1 Network Layer Characteristics

The network layer provides services to allow end devices to exchange data THe principle network layer communication protocols are the IP version 4 and version 6 In this layer, there are four basic operations.

- Addressing End devices
- Encapsulation
- Routing
- De-Encapsulation

2 Ip Encapsulation

Ip encapsulates the transport layer segment and can either use an IPv4 or IPv6 packet and will not have an impact on 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. The NAT introduces changes in the addressing but it is for another topic

3 Characteristics of IP

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

- Connectionless
- Best Effort
- Media Independent

4 Connectionless

Recalling back to the Characteristic of Ip as Connectionless...

- Ip does not establish a connection with the destination before sending the packet.
- There is no control information needed such as synchronizations and acknowledgements
- 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

5 Best Effort

Recalling back to the Characteristic of IP as Best Effort...

- IP will not guranteed delivery
- IP has reduced overhead since there is no mechanism to resend unreceived data
- It does not expect acknowledgements
- there is no way to know if the other device is online or has received the packet

6 Media Independent

Recalling back to the Characteristic of IP as Media Independent...

Ip is unreliable since:

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

IP is media independent since:

- it does not concern itself with the type of fram required at the data link layer or the media type at the physical layer
- IP can be sent over any media type

The nework layer will establish teh Maximum Transmission Unit. It will receive it from the 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, while IPv6 does not. This introdces more latency. An example of this is when router goes from Ethernet to a slow WAN with a smaller MTU; MTU mismatch

7 IPv4 Packet Header

IPv4 is the primary communication protocol for the network layer. The network has many purposes

- ensures the packet is sent in the correct direction
- 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

8 IPv4 Packet Header Fields

The IPv4 network header is in binary, contains several fields of information the diagram is read from left to right, 4 bytes per each line. The two most important fields are the source and destination
Significant fields in the IPv4 header

Function	Description	Size
Version	This will be for V4 as opposed to V6, a 4 bit field = 0100	$\frac{1}{2}$ Byte
Differentiated Services	Used for QoS: DiffServ - DS field or the older interServe Type of Service	2 Bytes
header Checksum	Detect corruption n the IPv4 Header	2 Bytes
Time to Live	Layer 3 hop count. When it becomes 0 the router will discard the packet	1 Byte
Protocol	I.D.'s next level protocol: ICMP, TCP, UDP, etc.	1 Byte
Source IPv4 Address	32bit source address	4 Bytes
destination IPv4 Address	32bit destination address	4 Bytes

9 IPv6 Packets - Limitations of IPv4

IPv4 has three major limitations...

- IPv4 has address depletion, this means that we are running ot of IPv4 addresses. There are 4 billion possible addresses, while there are already 8 billion people in the world that may have 1 or more device that will need
- it lacks end to end connectivity, this is the reason why private addressing and NAT was created.
- Increases network complexity, NAT was made as a short term fix. NAT creates issues on the network as a side effect, causing latency and troubleshooting issues

10 IPv6 Overview

IPv6 was developed by Internet Engineering Task force in order to overcome the limitations of IPv4. IPv6 has increased address space from 32bit to 128bits. It also has improved packet handling with a simplified header and fewer fields. It also eliminates the need for NAT since there is a hge amount of addressing, there is no need to use private addressing internally

11 IPv4 vs IPv6 packet headers

- IPv6 header is simplified but not smaller
- The header is fixed at 40 bytes or octets long
- Several IPv4 fields were removed such as the flag, frament Offeset and Header Checksum

Significant fields in the IPv6 Header

Function	Description	Size
Version	This will be for v6 as opposed to v4, a 4 bit field = 0110	$\frac{1}{2}$ Byte
Traffic Class	Used for QoS: Equivalent to Diff-serv	1 Byte
Flow Label	Informs device to handle identical flow labels the same way, 20 bit field	$2\frac{1}{2}$ Byte
payload length	This 16-bit field indicates the length of the data portion of the IPv6 Packet	2 Byte
Next Header	I.D.'s the next level protocol: ICMP, TCP, UDP, etc.	1 Byte
Hop Limit	Replaces TTL field layer 3 hop count	1 Byte
Source IPv4 Address	128 bit source address	16 Byte
Destination IPv4 Address	128 bit destination address	16 Bytes

