OSI Model Overview

CompTIA Network+ (N10-007)

OSI Model (Open Systems Interconnection)

- Developed in 1977 by the International Organization for Standardization (ISO)
- Called the OSI model or OSI stack
- Consists of 7 layers
- Useful in troubleshooting networks
- Serves as a reference model in networks

Purpose of Reference Model

- Categorize functions of the network into particular layer(s)
- Compare technologies across different manufacturers
- By understanding its functions you can understand how best to communicate with that device

OSI Model Layers

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

OSI Model Layers

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

***P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way!*

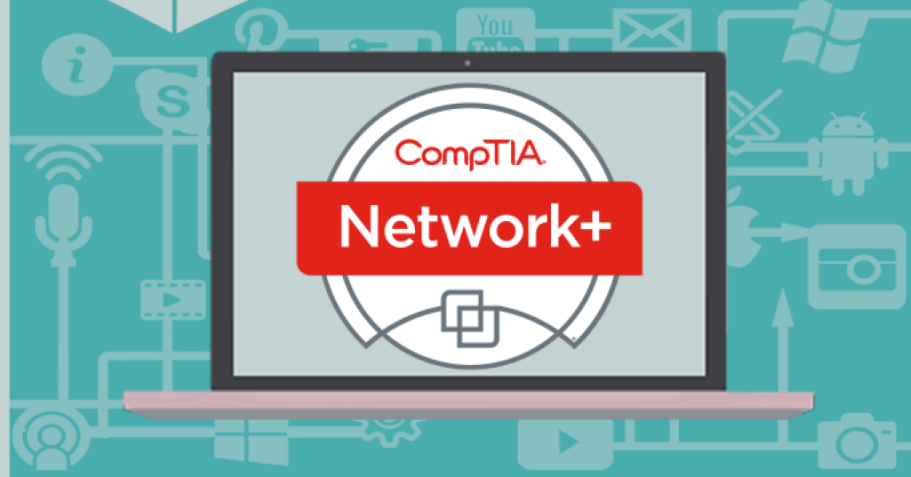
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

Data Types in the OSI Model

7	Application	7	Data
6	Presentation	6	
5	Session	5	
4	Transport	4	Segments
3	Network	3	Packets
2	Data Link	2	Frames
1	Physical	1	Bits

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

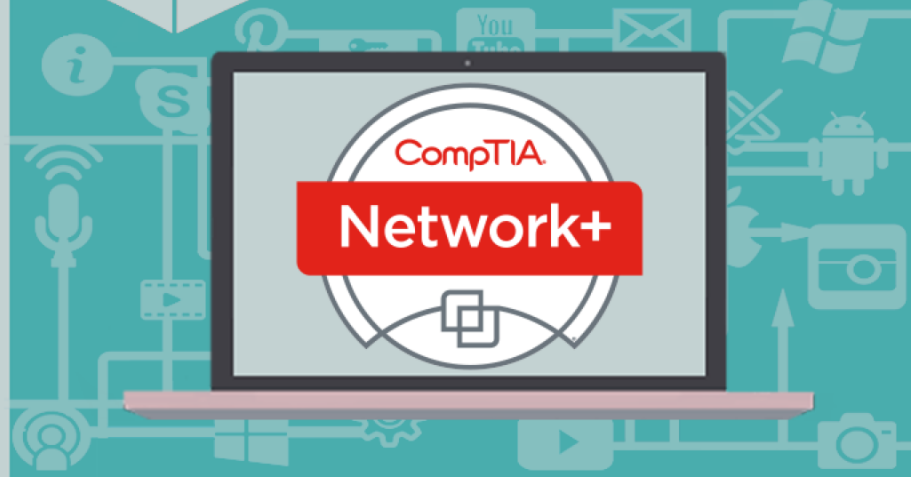


Data Types in the OSI Model

7	Application	7 Data
6	Presentation	6
5	Session	5
4	Transport	4 Segments
3	Network	3 Packets
2	Data Link	2 Frames
1	Physical	1 Bits

***D**on't **S**ome **P**eople **F**ear **B**irthdays?*

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

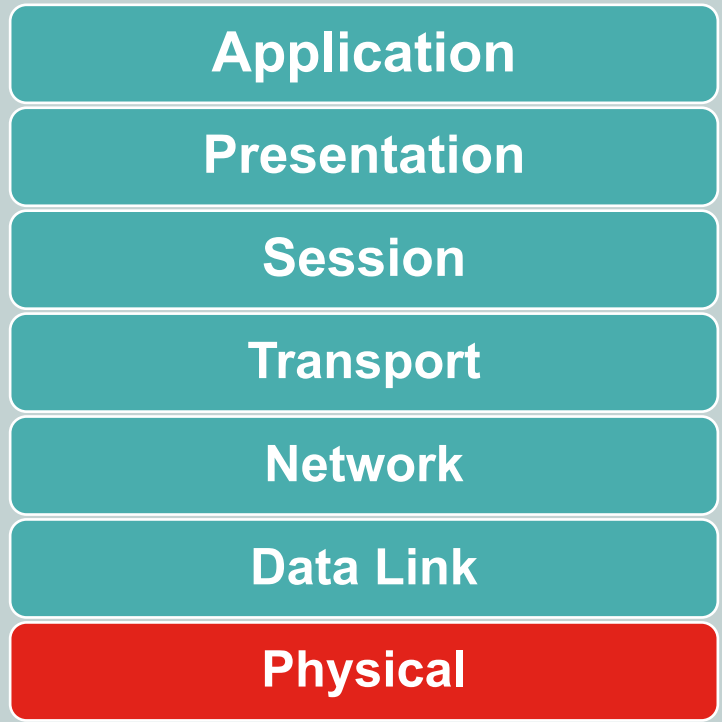


Layer 1 (Physical)

CompTIA Network+ (N10-007)

Physical Layer (Layer 1)

