



# Module 8: Network Layer

Thomas Wyseur

Introduction to Networks v7.0  
(ITN)





# Module 8: Network Layer

Introduction to Networks v7.0  
(ITN)

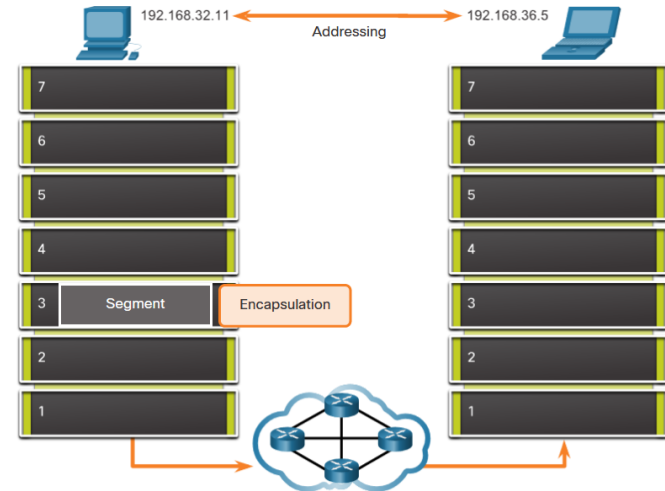
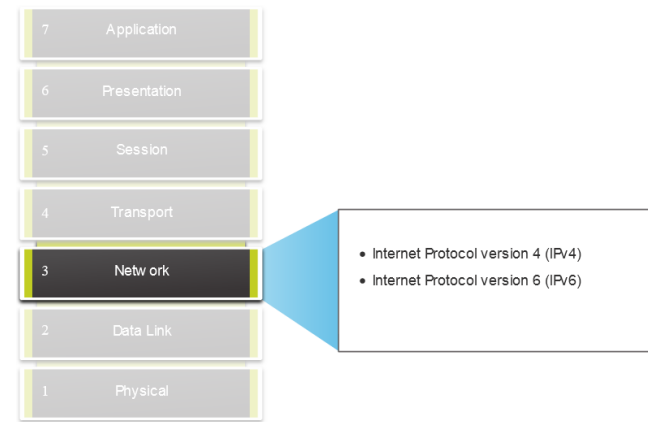


# 8.1 Network Layer Characteristics

# Network Layer Characteristics

## The Network Layer

- Provides services to allow end devices to exchange data
- IP version 4 (IPv4) and IP version 6 (IPv6) are the principle network layer communication protocols.
- The network layer performs four basic operations:
  - Addressing end devices
  - Encapsulation
  - Routing
  - De-encapsulation



Network layer protocols forward transport layer PDUs between hosts.

© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# IP Encapsulation

- IP encapsulates the transport layer segment.
- IP can use either an IPv4 or IPv6 packet and not impact the layer 4 segment.
- IP packet will be examined by all layer 3 devices as it traverses the network.
- The IP addressing does not change from source to destination.

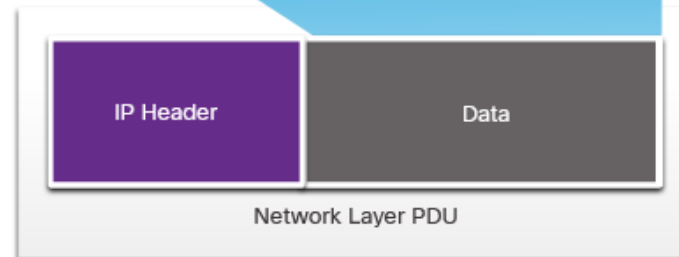
**Note:** NAT will change addressing, but will be discussed in a later module.

Transport Layer Encapsulation



Transport Layer PDU

Network Layer Encapsulation



Network Layer PDU

IP Packet

## Network Layer Characteristics

# Characteristics of IP

IP is meant to have low overhead and may be described as:

- Connectionless
- Best Effort
- Media Independent

# Network Layer Characteristics

## Connectionless

### IP is Connectionless

- IP does not establish a connection with the destination before sending the packet.
- There is no control information needed (synchronizations, acknowledgments, etc.).
- The destination will receive the packet when it arrives, but no pre-notifications are sent by IP.
- If there is a need for connection-oriented traffic, then another protocol will handle this (typically TCP at the transport layer).



