OSI Model – Layers 1-3

INFO-6078 – Managing Enterprise Networks

FANSHAWE

The OSI Model

- The Open Systems Interconnection (OSI) model was published in 1984 by the International Organization for Standardization (ISO)
- The OSI Model is a reference model that helps us to understand how data is transmitted from one device to another over a network
- It is based on open standards so that all network hardware will be compatible
- The standards provide an open structure for hardware and software developers to follow, ensuring compatibility with current and future technologies

The OSI Model

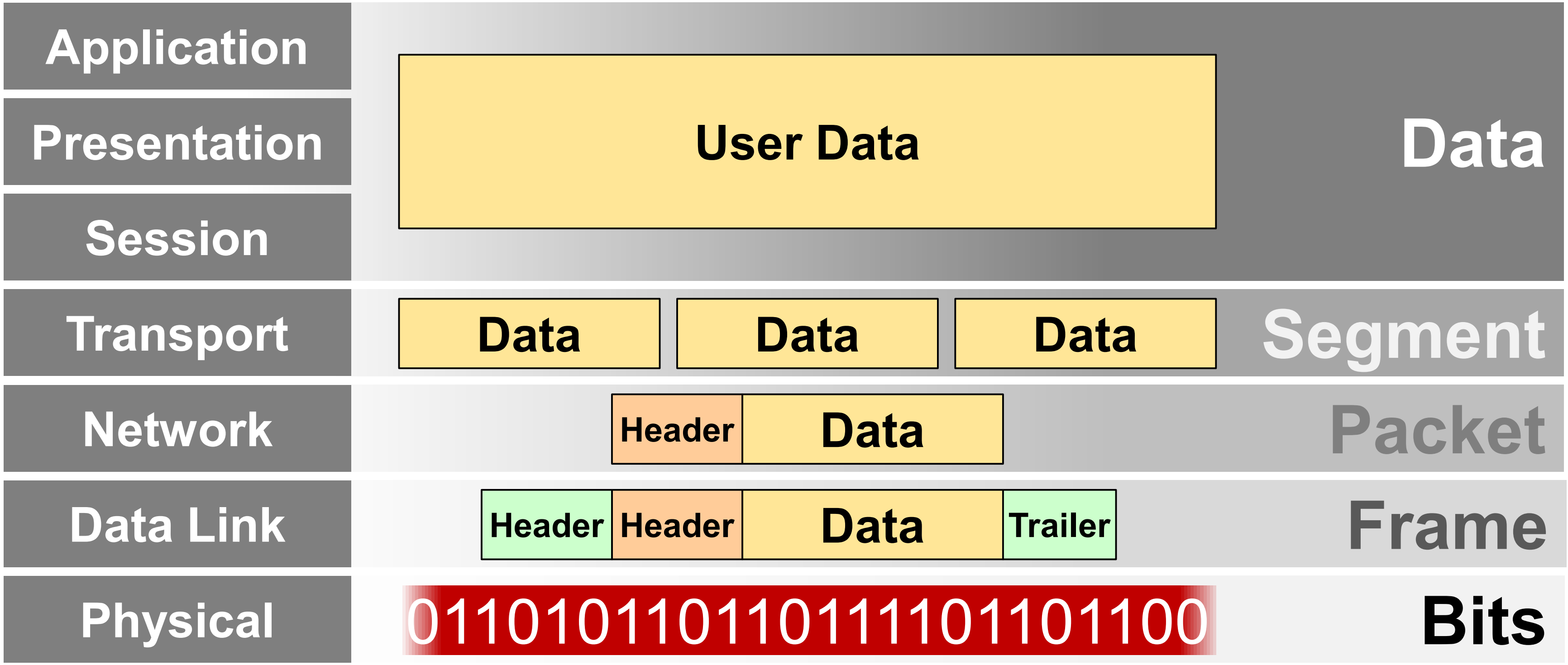
- The OSI model uses a technique called abstraction, separating the tasks performed in a particular layer from tasks performed in other layers
- Layers within the OSI model interact only with the layer above and below

The OSI Model

7	Application	High-level APIs that provide access to network resources
6	Presentation	Data translation services including encoding, compression and encryption
5	Session	Management of communication sessions
4	Transport	Provides segmentation and process-to-process message delivery
3	Network	Provides routing and node-to-node delivery
2	Data Link	Error-free transmission of frames between nodes
1	Physical	Transmission of bits over a medium; includes mechanical and electrical specifications

The OSI Model - PDU

- A protocol data unit (PDU) represents the name given to the unit of information in reference to it’s position in relation to an OSI model layer



Application

Presentation

Session

User Data

Data

Transport

Data Data Data

Segment

Network

Header Data

Packet

Data Link

Header Header Data Trailer

Frame

Physical

011010110110111101101100

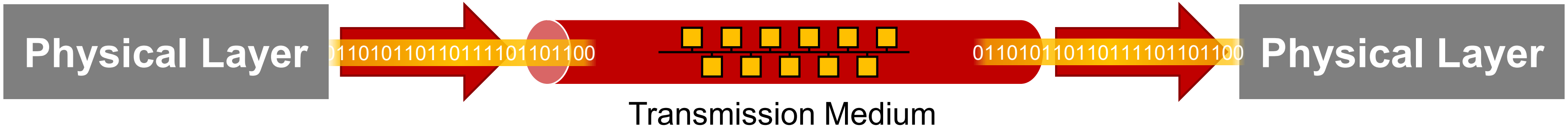
Bits

1 – The Physical Layer

7	Application	High-level APIs that provide access to network resources
6	Presentation	Data translation services including encoding, compression and encryption
5	Session	Management of communication sessions
4	Transport	Provides segmentation and process-to-process message delivery
3	Network	Provides routing and node-to-node delivery
2	Data Link	Error-free transmission of frames between nodes
1	**Physical**	**Transmission of bits over a medium; includes mechanical and electrical specifications**

1 – The Physical Layer

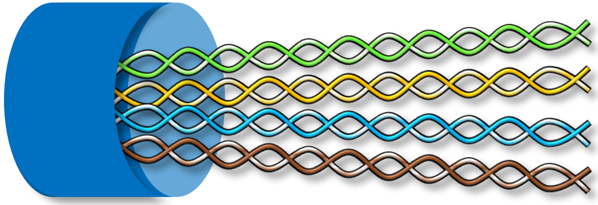
- The physical layer of the OSI model is responsible for the transmission of raw data across a physical medium
- It converts binary bits into the format specified by the transmission medium (electrical, light, radio frequency)
- The physical layer defines specifications for interfaces and cables, which includes pins, voltage, timing, cable length, frequency and signal strength (wireless),

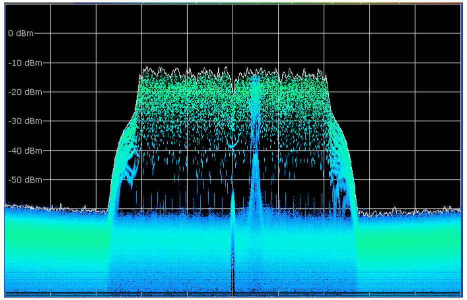


Physical Layer Media

Copper

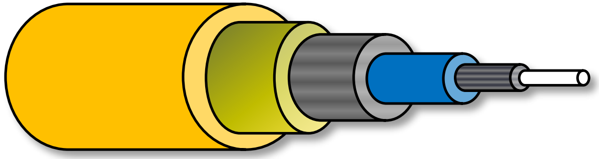
(Electrical signal)

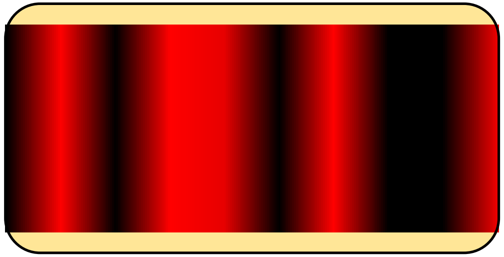




Fiber Optic

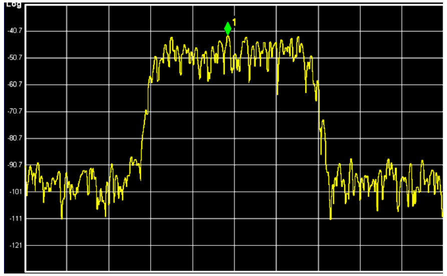
(Light pulses)





Wireless

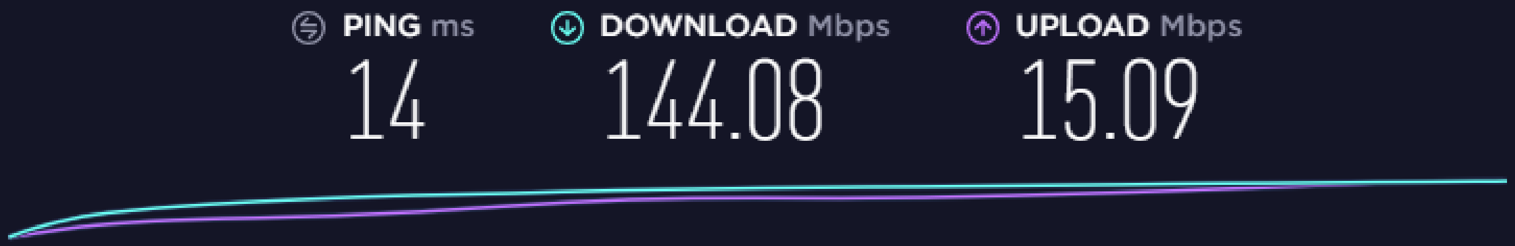
(RF Modulation)



Data Transmission Rates

- **Bandwidth** – The maximum amount of raw information (data) that can be transmitted between two nodes across a medium
- **Throughput** – The amount of successful communications over the medium including overhead and delays related to protocols and processing
- **Goodput** – The rate at which throughput is measured without consideration for protocol headers
- Usually measured in units of bits per second

Speed vs Bandwidth



PING ms
14

DOWNLOAD Mbps
144.08

UPLOAD Mbps
15.09

Unit	Bit rate
Bit per second (bps)	1 bps
Kilobit per second (kbps)	1 kbps = 1,000 bps
Megabit per second (Mbps)	1 Mbps = 1,000,000 bps
Gigabit per second (Gbps)	1 Gbps = 1,000,000,000 bps
Terabit per second (Tbps)	1 Tbps = 1,000,000,000,000 bps

