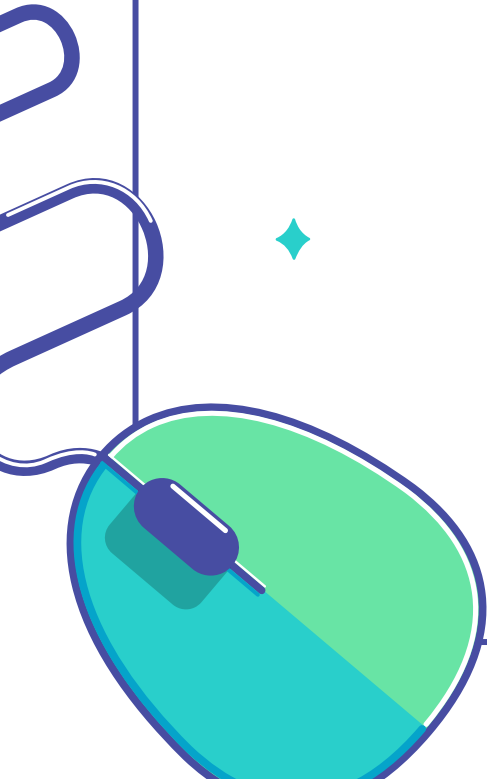


Sponsored by [veryofficialnft.com](https://www.veryofficialnft.com)

An Intro to Networking

Presented by Preston Sergent





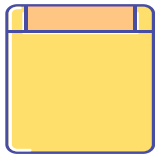
Pronouns

They/Them



Fedora User

For Real



Disclaimer

The views and opinions expressed in this presentation are solely those of the presenter and do not necessarily reflect the official policy or position of Cisco Systems. This presentation is not affiliated with Cisco Systems and should not be construed as work done as an employee of Cisco Systems.

Presentation Agenda



01

History of Networking

02

Ethernet Basics

03

IPv4 Addressing

04

Routing Basics

05

TCP and UDP

06

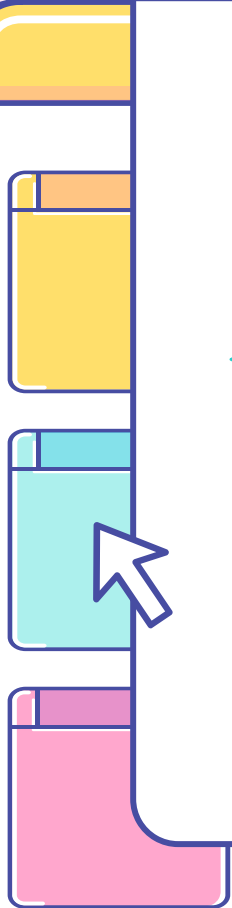
QUIC



There's no place like ~/



History of Networking





ARPANET

Developed in the 1960s by the Department of Defense, allowed researchers to share computing resources



◆ **ETHERNET**

Developed in the 1970s by Xerox, enabled faster data transmission and popularized LANs.

WANs

Developed in the 1980s, enabled computers in different locations to connect and communicate using TCP/IP.





ARCnet (Attached Resource Computer Network)

A LAN protocol using coaxial cables, replaced by Ethernet. ♦

FDDI (Fiber Distributed Data Interface)

♦ High-speed data transmission standard using fiber-optic cables, replaced by Ethernet.

Token Ring

LAN protocol using token-passing, slower than Ethernet and never widely adopted.

AppleTalk

Proprietary protocol for Macintosh computers, replaced by TCP/IP. ♦



Network Model

Defines a standard for how different devices communicate with each other over a network. 

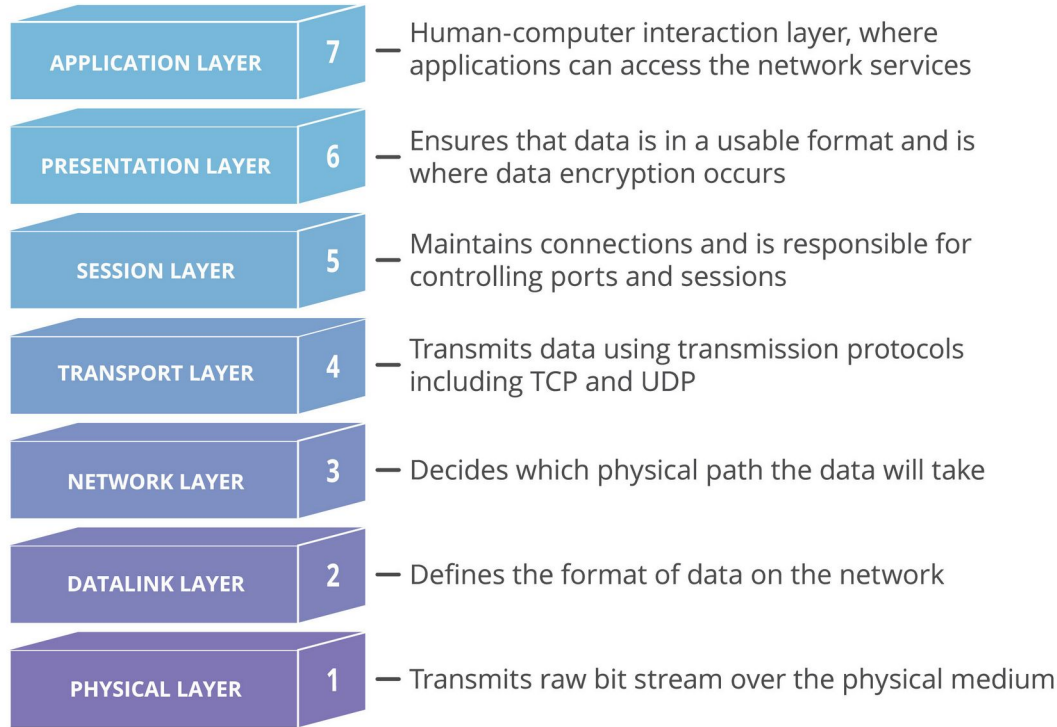


Layered Model

Seven-layer model for computer networks. Each layer builds upon the functions of the layer below it.