IPv6 packet may also contain extension headers. These provide optional network layer information it is placed betweein the IPv6 header and the payload. This may be used for fragementation, security, mobility support and etc. Routers will not fragment IPv6 packets

12 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

The source device determines whether the destination is local or Remote. It determines it using its own IP address and subnet mask and the destination IP address. For IPv6 the source uses the network address and prefix advertised by the local router.
Local traffic is then dumped out the host interface to be handled by an intermediary device. Remote traffic is forwarded directly to the default gateway on the lan.

13 Default Gateway

A router or layer 3 switch can be a defalt-gateway. A default gateway 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 the LAN. and most importantly, it can route to other networks.
If a device has no defalt gateway or a bad gateway, its traffic will not be able to leave the LAN

14 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 or can be configured manually. A DGW is a static route in the routing table. All devices on the LAN will need the DGW of the router if they intend to send traffic.

15 Host Routing Tables

On windows, rote print or netstat -r to display the routing table of the PC
Three sections displayed by these two commands
Interface List - all potential interface and MAC Addressing
IPv4 Routing table
IPv6 Routing table

16 Router Packet Forwarding Decision

When a router receives the frame from a host device...

- Packet arriveson the Gigabit Ethernet 0/0/0 interface of roter R1, which then the layer 2 ethernet header and trailer is de-encapsulated
- 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 R2
- R1 encapsulates the packet into an new ethernet header and trailer, forwards to the next hop router- R2

17 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 or Dynamically by using a routing protocol to have the routers share information with each other
Default Route - This forwards all traffic to a specific direction when there is not a match in the routing table

18 Static Routing

Static routes must be configured manually. It must also be adjusted manually by the administrator when there is a change in the topology. This is meant for small non-redundant networks. Often used in conjunction with a dynamic routing protocol for configuring a default rote

19 Dynamic Routing

Dynamic Routes Automaticall Discover remote networks. They also maintain up-to-date information. It chooses the best path to the destination. It also find new best paths when there is a change in the topology

20 Introdction 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 configred by an administrator
- **O** - OSPF
- **D** - EIGRP

This command shows types of routes:

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

21 Ethernet Frame Deciphering

Identify the Ethernet Header (14 bytes):

- The first 6 bytes represent the Destination MAC Address.
- The next 6 bytes represent the Source MAC Address.
- The last 2 bytes represent the EtherType, which indicates the type of the payload.

Identify the IP Header (20 bytes for IPv4):

- The first byte represents the Version and IHL (Internet Header Length).
- The next byte represents the DSCP (Differentiated Services Code Point) and ECN (Explicit Congestion Notification).
- The next 2 bytes represent the Total Length of the IP packet.
- The next 2 bytes represent the Identification.
- The next 2 bytes represent the Flags and Fragment Offset.
- The next byte represents the TTL (Time To Live).
- The next byte represents the Protocol.
- The next 2 bytes represent the Header Checksum.
- The next 4 bytes represent the Source IP Address.
- The last 4 bytes represent the Destination IP Address.

Identify the TCP Header (20 bytes minimum)

- The first 2 bytes represent the Source Port.
- The next 2 bytes represent the Destination Port.
- The next 4 bytes represent the Sequence Number.
- The next 4 bytes represent the Acknowledgment Number.
- The next 2 bytes represent the Data Offset, Reserved, and Flags.
- The next 2 bytes represent the Window Size.
- The next 2 bytes represent the Checksum.
- The next 2 bytes represent the Urgent Pointer.
- The remaining bytes represent the Options (if any).

pneumonics
6 6 2 1 1 2 2 2 1 1 2 4 4