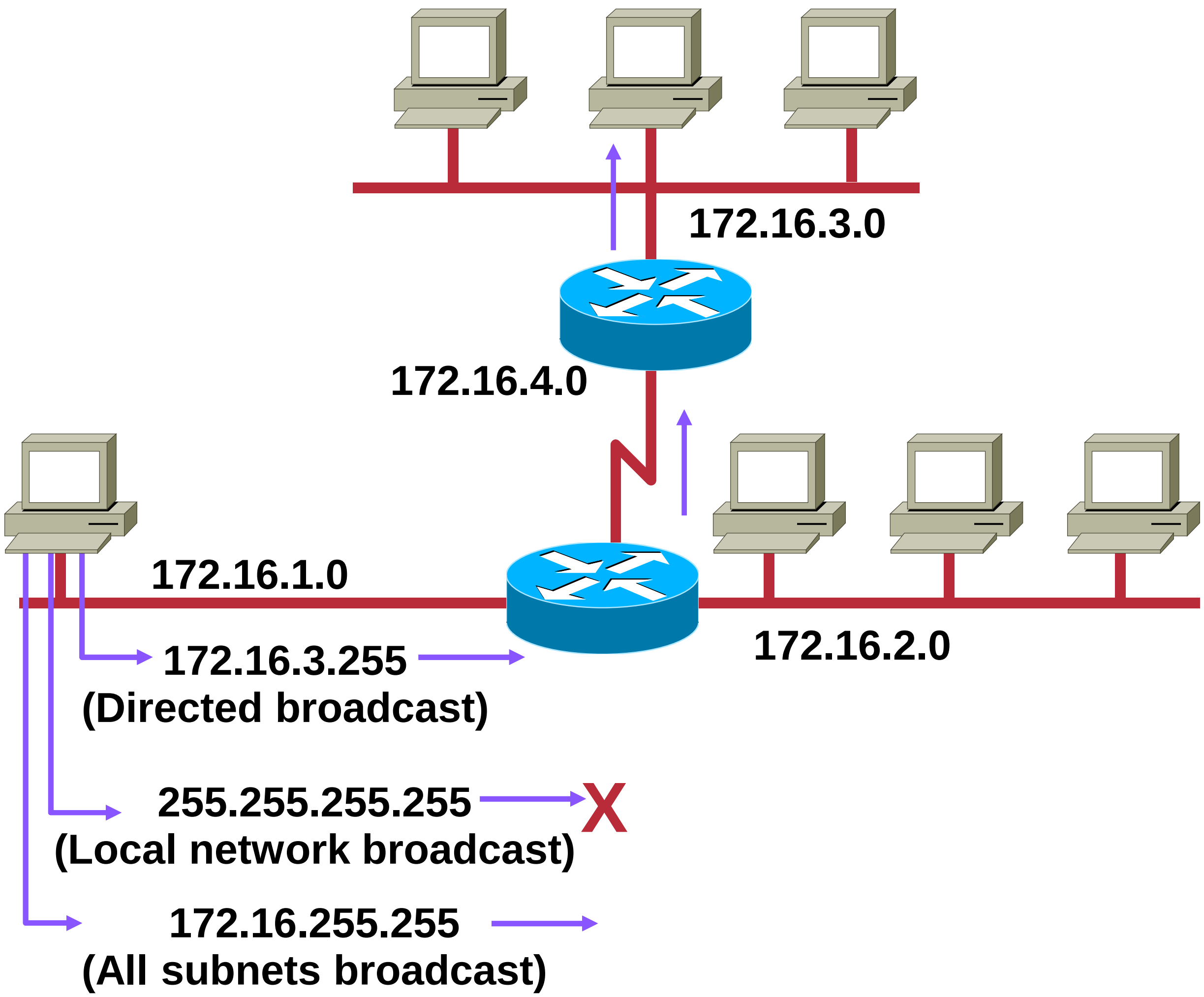
Cisco.com

	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.192	11111111	11111111	11111111	11000000
	10101100	00010000	00000010	10000000
			128 192 224 240 248 252 254 255	128 192 224 240 248 252 254 255