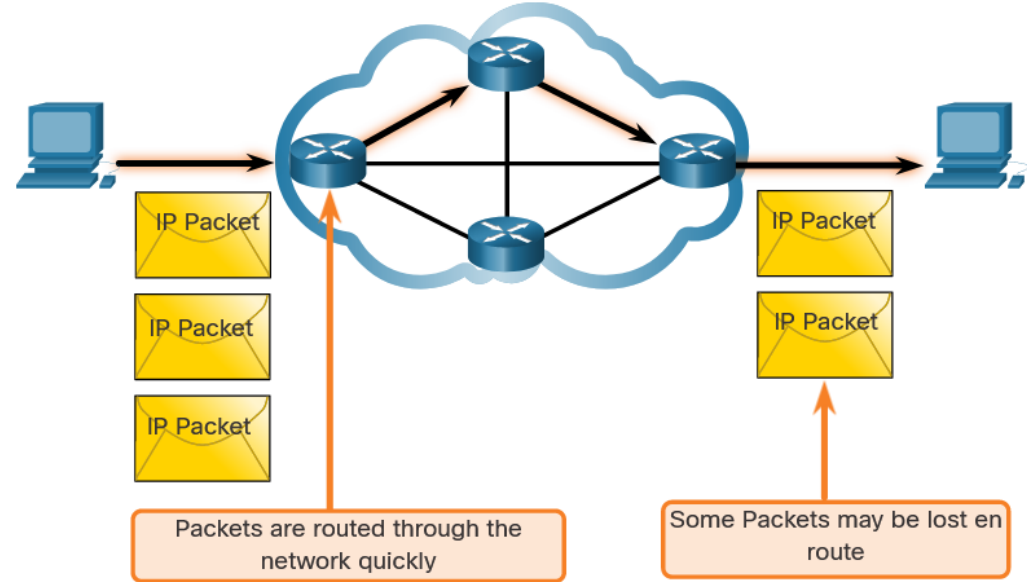
A letter is sent.

# Network Layer Characteristics

## Best Effort

### IP is Best Effort

- IP will not guarantee delivery of the packet.
- IP has reduced overhead since there is no mechanism to resend data that is not received.
- IP does not expect acknowledgments.
- IP does not know if the other device is operational or if it received the packet.





# Network Layer Characteristics

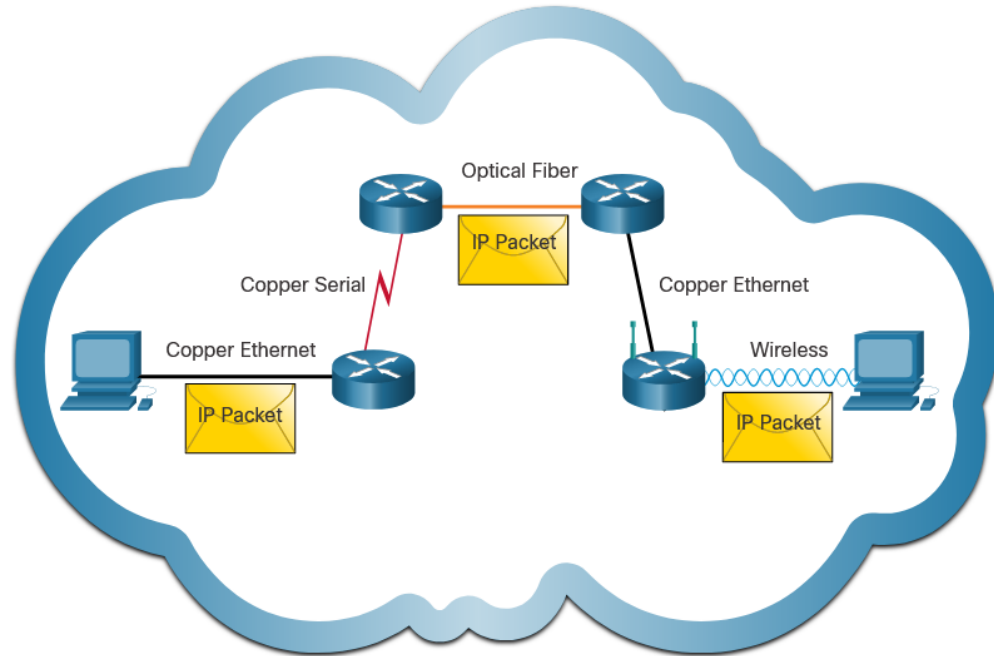
## Media Independent

IP is unreliable:

- It cannot manage or fix undelivered or corrupt packets.
- IP cannot retransmit after an error.
- IP cannot realign out of sequence packets.
- IP must rely on other protocols for these functions.

IP is media Independent:

- IP does not concern itself with the type of frame required at the data link layer or the media type at the physical layer.
- IP can be sent over any media type: copper, fiber, or wireless.



