Networking: OSI and TCP/IP

EEL 4745C: Microprocessor Applications II

Fall 2022

Md Jahidul Islam

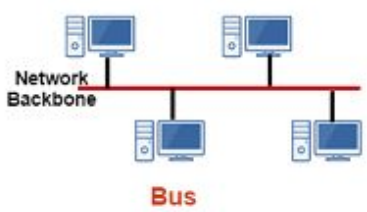
Lecture 7

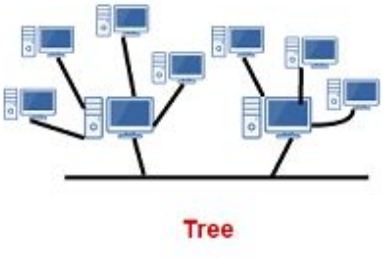
ECE | Florida
Electrical & Computer Engineering

UF | UNIVERSITY of FLORIDA

Network Topology

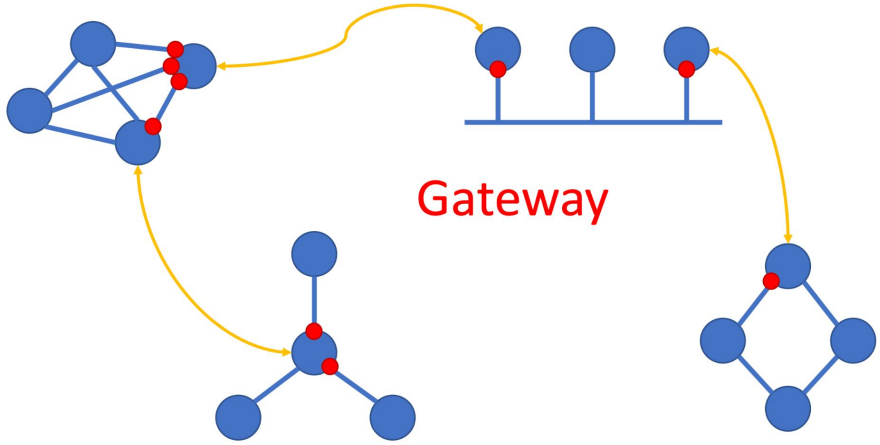
- Topology of a network consists
  - Nodes
  - Links between nodes
  - Protocols that govern data transmission between nodes
- Basic topologies
  - Point-to-point
  - Bus
  - Star
  - Ring or circular
  - Mesh
  - Tree hybrid



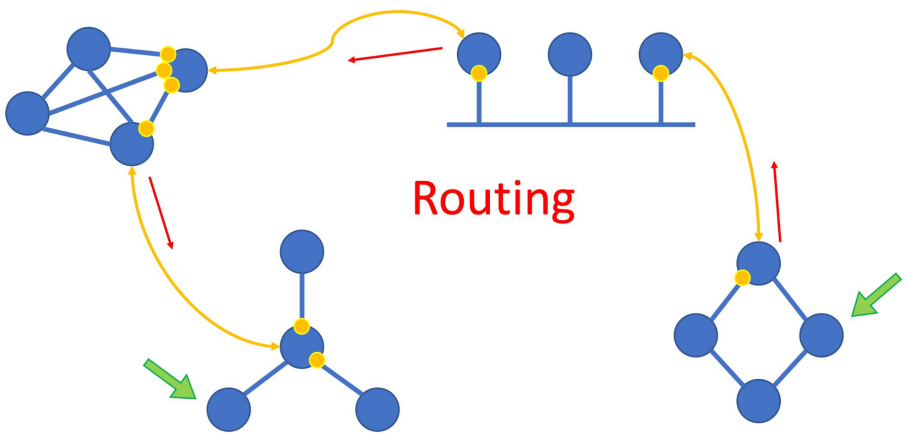


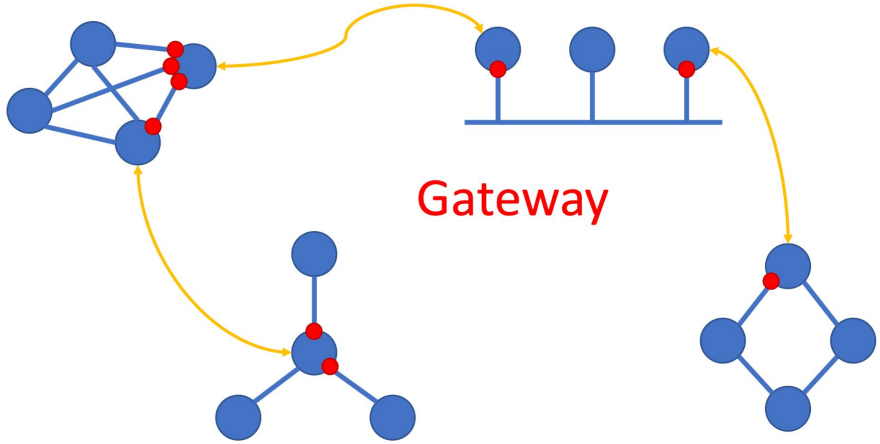
Network Gateways

- A gateway is a network node that
  - Forms a passage between two networks operating with different transmission protocols.
  - Links networks by performing translation between different protocols and data formats at the network boundary.
- ISPs may deploy gateways to connect the corporate LAN to the public Internet or to link different internal networks.
- Two main types of gateways
  - Unidirectional gateways
  - Bidirectional gateways



Network Routing





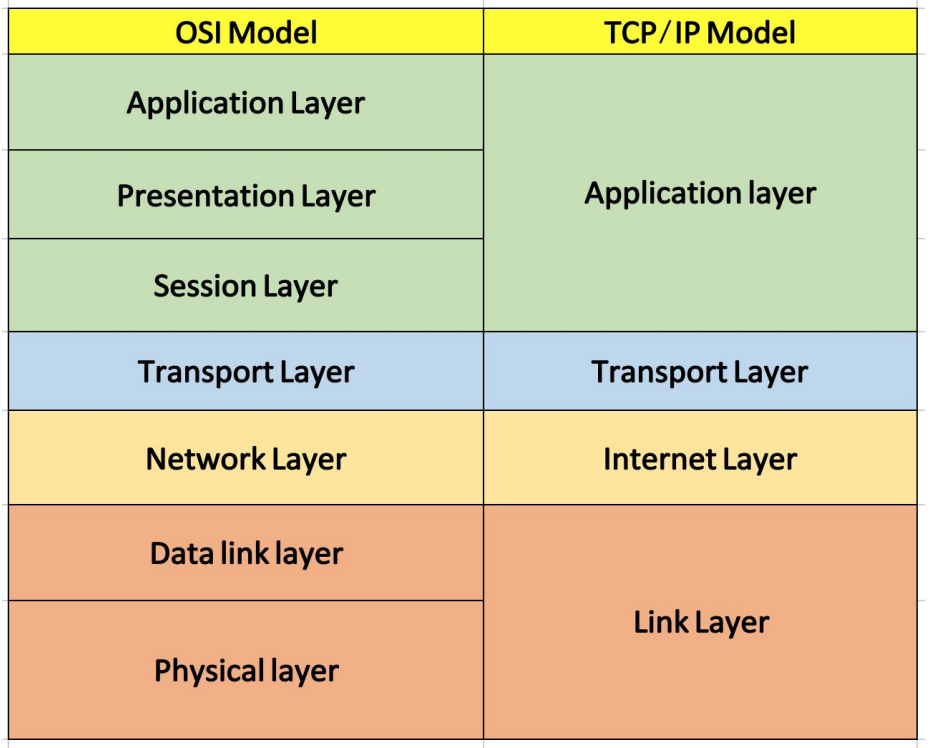
Router vs gateway

- *A router is a networking layer system used to manage and forward data packets to devices network.*
- *A gateway is simply a hardware that acts as a gate between the networks.*

Network System Models

- Operating System Interconnection model **(OSI model)**
  - Developed by the International Organization for Standardization (ISO): *1970-84*
  - Seven layers: protocols operate on certain layers; some protocols operate across layers
  - A conceptual model

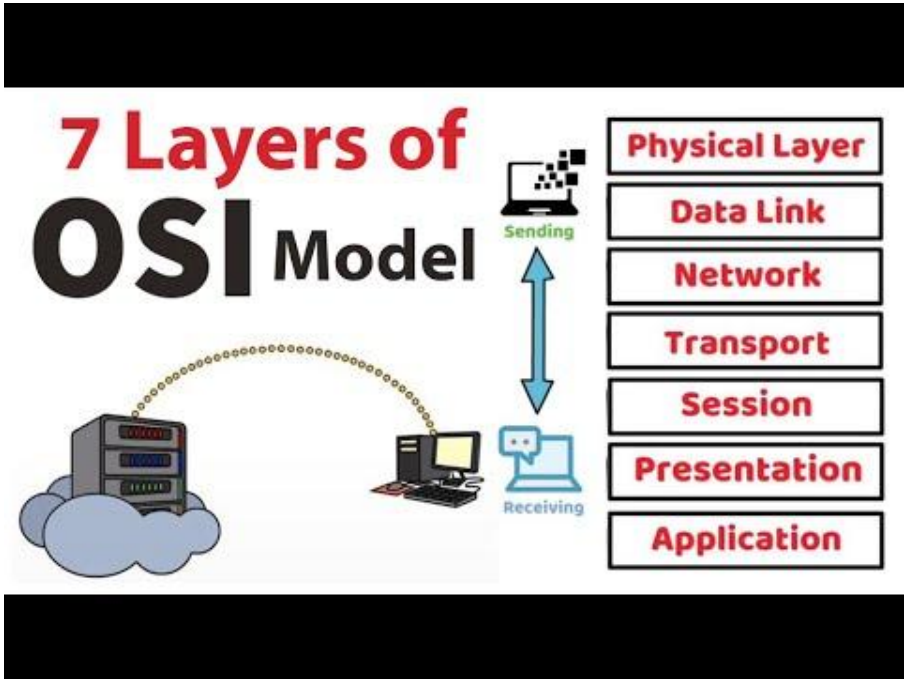
- **TCP/IP Model**
  - Similar to OSI model in nature: eliminates some protocols and complexity
  - Support for a flexible architecture
  - Adding more systems to a network is easy.
  - *See more here*



OSI and TCP/TP

	OSI	TCP/IP	Protocol Data Unit	Devices
7	Application	Application	Data	Layer 7 Firewall
6	Presentation			
5	Session			
4	Transport	Transport	Segments	Layer 4 Firewall
3	Network	Internet	Packets	Router, Multilayer Switch, Wireless Router
2	Data Link	Network Access	Frames	Switch, Bridge, NIC, Wireless Access Point
1	Physical		Bits	Hub, NIC, Wireless Access Point