OSI Model





Arch Penguins Slay Through Network Data Pipes

P

Can you think of a mnemonic for the layers of the OSI model that includes a distribution of the linux operating system within it?



Sure, here's a mnemonic for the OSI model layers that includes a distribution of the Linux operating system:

"Arch Penguins Slay Through Network Data Pipes"

- Arch: Arch Linux, a popular Linux distribution
- Penguins: Presentation Layer, responsible for formatting data for presentation to the application layer
- Slay: Session Layer, responsible for managing the sessions between applications
- Through: Transport Layer, responsible for reliable data transfer between endpoints
- Network: Network Layer, responsible for routing data across networks
- Data Pipes: Data Link Layer, responsible for managing the flow of data between devices
- Physical: Physical Layer, responsible for transmitting raw data across a physical medium.

This mnemonic can be a fun way for Linux users to remember the layers of the OSI model, and to relate them to a distribution of the Linux operating system.



All Penguins Should Try New Distros Promptly



Sure, here's a mnemonic that includes a distribution of the Linux operating system to remember the seven layers of the OSI model:

"All Penguins Should Try New Distros Promptly"

Each word corresponds to the first letter of one of the seven layers in the OSI model, in order from the top layer to the bottom layer:

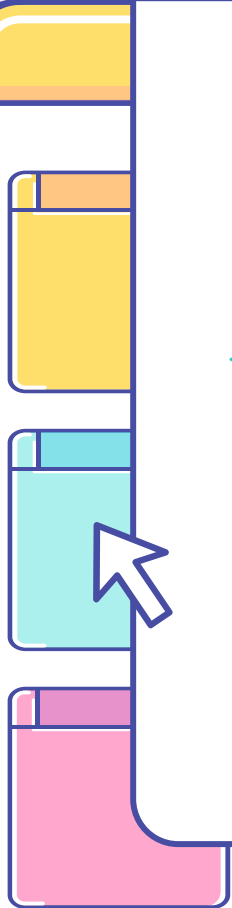
- Application layer
- Presentation layer
- Session layer
- Transport layer
- Network layer
- Data link layer
- Physical layer

This mnemonic incorporates the word "Penguins" to represent the Linux operating system, which is often associated with the penguin mascot. The phrase "Try New Distros Promptly" can also serve as a reminder to stay up-to-date with new Linux distributions as they are released.

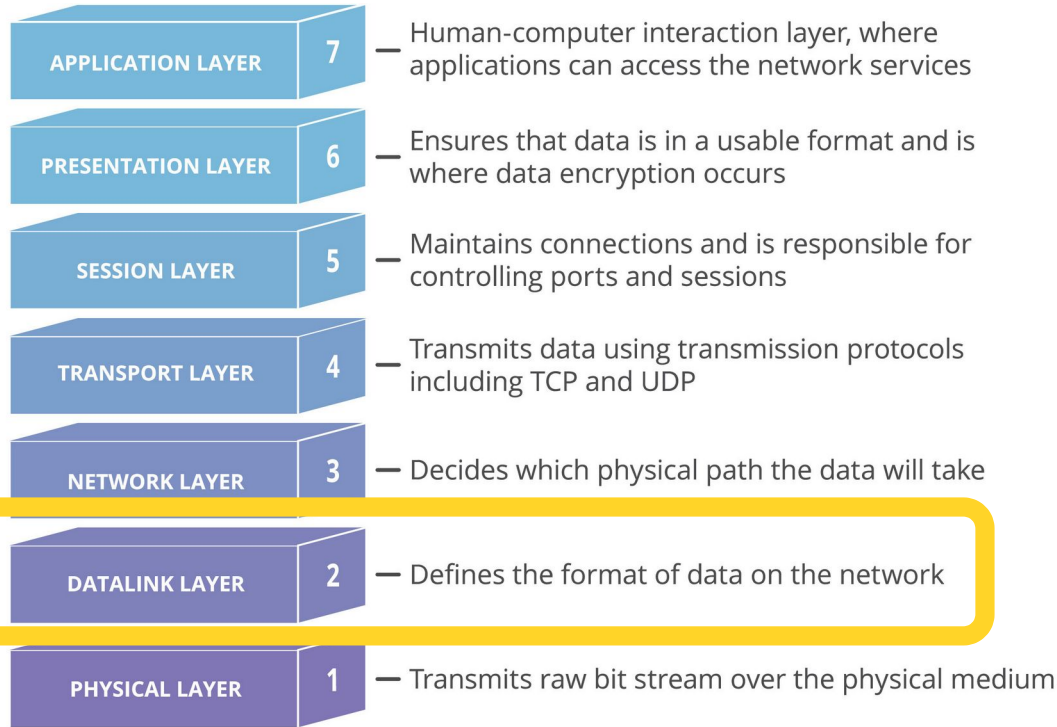
Xerox in the 70s was enough of a joke...



Ethernet Basics



What layer of the OSI Model are we on?





What is a layer 2 network?

A network that operates at layer 2 of the OSI model. This layer provides reliable communication between nodes on the same network segment.

Ethernet

Ethernet is a common layer 2 networking technology used in local area networks (LANs). MAC Addresses are used to make forwarding decisions.



Layer 2 Devices



- Network switches
- Bridges
- ◆ Network interface cards (NICs)
- Wireless access points (WAPs)
- Repeaters
- Ethernet hubs





Simplicity

Ethernet is easy to install, use and maintain.