Network Number	172	16	2	128

- Network number extended by ten bits

Broadcast Addresses

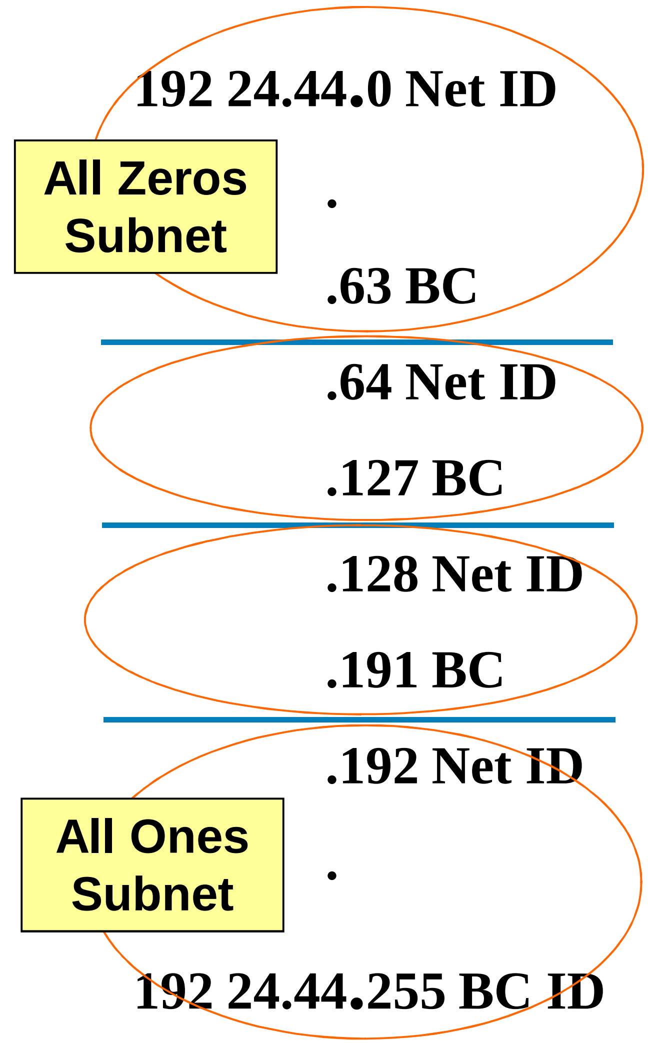


All Zeros and All Ones Subnets

RFC 1878 states:

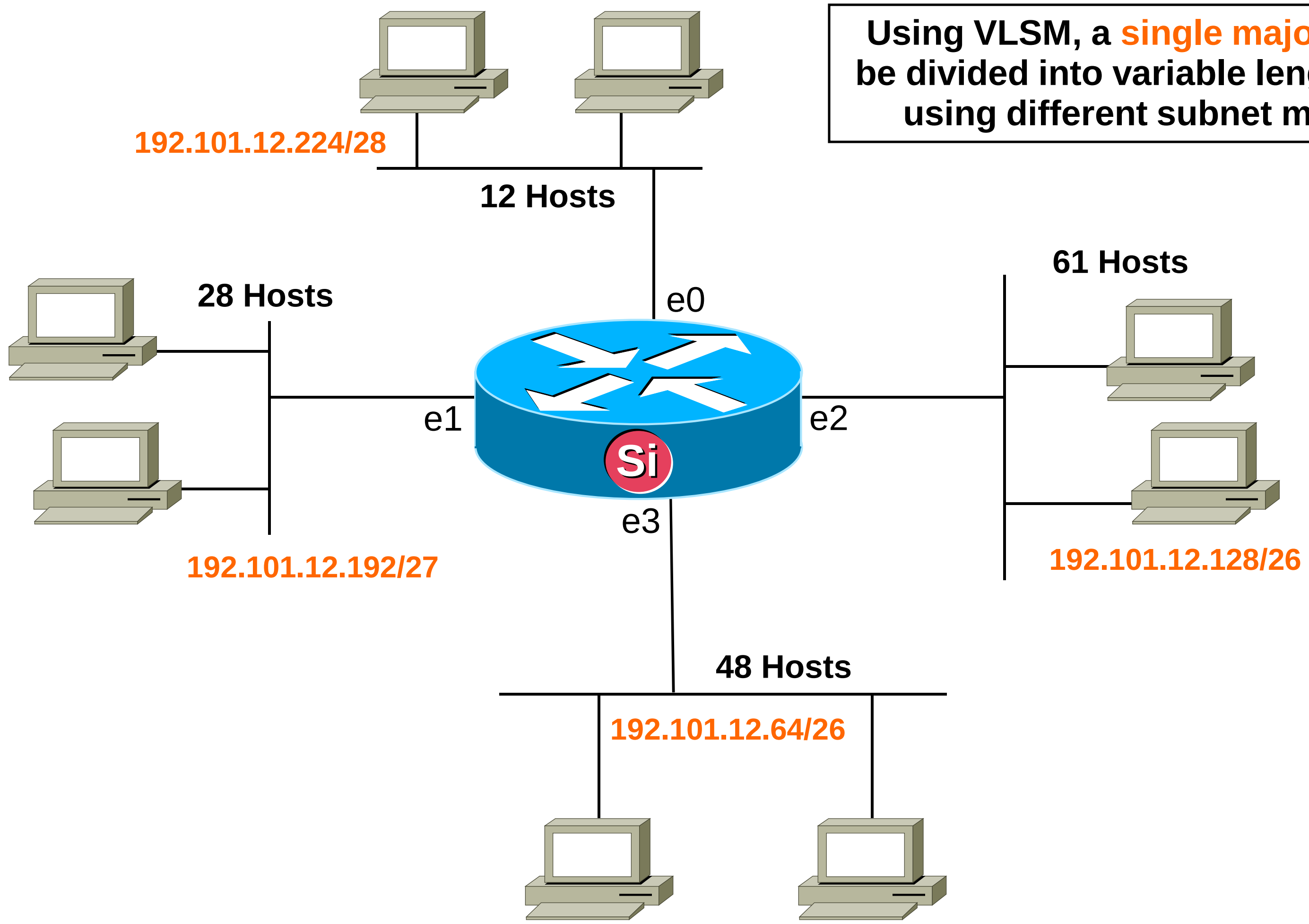
"This practice of excluding the "all-zeros subnet" and the "all-ones subnet" is obsolete! Modern software will be able to utilize all definable sub-networks."

