IPV4 VERSUS IPV6

Routing: How communication between networks is facilitated
Function of the Network layer: To facilitate transport of data from one network to another
The Network Layer

- Layer 3 provides services to allow end devices to exchange data across the network

The Network layer uses four basic processes:

Addressing end devices	– End devices must be configured with a unique IP for identification **Host:** An end device with a configured IP address
Encapsulation	– Layer 3 receives a PDU from transport – Network layer adds IP header information (address of source/destination hosts) – After header information is added to the PDU, it's called a packet
Routing	– Provides services to direct packets to a destination host – To travel, packets must be processed by a router – Routers direct packets towards destinations (routing) – Packets can cross many devices before reaching a destination **Hop:** Each route the packet takes to reach its destination
Decapsulation aka Deencapsulation	– Packets arrive at layer 3 of a destination host: The host checks the IP header – If the destination IP w/in the header matches its own IP: The IP header is removed from packet – Known as deencapsulation – After a packet is deencapsulated by layer 3: Layer 4 PDU is passed up to service at transport

Network layer protocols specify the packet structure/processing used to carry data from one host to another
Two Commonly Used Network Layer Protocols:
1. Internet Protocol version 4 (IPv4)
2. Internet Protocol version 6 (IPv6)

Legacy network layer protocols (uncommon use):
1. **Novell Internetwork Packet Exchange (IPX):** Part of Novell Netware/Popular in the 80's/90's
2. **AppleTalk:** Apple's proprietary protocol
3. **Connectionless Network Service (CLNS/DECNet):** Telecommunications networks/doesn't require established circuits

Characteristics of IP
– Implemented by the TCP/IP suite
– Low overhead
– Not designed to track/manage the flow of packets

Basic characteristics of IP

Connectionless	– No connection with the destination is established before sending packets – Layer 3 isn't concerned with the type of communication inside – No dedicated end-to-end connection is created before data is sent **Example:** Think of a letter sent without the receivers knowledge
Best effort (unreliable)	– Packet delivery isn't guaranteed – IP doesn't have the capability to manage/recover from undelivered/corrupt packets – No acknowledgements/data tracking/error control/etc…
Media Independent	– Independent of the medium carrying the data – IP packets can be communicated electrically/wirelessly/over fiber etc.. – DLL's responsibility to take IP and prepare it for transmission **MTU: Maximum transmission unit** – The maximum size of the PDU each medium can transport

	– Part of the control communication between IP/Network layer – The establishment of a maximum size for a packet **Network layer determines how large packets should be**

Fragmentation: When a device (router) splits a packet: Forwarding from 1 medium to another with a smaller MTU
IPv4 Packet: Been in use since 1983: Deployed on ARPANET (Advanced Research Projects Agency Network)
An IPv4 packet has 2 parts:
1. **IP header:** Identifies packet characteristics
2. **Payload:** Contains layer 4 segment information/data

Significant fields in the IPv4 header include:

Version	– 4bit binary value identifying IP packet version – IPv4 always sets this field to 0100
Differentiated Services (DS)	– 8bit field used to determine priority of packets – AKA ToS or Type of Service field – First 6bits identify **Differentiated Services Code Point (DSCP)** – DSCP is a value used by QoS mechanisms – Last 2 bits identify **Explicit Congestion Notification (ECN)** – ECN can be used to prevent dropped packets during congestion
Time-to-Live (TTL)	– 8bit binary value used to limit packet lifetime – AKA a hop count – Value decreases by 1 each time the packet is processed by a router/hop – If TTL field hits 0: Router discards packet – Sends an ICMP time exceeded message to source IP **ICMP: Internet Control Message Protocol** **traceroute:** Command uses field to identify routers used between source/destination
Protocol	– 8bit binary value indicates data payload type the packet is carrying – Enables network layer to pass data to right upper layer protocols **Common values include: ICMP (0x01) TCP (0x06) and UDP (0x11)**
Source IP address	– 32bit binary value represents source IP address of packet
Destination IP address	– 32bit binary value represents destination IP address of packet

IPv4 Header Fields:

Internet Header Length (IHL)	– 4bit binary value identifying the number of 32bit words in header – IHL value varies b/c of Options/Padding fields **Minimum value:** 5 (532 = 160bits = 20bytes) **Maximum value:** 15 (1532 = 480 bits = 60 bytes)
Total Length	– 16bit field defines the entire packet (fragment) size; including header/data in bytes – AKA packet length **Minimum-length packet:** 20 bytes (20byte header + 0bytes data)**Maximum-length packet:** 65,535
Header Checksum	– 16bit field used for error checking of the IP header – Checksum of the header is recalculated/compared to the value in checksum field – If values don't match, the packet is dropped

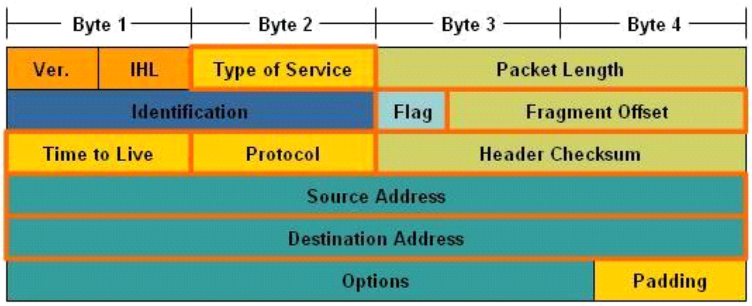
When fragmentation occurs, the following fields keep track:

Identification	-16bit field identifies the fragment of an original IP packet
Flags	– 3bit field identifies how packet is fragmented – Used with Fragment Offset and Identification fields to help reconstruct the fragment
Fragment Offset	– 13bit field identifies the order in which to place the packet fragment – In reconstruction of original unfragmented packet

Limitations of IPv4:
IP address depletion: Limited number of addresses: 4 billion addresses isn't enough
Internet routing table expansion: Routes consume tons of memory/processor resources on Internet routers

Lack of end-to-end connectivity: NAT provides a way for multiple devices to share a single IP
– Problematic for technologies that require end-to-end connectivity
NAT: Network Address Translation

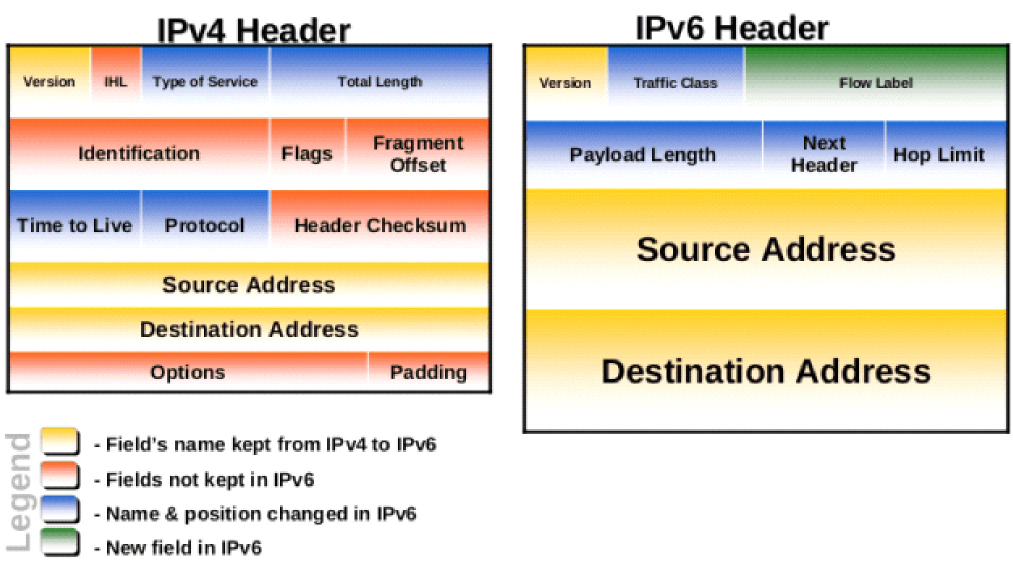
IPv4 Packet Header Fields



IPv6: Introduced in the 90's by the IETF (Internet Engineering Task Force) to help replace IPv4
– Helps overcome the limitations of IPv4 with enhancements
Improvements to IPv6 are:

Increased address space	– IPv6 addresses are based on 128bit hierarchical addressing – IPv4 only had 32bit – Increases the number of available IP addresses
Improved packet handling	– Header has been simplified with fewer fields – Improves handling by routers – Also provides support for extensions/options for increased scalability/longevity
Eliminates need for NAT	– NAT is no longer needed
Integrated security	– Supports authentication and privacy capabilities – IPv4 had to be implemented with additional features to do that

IPv4: 5billion addresses
IPv6: 340undecillion addresses



IPv4 header consists of:
– 20 octets (up to 60bytes if Options field is used)
– 12 basic header fields (not including Options/Padding)
IPv6 header consists of:
– 40 octets (length of source/destination addresses)
– 8 header fields (3 IPv4 basic fields + 5 additional header fields)
IPv6 simplified header advantages:

1. Better routing for performance/forwarding-rate scalability
2. No requirement for processing checksums
3. Simplified extension header mechanisms (opposed to IPv4 Options)
4. Flow Label field for per-flow processing with no need to open transport inner packet to identify traffic flows

IPv6 Packet Header:

Version	– 4bit binary value identifying IP packet version – With IPv6, this field is always set to 0110
Traffic Class	– 8bit field equivalent to IPv4 Differentiated Services (DS) field – Contains a 6bit DSCP value to classify packets – 2bit ECN used for traffic congestion control
Flow Label	– 20bit field provides special service for real-time applications – Can be used to inform routers/switches to maintain the same path for packet flow – Prevents packets from being reordered
Payload Length	– 16bit field equivalent to the Total Length field in IPv4 – Defines the entire packet (fragment) size, including header/optional extensions
Next Header	– 8bit field equivalent to the Protocol field – Indicates data payload type packet is carrying – This enables the network layer to pass the data to appropriate upper layer protocols – Also used as an optional extension header
Hop Limit	– 8bit field replaces TTL field – Value is decremented by 1 each router that forwards the packet – When counter reaches o: The packet is discarded – ICMPv6 message is forwarded to the sending host
Source Address	– 128bit field represents IPv6 address of receiving host
Destination Address	– 189 bit field represents IPv6 address of receiving host