131.68
Mbps

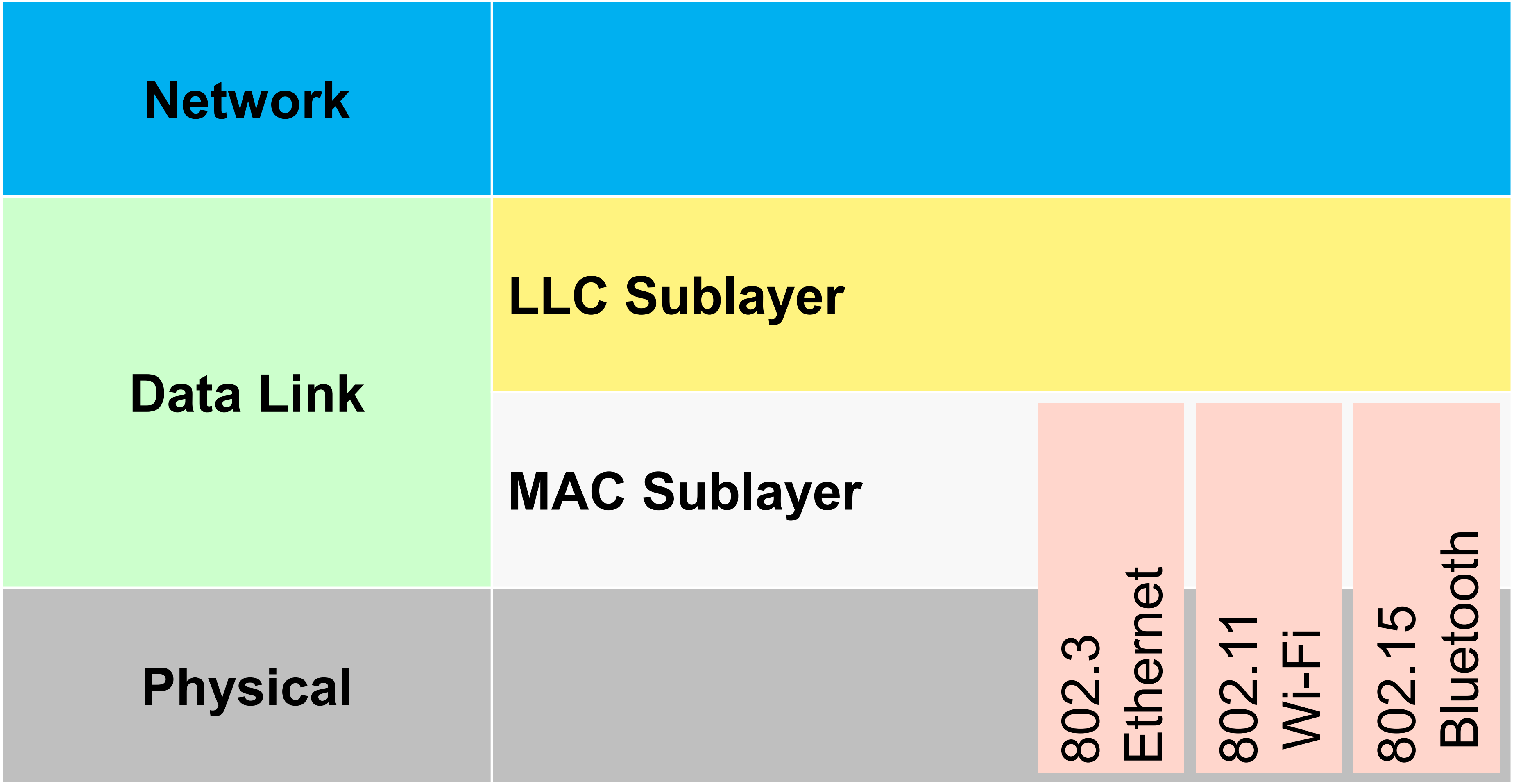
2 – The Data Link Layer

7	Application	High-level APIs that provide access to network resources
6	Presentation	Data translation services including encoding, compression and encryption
5	Session	Management of communication sessions
4	Transport	Provides segmentation and process-to-process message delivery
3	Network	Provides routing and node-to-node delivery
2	**Data Link**	**Error-free transmission of frames between nodes**
1	Physical	Transmission of bits over a medium; includes mechanical and electrical specifications

2 – The Data Link Layer

- The data link layer of the OSI model is responsible for the delivery of data between nodes in a local or wide area network
- Control information is added to data in the form of headers and trailers to assist with data delivery
- The data link layer may also perform error checking and recovery services

Data Link Sublayers



Data Link Sublayers

- **Media Access Control (MAC) Sublayer**
  - Provides addressing, multiplexing and flow control for the transmission medium
  - Encapsulates packets into frames appropriate for the transmission medium
  - Responsible for the addition and calculation of the Frame Check Sequence (FCS), normally in the format of a 32 bit Cyclic Redundancy Check (CRC32)
  - Manages multiaccess protocols such as Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Data Link Sublayers

- **Logical Link Control (LLC) Sublayer**
  - Provides Multiplexing and flow control for the logical link
  - Controls synchronization between devices
  - On non-Ethernet networks, can provide flow control and Automatic Repeat Requests (ARQ)
  - Optional for 802.3 operation

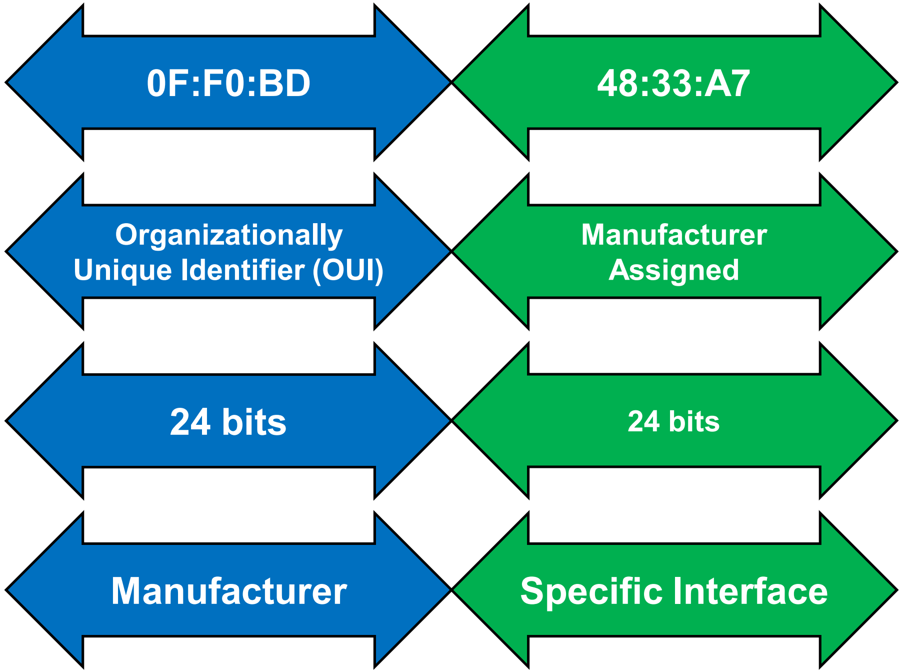
MAC Address

- A MAC address is a unique identifier as managed by the IEEE EUI-48 standard, and assigned to a network interface for communication at layer 2 of the OSI model
- Addresses are expressed as 12 hexadecimal digits (48 bits) separated by hyphens, colons or dots
- MACs are often referred to as a physical, or burned-in address, and are normally stored in an interfaces read only memory (ROM)
- Universally Administered Addresses provide a unique address assigned by the manufacturer

MAC Address

- The first three bytes of the address identify the manufacturer and is know as the Organizationally Unique Identifier (OUI)
- The remaining three bytes are assigned by the manufacturer, subject to providing a unique address to each device

0F:F0:BD:48:33:A7



0F:F0:BD

Organizationally Unique Identifier (OUI)

