Lecture#6: Network Layer

Internetworking

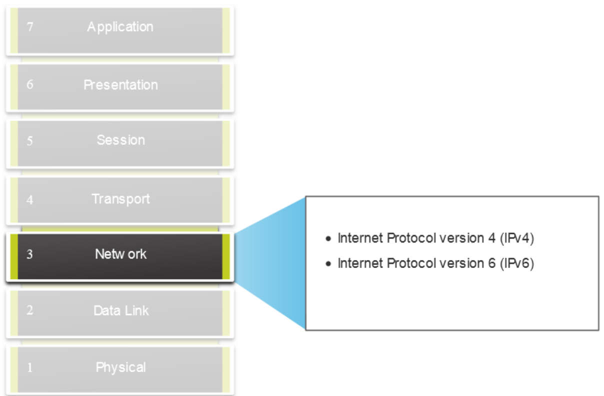
Introduction to Networks v7.0 (ITN) Module: 8

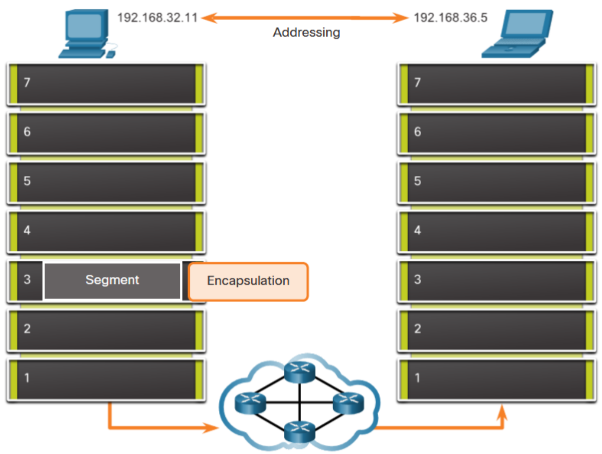
6.1 Layer 3 Characteristics

Network Layer Characteristics
The Network Layer

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: i) Addressing end devices, ii) Encapsulation, iii) Routing and iv) De-encapsulation.



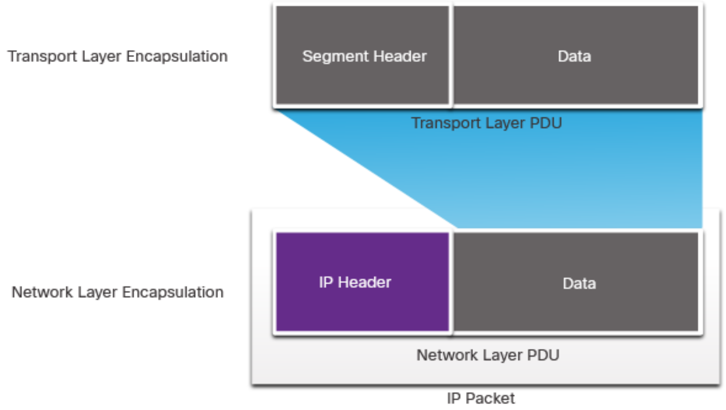


Network layer protocols forward transport layer PDUs between hosts.

Network Layer Characteristics

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.*

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
- If there is a need for connection-oriented traffic, then another protocol will handle this (typically TCP at the transport layer).

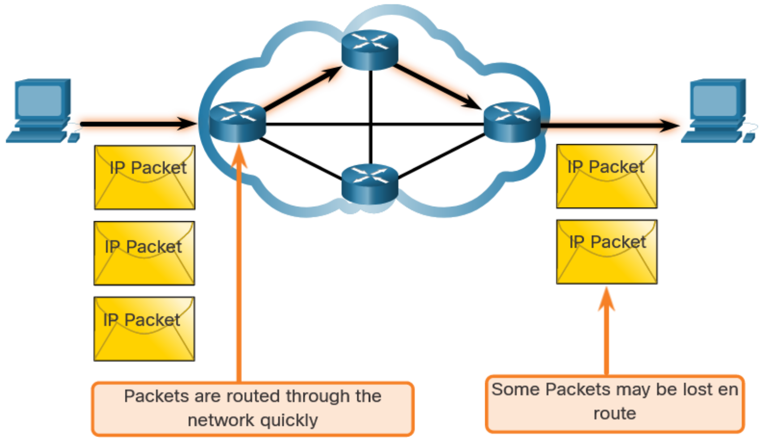
A letter is sent.

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.