Today, the use of subnet zero and the all-ones subnet is generally accepted and most vendors support their use, though, on certain networks (and the CCNA Exam), particularly the ones using legacy software, the use of subnet zero and the all-ones subnet can lead to problems.



VLSM - Variable Length Subnet Mask

Using VLSM, a single major network can be divided into variable length subnets by using different subnet mask lengths



Topic 3 IP Addressing Lab Guide

All devices on a network, whether they are end systems like laptops and servers or networking equipment like switches and routers, communicate with each other using different forms of addresses. On an Ethernet network, each device has a globally unique address that is normally assigned during manufacturing. Thus, it is often times known as the hardware or physical address. This 48-bit address is actually called the Media Access Control (MAC) address and is expressed in hexadecimal format, e.g. AA:BB:CC:12:34:56. Under the OSI Reference Model, it is aligned at the Data layer (Layer 2). Though it is a flat address without any hierarchy, it is based on a centrally assigned model, whereby the first six hexadecimal characters identify the manufacturer and are issued by the Institute for Electrical and Electronics Engineers (IEEE). This portion of the MAC is known as the Organizationally Unique Identifier (OUI). The last six remaining hexadecimal characters are assigned by each manufacturer independently. The MAC address is important because it is the address that devices actually use to deliver packets to each other on a physical wire.

As opposed to the burned-in MAC address, an IP address is a logical address that can be assigned and changed at will on a device. Under the OSI Reference Model, it is considered as the Network layer (Layer 3). It is hierarchical and is assigned based on the network where the device resides. For TCP/IP applications (e.g. web browsers, online games, etc…), it is the IP address that is used for communication, whether it is between adjacent devices or devices on different sides of the world. The application data, along with the source and destination IP addresses, is encapsulated within a frame that contains the source and destination MAC addresses, before the frame is sent onto the wire to the next hop.

To summarize, all Ethernet frames that are sent on a network wire contain the source and destination MAC addresses on the outermost layer of the frames. The next layer of the frames contains the source and destination IP addresses, if the frames are for a TCP/IP application. Actual application data is contained in an even deeper layer.

