Elk Technologies
https://elktech.org
Scott Stephenson

Module 8: Network Layer

Introduction to Networks

Cisco | Networking Academy®
Mind Wide Open™

Module 8: Topics

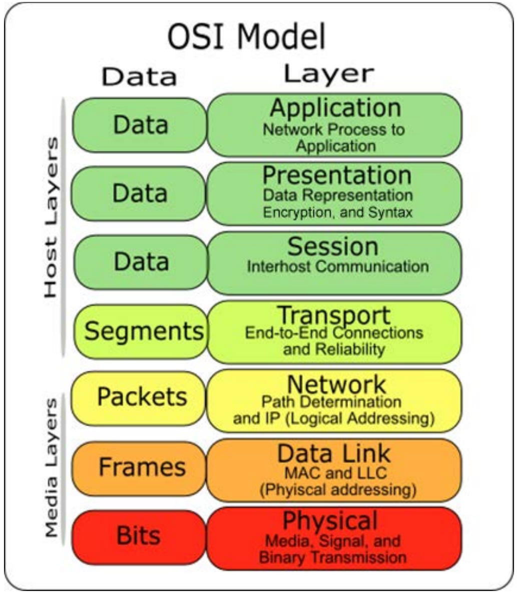
- What will I learn to do in this module?

Topic Title	Topic Objective
8.1 Network Layer Characteristics	Explain how the network layer uses IP protocols for reliable communications.
8.2 IPv4 Packet	Explain the role of the major header fields in the IPv4 packet.
8.3 IPv6 Packet	Explain the role of the major header fields in the IPv6 packet.
8.4 How a Host Routes	Explain how network devices use routing tables to direct packets to a destination network.
8.5 Router Routing Tables	Explain the function of fields in the routing table of a router.

8.1 Network Layer Characteristics

The Network Layer

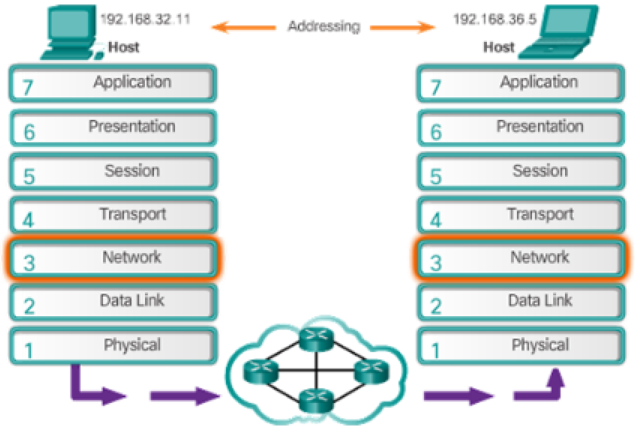
- Provides services to allow end devices to exchange data.
- Common Network Layer Routed Protocols
  - Internet Protocol version 4 (IPv4)
  - Internet Protocol version 6 (IPv6)
- Legacy Network Layer Protocols
  - Novell Internetwork Packet Exchange (IPX)
  - AppleTalk
  - Connectionless Network Service (CLNS/DECNet)
- Note: Legacy network layer protocols are not discussed in this course



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
    - Ability to operate without regard to the data that is carried in each packet .
  - **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.
    - **Path Determination** – 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.

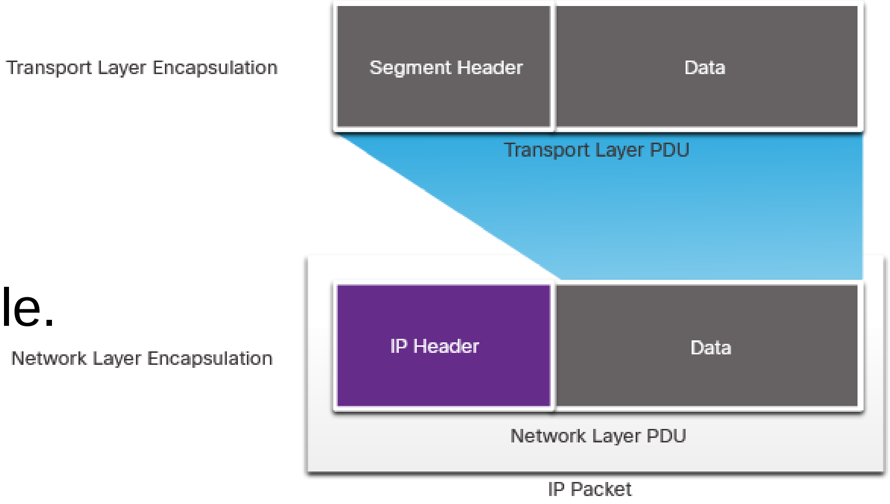
The Exchange of Data



Network layer protocols forward transport layer PDUs between hosts.

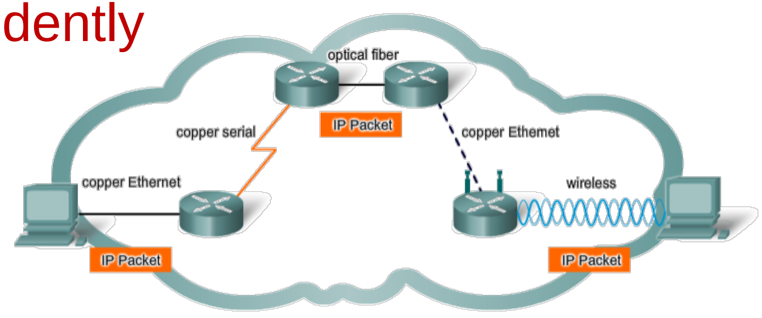
IP Encapsulation

- IP encapsulates the transport layer segment.
- Network layer protocols forward Transport layer PDUs between hosts.
- 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.



