Chapter 7: IP Addressing

CCNA Routing and Switching

Introduction to Networks v6.0

Chapter 7 - Sections & Objectives

- 7.1 IPv4 Network Addresses
- Explain the use of IPv4 addresses to provide connectivity in small to medium-sized business networks
  - Convert between binary and decimal numbering systems.
  - Describe the structure of an IPv4 address including the network portion, the host portion, and the subnet mask.
  - Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses.
  - Explain public, private, and reserved IPv4 addresses.
- 7.2 IPv6 Network Addresses
- Configure IPv6 addresses to provide connectivity in small to medium-sized business networks.
  - Explain the need for IPv6 addressing.
  - Describe the representation of an IPv6 address.
  - Compare types of IPv6 network addresses.
  - Configure global unicast addresses.
  - Describe multicast addresses.

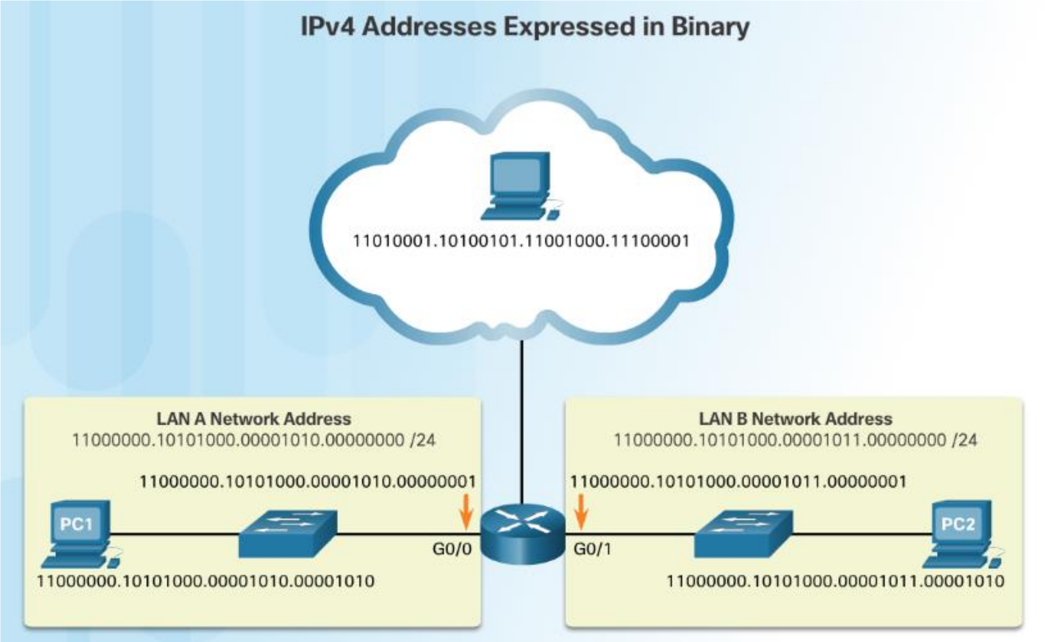
Chapter 7 - Sections & Objectives (Cont.)

- 7.3 Connectivity Verification
- Use common testing utilities to verify and test network connectivity.
  - Explain how ICMP is used to test network connectivity.
  - Use ping and traceroute utilities to test network connectivity.

7.1 IPv4 Network Addresses

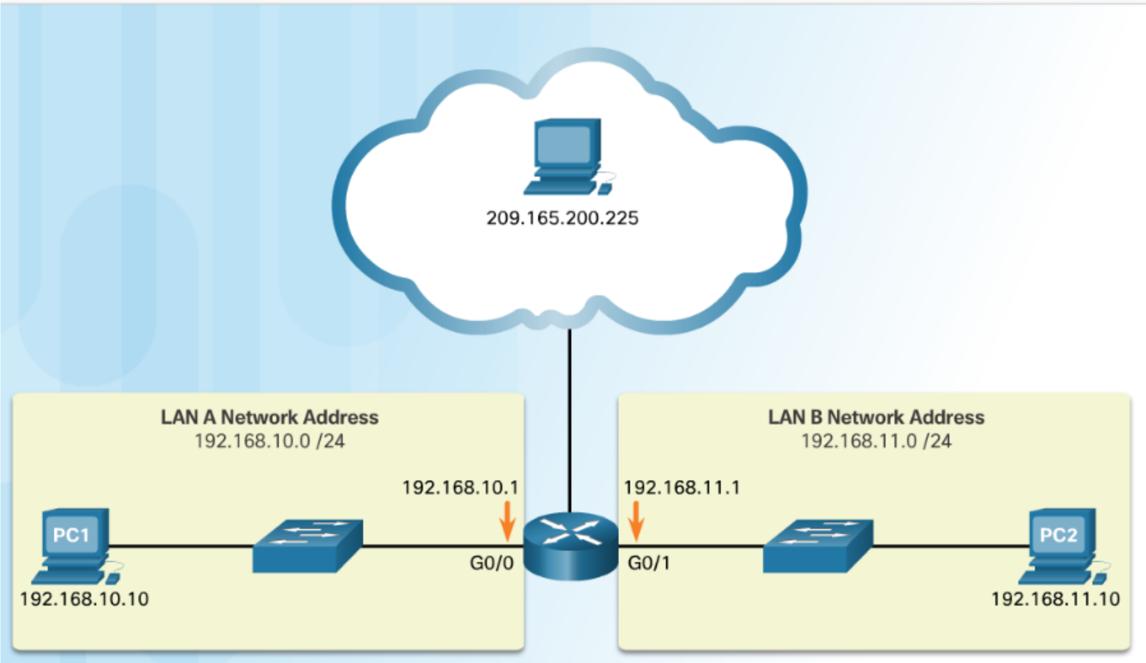
IPv4 Addresses

- Binary numbering system consists of the numbers 0 and 1 called bits
  - IPv4 addresses are expressed in 32 binary bits divided into 4 8-bit octets



IPv4 Addresses (Cont.)

- IPv4 addresses are commonly expressed in dotted decimal notation



Binary and Decimal Conversion

Positional Notation

- The first row identifies the number base or radix. Decimal is 10. Binary is based on 2, therefore radix will be 2
- The 2nd row considers the position of the number starting with 0. These numbers also represent the exponential value that will be used to calculate the positional value (4th row).
- The 3rd row calculates the positional value by taking the radix and raising it by the exponential value of its position. Note: n^0 is always = 1.
- The positional value is listed in the fourth row.

Decimal Positional Notation

Radix	10	10	10	10
Position in Number	3	2	1	0
Calculate	(10^3)	(10^2)	(10^1)	(10^0)
Positional Value	1000	100	10	1

Applying decimal positional notation

	Thousands	Hundreds	Tens	Ones
Positional Value	1000	100	10	1
Decimal Number (1234)	1	2	3	4
Calculate	1 x 1000	2 x 100	3 x 10	4 x 1
Add them up ...	1000	+ 200	+ 30	+ 4
Result	1,234			

Positional Notation (Cont.)

Binary Positional Notation

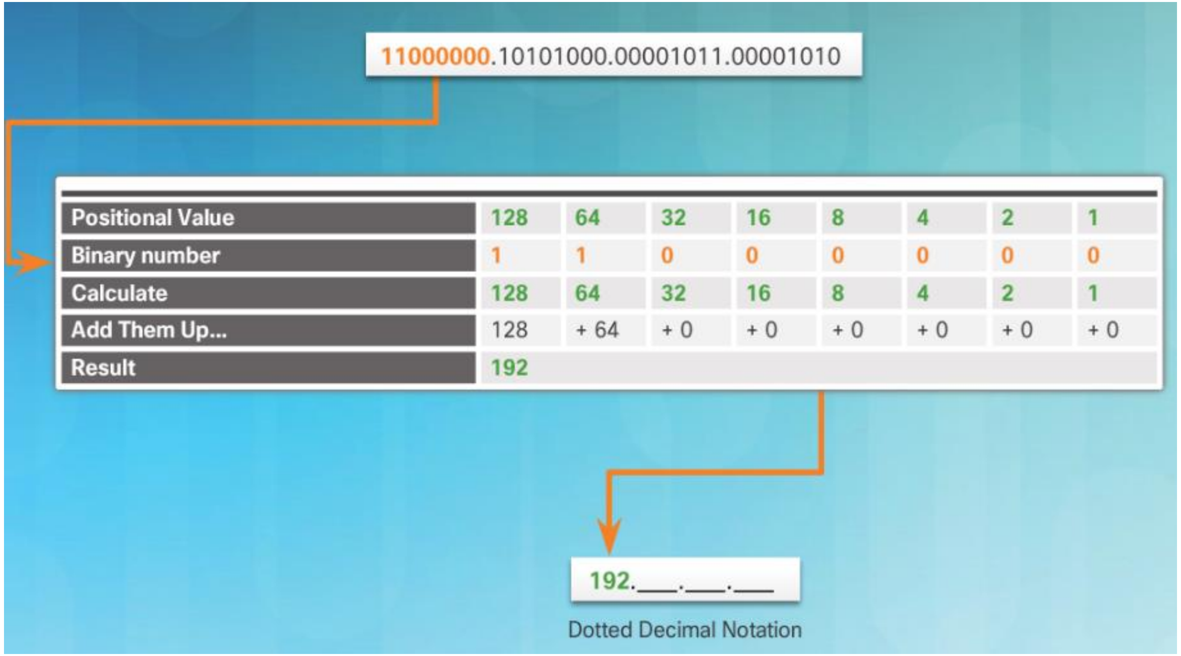
Radix	2	2	2	2	2	2	2	2
Position in Number	7	6	5	4	3	2	1	0
Calculate	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)
Positional Value	128	64	32	16	8	4	2	1

- Applying binary positional notation.

Positional Value	128	64	32	16	8	4	2	1
Binary Number (11000000)	1	1	0	0	0	0	0	0
Calculate	1 x 128	1 x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	0 x 1
Add Them Up ...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	192							

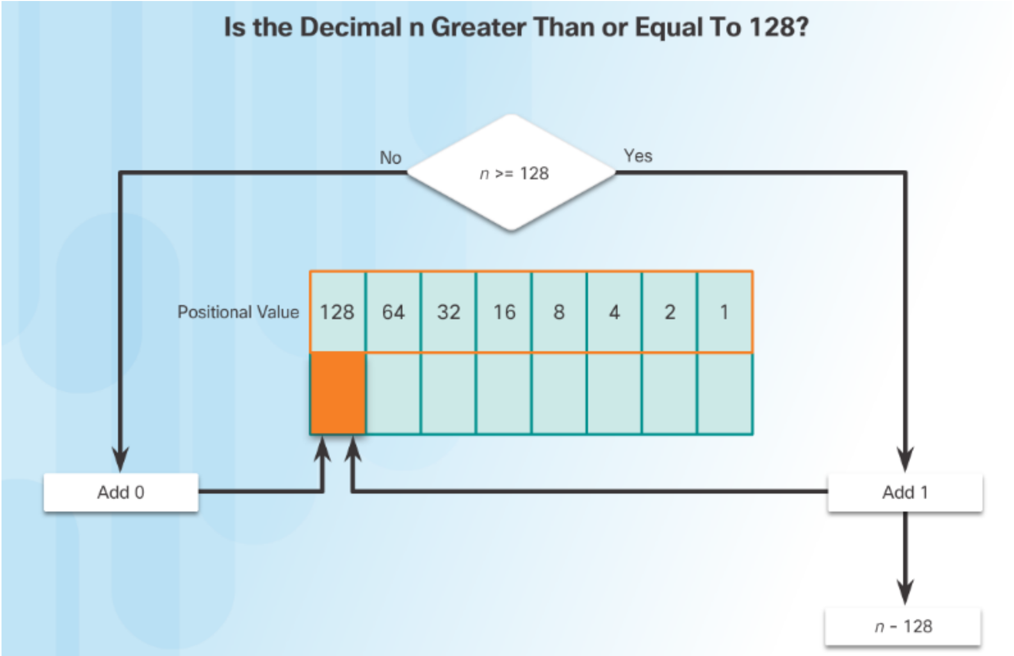
Binary to Decimal Conversion

- To convert a binary IPv4 address to decimal enter the 8-bit binary number of each octet under the positional value of row 1 and then calculate to produce the decimal.

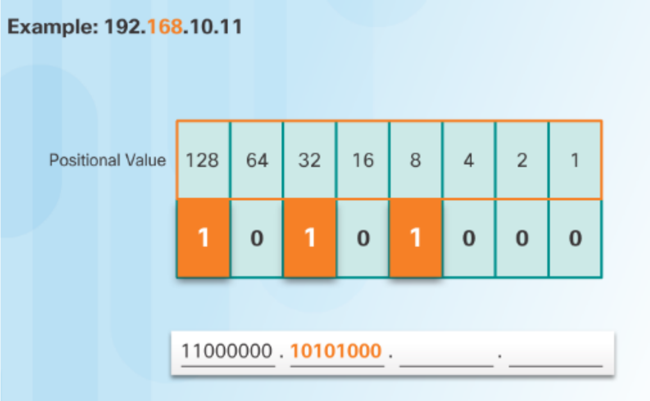


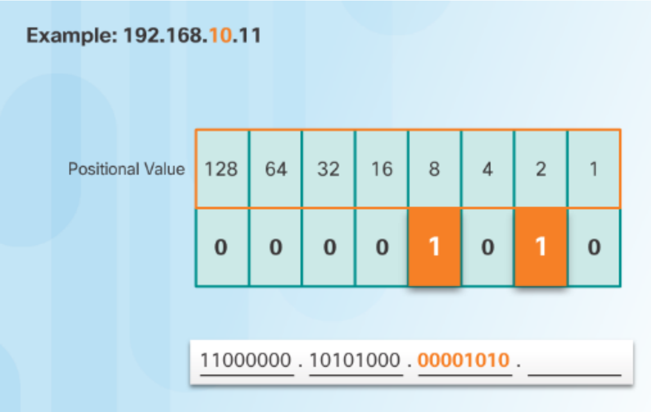
Decimal to Binary Conversion

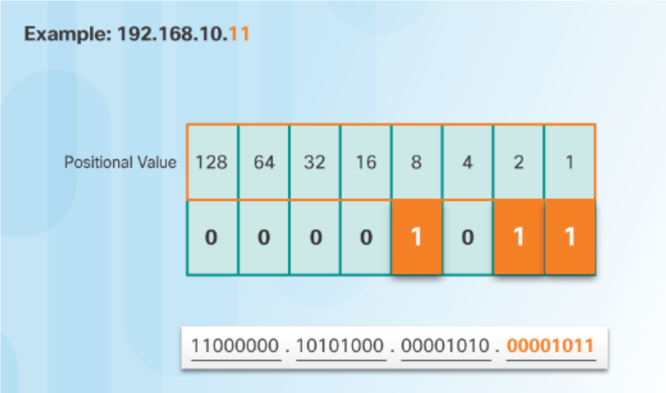
- To convert a decimal IPv4address to binary use the positional chart and check first if the number is greater than the 128 bit. If no a 0 is placed in this position. If yes then a 1 is placed in this position.
- 128 is subtracted from the original number and the remainder is then checked against the next position (64) If it is less than 64 a 0 is placed in this position. If it is greater, a 1 is placed in this position and 64 is subtracted.
- The process repeats until all positional values have been entered.