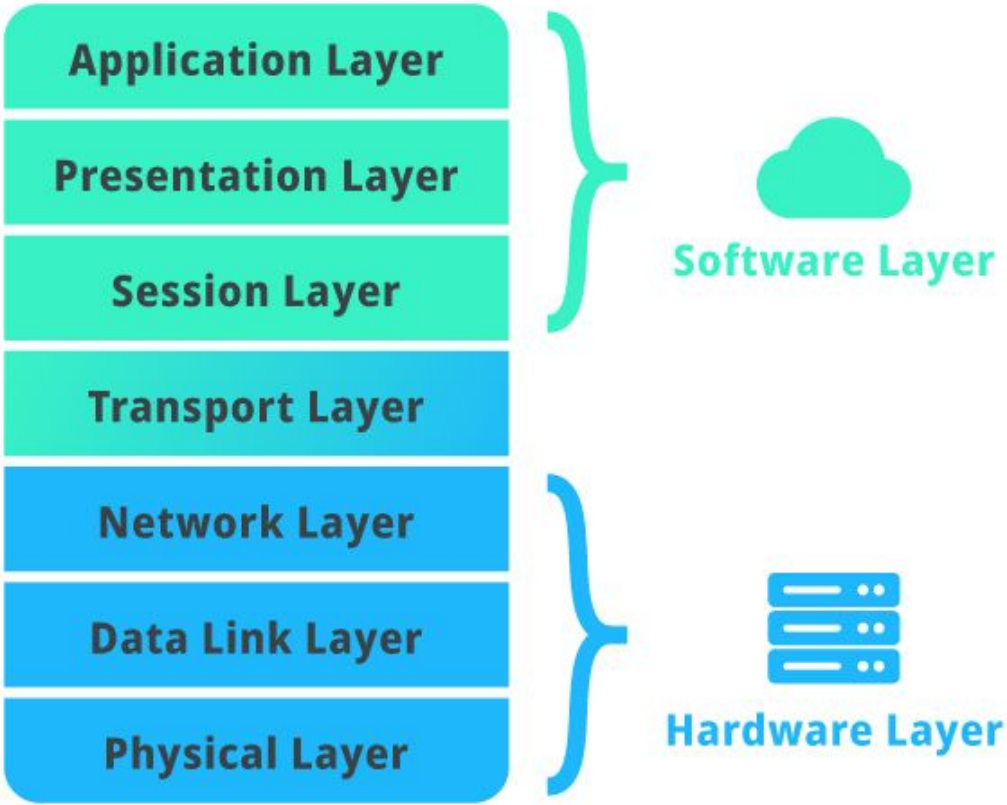
OSI and TCP/TP



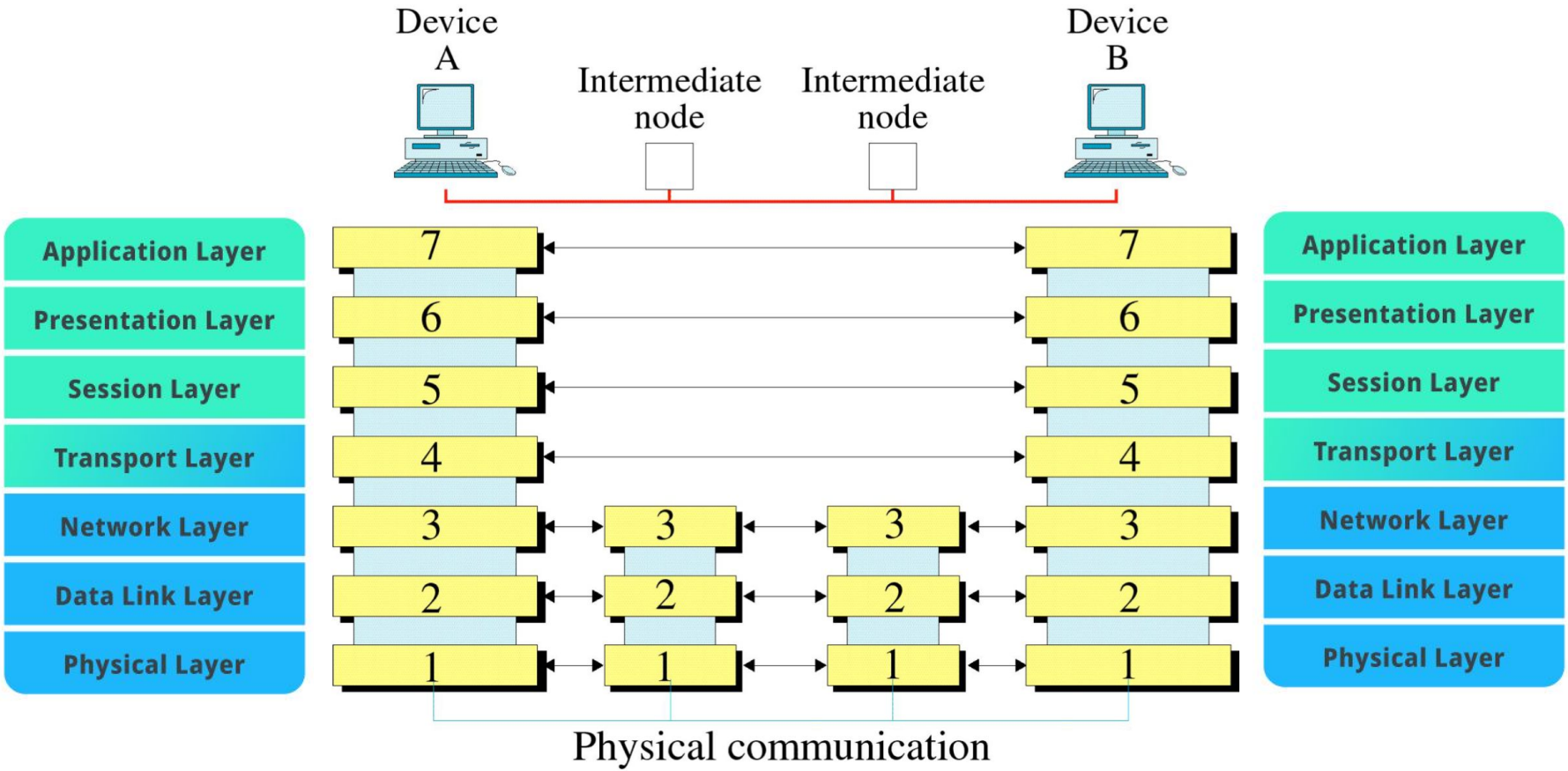
https://youtu.be/Ca1jnqwqzg0

https://youtu.be/LX_b2M3IzN8

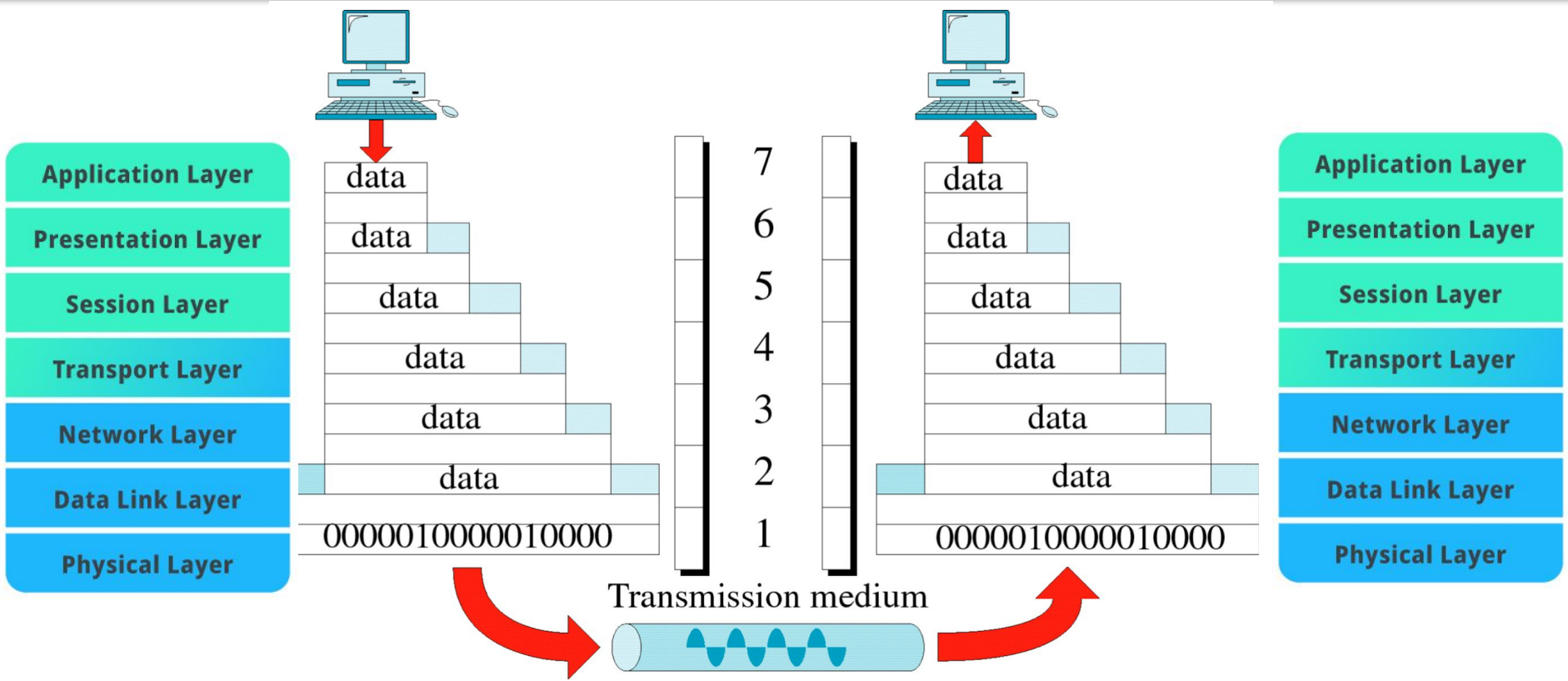
OSI Model: Layered Communication



OSI Model: Layered Communication

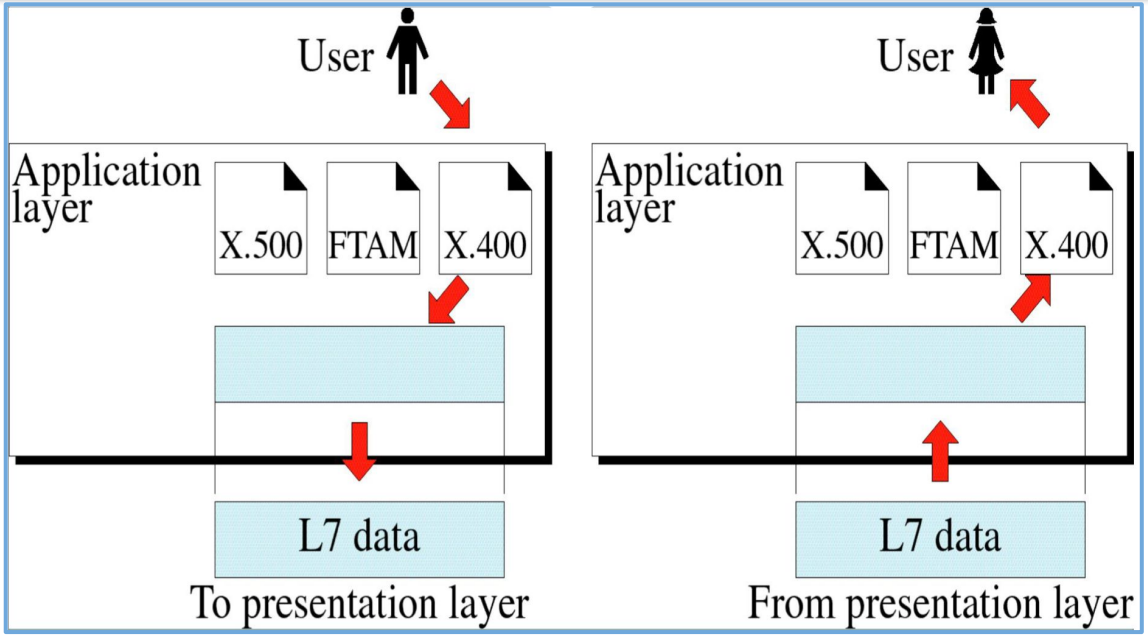


OSI Model: Layered Communication



OSI Model: Application Layer

- Enables the user to access network.
- Provides user interface & supports for services such as e-mail, file transfer, access to the world wide web.
- Provides services to different user applications.
- A few example protocols:
  - Hypertext Transfer Protocol (HTTP)
  - File Transfer Protocol (FTP)
  - Post Office Protocol (POP)
  - Simple Mail Transfer Protocol (SMTP)
  - Domain Name System (DNS)

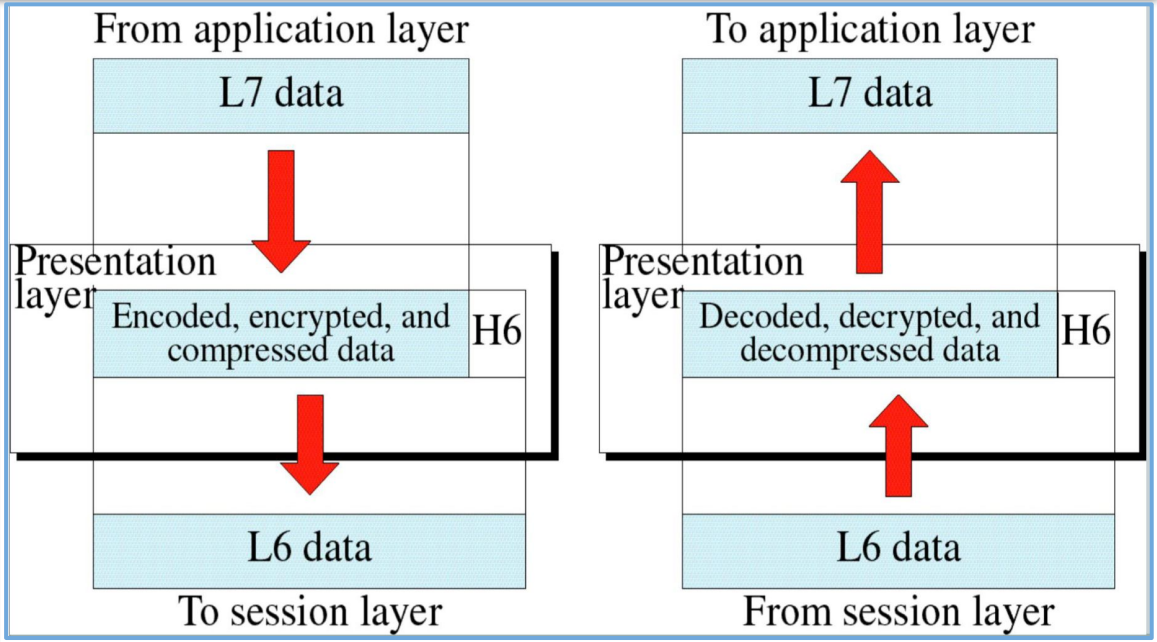


OSI Model: Application Layer Protocols

Protocol	Name	Description
HTTP	Hypertext Transfer Protocol	Allows bidirectional transfer of data between a client and a server. Most commonly used by web browsers.
FTP	File Transfer Protocol	Allows bidirectional data transfer between clients and servers. Optimized to transfer individual files.
IRC	Internet Relay Chat	Allows bidirectional text data streams to be sent across clients and servers. Used in some chat services.
SSH	Secure Shell	Allows for secure remote access.
SMTP	Simple Mail Transfer Protocol	Used to send e-mails to a server.
POP	Post Office Protocol	Used to receive e-mails from a server.
IMAP	Internet Message Access Protocol	Used by e-mail clients to retrieve messages from a server.
XMPP	Extensible Messaging and Presence Protocol	Used in some chat applications to allow client-to-client communications over a distributed network.

