

Topic: IP Address

Presenter

Dr. Md Forhad Rabbi, SMIEE

Associate Professor, Department of CSE,
Shahjalal University of Science and Technology, Sylhet

Coordinator, Pipilika Search Engine

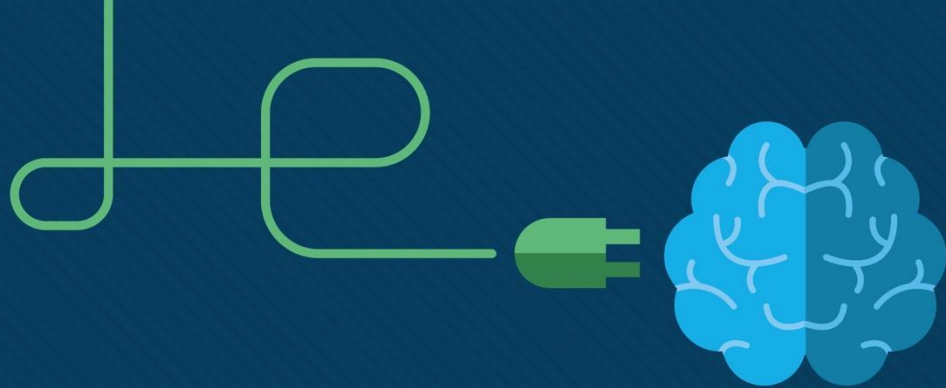
Instructor, Cisco Networking Academy, SUST

Consultant, Digital Sylhet City Project, BCC

Email: frabbi-cse@sust.edu

whatsapp:+8801844175805

IP Address basics Dr. Md. Forhad Rabbi, Associate Professor, Department of CSE. SUST	Class A, B, C IP Address, IPV6 Dr. Md. Forhad Rabbi, Associate Professor, Department of CSE. SUST	frabbi-cse@sust.edu 01844-175805
--	---	---



Network Layer

CCNA Routing and Switching
Introduction to Networks v6.0

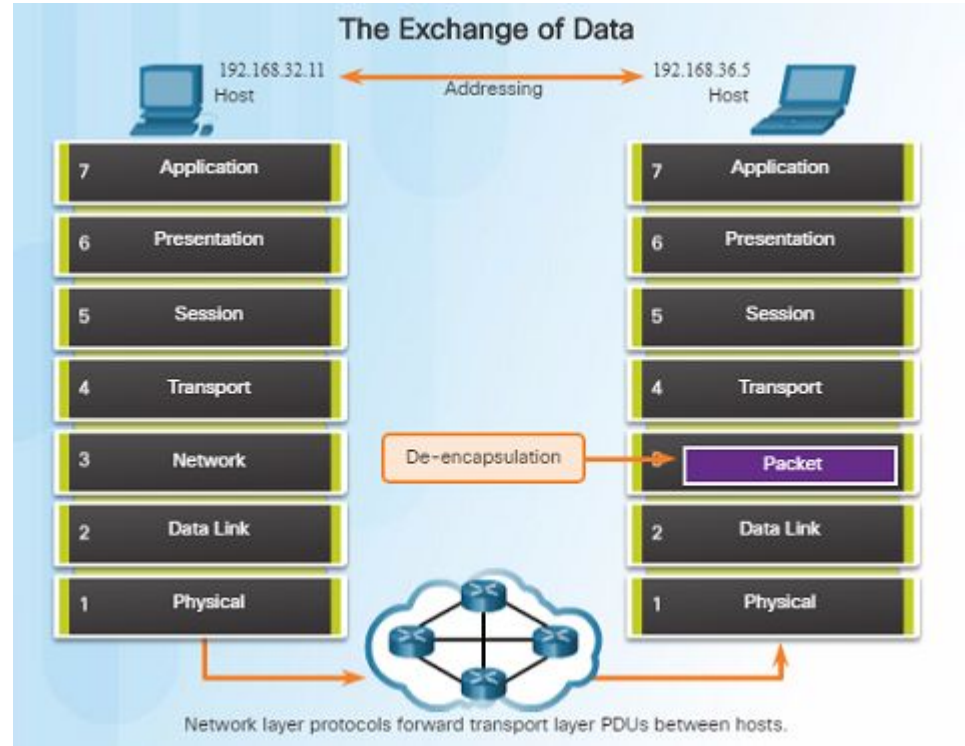


Network Layer Protocols

Network Layer in Communications

The Network Layer

- The network layer, which resides at OSI Layer 3, provides services that allow end devices to exchange data across a network.
- The network layer uses four processes in order to provide end-to-end transport:
 - Addressing of end devices – IP addresses must be unique for identification purposes.
 - Encapsulation – The protocol data units from the transport layer are encapsulated by adding IP header information including source and destination IP addresses.
 - Routing – The network layer provides services to direct packets to other networks. Routers select the best path for a packet to take to its destination network.
 - De-encapsulation – The destination host de-encapsulates the packet to see if it matches its own.

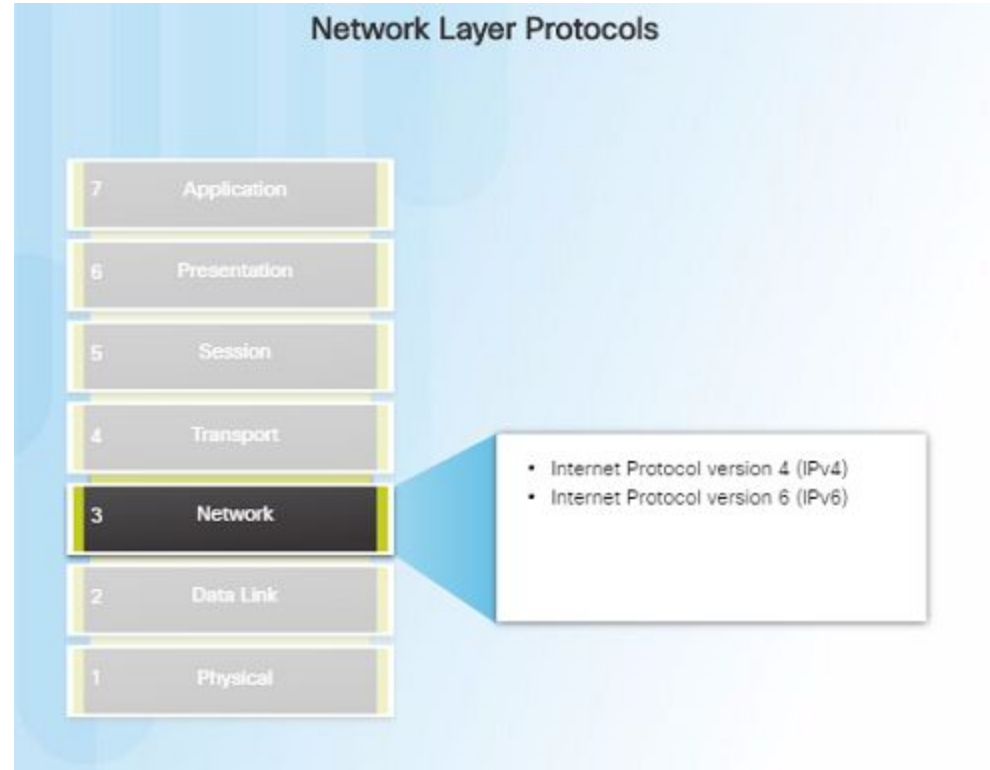


Network Layer in Communications

Network Layer Protocols

- There are several network layer protocols in existence; however, the most commonly implemented are:
 - Internet Protocol version 4 (IPv4)
 - Internet Protocol version 6 (IPv6)

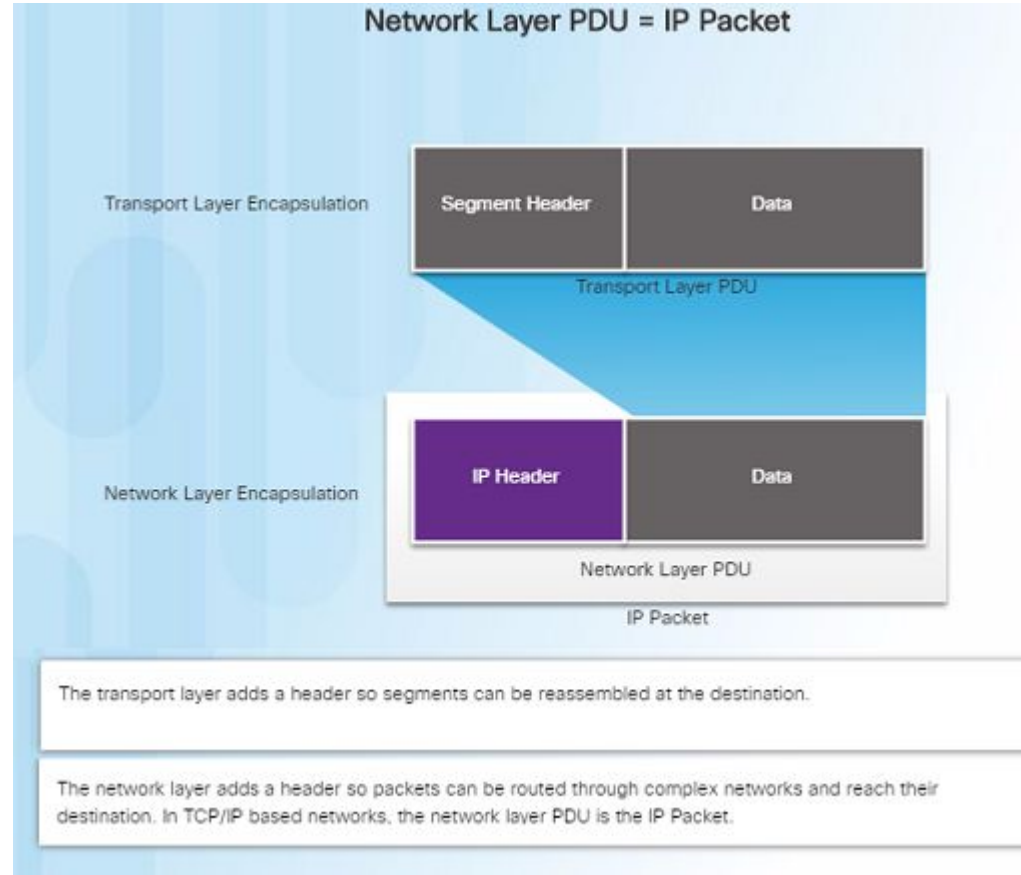
Note: Legacy network layer protocols are not discussed in this course.



Characteristics of the IP Protocol

Encapsulating IP

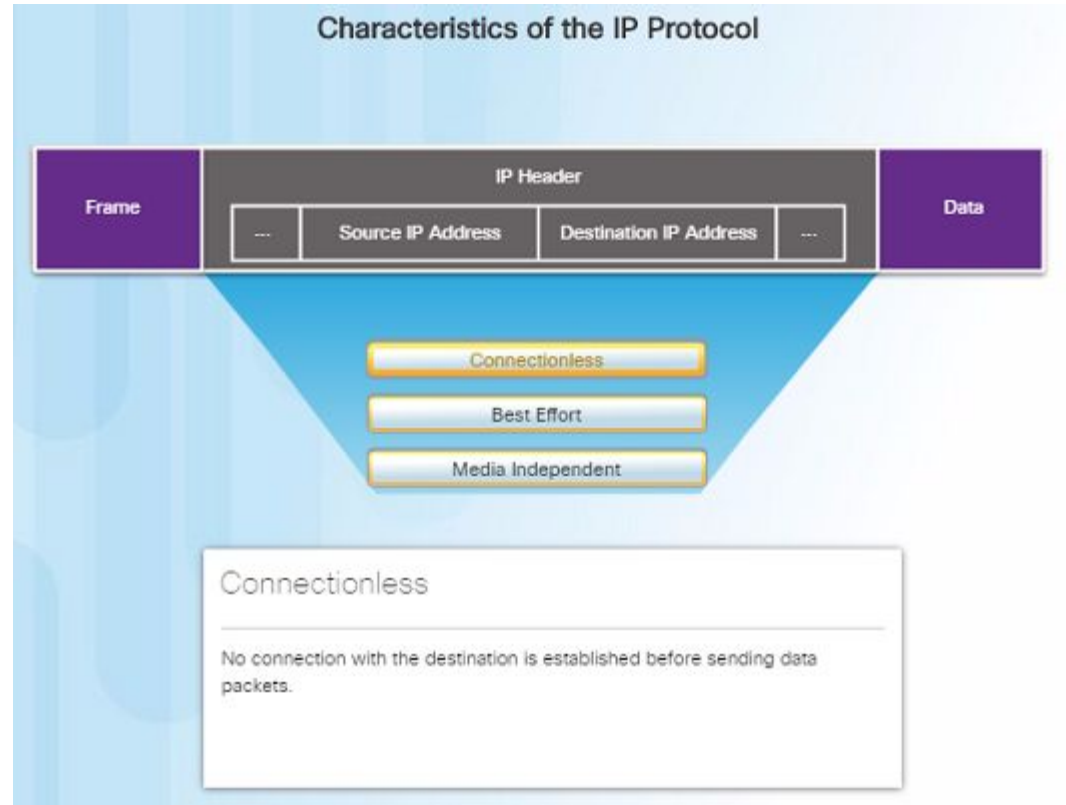
- At the network layer, IP encapsulates the transport layer segment by adding an IP header for the purpose of delivery to the destination host.
- The IP header stays the same from the source to the destination host.
- The process of encapsulating data layer by layer enables the services at different layers to scale without affecting other layers.
- Routers implement different network layer protocols concurrently over a network and use the network layer packet header for routing.