Decimal to Binary Conversion Examples

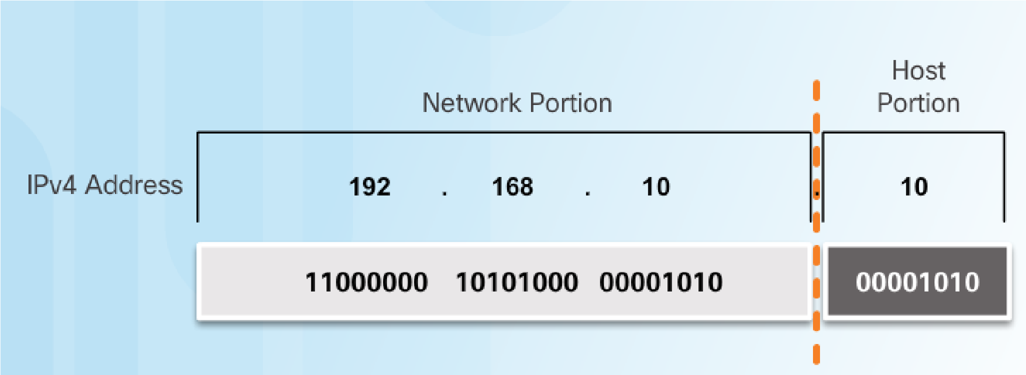






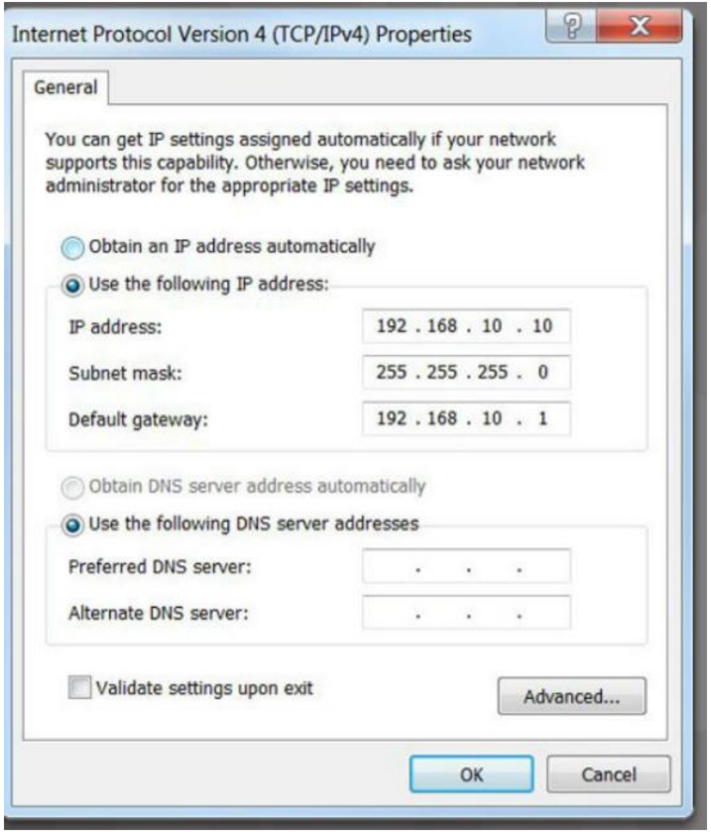
Network and Host Portions

- An IPv4 address is hierarchical.
  - Composed of a Network portion and Host portion.
- All devices on the same network must have the identical network portion.
- The Subnet Mask helps devices identify the network portion and host portion.



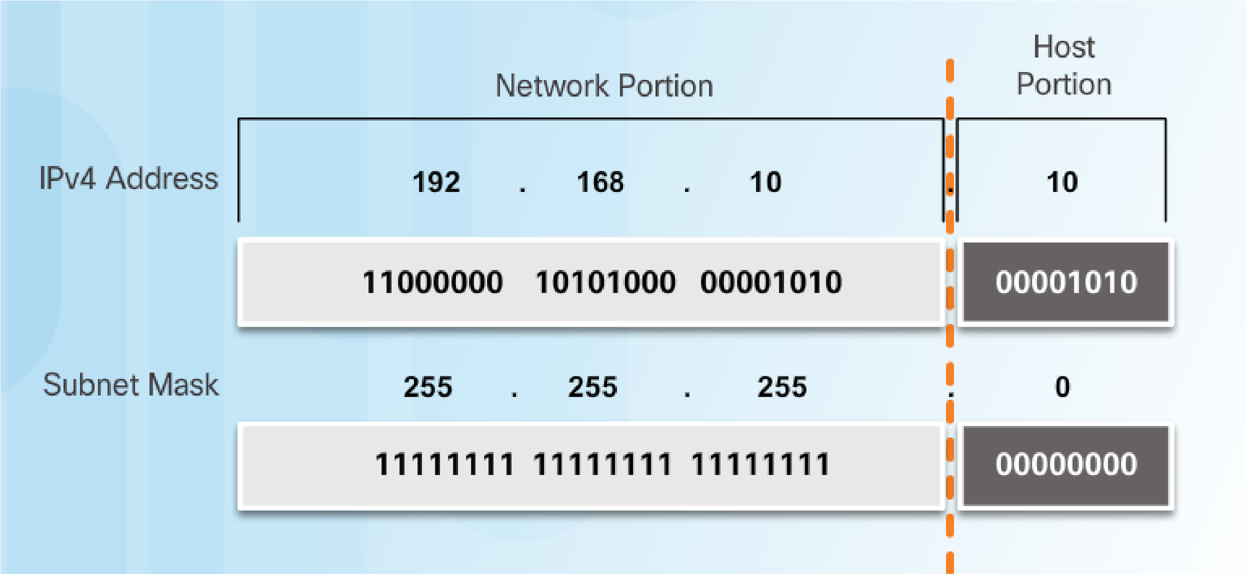
The Subnet Mask

- Three IPv4 addresses must be configured on a host:
  - Unique IPv4 address of the host.
  - Subnet mask - identifies the network/host portion of the IPv4 address.
  - Default gateway -IP address of the local router interface.



The Subnet Mask (Cont.)

- The IPv4 address is compared to the subnet mask bit by bit, from left to right.
- A 1 in the subnet mask indicates that the corresponding bit in the IPv4 address is a network bit.



Logical AND

- A logical AND is one of three basic binary operations used in digital logic.
- Used to determine the Network Address
- The Logical AND of two bits yields the following results:

1 AND 1 = 1
0 AND 1 = 0
0 AND 0 = 0
1 AND 0 = 0

IP Address	192 .	168 .	10 .	10
Binary	11000000	10101000	00001010	00001010
Subnet mask	255 .	255 .	255 .	0
	11111111	11111111	11111111	00000000
AND Results	11000000	10101000	00001010	00000000
Network Address	192 .	168 .	10 .	0

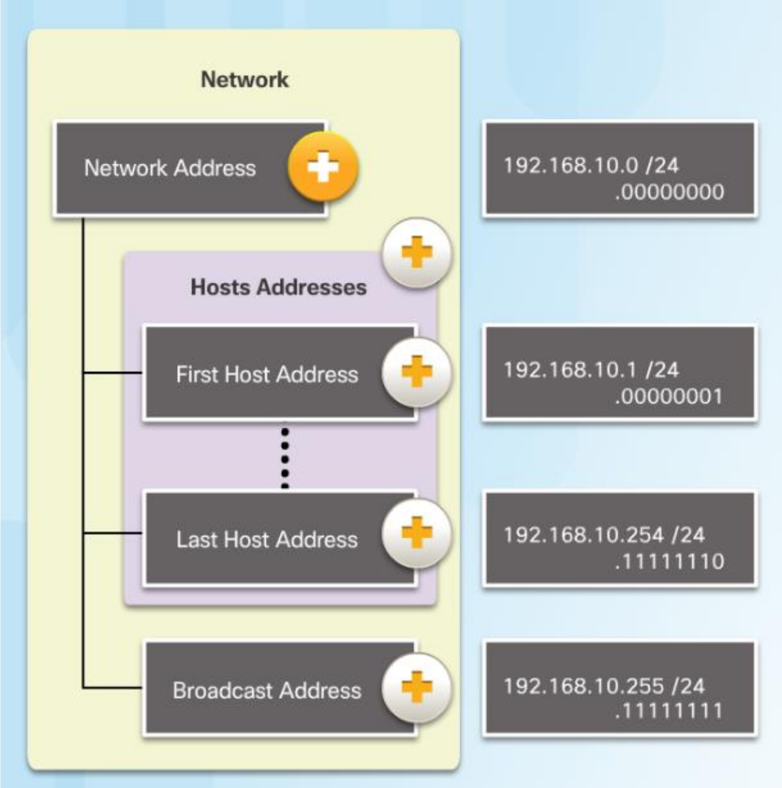
The Prefix Length

Comparing the Subnet Mask and Prefix Length

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

- The Prefix Length:
  - Shorthand method of expressing the subnet mask.
  - Equals the number of bits in the subnet mask set to 1.
  - Written in slash notation, / followed by the number of network bits.

Network, Host, and Broadcast Addresses



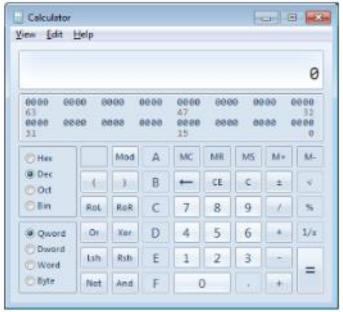
- Types of Addresses in Network 192.168.10.0/24
  - Network Address - host portion is all 0s (.00000000)
  - First Host address - host portion is all 0s and ends with a 1 (.00000001)
  - Last Host address - host portion is all 1s and ends with a 0 (.11111110)
  - Broadcast Address - host portion is all 1s (.11111111)

Lab – Using the Windows Calculator with Network Addresses

Cisco Networking Academy®

Mind Wide Open™

Lab – Using the Windows Calculator with Network Addresses



Objectives

Part 1: Access the Windows Calculator

Part 2: Convert between Numbering Systems

Part 3: Convert Host IPv4 Addresses and Subnet Masks into Binary

Part 4: Determine the Number of Hosts in a Network Using Powers of 2

Part 5: Convert MAC Addresses and IPv6 Addresses to Binary

Background / Scenario

Network technicians use binary, decimal, and hexadecimal numbers when working with computers and networking devices. Microsoft provides a built-in Calculator application as part of the operating system. The Windows 7 version of Calculator includes a Standard view that can be used to perform basic arithmetic tasks such as addition, subtract, multiplication, and division. The Calculator application also has advanced programming, scientific, and statistical capabilities.

In this lab, you will use the Windows 7 Calculator application Programmer view to convert between the binary, decimal, and hexadecimal number systems. You will also use the Scientific view powers function to determine the number of hosts that can be addressed based on the number of host bits available.

Required Resources

- 1 PC (Windows 7 or 8)

Lab – Converting IPv4 Addresses to Binary

Cisco Networking Academy® Mind Wide Open®

Lab – Converting IPv4 Addresses to Binary

Objectives

Part 1: Convert IPv4 Addresses from Dotted Decimal to Binary

Part 2: Use Bitwise ANDing Operation to Determine Network Addresses

Part 3: Apply Network Address Calculations

Background / Scenario

Every IPv4 address is comprised of two parts: a network portion and a host portion. The network portion of an address is the same for all devices that reside in the same network. The host portion identifies a specific host within a given network. The subnet mask is used to determine the network portion of an IP address. Devices on the same network can communicate directly; devices on different networks require an intermediary Layer 3 device, such as a router, to communicate.

To understand the operation of devices on a network, we need to look at addresses the way devices do—in binary notation. To do this, we must convert the dotted decimal form of an IP address and its subnet mask to binary notation. After this has been done, we can use the bitwise ANDing operation to determine the network address.

This lab provides instructions on how to determine the network and host portion of IP addresses by converting addresses and subnet masks from dotted decimal to binary, and then using the bitwise ANDing operation. You will then apply this information to identify addresses in the network.

Part 1: Convert IPv4 Addresses from Dotted Decimal to Binary

In Part 1, you will convert decimal numbers to their binary equivalent. After you have mastered this activity, you will convert IPv4 addresses and subnet masks from dotted decimal to their binary form.

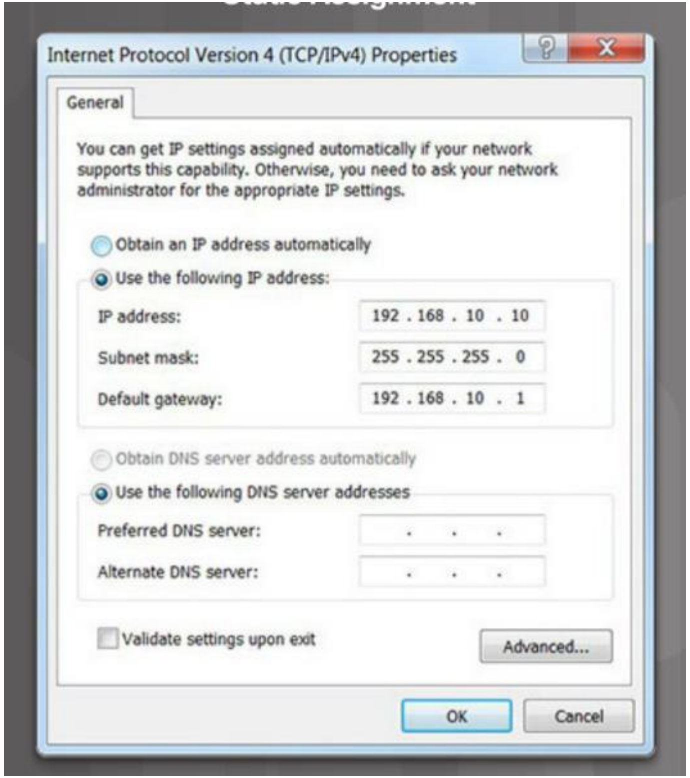
Step 1: Convert decimal numbers to their binary equivalent.