## Network Layer Characteristics

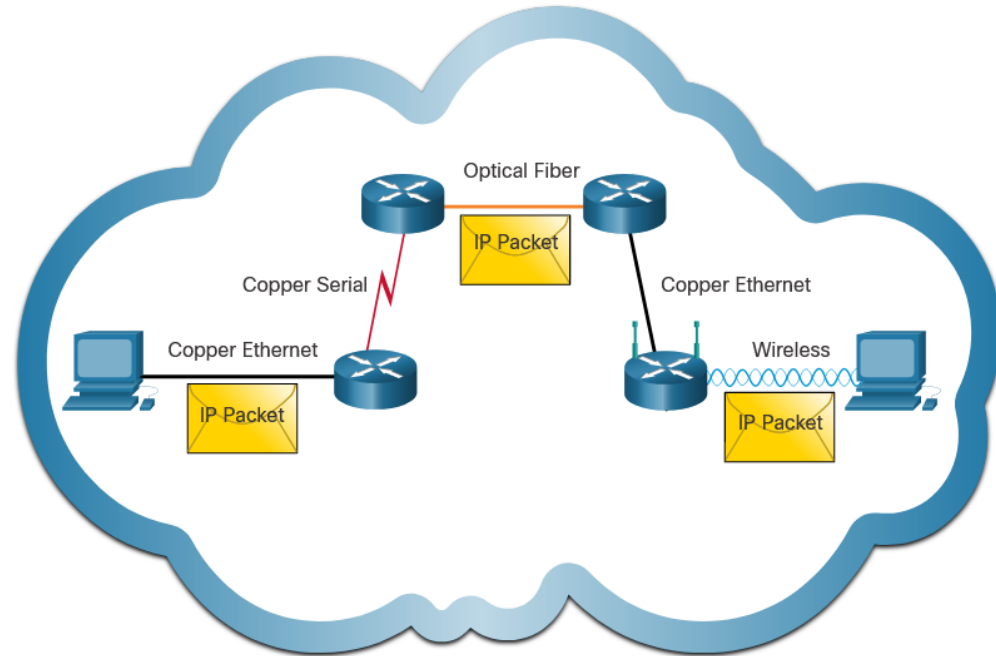
# Media Independent (Contd.)

The network layer will establish the Maximum Transmission Unit (MTU).

- Network layer receives this from control information sent by the data link layer.
- The network then establishes the MTU size.

Fragmentation is when Layer 3 splits the IPv4 packet into smaller units.

- Fragmenting causes latency.
- IPv6 does not fragment packets.
- Example: Router goes from Ethernet to a slow WAN with a smaller MTU



# 8.2 IPv4 Packet

# IPv4 Packet Header

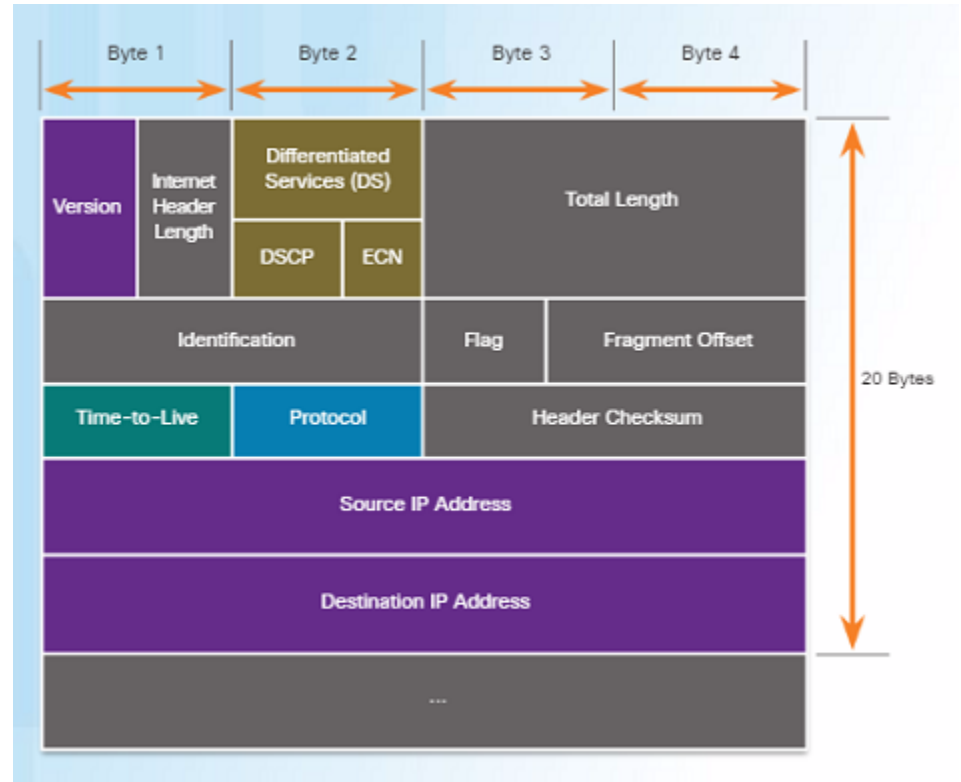
IPv4 is the primary communication protocol for the network layer.