Characteristics of IP

- IP provides only the functions required to deliver a packet from the source to a destination.
- IP is meant to have low overhead and may be described as:
  - **Connectionless** – Packet is sent to the destination without prior establishment of a connection.
  - **Best Effort** – Was not designed to track and manage the flow of packets.
  - **Media Independent** – Operates independently from the media.
- Note: These functions, if required, are performed by other layers – primarily TCP.



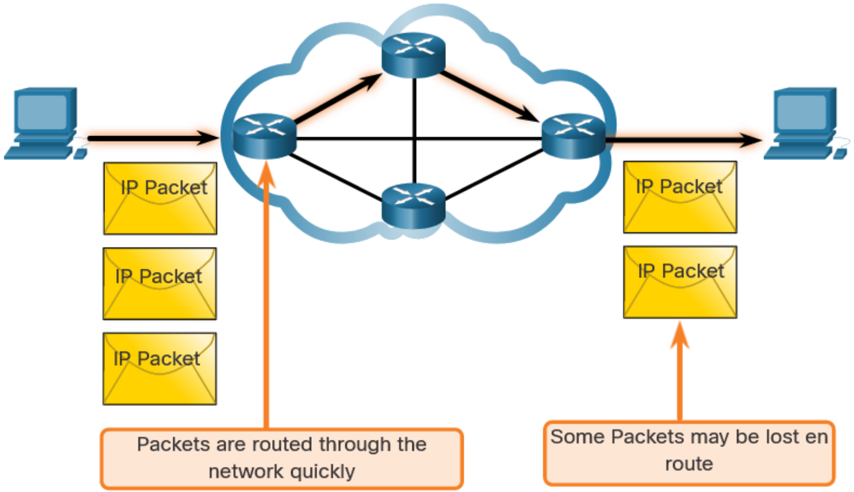
IP packets can travel over different media.

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).

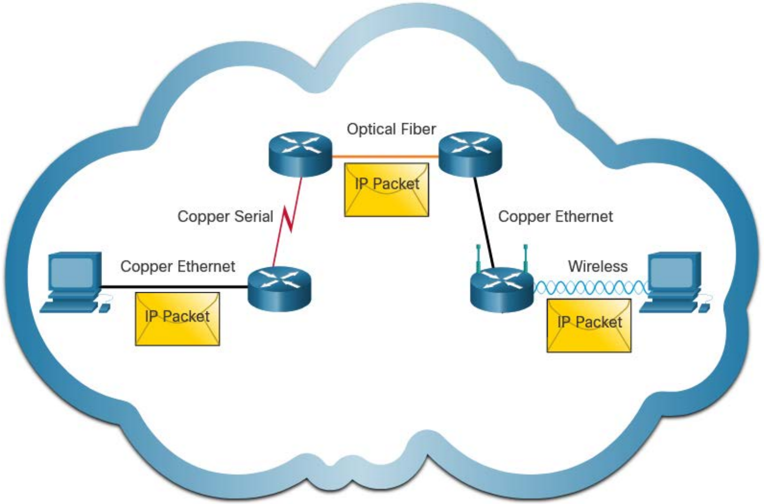
Best Effort

- 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.
- IP relies on upper layer services to handle situations of missing or out-of-order packets.



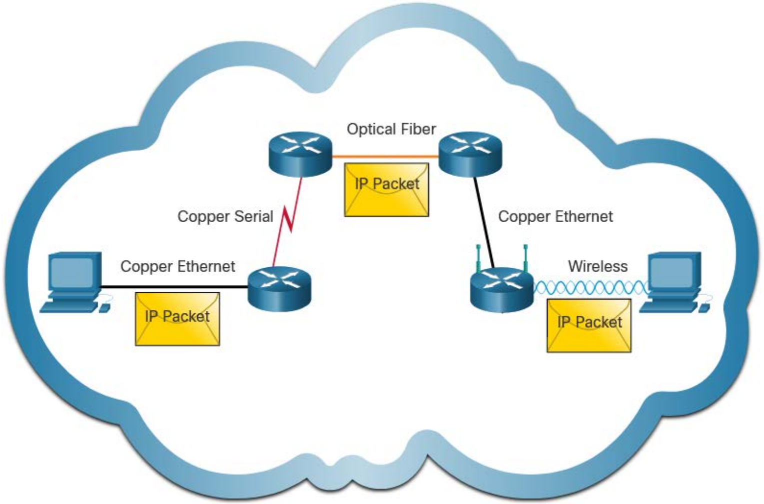
Media Independent

- 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.