Fill in the following table by converting the decimal number to an 8-bit binary number. The first number has been completed for your reference. Recall that the eight binary bit values in an octet are based on the powers of 2, and from left to right are 128, 64, 32, 16, 8, 4, 2, and 1.

Decimal	Binary
192	11000000
168	

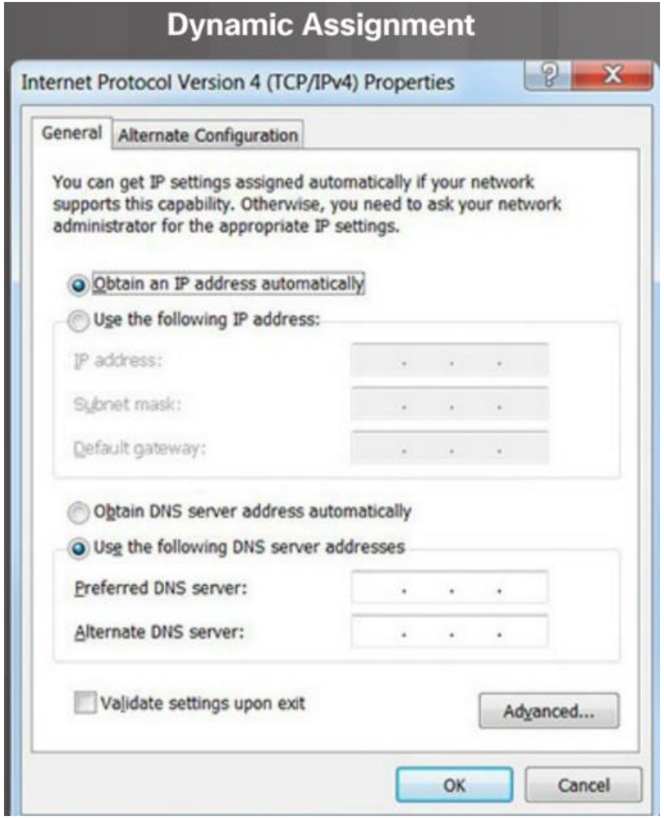
Static IPv4 Address Assignment to a Host

- Some devices like printers, servers and network devices require a fixed IP address.
- Hosts in a small network can also be configured with static addresses.

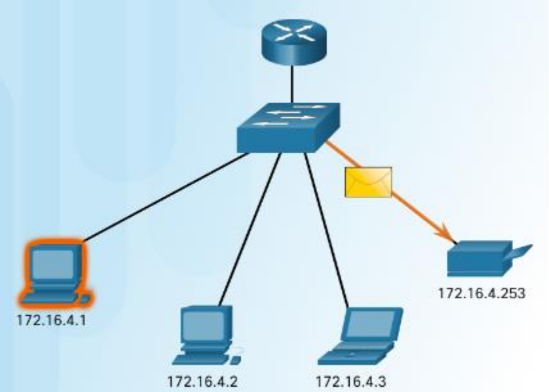


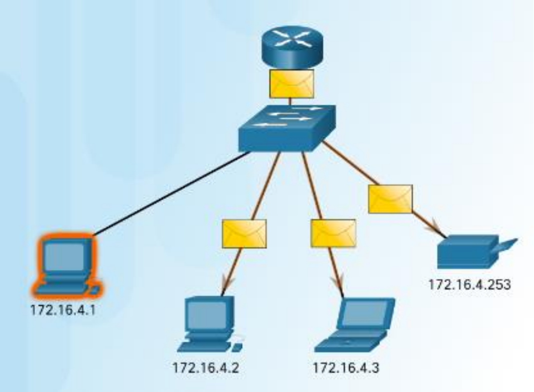
Dynamic IPv4 Address Assignment to a Host

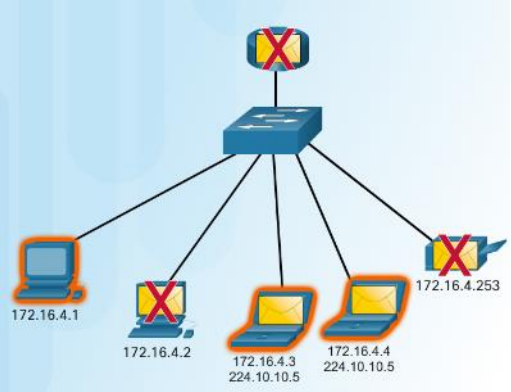
- Most networks use Dynamic Host Configuration Protocol (DHCP) to assign IPv4 addresses dynamically.
- The DHCP server provides an IPv4 address, subnet mask, default gateway, and other configuration information.
- DHCP leases the addresses to hosts for a certain length of time.
- If the host is powered down or taken off the network, the address is returned to the pool for reuse.



IPv4 Communication



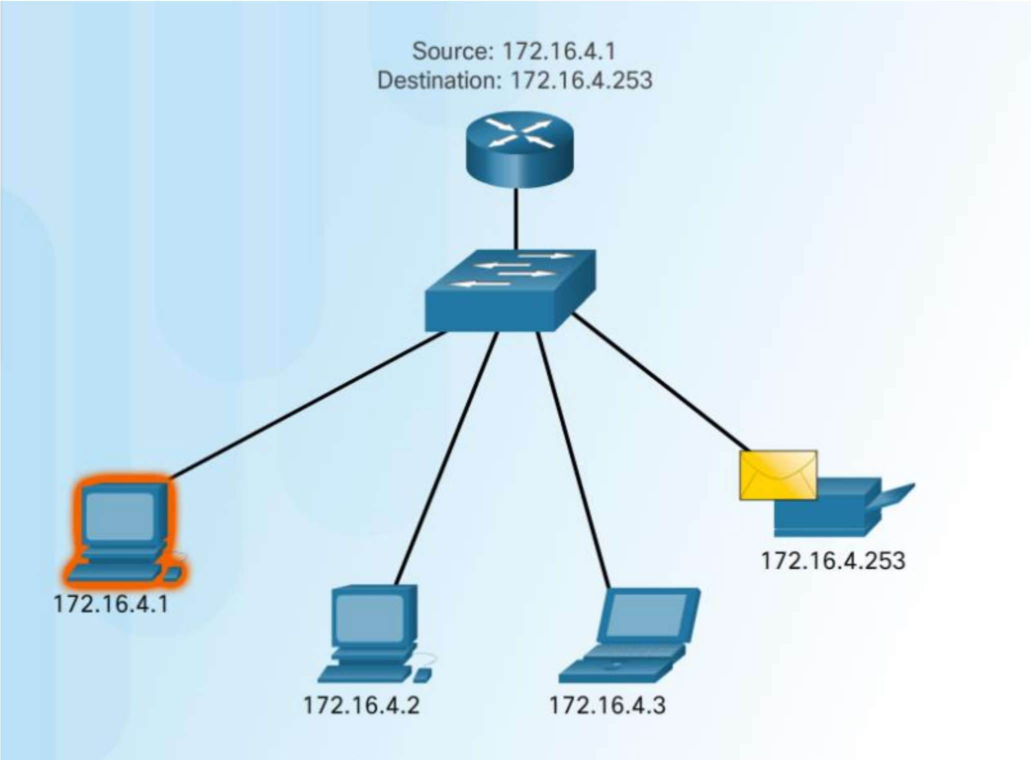




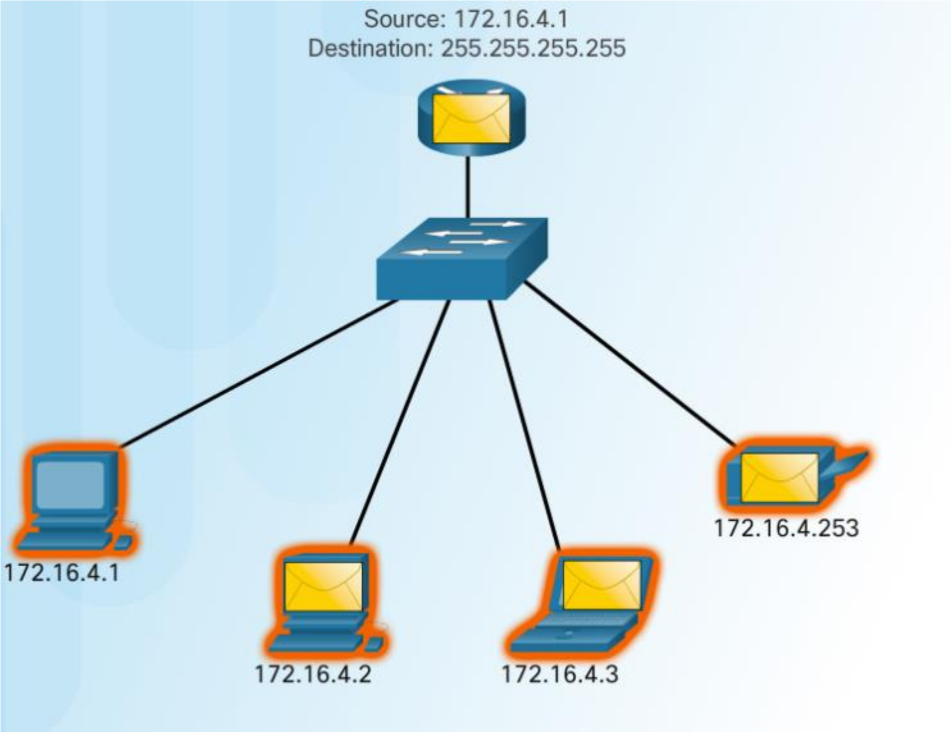
- Unicast – one to one communication.
- Broadcast– one to all.
- Multicast – one to a select group.

Unicast Transmission

- Unicast – one to one communication.
  - Use the address of the destination device as the destination address.

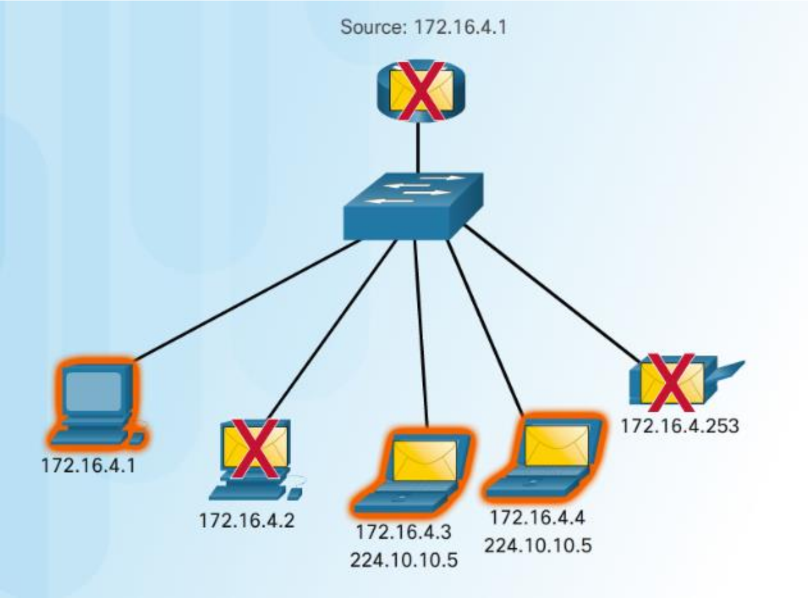


Broadcast Transmission



- Broadcast– one to all
  - Message sent to everyone in the LAN (broadcast domain.)
  - destination IPv4 address has all ones (1s) in the host portion.

Multicast Transmission



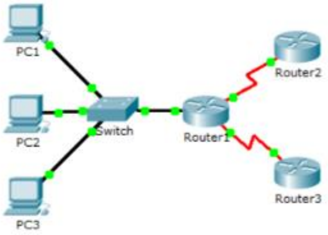
- Multicast– one to a select group.
  - 224.0.0.0 to 239.255.255.255 addresses reserved for multicast.
  - routing protocols use multicast transmission to exchange routing information.

Packet Tracer – Investigate Unicast, Broadcast, and Multicast Traffic

Cisco Networking Academy® Mind Wide Open®

Packet Tracer - Investigate Unicast, Broadcast, and Multicast Traffic

Topology



Objectives

Part 1: Generate Unicast Traffic

Part 2: Generate Broadcast Traffic

Part 3: Investigate Multicast Traffic

Background / Scenario

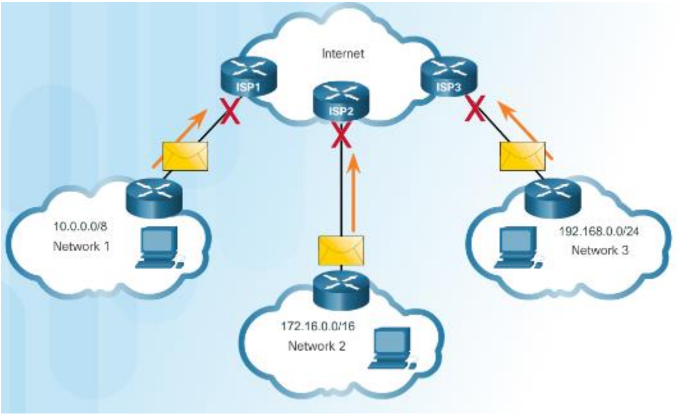
This activity will examine unicast, broadcast, and multicast behavior. Most traffic in a network is unicast. When a PC sends an ICMP echo request to a remote router, the source address in the IP packet header is the IP address of the sending PC. The destination address in the IP packet header is the IP address of the interface on the remote router. The packet is sent only to the intended destination.

Using the **ping** command or the Add Complex PDU feature of Packet Tracer, you can directly ping broadcast addresses to view broadcast traffic.