The network header has many purposes:

- It ensures the packet is sent in the correct direction (to the destination).
- It contains information for network layer processing in various fields.
- The information in the header is used by all layer 3 devices that handle the packet

# 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.



# Video – Sample IPv4 Headers in Wireshark

This video will cover the following:

- IPv4 Ethernet packets in Wireshark
- The control information
- The difference between packets

## 8.3 IPv6 Packets

# 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 Overview


- IPv6 was developed by Internet Engineering Task Force (IETF).
- IPv6 overcomes the limitations of IPv4.
- Improvements that IPv6 provides:
  - **Increased address space** – based on 128 bit address, not 32 bits
  - **Improved packet handling** – simplified header with fewer fields
  - **Eliminates the need for NAT** – since there is a huge amount of addressing, there is no need to use private addressing internally and be mapped to a shared public address

## IPv4 and IPv6 Address Space Comparison

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

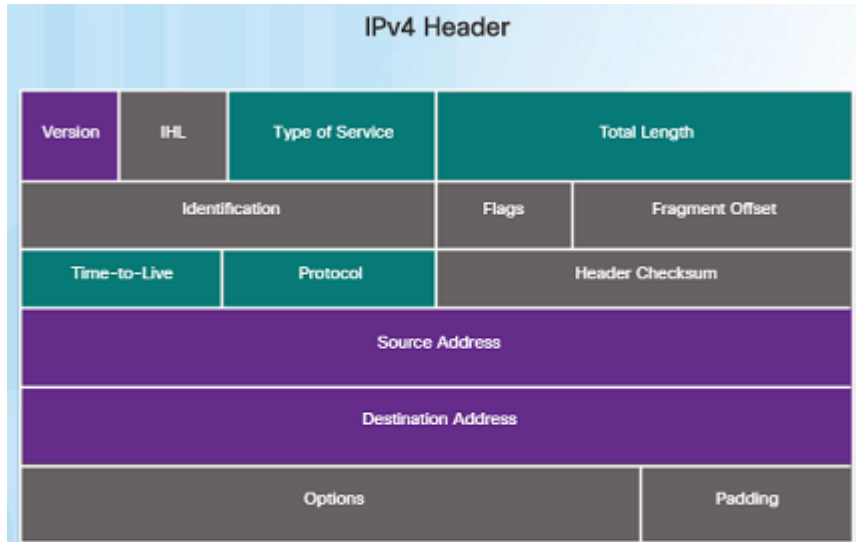
Legend

 There are 4 billion IPv4 addresses

 There are 340 undecillion IPv6 addresses

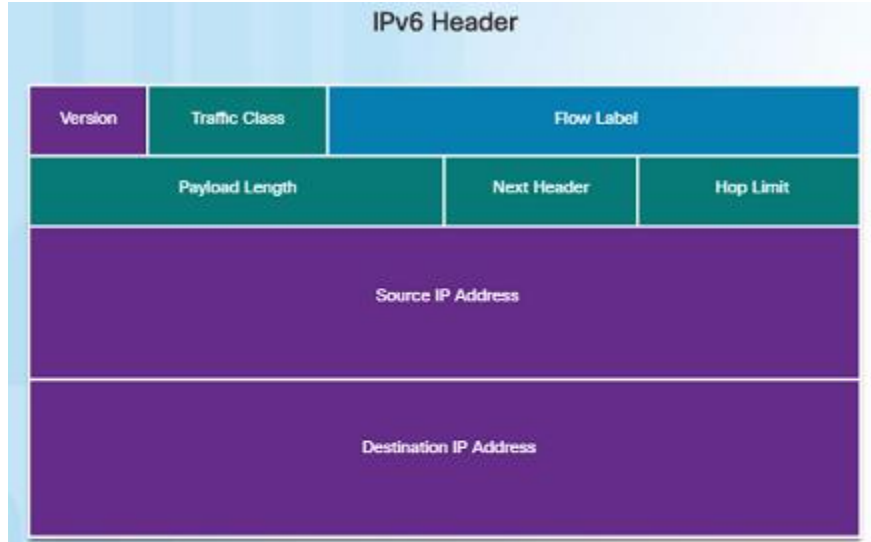
## Encapsulating IPv6

- The IPv6 header is simpler than the IPv4 header.