- Transmission of *bits* across the network
- Physical and electrical characteristics
- Characteristics:
  - How bits are represented on the medium
  - Wiring standards for connectors and jacks
  - Physical topology
  - Synchronizing bits
  - Bandwidth usage
  - Multiplexing strategy

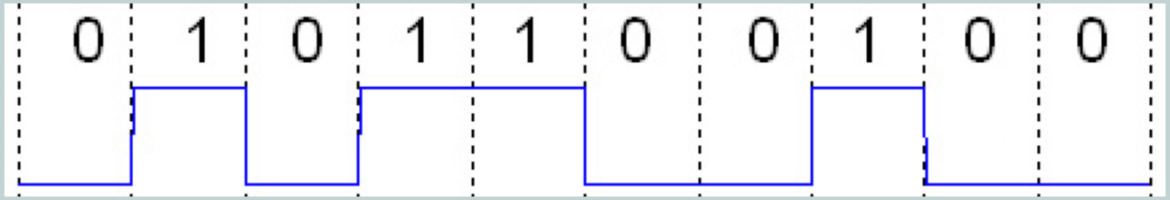


How are bits represented on the medium?

- Electrical voltage (copper wiring) or light (fiber optics) represent 1's and 0's (bits)

- Current State
  - If 0 volts, then 0 is represented
  - If +/- 5 volts, then 1 is represented

- Transition Modulation
  - If it changed during the clock cycle, then a 1 is represented otherwise a 0



How are the cables wired?

- TIA/EIA-568-B is standard wiring for RJ-45 cables and ports
- Crossover cables use T-568A and T-568B
- Straight-thru cables typically use T-568B on both ends, but could use T-568A on both

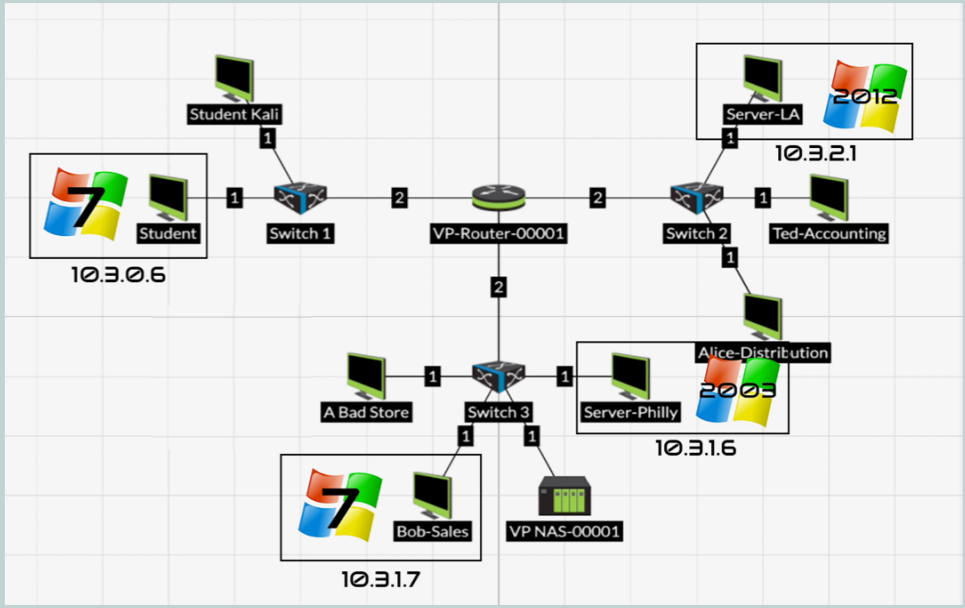
Wiring standards will be address in-depth in the Ethernet module

Pin	Color
1	white/orange
2	orange
3	white/green
4	blue
5	white/blue
6	green
7	white/brown
8	brown

How are the cables connected?

- Layer 1 devices view networks from a physical topology perspective

- Includes:
  - Bus
  - Ring
  - Star
  - Hub-and-Spoke
  - Full Mesh
  - Partial Mesh



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

How is communication synchronized?

- Asynchronous
  - Uses start bits and stop bits to indicate when transmissions occur from sender to receiver
- Synchronous
  - Uses a reference clock to coordinate the transmissions by both sender and receiver

How is bandwidth utilized?

- Broadband
  - Divides bandwidth into separate channels
  - Example:
    - Cable TV

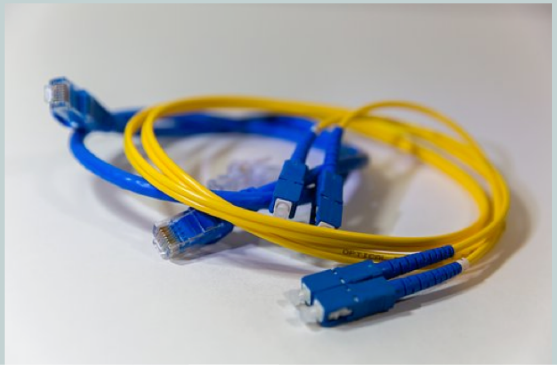
- Baseband
  - Uses all available frequency on a medium (cable) to transmit data and uses a reference clock to coordinate the transmissions by both sender and receiver
  - Example:
    - Ethernet

How can we get more out of a limited network?