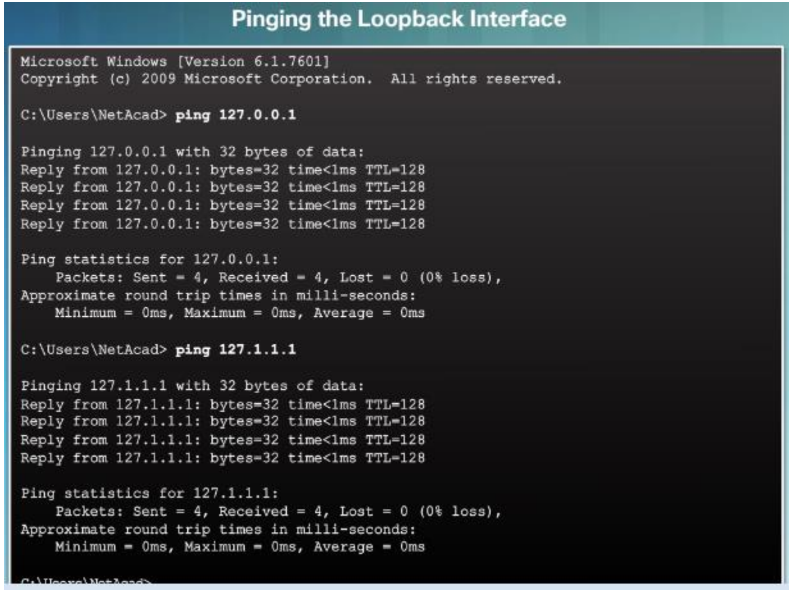
For multicast traffic, you will view EIGRP traffic. EIGRP is used by Cisco routers to exchange routing information between routers. Routers using EIGRP send packets to multicast address 224.0.0.10, which represents the group of EIGRP routers. Although these packets are received by other devices, they are dropped at Layer 3 by all devices except EIGRP routers, with no other processing required.

Public and Private IPv4 Addresses

- Private Addresses
  - Not routable
  - Introduced in mid 1990s due to depletion of IPv4 addresses
  - Used only in internal networks.
  - Must be translated to a public IPv4 to be routable.
  - Defined by RFC 1918
- Private Address Blocks
  - 10.0.0.0 /8 or 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 /12 or 172.16.0.0 to 172.31.255.255192.168.0.0 /16
  - 192.168.0.0 to 192.168.255.255



Special User IPv4 Addresses



- Loopback addresses (127.0.0.0 /8 or 127.0.0.1)
  - Used on a host to test if the TCP/IP configuration is operational.
- Link-Local addresses (169.254.0.0 /16 or 169.254.0.1)
  - Commonly known as Automatic Private IP Addressing (APIPA) addresses.
  - Used by Windows client to self configure if no DHCP server available.
- TEST-NET addresses (192.0.2.0/24 or 192.0.2.0 to 192.0.2.255)
  - Used for teaching and learning.

Legacy Classful Addressing

Class A Specifics	
Address Block	0.0.0.0 - 127.0.0.0
Default Subnet Mask	/8 (255.0.0.0)
Maximum Number of Networks	128
Number of Host per Network	16,777,214
High order bit	0xxxxxxx.___.___.___

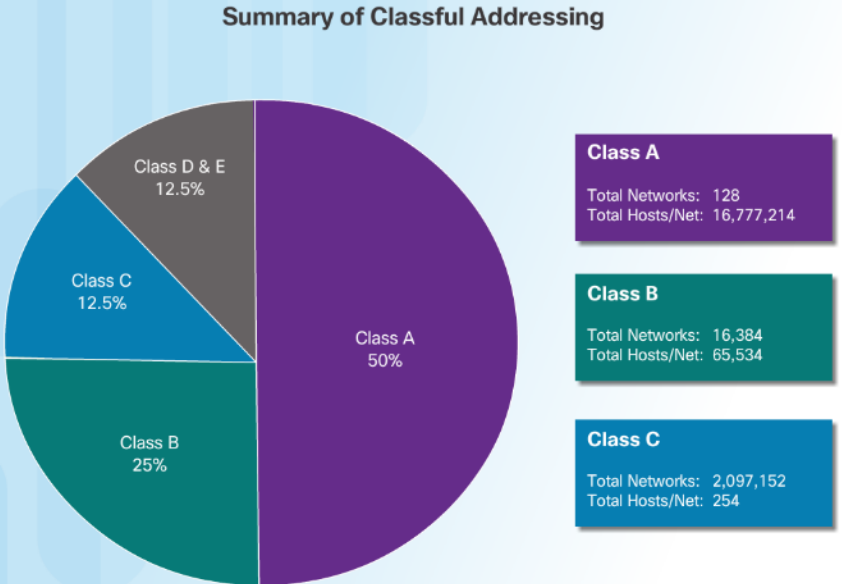
* 0.0.0.0 and 127.0.0.0 are reserved and cannot be assigned

Class B Specifics	
Address Block	128.0.0.0 - 191.255.0.0
Default Subnet Mask	/16 (255.255.0.0)
Maximum Number of Networks	16,384
Number of Host per Network	65,534
High order bit	10xxxxxx.___.___.___

Class C Specifics	
Address Block	192.0.0.0 - 223.255.255.0
Default Subnet Mask	/24 (255.255.255.0)
Maximum Number of Networks	2,097,152
Number of Host per Network	254
High order bit	110xxxxx.___.___.___

- In 1981, Internet IPv4 addresses were assigned using classful addressing (RFC 790)
- Network addresses were based on 3 classes:
  - **Class A** (0.0.0.0/8 to 127.0.0.0/8) – Designed to support extremely large networks with more than 16 million host addresses.
  - **Class B** (128.0.0.0 /16 – 191.255.0.0 /16) – Designed to support the needs of moderate to large size networks up to approximately 65,000 host addresses.
  - **Class C** (192.0.0.0 /24 – 223.255.255.0 /24) – Designed to support small networks with a maximum of 254 hosts.

Classless Addressing



- Classful Addressing wasted addresses and exhausted the availability of IPv4 addresses.
- Classless Addressing Introduced in the 1990s
  - Classless Inter-Domain Routing (CIDR, pronounced “cider”)
  - Allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B, or C.

Assignment of IP Addresses

- The following organizations manage and maintain IPv4 and IPv6 addresses for the various regions.
  - American Registry for Internet Numbers (ARIN)- North America.
  - Réseaux IP Europeans (RIPE) - Europe, the Middle East, and Central Asia
  - Asia Pacific Network Information Centre (APNIC) - Asia and Pacific regions
  - African Network Information Centre (AfriNIC) – Africa
  - Regional Latin-American and Caribbean IP Address Registry (LACNIC) - Latin America and some Caribbean islands

Lab – Identifying IPv4 Addresses

Cisco Networking Academy® Mind Wide Open™

Lab– Identifying IPv4 Addresses

Objectives

Part 1: Identify IPv4 Addresses

Part 2: Classify IPv4 Addresses

Background / Scenario

In this lab, you will examine the structure of Internet Protocol version 4 (IPv4) addresses. You will identify the various types of IPv4 addresses and the components that help comprise the address, such as network portion, host portion, and subnet mask. Types of addresses covered include public, private, unicast, and multicast.

Required Resources

- Device with Internet access
- Optional: IPv4 address calculator

Part 1: Identify IPv4 Addresses

In Part 1, you will be given several examples of IPv4 addresses and will complete tables with appropriate information.

Step 1: Analyze the table shown below and identify the network portion and host portion of the given IPv4 addresses.

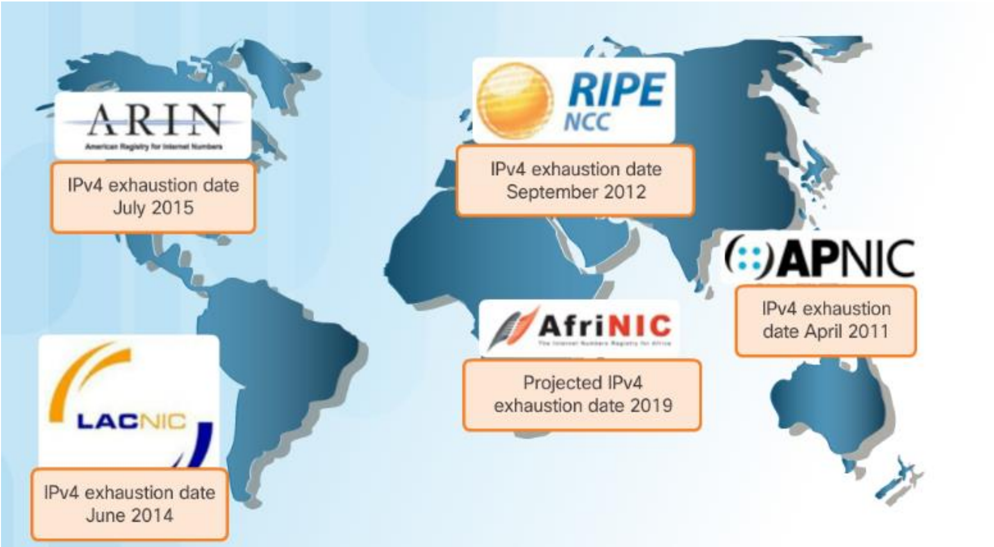
The first two rows show examples of how the table should be completed.

Key for table:
N = all 8 bits for an octet are in the network portion of the address
n = a bit in the network portion of the address
H = all 8 bits for an octet are in the host portion of the address
h = a bit in the host portion of the address

IP Address/Prefix	Network/Host N,n = Network, H,h = Host	Subnet Mask	Network Address
192.168.10.10/24	N.N.N.H	255.255.255.0	192.168.10.0
10.101.99.17/23	N.N.nnnnnnnh.H	255.255.254.0	10.101.98.0
209.165.200.227/27			
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
[illegible]			

7.2 IPv6 Network Addresses

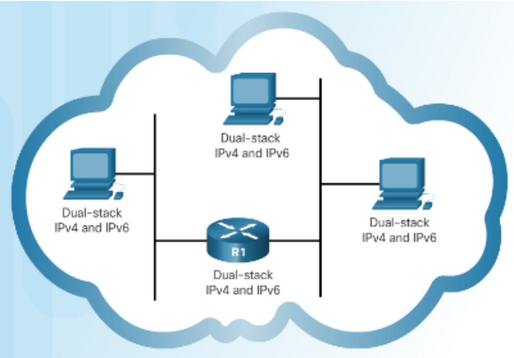
The Need for IPv6

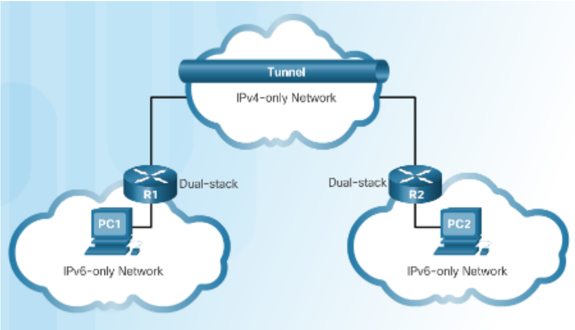


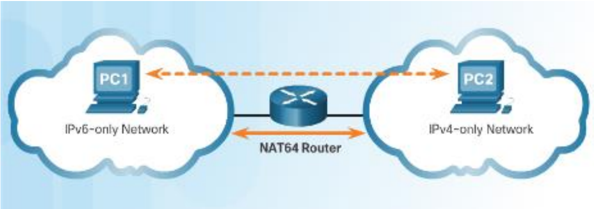
- IPv6 versus IPv4:
  - Has a larger 128-bit address space
  - 340 undecillion addresses
  - Solves limitations with IPv4
  - Adds enhancement like address auto-configuration.
- Why IPv6 is needed:
  - Rapidly increasing Internet population
  - Depletion of IPv4
  - Issues with NAT
  - Internet of Things

IPv4 and IPv6 Coexistence

- Migration from IPv4 to IPv6 Techniques







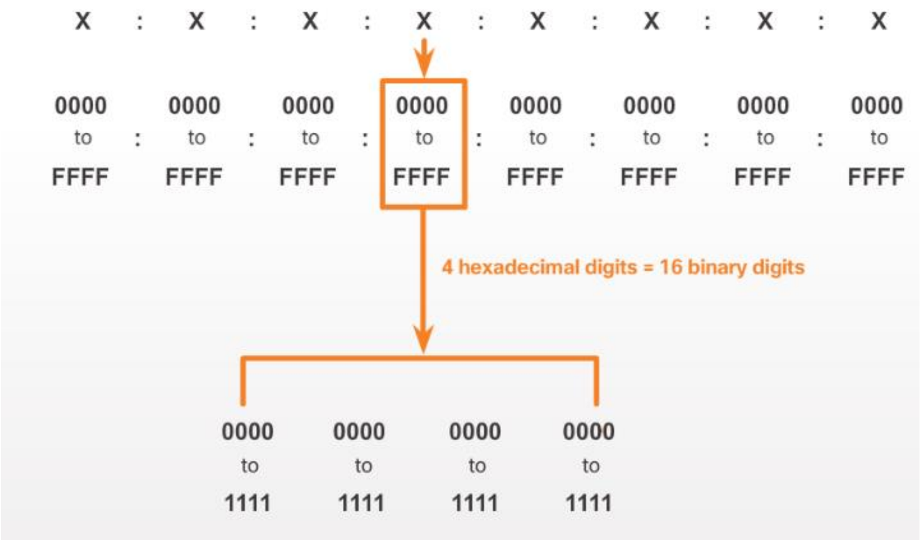
Dual stack - Devices run both IPv4 and IPv6 protocol stacks simultaneously.

Tunneling - The IPv6 packet is encapsulated inside an IPv4 packet.

Translation - Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4 devices.

IPv6 Address Representation

- IPv6 Addresses:
  - 128 bits in length
  - Every 4 bits is represented by a single hexadecimal digit
  - Hextet - unofficial term referring to a segment of 16 bits or four hexadecimal values.



IPv6 Address Representation (Cont.)

- Preferred format for IPv6 representation

2001	:	0DB8	:	0000	:	1111	:	0000	:	0000	:	0000	:	0200
2001	:	0DB8	:	0000	:	00A3	:	ABCD	:	0000	:	0000	:	1234
2001	:	0DB8	:	000A	:	0001	:	0000	:	0000	:	0000	:	0100
2001	:	0DB8	:	AAAA	:	0001	:	0000	:	0000	:	0000	:	0200
FE80	:	0000	:	0000	:	0000	:	0123	:	4567	:	89AB	:	CDEF
FE80	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
FF02	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
FF02	:	0000	:	0000	:	0000	:	0000	:	0001	:	FF00	:	0200
0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000

Rule 1 – Omit Leading 0s

- In order to reduce or compress IPv6
  - First rule is to omit leading zeros in any hextet.