**Legend**

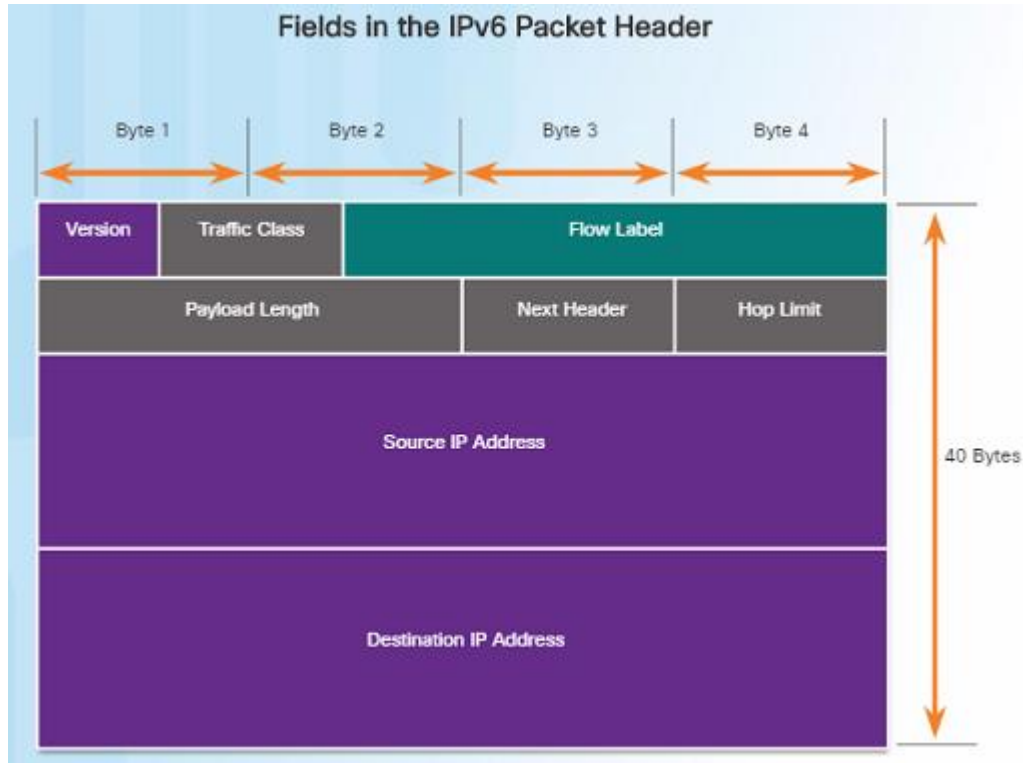
- Field names kept from IPv4 to IPv6
- Name and position changed in IPv6
- Fields not kept in IPv6



**Legend**

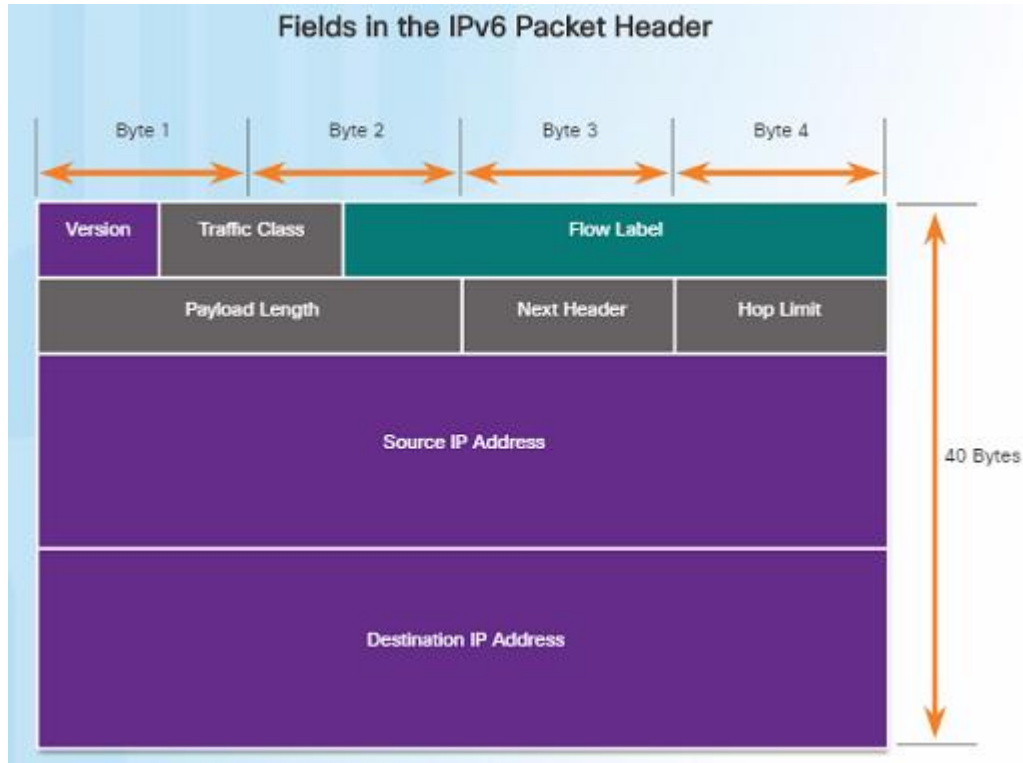
- Field names kept from IPv4 to IPv6
- Name and position changed in IPv6
- New field in IPv6

## 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.

# IPv6 Packet Header (Cont.)

IPv6 packet may also contain extension headers (EH).