Media Independent

- 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

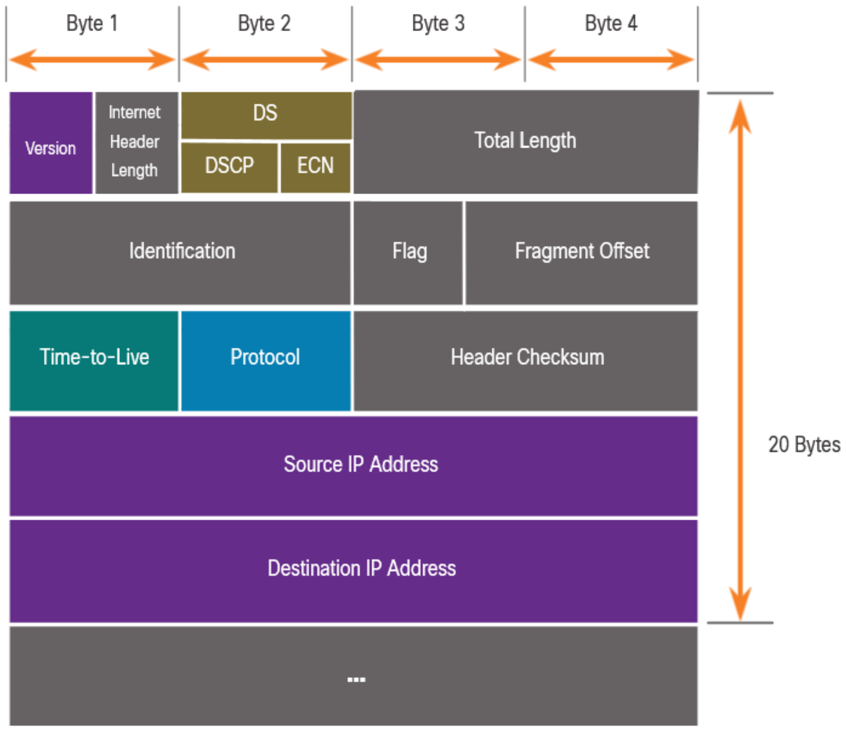
IPv4 Packet Header

- 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 Fields

- The IPv4 network header characteristics:
  - It is in binary.
  - Contains several fields of information
  - Diagram is read from left to right, 4 bytes per line
  - The two most important fields are the source and destination.

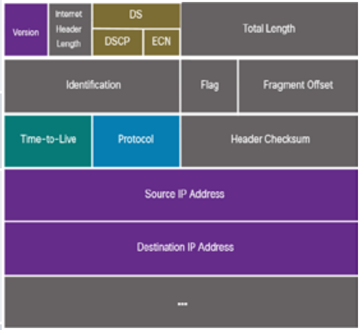
- Protocols may have may have one or more functions.



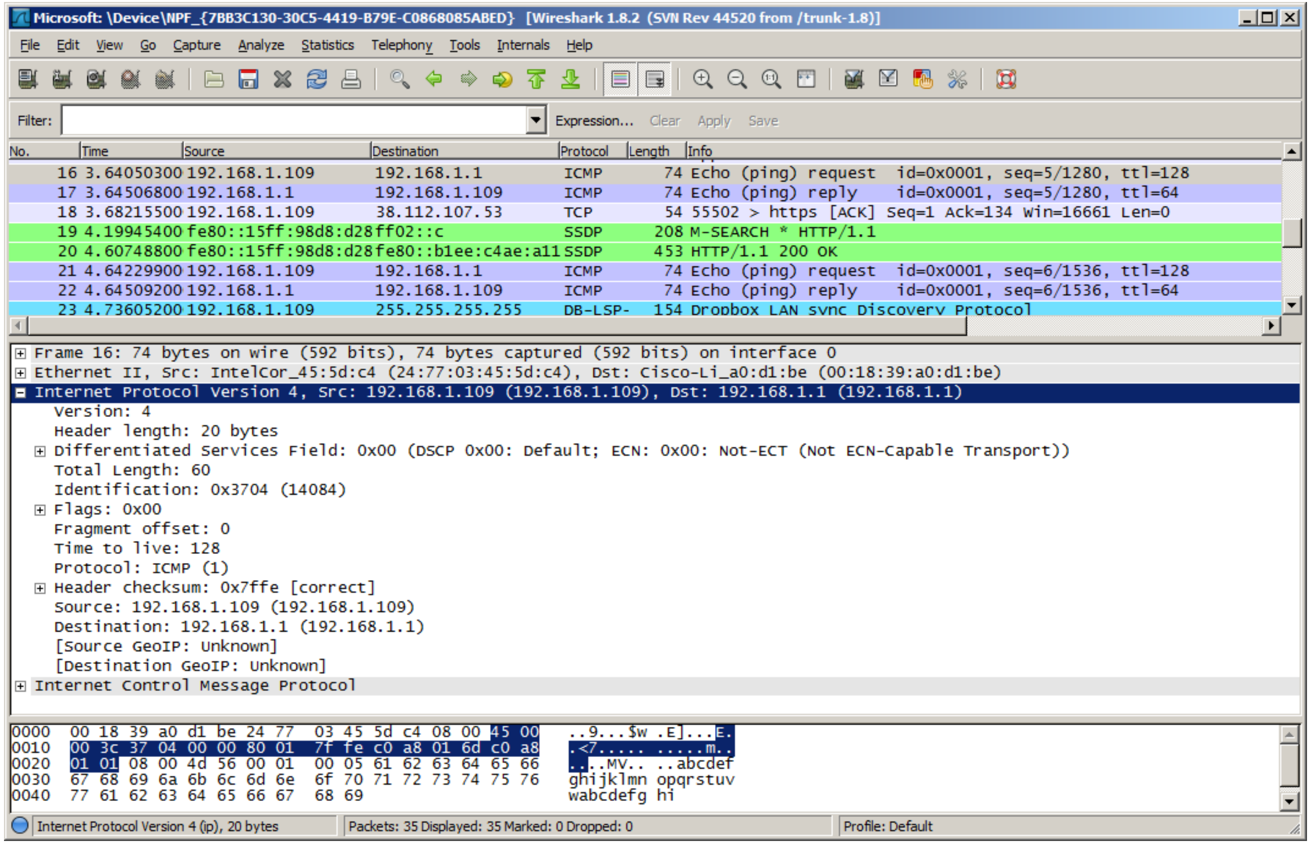
IPv4 Packet Header Fields

- Significant fields in the IPv4 header:

Function	Description
Version	This will be for v4, as opposed to v6, a 4 bit field= 0100
Differentiated Services	Used to determine priority and for QoS: DiffServ – DS field or the older IntServ – Type of Service (ToS)
Header Checksum	Detect corruption in the IPv4 header
Time to Live (TTL)	Prevents a packet from traversing a network endlessly. Layer 3 hop count. When it becomes zero the router will discard the packet.
Protocol	Identifies the next or upper level protocol: ICMP, TCP, UDP, etc.
Source IPv4 Address	32 bit source address
Destination IPV4 Address	32 bit destination address



Sample IPv4 Headers



8.3 IPv6 Packets

Limitations of IPv4

- IPv4 has three major limitations:
  - **IPv4 address depletion** – Although there are about 4 billion IPv4 addresses, we have basically run out of IPv4 addressing.
  - **Lack of end-to-end connectivity** – To make IPv4 survive this long, private addressing and NAT were created. This ended direct communications with public addressing.
  - **Increased network complexity** – NAT was meant as temporary solution and creates issues on the network as a side effect of manipulating the network headers addressing. NAT causes latency and troubleshooting issues.

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.
  - **Integrated security**

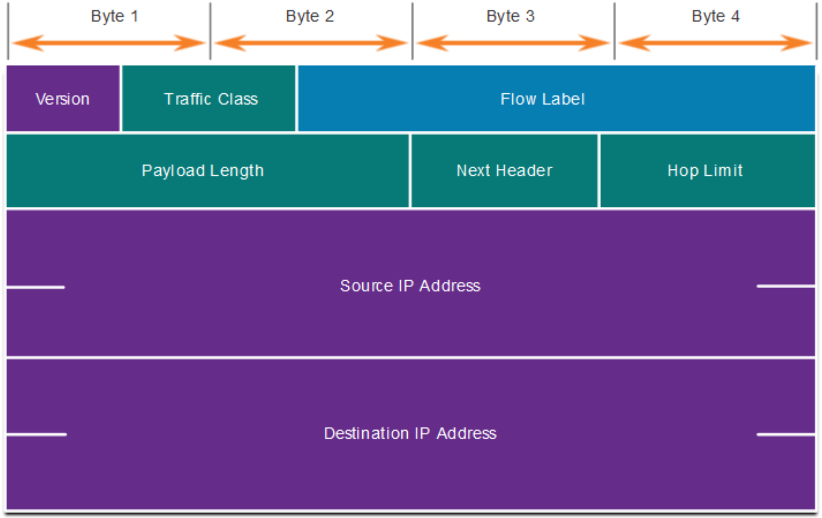
IPv4 and IPv6 Address Space Comparison

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
- (orange) There are 4 billion IPv4 addresses
- (green) There are 340 undecillion IPv6 addresses

IPv4 Packet Header Fields in the IPv6 Packet Header

- The IPv6 header is simplified, but not smaller.
- The header is fixed at 40 Bytes or octets long.
  - No checksum process requirement
- Several IPv4 fields were removed to improve performance.
  - More efficient packet handling
- Some IPv4 fields were removed to improve performance:
  - Flag
  - Fragment Offset
  - Header Checksum
- Autoconfiguration for addresses.
- Flow Label field makes it more efficient.



IPv6 Packet Header

- Significant fields in the IPv6 header:

Function	Description
Version	This will be for v6, as opposed to v4, a 4 bit field= 0110
Traffic Class	Used for QoS: Equivalent to DiffServ – DS field
Flow Label	Informs device to handle identical flow labels the same way, 20 bit field
Payload Length	This 16-bit field indicates the length of the data portion or payload of the IPv6 packet
Next Header	I.D.s next level protocol: ICMP, TCP, UDP, etc.
Hop Limit	Replaces TTL field Layer 3 hop count
Source IPv4 Address	128 bit source address
Destination IPV4 Address	128 bit destination address

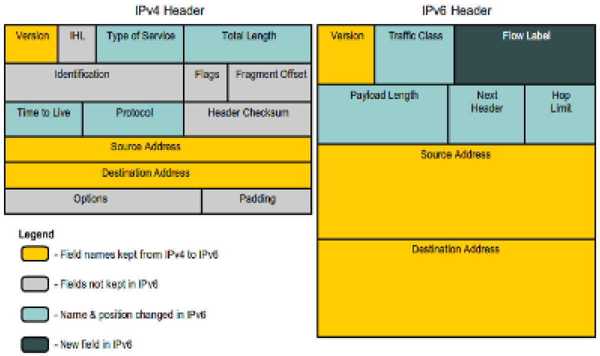
IPv6 Packet Header

- 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.