OSI Model: Presentation Layer

- It is concerned with the syntax & semantics of the information exchanged between two devices.
- Takes any data transmitted by the application layer and prepares it for transmission over the session layer.
- A few example protocols:
  - Apple Filing Protocol (AFP)
  - Lightweight Presentation Protocol (LPP)
  - NetWare Core Protocol (NCP)
  - Teletype Network (Telnet)

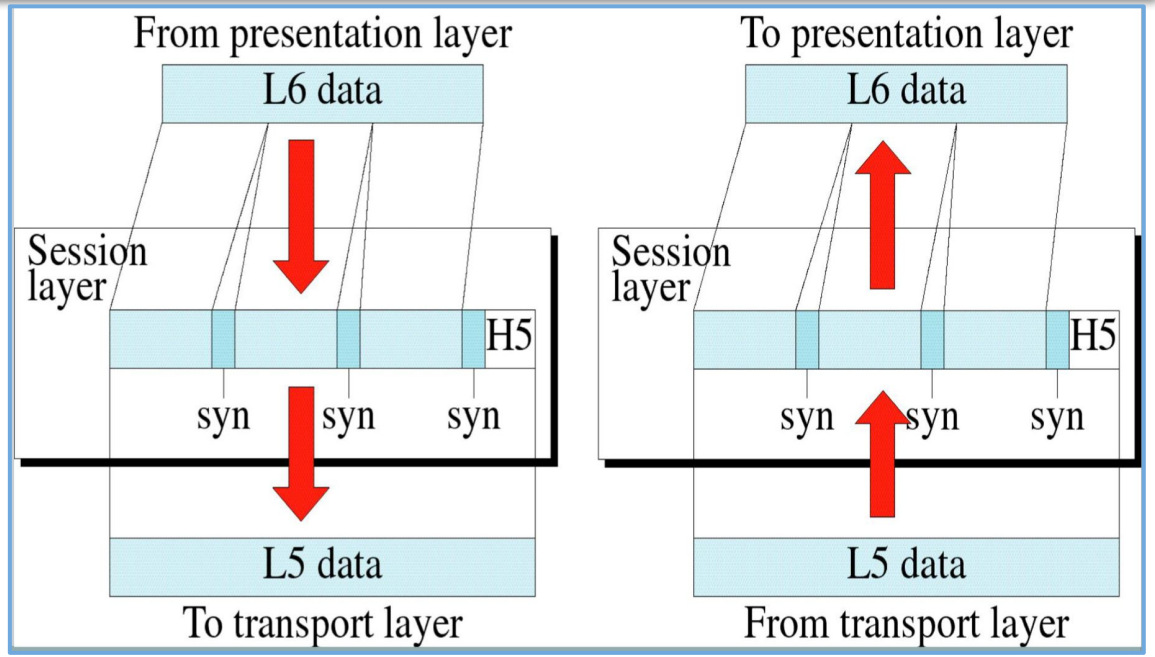


OSI Model: Presentation Layer

Protocol	Name	Description
Telnet	Teletype Network	Provides a bidirectional, text oriented communication facility using virtual terminals
NCP	NetWare Core Protocol	Allows for clock synchronization, file, directory access, messaging and remote command execution
LPP	Lightweight Presentation Protocol	Used to provide ISO presentation services to L5 of the OSI model
AFP	Apple Filing Protocol	Part of the Apple File Service, allowing remote access of directories and files.

OSI Model: Session Layer

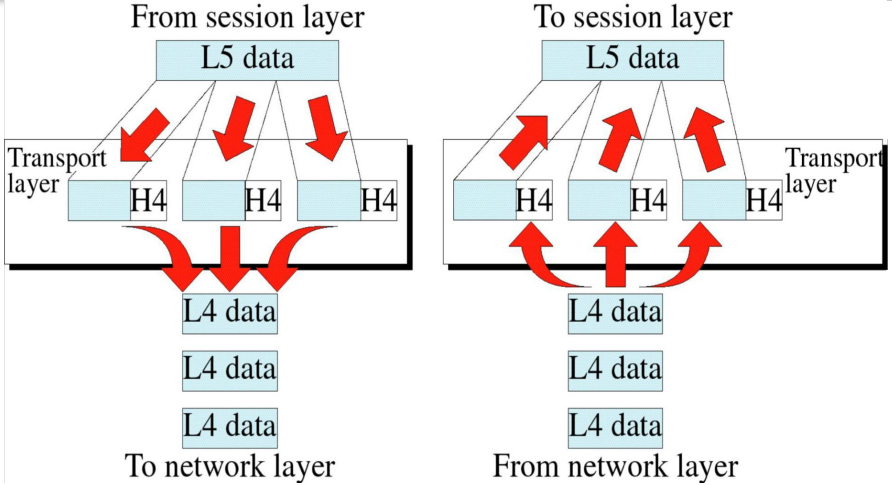
- It is responsible for establishing, managing, synchronizing and terminating sessions between end-user application processes.
  - Opens sessions
  - Ensures they remain open and functional while data is being transferred
  - Closes sessions safely when communication ends
- The session layer can also set checkpoints during a data transfer
  - If the session is interrupted, devices can resume data transfer from the last checkpoint.



OSI Model: Session Layer Protocols

Protocol	Name	Description
PPTP	Point-to-Point Tunneling Protocol	Method for implementing virtual private networks, now obsolete. Has many known security issues.
RPC	Remote Procedure Call	Used for distributed computing to request execution of remote subroutines and obtain the result of the computation as if executed in the local machine.
NetBIOS	Network Basic Input Output System	Non-routable protocol that allows applications to communicate over a network, providing name services, datagram distribution services (stateless), and session services (stateful).
L2TP	Layer 2 Tunneling Protocol	Used to support virtual private networks by providing a tunneling mechanism.
H.245	Call Control Protocol for Multimedia Applications	Used for the line transmission of non-telephone signals.
SOCKS	Secure Sockets	Allows for the exchange of network packets between a client and a server over a proxy server.
SSL	Secure Sockets Layer	Provides communication security over a computer network. Superseded by TLS.
TLS	Transport Layer Security	Modern version of SSL. Provides communication security over a computer network.

OSI Model: Transport Layer

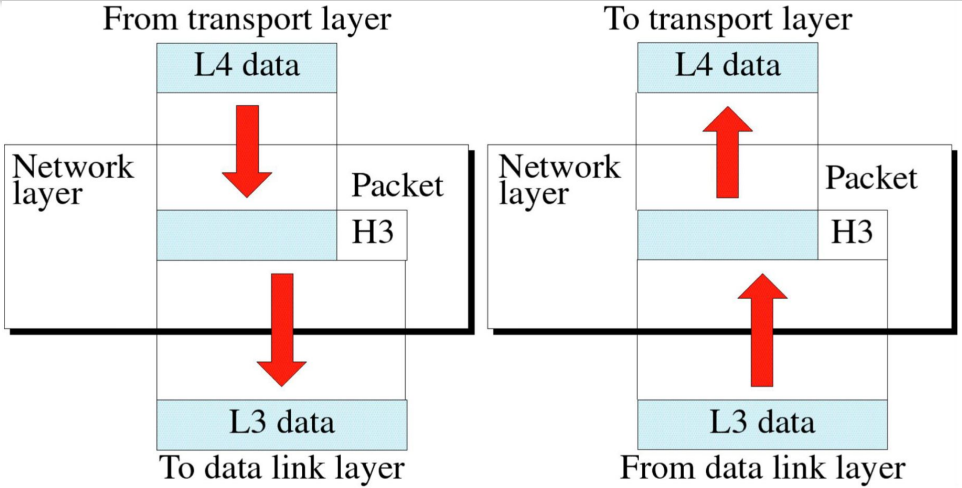


- The transport layer takes data transferred in the session layer and breaks it into *"segments"* on the transmitting end. It is also responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer.
- The transport layer carries out flow control, sending data at a rate that matches the connection speed of receiving device, error control, checking if data was received incorrectly and if not, requesting it again.
- Protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

OSI Model: Transport Layer Protocols

Protocol	Name	Description
TCP	Transmission Control Protocol	Stream-oriented protocol that provides reliable, ordered, and error-checked delivery over an IP network.
UDP	User Datagram Protocol	Datagram-oriented (message oriented) protocol that provides error-checking but does not guarantee delivery, ordering, or datagram duplication.
RDP	Reliable Data Protocol	Connection-oriented protocol that provides facilities for remote loading, debugging, and bulk transfer of images and data, but does not guarantee ordering.
ATP	AppleTalk Transmission Protocol	Used in old Apple machines as the backbone for AppleTalk services.
SST	Structured Stream Transport Protocol	Experimental protocol that provides reliable, ordered, and error-checked delivery ove IP networks with enhanced stream management.

OSI Model: Network Layer

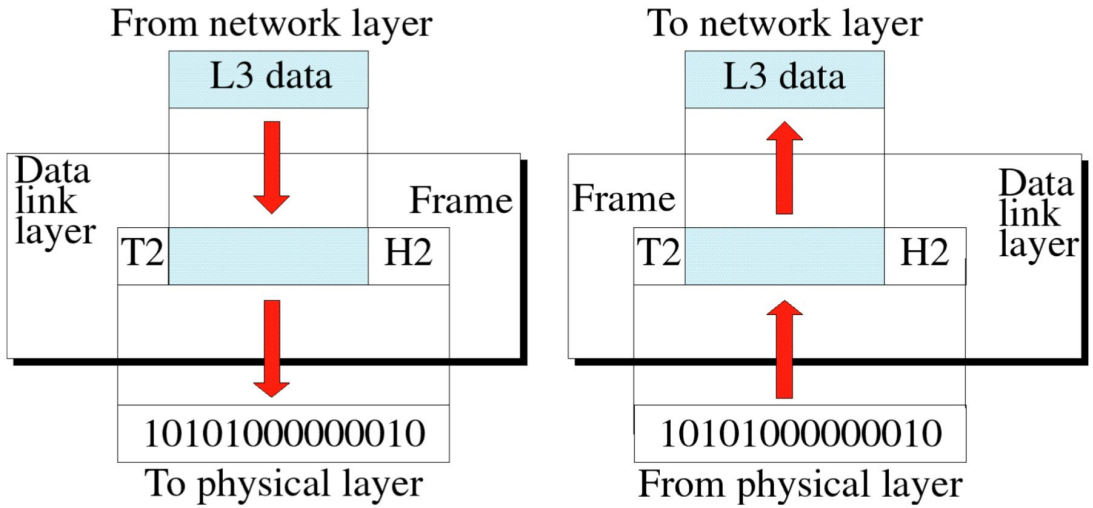


- The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network.
- It uses network addresses (typically IP addresses) to route packets to a destination node.
- Protocols: Internet Protocol (IP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP)

OSI Model: Network Layer Protocols

Protocol	Name	Description
IP	Internet Protocol	Allows routing between networks in the Internet protocol suite.
IPX	Internetwork Packet Exchange	Allows routing between networks in the IPX/SPX protocol suite.
IPsec	Internet Protocol Security	Authenticates and encrypts packets of data sent over an IPv4 network.
ICMP	Internet Control Message Protocol	Used to send error messages and operational information.
RIP	Routing Information Protocol	Distance-vector routing protocol used to propagate routing tables across routers.
OSPF	Open Shortest Path First Protocol	Protocol used to propagate routing tables using a link state routing algorithm.
EIGRP	Enhanced Interior Gateway Routing Protocol	Allows for automatic routing decision and configuration of routing tables.
BGP	Border Gateway Protocol	Allows for propagation of routing and reachability information.

OSI Model: Data Link Layer

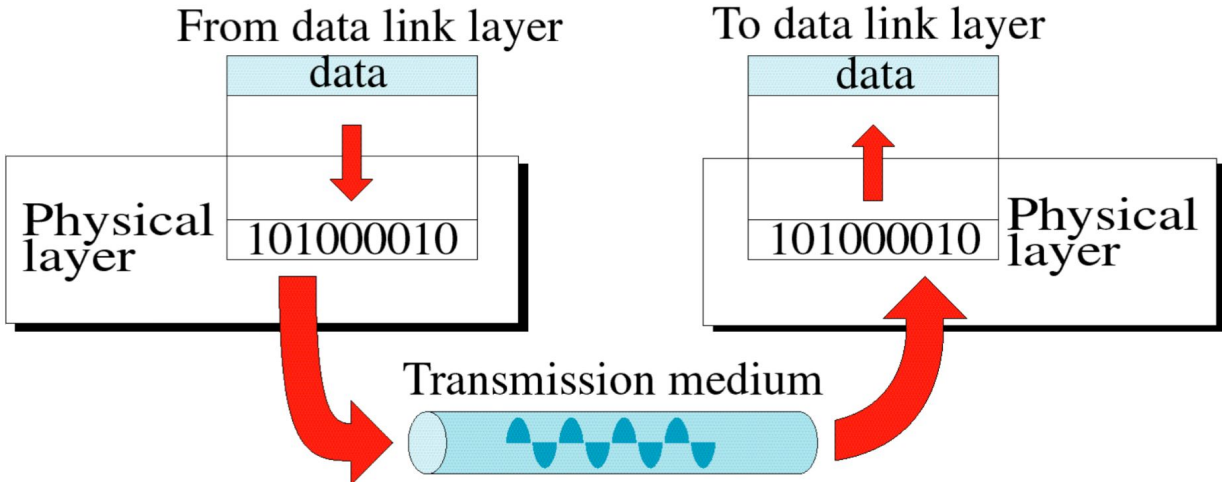


- The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination.
- This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.
- Protocols: Ethernet, Wi-Fi, STP, token ring, and FDDI

OSI Model: Data Link Layer Protocols

Protocol	Name	Description
STP	Spanning Tree Protocol	Builds a loop free topology for Ethernet networks allowing for backup links and eliminating broadcast radiation caused by loops.
IEEE 802.3	Ethernet	Portions of Ethernet are in L2, such as the parts that deal with media access controls.
IEEE 802.11	Wi-Fi	Portions of Wi-Fi are in L2, such as the parts that deal with media access controls.