Flexibility

◆ Ethernet can adapt to different network needs. This is especially true since it can be used with different physical mediums.

Cost-effectiveness

Ethernet was designed to be a cost-effective networking solution that could be easily implemented by businesses of all sizes.





Twisted Pair Copper Cable

This is the most common physical medium used for Ethernet. Twisted pair cables come in different categories (e.g., Cat5e, Cat6) that can support different transmission speeds and distances.

Fiber Optic Cable

This physical medium uses optical fibers to transmit data as light signals. Fiber optic cables have higher bandwidth and can transmit data over longer distances than copper cables.



Coaxial Cable

Ethernet can also be implemented on coaxial cables, which were used in the early days of Ethernet. Coaxial cables have been largely replaced by twisted pair and fiber optic cables, but some legacy systems still use them.





Unique Identifier

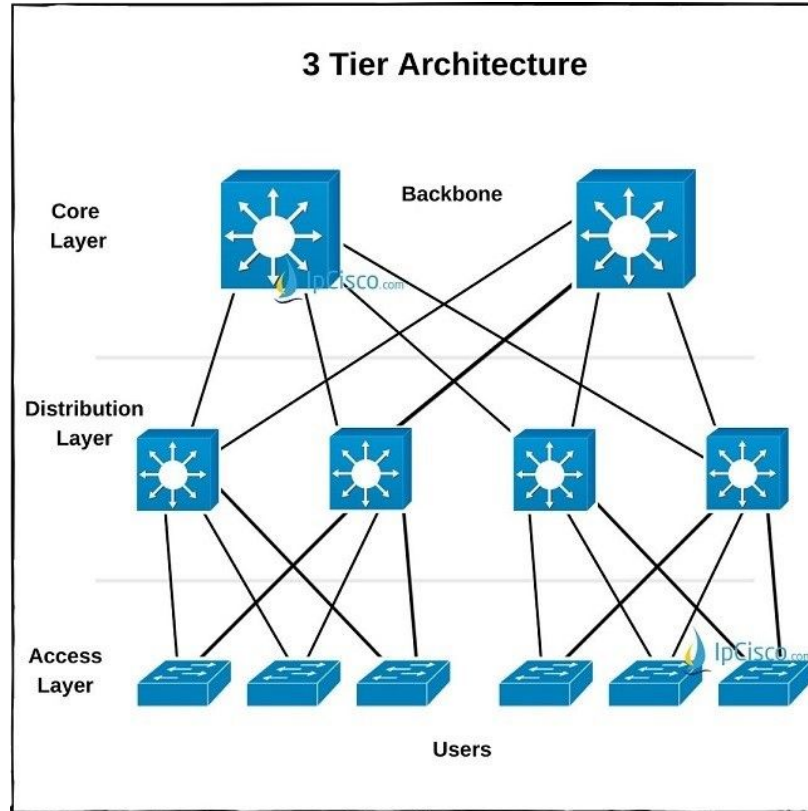
MAC addresses are unique identifiers assigned to network interface controllers (NICs) by the manufacturer. They are used to identify layer 2 devices on a network. They can, however be spoofed.

Address Format

MAC addresses are 48 bits long, represented by a string of 12 hexadecimal digits (e.g., 00:1A:2B:3C:4D:5E). The first three octets are known as the OUI.



Three-Tier Network Design



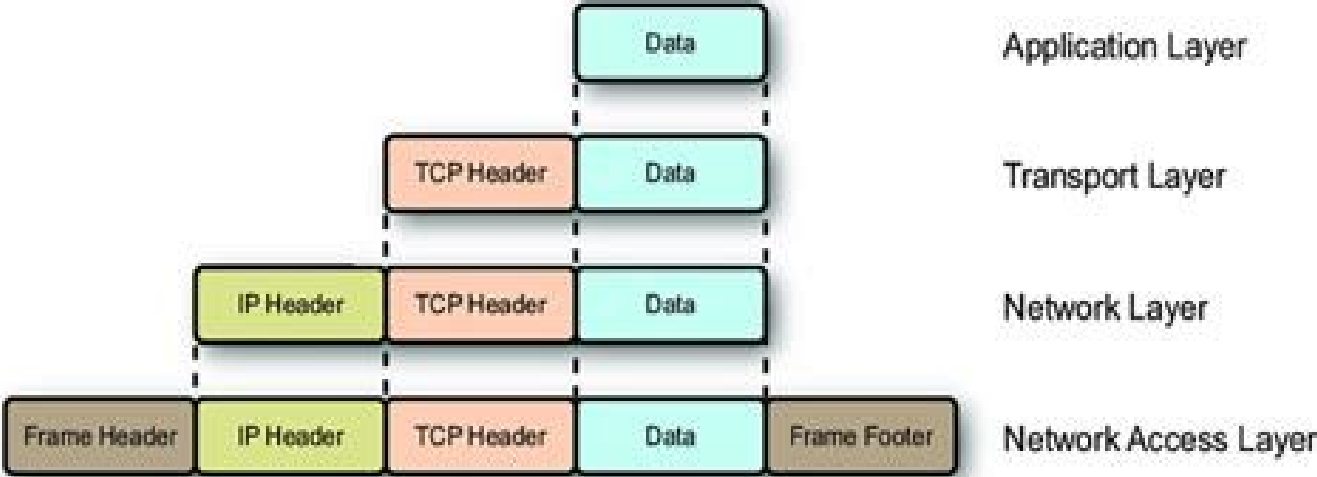
Frame fields



Ethernet II					
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 to 1500 Bytes	4 Bytes
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence



Encapsulation



Encapsulation



Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2031	36.951443	2607:f8b0:400e:c04:...	2601:1c0:cf00:8961:...	TLSv1.2	120	Application D
2032	36.951504	2601:1c0:cf00:8961:...	2607:f8b0:400e:c04:...	TCP	74	58841 → 443 [
2033	36.951770	2601:1c0:cf00:8961:...	2607:f8b0:400e:c04:...	TLSv1.2	120	Application D
2034	37.017175	2607:f8b0:400e:c04:...	2601:1c0:cf00:8961:...	TCP	74	443 → 58841 [
2035	37.216674	2601:1c0:cf00:8961:...	2607:f8b0:400e:c04:...	TCP	127	[TCP segment

> Frame 2032: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

> Ethernet II, Src: IntelCor_38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC_35:e4:c8 (1c:87:2c:35:e4:c8)

> Internet Protocol Version 6, Src: 2601:1c0:cf00:8961:e182:3669:c103:5336, Dst: 2607:f8b0:400e:c04:...