24 bits

Manufacturer

48:33:A7

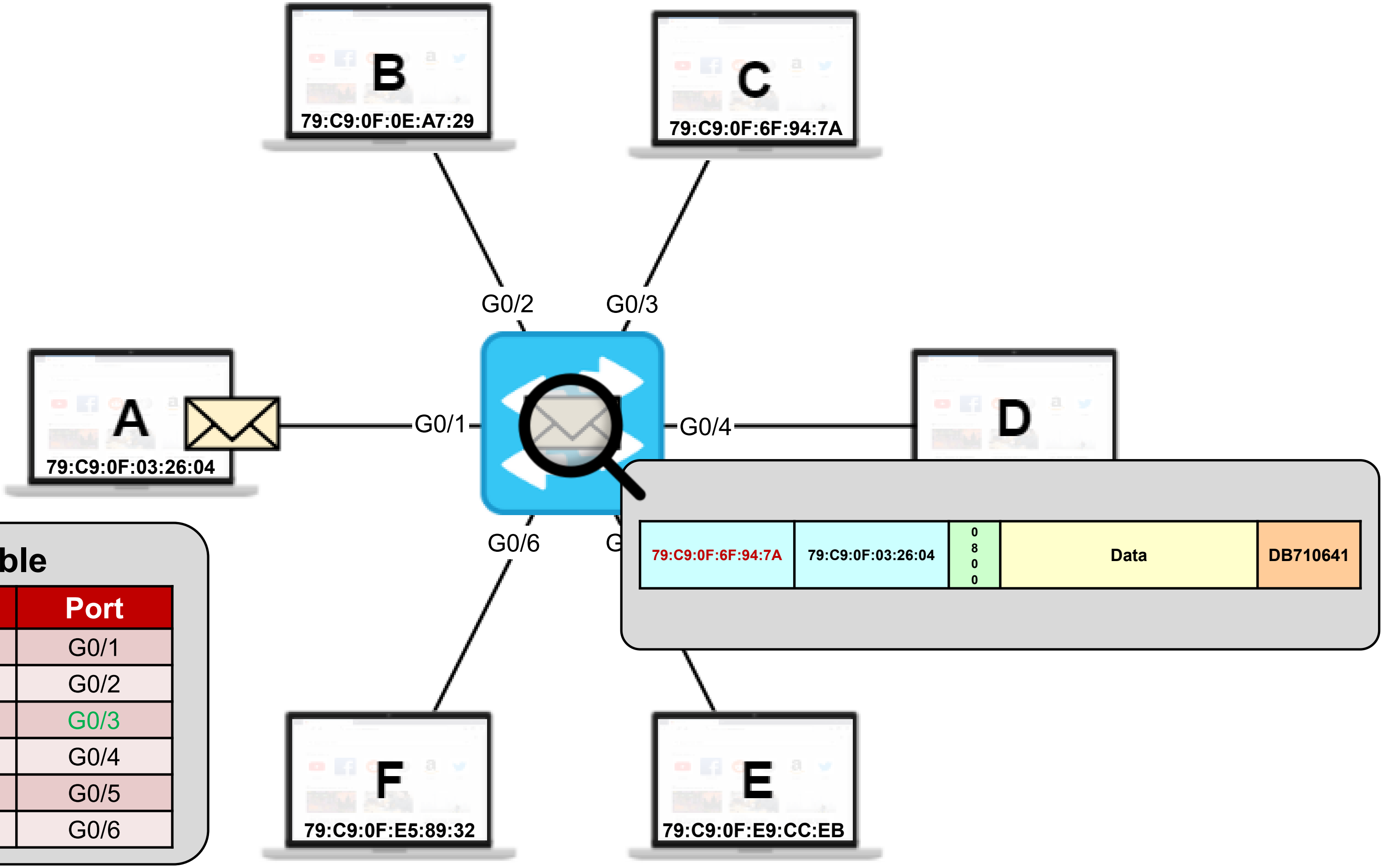
Manufacturer Assigned

24 bits

Specific Interface

OUI Lookup Tool

Message Delivery Options - Unicast

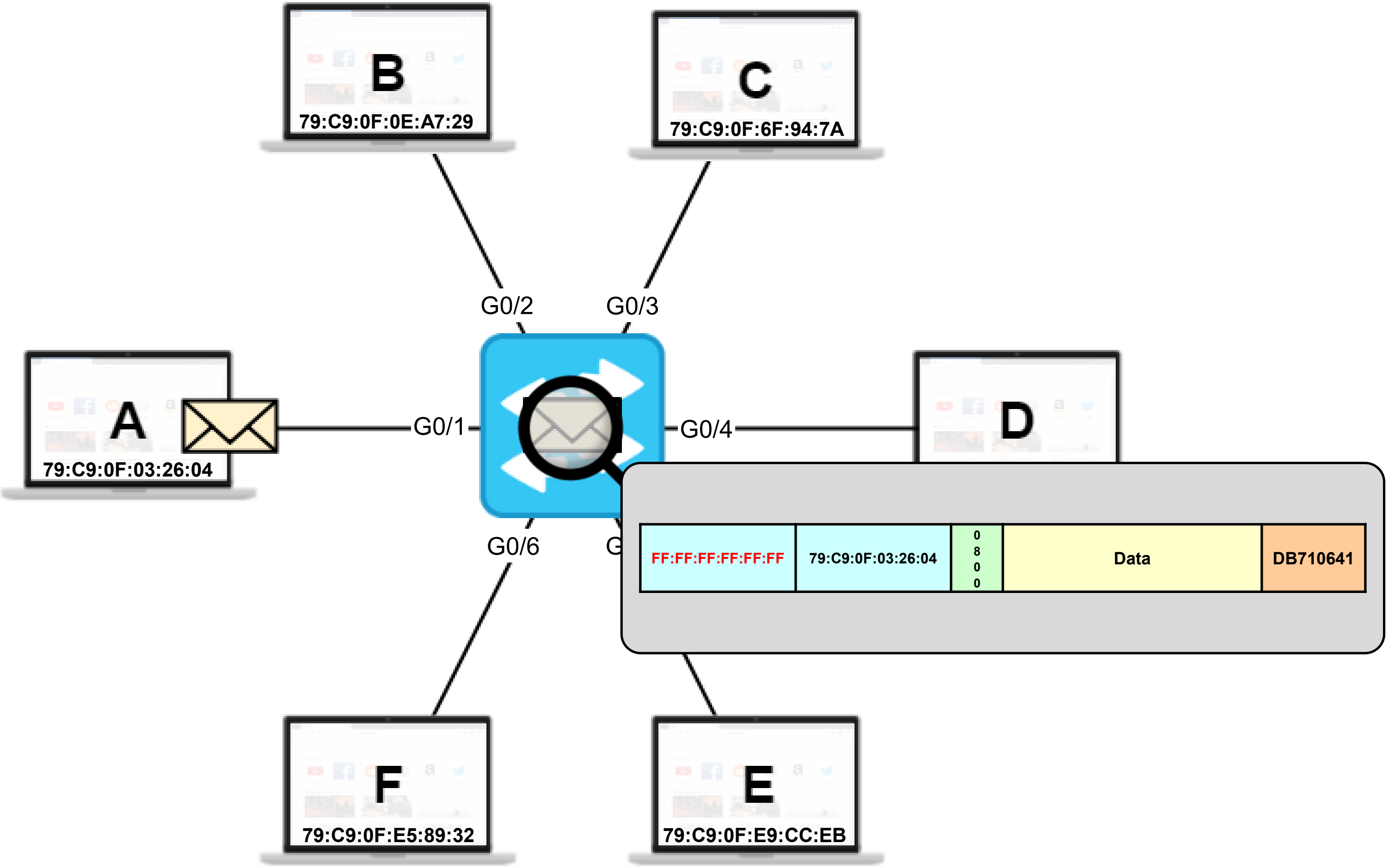


79:C9:0F:6F:94:7A	79:C9:0F:03:26:04	0 8 0 0	Data	DB710641

CAM Table

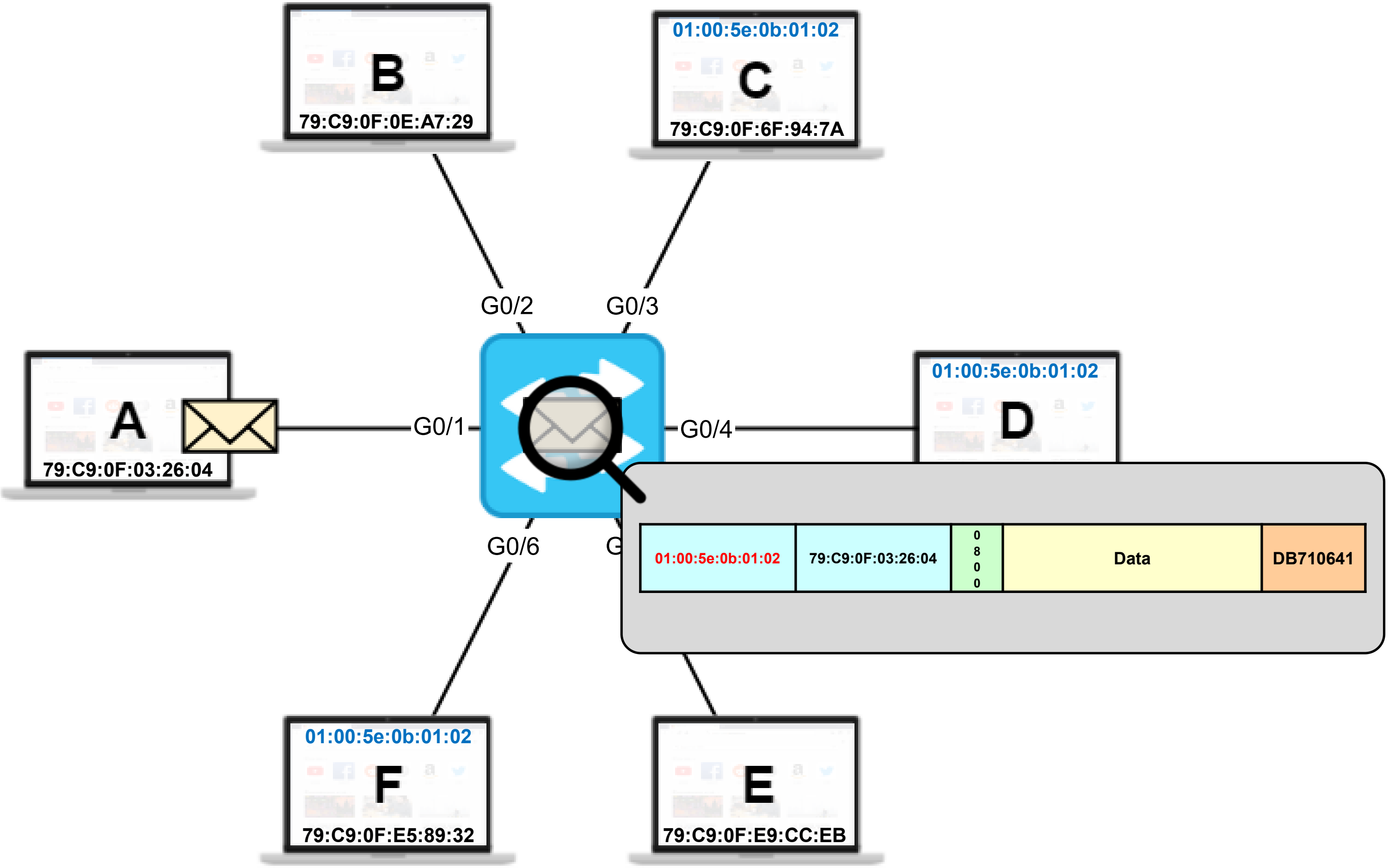
MAC	Port
79:C9:0F:03:26:04	G0/1
79:C9:0F:0E:A7:29	G0/2
79:C9:0F:6F:94:7A	G0/3
79:C9:0F:0F:C0:AF	G0/4
79:C9:0F:E9:CC:EB	G0/5
79:C9:0F:E5:89:32	G0/6

Message Delivery Options - Broadcast



FF:FF:FF:FF:FF:FF	79:C9:0F:03:26:04	0 8 0 0	Data	DB710641

Message Delivery Options - Multicast



01:00:5e:0b:01:02	79:C9:0F:03:26:04	0 8 0 0	Data	DB710641

Data-Link Layer Frame Headers

Ethernet II

6	6	2	46-1500	4
Destination MAC	Source MAC	Type	Data	FCS

802.2

6	6	2	46-1500	4
Destination MAC	Source MAC	Length	Data	FCS

Data-Link Layer Frame Headers – Ethernet II

6	6	2	46-1500	4
Destination MAC	Source MAC	Type	Data	FCS

Destination/Source MAC (48 bit):

- The MAC address of the receiving/sending device

Data-Link Layer Frame Headers – Ethernet II

6	6	2	46-1500	4
Destination MAC	Source MAC	Type	Data	FCS

EtherType (Type) (16 bit):

- Identifies the upper layer protocol that is encapsulated in the frame
- To conform with 802.3 standards, EtherType values must be equal to or greater than 1536 (0x600)

Value	Protocol
0x0800	Internet Protocol version 4 (IPv4)
0x86DD	Internet Protocol version 6 (IPv6)
0x0806	Address Resolution Protocol (ARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q)
0x0842	Wake-on-LAN

Data-Link Layer Frame Headers – 802.2

6	6	2	46-1500	4
Destination MAC	Source MAC	Length	Data	FCS

EtherType (Length) (16 bit):

- Specifies the length of the data payload for protocols that run directly on top of IEEE 802.2 LLC encapsulation
- When used as a length field, EtherType values must be less than or equal to 1500 (0x05DC)
- Protocols such as Spanning Tree use 802.2 frames

Data-Link Layer Frame Headers – Ethernet II

6	6	2	46-1500	4
Destination MAC	Source MAC	Type	Data	FCS

Data (varies):

- The encapsulated payload that is between 46-1500 bytes (42-1500 if 802.1Q tag present)

Data-Link Layer Frame Headers – Ethernet II

6	6	2	46-1500	4
Destination MAC	Source MAC	Type	Data	FCS

Frame Check Sequence (32 bit):