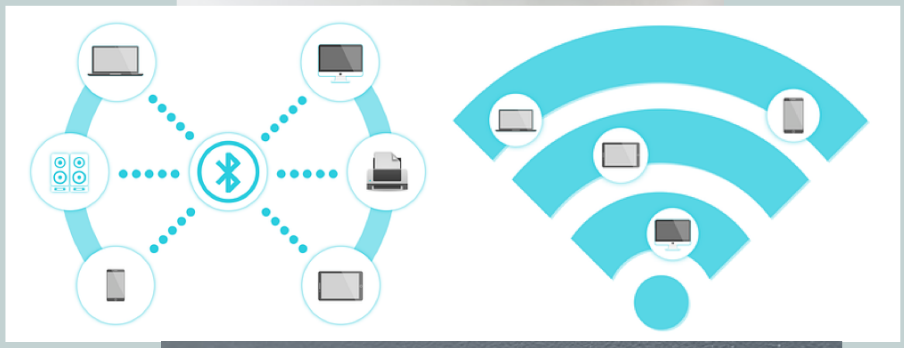
- Time-Division Multiplexing (TDM)
  - Each session takes turns, using time slots, to share the medium between all users
- Statistical Time-Division Multiplexing (StatTDM)
  - More efficient version of TDM, it dynamically allocates time slots on an as-needed basis instead of statically assigning
- Frequency-Division Multiplexing (FDM):
  - Medium is divided into various channels based on frequencies and each session is transmitted over a different channel
    - Broadband

Examples at Layer 1

- Cables
  - Ethernet
  - Fiber optic



- Radio frequencies
  - Wi-Fi
  - Bluetooth



- Infrastructure devices
  - Hubs
  - Wireless Access Points
  - Media Converters

Layer 2 (Data Link)

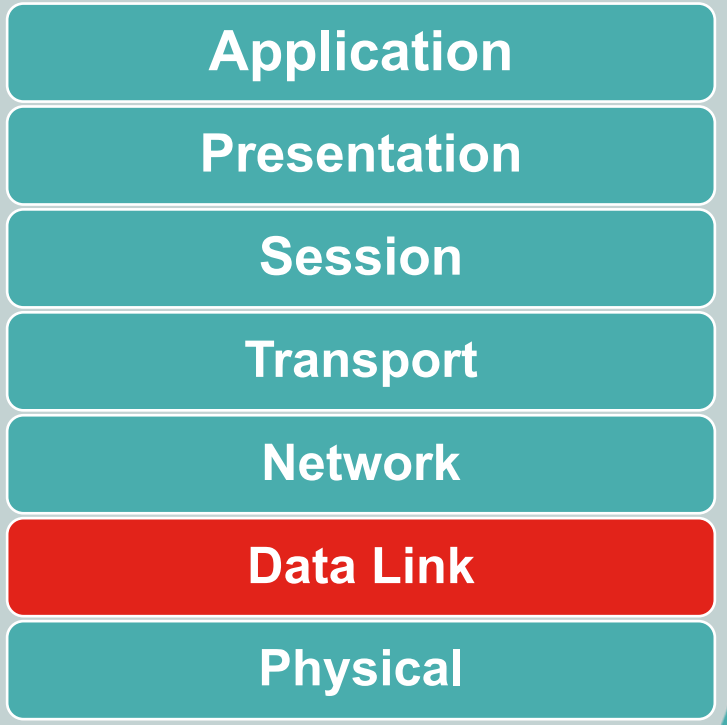
CompTIA Network+ (N10-007)

Data Link Layer (Layer 2)

- Packages data into frames and transmitting those frames on the network, performing error detection/correction, and uniquely identifying network devices with an address (MAC), and flow control

- MAC
  - Physical addressing
  - Logical topology
  - Method of Transmission

- LLC
  - Connection services
  - Synchronizing transmissions



Media Access Control (MAC)

- Physical addressing — 3A:34:65:D2:51:F1
  - Uses 48-bit address assigned to a network interface card (NIC) by manufacturer
  - First 24-bits is the vendor code
  - Second 24-bits is a unique value
- Logical topology
  - Layer 2 devices view networks logically
    - Ring, bus, star, mesh, hub-and-spoke, ...
- Method of transmission
  - Many devices are interconnected
  - Determines whose turn it is to transmit to prevent interference with other devices

Logical Link Control (LLC)

- Provides connection services
- Acknowledgement of receipt of a message
- Flow control
  - Limits amount of data sender can send at one time to keep receiver from becoming overwhelmed
- Error control
  - Allows receiver to let sender know when an expected data frame wasn't received or was corrupted by using a checksum

How is communication synchronized?

- Isochronous
  - Network devices use a common reference clock source and create time slots for transmission
  - Less overhead than synchronous or asynchronous
- Synchronous
  - Network devices agree on clocking method to indicate beginning and end of frames
  - Uses control characters or separate timing channel
- Asynchronous
  - Network devices reference their own internal clocks and use start/stop bits

Examples at Layer 2

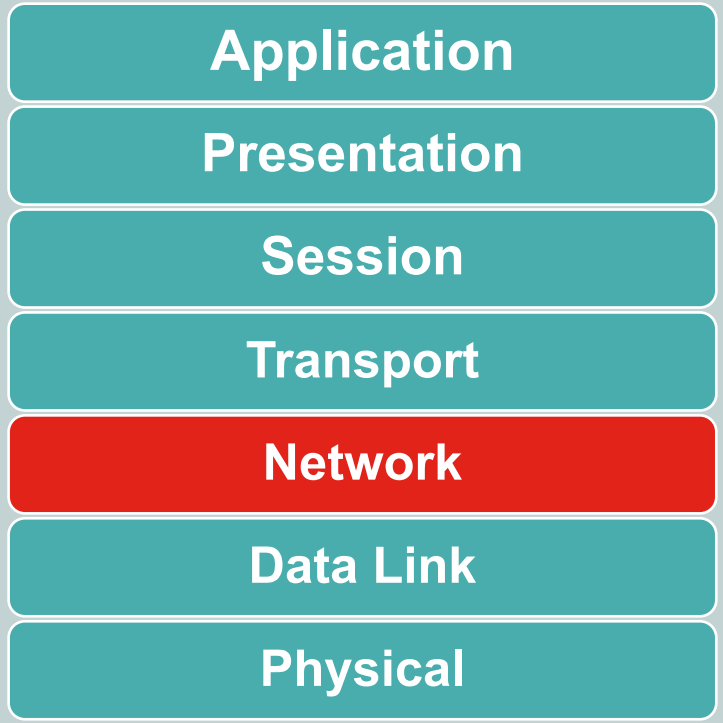
- Network Interface Cards (NIC)
- Bridges
- Switches