> Transmission Control Protocol, Src Port: 58841, Dst Port: 443, Seq: 3873, Ack: 72837, Len: 74

Offset	Hex	ASCII
0000	1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 86 dd 60 04	...,5.. \ .8....`.
0010	31 8f 00 14 06 40 26 01 01 c0 cf 00 89 61 e1 82	1....@&.a..
0020	36 69 c1 03 53 36 26 07 f8 b0 40 0e 0c 04 00 00	6i..S6&. ..@.....
0030	00 00 00 00 00 68 e5 d9 01 bb 91 1f c7 c3 4e 79h..Ny
0040	b8 21 50 10 01 04 50 42 00 00	!.P...PB ..

Wi-Fi: <live capture in progress> | Packets: 2422 · Displayed: 2422 (100.0%) | P

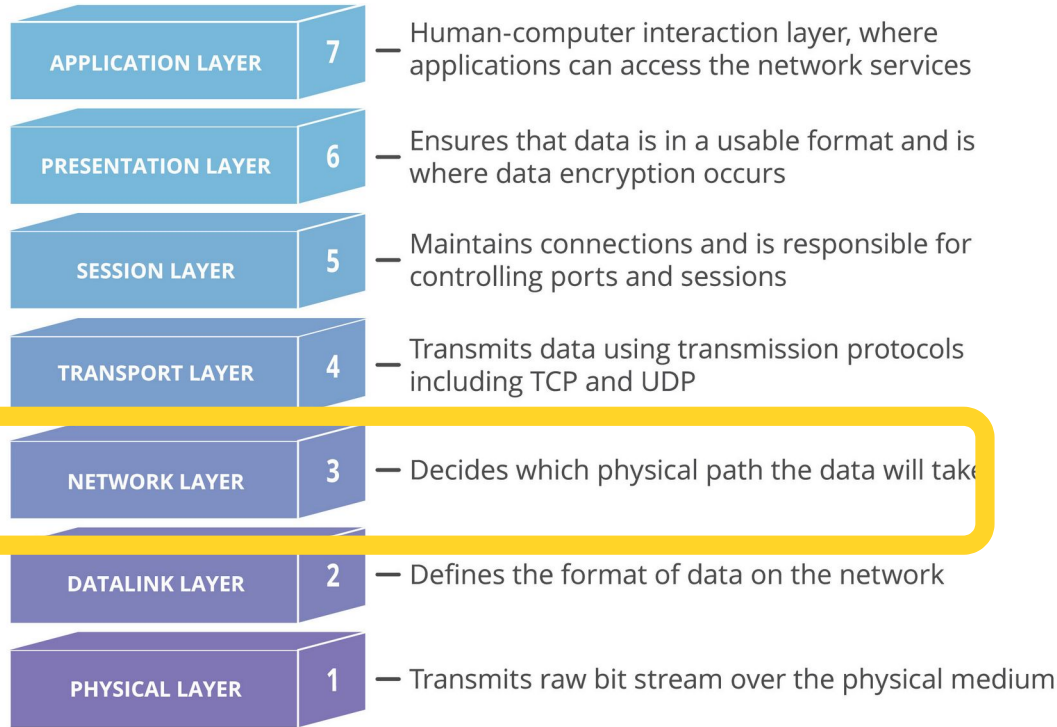


**Break
time?**

No one cared what IP I had until I applied the subnet mask

IPv4 Addressing

What layer of the OSI Model are we on?





What is a Layer 3 network?

A network that operates at the network layer of the OSI model. It uses IP addresses to forward packets between networks.



Why use a Layer 3 Network?

Layer 3 networks are used to connect multiple layer 2 networks together, and provide the ability to communicate with devices that are not on the same network segment.



Layer 2 Devices



- Network switches
- Bridges
- ◆ Network interface cards (NICs)
- Wireless access points (WAPs)
- Repeaters
- Ethernet hubs





Address Format

An IPv4 address is made up of four octets, or 32 bits of data, typically represented in dotted decimal notation, such as 192.168.1.1. They may be dynamically or statically allocated.

Network Portion

Identifies the network to which the device belongs.
Determined by the subnet mask.

Host Portion

Identifies the specific device on that network. Determined by the subnet mask.



Format

A subnet mask is a 32-bit value used to divide an IP address into a network and host portion. It consists of a series of 1s and 0s, where the 1s represent the network portion and the 0s represent the host portion.

Example

A subnet mask of 255.255.255.0 can be represented as:

11111111 11111111 11111111 00000000

And will have a network prefix of /24



Are two IP Addresses are on the same network?