OSI Model: Physical Layer



- The physical layer is responsible for the physical cable or wireless connection between network nodes.
- It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of **0**s and **1**s, while taking care of bit rate control.
- Protocols: IEEE 802.x, Infrared Data Association, Universal Serial Bus (USB), Bluetooth.

OSI Model: Physical Layer Protocols

Protocol	Name	Description
IEEE 802.3	Ethernet	Portions of IEEE 802.3 reside at this layer, such as those dealing with cabling and modulation.
IEEE 802.11	Wi-Fi	Portions of IEEE 802.11 reside at this layer, such as those dealing with frequencies used and modulation schemes.
IEEE 802.15.1	Bluetooth	Portions of this protocol suite reside at this layer, such as those dealing with frequencies used and modulation schemes.
IEEE 802.15.4	ZigBee, et al	Portions of this protocol suite reside at this layer, such as those dealing with frequencies used and modulation schemes.

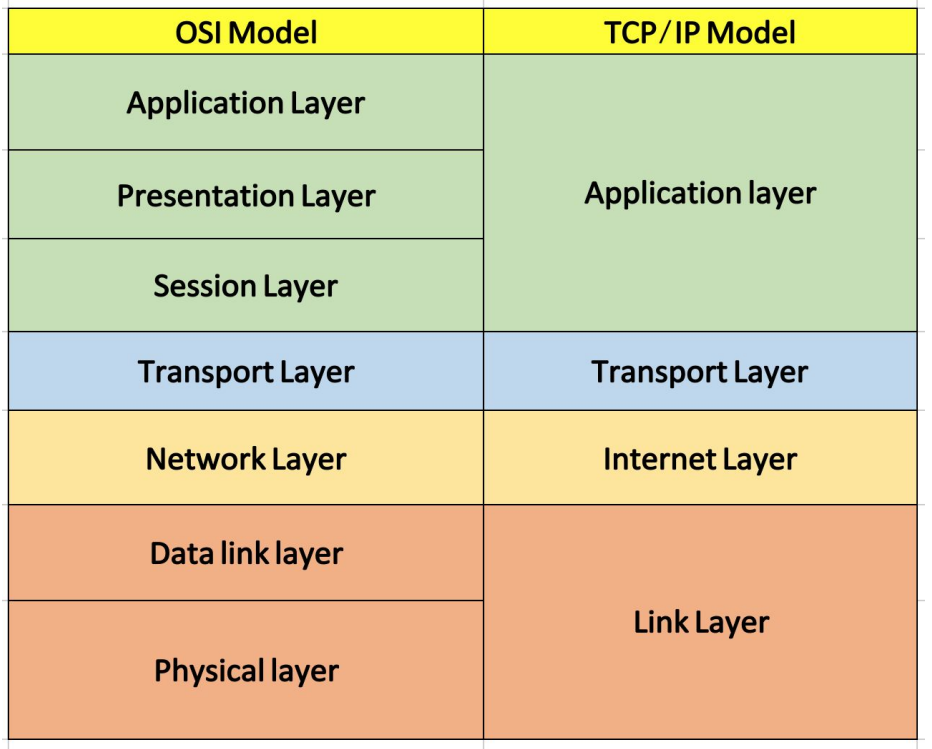
OSI Model: Summary

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY Can be used on all layers		Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

Recap: OSI and TCP/IP Model

- Operating System Interconnection model **(OSI model)**
  - Developed by the International Organization for Standardization (ISO): *1970-84*
  - Seven layers: protocols operate on certain layers; some protocols operate across layers
  - A conceptual model

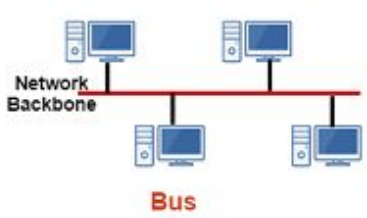
- **TCP/IP Model**
  - Similar to OSI model in nature: eliminates some protocols and complexity
  - Support for a flexible architecture
  - Adding more systems to a network is easy.
  - *See more here*

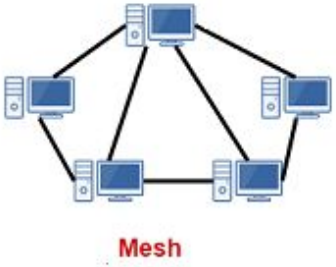


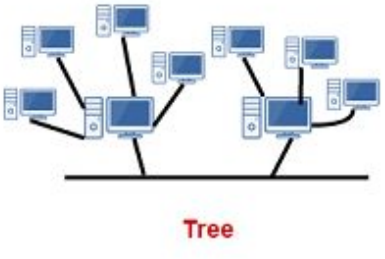
Network Topology

- Topology of a network consists
  - Nodes
  - Links between nodes
  - Protocols that govern data transmission between nodes

- Basic topologies
  - Point-to-point
  - Bus
  - Star
  - Ring or circular
  - Mesh
  - Tree hybrid

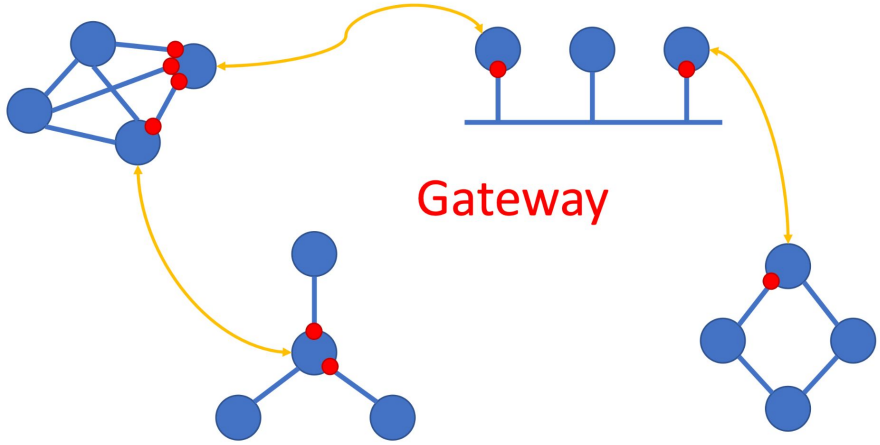




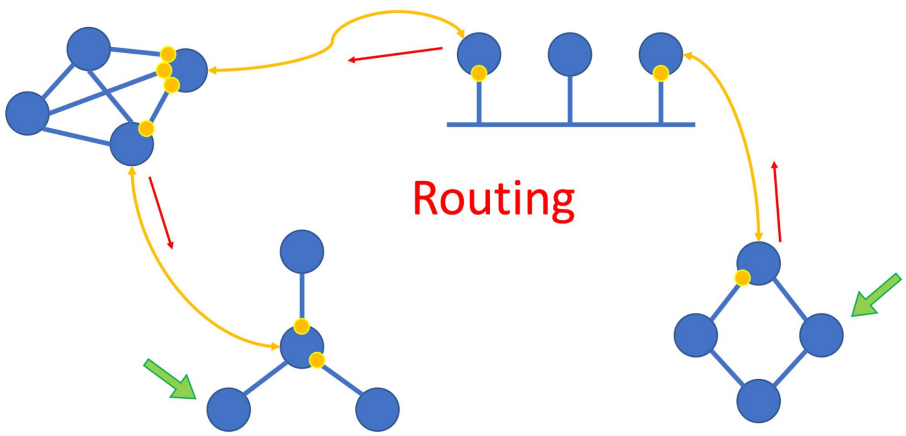


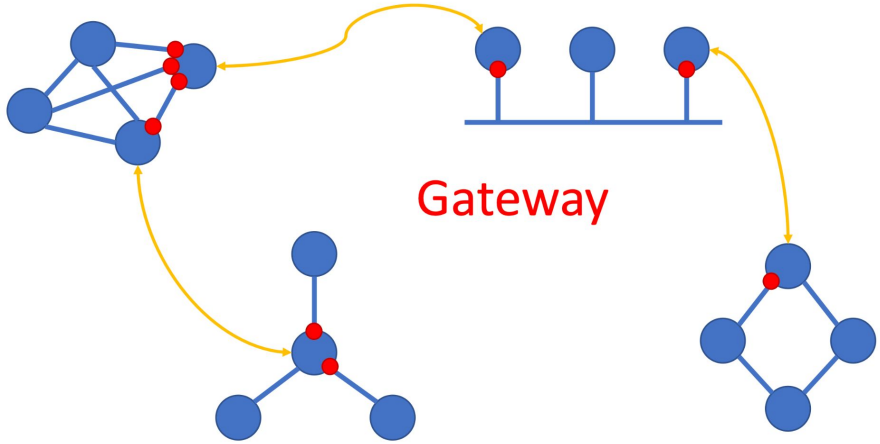
Network Gateways

- A gateway is a network node that
  - Forms a passage between two networks operating with different transmission protocols.
  - Links networks by performing translation between different protocols and data formats at the network boundary.
- ISPs may deploy gateways to connect the corporate LAN to the public Internet or to link different internal networks.
- Two main types of gateways
  - Unidirectional gateways
  - Bidirectional gateways



Network Routing

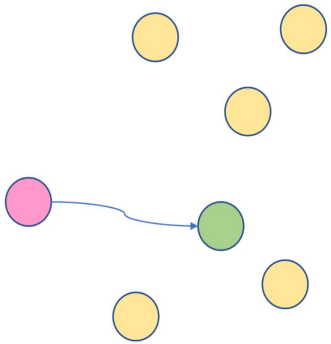


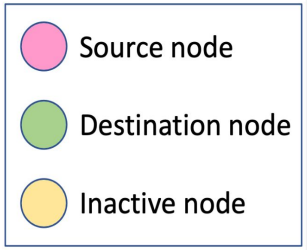


Router vs gateway

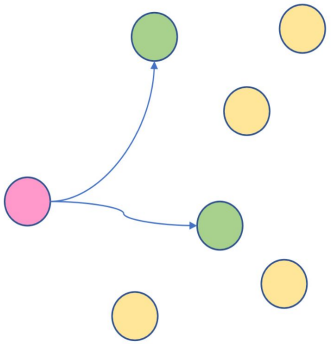
- *A router is a networking layer system used to manage and forward data packets to devices network.*
- *A gateway is simply a hardware that acts as a gate between the networks.*

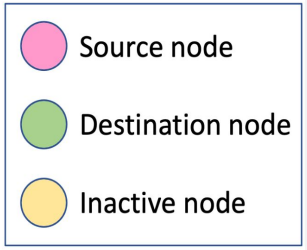
Types of IP Traffic





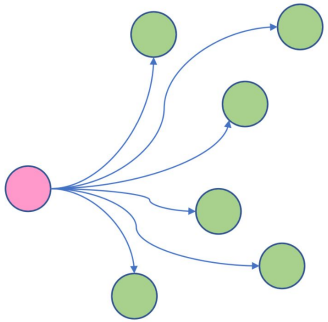
Unicast transmissions refer to one-to-one transmissions from one point in a network to another point in [possibly another] network.

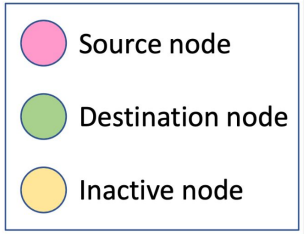




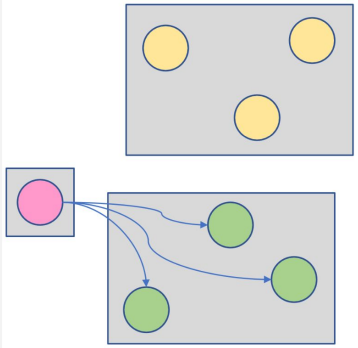
Multicast transmissions refer to one-to-many or many-to-many model. Packets are routed simultaneously in a single transmission to many recipients.

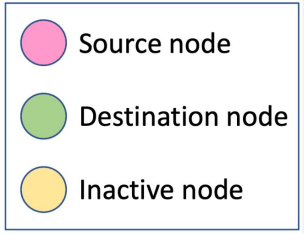
Types of IP Traffic





Broadcast transmissions refer to a one-to-all transmission. The network automatically replicates datagrams (packets) as needed in order to reach all recipients.