Layer 3 (Network)

CompTIA Network+ (N10-007)

Network Layer (Layer 3)

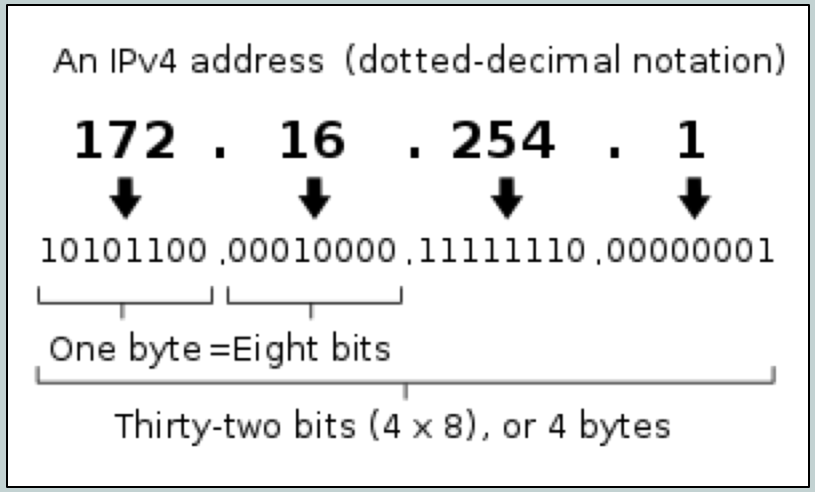
- Forwards traffic (routing) with logical address
  - Example: IP Address (IPv4 or IPv6)
- Logical addressing
- Switching
- Route discovery and selection
- Connection services
- Bandwidth usage
- Multiplexing strategy



Logical Address

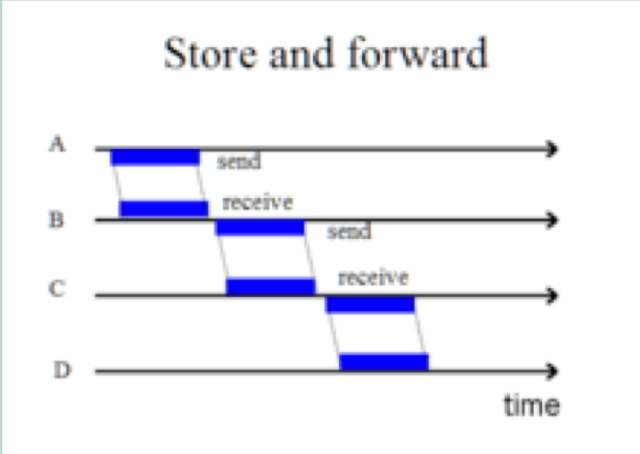
- Numerous routed protocols were used for logical addressing over the years:
  - AppleTalk
  - Internetwork Packet Exchange (IPX)
  - Internet Protocol (IP)

- Only Internet Protocol (IP) remains dominant
  - IP v4
  - IP v6



How should data be forwarded or routed?

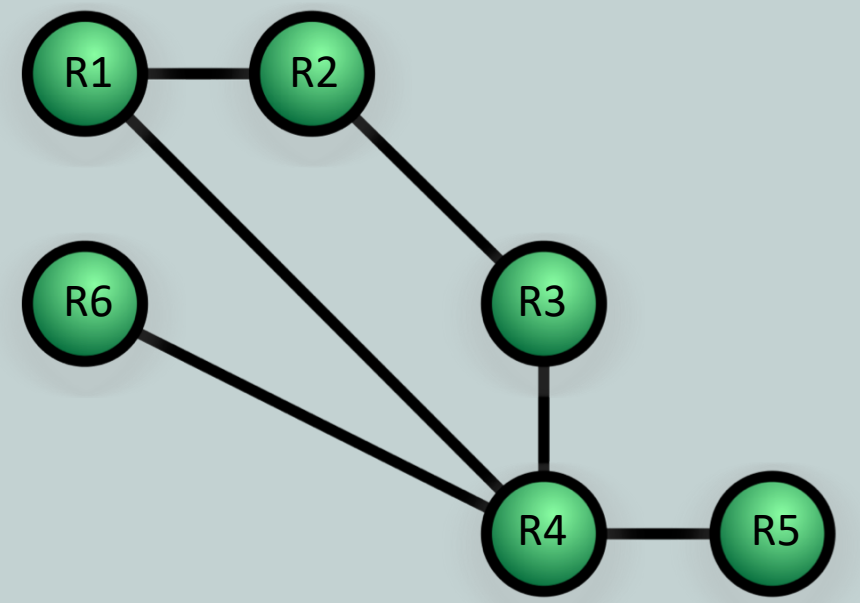
- Packet switching (known as *routing*)
  - Data is divided into packets and forwarded
- Circuit switching
  - Dedicated communication link is established between two devices
- Message switching
  - Data is divided into messages, similar to packet switching, except these messages may be stored then forwarded



Route Discovery and Selection

- Routers maintain a routing table to understand how to forward a packet based on destination IP address

- Manually configured as a static route or dynamically through a routing protocol
  - RIP
  - OSPF
  - EIGRP



Connection Services

- Layer 3 augment Layer 2 to improve reliability
- Flow control
  - Prevents sender from sending data faster than receiver can get it
- Packet reordering
  - Allows packets to be sent over multiple links and across multiple routes for faster service

Internet Control Message Protocol (ICMP)