1. Convert the IPv4 Addresses and Subnet mask to Binary

192.168.1.10 -> 11000000 10101000 00000001 00001010

192.168.1.20 -> 11000000 10101000 00000001 00010100

◆ 255.255.255.0 -> 11111111 11111111 11111111 00000000





2. Apply a logical AND and compare the result

11000000 10101000 00000001 00001010 (192.168.1.10) 

AND

11111111 11111111 11111111 00000000 (subnet mask)

→ 11000000 10101000 00000001 00000000 

11000000 10101000 00000001 00010100 (192.168.1.20)

AND

11111111 11111111 11111111 00000000 (subnet mask)

→ 11000000 10101000 00000001 00000000





Address Format

An IPv4 address is made up of four octets, or 32 bits of data, typically represented in dotted decimal notation, such as 192.168.1.1. They may be dynamically or statically allocated.

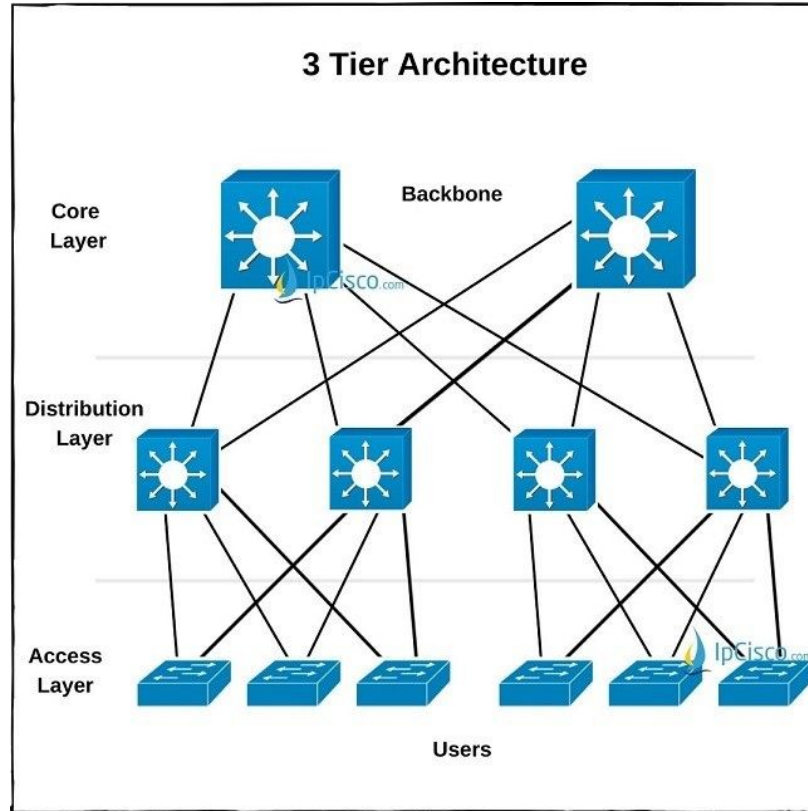
Network Portion

Identifies the network to which the device belongs. Determined by the subnet mask.

Host Portion

Identifies the specific device on that network. Determined by the subnet mask.