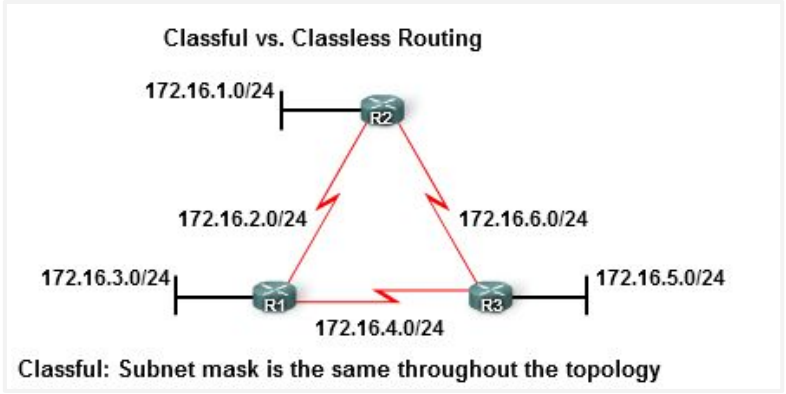
Geocast deliver packets to a group of destinations defined by their geographical location.

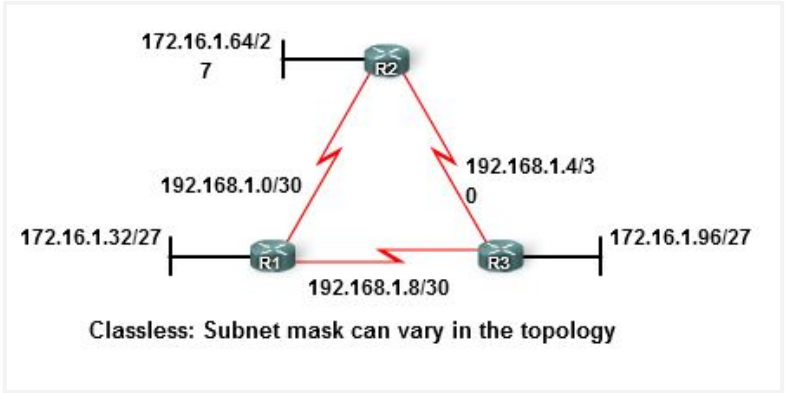
IP: Internet Protocol

- Internet Protocol (IP) addresses are the unique numbers assigned to every computer or device that is connected to the Internet
- **IPv4**: introduced by ARPANET in 1980s
  - 4.29B addresses, about a 1:1 ratio with the world's population in 1980s
  - The available IPv4 addresses have been fully allocated to ISPs and users which is 32-bits long.
- Short-term solution
  - Network Address Translation (NAT) & Port Address Translation (PAT)
  - Private address space
  - Classless Inter-Domain Routing (CIDR)
- **The long-term solution: IPv6**

IPv4

- Most widely deployed version of the Internet Protocol
- Addresses consist of **four** octets groups of **8 bits**
  - 0.0.0.0 – 255.255.255.255
  - 4,394,967,296 addresses in total
  - Not all addresses are actually available
  - IP address divided into two parts:
    - Network identifier and host identifier
- Classful networks
  - Divides the address space for IPv4 into classes
    - Class A - Class E
- Classless Inter-Domain Routing (CIDR)
  - Subverts exhaustion problem in classful addressing
  - Slows growth of routing tables





IPv4: Classful Addressing

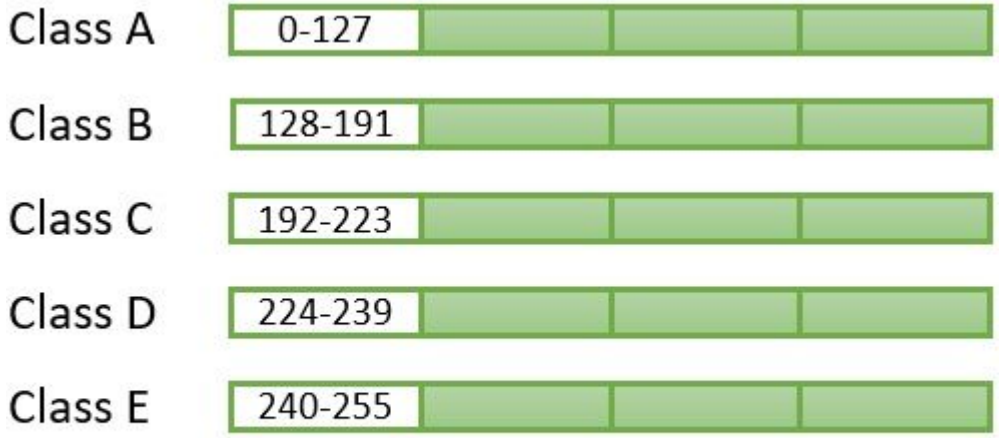
Class	Leading Bits	Size of NNB	Size of Rest Bitfield	# of Networks	Addresses per Network	Total Addresses
A	0	8	24	128	2^{24}	2^{31}
B	10	16	16	2^{14}	2^{16}	2^{30}
C	110	24	8	2^{21}	2^{8}	2^{20}
D	1110	-	-	-	-	2^{28}
E	1111	-	-	-	-	2^{28}

Class	Start Address	End Address
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.255

This scheme is obviously deficient when it comes to IP address distributions.

IPv4: Classful Addressing

- Class A, B, and C, are for "public addressing"
  - Communication is always one-to-one
  - When data is transmitted from a source, it is only sent to a single network host.
  - The first addressing part is network ID
  - The rest is Host ID
- Class D and Class E: reserved categories
  - Class D being utilized for multicast, and
  - Class E being saved for future usage.

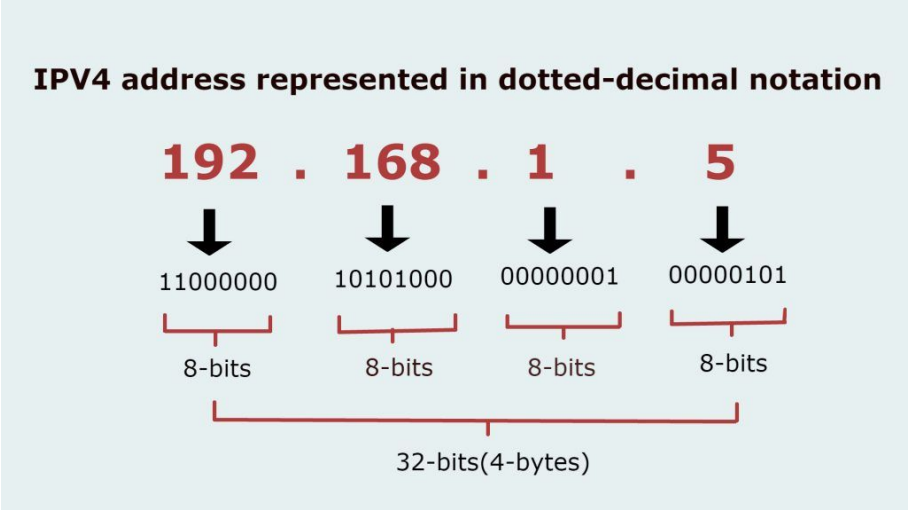


Addressing without a class is more practical and helpful than addressing with a class; it avoids the problem of IP address exhaustion.

IPv4: Classless Addressing

- Assume the classless address: 192.168.1.5 / **24**.
  - The network component has bit count of 24
  - The host portion has a bit count of 8. (32-25)
  - User IP address
    - 11000000.10101000.00000001.00000**101**
  - Subnet Mask (**/24**)
    - **11111111.11111111.11111111**.00000000

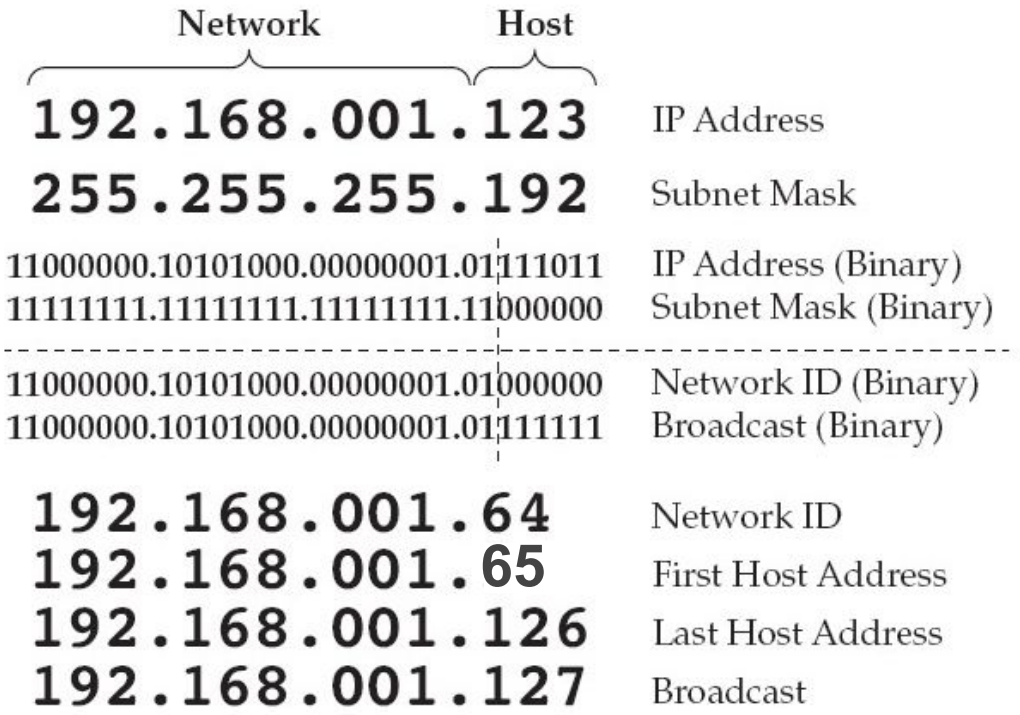
- Not all addresses are available in IPv4
  - Network Address: the lowest address
  - Broadcast Address: the highest address
  - Other special IPs can be reserved by ISP



  - Network Address: 192.168.1.0
  - Broadcast Address: 192.168.1.255
  - User addresses:
    - 192.168.1.1 - 192.168.1.254
    - # of available IPs: 253

IPv4: Classless Addressing

192.168.001.123 / **26**



IPv4: Classless Inter-Domain Routing (CIDR)

CIDR	# of addresses	Usage	Purpose
0.0.0.0/8	16,777,216	Software	For broadcast messages to the current host (source only)
10.0.0.0/8	16,777,216	Private network	Local communications within a private network
100.64.0.0/10	4,194,304	Private network	For communications between a service provider and subscribers when using Network Address Translation
127.0.0.0/8	16,777,216	Host	Loopback address to the local host (no place like 127.0.0.1)
169.254.0.0/16	65,536	Subnet	Link-local addresses between two hosts configured using Automatic Private IP Addressing (APIPA)
172.16.0.0/12	1,048,576	Private network	Local communications within a private network
192.0.0.0/24	256	Private network	For the IANA IPv4 Special Address Registry
192.0.2.0/24	256	Documentation	TEST-NET-1; for use in documentation and examples
192.88.99.0/24	256	Internet	Before deprecation, used by 6to4 anycast

IPv4: Classless Inter-Domain Routing (CIDR)

CIDR	# of addresses	Usage	Purpose
192.168.0.0/16	65,536	Private network	Local communications within a private network
198.18.0.0/15	131,072	Private network	Testing of inter-network communications between two separate subnets
198.51.100.0/24	256	Documentation	TEST-NET-2; for use in documentation and examples
203.0.113.0/24	256	Documentation	TEST-NET-3; for use in documentation and examples
224.0.0.0/4	268,435,456	Internet	Multicast
240.0.0.0/4	268,435,456	Internet	Experimental, reserved for future use
255.255.255.255 /32	1	Subnet	Reserved for the *limited broadcast* destination address

IPv4: Packet Header

	0								1								2								3							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
0	Version				IHL				DSCP						ECN		Total Length															
4	Identification																Flags			Fragment Offset											
8	TTL								Protocol								Checksum															
12	Source																															
16	Destination																															
20	Options																															
24																																
28																																
32																																

IPv4: Packet Header

Field	Name	Description
Version	Version	IP packet version. For IPv4, this is always 4.
IHL	Internet Header Length	Number of 32 bit words in the header. Minimum value is 5. If options are used, value will be greater than 5.
DSCP	Differentiated Service Code Point	Used to provide quality of service for packet, e.g. give low latency service to critical network traffic while providing best-effort service to non-critical traffic.
ECN	Explicit Congestion Notification	Allows end-to-end notification of network congestion without dropping packets. Used only when both endpoints and network support it. Endpoints must agree to use it.
Total Length	Total Length	Total packet length in bytes, including header and data. Minimum value is 20, which is a header, no options and data.
Identification	Identification	Used for uniquely identifying the group of fragments in a single IP datagram.

IPv4: Packet Header

Field	Name	Description
Flags	Flags	Bitfield used to control or identify the fragment.
Fragment offset	Fragment offset	Offset of the fragment relative to the start of the original unfragmented packet. Measured in 8 byte blocks.
TTL	Time To Live	Amount of time the packet has to live. Decremented by one on each routing hop. If it reaches zero, packet is dropped and router sends an ICMP Time Exceeded Message to the sender.