Characteristics of the IP Protocol

Characteristics of IP

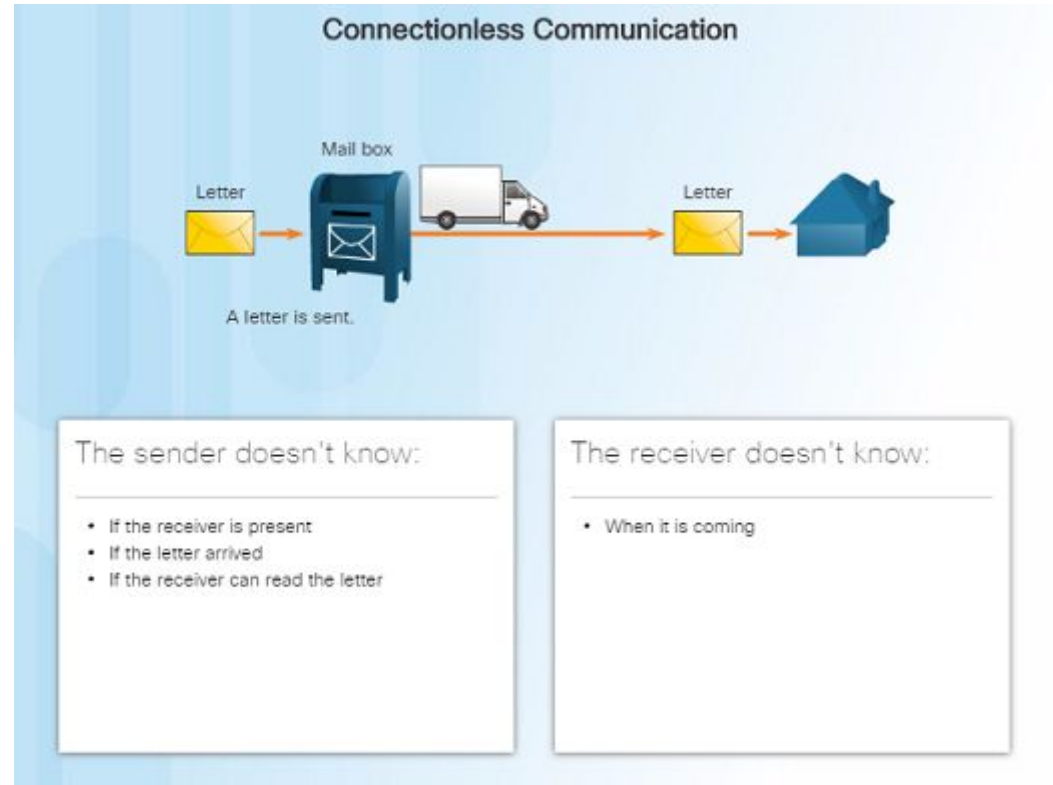
- IP was designed as a protocol with low overhead – it provides only the functions required to deliver a packet from the source to a destination.
- An IP packet is sent to the destination without prior establishment of a connection
- IP was not designed to track and manage the flow of packets.
- These functions, if required, are performed by other layers – primarily TCP



Characteristics of the IP Protocol

IP - Connectionless

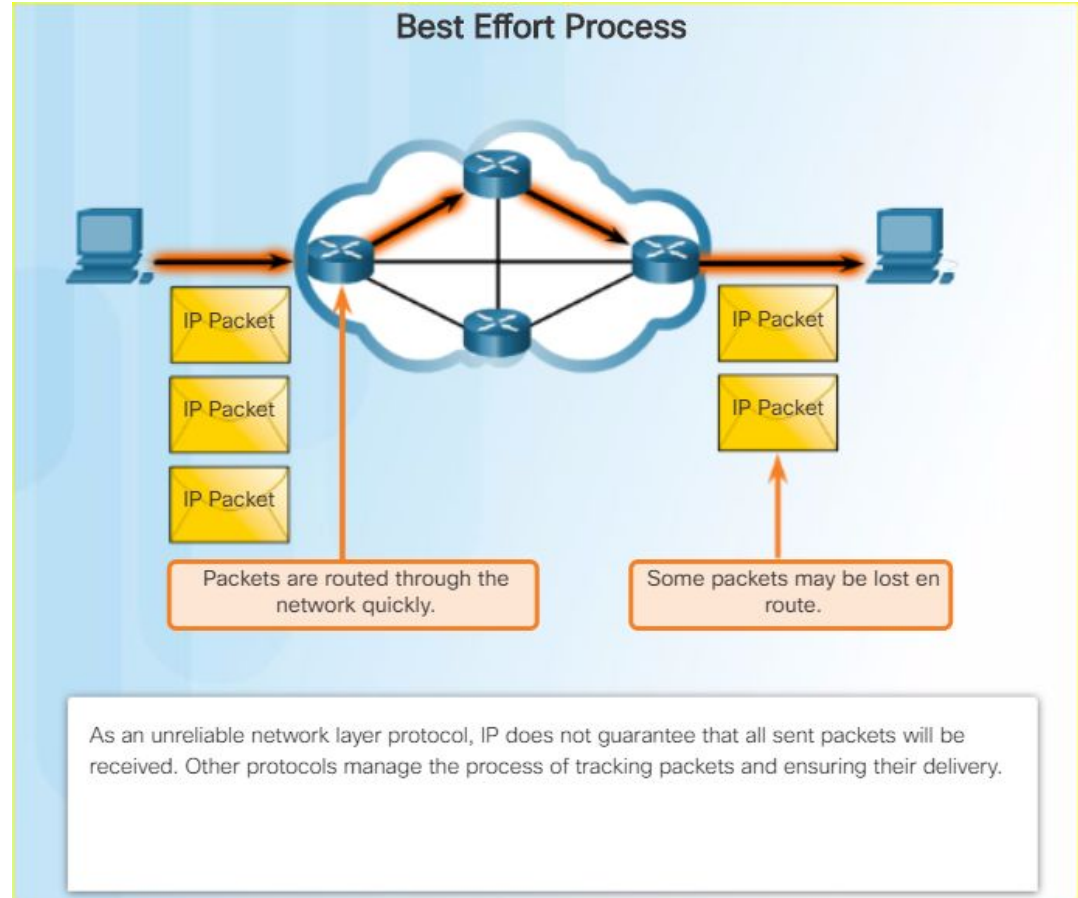
- IP is a connectionless protocol:
 - No dedicated end-to-end connection is created before data is sent.
 - Very similar process as sending someone a letter through snail mail.
 - Senders do not know whether or not the destination is present, reachable, or functional before sending packets.
 - This feature contributes to the low overhead of IP.



Characteristics of the IP Protocol

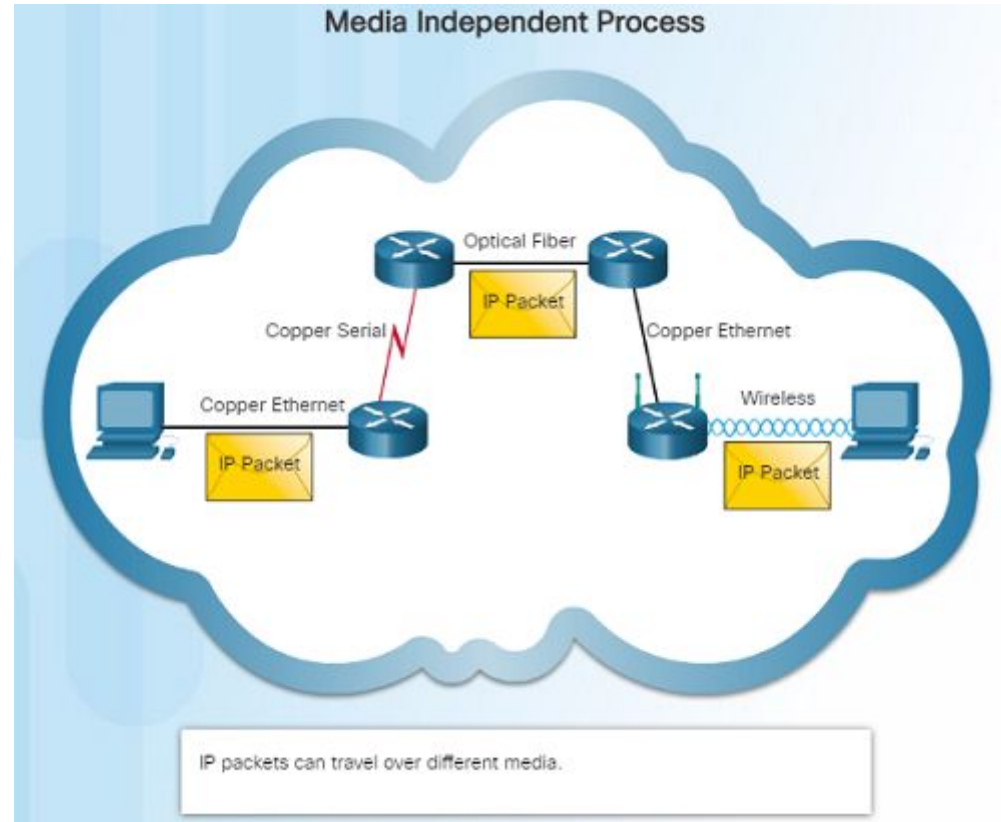
IP – Best Effort Delivery

- IP is a Best Effort Delivery protocol:
 - IP is considered “unreliable” because it does not guarantee that all packets that are sent will be received.
 - Unreliable means that IP does not have the capability to manage and recover from undelivered, corrupt, or out of sequence packets.
 - If packets are missing or not in the correct order at the destination, upper layer protocols/services must resolve these issues.



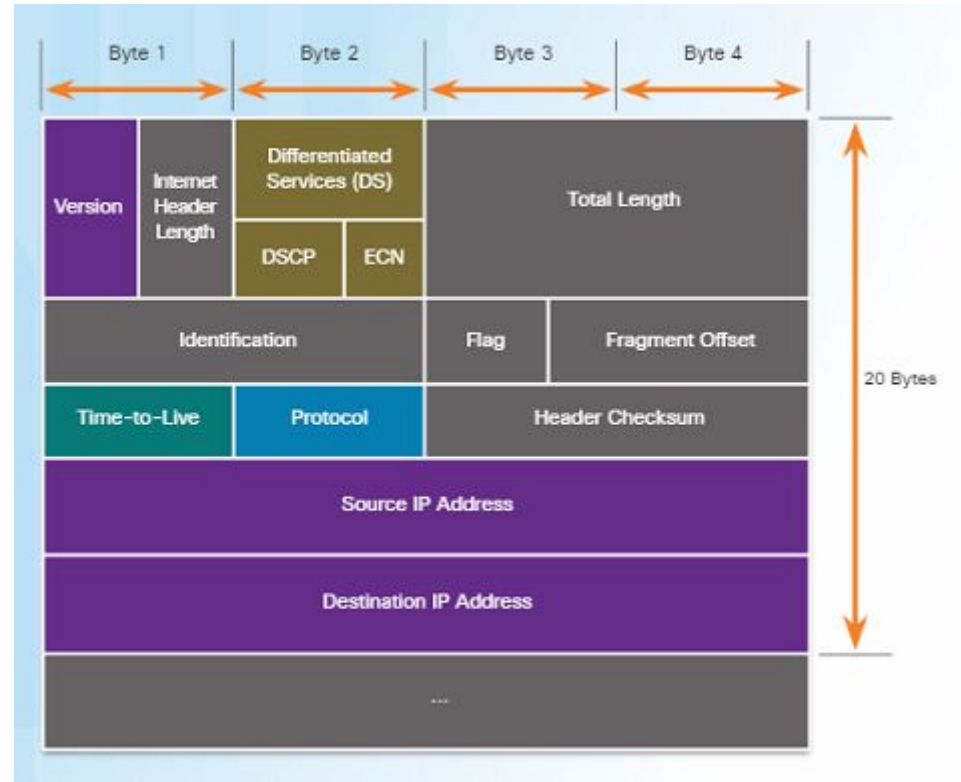
IP – Media Independent

- IP operates independently from the media that carries the data at lower layers of the protocol stack – it does not care if the media is copper cables, fiber optics or wireless.
- The OSI data link layer is responsible for taking the IP packet and preparing it for transmission over the communications medium.
- The network layer does have a maximum size of the PDU that can be transported – referred to as MTU (maximum transmission unit).
- The data link layer tells the network layer the MTU.



IPv4 Packet Header

- An IPv4 packet header consists of the fields containing binary numbers. These numbers identify various settings of the IP packet which are examined by the Layer 3 process.
- Significant fields include:
 - Version – Specifies that the packet is IP version 4
 - Differentiated Services or DiffServ (DS) – Used to determine the priority of each packet on the network.
 - Time-to-Live (TTL) – Limits the lifetime of a packet – decreased by one at each router along the way.
 - Protocol – Used to identify the next level protocol.
 - Source IPv4 Address – Source address of the packet.
 - Destination IPv4 Address – Address of destination.



Limitations of IPv4

- IPv4 has been updated to address new challenges.
- Three major issues still exist with IPv4:
 - IP address depletion – IPv4 has a limited number of unique public IPv4 addresses available. Although there are about 4 billion IPv4 addresses, the exponential growth of new IP-enabled devices has increased the need.
 - Internet routing table expansion – A routing table contains the routes to different networks in order to make the best path determination. As more devices and servers are connected to the network, more routes are created. A large number of routes can slow down a router.
 - Lack of end-to-end connectivity – Network Address Translation (NAT) was created for devices to share a single IPv4 address. However, because they are shared, this can cause problems for technologies that require end-to-end connectivity.



IPv6 Packet

Introducing IPv6

- In the early '90s, the IETF started looking at a replacement for IPv4 – which led to IPv6.
- Advantages of IPv6 over IPv4 include:
 - Increased address space – based on 128-bit addressing vs. 32-bit with IPv4
 - Improved packet handling – fewer fields with IPv6 than IPv4
 - Eliminates the need for NAT – no need to share addresses with IPv6
- There are roughly enough IPv6 addresses for every grain of sand on Earth.

How Many Addresses Are Available with IPv6?