In this lab, we will go through a series of tasks to demonstrate the nature of MAC and IP addresses. In the interest of time, the lab has been pre-populated with the necessary equipment. The tasks will include:

Task 1: Assign interface Vlan1 on Switch1 and its hosts to IP addresses within the subnet 10.10.1.0/24

Task 2: Assign interface Vlan1 on Switch2 and its hosts to IP addresses within the subnet 10.10.1.0/24

Task 3: Re-assign interface Vlan1 on Switch2 and its hosts to subnet 10.10.2.0/24

Task 4: Enable ports Gig0/0 and Gig0/1 on Router1. Assign Gig0/0 to subnet 10.10.1.0/24 and Gig0/1 to subnet 10.10.2.0/24

Task 5: Ensure all switches, routers and end hosts can ping each other's IP address

Task 1: Assign interface Vlan1 on Switch1 and its hosts to IP addresses within the subnet 10.10.1.0/24

In this task, we will assign IP addresses to interface Vlan1 on Switch1 and its connected hosts. We will verify the MAC and IP addresses of these systems, as well as the connectivity among them.

1. Assign IP addresses to Laptop1 and Laptop2 on the FastEthernet0 interface under Config for each host.
    a. Laptop1 should have IP address 10.10.1.1 with subnet mask of 255.255.255.0
    b. Laptop2 should have IP address 10.10.1.2 with subnet mask of 255.255.255.0
2. Assign the IP address 10.10.1.11 to interface Vlan1 on Switch1 using the CLI.
    a. enable
    b. configure terminal
    c. interface vlan1
    d. ip address 10.10.1.11 255.255.255.0
    e. no shutdown
    f. end
    g. copy run start
3. Verify that all systems can communicate with each other. On Laptop1, perform these steps via the Command Prompt under Desktop and verify that the pings are successful.
    a. ping 10.10.1.2
    b. ping 10.10.1.11
4. Record the MAC and IP addresses of Switch1 and its connected hosts. This can be accomplished on Laptop1 via the command "arp -a" on the Command Prompt, which displays the ARP table. The ARP process is a mechanism used by devices to query for the MAC address that corresponds to an IP address since a device needs the MAC address in order to communicate with other devices on the wire. Under the "arp -a" output, the "Internet Address" is the IP address and the "Physical Address" is the MAC address. The IP and MAC addresses of Laptop1 itself can be obtained via the command "ipconfig /all".
    a. Laptop1: IP Address:____________________, MAC:_____________________
    b. Laptop2: IP Address:____________________, MAC:_____________________
    c. Switch1: IP Address:____________________, MAC:_____________________

Task 2: Assign interface Vlan1 on Switch2 and its hosts to IP addresses within the subnet 10.10.1.0/24

In this task, we will expand the network created in Task 1. Assign IP addresses to interface Vlan1 on Switch2 and its connected hosts. We will verify the MAC and IP addresses of these systems, as well as the connectivity among the laptops and switches.

1. Assign IP addresses to Laptop3 and Laptop4 on the FastEthernet0 interface under Config for each host.
    a. Laptop3 should have IP address 10.10.1.3 with subnet mask of 255.255.255.0
    b. Laptop4 should have IP address 10.10.1.4 with subnet mask of 255.255.255.0
2. Assign the IP address 10.10.1.12 to interface Vlan1 on Switch2 using the CLI.

a. enable
b. configure terminal
c. interface vlan1
d. ip address 10.10.1.12 255.255.255.0
e. no shutdown
f. end
g. copy run start

3. Verify that all systems can communicate with each other. On Laptop1, perform these steps via the Command Prompt under Desktop and verify that the pings are successful.
    a. ping 10.10.1.2
    b. ping 10.10.1.3
    c. ping 10.10.1.4
    d. ping 10.10.1.11
    e. ping 10.10.1.12
4. Record the MAC and IP addresses of all the laptops and switches. This can be accomplished on Laptop1 via the command “arp -a” on the Command Prompt. The “Internet Address” is the IP address and the “Physical Address” is the MAC address. The IP and MAC addresses of Laptop1 itself can be obtained via the command “ipconfig /all”.
    a. Laptop1: IP Address:____________________, MAC:_____________________
    b. Laptop2: IP Address:____________________, MAC:_____________________
    c. Laptop3: IP Address:____________________, MAC:_____________________
    d. Laptop4: IP Address:____________________, MAC:_____________________
    e. Switch1: IP Address:____________________, MAC:_____________________
    f. Switch2: IP Address:____________________, MAC:_____________________

Task 3: Re-assign interface Vlan1 on Switch2 and its hosts to subnet 10.10.2.0/24

In this task, we will re-assign the IP addresses to interface Vlan1 on Switch2 and Laptop3 and Laptop4. We will examine the MAC and IP addresses of these systems, as well as how connectivity among the laptops and switches have changed.