Bit	Description
0	Reserved, must be zero.
1	Do not fragment (DF) packet if set. If fragmentation is required, drop packet.
2	More fragments (MF). For fragmented packets, MF is set except for the last one.

IPv4: Packet Header

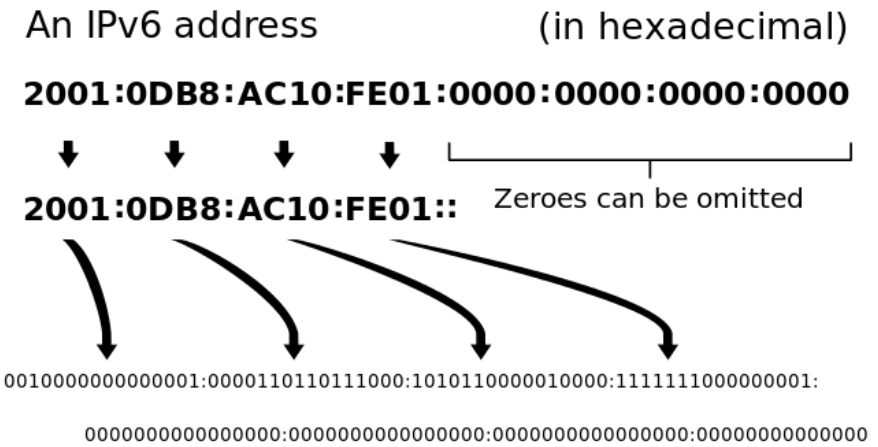
Field	Name	Description
Protocol	Protocol	Used to define the protocol contained in the data portion of the packet. The Internet Assigned Numbers Authority (IANA) maintains the list of protocol numbers. For example, TCP is 6, ICMP is 1, and UDP is 17.
Checksum	Header Checksum	Header checksum computed as the 16 bit one's complement of the one's complement sum of all 16 bit words in the header. When computing the checksum, the value of the checksum field is 0. Each time a router decreases the TTL of a packet, a new checksum is computed.
Source	Source	Source address of IP packet. If using a NAT/PAT setup, source address may be changed.
Destination	Destination	Destination address of IP packet. If using a NAT/PAT setup, destination address may be changed.

10/28: Logistics

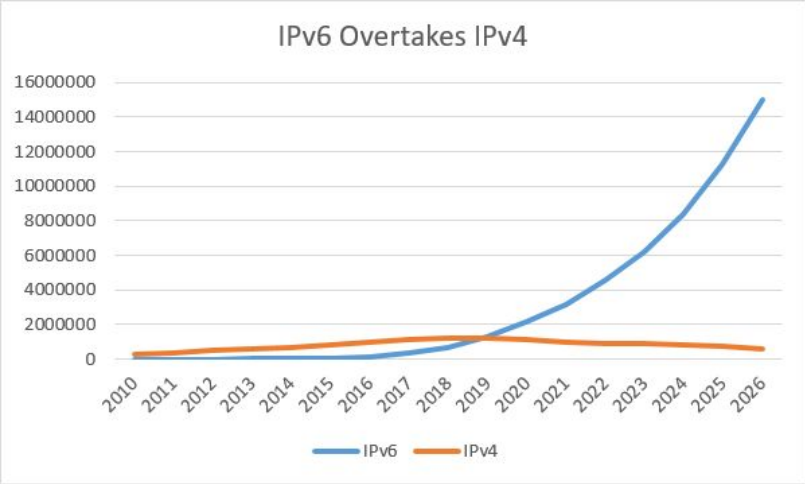
- *Mid-term grades are out*
  - *Mean: 10.14*
  - *Median: 10*
- Lab-4 and quiz-2
  - On the 10/31-11/03 dates in respective labs
- Next week materials
  - Lab-5 and Beagle materials
  - On-device AI contents

IPv6

- Newer version of IP for the growing internet
- Addresses consist of **128 bits** in length and
  - Eight, 16-bit fields, separated by a colon
  - 0:0:0:0:0:0:0:0 – ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  - 2^{128} addresses in total
  - Not all addresses are actually available
- The three types of IPv6 addresses are:
  - Unicast, anycast, and multicast.
  - Does not support broadcast traffic
- IPv6 offers more advanced features than IPv4



IPv6 vs IPv4



https://blogs.infoblox.com/ipv6-coe/ipv6-is-accelerating-as-ipv4-is-nearing-its-peak/

IPv4

Address Size:
32-bit number

Address Format:
Dotted Decimal Notation:
192.168.1.1

Prefix Notation:
255.255.255.0
/24

Number of addresses:
2**32 = 4,294,967,296

IPv6

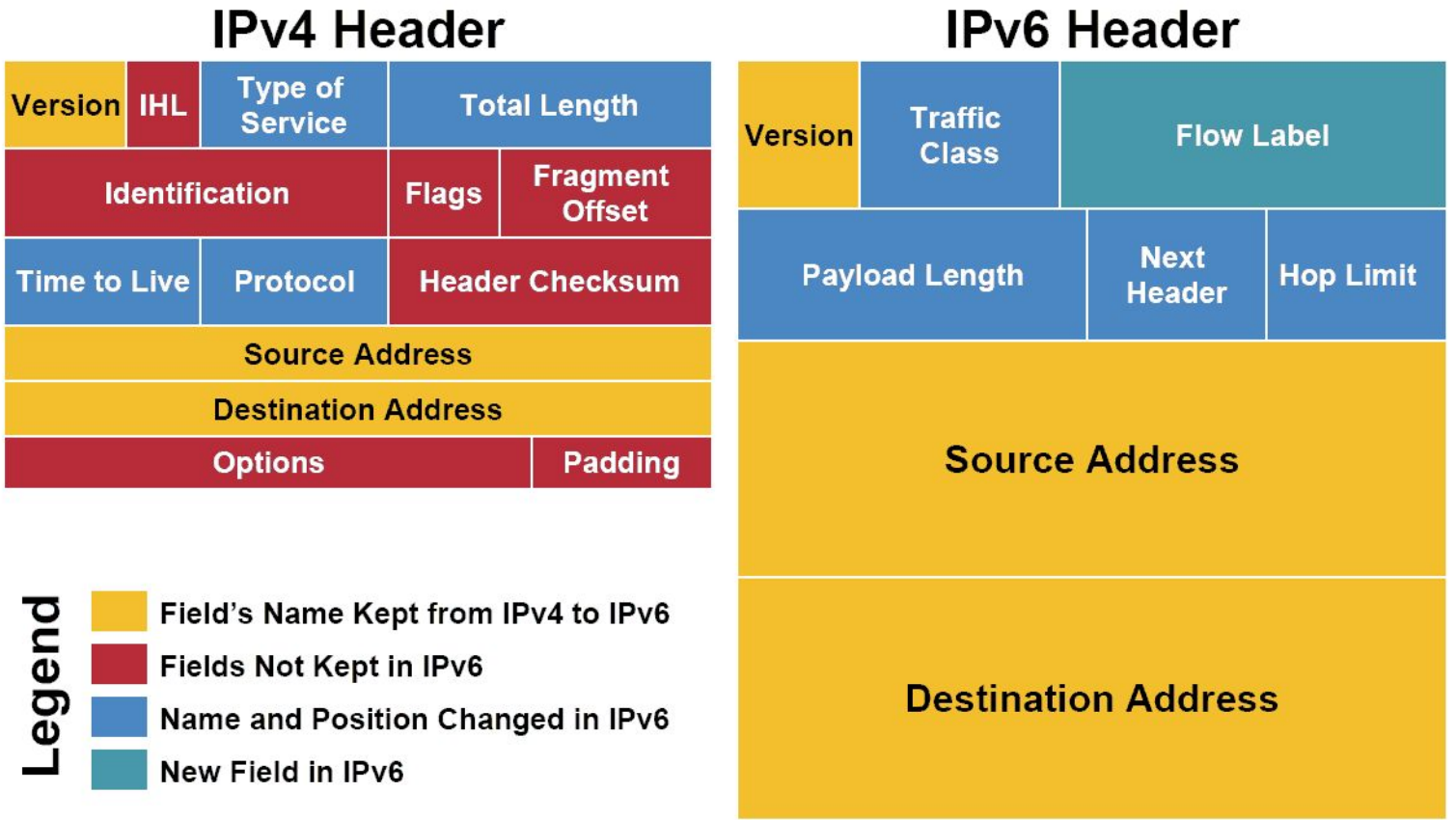
Address Size:
128-bit number

Address Format:
Hexadecimal Notation:
fe80::94db:946e:8d4e:129e

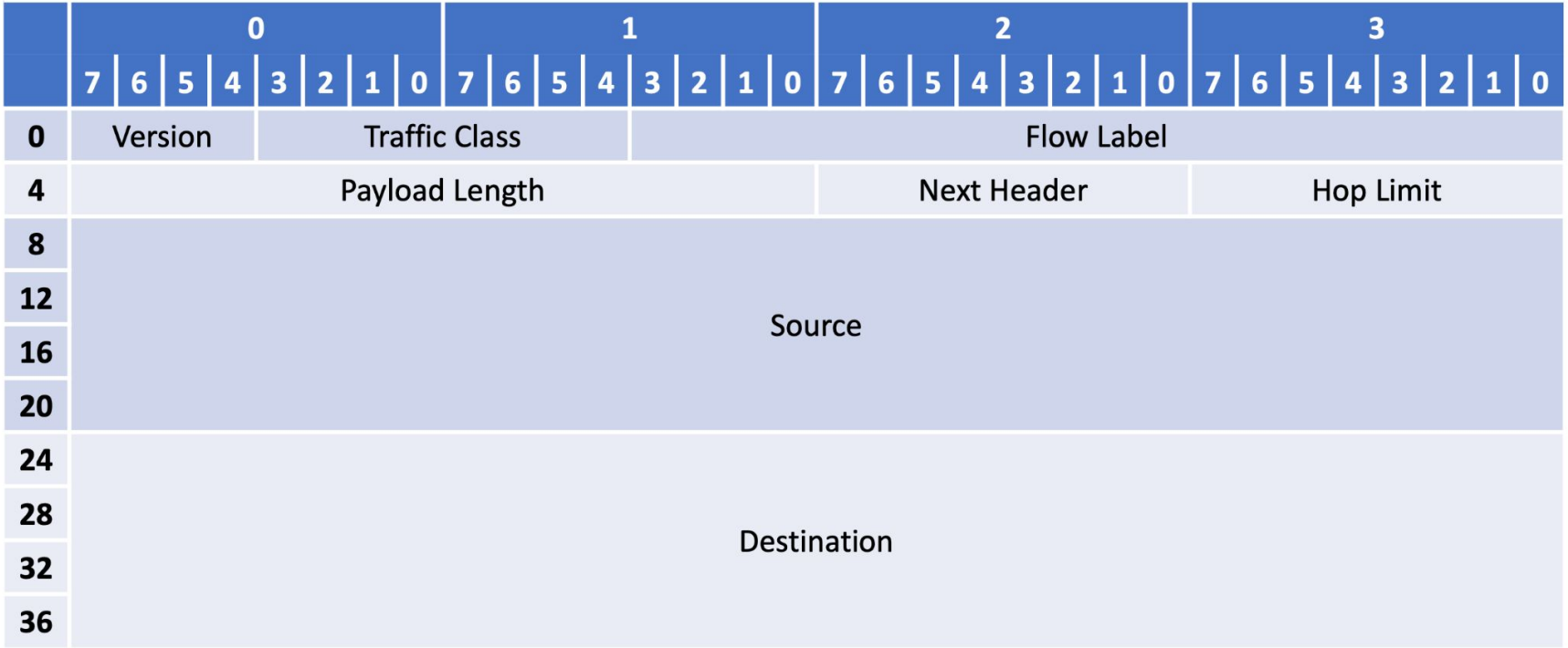
Prefix Notation:
/64

Number of addresses:
2**128 =
340,282,366,920,938,463,463,374,607,
431,768,211,456

IPv6 vs IPv4


IPv4 Header
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
IPv6 Header
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
Legend
Field's Name Kept from IPv4 to IPv6
Fields Not Kept in IPv6
Name and Position Changed in IPv6
New Field in IPv6

IPv6: Packet Header

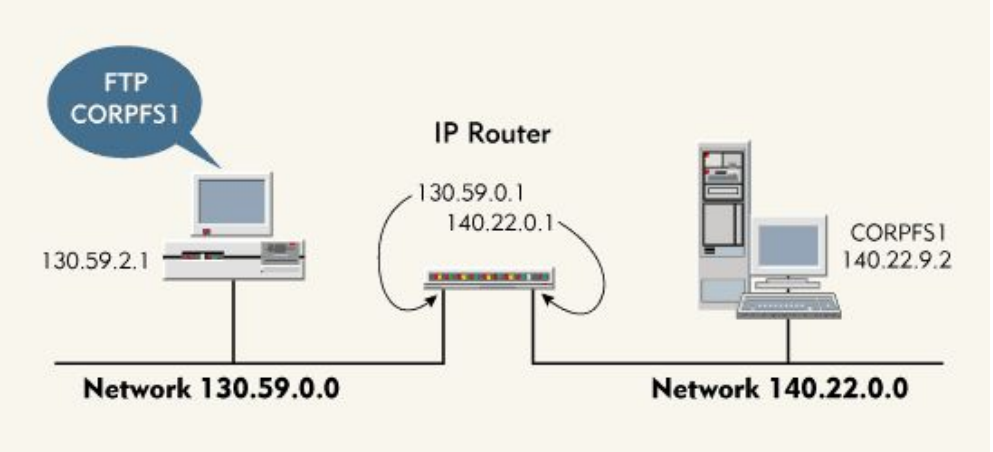


IPv6: Packet Header

Field	Description
Version	IP packet version. For IPv6, this is always 6.
Traffic Class	This field is a combination of the DSCP and ECN fields from IPv4. The 6 most significant bits are for DSCP and the remaining two bits for ECN.
Flow Label	If set, this field is used to hint routers to allow packets to be routed using the same path when multiple outbound paths are available.
Payload Length	The size of the payload in bytes, including headers any extension headers.
Next Header	Specifies the type of header contained in the data portion of the packet. Equivalent to the Protocol field in IPv4.
Hop Limit	Same as modern use of TTL field in IPv4.
Source address	The IPv6 address of the source node.
Destination address	The IPv6 address of the target node.