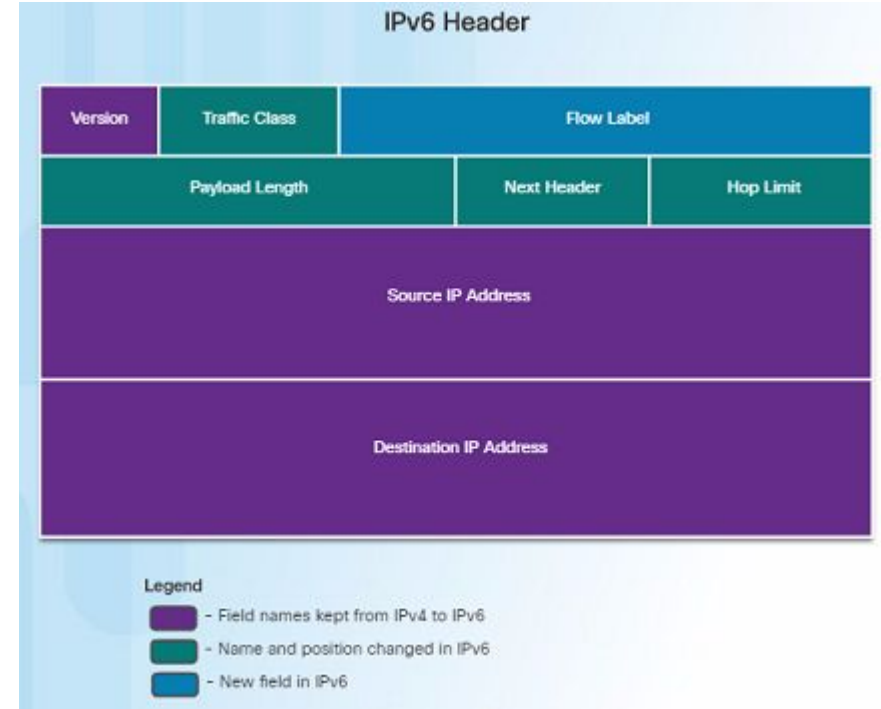
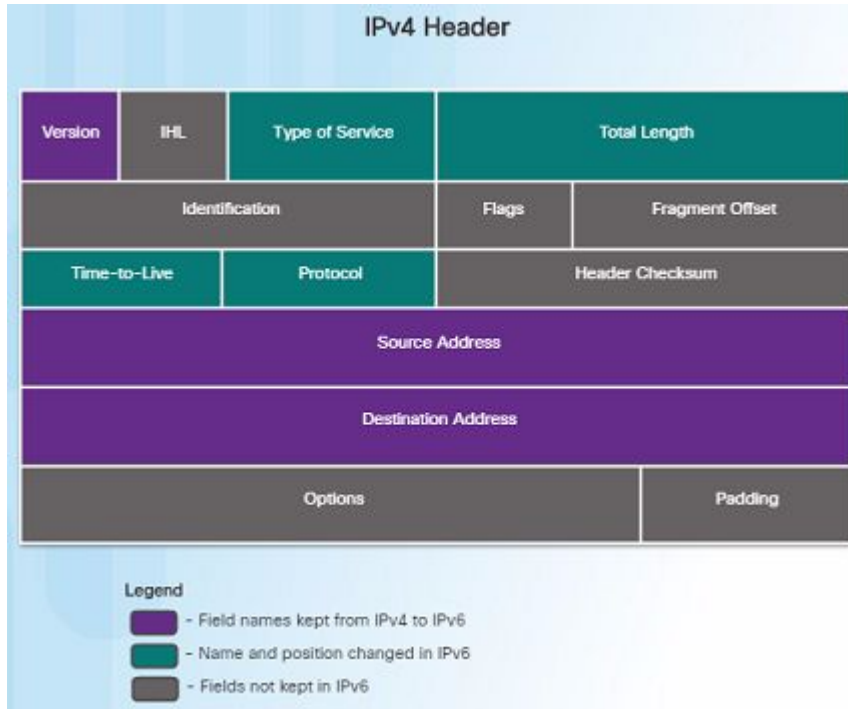
Number Name	Scientific Notation	Number of Zeros
1 Thousand	10^3	1,000
1 Million	10^6	1,000,000
1 Billion	10^9	1,000,000,000
1 Trillion	10^{12}	1,000,000,000,000
1 Quadrillion	10^{15}	1,000,000,000,000,000
1 Quintillion	10^{18}	1,000,000,000,000,000,000
1 Sextillion	10^{21}	1,000,000,000,000,000,000,000
1 Septillion	10^{24}	1,000,000,000,000,000,000,000,000
1 Octillion	10^{27}	1,000,000,000,000,000,000,000,000,000
1 Nonillion	10^{30}	1,000,000,000,000,000,000,000,000,000,000
1 Decillion	10^{33}	1,000,000,000,000,000,000,000,000,000,000,000
1 Undecillion	10^{36}	1,000,000,000,000,000,000,000,000,000,000,000,000

Legend

- There are 4 billion IPv4 addresses
- There are 340 undecillion IPv6 addresses

Encapsulating IPv6

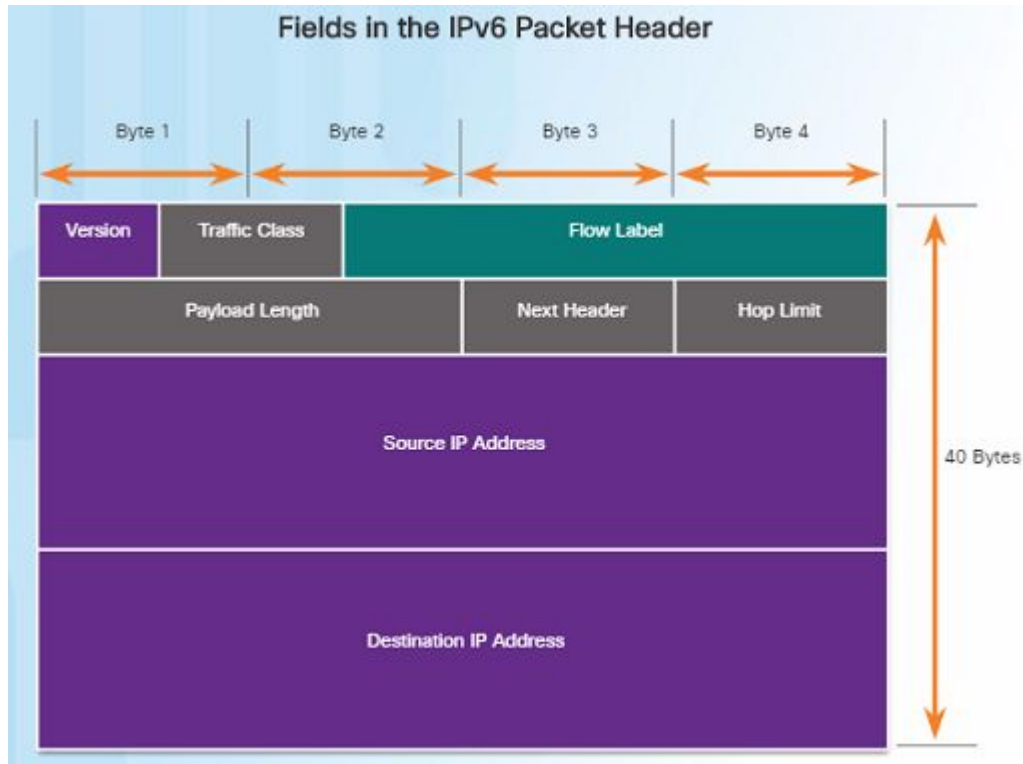
- The IPv6 header is simpler than the IPv4 header.



Encapsulating IPv6 (Cont.)

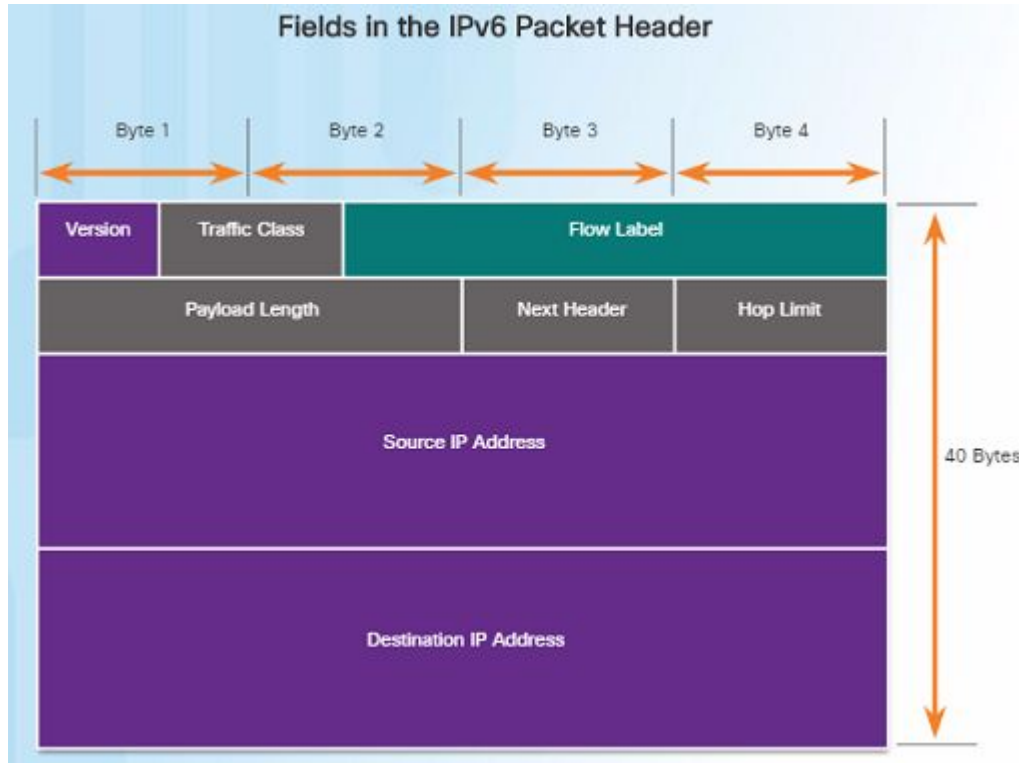
- Advantages of IPv6 over IPv4 using the simplified header:
 - Simplified header format for efficient packet handling
 - Hierarchical network architecture for routing efficiency
 - Autoconfiguration for addresses
 - Elimination of need for network address translation (NAT) between private and public addresses

IPv6 Packet Header



- IPv6 packet header fields:
 - Version – Contains a 4-bit binary value set to 0110 that identifies it as a IPv6 packet.
 - Traffic Class – 8-bit field equivalent to the IPv4 Differentiated Services (DS) field.
 - Flow Label – 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.
 - Payload Length – 16-bit field indicates the length of the data portion or payload of the packet.
 - Next Header – 8-bit field is equivalent to the IPv4 Protocol field. It indicates the data payload type that the packet is carrying.

IPv6 Packet Header (Cont.)

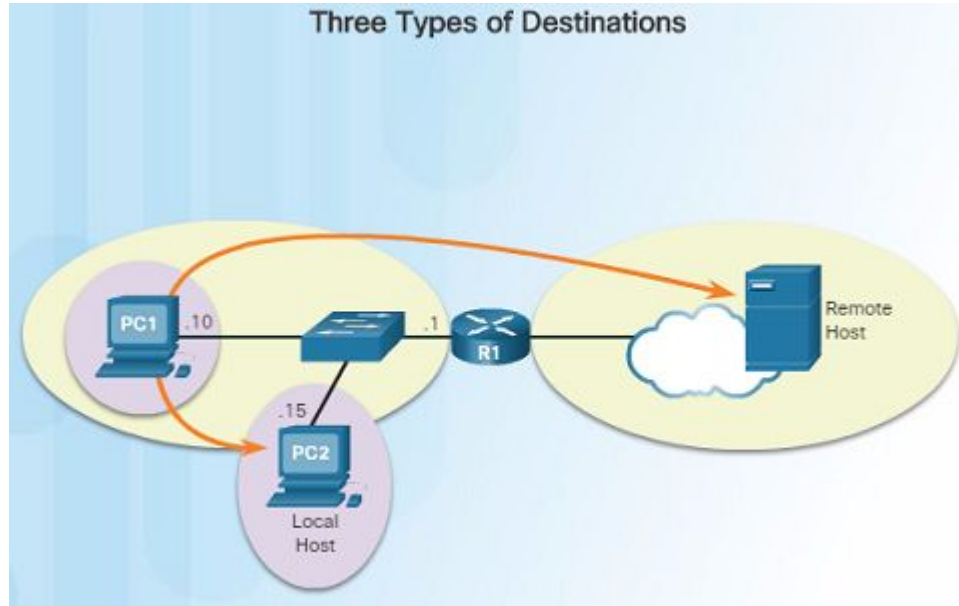


- IPv6 packet header fields:
 - Hop Limit – 8-bit field replaces the IPv4 TTL field. This value is decremented by 1 as it passes through each router. When it reaches zero, the packet is discarded.
 - Source IPv6 Address – 128-bit field that identifies the IPv6 address of the sending host.
 - Destination IPv6 Address – 128-bit field that identifies the IPv6 address of the receiving host.

Routing

How a Host Routes

Host Forwarding Decision



- An important role of the network layer is to direct packets between hosts. A host can send a packet to:
 - Itself – A host can ping itself for testing purposes using 127.0.0.1 which is referred to as the loopback interface.
 - Local host – This is a host on the same local network as the sending host. The hosts share the same network address.
 - Remote host – This is a host on a remote network. The hosts do not share the same network address.
- The source IPv4 address and subnet mask is compared with the destination address and subnet mask in order to determine if the host is on the local network or remote network.

How a Host Routes

Default Gateway

Default Gateway Functions

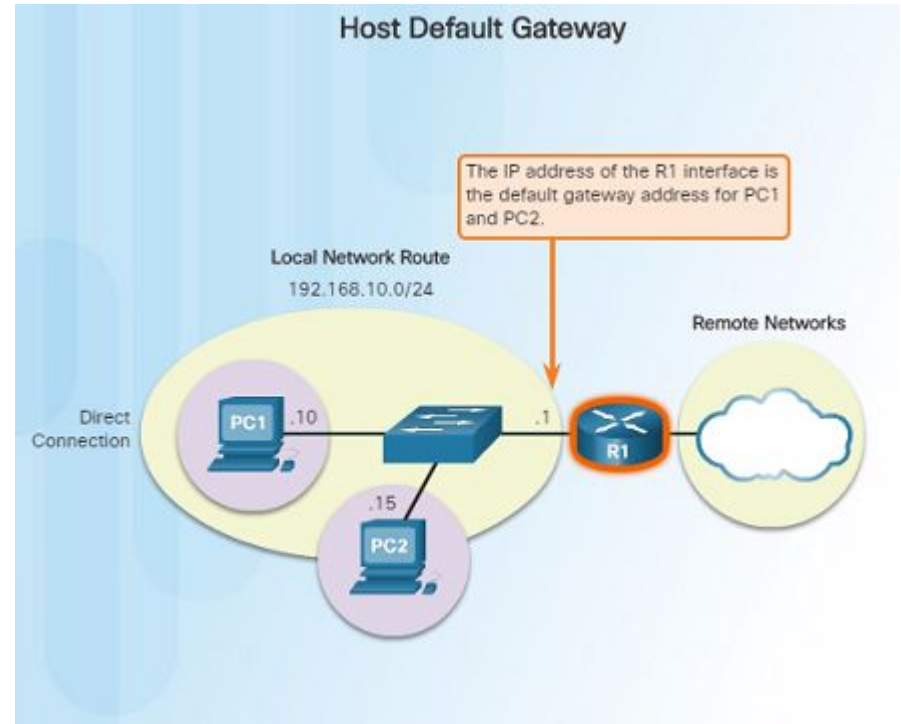
A Default Gateway ...