Preferred	2001:0DB8:0000:1111:0000:0000:0000:0200
No leading 0s	2001:DB8:0:1111:0:0:0:200

Preferred	2001:0DB8:000A:1000:0000:0000:0000:0100
No leading 0s	2001:DB8:A:1000:0:0:0:100

Preferred	0000:0000:0000:0000:0000:0000:0000:0000
No leading 0s	0:0:0:0:0:0:0:0

Rule 2 – Omit All 0 Segments

- Rule 2 – Omit All 0 Segments
  - A double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0s.

Preferred	2001:0DB8:0000:0000:ABCD:0000:0000:0100
No leading 0s	2001: DB8: 0: 0:ABCD: 0: 0: 100
Compressed	2001:DB8::ABCD:0:0:100
or	
Compressed	2001:DB8:0:0:ABCD::100

Only one :: may be used.

Rule 2 – Omit All 0 Segments (Cont.)

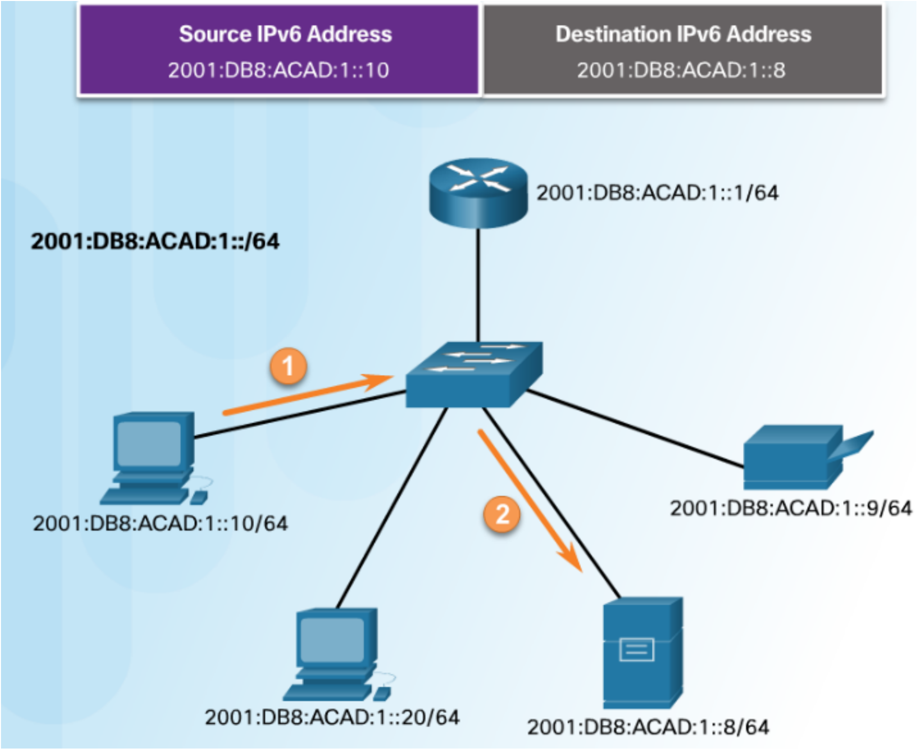
- Rule 2 – Omit All 0 Segments
  - A double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0s.

Preferred	FF02:0000:0000:0000:0000:0000:0000:0001
No leading 0s	FF02:0:0:0:0:0:0:1
Compressed	FF02::1

Preferred	0000:0000:0000:0000:0000:0000:0000:0000
No leading 0s	0:0:0:0:0:0:0:0
Compressed	::

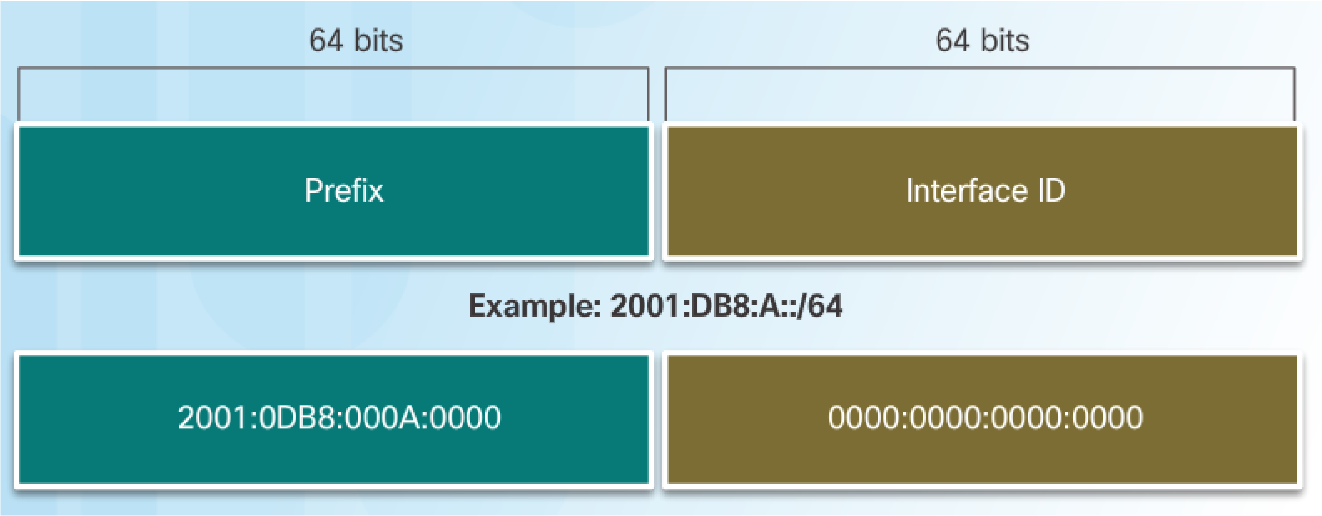
IPv6 Address Types

- Three types of IPv6 addresses:
  - **Unicast**- Single source IPv6 address.
  - **Multicast** - An IPv6 multicast address is used to send a single IPv6 packet to multiple destinations.
  - **Anycast** - An IPv6 anycast address is any IPv6 unicast address that can be assigned to multiple devices.



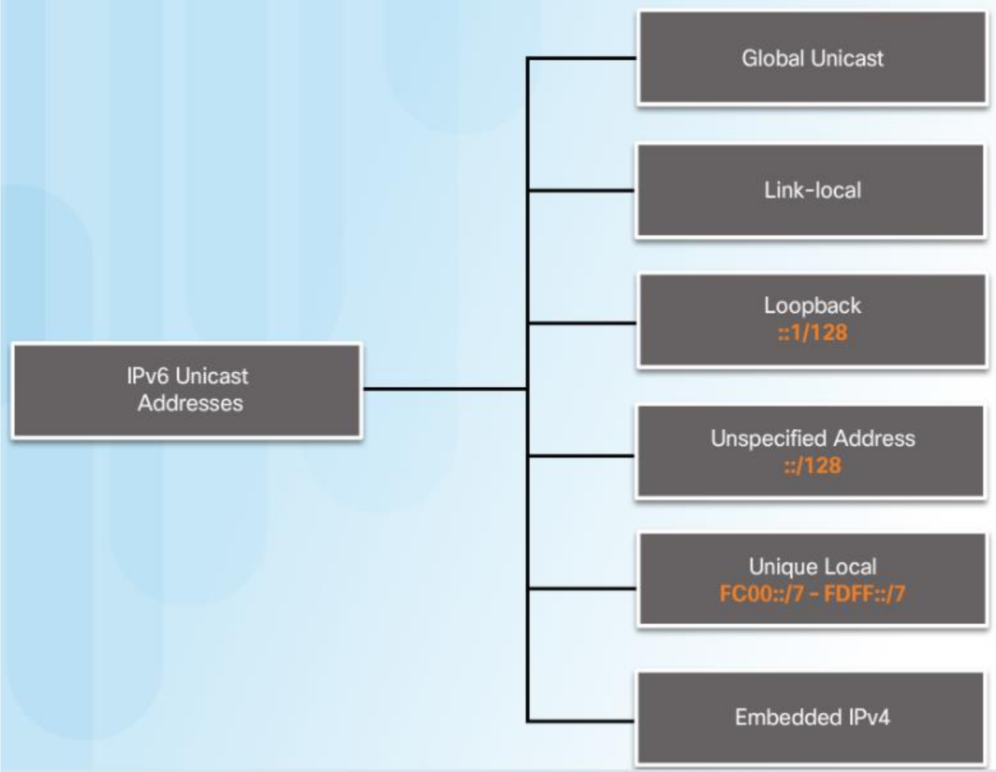
IPv6 Prefix Length

- The IPv6 prefix length is used to indicate the network portion of an IPv6 address:
  - The prefix length can range from 0 to 128.
  - Typical IPv6 prefix length for most LANs is /64



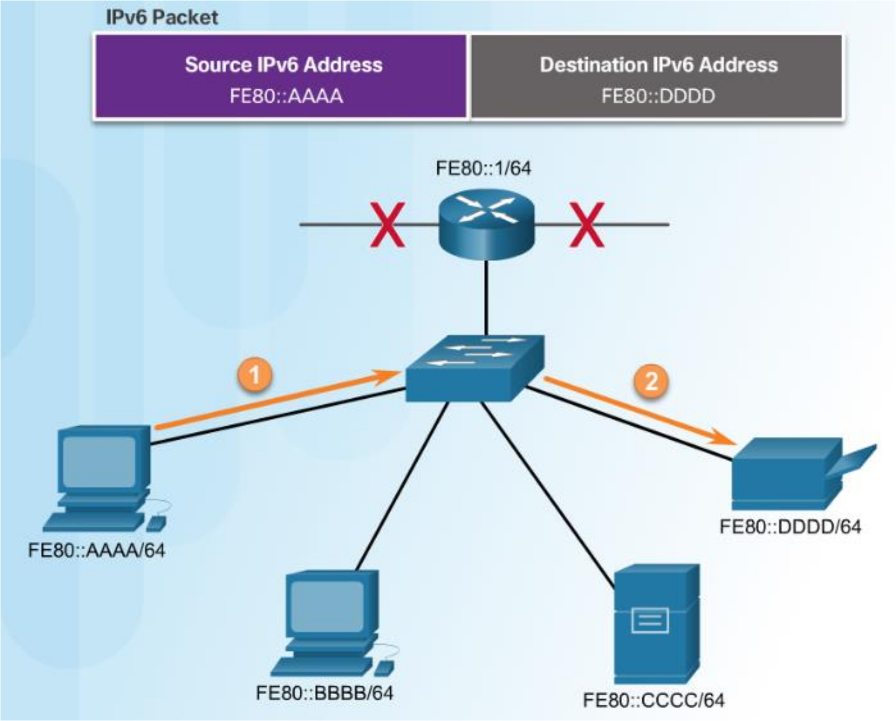
IPv6 Unicast Addresses

- **Global Unicast** - These are globally unique, Internet routable addresses.
- **Link-local** - used to communicate with other devices on the same local link. Confined to a single link.
- **Unique Local** - used for local addressing within a site or between a limited number of sites.



IPv6 Link-Local Unicast Addresses

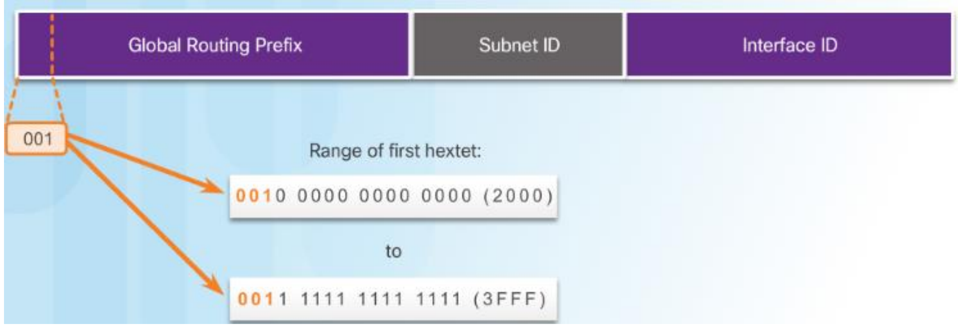
- IPv6 link-local addresses:
  - Enable a device to communicate with other IPv6-enabled devices on the same link only.
    - Are created even if the device has not been assigned a global unicast IPv6 address.
  - Are in the FE80::/10 range.

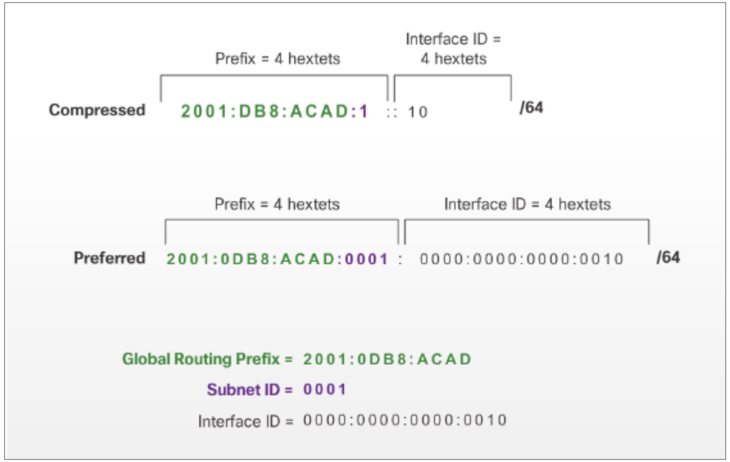


Note: Typically, it is the link-local address of the router that is used as the default gateway for other devices on the link.