Limitations Of IP

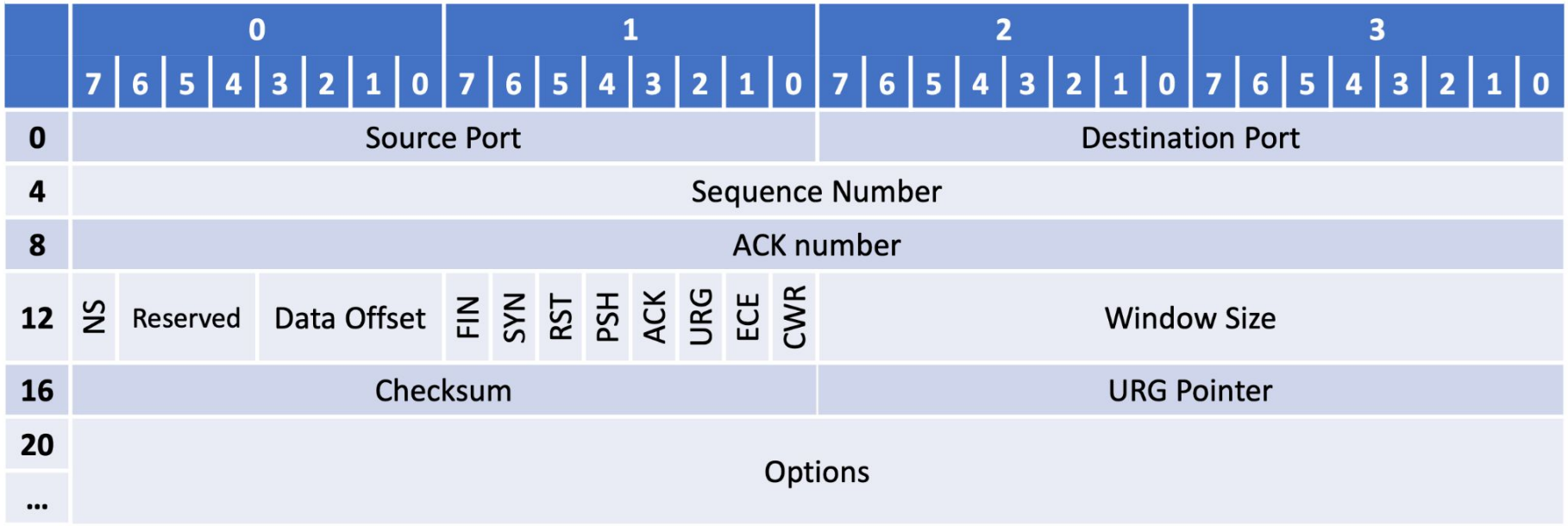
- Does not guarantee
  - Data delivery
  - Integrity of payload
  - Data ordering!!
- Packets can be lost
  - TTL reaches 0, corrupted headers
- *How can this be solved?*
  - *This is the job of the Transport Layer*



TCP: Transmission Control Protocol

- TCP offers a set of communications standard defined by the Internet Engineering Task Force (IETF).
- Designed to send packets across the internet and ensure the successful delivery across networks.
- It is one of the most commonly used protocols within digital network communications.
- TCP organizes data so that it can be transmitted between a server and a client.
- It guarantees the integrity of the data being communicated over a network.
  - Before it transmits data, TCP establishes a connection between a source and its destination, which it ensures remains live until communication begins.
  - It then breaks large amounts of data into smaller packets, while ensuring data integrity is in place throughout the process.
- As a result, high-level protocols that need to transmit data all use TCP Protocol.
  - Examples include: FTP, SSH, Telnet, IMAP, POP, SMTP, HTTP.

TCP: Header


0
1
2
3
7 6 5 4 3 2 1 0 7 6 5 4 3 2 1 0 7 6 5 4 3 2 1 0 7 6 5 4 3 2 1 0
0
Source Port
Destination Port
4
Sequence Number
8
ACK number
12
NS
Reserved
Data Offset
FIN
SYN
RST
PSH
ACK
URG
ECE
CWR
Window Size
16
Checksum
URG Pointer
20
...
Options

TCP: Header

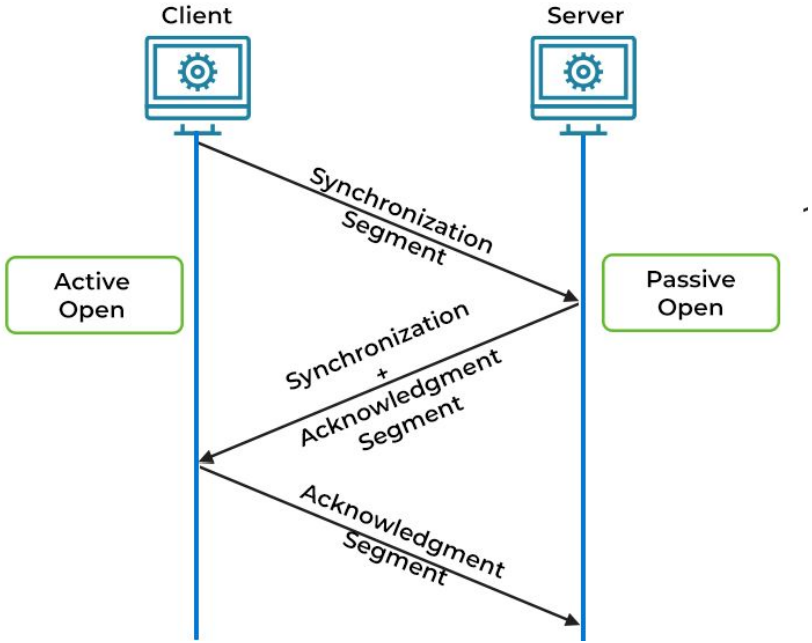
Field	Description
Source Port	Identification of the sending internet socket
Destination Port	Identification of the receiving internet socket
Sequence Number	If the SYN flag is set, this field contains the *initial* sequence number. If the SYN flag is clear, this field contains the *accumulated* sequence number for the session.
ACK Number	If the ACK flag is set, this field contains the *next sequence number that the sender is expecting*. This acknowledges the receipt of all previous bytes.
NS	ECN-nonce, adding concealment protection
Reserved	Should be set to 0.
Data offset	Number of words in the header size, minimum size is 5 words and maximum is 15.
FIN	Indicates last segment from sender.
SYN	Synchronize sequence numbers. Only used in opening a connection.
RST	Reset connection
PSH	Push function to push the buffered data to receiving application.

TCP: Header

Field	Description
ACK	Indicates that the ACK Number field is significant. All segments after SYN should have this field set.
URG	URG Pointer field is valid.
ECE	ECN-Echo: If SYN is set, then the peer is ECN capable. If SYN is clear, indicates network congestion (or possibly impending congestion) to the TCP sender. Flag is set this way if IP packet with Congestion Experienced flag (ECN=11) set in the IP header is was received.
CWR	Congestion Window Reduced. Set by sending host to indicate that it received the TCP segment with ECE flag and has responded with the congestion control mechanism.
Window Size	The size of the receive window specifying the number of window size units (usually in bytes).
Checksum	16-bit checksum in the header, payload, and pseudoheader.
URG Pointer	Urgent Pointer: If URG is set, this field contains an offset from the sequence number indicating the last urgent data byte.
Options	Additional options to the segment.

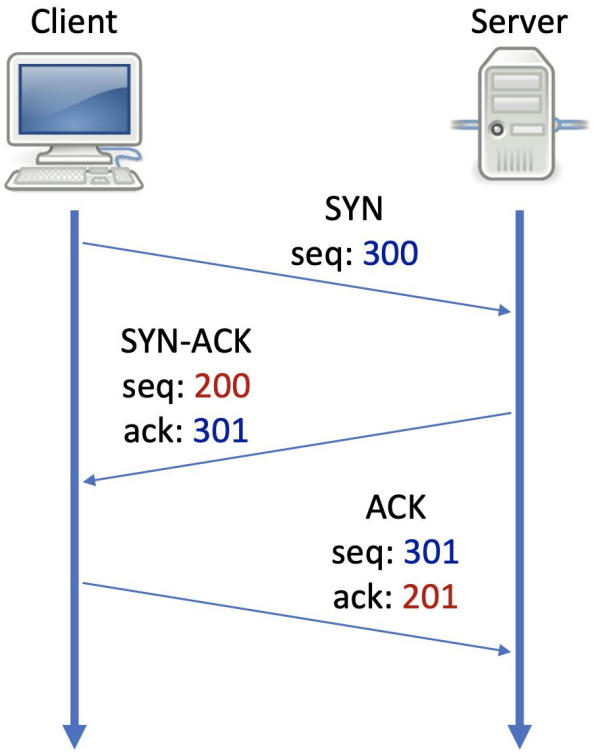
TCP: Workflow

- Stateful system
- Divided into three phases
  - Connection Establishment: three-way handshake
  - Data Transfer: data transfer and congestion control
  - Connection Termination: four-way handshake.
- TCP performs the following actions:
  - Determines how to break application data into packets that networks can deliver
  - Sends/accepts packets to/from the network layer
  - Handles retransmission of dropped or garbled packets, as it's meant to provide error-free data transmission
  - Manages flow control and acknowledges all packets that arrive



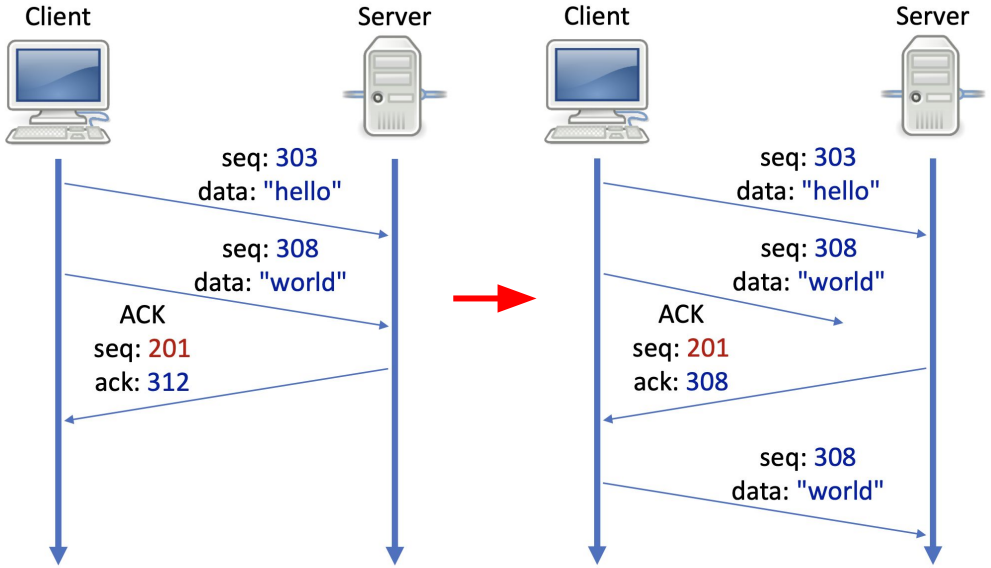
TCP: Connection Establishment

- **Connection Establishment:** three-way handshake
  - Server binds to port (passive open)
  - Client is free to connect to this port
  - Client initiates connection (active open)
- Client sends **`SYN`** segment to server using random segment sequence number ***n***
- Server responds with **`SYN-ACK`** segment, number is set to ***n+1***. Server chooses its own sequence number ***m***.
- Client sends an ACK segment to server, sequence number ***n+1***, and acknowledgement number is ***m+1***.