- Routes traffic to other networks.
- Has a local IP address in the same address range as other hosts on the network.
- Can take data in and forward data out.

- The default gateway is the network device that can route traffic out to other networks. It is the router that routes traffic out of a local network.
- This occurs when the destination host is not on the same local network as the sending host.
- The default gateway will know where to send the packet using its routing table.
- The sending host does not need to know where to send the packet other than to the default gateway – or router.

How a Host Routes Using the Default Gateway

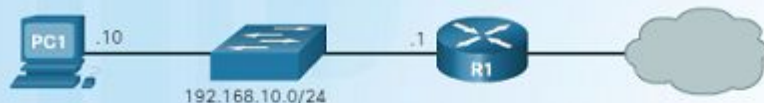
- A host's routing table usually includes a default gateway address – which is the router IP address for the network that the host is on.
- The host receives the IPv4 address for the default gateway from DHCP, or it is manually configured.
- Having a default gateway configured creates a default route in the routing table of a host - which is the route the computer will send a packet to when it needs to contact a remote network.



How a Host Routes

Host Routing Tables

IPv4 Routing Table for PC1



```
C:\Users\PC1> netstat -r
```

```
<output omitted>
```

```
IPv4 Route Table
```

```
=====
```

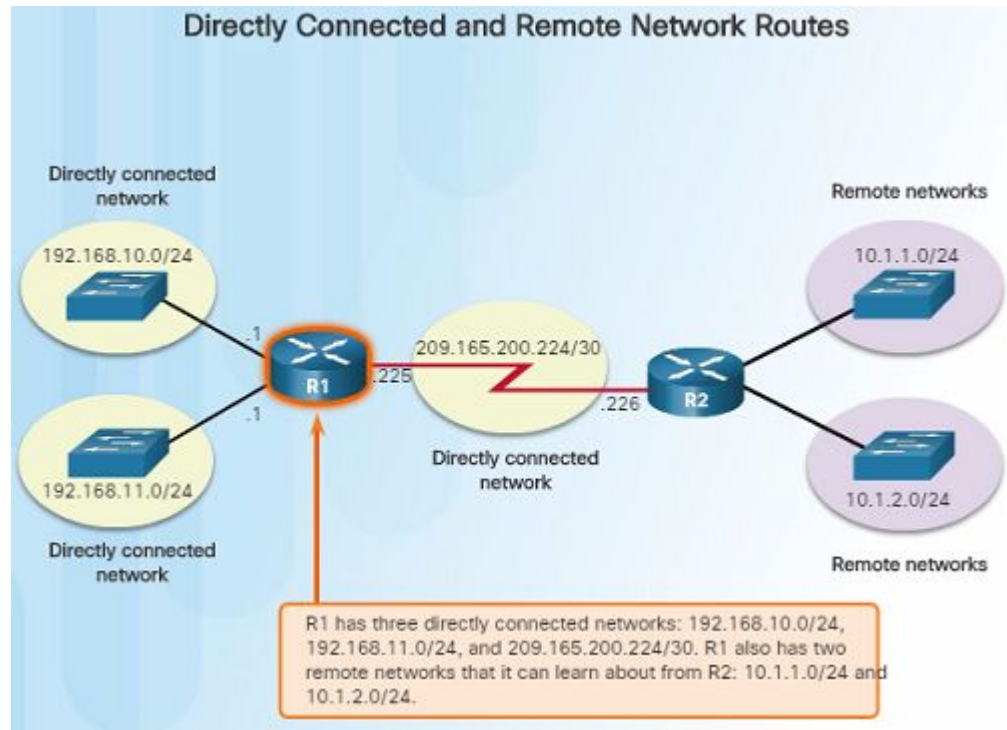
```
Active Routes:
```

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	25
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.10.0	255.255.255.0	255.255.255.0	On-link	192.168.10.10	281
192.168.10.10	255.255.255.255	255.255.255.255	On-link	192.168.10.10	281
192.168.10.255	255.255.255.255	255.255.255.255	On-link	192.168.10.10	281
224.0.0.0	240.0.0.0	240.0.0.0	On-link	127.0.0.1	306
224.0.0.0	240.0.0.0	240.0.0.0	On-link	192.168.10.10	281
255.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	255.255.255.255	On-link	192.168.10.10	281

```
<output omitted>
```

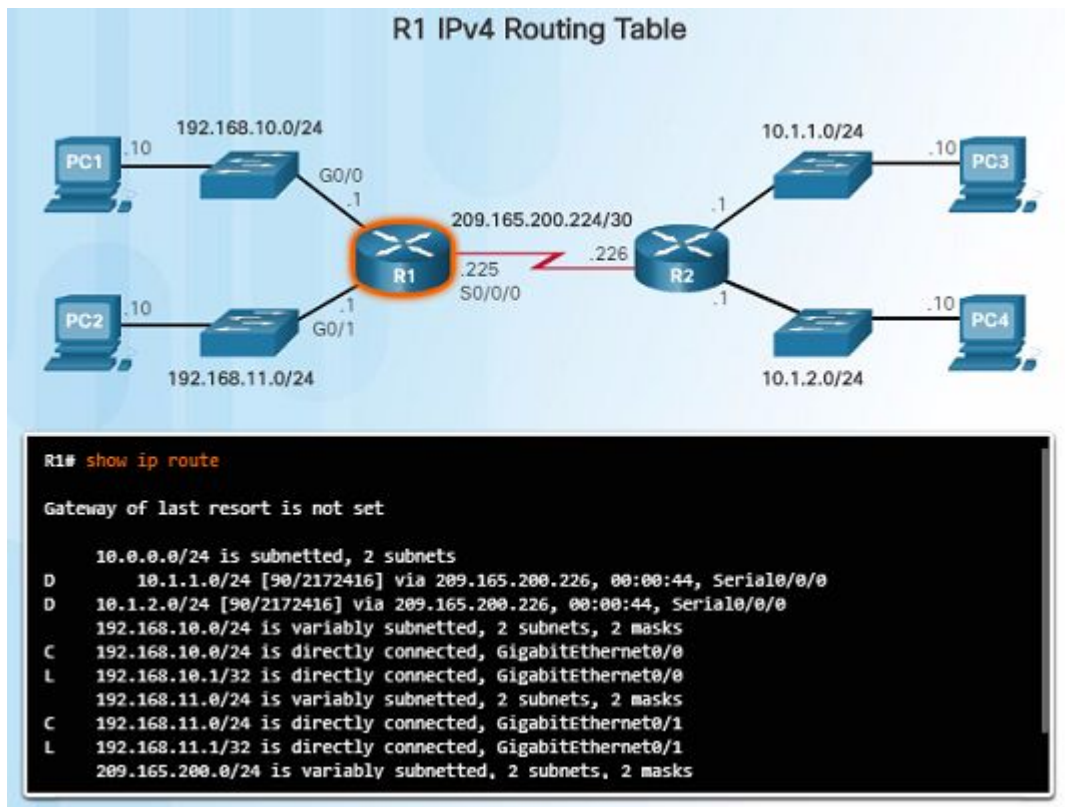
- On a Windows host, you can display the routing table using:
 - **route print**
 - **netstat -r**
- Three sections will be displayed:
 - Interface List – Lists the Media Access Control (MAC) address and assigned interface number of network interfaces on the host.
 - IPv4 Route Table – Lists all known IPv4 routes.
 - IPv6 Route Table – Lists all known IPv6 routes.

Router Packet Forwarding Decision



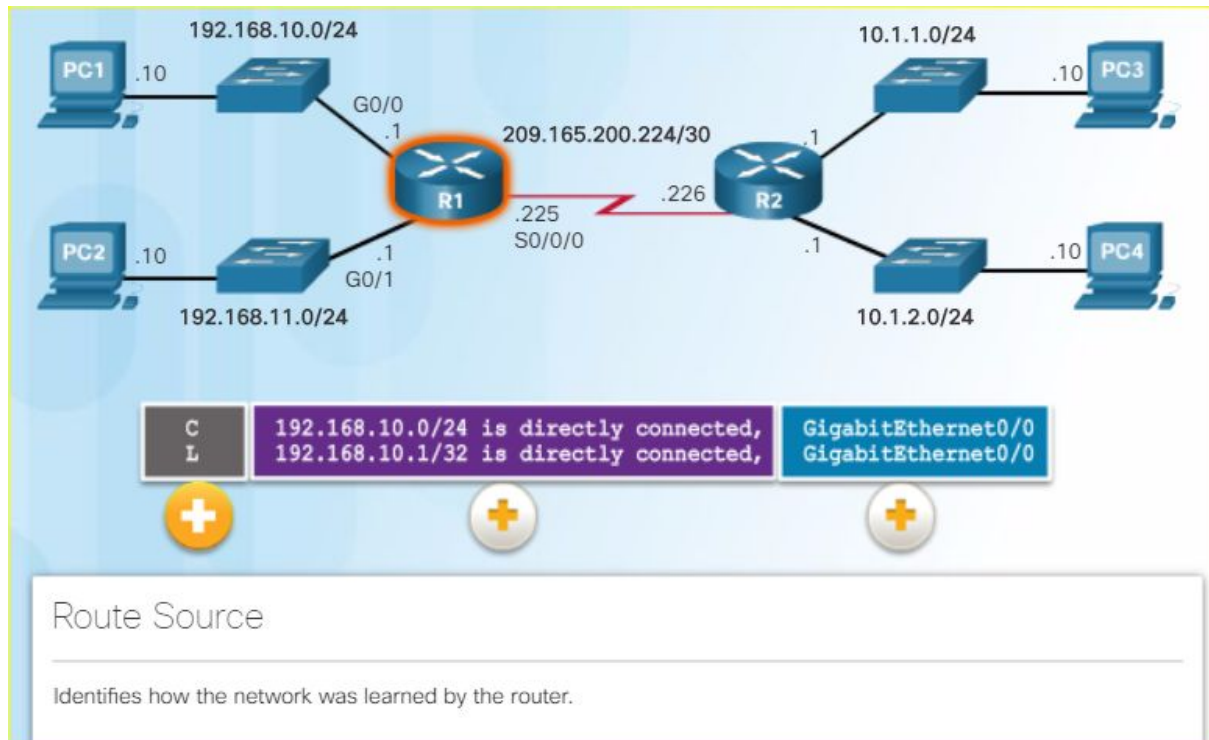
- When a router receives a packet destined for a remote network, the router has to look at its routing table to determine where to forward the packet. A router's routing table contains:
 - Directly-connected routes – These routes come from the active router interfaces configured with IP addresses.
 - Remote routes – These routes come from remote networks connected to other routers. They are either configured manually or learned through a dynamic routing protocol.
 - Default route – This is where the packet is sent when a route does not exist in the routing table.

IPv4 Router Routing Table



- On a Cisco IOS router, the **show ip route** command is used to display the router's IPv4 routing table. The routing table shows:
 - Directly connected and remote routes
 - How each route was learned
 - Trustworthiness and rating of the route
 - When the route was last updated
 - Which interface is used to reach the destination
- A router examines an incoming packet's header to determine the destination network. If there's a match, the packet is forwarded using the specified information in the routing table.

Directly Connected Routing Table Entries

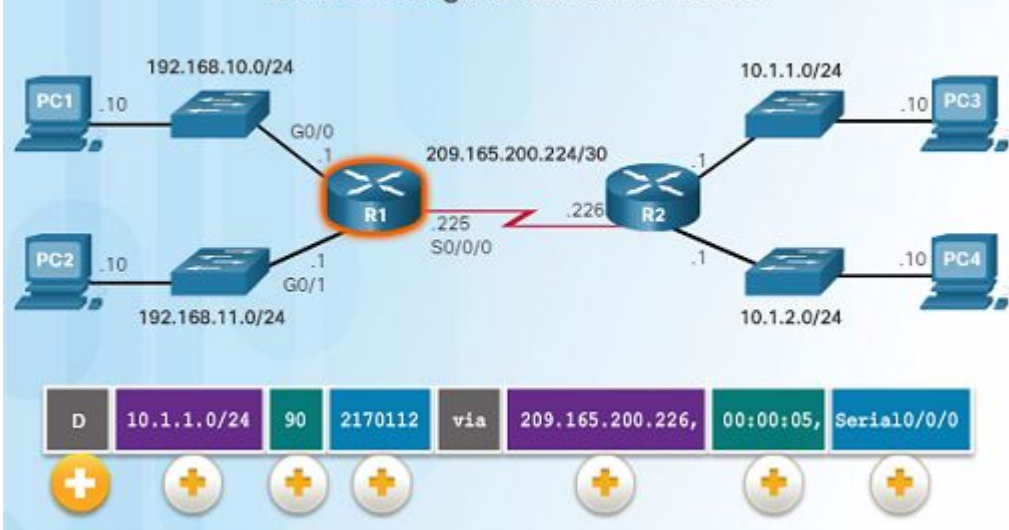


When a router interface is configured and activated, the following two routing table entries are created automatically:

- **C** – Identifies that the network is directly connected and the interface is configured with an IP address and activated.
- **L** – Identifies that it is a local interface. This is the IPv4 address of the interface on the router.