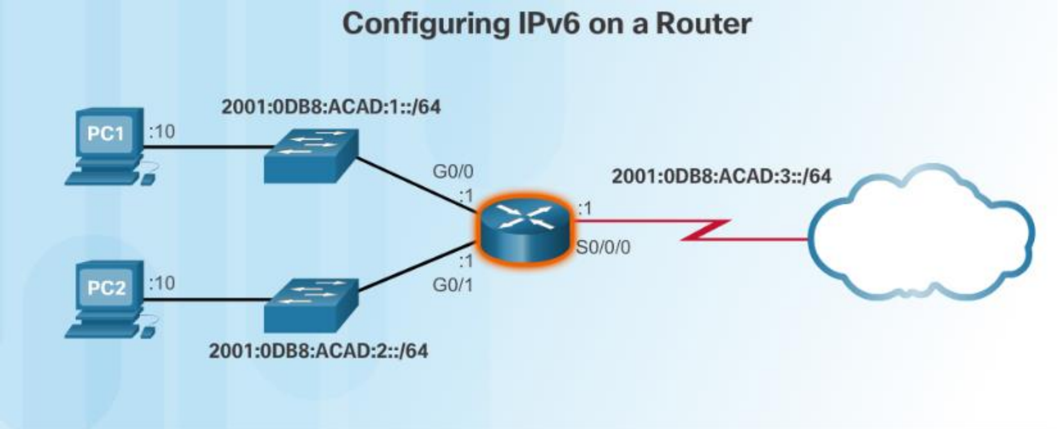
Structure of an IPv6 Global Unicast Address

- Currently, only global unicast addresses with the first three bits of 001 or 2000::/3 are being assigned
- A global unicast address has three parts:
  - **Global routing prefix** - network, portion of the address that is assigned by the provider. Typically /48.
  - **Subnet ID –** Used to subnet within an organization.
  - **Interface ID** - equivalent to the host portion of an IPv4 address.





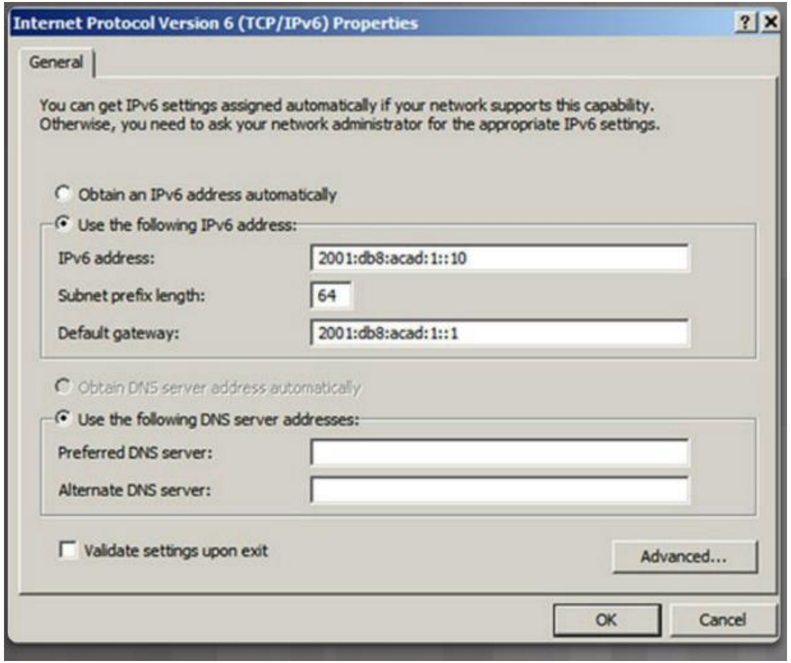
Static Configuration of a Global Unicast Address




```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# clock rate 56000
R1(config-if)# no shutdown
```

- Router Configuration:
  - Similar commands to IPv4, replace IPv4 with IPv6
  - Command to configure andIPv6 global unicast on an interface is **ipv6 address** *ipv6-address/prefix-length*

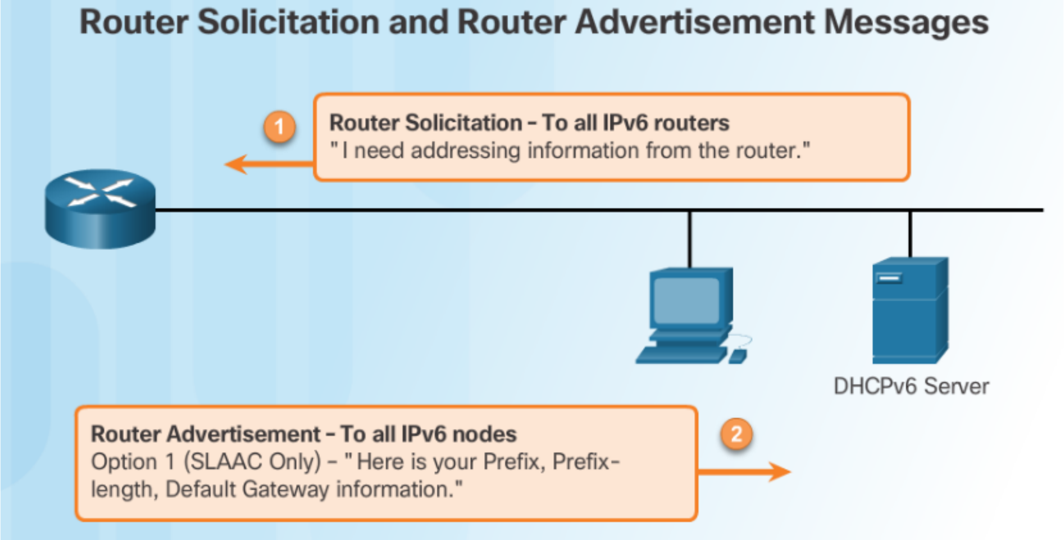
Static Configuration of a Global Unicast Address (Cont.)



- Host Configuration:
  - Manually configuring the IPv6 address on a host is similar to configuring an IPv4 address
  - Default gateway address can be configured to match the link-local or global unicast address of the Gigabit Ethernet interface.
- Dynamic assignment of IPv6 addresses:
  - Stateless Address Autoconfiguration (SLAAC)
  - Stateful DHCPv6

Dynamic Configuration - SLAAC

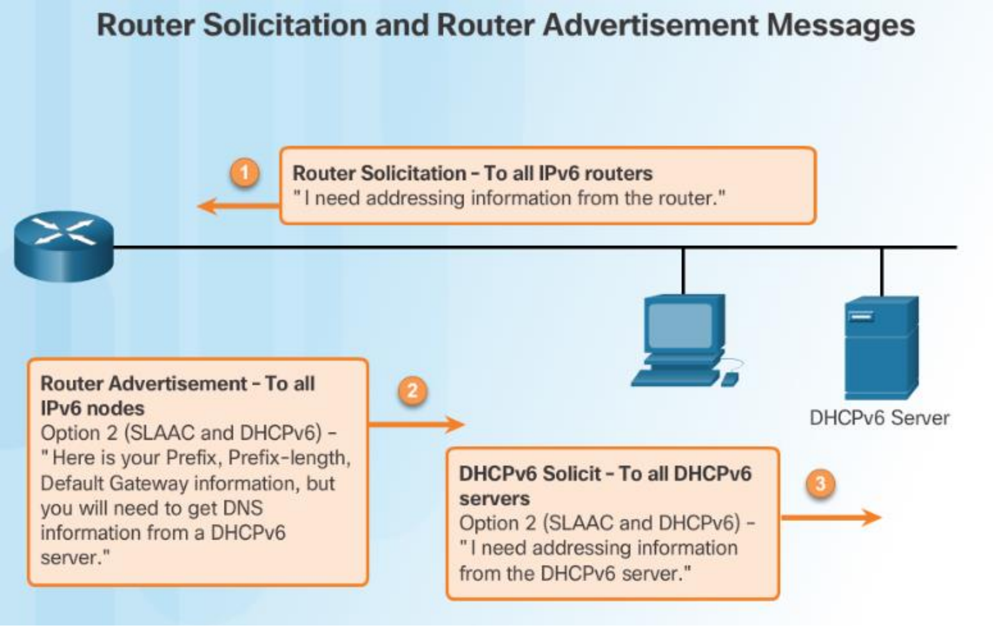
- Stateless Address Autoconfiguration (SLAAC):
  - A device can obtain its prefix, prefix length, default gateway address, and other information from an IPv6 router.
  - Uses the local router's ICMPv6 Router Advertisement (RA) messages
- ICMPv6 RA messages sent every 200 seconds to all IPv6-enabled devices on the network.



Option 1 (SLAAC Only) – "I'm everything you need (Prefix, Prefix-length, Default Gateway)"
Option 2 (SLAAC and DHCPv6) – "Here is my information but you need to get other information such as DNS addresses from a DHCPv6 server."
Option 3 (DHCPv6 Only) – "I can't help you. Ask a DHCPv6 server for all your information."

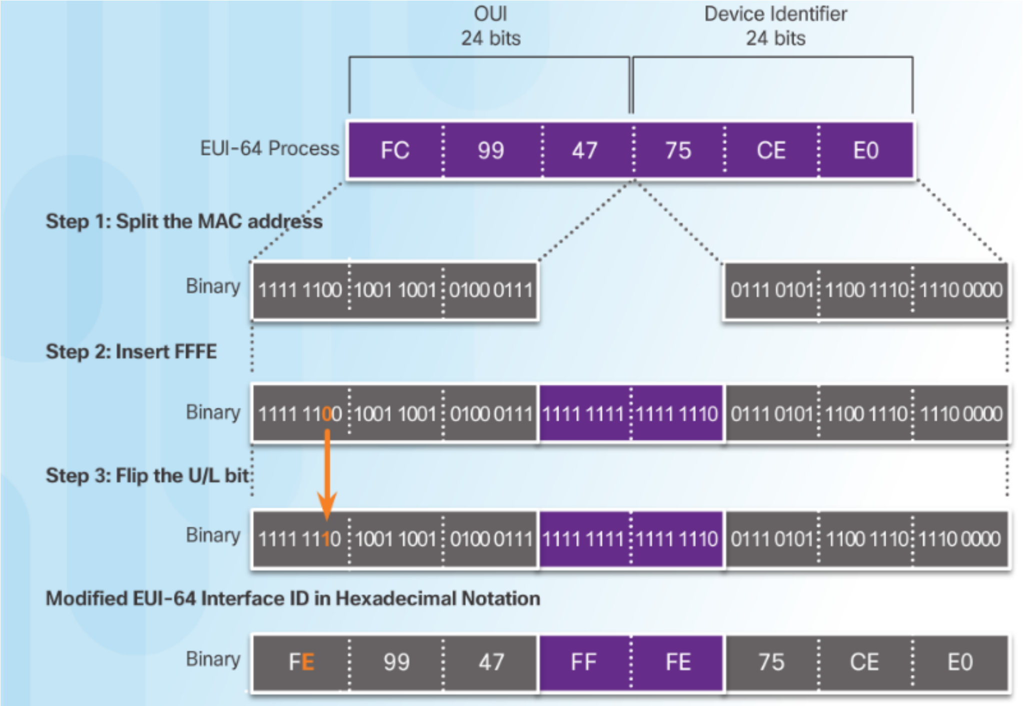
Dynamic Configuration – DHCPv6

- The RA Option 1: SLAAC only (this is the default)
- RA Option 2: SLAAC and Stateless DHCPv6:
  - Uses SLAAC for IPv6 global unicast address and default gateway.
  - Uses a stateless DHCPv6 server for other information.
- RA Option 3: Stateful DHCPv6
  - Uses the Routers link-local address for the default gateway.
  - Uses DHCPv6 for all other information.



EUI-64 Process and Randomly Generated

- When the RA message is SLAAC or SLAAC with stateless DHCPv6, the client must generate its own Interface ID
  - The Interface ID can be created using the EUI-64 process or a randomly generated 64-bit number
- An EUI-64 Interface ID is represented in binary and is made up of three parts:
  - 24-bit OUI from the client MAC address, but the 7th bit (the Universally/Locally (U/L) bit) is reversed.
  - The inserted 16-bit value FFFE (in hexadecimal).
  - 24-bit Device Identifier from the client MAC address.



EUI-64 Process and Randomly Generated (Cont.)

- Randomly Generated Interface IDs
  - Windows uses a randomly generated Interface ID

From RA Message

Random 64-bit number

```
PCB> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  :
   IPv6 Address. . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway   . . . . . . . : fe80::1
```

Dynamic Link-Local Addresses

- Link-local address can be established dynamically or configured manually.
- Cisco IOS routers use EUI-64 to generate the Interface ID for all link-local address on IPv6 interfaces.
- Drawback to using the dynamically assigned link-local address is the long interface ID, therefore they are often configured statically.

```
R1# show interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
<Output Omitted>

R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
R1#
```

Link-local Addresses Using EUI-64

Static Link-Local Addresses

- Manual Configuration of the link-local address allows the creation of a simple, easy to remember address.

```
Router(config-if)#
ipv6 address link-local-address link-local
```

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#
```

Verifying IPv6 Address Configuration

- The commands to verify IPv6 configuration are similar to IPv4
  - show ipv6 interface brief
  - show ipv6 route
- The ping command for IPv6 is identical to the command used with IPv4, except that an IPv6 address is used.