Three-Tier Network Design

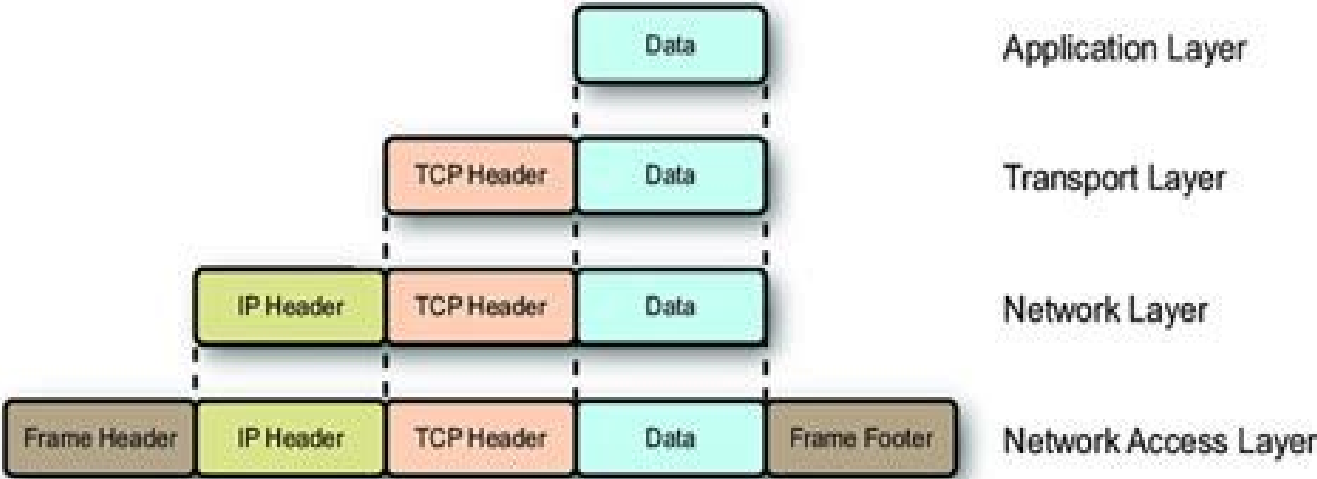


Packet fields



Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

Encapsulation



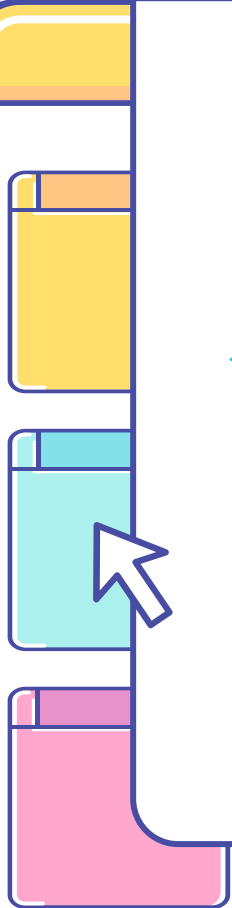


**Break
time!**

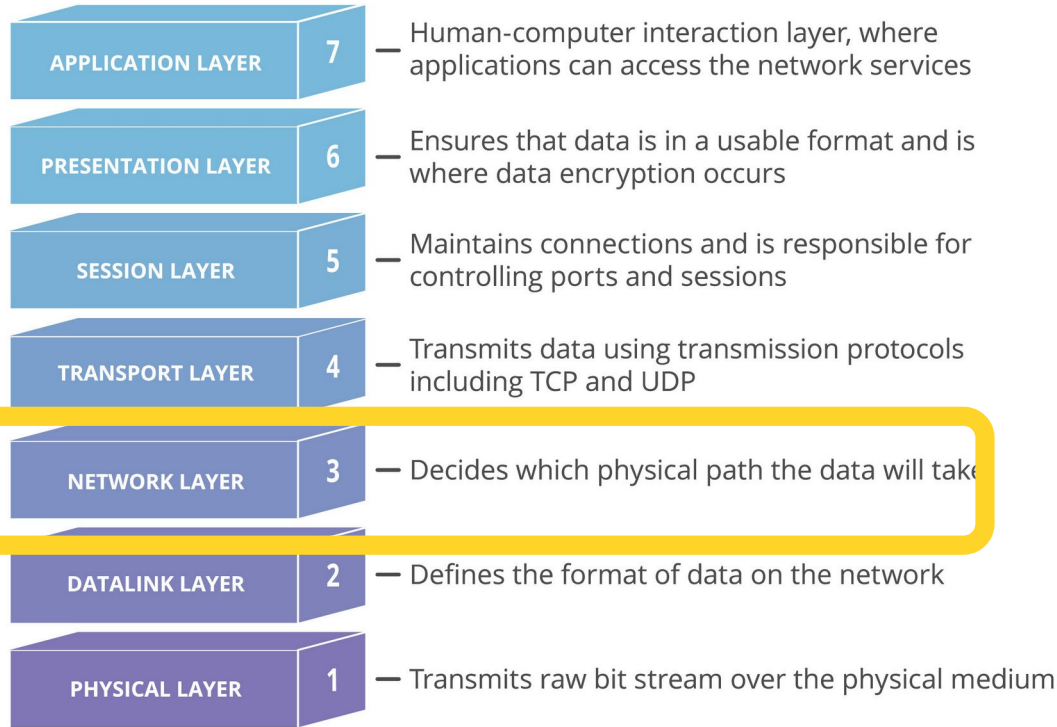
Router? I barely know her.



Routing Basics



What layer of the OSI Model are we on?





What is Routing?

Routing is the process of forwarding data packets between networks based on their IP addresses



What does a Router do?

Routers use routing tables and algorithms to determine the best path for data packets to reach their destination across different networks.



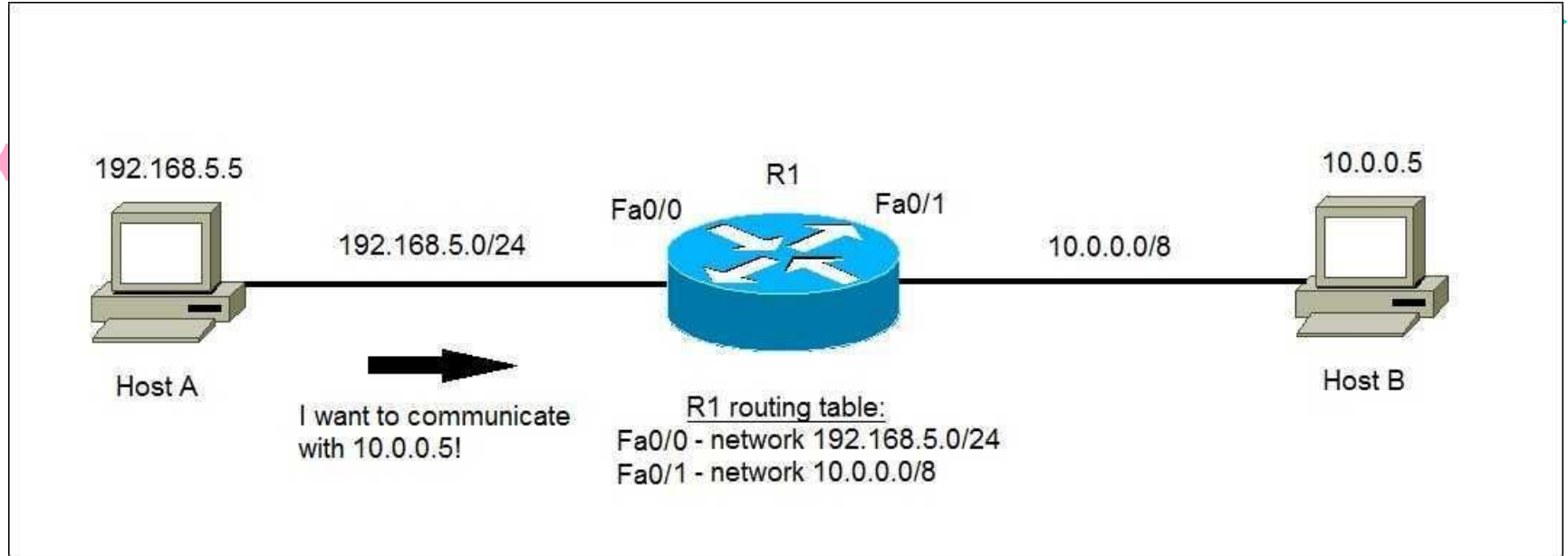


How can routing be performed?

Routing can be done through static routing, where administrators manually configure the routing tables, or dynamic routing, where routers exchange routing information using routing protocols such as OSPF or BGP.