- A cyclic redundancy check (CRC) that is used to identify frames that arrive at the destination corrupted

Ethernet Frames

- A standard Ethernet frame is defined as having a minimum size of 64 bytes, and maximum size of 1522 bytes

Runt Frames

- A runt frame is a frame who's total size is less than the IEEE 802.3’s minimum length of 64 bytes
  - Common causes for runt frames include network collisions or hardware failure
  - Runt frames are also known as collision fragments

Ethernet Frames

Jumbo Frames

- A jumbo frame is an Ethernet frame that contains a payload greater than the standard of 1500 bytes
- By altering the MTU of the network, jumbo frames can carry a payload of up to around 9000 bytes, increasing the efficiency of the network; however, jumbo frames are not included in the IEEE 802.3 specifications and results may vary

Baby Giant Frames

- Baby giant or baby jumbo frames are slightly larger than the standard 1500 byte frame
- MPLS over Ethernet requires baby giant frames

3 – The Network Layer

7	Application	High-level APIs that provide access to network resources
6	Presentation	Data translation services including encoding, compression and encryption
5	Session	Management of communication sessions
4	Transport	Provides segmentation and process-to-process message delivery
3	**Network**	**Provides routing and node-to-node delivery**
2	Data Link	Error-free transmission of frames between nodes
1	Physical	Transmission of bits over a medium; includes mechanical and electrical specifications

3 – The Network Layer

- The network layer of the OSI model is responsible for end-to-end packet delivery including routing the traffic through any applicable internetworks
- The network layer services requests to/from the transport and data link layers
- The network layer is responsible for addressing end devices, encapsulating data into packets and routing the packets across the network

3 – The Network Layer – MTU

- The maximum transmission unit (MTU) is the size of the largest datagram that can be communicated across the network in a single transaction
- The MTU does not include data from lower layer protocols such as the Ethernet headers
- If a device between two communicating hosts has an MTU lower than the standard 1500 bytes, fragmentation is required to complete the communication

3 – The Network Layer – MTU

- MTUs of common protocols include:
  - Ethernet II – 1500 bytes
  - PPPoE v2 – 1492 bytes
  - IEEE 802.11 – 2304 bytes
  - GRE – 1476 bytes
  - MPLS – 1496 bytes

Internet Protocol

- In the past, many network layer protocols have been used, but Internet Protocol (IP) is the clear leader in terms of usage
- Internet Protocol version 4 (IPv4) is one of the core networking protocols of the internet, and is responsible for most of the routing that occurs
- Internet Protocol version 6 (IPv6) is the emerging protocol that is set to provide services on the internet for generations to come

Internet Protocol Addressing

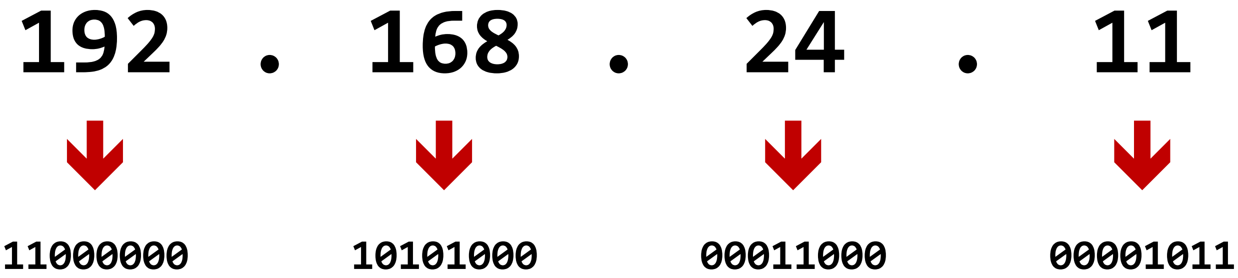
- IP addressing requires that each host is uniquely identifiable for most traffic operations
- Address spaces may also be divided into subnetworks, partitioning certain hosts onto a separate network
- Routing then provides connection between the different networks

Internet Protocol Characteristics

- IP conforms to the end-to-end principle developed by Paul Baran and Donald Davies, and as a result provides only best-effort delivery
- IP is also a connectionless protocol, and does not establish communications before transmitting data
- Additionally, routers make routing decisions about each packet individually, which could result in traffic destined for the same destination taking different paths, arriving out of order, suffering packet loss, or packet corruption
- Any error conditions on IP networks must be resolved by end devices

Internet Protocol Version 4 – Addressing

- IPv4 utilizes 32 bit addresses in the dot-decimal notation to identify compatible devices
- The addresses consist of four decimal numbers that range from 0-255 separated by periods
- An IPv4 address is often expressed along with its relevant subnet mask or network prefix



192 . 168 . 24 . 11

11000000 10101000 00011000 00001011

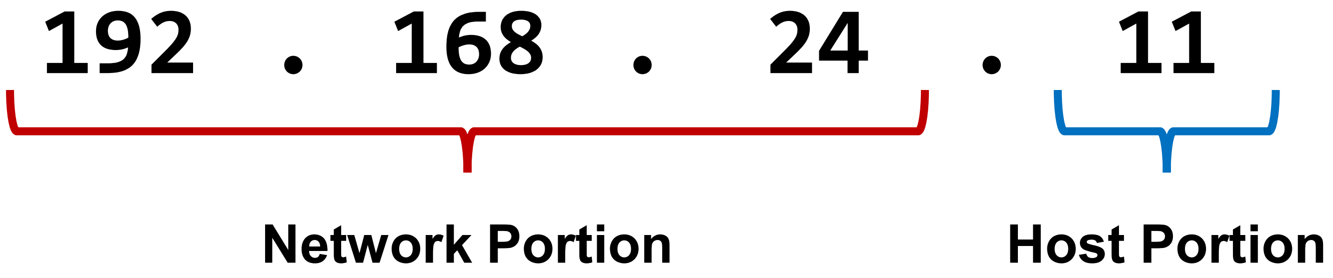
IP Version 4 – Classful Addressing

Class	Range	Network/Host Ranges	Subnets/Hosts
A	0-127	N.H.H.H	128 networks 16,777,216 hosts
B	128-191	N.N.H.H	16,384 networks 65,536 hosts
C	192-223	N.N.N.H	2,097,152 networks 256 hosts
D	224-239		
E	240-255		

- Until RFC 1517 was introduced in 1993, classful addressing was used without a network prefix of subnet mask
- Classless Inter-Domain Routing (CIDR) introduced subnets of various length by adding a subnet mask or prefix

Internet Protocol Version 4 – Subnet Mask

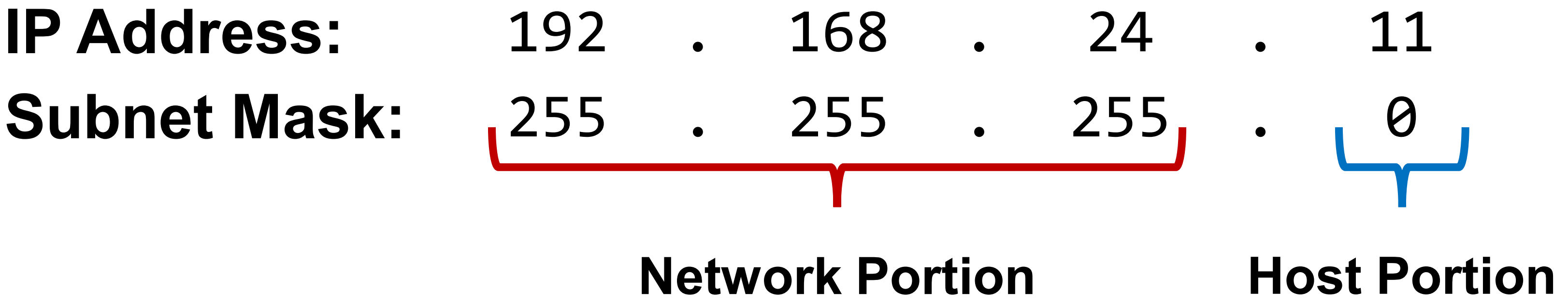
- A subnet is a logical division (segment) of an IP network
- A portion of the IP address for hosts that belong to the same subnet will identify the network (routing prefix) the hosts belong to
- The remainder of the IP address identifies the individual host within the subnet



Internet Protocol Version 4 – Subnet Mask

- In IPv4 networks, the subnet mask is used to determine the network and host portions of an IP address
- Like an IPv4 address, the subnet mask is expressed in dot-decimal notation, and contains 4 octets of 8 binary bits
- A subnet mask is identifiable as a string of one or more 1s followed by one or more 0s when expressed in binary
- The routing prefix can be determined by performing a bitwise AND operation on the IP address and subnet mask
- The routing prefix may also be expressed in CIDR notation, a slash (/) followed by the bit-length of the routing prefix

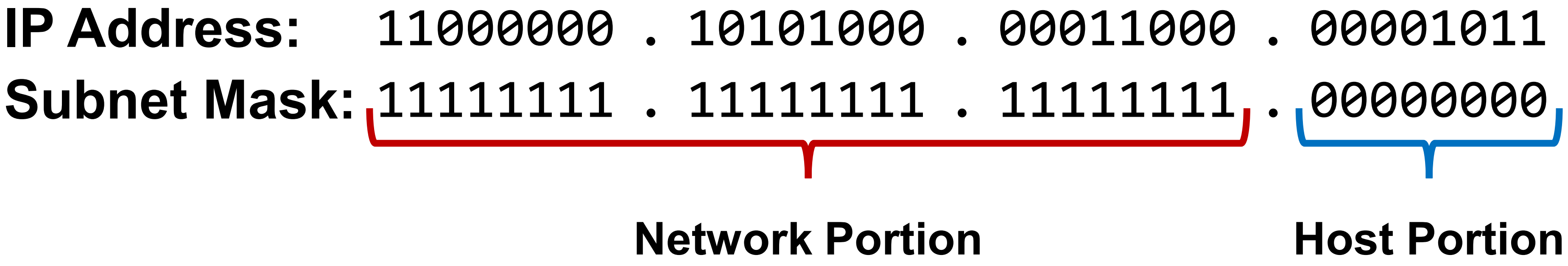
Internet Protocol Version 4 – Subnet Mask



IP Address: 192 . 168 . 24 . 11

Subnet Mask: 255 . 255 . 255 . 0

Network Portion **Host Portion**



IP Address: 11000000 . 10101000 . 00011000 . 00001011

Subnet Mask: 11111111 . 11111111 . 11111111 . 00000000

Network Portion **Host Portion**

CIDR Notation: 192 . 168 . 24 . 11 / 24

Internet Protocol Version 4 – Routing Prefix

IP Address:	192	.	168	.	24	.	11
Subnet Mask:	255	.	255	.	255	.	0
IP Address:	11000000	.	10101000	.	00011000	.	00001011
Bitwise AND	+		+		+		+
Subnet Mask:	11111111	.	11111111	.	11111111	.	00000000
	↓		↓		↓		↓
Result:	11000000	.	10101000	.	00011000	.	00000000
	192	.	**168**	.	**24**	.	**0**