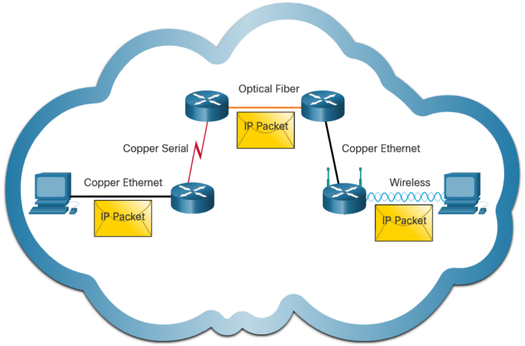
Network Layer Characteristics
Media Independent

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.

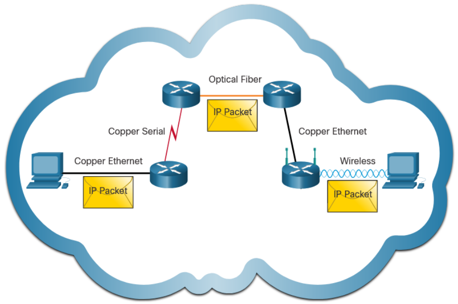
IP is **media Independen**t:

- 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 **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

6.2 IPv4 Packet

IPv4 Packet
IPv4 Packet Header

- IPv4 is the primary communication protocol for the network layer.

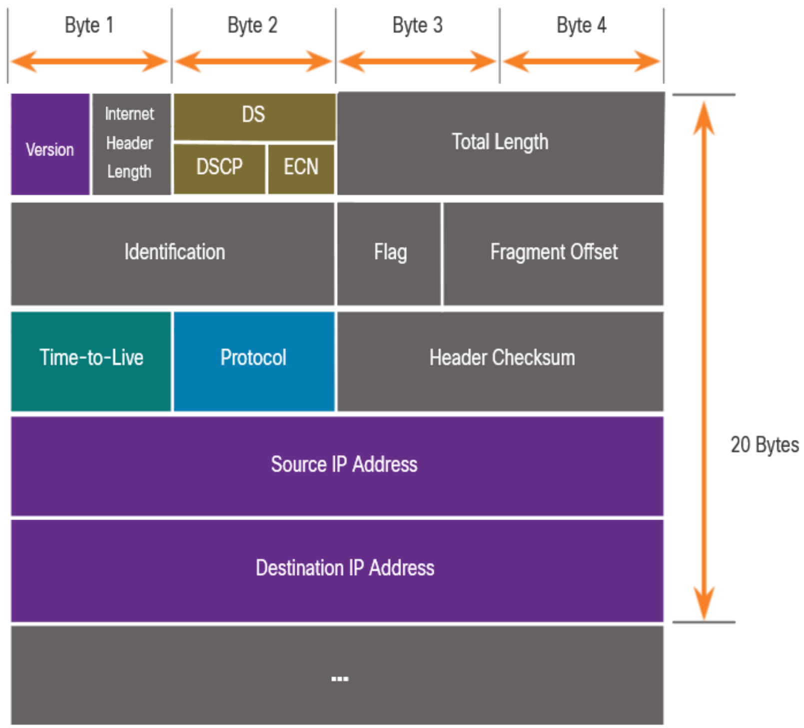
- The network header has many purposes:
  - It ensures the packet is sent in the correct direction (to the destination).
  - It contains information for network layer processing in various fields.
  - The information in the header is used by all layer 3 devices that handle the packet

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 for QoS: DiffServ – DS field or the older IntServ – ToS or Type of Service
Header Checksum	Detect corruption in the IPv4 header
Time to Live (TTL)	Layer 3 hop count. When it becomes zero the router will discard the packet.
Protocol	I.D.s next level protocol: ICMP, TCP, UDP, etc.
Source IPv4 Address	32 bit source address
Destination IPV4 Address	32 bit destination address

6.3 IPv6 Packets

IPv6 Packets

Limitations of IPv4

IPv4 has three major limitations:

- IPv4 address depletion – 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 Packets