Static Route Example



Dynamic Routing Protocols



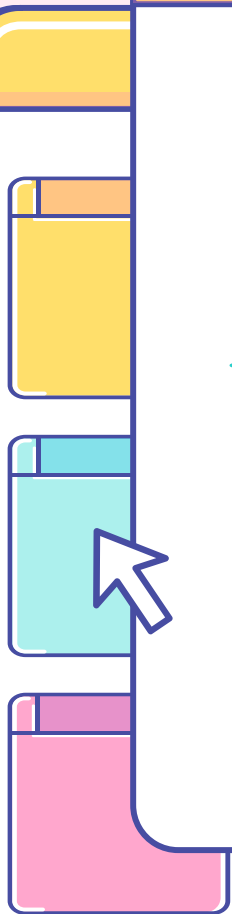
- Automatically update routing tables on routers by exchanging information about network topology. 
- Leverage metrics to determine the best path for data to travel through a network 
- Metrics can include congestion, available bandwidth, and hop count.
- Examples include OSPF, BGP, and EIGRP



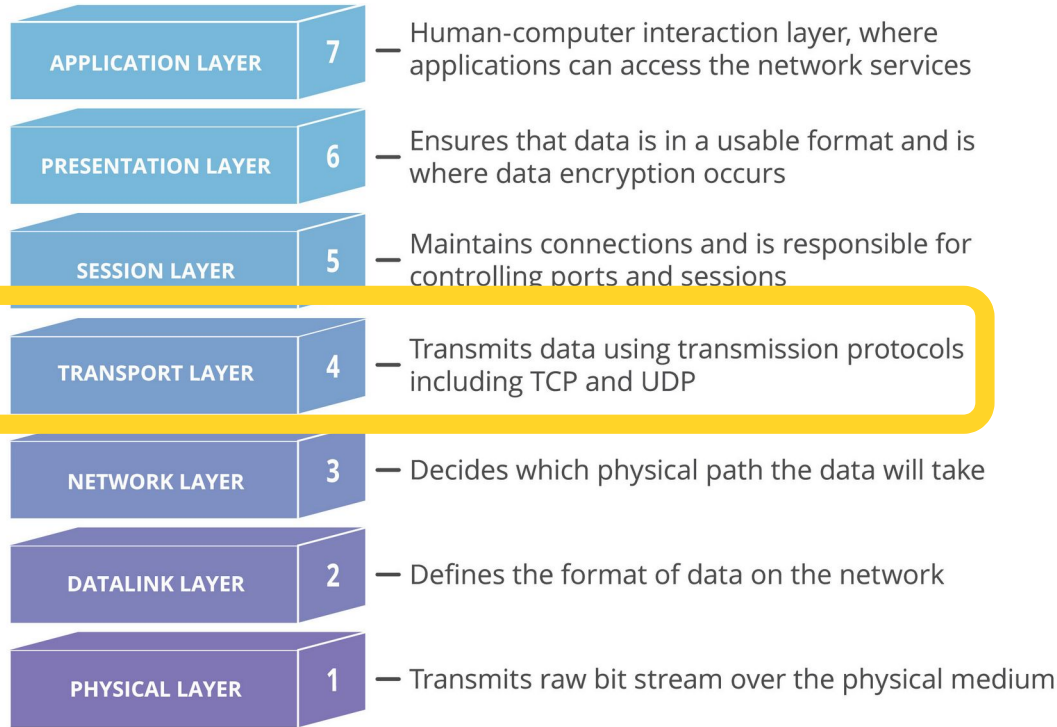
All your packets want is a firm handshake.



TCP and UDP




What layer of the OSI Model are we on?





What does TCP do?

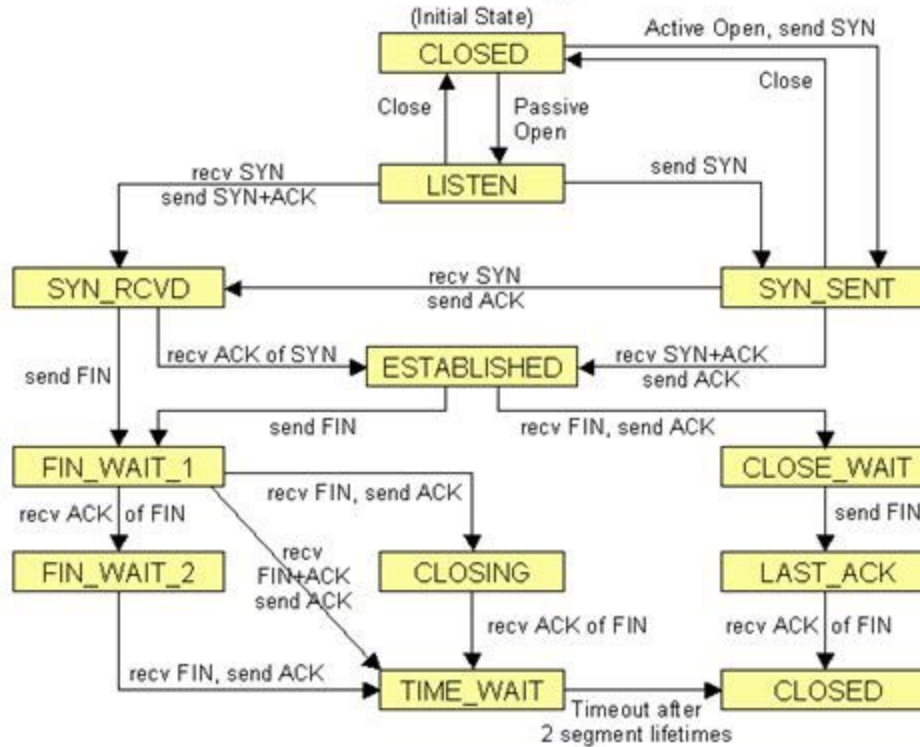
- TCP is a connection-oriented protocol used for reliable data transfer over an IP network. 
- ◆ TCP ensures that data packets are sent and received in the correct order and without errors or loss.
- TCP uses a system of acknowledgments and re-transmissions to guarantee reliable delivery of data.