```
R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
R1#
```

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static


C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)
R1#
```

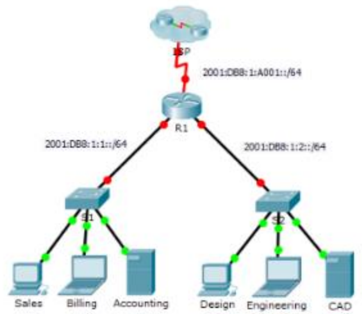
IPv6 Unicast Addresses

Packet Tracer – Configuring IPv6 Addressing

Cisco Networking Academy Mind Wide Open

Packet Tracer - Configuring IPv6 Addressing

Topology



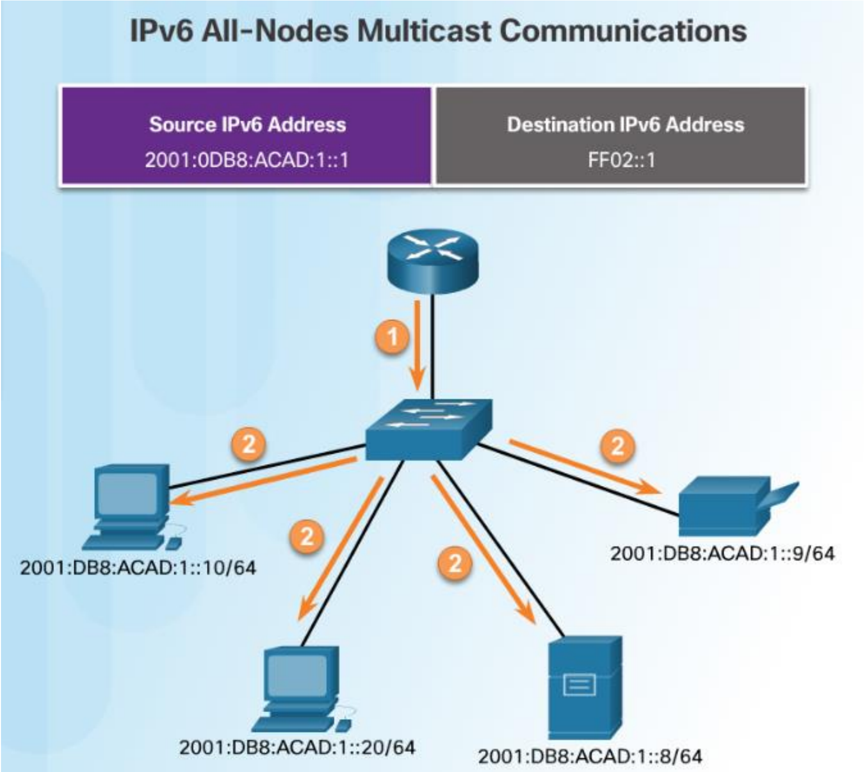
Addressing Table

Device	Interface	IPv6 Address/Prefix	Default Gateway
R1	G0/0	2001:DB8:1:1::1/64	N/A
	G0/1	2001:DB8:1:2::1/64	N/A
	S0/0/0	2001:DB8:1:A001::2/64	N/A
	Link-local	FE80::1	N/A
Sales	NIC	2001:DB8:1:1::2/64	FE80::1
Billing	NIC	2001:DB8:1:1::3/64	FE80::1
Accounting	NIC	2001:DB8:1:1::4/64	FE80::1
Design	NIC	2001:DB8:1:2::2/64	FE80::1
Engineering	NIC	2001:DB8:1:2::3/64	FE80::1
CAD	NIC	2001:DB8:1:2::4/64	FE80::1

Objectives

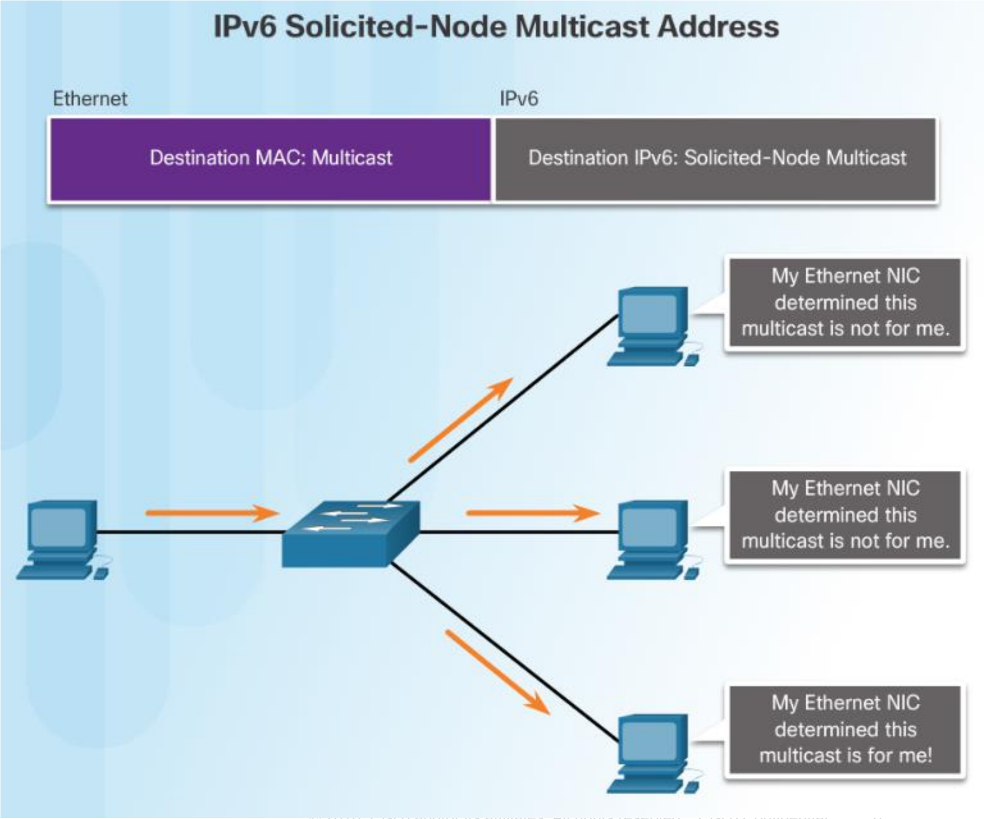
Assigned IPv6 Multicast Addresses

- There are two types of IPv6 multicast addresses:
  - Assigned multicast - reserved multicast addresses for predefined groups of devices
  - Solicited node multicast
- Two common IPv6 assigned multicast groups:
  - FF02::1 All-nodes multicast group – This is a multicast group that all IPv6-enabled devices join. Similar to a broadcast in IPv4
  - FF02::2 All-routers multicast group – This is a multicast group that all IPv6 routers join.



Solicited-Node IPv6 Multicast Addresses

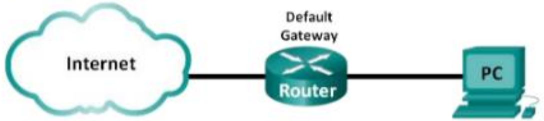
- Solicited-node multicast address:
  - Mapped to .a special Ethernet multicast address
  - Allows Ethernet NIC to filter frame on destination MAC.



Lab – Identifying IPv6 Addresses

Lab – Identifying IPv6 Addresses

Topology



Objectives

Part 1: Identify the Different Types of IPv6 Addresses

Part 2: Examine a Host IPv6 Network Interface and Address

Part 3: Practice IPv6 Address Abbreviation

Background / Scenario

With the depletion of the Internet Protocol version 4 (IPv4) network address space and the adoption and transition to IPv6, networking professionals must understand how both IPv4 and IPv6 networks function. Many devices and applications already support IPv6. This includes extensive Cisco device Internetwork Operating System (IOS) support and workstation/server operating system support, such as that found in Windows and Linux.

This lab focuses on IPv6 addresses and the components of the address. In Part 1, you will identify the IPv6 address types, and in Part 2, you will view the IPv6 settings on a PC. In Part 3, you will practice IPv6 address abbreviation.

Required Resources

- 1 PC (Windows 7 or 8 with Internet access)

Part 1: Identify the Different Types of IPv6 Addresses

In Part 1, you will review the characteristics of IPv6 addresses to identify the different types of IPv6 addresses.

Step 1: Review the different types of IPv6 addresses.

An IPv6 address is 128 bits long. It is most often presented as 32 hexadecimal characters. Each hexadecimal character is the equivalent of 4 bits (4 x 32 = 128). A non-abbreviated IPv6 host address is shown here:

2001:0DB8:0001:0000:0000:0000:0000:0001

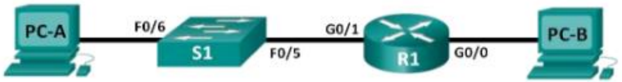
A hextet is the hexadecimal, IPv6 version of an IPv4 octet. An IPv4 address is 4 octets long, separated by dots. An IPv6 address is 8 hextets long, separated by colons.

Lab – Configuring IPv6 Addresses on Network Devices

Cisco Networking Academy® Mind Wide Open™

Lab - Configuring IPv6 Addresses on Network Devices

Topology



Addressing Table

Device	Interface	IPv6 Address	Prefix Length	Default Gateway
R1	G0/0	2001:DB8:ACAD:A::1	64	N/A
	G0/1	2001:DB8:ACAD:1::1	64	N/A
S1	VLAN 1	2001:DB8:ACAD:1::B	64	N/A
PC-A	NIC	2001:DB8:ACAD:1::3	64	FE80::1
PC-B	NIC	2001:DB8:ACAD:A::3	64	FE80::1

Objectives

Part 1: Set Up Topology and Configure Basic Router and Switch Settings

Part 2: Configure IPv6 Addresses Manually

Part 3: Verify End-to-End Connectivity

Background / Scenario

Knowledge of the Internet Protocol version 6 (IPv6) multicast groups can be helpful when assigning IPv6 addresses manually. Understanding how the all-router multicast group is assigned and how to control address assignments for the Solicited Nodes multicast group can prevent IPv6 routing issues and help ensure best practices are implemented.

In this lab, you will configure hosts and device interfaces with IPv6 addresses and explore how the all-router multicast group is assigned to a router. You will use **show** commands to view IPv6 unicast and multicast addresses. You will also verify end-to-end connectivity using the **ping** and **traceroute** commands.

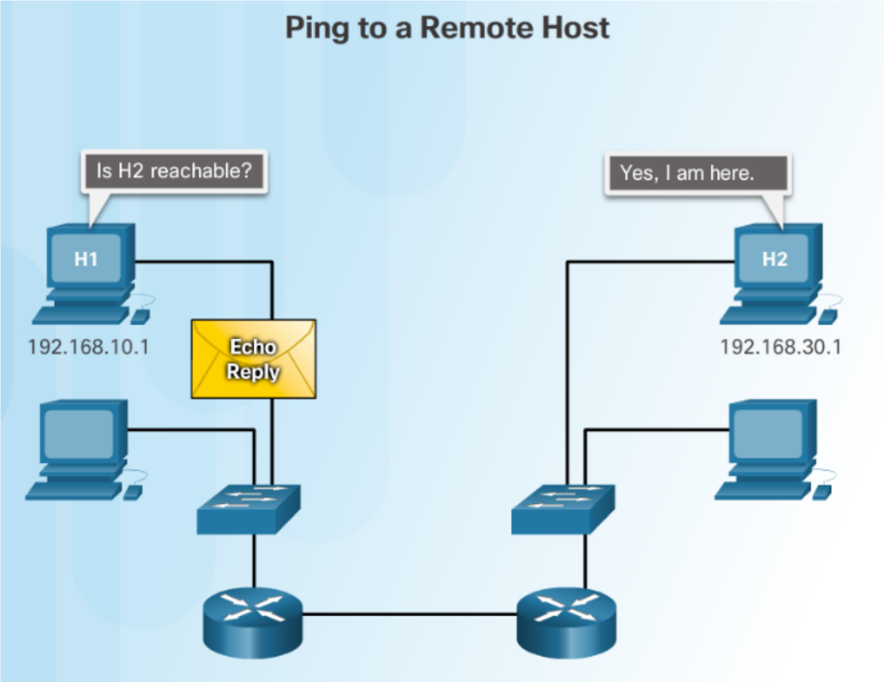
Note: The routers used with CCNA hands-on labs are Cisco 1941 ISRs with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

7.3 Connectivity Verification

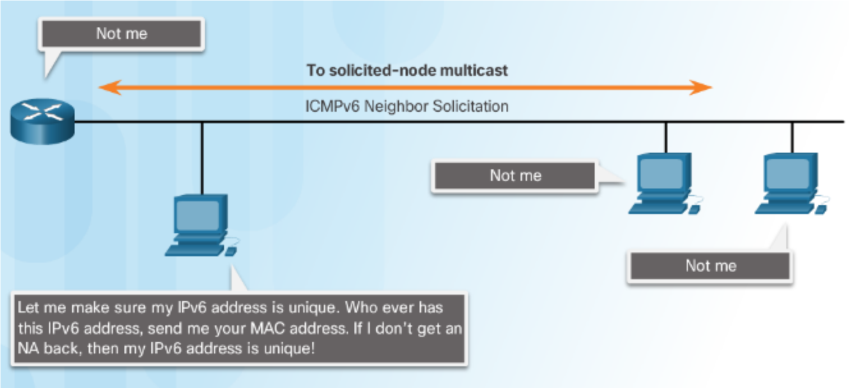
ICMPv4 and ICMPv6

- ICMPv4 is the messaging protocol for IPv4. ICMPv6 provides the same services for IPv6
- ICMP messages common to both include:
  - Host confirmation
  - Destination or Service Unreachable
  - Time exceeded
  - Route redirection

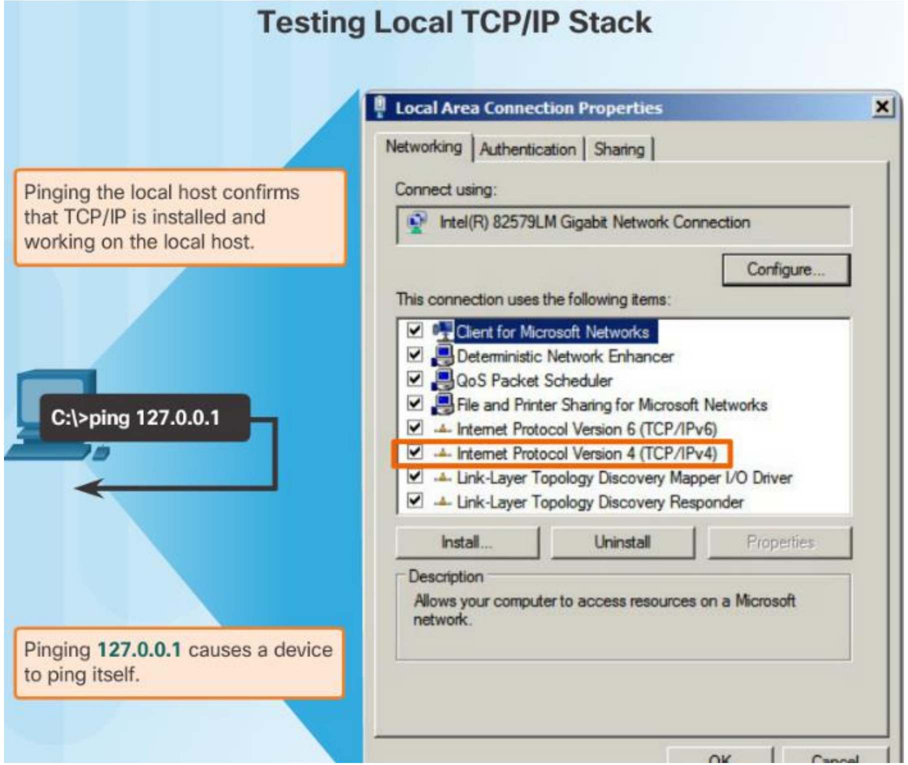


ICMPv6 Router Solicitation and Router Advertisement Messages

- ICMPv6 includes four new protocols as part of the Neighbor Discovery Protocol (ND or NDP)
  - Router Solicitation (RS) message
  - Router Advertisement (RA) message
- RA messages used to provide addressing information to hosts
  - Neighbor Solicitation (NS) message
  - Neighbor Advertisement (NA) message
- Neighbor Solicitation and Neighbor Advertisement messages are used for Address resolution and Duplicate Address Detection (DAD).