IP Version 4 – Address Space Exhaustion

- To successfully communicate on the public internet, both the sending and receiving devices must have unique IP address in one of the public ranges
- Based on IANA IPv4 Special-Purpose Address Registry, if 588,514,304 addresses are reserved from a possible total of 4,294,967,296 (2^{32}), there are 3,706,452,992 public IP addresses
- When the protocol was initially created, the wide-spread availability of the internet was not anticipated
- As we have surpassed 7.5 billion people on the planet, we have a shortage of IPv4 addresses

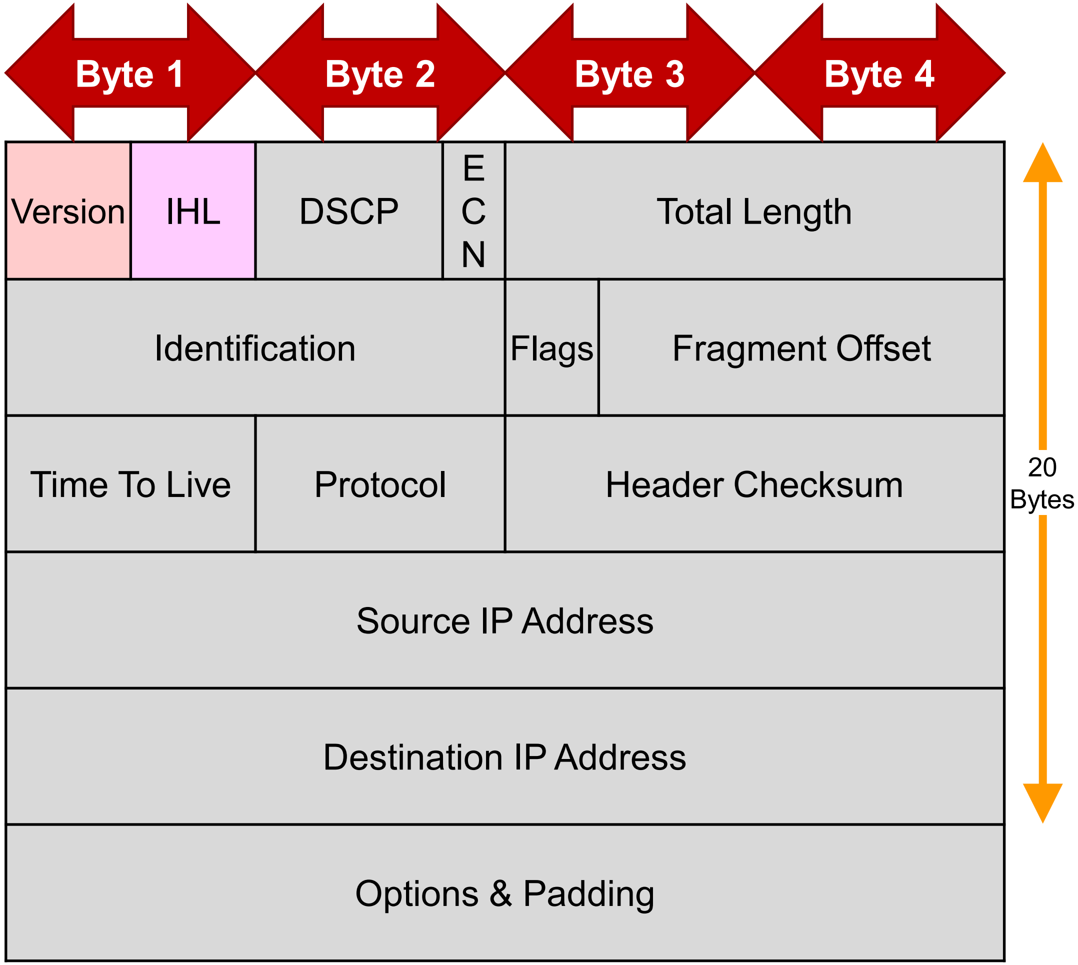
IP Version 4 – Public and Private Addressing

- To compensate for this shortage, private address ranges were designated for use within privately controlled networks
- Private address ranges are combined with Network Address Translation (NAT) to conserve the public IP address space
- Private addresses allow many devices inside a private network to communicate on the internet using a single IP address, or a range of addresses

IP Version 4 – Special Use Address Ranges

Class	Range	Scope	RFC	Description
A	0.0.0.0/8	Software	1122	Represents current host (source only)
	10.0.0.0/8	**Private**	**1918**	**Used for private networks**
	127.0.0.1/8	Host	1122	Used as a loopback address for the local host
B	169.254.0.0/16	Link-Local	3927	Used for Automatic Private IP Addressing (APIPA)
	172.16.0.0/12	**Private**	**1918**	**Used for private networks**
C	192.0.2.0/24	Documentation	5737	TEST-NET-1 - To be used only for documentation
	192.168.0.0/16	**Private**	**1918**	**Used for private networks**
	198.51.100.0/24	Documentation	5737	TEST-NET-2 - To be used only for documentation
	203.0.113.0/24	Documentation	5737	TEST-NET-3 - To be used only for documentation
Other	255.255.255.255/32	Subnet	8190/919	Use for limited broadcast

Network Layer Packet Headers – IPv4



Byte 1 | Byte 2 | Byte 3 | Byte 4

Version | IHL | DSCP | ECN | Total Length

Identification | Flags | Fragment Offset

Time To Live | Protocol | Header Checksum

Source IP Address

Destination IP Address

Options & Padding

20 Bytes

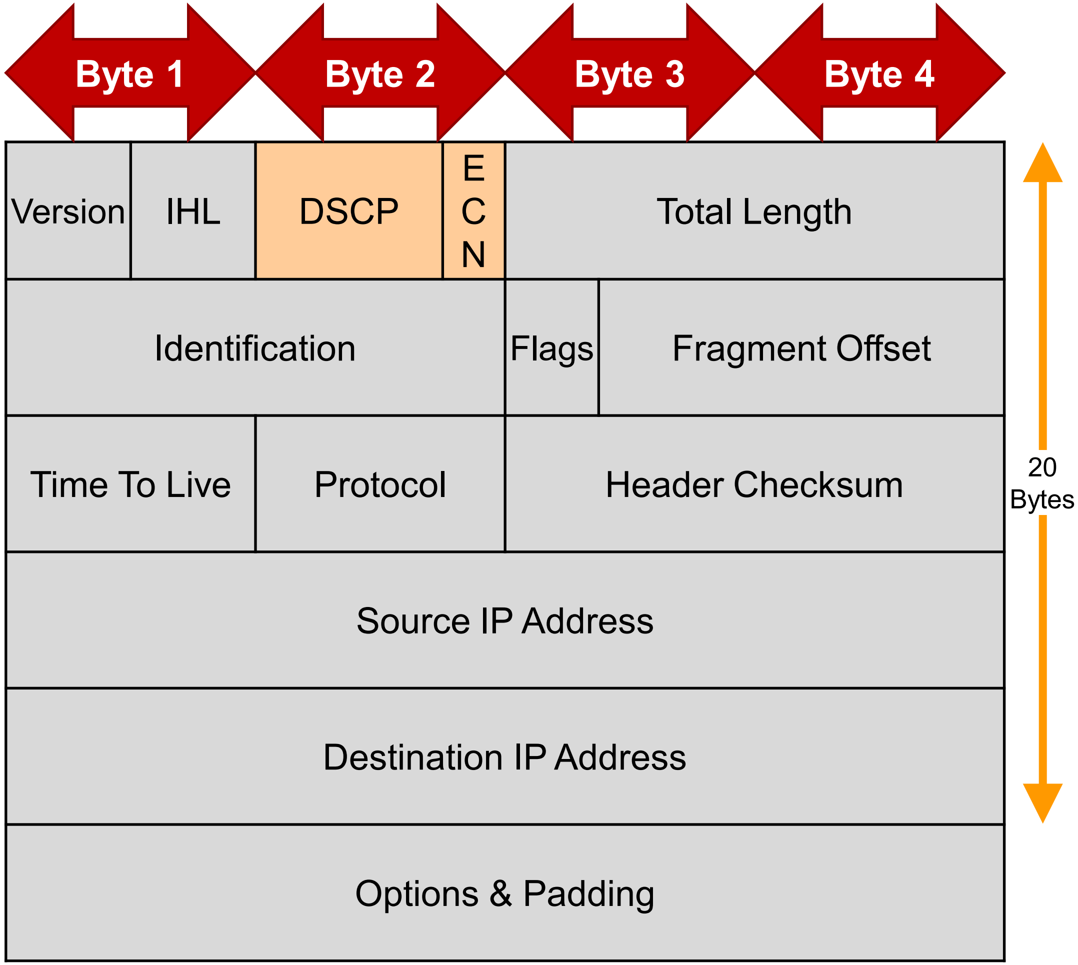
Version 4 bits:

- Identifies the header
- For IPv4, this field always equals 4

Internet Header Length (IHL) 4 bits:

- The length of the header, in 32 bit boundaries 5x32=160 bits or 20 Bytes
- A value larger than 5 means options are used

Network Layer Packet Headers – IPv4



Byte 1 | Byte 2 | Byte 3 | Byte 4

Version | IHL | DSCP | ECN | Total Length

Identification | Flags | Fragment Offset

Time To Live | Protocol | Header Checksum

Source IP Address

Destination IP Address

Options & Padding

20 Bytes

Differentiated Services Code Point (DSCP)

8 bits:

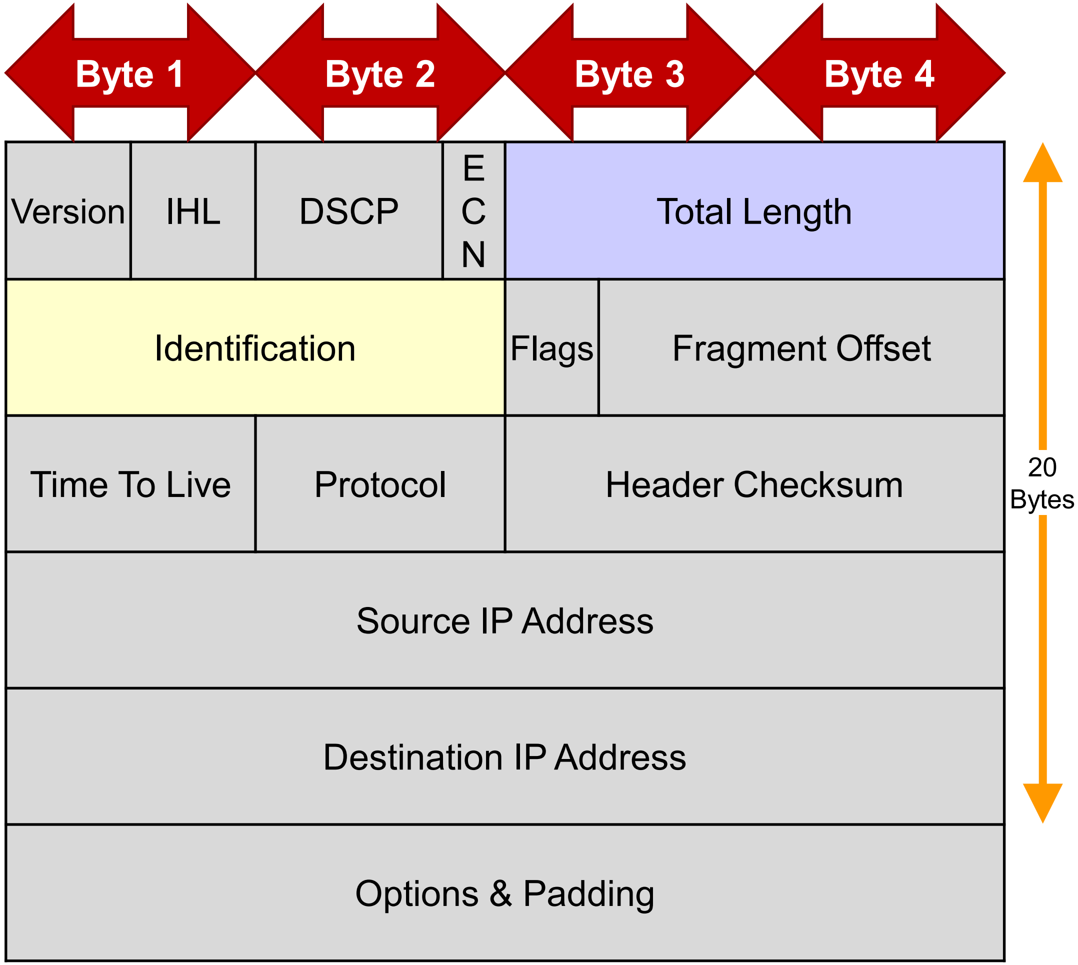
- Classifies traffic for QoS operations

Explicit Congestion Notification (ECN)

2 bits:

- Provides end-to-end notification of congestion

Network Layer Packet Headers – IPv4



Byte 1
Byte 2
Byte 3
Byte 4

Version | IHL | DSCP | ECN | Total Length

Identification | Flags | Fragment Offset

Time To Live | Protocol | Header Checksum

Source IP Address

Destination IP Address

Options & Padding

20 Bytes

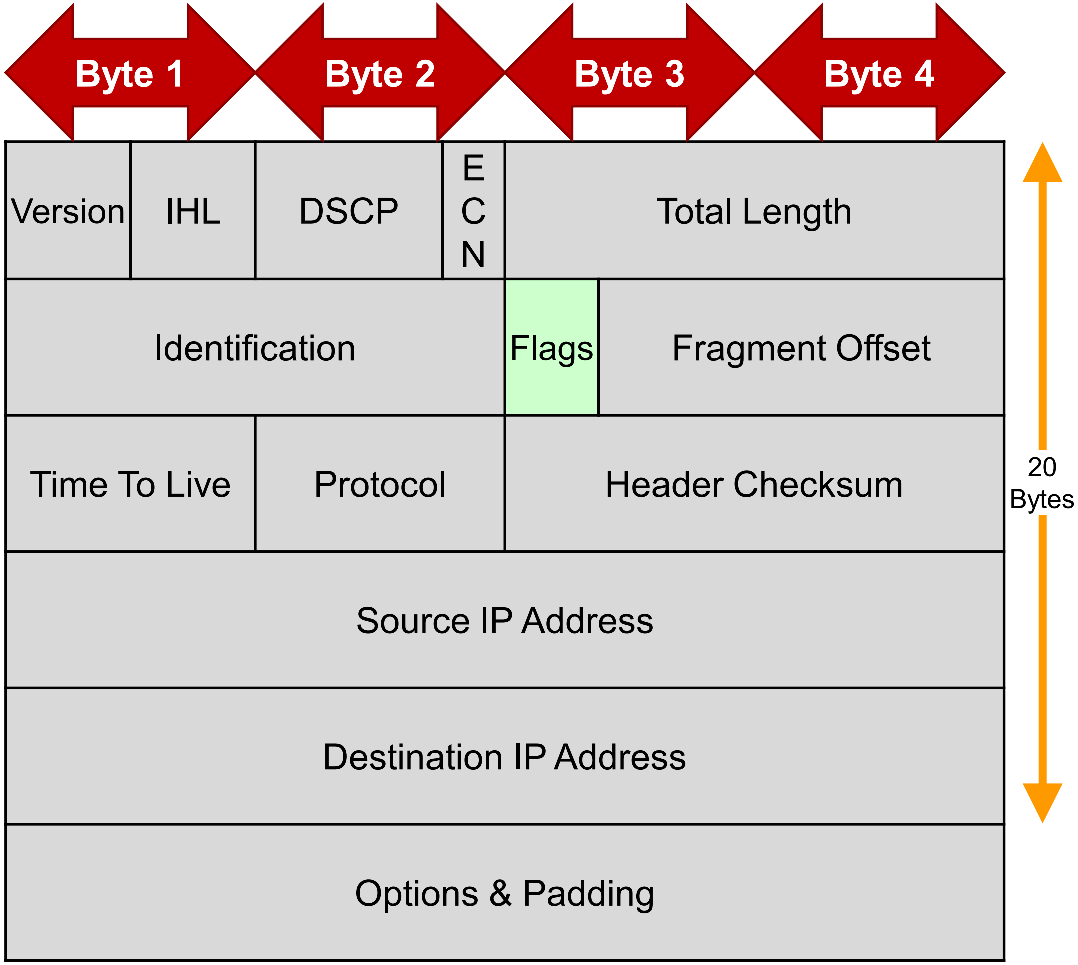
Total Length 16 bits:

- Defines the total length of the packet including header and data (does not include padding)
- Packets can be up to 65,535 bytes long

Identification 16 bits:

- A unique packet identifier is assigned to each datagram

Network Layer Packet Headers – IPv4



Byte 1

Byte 2

Byte 3

Byte 4

Version

IHL

DSCP

ECN

Total Length

Identification

Flags

Fragment Offset

Time To Live

Protocol

Header Checksum

Source IP Address

Destination IP Address

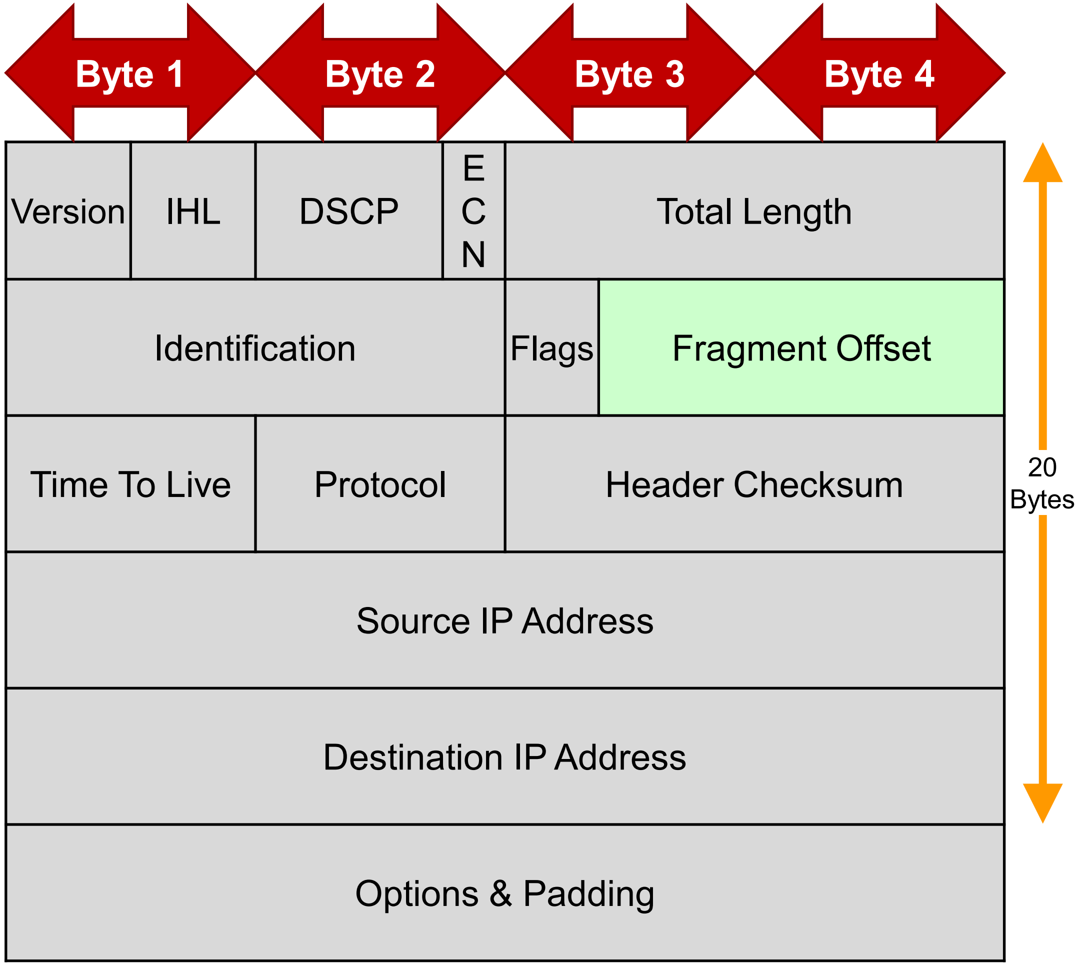
Options & Padding

20 Bytes

Flags 3 bits:

- Used for fragmentation
- **Bit 0 Reserved** – must be set to zero
- **Bit 1 Don’t Fragment (DF)** - tells forwarding devices to drop the packet if it is too large to continue
- **Bit 2 More Fragments (MF)** – set to notify the receiving device that more fragments will arrive