Understanding Remote Route Entries

Understanding Remote Route Entries



- The **D** represents the Route Source which is how the network was learned by the router. **D** identifies the route as an EIGRP route or (Enhanced Interior Gateway Routing Protocol)

- **10.1.1.0/24** identifies the destination network.
- **90** is the administrative distance for the corresponding network – or the trustworthiness of the route. The lower the number, the more trustworthy it is.
- **2170112** – represents the metric or value assigned to reach the remote network. Lower values indicate preferred routes.
- **209.165.200.226** – Next-hop or IP address of the next router to forward the packet.
- **00:00:05** - Route Timestamp identifies when the router was last heard from.
- **Serial/0/0/0** – Outgoing Interface

Router Routing Tables

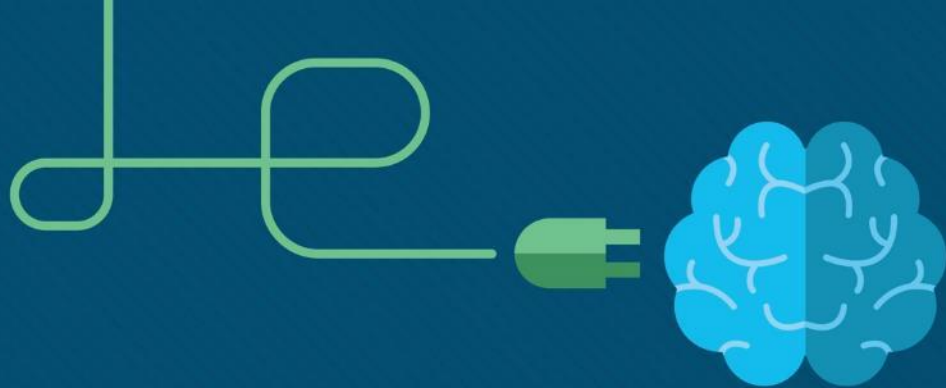
Next-Hop Address



```
R1# show ip route
<output omitted>
Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D   10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
    Serial0/0/0
D   10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
    Serial0/0/0
C   192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
L   192.168.10.0/24 is directly connected, GigabitEthernet0/0
L   192.168.10.1/32 is directly connected, GigabitEthernet0/0
L   192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C   192.168.11.0/24 is directly connected, GigabitEthernet0/1
L   192.168.11.1/32 is directly connected, GigabitEthernet0/1
C   209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C   209.165.200.224/30 is directly connected, Serial0/0/0
L   209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

- When a packet arrives at a router destined for a remote network, it will send the packet to the next hop address corresponding to the destination network address in its routing table.
- For example, if the R1 router in the figure to the left receives a packet destined for a device on the 10.1.1.0/24 network, it will send it to the next hop address of 209.165.200.226.
- Notice in the routing table, a default gateway address is not set – if the router receives a packet for a network that isn't in the routing table, it will be dropped.



IP Addressing

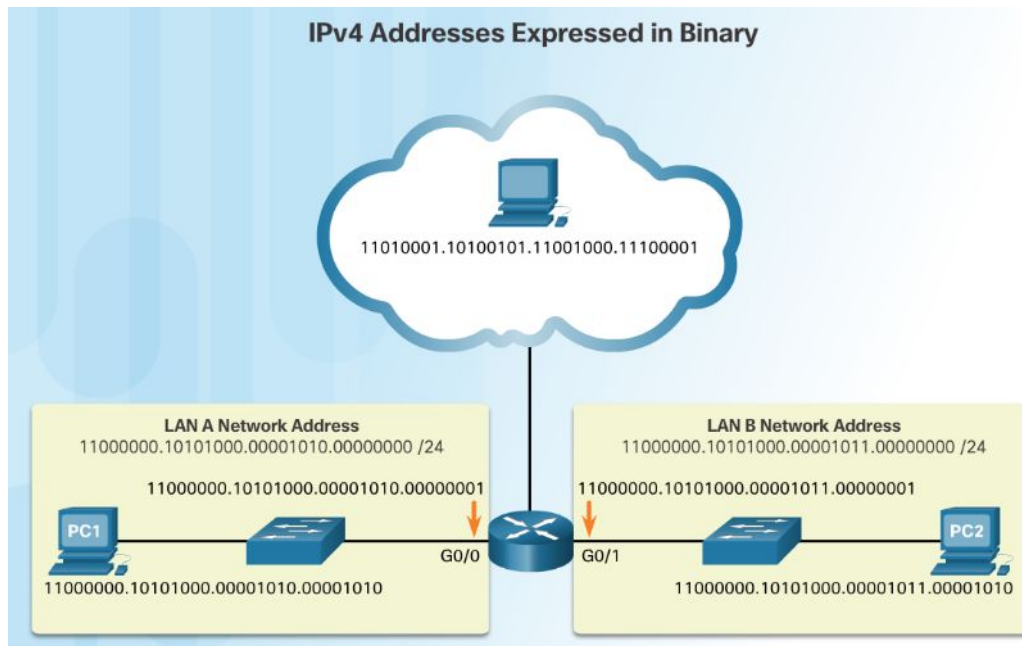
CCNA Routing and Switching
Introduction to Networks v6.0



IPv4 Network Addresses

IPv4 Addresses

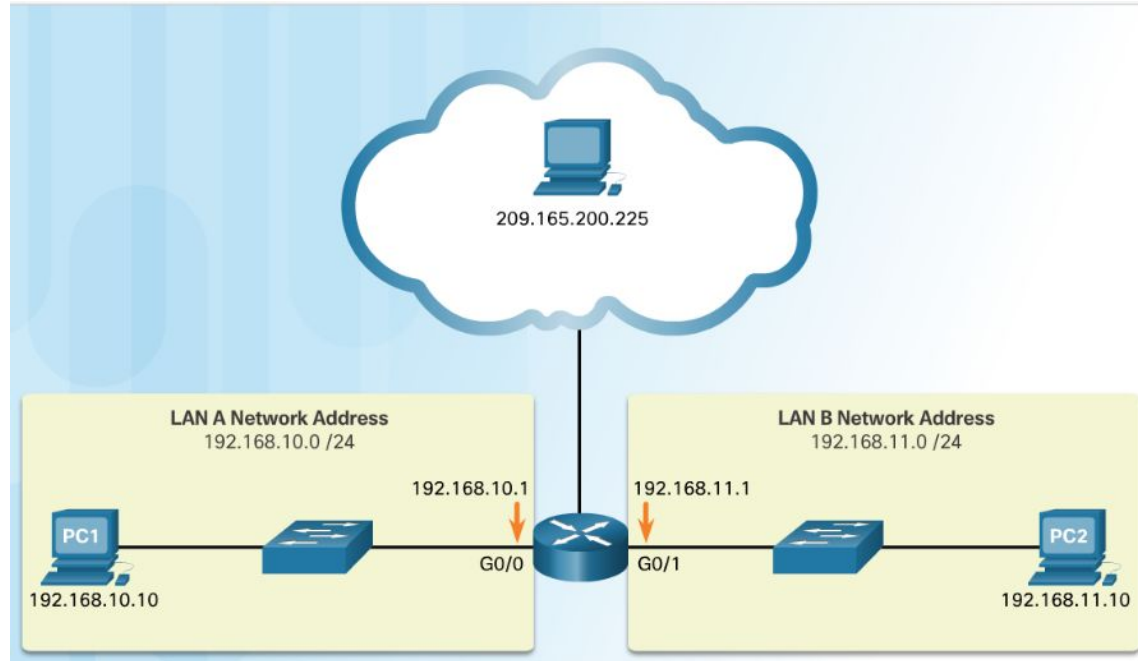
- Binary numbering system consists of the numbers 0 and 1 called bits
- IPv4 addresses are expressed in 32 binary bits divided into 4 8-bit octets



Binary and Decimal Conversion

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	1×1000	2×100	3×10	4×1
Add them up ...	1000	+ 200	+ 30	+ 4
Result	1,234			

Binary and Decimal Conversion

Positional Notation (Cont.)

Binary Positional Notation									
	Radix	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.

11000000.10101000.00001011.00001010

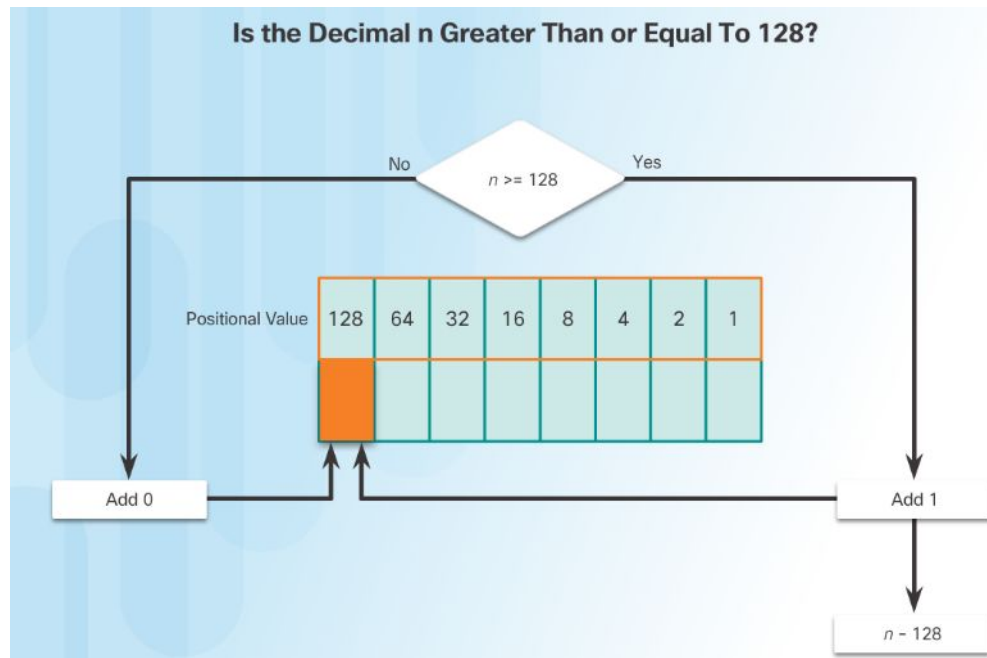
Positional Value	128	64	32	16	8	4	2	1
Binary number	1	1	0	0	0	0	0	0