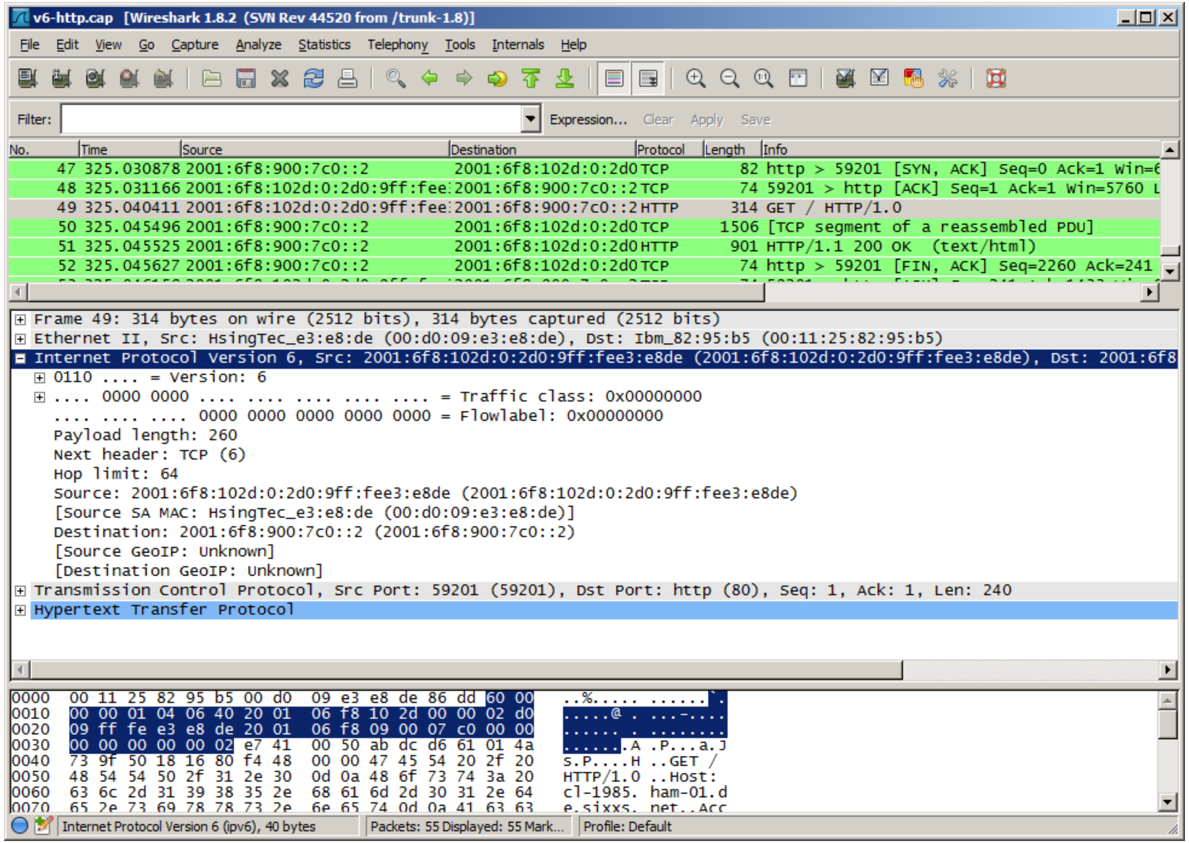
- Note: Unlike IPv4, routers do not fragment IPv6 packets.

IPv6 Packet Header Fields

- The IPv6 header is simpler than the IPv4 header is, which improves packet handling:
  - **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 informs network devices to maintain the same path for real-time application packets
  - **Payload Length** – 16-bit field indicates the length of the data portion or payload of the packet (same as total length)
  - **Next Header** – 8-bit field is equivalent to the IPv4 Protocol field and indicates the data payload type that the packet is carrying
  - **Hop Limit** – 8-bit field replaces the IPv4 TTL field - This value is decremented by 1 as it passes through each router and 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