EH headers characteristics:

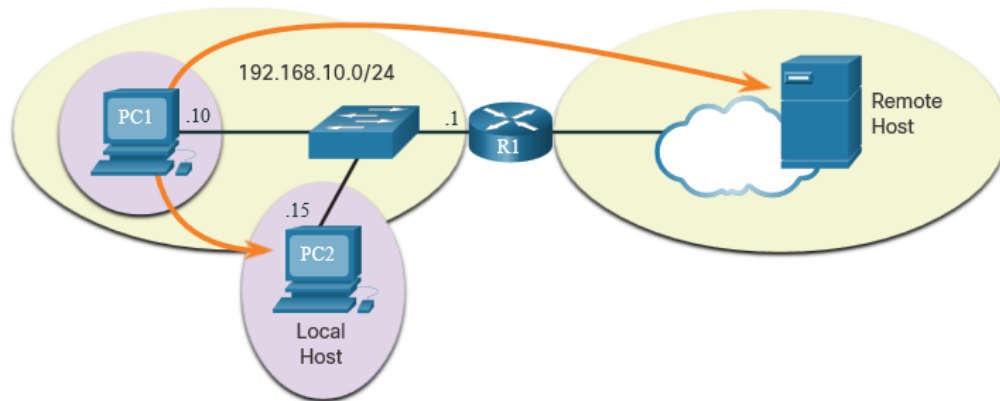
- provide optional network layer information
- are optional
- are placed between IPv6 header and the payload
- may be used for fragmentation, security, mobility support, etc.

**Note:** Unlike IPv4, routers do not fragment IPv6 packets.

# 8.4 How a Host Routes

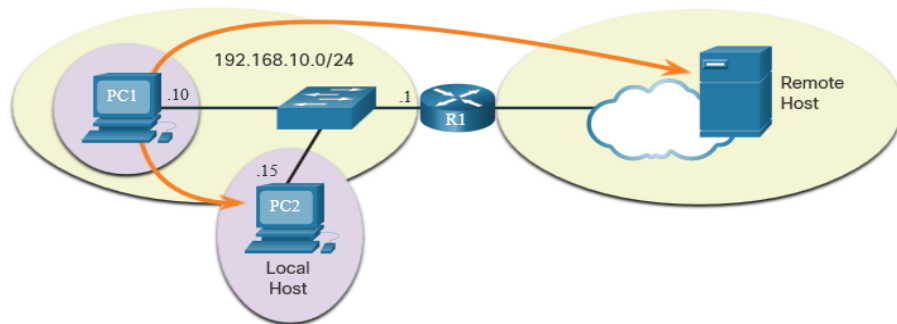
# Host Forwarding Decision

- Packets are always created at the source.
- Each host devices creates their own routing table.
- A host can send packets to the following:
  - Itself – 127.0.0.1 (IPv4), ::1 (IPv6)
  - Local Hosts – destination is on the same LAN
  - Remote Hosts – devices are not on the same LAN



# Host Forwarding Decision (Cont.)

- The Source device determines whether the destination is local or remote
- Method of determination:
  - IPv4 – Source uses its own IP address and Subnet mask, along with the destination IP address
  - IPv6 – Source uses the network address and prefix advertised by the local router
- Local traffic is dumped out the host interface to be handled by an intermediary device.
- Remote traffic is forwarded directly to the default gateway on the LAN.





# Default Gateway

A router or layer 3 switch can be a default-gateway.

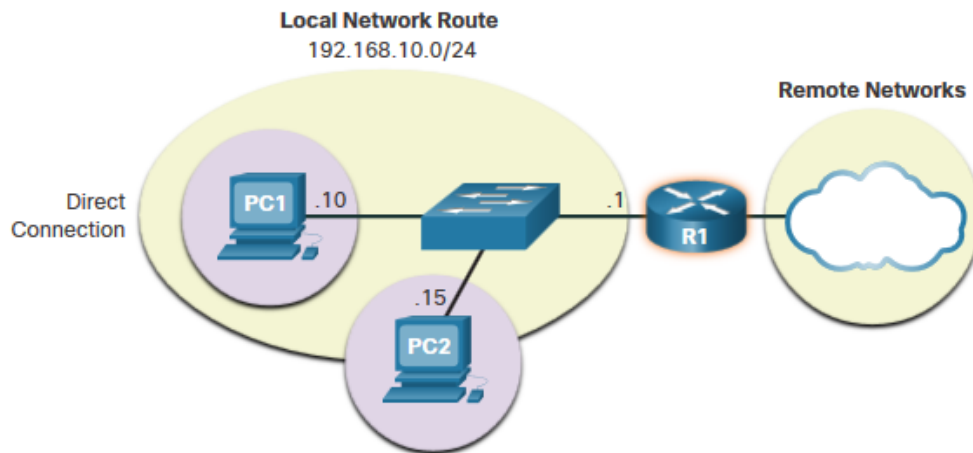
Features of a default gateway (DGW):

- It must have an IP address in the same range as the rest of the LAN.
- It can accept data from the LAN and is capable of forwarding traffic off of the LAN.
- It can route to other networks.

If a device has no default gateway or a bad default gateway, its traffic will not be able to leave the LAN.

# A Host Routes to the Default Gateway

- The host will know the default gateway (DGW) either statically or through DHCP in IPv4.
- IPv6 sends the DGW through a router solicitation (RS) or can be configured manually.
- A DGW is static route which will be a last resort route in the routing table.
- All device on the LAN will need the DGW of the router if they intend to send traffic remotely.