Calculate	128	64	32	16	8	4	2	1
Add Them Up...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	192							

192.____.____.____

Dotted Decimal Notation

Decimal to Binary Conversion

- To convert a decimal IPv4 address 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.



Binary and Decimal Conversion

Decimal to Binary Conversion Examples

Example: 192.168.10.11

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

11000000 . _____ . _____ . _____

Example: 192.168.10.11

Positional Value	128	64	32	16	8	4	2	1
	1	0	1	0	1	0	0	0

11000000 . 10101000 . _____ . _____

Example: 192.168.10.11

Positional Value	128	64	32	16	8	4	2	1
	0	0	0	0	1	0	1	0

11000000 . 10101000 . 00001010 . _____

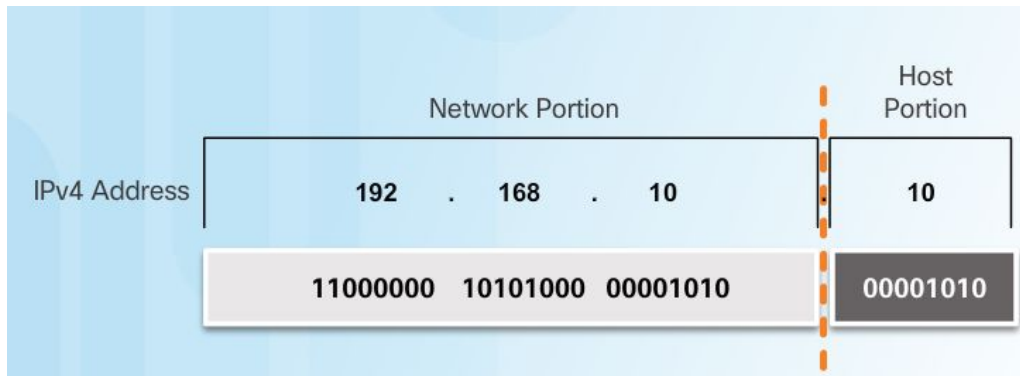
Example: 192.168.10.11

Positional Value	128	64	32	16	8	4	2	1
	0	0	0	0	1	0	1	1

11000000 . 10101000 . 00001010 . 00001011

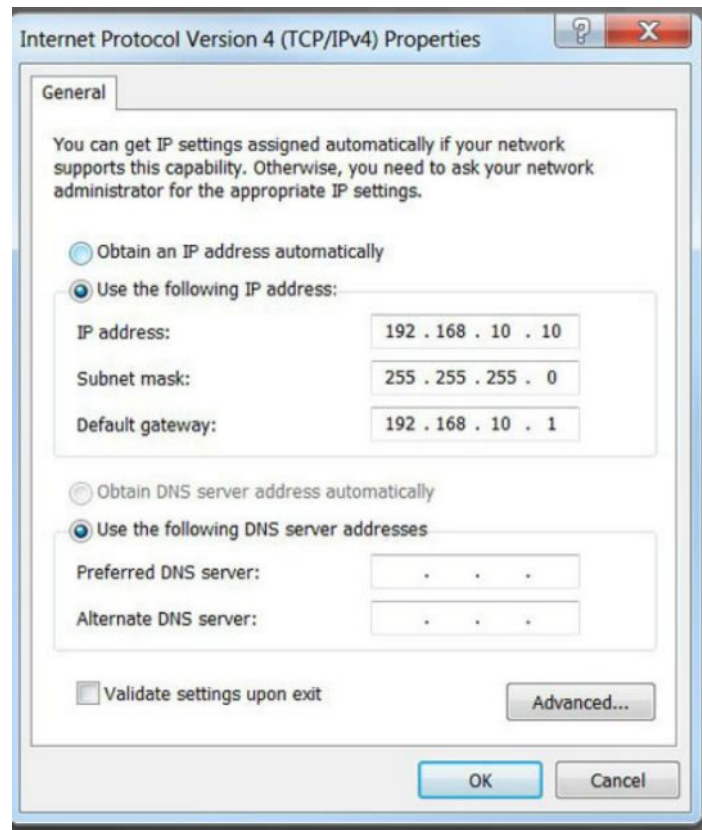
Network and Host Portions

- 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.



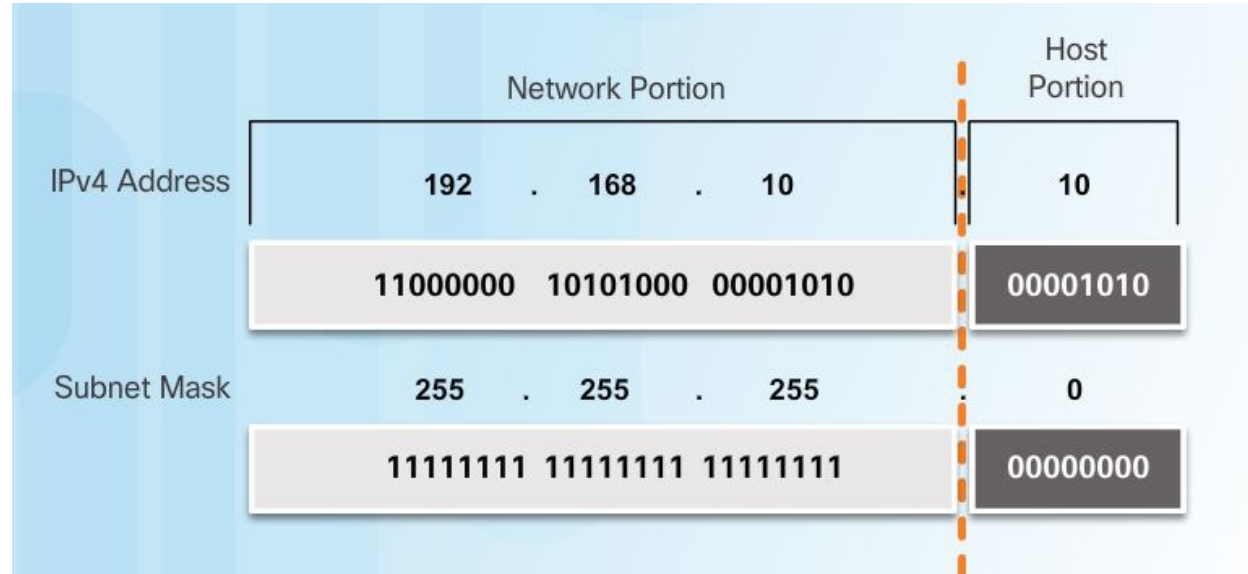
The Subnet Mask

- 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

IPv4 Address Structure

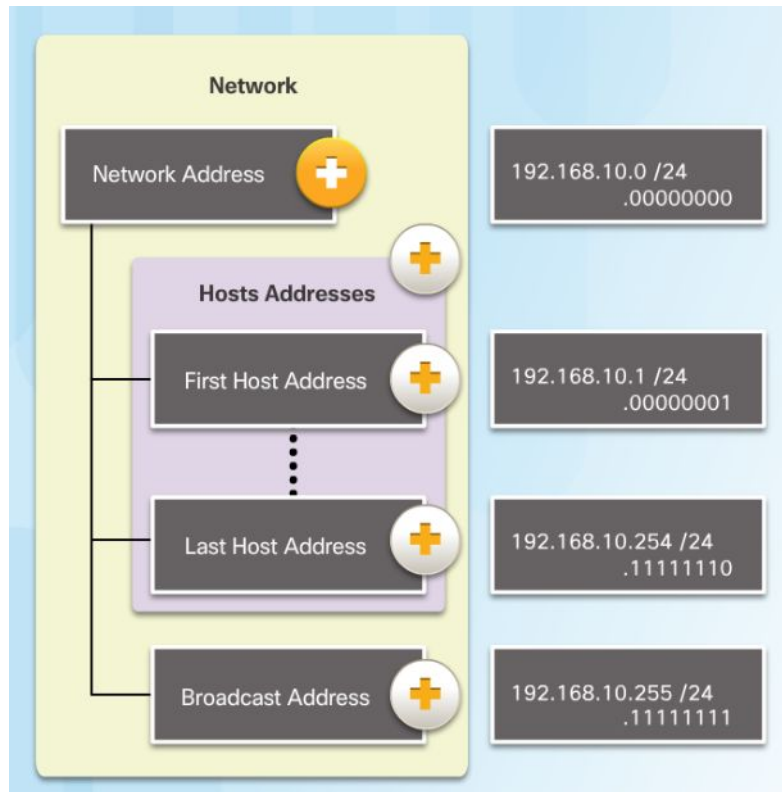
The Prefix Length

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

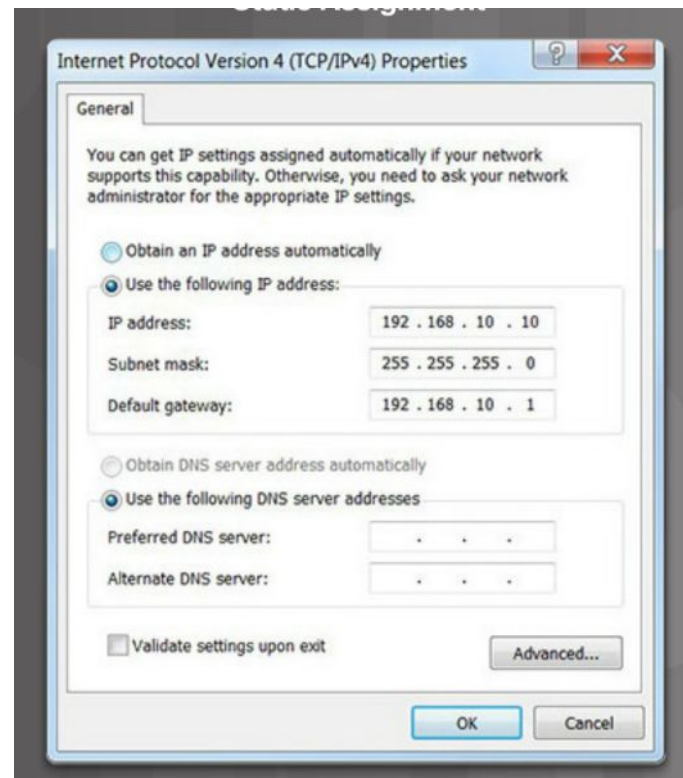


Types of Addresses in Network 192.168.10.0/24

- 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)

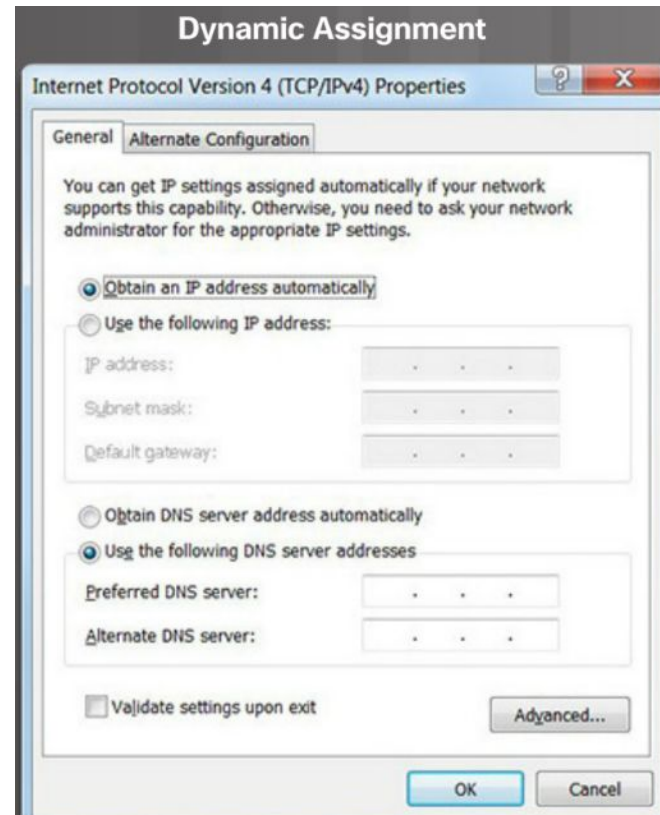
Static IPv4 Address Assignment to a Host

- 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.



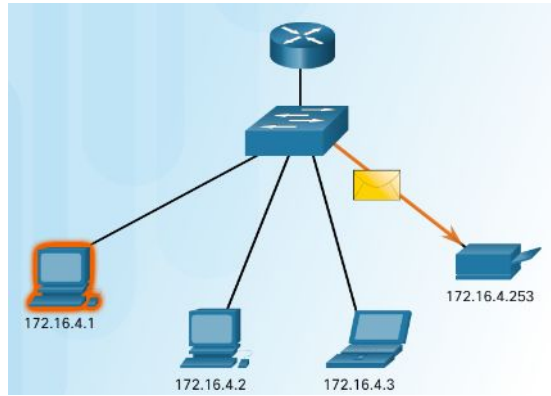
Dynamic IPv4 Address Assignment to a Host

- 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.

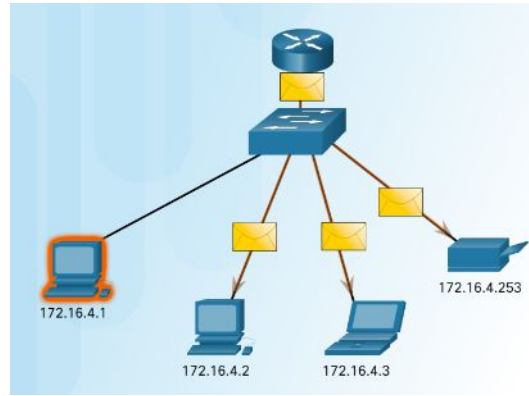


IPv4 Unicast, Broadcast, and Multicast

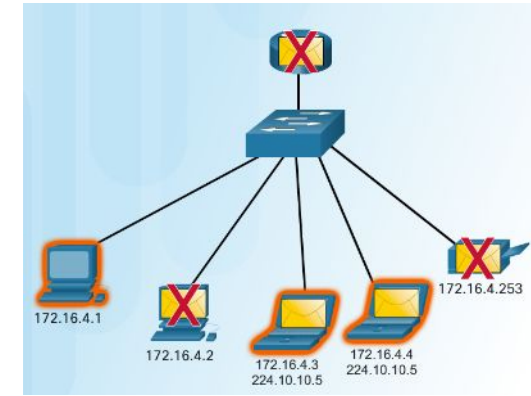
IPv4 Communication



- Unicast – one to one communication.



- Broadcast– one to all.

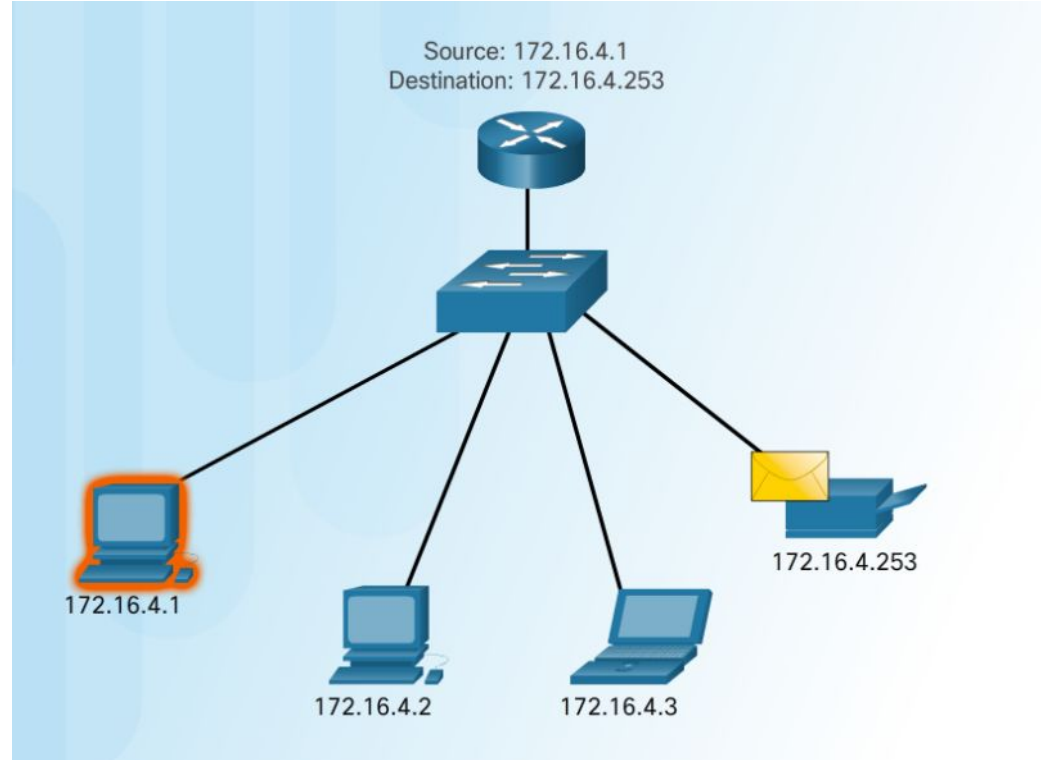


- Multicast – one to a select group.

IPv4 Unicast, Broadcast, and Multicast

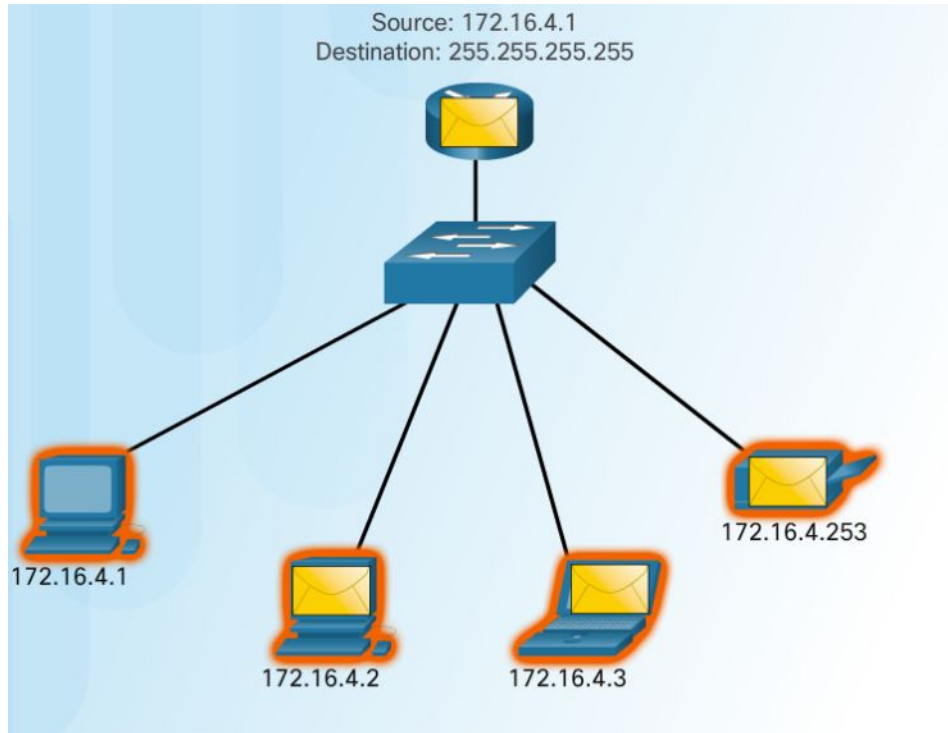
Unicast Transmission

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



IPv4 Unicast, Broadcast, and Multicast

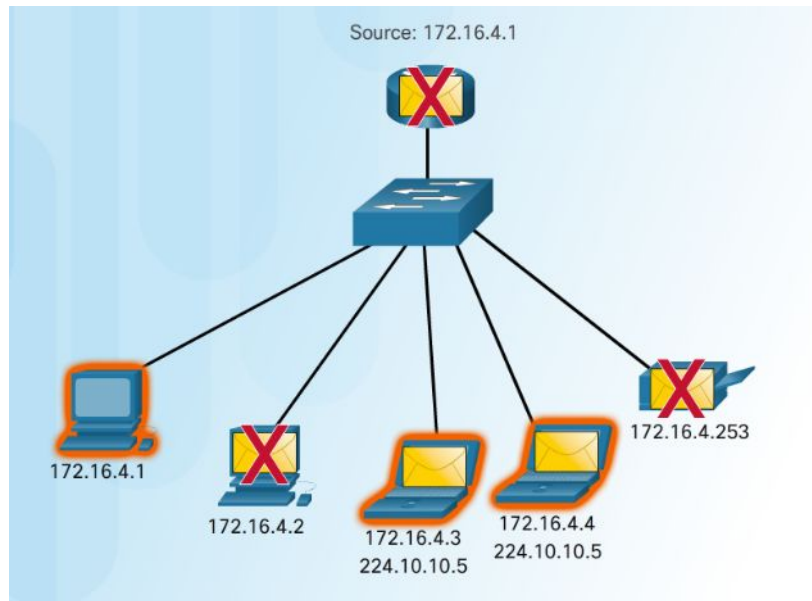
Broadcast Transmission



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

IPv4 Unicast, Broadcast, and Multicast

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.

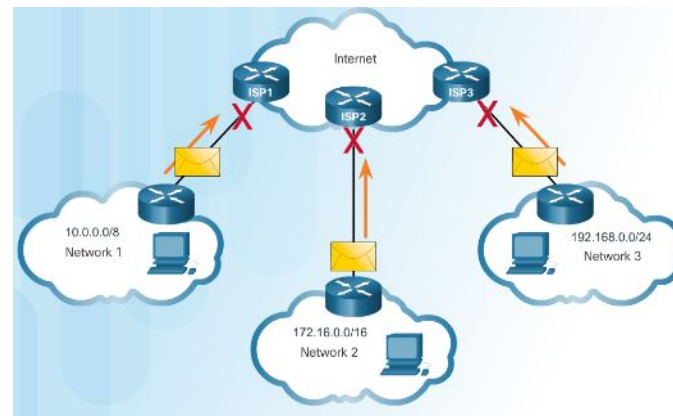
Public and Private IPv4 Addresses

▪ 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 172.31.255.255
- 192.168.0.0 /16 or 192.168.0.0 to 192.168.255.255



Special User IPv4 Addresses

Pinging the Loopback Interface

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad> ping 127.1.1.1

Pinging 127.1.1.1 with 32 bytes of data:

Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.1.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad>

- 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	0xxxxxx.____.____.____

* 0.0.0.0 and 127.0.0.0 are reserved and cannot be assigned