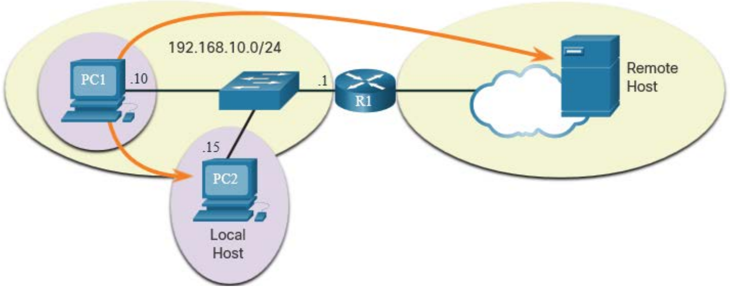
Sample IPv6 Header



8.4 How a Host Routes

Host Forwarding Decision

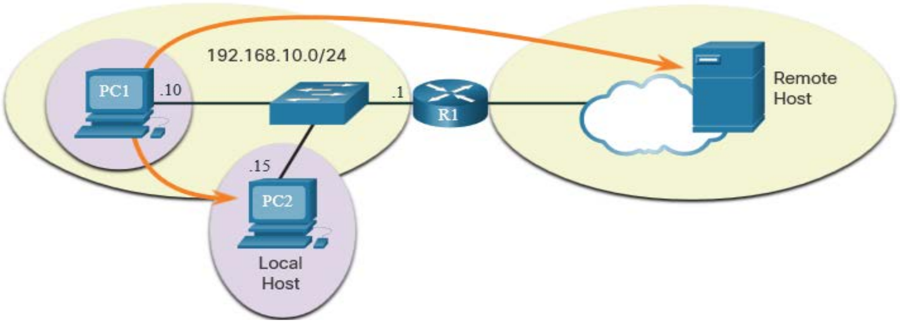
- An important role of the network layer is to:
  - Direct packets between local hosts (has a local IP address in the same address range as other hosts on the network).
  - Routes traffic to other networks (has a local IP address in a different address range).
  - Can take data in and forward data out.
  - Hosts will use the default gateway when sending packets to remote networks.
  - 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.
- Packets are always created at the source.
- Each host devices creates their own routing table.
- A host can send packets to the following:
  - Itself (Loopback) – 127.0.0.1 (IPv4), ::1 (IPv6)
  - Local Hosts – destination is on the same LAN
  - Remote Hosts – devices are not on the same LAN



- Note: The Loopback test demonstrates the TCP/IP stack on the device is working correctly.

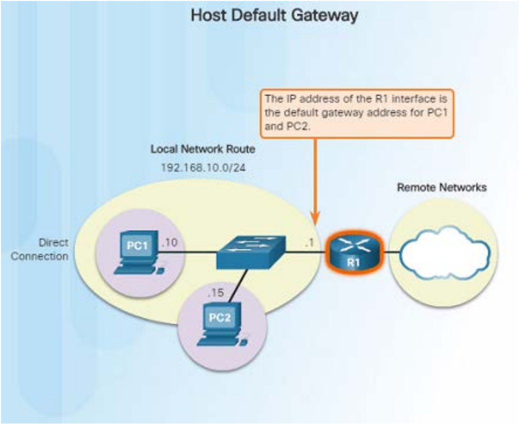
Host Forwarding Decision

- 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.



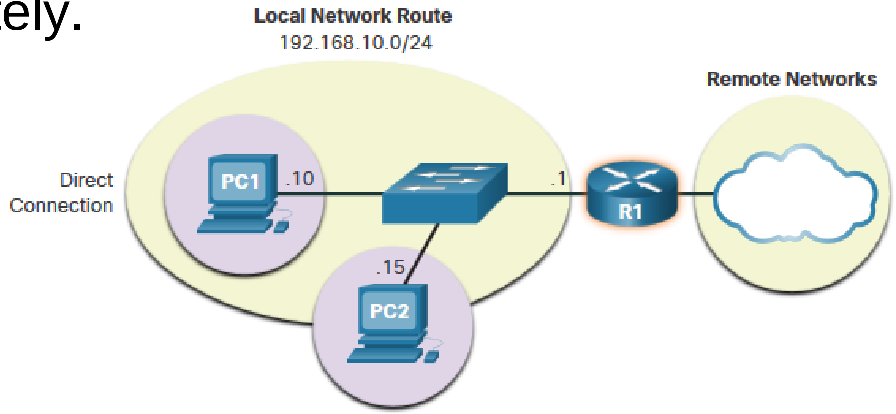
Default Gateway

- The default gateway is the network device that can route traffic out to other networks.
- A router or layer 3 switch can be a default-gateway.
- Features of a default gateway (DG or 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.



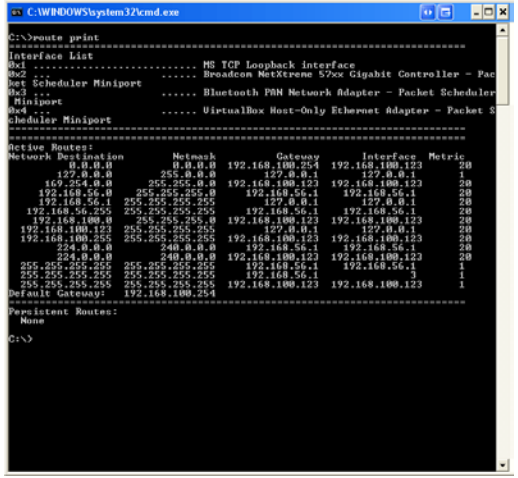
A Host Routes to the Default Gateway

- 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.



Host Routing Tables

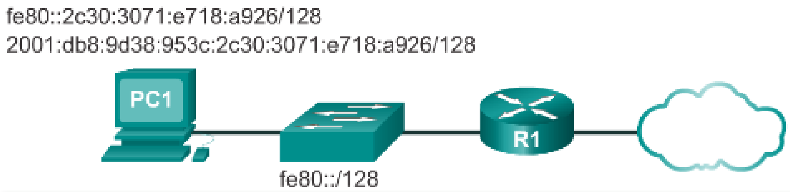
- Hosts must maintain their own local routing table to ensure that
  network layer packets are directed to the correct destination network
- The local table of the host typically contains:
  - Direct connection
  - Local network route
  - Local default route
- On Windows, **`route print`** or **`netstat -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
```

Sample IPv6 Host Routing Table

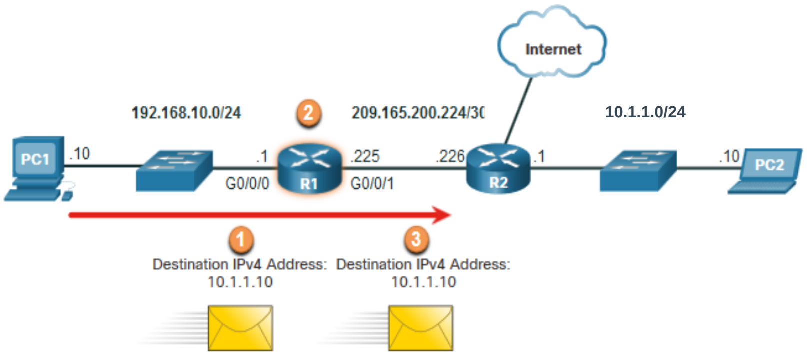