# How a Host Routes

## Host Routing Tables

- On Windows, route print or netstat -r to display the PC routing table
- Three sections displayed by these two commands:
  - Interface List – all potential interfaces and MAC addressing
  - IPv4 Routing Table
  - IPv6 Routing Table



### IPv4 Routing Table for PC1

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

#### IPv4 Route Table

##### Active Routes:

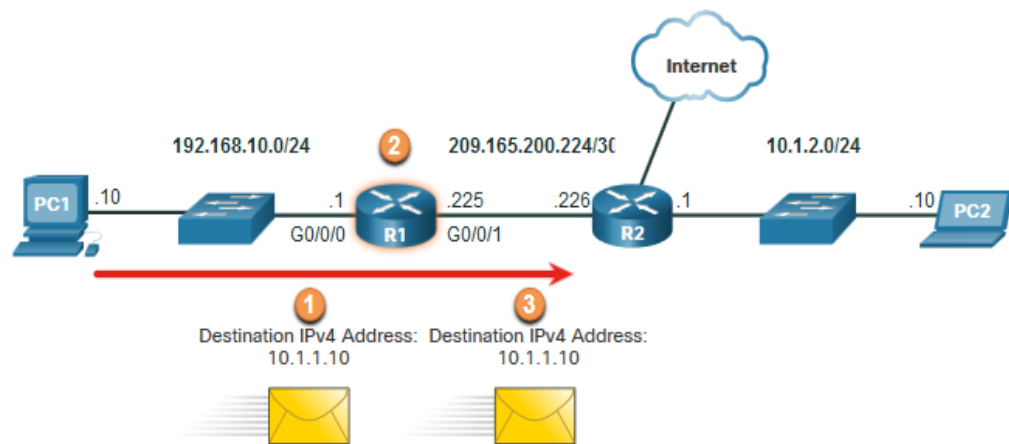
Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	25
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
	127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
	192.168.10.0	255.255.255.0	On-link	192.168.10.10	281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

# 8.5 Introduction to Routing

# Introduction to Routing

## Router Packet Forwarding Decision

What happens when the router receives the frame from the host device?



R1 Routing Table

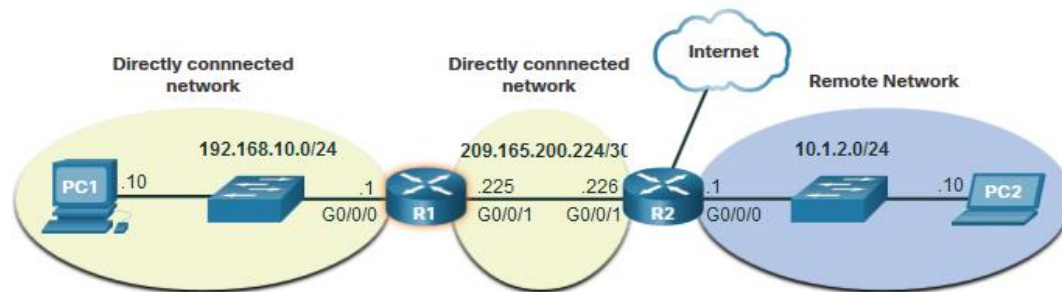
Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	via R2
Default Route 0.0.0.0/0	via R2

1. Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-encapsulates the Layer 2 Ethernet header and trailer.
2. Router R1 examines the destination IPv4 address of the packet and searches for the best match in its IPv4 routing table. The route entry indicates that this packet is to be forwarded to router R2.
3. Router R1 encapsulates the packet into a new Ethernet header and trailer, and forwards the packet to the next hop router R2.

# IP Router Routing Table

There are three types of routes in a router's routing table:

- **Directly Connected** – These routes are automatically added by the router, provided the interface is active and has addressing.
- **Remote** – These are the routes the router does not have a direct connection and may be learned:
  - Manually – with a static route
  - Dynamically – by using a routing protocol to have the routers share their information with each other
- **Default Route** – this forwards all traffic to a specific direction when there is not a match in the routing table