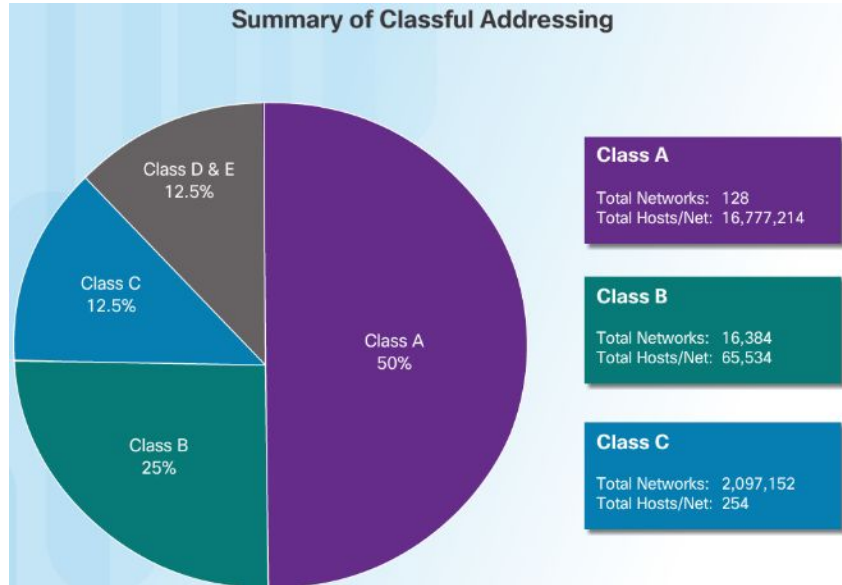
Class B Specifics	
Address Block	128.0.0.0 – 191.255.0.0
Default Subnet Mask	/16 (255.255.0.0)
Maximum Number of Networks	16,384
Number of Host per Network	65,534
High order bit	10xxxxxx.____.____.____

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.

Types of IPv4 Addresses

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.

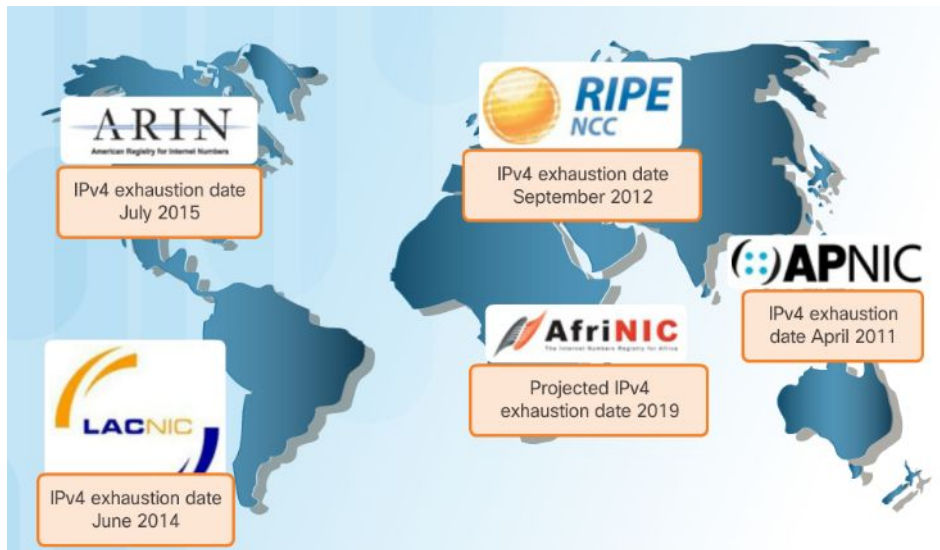
Assignment of IP Addresses



- The following organizations manage and maintain IPv4 and IPv6 addresses for the various regions.
 - American Registry for Internet Numbers (ARIN)- North America.
 - Réseaux IP Européens (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

IPv6 Network Addresses

The Need for IPv6



■ IPv6 versus IPv4:

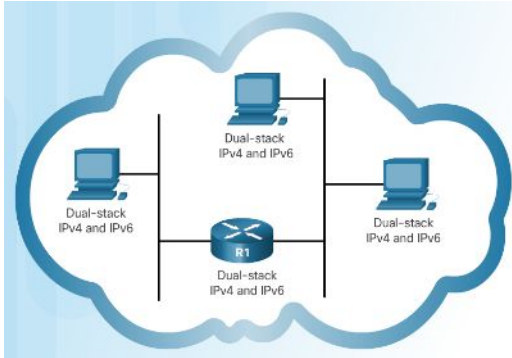
- Has a larger 128-bit address space
- 340 undecillion addresses
- Solves limitations with IPv4
- Adds enhancement like address auto-configuration.

■ Why IPv6 is needed:

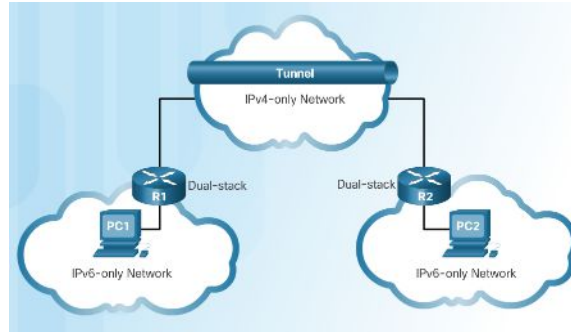
- Rapidly increasing Internet population
- Depletion of IPv4
- Issues with NAT
- Internet of Things

IPv4 and IPv6 Coexistence

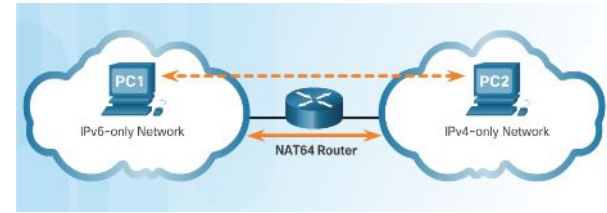
- Migration from IPv4 to IPv6 Techniques



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



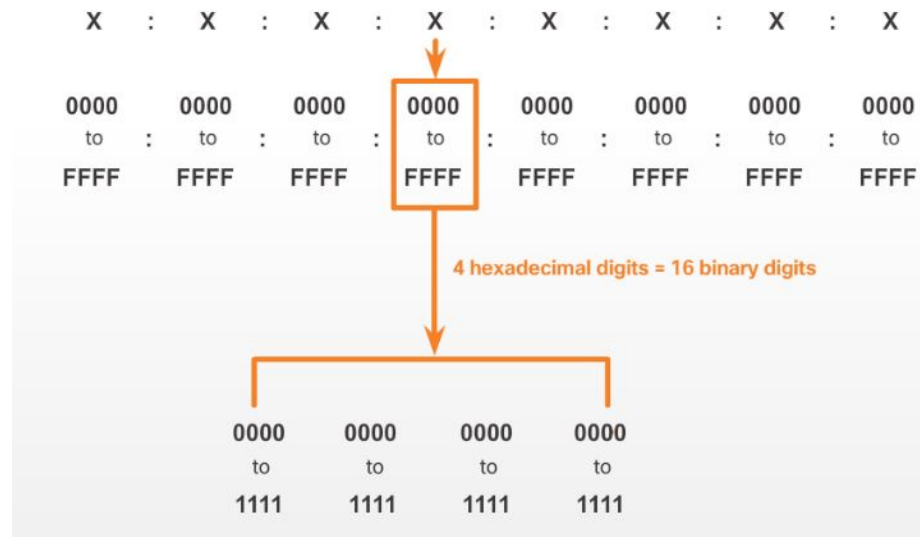
Tunneling - The IPv6 packet is encapsulated inside an IPv4 packet.



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 (hexets) 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.)

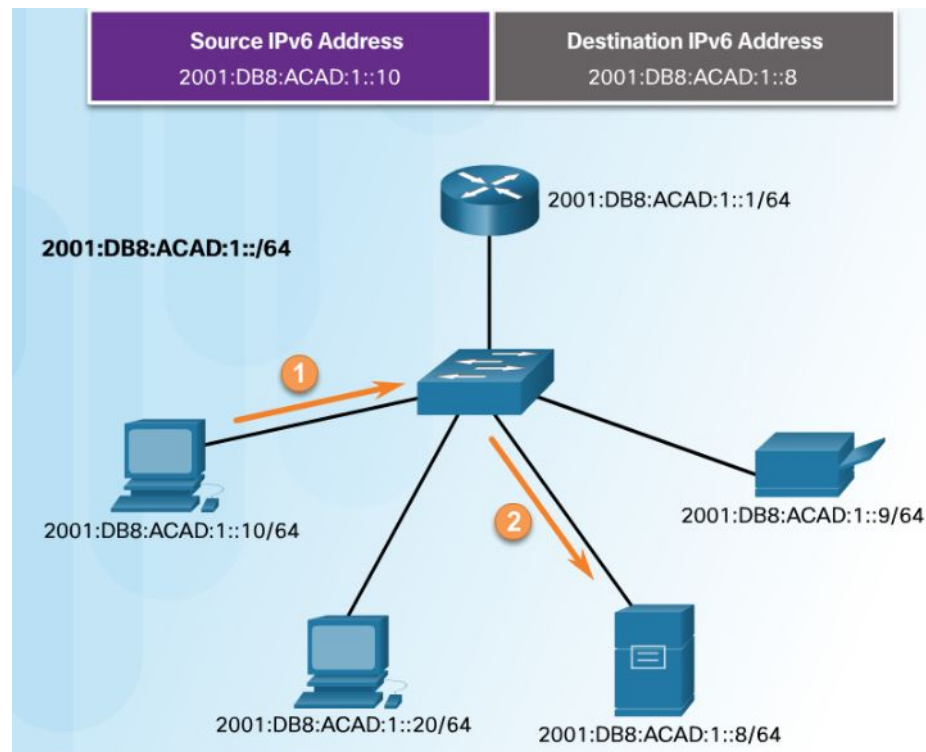
- Rule 2 – Omit All 0 Segments
 - A double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hexets) consisting of all 0s.

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	::

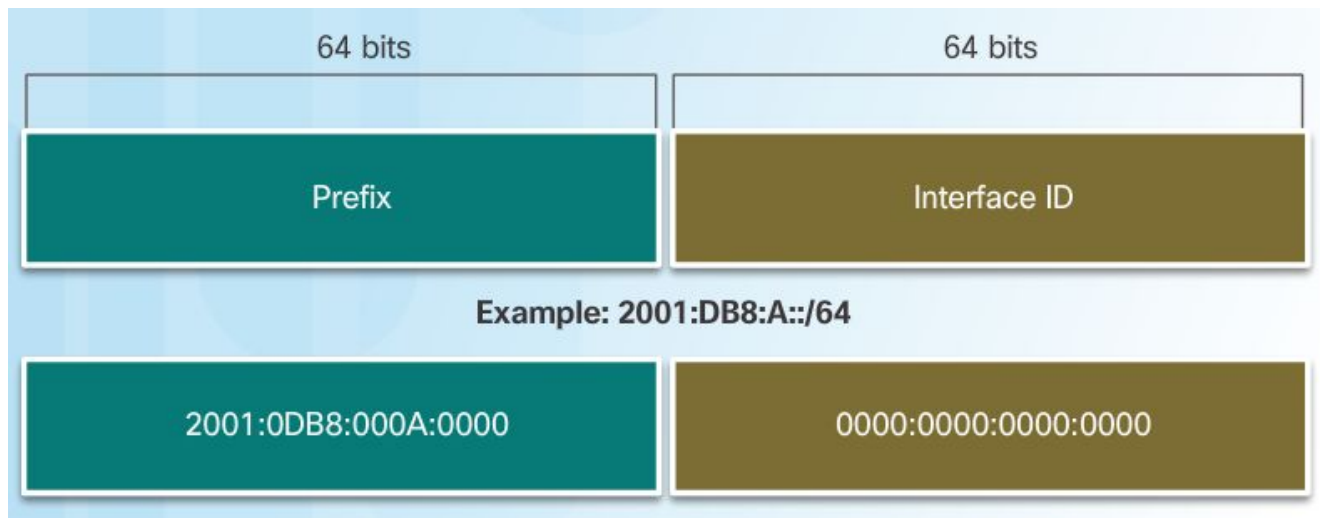
IPv6 Address Types

- 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.



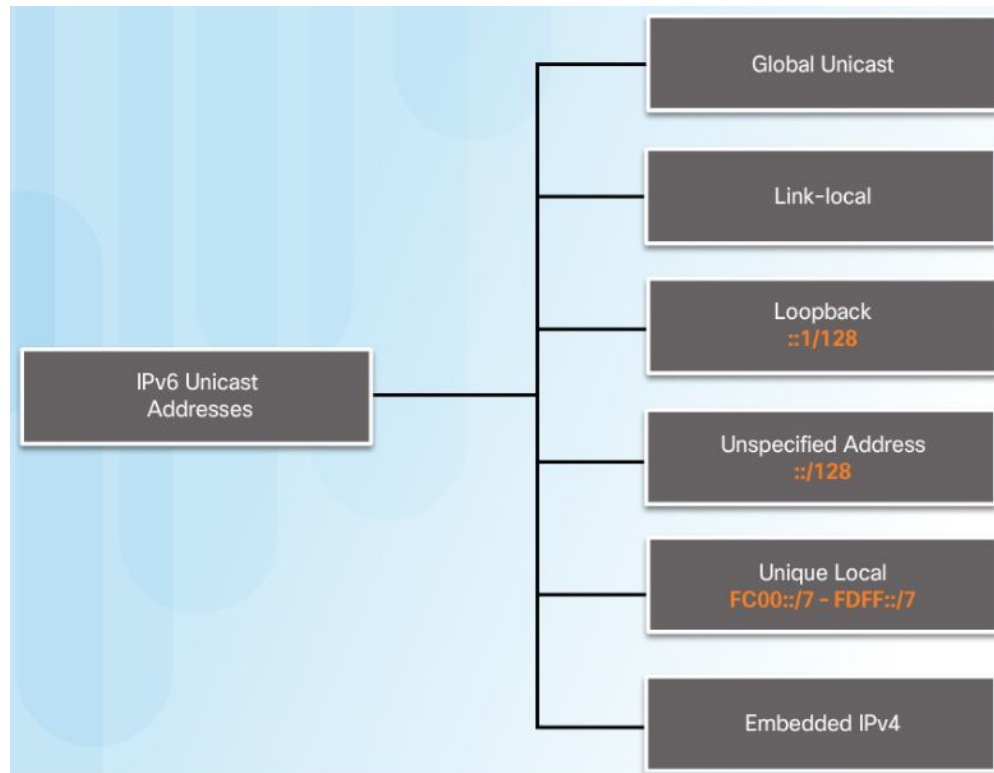
IPv6 Prefix Length

- 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

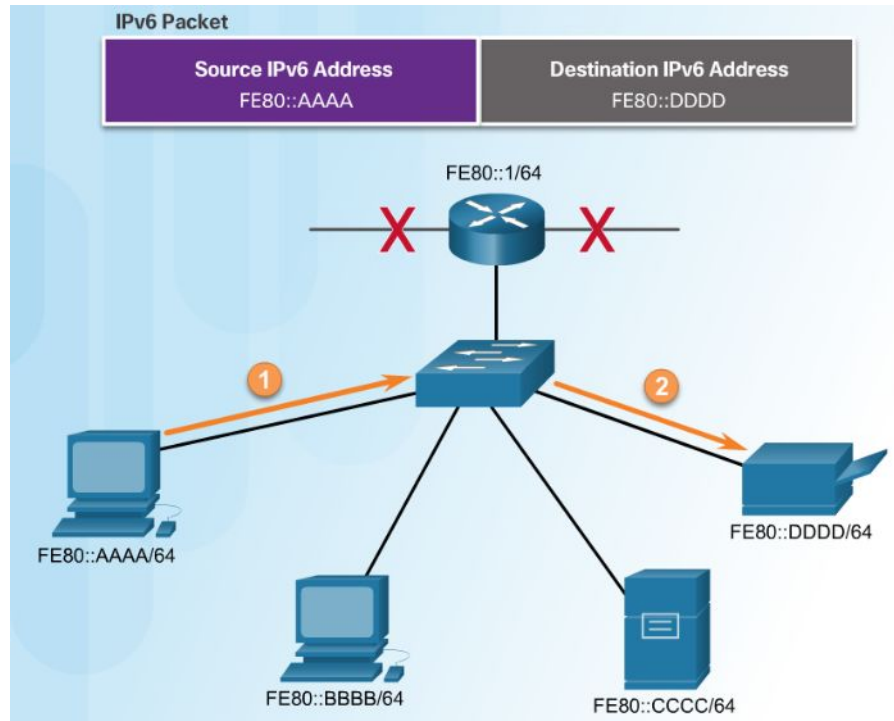
- **Global Unicast** - These are globally unique, Internet routable addresses.
- **Link-local** - used to communicate with other devices on the same local link. Confined to a single link.
- **Unique Local** - used for local addressing within a site or between a limited number of sites.



IPv6 Link-Local Unicast Addresses

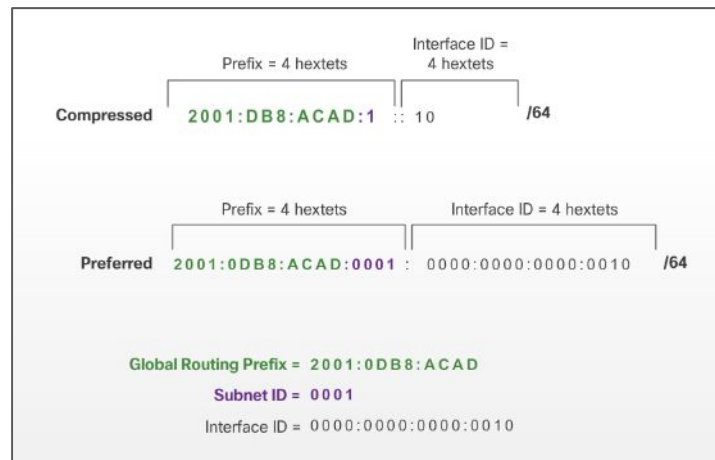
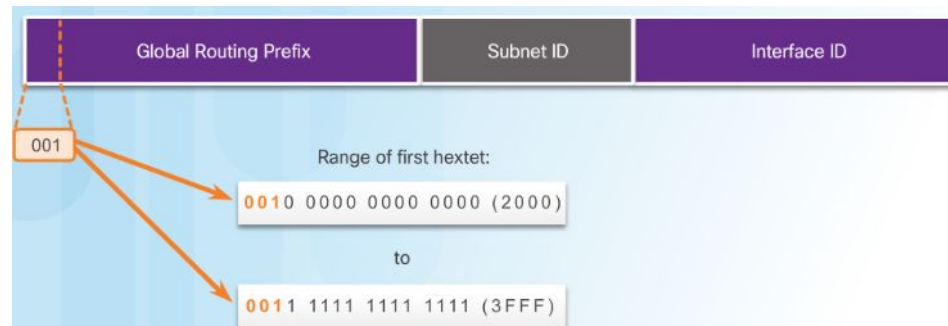
- IPv6 link-local addresses:
 - Enable a device to communicate with other IPv6-enabled devices on the same link only.
 - Are created even if the device has not been assigned a global unicast IPv6 address.
 - Are in the FE80::/10 range.

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



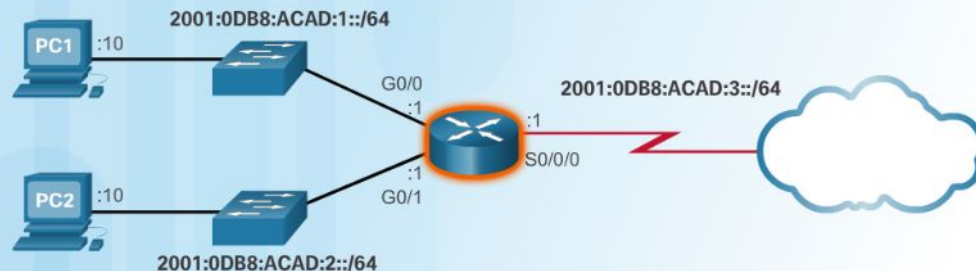
Structure of an IPv6 Global Unicast Address

- Currently, only global unicast addresses with the first three bits of 001 or 2000:: 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

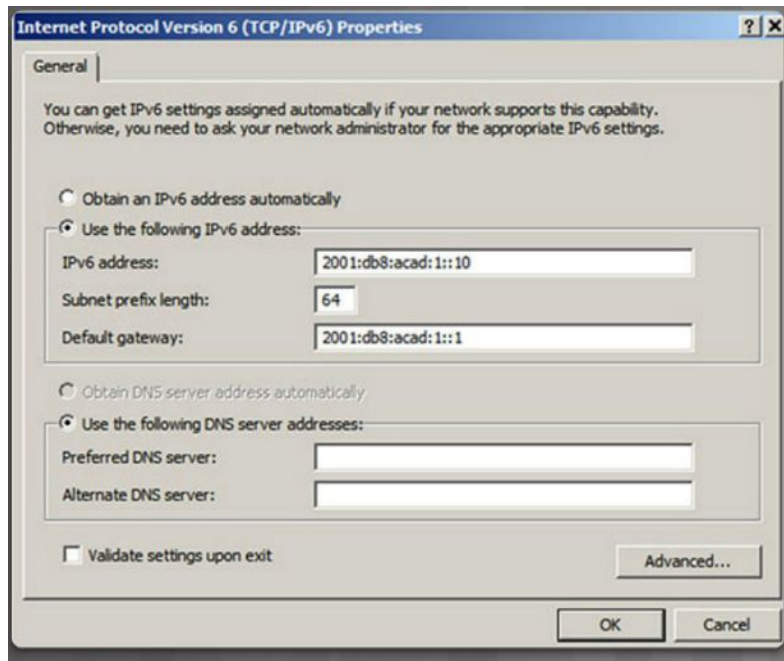
Configuring IPv6 on a Router