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

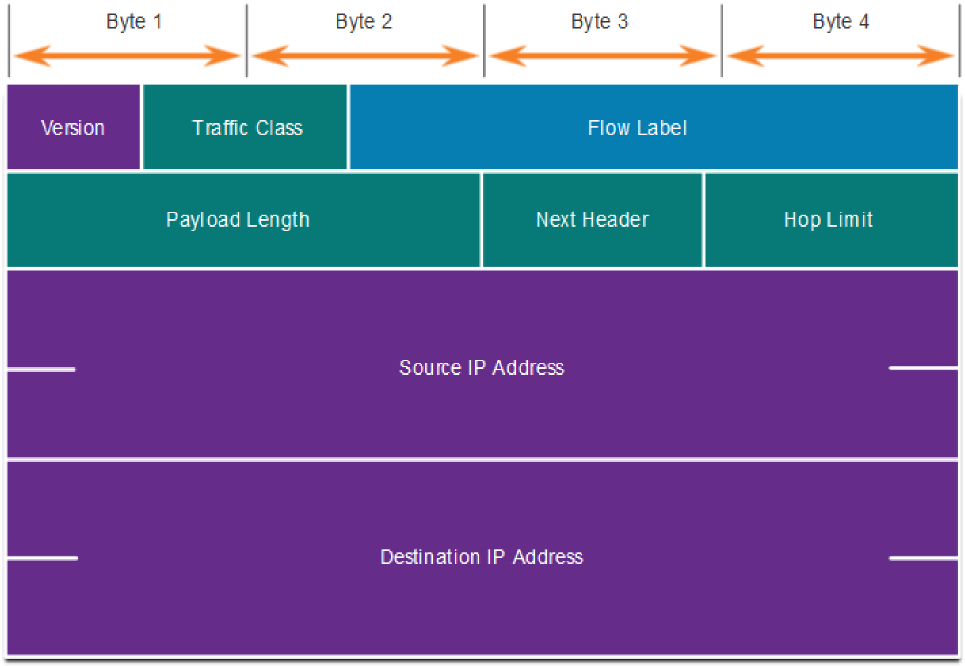
Legend

There are 4 billion IPv4 addresses

There are 340 undecillion IPv6 addresses

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.
- Some IPv4 fields like Flag, Fragment Offset, Header Checksum etc were removed to improve performance:



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 and Destination IPv6 Addresses	128 bit source and destination addresses

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.

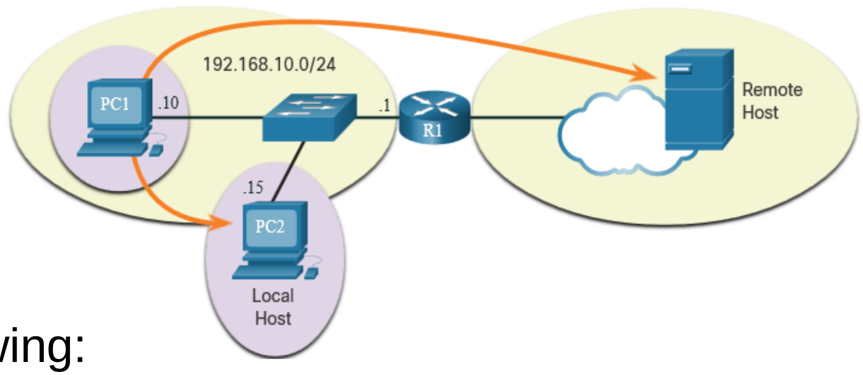
Note: *Unlike IPv4, routers do not fragment IPv6 packets.*

6.4 How a Host Routes

How a Host Routes

Host Forwarding Decision

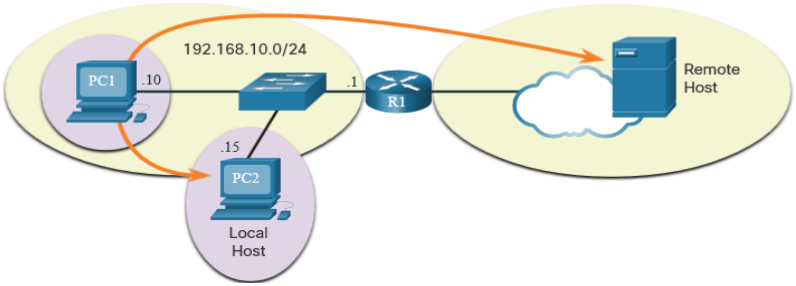
- Packets are always created at the source.
- Each host devices creates their own routing table.



- 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.

How a Host Routes

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.

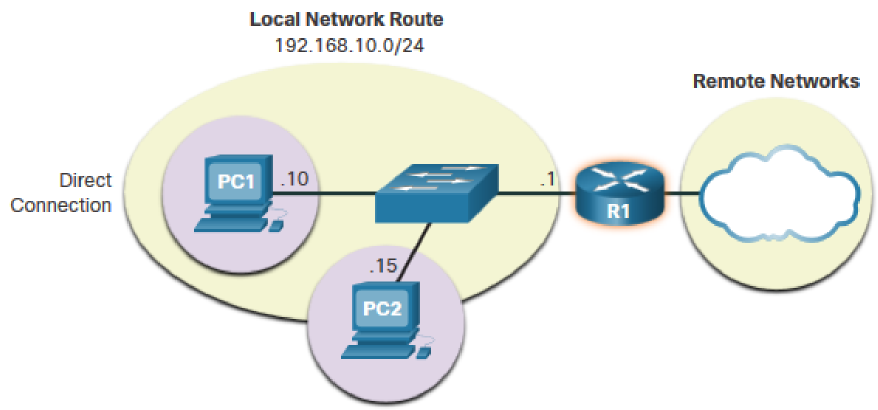
How a Host Routes

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

- 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
```

cisco