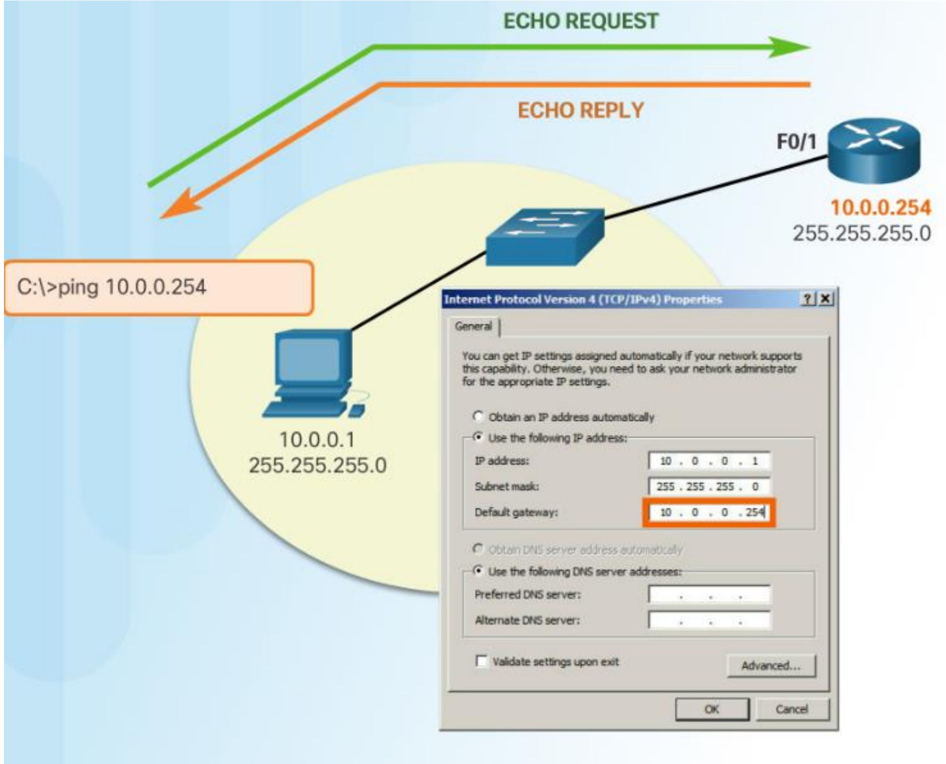


Ping - Testing the Local Stack



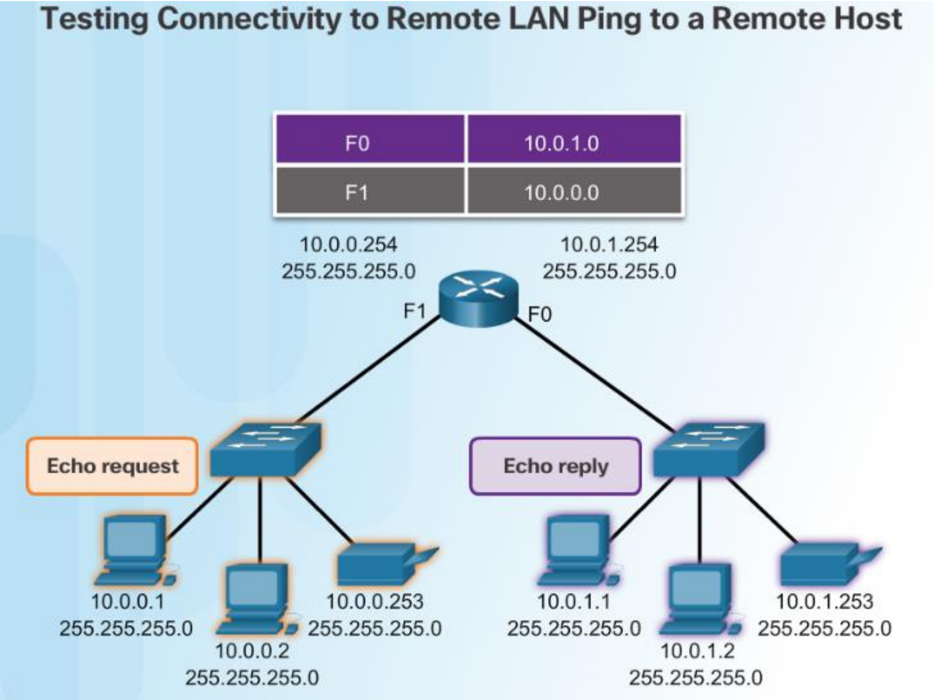
- Ping the local loopback address of 127.0.0.1 for IPv4 or ::1 for IPv6 to verify that IP is properly installed on the host.

Ping – Testing Connectivity to the Local LAN



- Use ping to test the ability of a host to communicate on the local network.

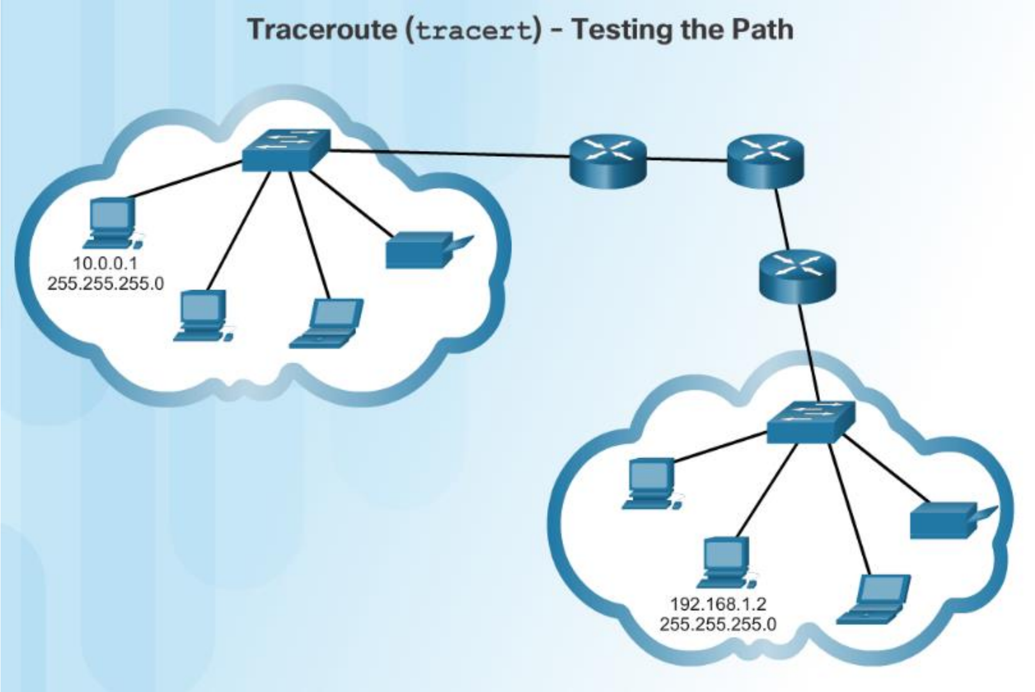
Ping – Testing Connectivity to a Remote Host



- Use ping to test the ability of a host to communicate across an internetwork.

Traceroute – Testing the Path

- Traceroute (tracert) is a utility that generates a list of hops that were successfully reached along the path.
  - Round Trip Time (RTT) – Time it takes the packet to reach the remote host and for the response from the host to return.
  - Asterisk (*) is used to indicate a lost packet.



Testing and Verification

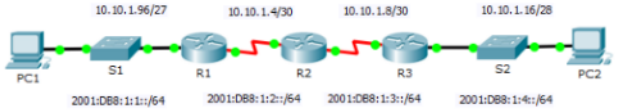
Packet Tracer – Verifying IPv4 and IPv6 Addressing

Cisco Networking Academy

Mind Wide Open

Packet Tracer - Verifying IPv4 and IPv6 Addressing

Topology



Addressing Table

Device	Interface	IPv4 Address / IPv6 Address/Prefix	Subnet Mask	Default Gateway
R1	G0/0	10.10.1.97	255.255.255.224	N/A
		2001:DB8:1:1::1/64		N/A
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:DB8:1:2::2/64		N/A
	Link-local	FE80::1		N/A
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:DB8:1:2::1/64		N/A
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:DB8:1:3::1/64		N/A
	Link-local	FE80::2		N/A
R3	G0/0	10.10.1.17	255.255.255.240	N/A
		2001:DB8:1:4::1/64		N/A
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:DB8:1:3::2/64		N/A

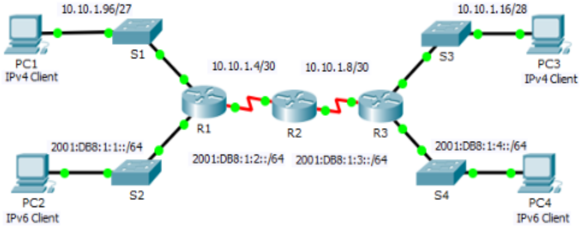
Packet Tracer – Pinging and Tracing to Test the Path

Cisco Networking Academy

Mind Wide Open

Packet Tracer - Pinging and Tracing to Test the Path

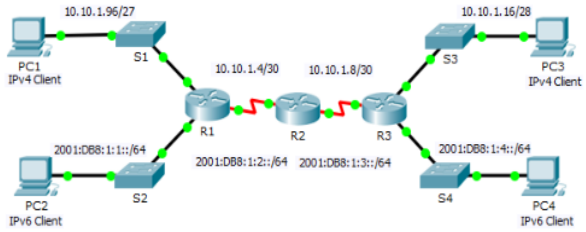
Topology



Lab – Testing Network Connectivity with Ping and Traceroute

Packet Tracer - Pinging and Tracing to Test the Path

Topology



Lab – Mapping the Internet

Cisco Networking Academy® Mind Wide Open™

Lab - Mapping the Internet

Objectives

Part 1: Test Network Connectivity Using Ping

Part 2: Trace a Route to a Remote Server Using Windows Tracert

Background

Route tracing computer software is a utility that lists the networks data has to traverse from the user's originating end device to a distant destination network.

This network tool is typically executed at the command line as:

```
tracert <destination network name or end device address>
```

(Microsoft Windows systems)

or

```
traceroute <destination network name or end device address>
```

(UNIX and similar systems)

Route tracing utilities allow a user to determine the path or routes as well as the delay across an IP network. Several tools exist to perform this function.

The **traceroute** (or **tracert**) tool is often used for network troubleshooting. By showing a list of routers traversed, it allows the user to identify the path taken to reach a particular destination on the network or across internetworks. Each router represents a point where one network connects to another network and through which the data packet was forwarded. The number of routers is known as the number of "hops" the data traveled from source to destination.

The displayed list can help identify data flow problems when trying to access a service such as a website. It can also be useful when performing tasks such as downloading data. If there are multiple websites (mirrors) available for the same data file, one can trace each mirror to get a good idea of which mirror would be the fastest to use.

Two trace routes between the same source and destination conducted some time apart may produce different results. This is due to the "meshed" nature of the interconnected networks that comprise the Internet and the Internet Protocols ability to select different pathways over which to send packets.

Command-line-based route tracing tools are usually embedded with the operating system of the end device.

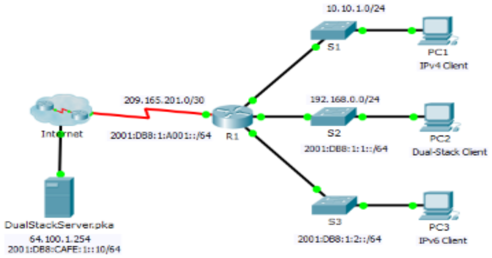
Scenario

Packet Tracer – Troubleshooting IPv4 and IPv6 Addressing

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Troubleshooting IPv4 and IPv6 Addressing

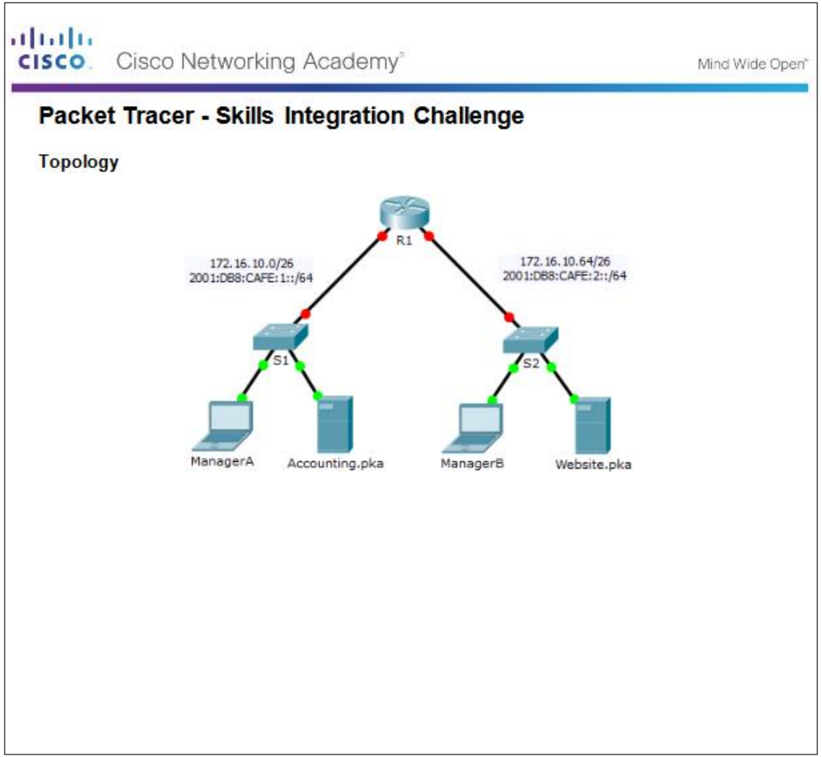
Topology



7.4 Chapter Summary

Conclusion

Packet Tracer – Skills Integration Challenge


Cisco Networking Academy
Mind Wide Open

Packet Tracer - Skills Integration Challenge

Topology

Chapter 7: IP Addressing

- Explain the use of IPv4 addresses to provide connectivity in small to medium-sized business networks
- Configure IPv6 addresses to provide connectivity in small to medium-sized business networks.
- Use common testing utilities to verify and test network connectivity.