1. Assign IP addresses to Laptop3 and Laptop4 on the FastEthernet0 interface under Config for each host.
    a. Laptop3 should have IP address 10.10.2.3 with subnet mask of 255.255.255.0
    b. Laptop4 should have IP address 10.10.2.4 with subnet mask of 255.255.255.0
2. Assign the IP address 10.10.2.12 to interface Vlan1 on Switch2 using the CLI.
    a. enable
    b. configure terminal
    c. interface vlan1
    d. ip address 10.10.2.12 255.255.255.0
    e. no shut
    f. end
    g. copy run start

3. Let's examine how connectivity between the switches and laptops has changed. On Laptop1, perform the following ping tests via the Command Prompt under Desktop. Which pings are successful and which are not?
   a. ping 10.10.1.2
   b. ping 10.10.1.11
   c. ping 10.10.2.3
   d. ping 10.10.2.4
   e. ping 10.10.2.12
4. On Laptop3, perform these similar ping tests. Which pings are successful and which are not?
   a. ping 10.10.1.1
   b. ping 10.10.1.2
   c. ping 10.10.1.11
   d. ping 10.10.2.4
   e. ping 10.10.2.12
5. For Step 3, all ping tests to addresses within the subnet 10.10.2.X should have failed. Ping is a TCP/IP application and the change in logical IP network for Switch2 and its connected laptops (Laptop3 and Laptop4) would cause the ping tests to fail on Laptop1 in this situation, even though the physical wiring has not changed. Although we changed the IP addresses on Switch2 and its connected laptops, would the MAC addresses for those devices have changed as well? Let's examine by using the "arp –a" and "ipconfig /all" commands on Laptop1. Notice that Laptop1 does not display any information for hosts within the 10.10.2.x subnet, while still displaying stale information regarding Switch2 and its connected laptops.
   a. Laptop1: IP Address:____________________, MAC:_____________________
   b. Laptop2: IP Address:____________________, MAC:_____________________
   c. Switch1: IP Address:____________________, MAC:_____________________
6. Similarly for Step 4, Laptop3 would have failed to successfully ping all addresses on the 10.10.1.x subnet. Let's see what Laptop3 knows about its neighbors' IP and MAC addresses. Use the "arp –a" and "ipconfig /all" commands on Laptop3 to obtain the following information.
   a. Laptop3: IP Address:____________________, MAC:_____________________
   b. Laptop4: IP Address:____________________, MAC:_____________________
   c. Switch2: IP Address:____________________, MAC:_____________________
7. Compare the IP and MAC address information from Laptop1 and Laptop3 with that of Step 4 of Task 2. Notice that although the IP addresses have changed, all of the MAC addresses are still the same. This is because MAC addresses are ultimately the addresses used by devices for communicating on the physical wire but successful communication for applications will need to take into account higher layer information like IP addresses.

Task 4: Enable ports Gig0/0 and Gig0/1 on Router1. Assign Gig0/0 to subnet 10.10.1.0/24 and Gig0/1 to subnet 10.10.2.0/24

In this task, we will enable the ports on Router1 and assign them to the proper subnets. We will then examine if all switches and routers can communicate with each other after enabling Router1.