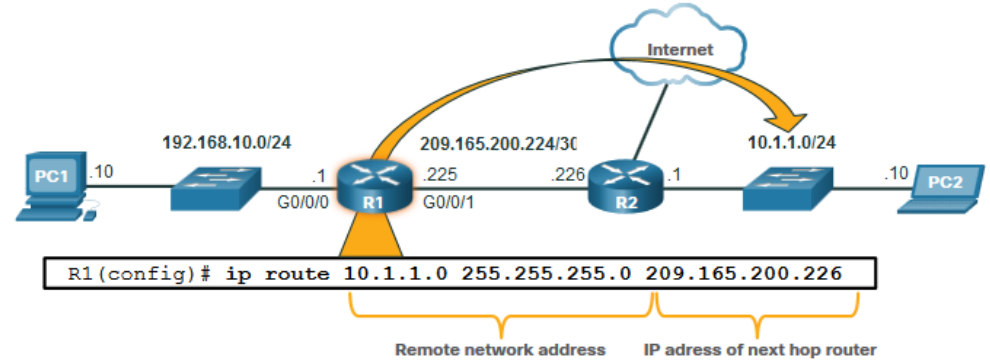


# Introduction to Routing

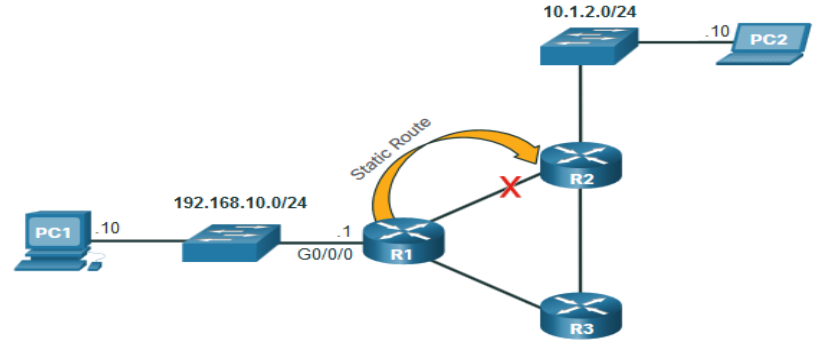
## Static Routing

### Static Route Characteristics:

- Must be configured manually
- Must be adjusted manually by the administrator when there is a change in the topology
- Good for small non-redundant networks
- Often used in conjunction with a dynamic routing protocol for configuring a default route



R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.



If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

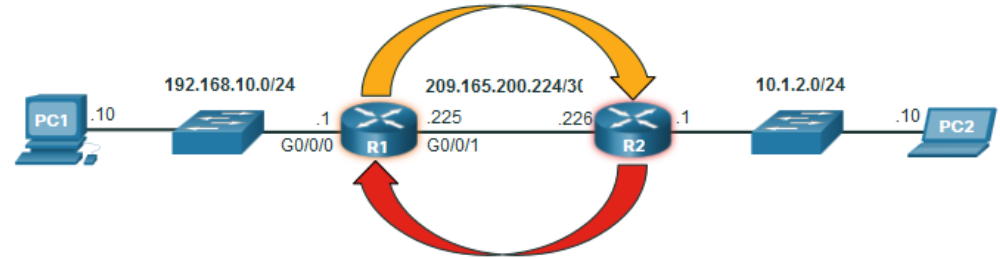
# Introduction to Routing

## Dynamic Routing

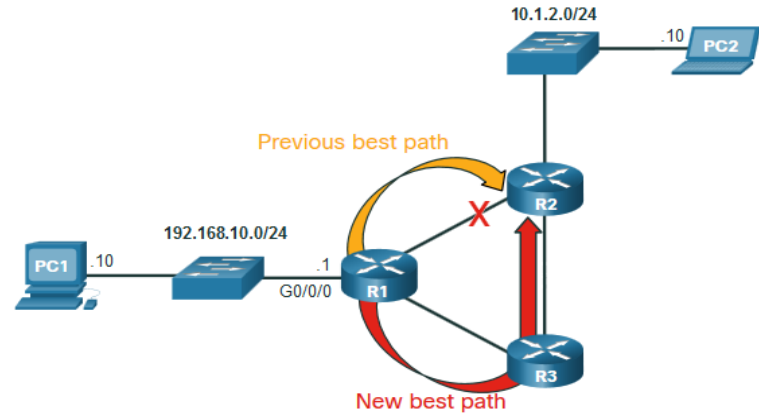
### Dynamic Routes Automatically:

- Discover remote networks
- Maintain up-to-date information
- Choose the best path to the destination
- Find new best paths when there is a topology change

Dynamic routing can also share static default routes with the other routers.



- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.



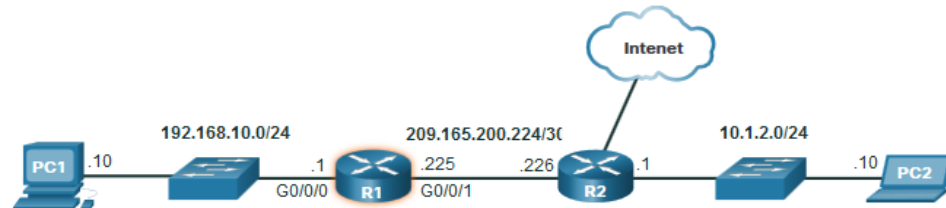
R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.



# Introduction to an IPv4 Routing Table

The **show ip route** command shows the following route sources:

- **L** - Directly connected local interface IP address
- **C** – Directly connected network
- **S** – Static route was manually configured by an administrator
- **O** – OSPF
- **D** – EIGRP



This command shows types of routes:

- Directly Connected – C and L
- Remote Routes – O, D, etc.
- Default Routes – S\*

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*   0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
     10.0.0.0/24 is subnetted, 1 subnets
O    10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.0/24 is directly connected, GigabitEthernet0/0/1
L    209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

# 8.6 Module Practice and Quiz