Network Layer Packet Headers – IPv4



Byte 1 | Byte 2 | Byte 3 | Byte 4

Version | IHL | DSCP | ECN | Total Length

Identification | Flags | Fragment Offset

Time To Live | Protocol | Header Checksum

Source IP Address

Destination IP Address

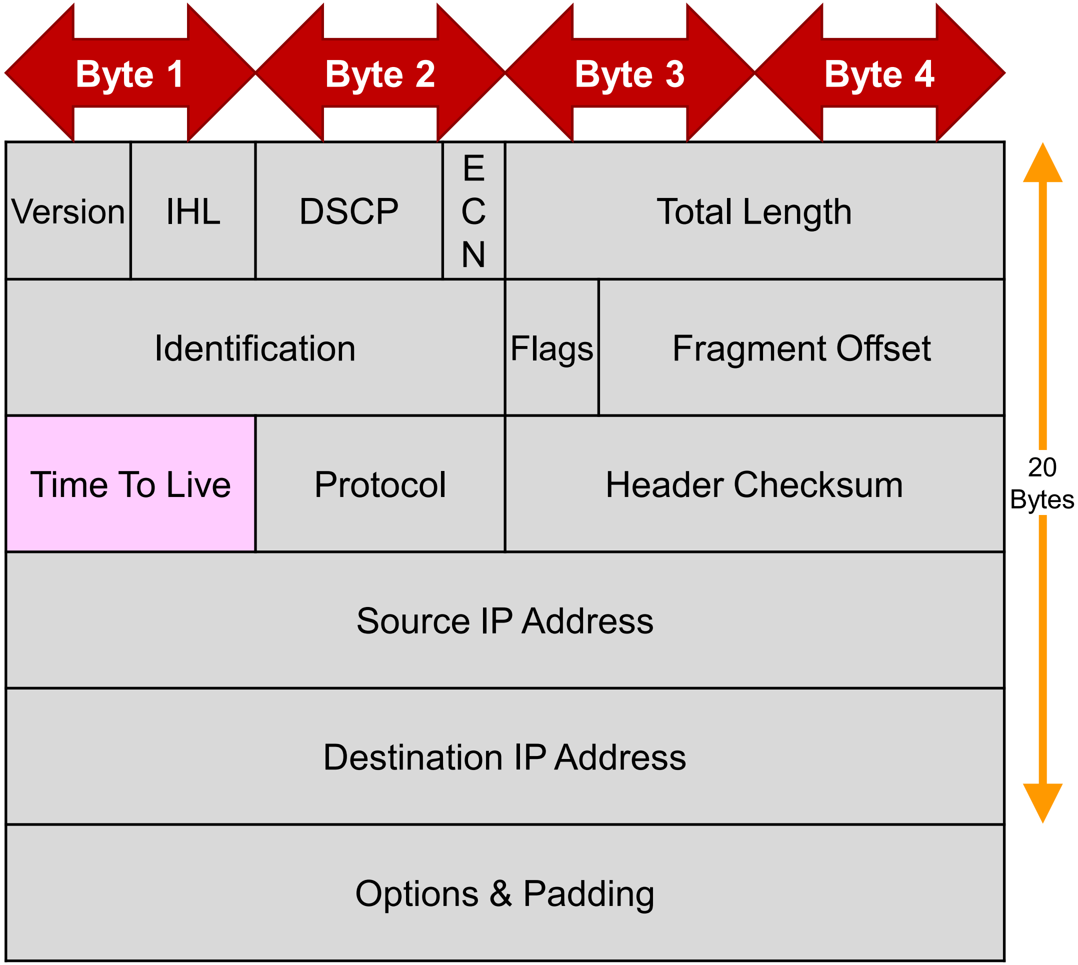
Options & Padding

20 Bytes

Fragment Offset 13 bits:

- Specifies the offset of a particular fragment in 8 byte blocks that relate to the beginning of the original unfragmented packet
- The first fragmented packet has an offset of zero

Network Layer Packet Headers – IPv4



Byte 1

Byte 2

Byte 3

Byte 4

Version

IHL

DSCP

ECN

Total Length

Identification

Flags

Fragment Offset

Time To Live

Protocol

Header Checksum

Source IP Address

Destination IP Address

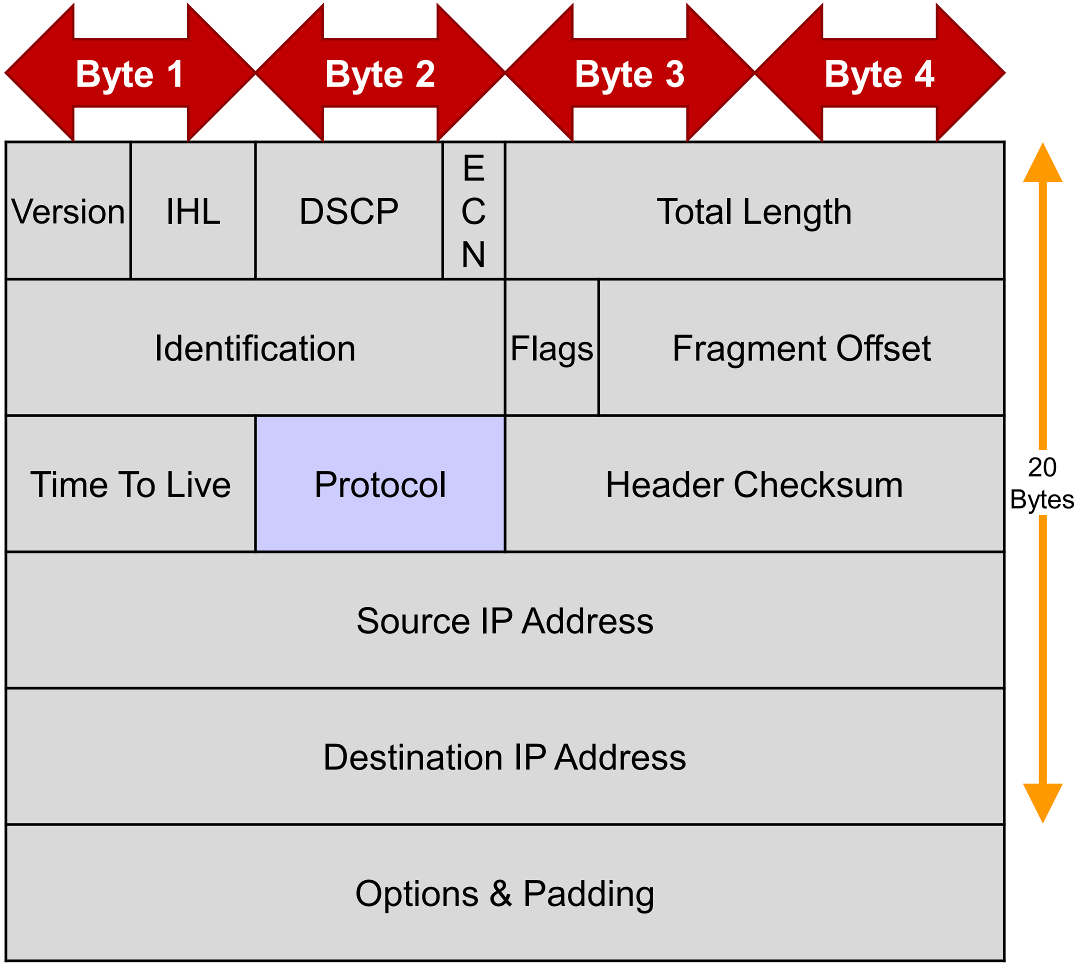
Options & Padding

20 Bytes

Time To Live (TTL)
8 bits:

- Specifies how long a packet can live before being dropped
- This life is not measured in seconds, but in “hops”
- When the count reaches zero the packet is dropped and an ICMP Time Exceeded message is sent to the sending host

Network Layer Packet Headers – IPv4



Byte 1 Byte 2 Byte 3 Byte 4

Version | IHL | DSCP | ECN | Total Length

Identification | Flags | Fragment Offset

Time To Live | Protocol | Header Checksum

Source IP Address

Destination IP Address

Options & Padding

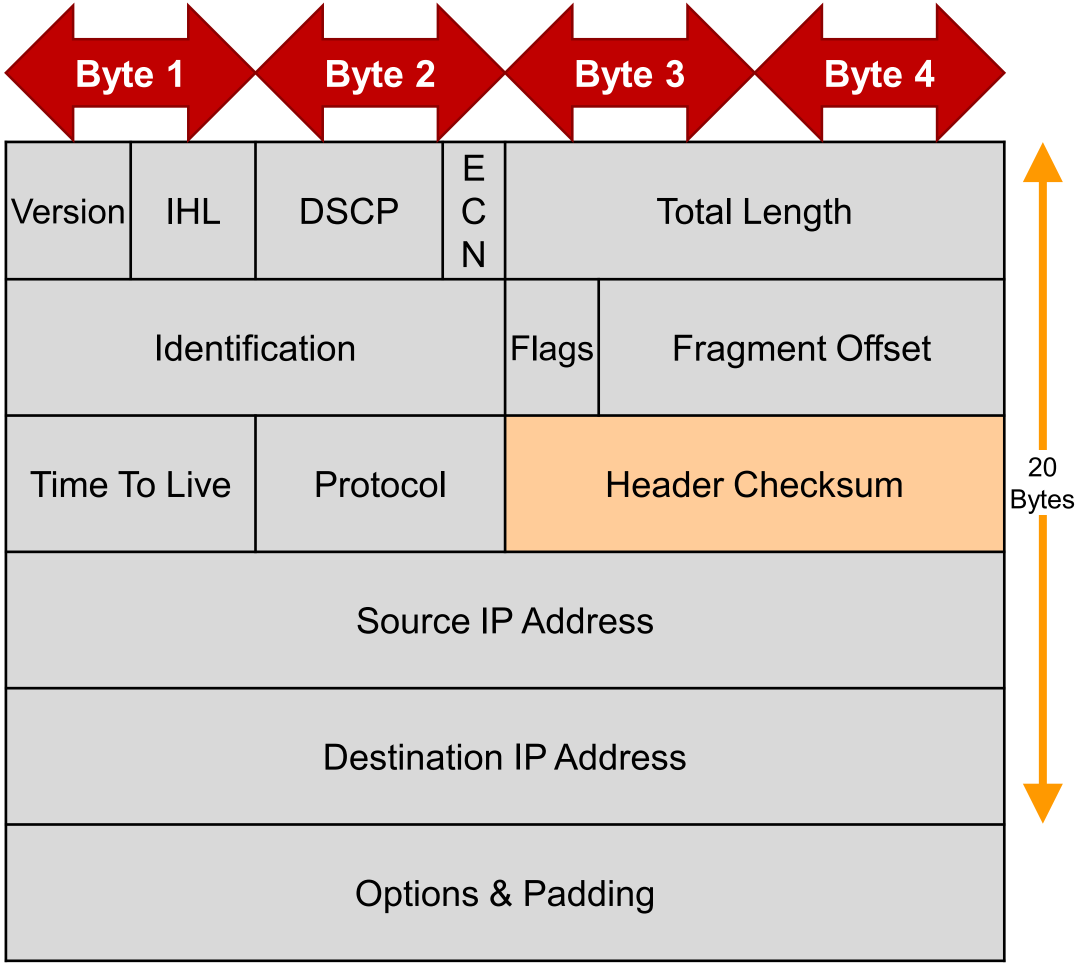
20 Bytes

Protocol 8 bits:

- Specifies the upper layer protocol that is encapsulated in the packet
- Possible values include:

#	Protocol	Description
1	ICMP	Internet Control Message Protocol
6	TCP	Transport Control Protocol
17	UDP	User Datagram Protocol
89	OSPF	Open Shortest Path First

Network Layer Packet Headers – IPv4



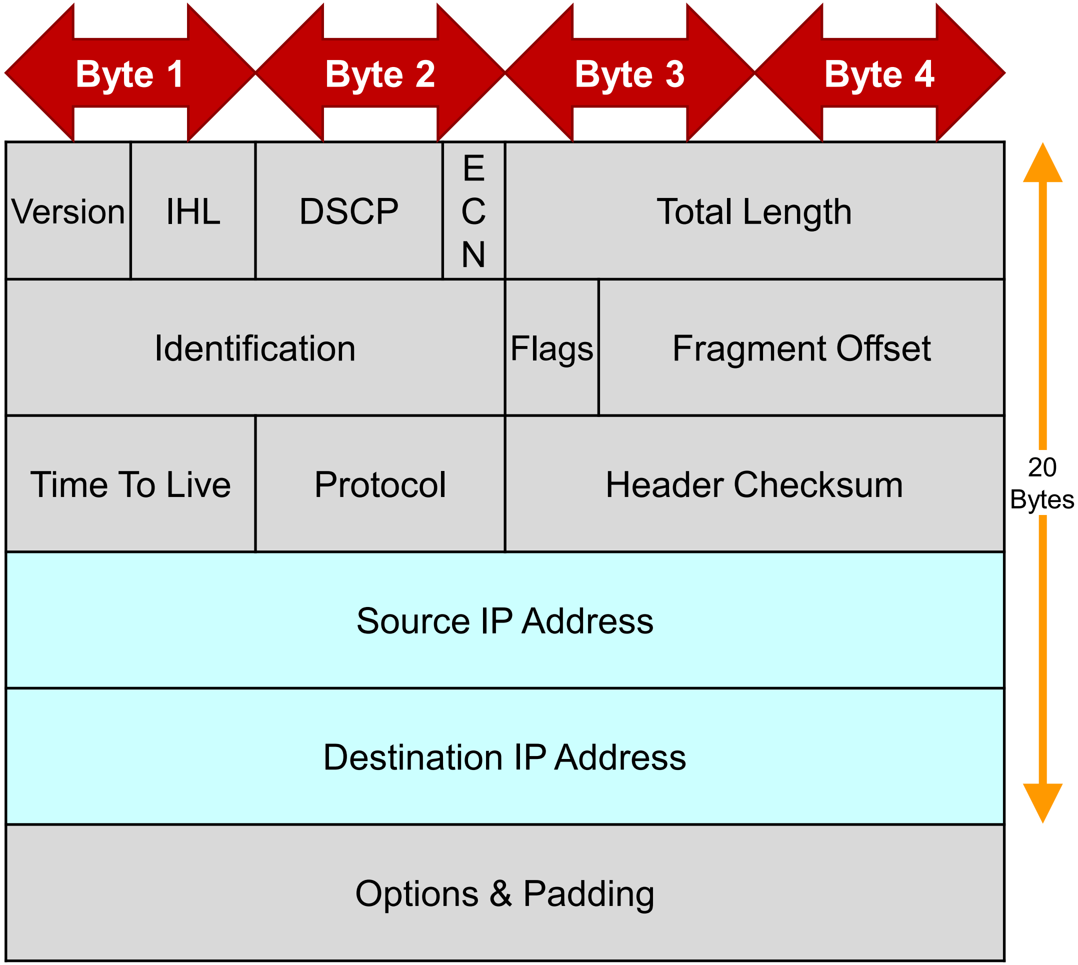
Header Checksum

16 bits:

- Used to verify that the header (not the actual data) has not been corrupted during transmission

NOTE: checksum is a ones compliment of the original sum, so if it is added to the sum at this host it should result in all ones

Network Layer Packet Headers – IPv4

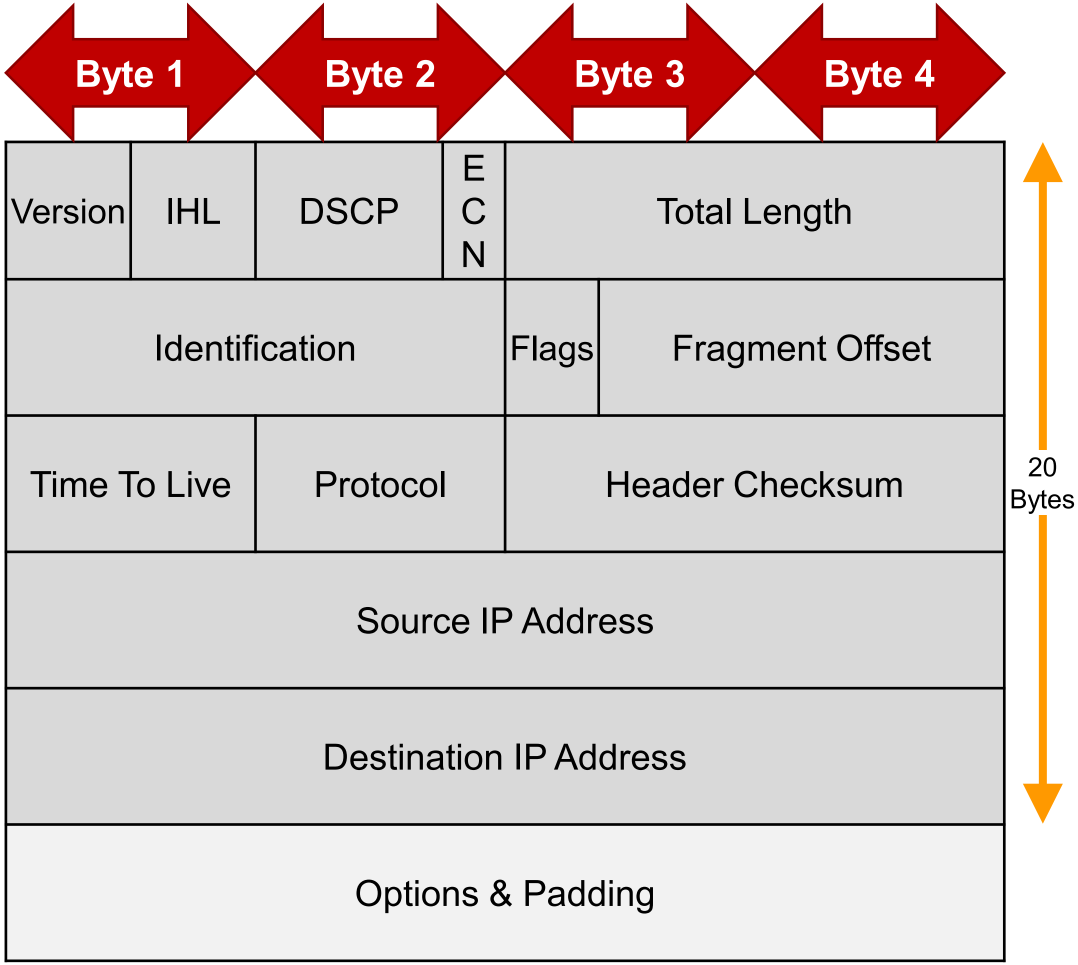


<table>
<tr><td>Version</td><td>IHL</td><td>DSCP</td><td>ECN</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="4">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time To Live</td><td colspan="2">Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="6">Source IP Address</td></tr>
<tr><td colspan="6">Destination IP Address</td></tr>
<tr><td colspan="6">Options & Padding</td></tr>
</table>

Source/Destination IPv4 Address 32 bits:

- The IPv4 addresses of the sending and receiving devices
- May be changed in-transit if the packet undergoes translation

Network Layer Packet Headers – IPv4



Byte 1

Byte 2

Byte 3

Byte 4

Version

IHL

DSCP

ECN

Total Length

Identification

Flags

Fragment Offset

Time To Live

Protocol

Header Checksum

Source IP Address

Destination IP Address

Options & Padding

20 Bytes

Options varies:

- Not commonly used
- The IHL value must be adjusted if options are used

Padding varies:

- A number of zeros that is added when options are used to ensure the packet is a multiple of 32 bits

IP version 4 - Fragmentation

- When a router encounters a packet that is larger than the egress interface’s MTU, and the Don’t Fragment bit is set to 0, the router must fragment the packet so it can successfully traverse the link
- The router will divide the packet into fragments that equal the MTU of the egress interface minus the size of the IP header
- The router adds an IP header to each fragment, but modifies the following fields:
  - **Total Length:** set to the size of the fragment
  - **More Fragments:** set to 1, except on the last fragment
  - **Fragment Offset:** Set based on the relation of the current fragment to the original packet
  - **Header Checksum:** Calculated based on the new packet

IP version 4 - Fragmentation

Fragmentation Example:

- A packet with a size of 3,660 bytes is sent across the network
- Upon leaving the organization, the packet comes across a connection with an MTU of 1,480 bytes
- As the Don’t Fragment bit is set to 0, the border router is responsible for fragmenting the packet and does so
- This process results in the following fragments:

#	Identification	Total Bytes	IP Header	Payload	More Fragments	Fragment Offset
1	0x0087	1480	20	1460	1	0
2	0x0087	1480	20	1460	1	185
3	0x0087	760	20	740	0	370

Internet Protocol – MTU Path Discovery

- Path MTU is defined as the smallest MTU of any device between the source and destination
- MTU path discovery is a technique to identify the smallest MTU along a path
- In order to accomplish this, the sending device sets the Don’t Fragment bit on outgoing packets
- If a device along the path has an MTU smaller than the size of the packet, the device will drop the packet and send an ICMP Destination Unreachable (Fragmentation Required, and DF flag set) to the source along with the MTU of the next hop

Internet Protocol – MTU Path Discovery

- The source can then adjust its assumed MTU appropriately and retransmit the data
- This process will repeat until the packet successfully reaches the destination
- The MTU path discovery process may fail if an administrator has blocked all ICMP messages from entering the network to prevent denial of service attacks
- If ICMP traffic is not desired on the network, it should be appropriately filtered, not blocked entirely

References

- UTP Cabling Image - Retrieved from: https://www.flickr.com/photos/33399192@N02/3113089409
- Spectrum Analyzer Image (cropped) – Retrieved from: https://en.wikipedia.org/wiki/File:Bluetooth_signal_behind_wireless_lan_signal.png
- SC Optical Fiber Image – Retrieved from: https://commons.wikimedia.org/wiki/File:SC-optical-fiber-connector-hdr-0a.jpg
- Spectrum Analyzer 5Ghz (modified) – Retrieved from: https://commons.wikimedia.org/wiki/File:SpectrumAnalyzerDisplay.png

References

- Speedtest.net Images - Retrieved from: https://www.speedtest.net
- IP Version 4 – Special Use Address Ranges:
  - https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
- Session Layer
  - https://searchnetworking.techtarget.com/definition/Session-layer