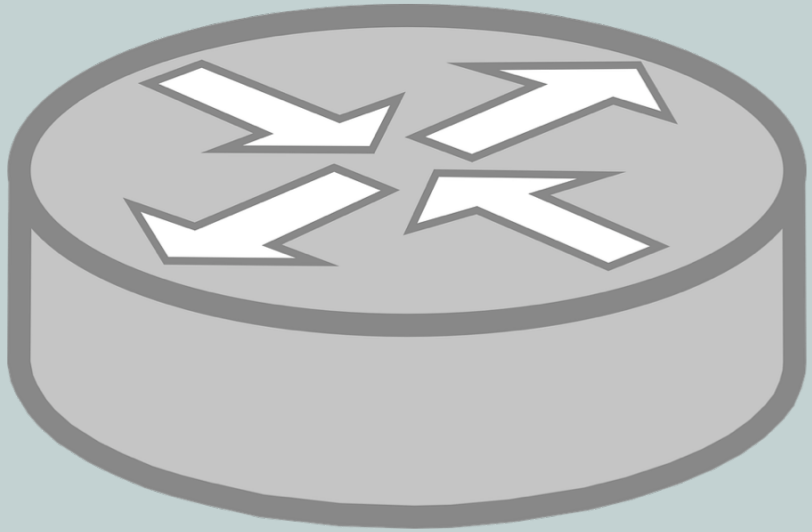
- Used to send error messages and operational information about an IP destination
- Not regularly used by end-user applications
- Used in troubleshooting (*ping* and *traceroute)*

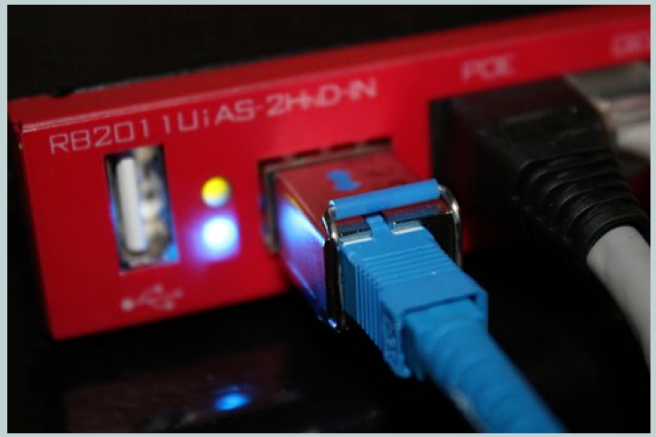
```
$ ping -c 5 www.example.com
PING www.example.com (93.184.216.34): 56 data bytes
64 bytes from 93.184.216.34: icmp_seq=0 ttl=56 time=11.632 ms
64 bytes from 93.184.216.34: icmp_seq=1 ttl=56 time=11.726 ms
64 bytes from 93.184.216.34: icmp_seq=2 ttl=56 time=10.683 ms
64 bytes from 93.184.216.34: icmp_seq=3 ttl=56 time=9.674 ms
64 bytes from 93.184.216.34: icmp_seq=4 ttl=56 time=11.127 ms

--- www.example.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 9.674/10.968/11.726/0.748 ms
```

Examples at Layer 3

- Routers
- Multilayer switches
- IPv4 protocol
- IPv6 protocol
- Internet Control Message Protocol (ICMP)



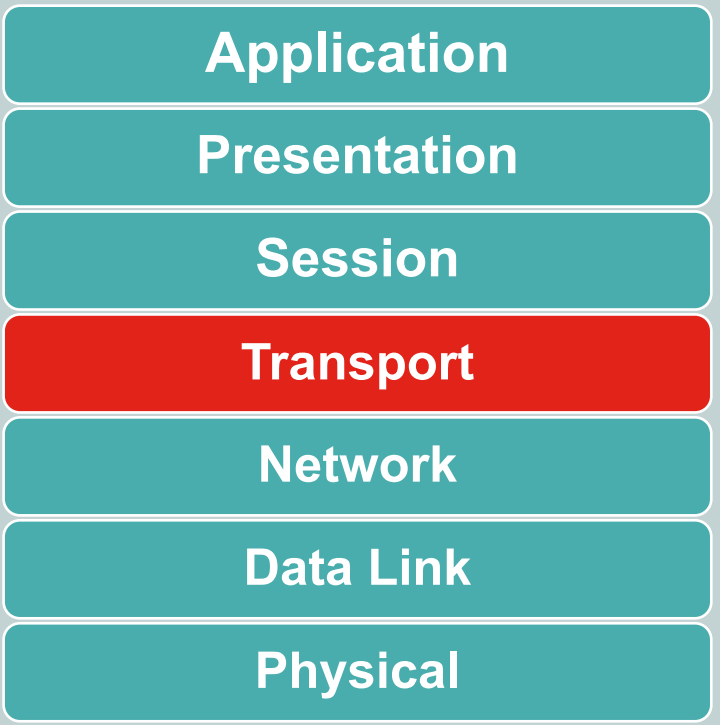


Layer 4 (Transport)

CompTIA Network+ (N10-007)

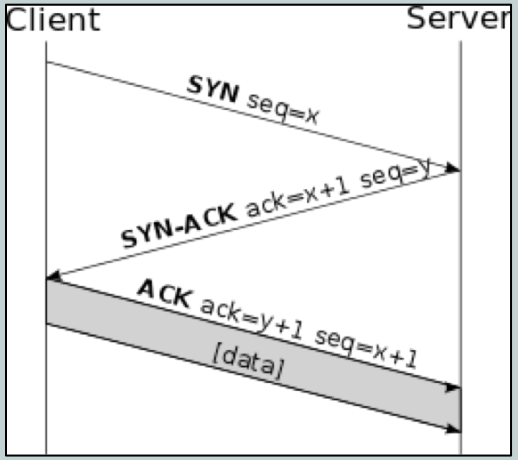
Transport Layer (Layer 4)

- Dividing line between upper and lower layers of the OSI model
- Data is sent as segments
- TCP/UDP
- Windowing
- Buffering



TCP (Transmission Control Protocol)