```
C:\Users\PC1> netstat -r

<Output omitted>

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 16     58 ::/0                     On-link
  1    306 ::1/128                  On-link
 16     58 2001::/32                On-link
 16    306 2001:0:9d38:953c:2c30:3071:e718:a926/128
                                    On-link
 15    281 fe80::/64                On-link
 16    306 fe80::/64                On-link
 16    306 fe80::2c30:3071:e718:a926/128
                                    On-link
 15    281 fe80::b1ee:c4ae:a117:271f/128
                                    On-link
  1    306 ff00::/8                 On-link
 16    306 ff00::/8                 On-link
 15    281 ff00::/8                 On-link
===========================================================================
<Output omitted>
```

8.5 Introduction to Routing

Router Packet Forwarding Decision

- What happens when the router receives the frame from the host device?
  1. Packet arrives on the G0/0/0 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 router 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.

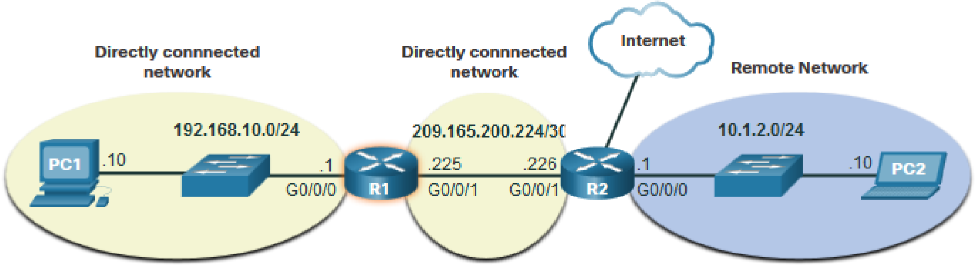


R1 Routing Table

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

IP Router Routing Table

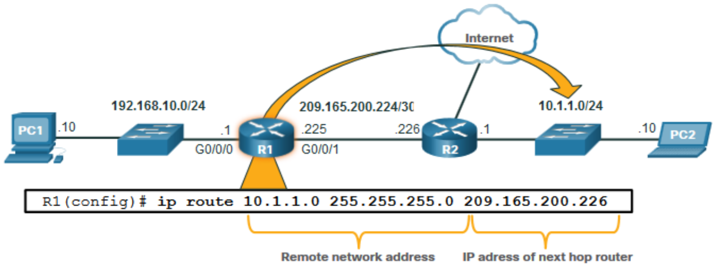
- There three types of routes in a router’s routing table:
  - **Directly Connected** – These routes are automatically added by the router, provided the interface is active and has addressing.
  - **Remote** – These are the routes the router does not have a direct connection and may be learned:
    - 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.



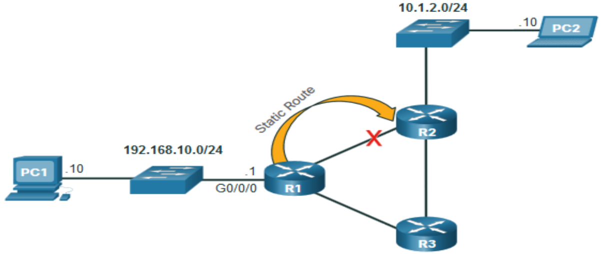
- If multiple routes are available, the lower metric value that is associated with the destination network is chosen as the best path.

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



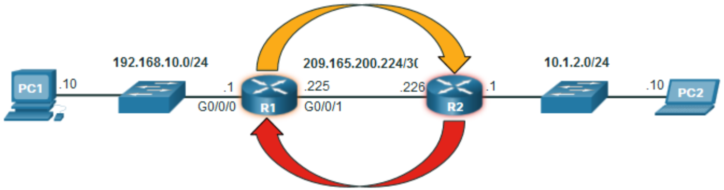
R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.



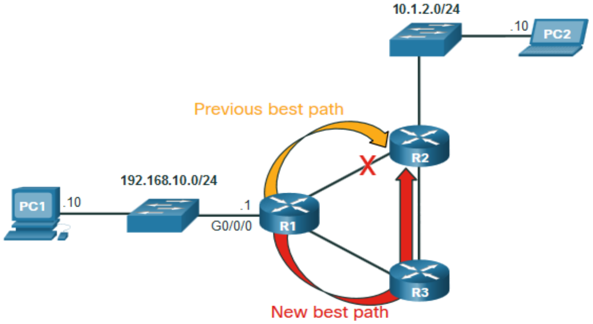
If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

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.

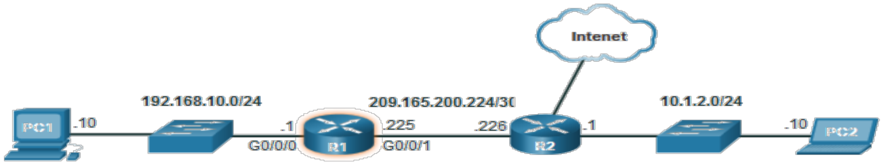
Introduction to an IPv4 Routing Table

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
- **R** – RIP

This command shows types of routes:

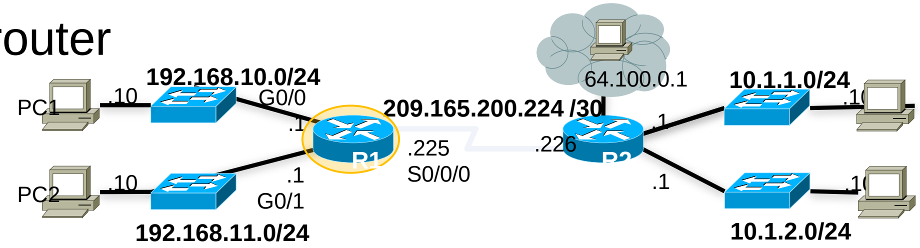
- Directly Connected – C and L
- Remote Routes – R, O, D, etc.
- Default Routes – S*