1. Using the CLI on Router1, enable Gig0/0 and assign it the address 10.10.1.254 with subnet mask 255.255.255.0. Enable Gig0/1 and assign it the IP address 10.10.2.254 with subnet mask 255.255.255.0.
    a. enable
    b. configure terminal
    c. interface gig0/0
    d. ip address 10.10.1.254 255.255.255.0
    e. no shutdown
    f. exit
    g. interface gig0/1
    h. ip address 10.10.2.254 255.255.255.0
    i. no shutdown
    j. end
    k. copy run start
2. Verify that Router1 can successfully ping all switches and laptops. Successful pings are indicated by exclamation points.
    a. ping 10.10.1.1
    b. ping 10.10.1.2
    c. ping 10.10.1.11
    d. ping 10.10.2.3
    e. ping 10.10.2.4
    f. ping 10.10.2.12
3. On Router1, record the IP and MAC address information for all devices, including Router1 itself, using the CLI command "show ip arp". The dash ("-") under the "Age (min)" column indicates that the information is local to the device. Note that the IP and MAC addresses are still the same from Task 3. This is expected since we have not changed the configuration on the switches and routers.
    a. Laptop1: IP Address:______________________, MAC:_______________________
    b. Laptop2: IP Address:______________________, MAC:_______________________
    c. Laptop3: IP Address:______________________, MAC:_______________________
    d. Laptop4: IP Address:______________________, MAC:_______________________
    e. Switch1: IP Address:______________________, MAC:_______________________
    f. Switch2: IP Address:______________________, MAC:_______________________
    g. Router1, Gig0/0: IP Address:______________________, MAC:_______________________
    h. Router1, Gig0/1: IP Address:______________________, MAC:_______________________
4. Now that we have enabled Router1 and it is able to ping all switches and laptops on the network, does this mean that connectivity between all laptops and switches have been restored? Let's examine by running our ping tests on Laptop1. Are all the tests successful?
    a. ping 10.10.1.2
    b. ping 10.10.1.11
    c. ping 10.10.1.254
    d. ping 10.10.2.3
    e. ping 10.10.2.4
    f. ping 10.10.2.12

   g. ping 10.10.2.254
5. Similarly, run the ping tests on Laptop3. Which pings are successful and which are not?
   a. ping 10.10.1.1
   b. ping 10.10.1.2
   c. ping 10.10.1.11
   d. ping 10.10.1.254
   e. ping 10.10.2.4
   f. ping 10.10.2.12
   g. ping 10.10.2.254

Task 5: Ensure all switches, routers and end hosts can ping each other's IP address

Steps 4 and 5 of Task 4 show us that connectivity between all devices have not been restored even after enabling Router1 within the network. This is because hosts connected to switches 1 and 2 are on different logical IP network despite being in the same broadcast domain. Devices on different logical IP networks need to know the intermediary device that will assist in the communication across these logical networks. A router is designed to function in this capacity, known as the gateway, but hosts need to be configured to send information destined for different logical networks to the router in order for the communication to be successful.

1. Configure Laptop1 and Laptop2 to use Router1 Gig0/0 as the gateway address.
   a. Under the Global Config for Laptop1, enter 10.10.1.254 as the Gateway address (not IPv6 Gateway).
   b. Under the Global Config for Laptop2, enter 10.10.1.254 as the Gateway address (not IPv6 Gateway).
2. Configure Laptop2 and Laptop3 to use Router1 Gig0/1 as the gateway address.
   a. Under the Global Config for Laptop3, enter 10.10.2.254 as the Gateway address (not IPv6 Gateway).
   b. Under the Global Config for Laptop4, enter 10.10.1.254 as the Gateway address (not IPv6 Gateway).
3. Using the CLI, configure the default gateway for Switch1.
   a. enable
   b. configure terminal
   c. ip default-gateway 10.10.1.254
   d. end
   e. copy run start
4. Using the CLI, configure the default gateway for Switch2.
   a. enable
   b. configure terminal
   c. ip default-gateway 10.10.2.254
   d. end
   e. copy run start

5. Verify that communication for all devices have been restored by running our ping tests on Laptop1. Clear the ARP table before running the ping tests. All ping tests should be successful.
    a. arp -d
    b. ping 10.10.1.2
    c. ping 10.10.1.11
    d. ping 10.10.1.254
    e. ping 10.10.2.3
    f. ping 10.10.2.4
    g. ping 10.10.2.12
    h. ping 10.10.2.254
6. View the ARP table on Laptop1. Note that although Laptop1 can now reach all devices on the network, its ARP table only has information for devices within its own logical IP network. Communication with devices outside of its logical network would go through Router1. Hence, all frames sent to other logical networks would contain the Gig0/0 MAC address of Router1 as the destination MAC address once they are sent on the wire, while the destination IP address contained in those frames would be that of the remote device. When Router1 receives the frames from Laptop1 and forwards them along, it will change the source MAC address to that of its Gig0/1 interface and the destination MAC address to that of the intended host on the 10.10.2.x logical network. The source and destination IP addresses of the frames remain unchanged.