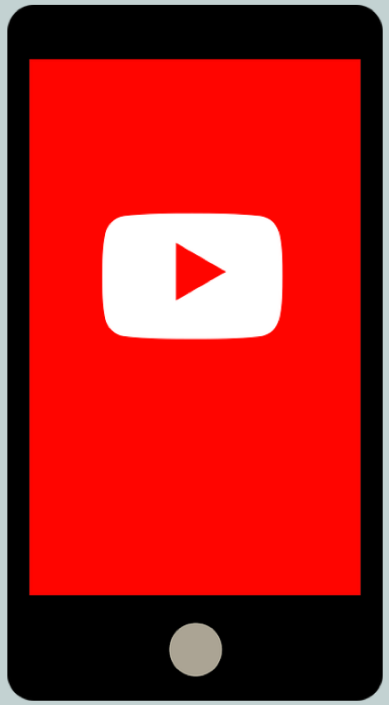
- Connection-oriented protocol



- Reliable transport of segments
  - If segment is dropped, protocol detects it and resends segment
- Acknowledgements received for successful communications
- Used for all network data that needs to be assured to get to its destination

UDP
(User Datagram Protocol)

- Connectionless protocol
- Unreliable transport of segments
  - If dropped, sender is unaware
- No retransmission
- Good for audio/video streaming
- Lower overhead for increased performance



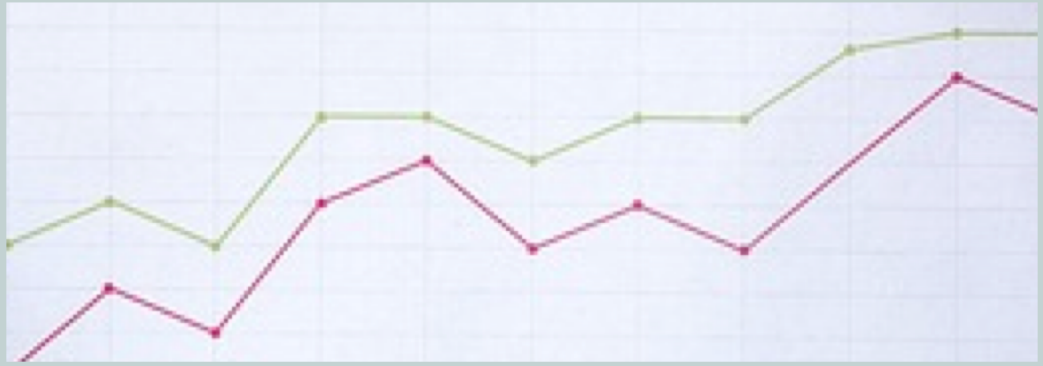
TCP vs UDP

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

Windowing

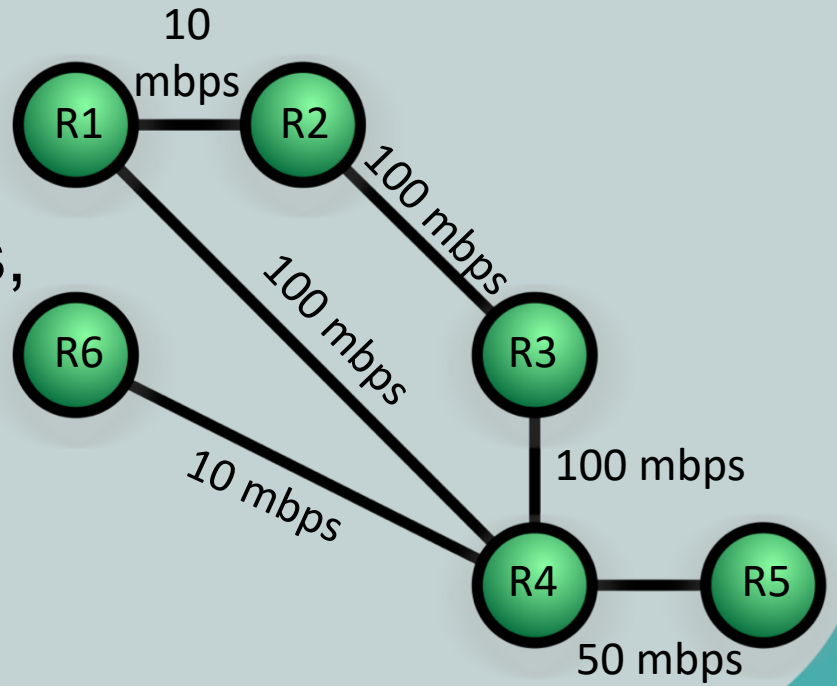
- Allows the clients to adjust the amount of data sent in each segment

- Continually adjusts to send more or less data per segment transmitted
  - Adjusts lower as number of retransmissions occur
  - Adjusts upwards as retransmissions are eliminated



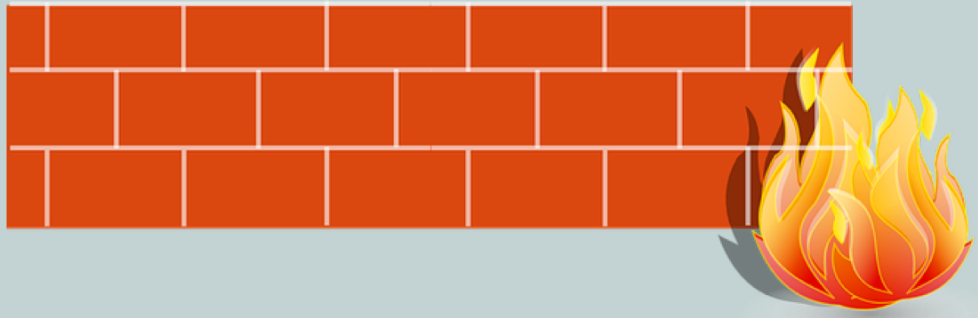
Buffering

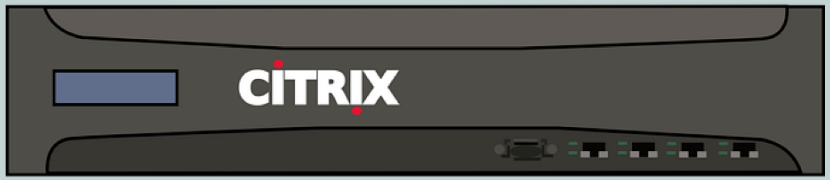
- Devices, such as routers, allocate memory to store segments if bandwidth isn't readily available
- When available, it transmits the contents of the buffer
- If the buffer overflows, segments will be dropped