```
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 and IPv6 global unicast on an interface is **ipv6 address**
ipv6-address/prefix-length

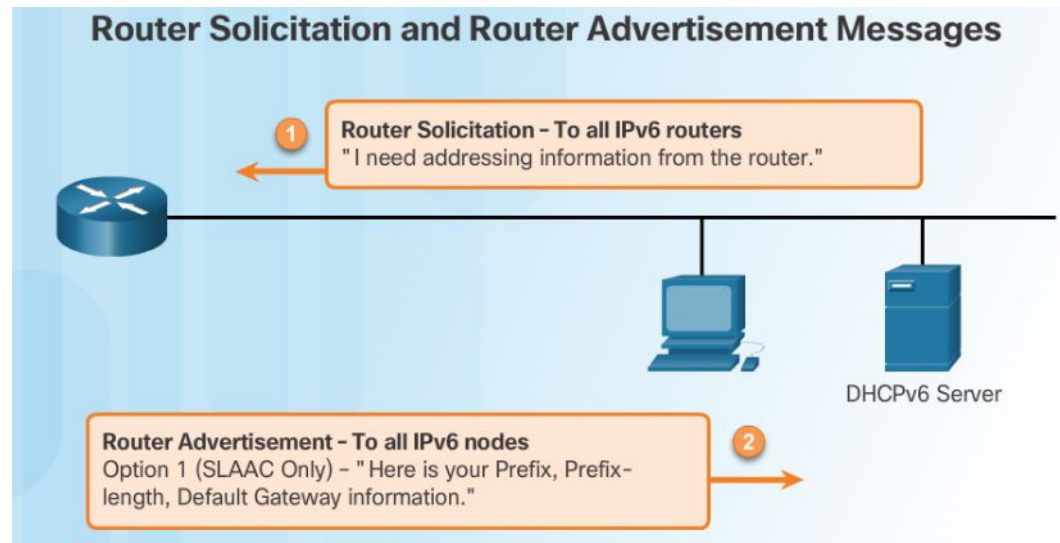
Static Configuration of a Global Unicast Address (Cont.)



- 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.



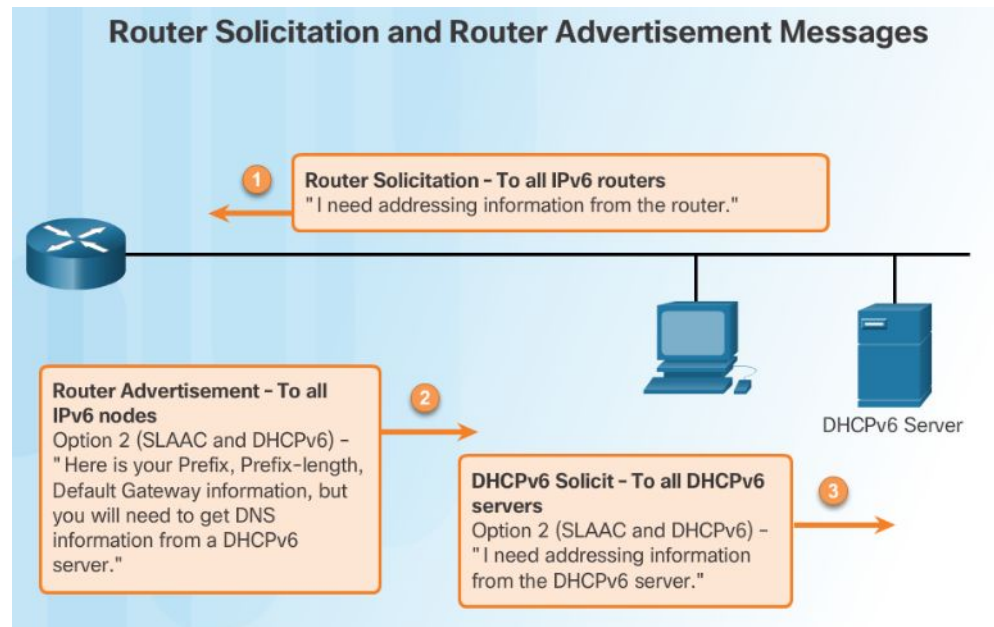
Option 1 (SLAAC Only) – "I'm everything you need (Prefix, Prefix-length, Default Gateway)"

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.



Thanks