```
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        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

Directly Connected Routing Table Entries

- When a router interface is configured and activated, the following two routing table entries are created automatically:
  - **C** - Identifies a directly-connected network, automatically created when an interface is configured with an IP address and activated
  - **L** - Identifies that this is a local interface and this is the IPv4 address of the interface on the router



A	B	C
C	192.168.10.0/24 is directly connected,	GigabitEthernet0/0
L	192.168.10.1/32 is directly connected,	GigabitEthernet0/0

A	Identifies how the network was learned by the router.
B	Identifies the destination network and how it is connected.
C	Identifies the interface on the router connected to the destination network.

Remote Network Routing Table Entries

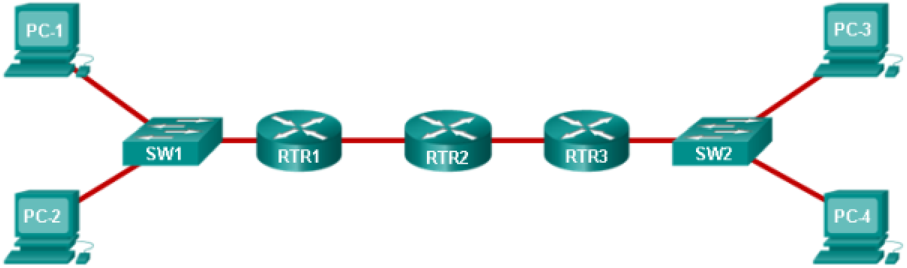
- Remote destinations can’t be reached directly
- Remote routes contain the address of the intermediate network device to be used to reach the destination
- Next-Hop address is the address of the intermediate device used to reach a specific remote destination

A	B	C	D		E	F	G
D	10.1.1.0/24	[90	/2170112]	via	209.165.200.226,	00:00:05,	Serial0/0/0

A	Identifies how the network was learned by the router.
B	Identifies the destination network.
C	Identifies the administrative distance (trustworthiness) of the route source.
D	Identifies the metric to reach the remote network.
E	Identifies the next hop IP address to reach the remote network.
F	Identifies the amount of elapsed time since the network was discovered.
G	Identifies the outgoing interface on the router to reach the destination network.

Hops

- A hop is an intermediary Layer 3 device (router) that a packet has to traverse to reach its destination
- 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
- If 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



- A packet from PC-1 to PC-4 has to traverse how many hops?

3

Routing

- Match the packets with their destination IP address to the exiting interfaces on the router.
  1. packets with destination of 172.17.6.15
  2. packets with destination of 172.17.14.8
  3. packets with destination of 172.17.12.10
  4. packets with destination of 172.17.10.5
  5. packets with destination of 172.17.8.20

1. FastEthernet0/0
2. FastEthernet0/1
3. FastEthernet1/0
4. FastEthernet1/1
5. The packet is dropped

```
<output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, Serial0/0/0
     172.17.0.0/24 is subnetted, 4 subnets
O       172.17.6.0 [110/2] via 192.168.3.4, 00:10:41, FastEthernet0/0
O       172.17.10.0 [110/2] via 192.168.5.2, 00:09:52, FastEthernet1/1
O       172.17.12.0 [110/2] via 192.168.4.2, 00:12:23, FastEthernet1/0
C       172.17.14.0 is directly connected, FastEthernet0/1
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet1/0
C    192.168.5.0/24 is directly connected, FastEthernet1/1
S*   0.0.0.0/0 is directly connected, Serial0/0/0
```

8.6 Module Practice and Quiz

What did I learn in this module?

- IP is connectionless, best effort, and media independent.
- IP does not guarantee packet delivery.
- IPv4 packet header consists of fields containing information about the packet.
- IPv6 overcomes IPv4 lack of end-to-end connectivity and increased network complexity.
- A device will determine if a destination is itself, another local host, and a remote host.
- A default gateway is router that is part of the LAN and will be used as a door to other networks.
- The routing table contains a list of all known network addresses (prefixes) and where to forward the packet.
- The router uses longest subnet mask or prefix match.
- The routing table has three types of route entries: directly connected networks, remote networks, and a default route.

New Terms and Commands

- netstat –r
- route print
- interface list
- IPv4 Route Table
- IPv6 Route Table
- directly-connected routes
- remote routes
- default route
- show ip route
- route source
- destination network
- outgoing interface
- administrative distance
- metric
- next-hop
- route timestamp

Elk Technologies

https://elktech.org

Scott Stephenson