Examples at Layer 4

- TCP
- UDP
- WAN Accelerators
- Load Balancers
- Firewalls



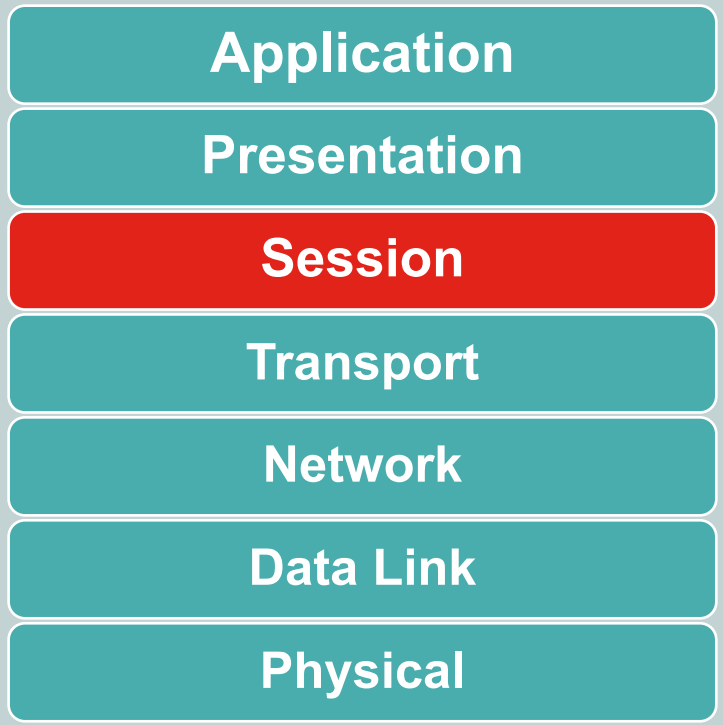


Layer 5 (Session)

CompTIA Network+ (N10-007)

Session Layer (Layer 5)

- Think of a session as a conversation that must be kept separate from others to prevent intermingling of the data
- Setting up sessions
- Maintaining sessions
- Tearing down sessions



Setting up a Session

- Check user credentials
- Assign numbers to session to identify them
- Negotiate services needed for session
- Negotiate who begins sending data

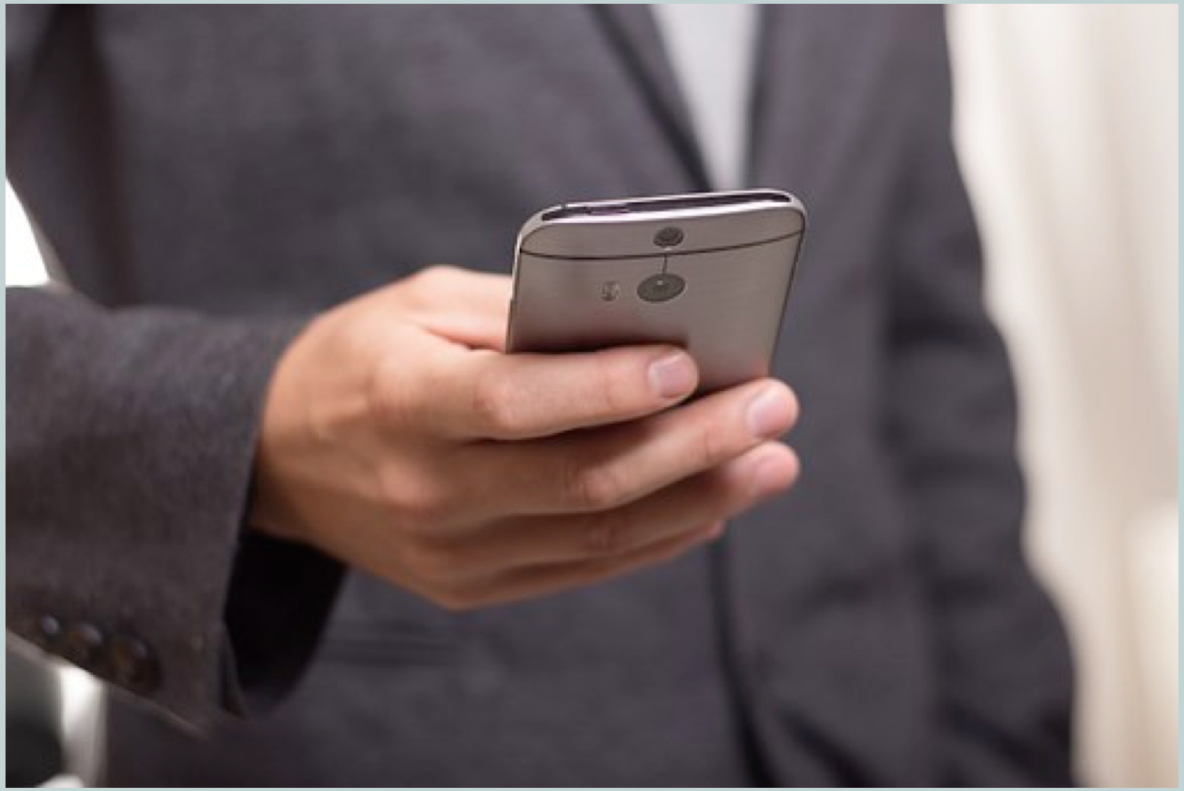
Maintaining a Session

- Transfer the data
- Reestablish a disconnected session
- Acknowledging receipt of data