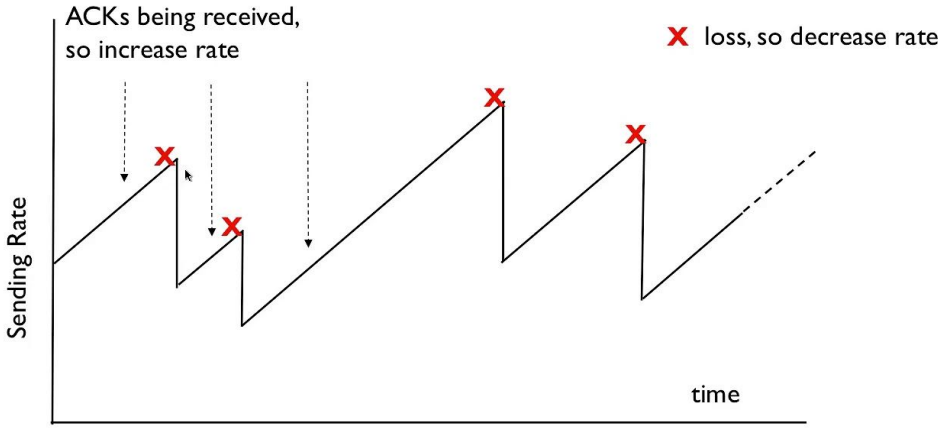
TCP: Data Transfer

- Sender transmits multiple segments with increasing `SYN` numbers
- Receiver replies with `ACK` segments and increasing `SYN` numbers
- `ACK` number given by `SEND_SYN_SEQ` + the highest octet sequence number it has correctly received
- Lost segments are detected by not receiving ACK segment from receiver.
  - Retransmit after timeout.
  - If ACK is lost
    - Sender transmits copy of segment.
    - Receiver ACKs it and ignores it.



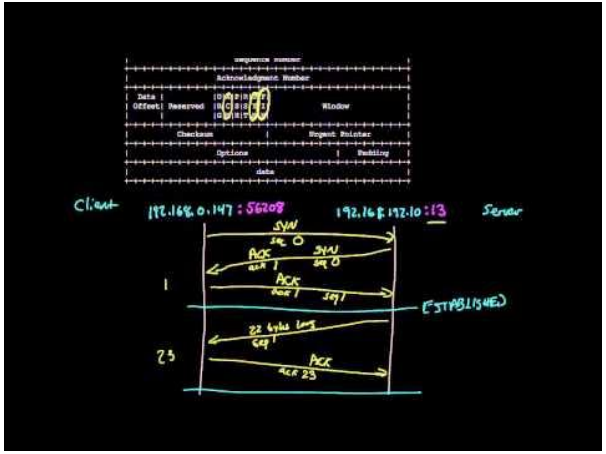
TCP: Congestion Control

- TCP uses a congestion window in the sender side to do congestion avoidance.
- The congestion window indicates the maximum amount of data that can be sent out on a connection without being acknowledged.
- TCP detects congestion when it fails to receive an acknowledgement for a packet within the estimated timeout.
- Four algorithms are currently used
  - Slow Start
  - Congestion Avoidance
  - Fast Retransmit
  - Fast Recovery
- More: wikipedia.org/wiki/TCP_congestion_control

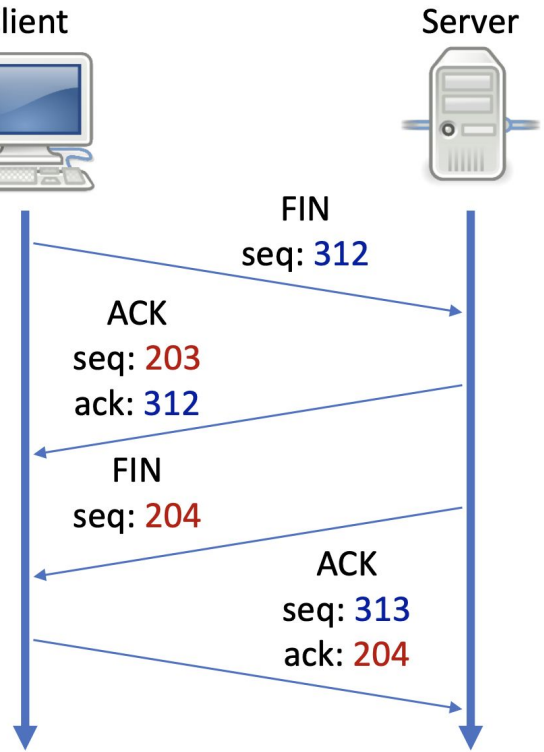


TCP: Connection Termination

- Can be terminated by either endpoint
- Uses four way handshake
  - Endpoint wishing to terminate (A) sends `FIN` segment
  - Other endpoint (B) sends `ACK`
  - Then (B) sends own `FIN` segment
  - Finally (A) replies with `ACK` segment



https://youtu.be/F27PLin3TV0

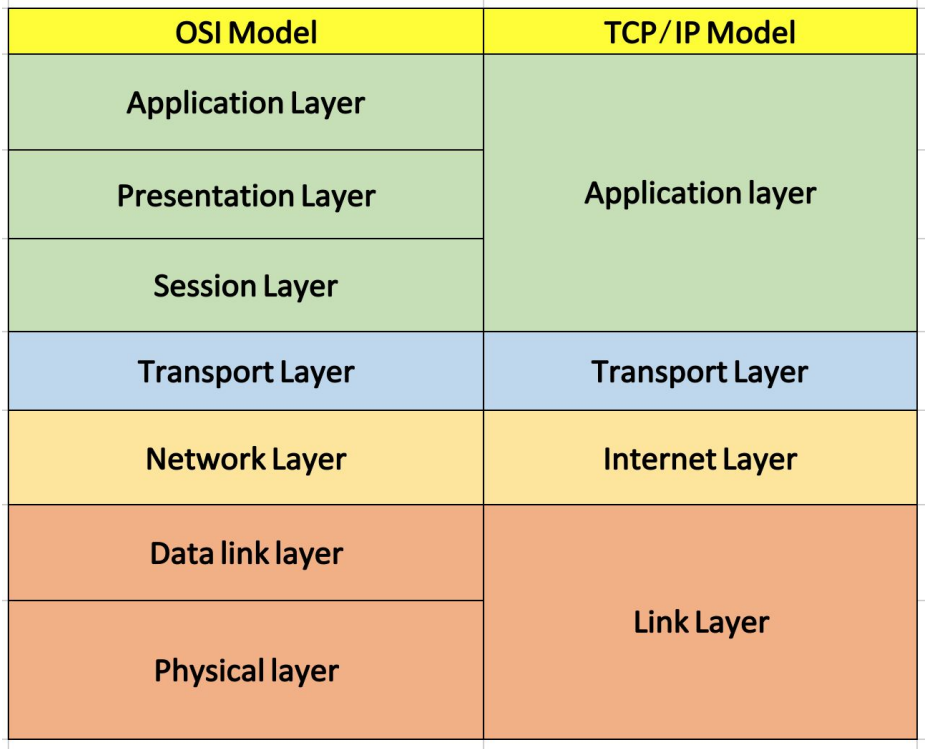


TCP: Common Internet Sockets

Port	Protocol	Description
20	FTP	Active mode data transmission in File Transfer Protocol.
21	FTP	Standard listening port in FTP, passive mode data transmission.
22	SSH	Secure Shell protocol.
23	Telnet	Telnet remote login.
25	SMTP	Plaintext Simple Mail Transfer Protocol.
80	HTTP	Plaintext Hypertext Transfer Protocol (unencrypted web servers)
110	POP	Plaintext Post Office Protocol (unencrypted read access to e-mail servers)
143	IMAP	Plaintext Internet Message Access Protocol
194	IRC	Plaintext Internet Relay Chat
443	HTTPS	Secure Hypertext Transfer Protocol (encrypted web servers)

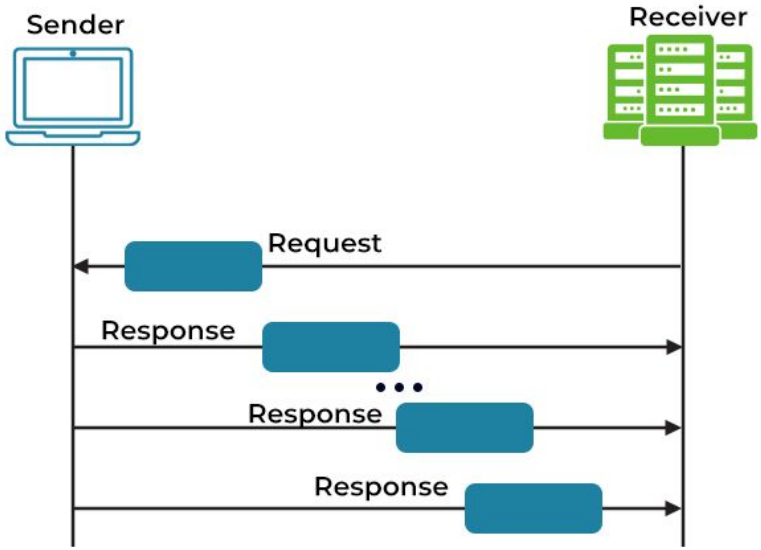
TCP/IP Model

- TCP/IP model is the default method of data communication on the Internet.
  - TCP/IP divides communication tasks into layers that keep the process standardized, without hardware and software providers doing the management themselves.
  - The data packets pass through four layers before they are received by the destination device, then TCP/IP goes through the layers in reverse order to put the message back into its original format.
- Four comprehensive layers
  - Application (OSI layer 7, 6, 5)
  - Transport (OSI layer 4)
  - Network layer (OSI layer 3)
  - Physical layer (OSI layer 1, 2)



UDP: User Datagram Protocol

- A connectionless communication model with little or no overhead over two nodes
- Runs exclusively over the IP protocol
  - Hence the common UDP/IP name
- No client-server model
  - No handshaking dialog, no guarantee delivery
  - No ordering, no duplicate detection
- Application is directly exposed to any unreliability on the underlying network
- Examples include: DNS, VoIP, TFTP, NTP



UDP: Header

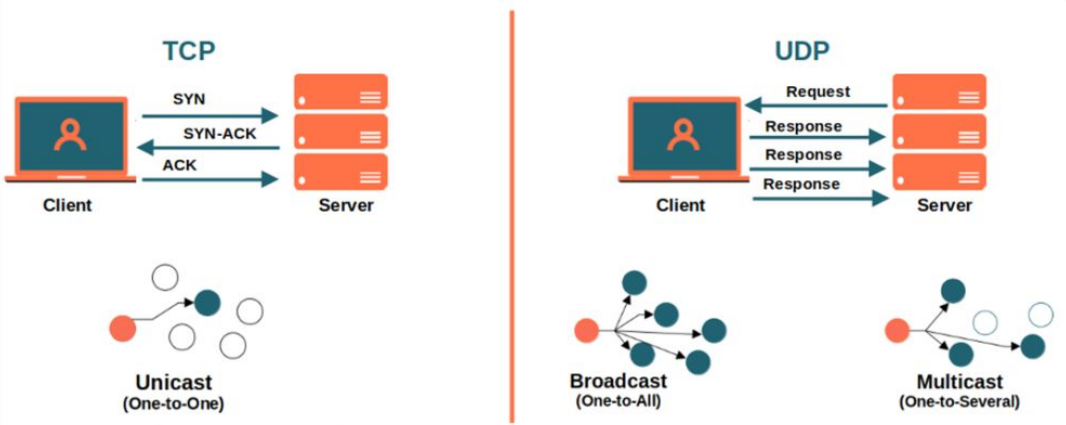
	0								1								2								3							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
0	Source Port																Destination Port															
4	Length																Checksum															

Field	Description
Source Port	Identification of the sending internet socket, when meaningful. Assumed to be the port to reply to if needed. If not used, this field should be set to 0. If the source is the client, the port number is likely to be an ephemeral port (a port that is only utilized for the current UDP session).
Destination Port	Identification of the receiving internet socket. This field is required.
Length	The number of bytes in the UDP header and data. The minimum length is 8 bytes (the size of the UDP header).
Checksum	Contains a checksum of the header and the accompanying data. The field is optional in IPv4 and set to zero if unused. The field is mandatory in IPv6.

UDP: Common Internet Sockets

Port	Protocol	Description
53	DNS	Domain Name System protocol (resolve hostnames)
67	BOOTP	Bootstrap Protocol server, also used by DHCP (Dynamic Host Configuration Protocol)
68	BOOOTP	Bootstrap Protocol client, also used by DHCP
69	TFTP	Trivial File Transfer Protocol, used in some bootloaders to download firmware images
123	NTP	Network Time Protocol, network latency aware clock synchronization protocol
161	SNMP	Simple Network Management Protocol, used for management of devices in a network

TCP vs UDP



- Connected
- State Memory
- Byte Stream
- Ordered Data Delivery
- Reliable
- Error Free
- Handshake
- Flow Control
- Relatively Slow
- Point to Point
- Security: SSL/TLS

- Connectionless
- Stateless
- Packet/Datagram
- No Sequence Guarantee
- Lossy
- Error Packets Discarded
- No Handshake
- No Flow Control
- Relatively Fast
- Supports Multicast
- Security: DTLS

TCP vs UDP: Summary

"Hi, I'd like to hear a TCP joke."
"Hello, would you like to hear a TCP joke?"
"Yes, I'd like to hear a TCP joke."
"OK, I'll tell you a TCP joke."
"Ok, I will hear a TCP joke."
"Are you ready to hear a TCP joke?"
"Yes, I am ready to hear a TCP joke."
"Ok, I am about to send the TCP joke. It will last 10 seconds, it has two characters, it does not have a setting, it ends with a punchline."
"Ok, I am ready to get your TCP joke that will last 10 seconds, has two characters, does not have an explicit setting, and ends with a punchline."
"I'm sorry, your connection has timed out. ... Hello, would you like to hear a TCP joke?"