Tearing Down a Session

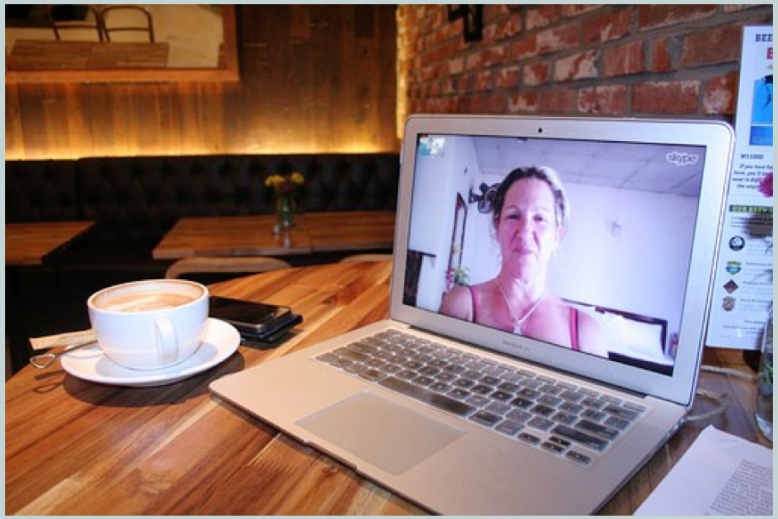
- Due to mutual agreement
  - After the transfer is done

- Due to other party disconnecting



Examples at Layer 5

- H.323
  - Used to setup, maintain, and tear down a voice/video connection
- NetBIOS
  - Used by computers to share files over a network



Layer 6 (Presentation)

CompTIA Network+ (N10-007)

Presentation Layer (Layer 6)

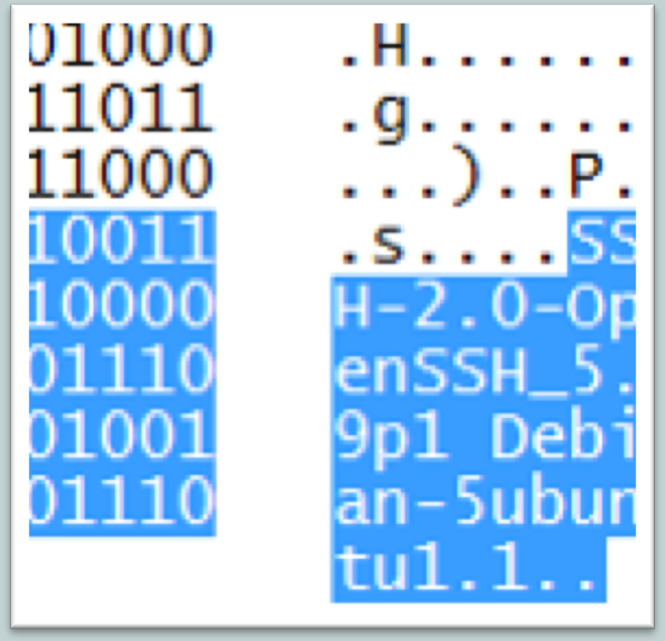
- Responsible for formatting the data exchanged and securing that data with proper encryption

- Functions
  - Data formatting
  - Encryption

Application
Presentation
Session
Transport
Network
Data Link
Physical

Data Formatting

- Formats data for proper compatibility between devices
  - ASCII
  - GIF
  - JPG



- Ensures data is readable by receiving system
- Provides proper data structures
- Negotiates data transfer syntax for the Application Layer (Layer 7)

Encryption

- Used to scramble the data in transit to keep it secure from prying eyes
- Provides confidentiality of data
- Example:
  - TLS to secure data between your PC and website

Examples at Layer 6

- HTML, XML, PHP, JavaScript, …
- ASCII, EBCDIC, UNICODE, …
- GIF, JPG, TIF, SVG, PNG, …
- MPG, MOV, …
- TLS, SSL, …

Layer 7 (Application)

CompTIA Network+ (N10-007)

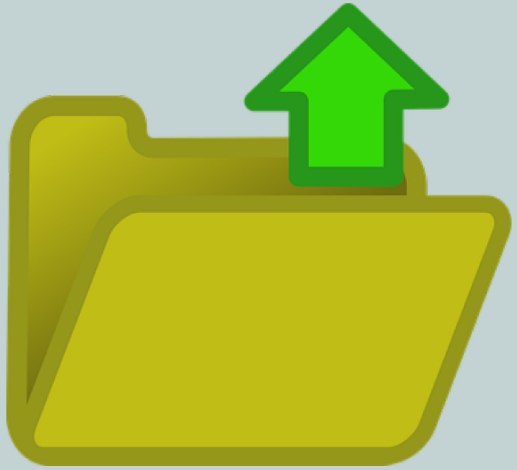
Application Layer (Layer 7)

- Provides application level services
  - Not Microsoft Word or Notepad
- Layer where the users communicate with the computer
- Functions:
  - Application services
  - Service advertisement

Application
Presentation
Session
Transport
Network
Data Link
Physical

Application Services

- Application services unite communicating components from more than one network application



- Examples:
  - File transfers and file sharing
  - E-mail
  - Remote access
  - Network management activities
  - Client/server processes

Service Advertisement

- Some applications send out announcements
- States the services they offer on the network
- Some centrally register with the Active Directory server instead
- Example:
  - Printers
  - File servers

Examples at Layer 7

- E-mail (POP3, IMAP, SMTP)
- Web Browsing (HTTP, HTTPS)
- Domain Name Service (DNS)
- File Transfer Protocol (FTP, FTPS)
- Remote Access (TELNET, SSH)
- Simple Network Management Protocol (SNMP)