TCP State Diagram



TCP State Diagram



TCP Handshake



Client

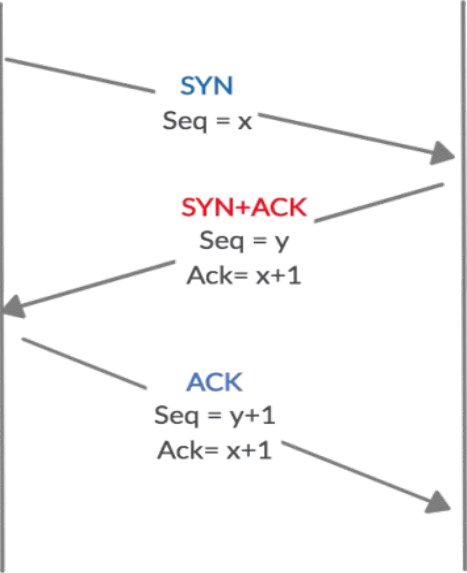


Server

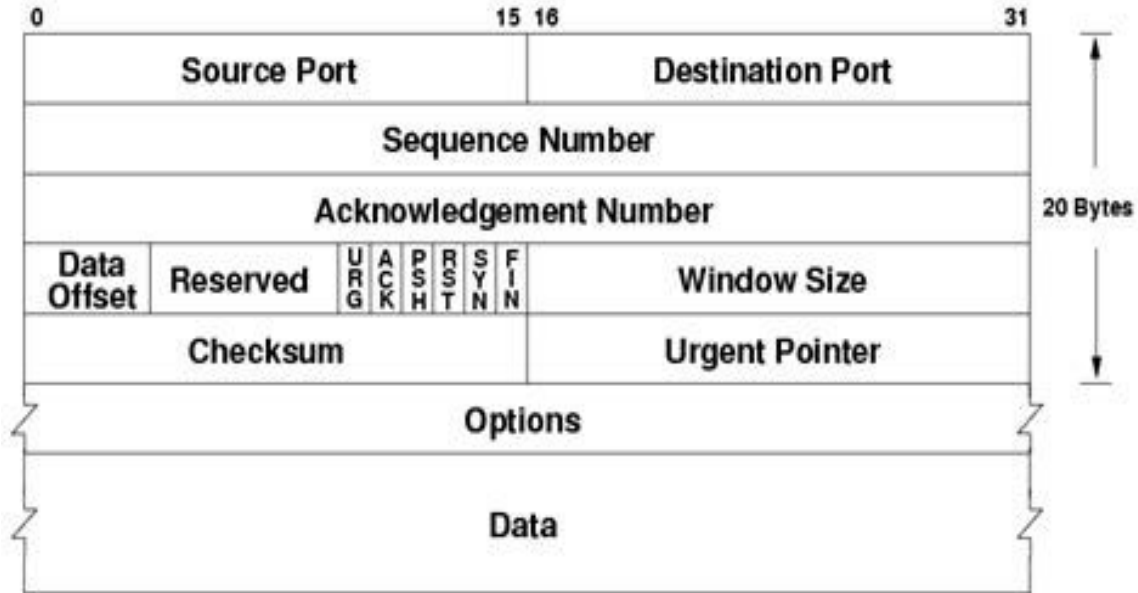
Closed

SYN-SENT

ESTABLISHED




TCP Fields



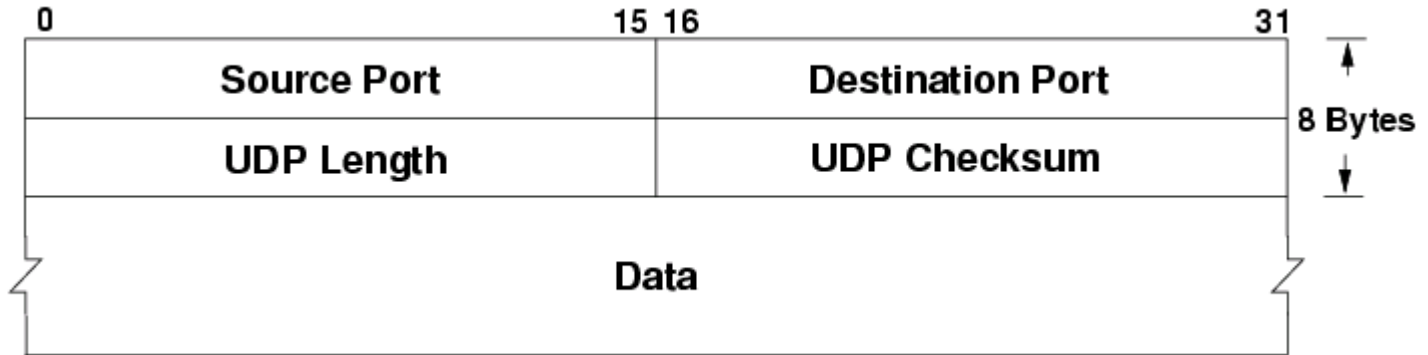


What does UDP do?

- UDP is a connectionless protocol that operates at the transport layer of the OSI model. 
- ◆ UDP is a lightweight and fast protocol that doesn't provide any error checking or flow control,
- UDP is ideal for applications that prioritize speed over reliability, such as online gaming and video streaming
- UDP doesn't establish a connection between two devices before sending data, and instead simply sends data packets to the destination address.



UDP Fields



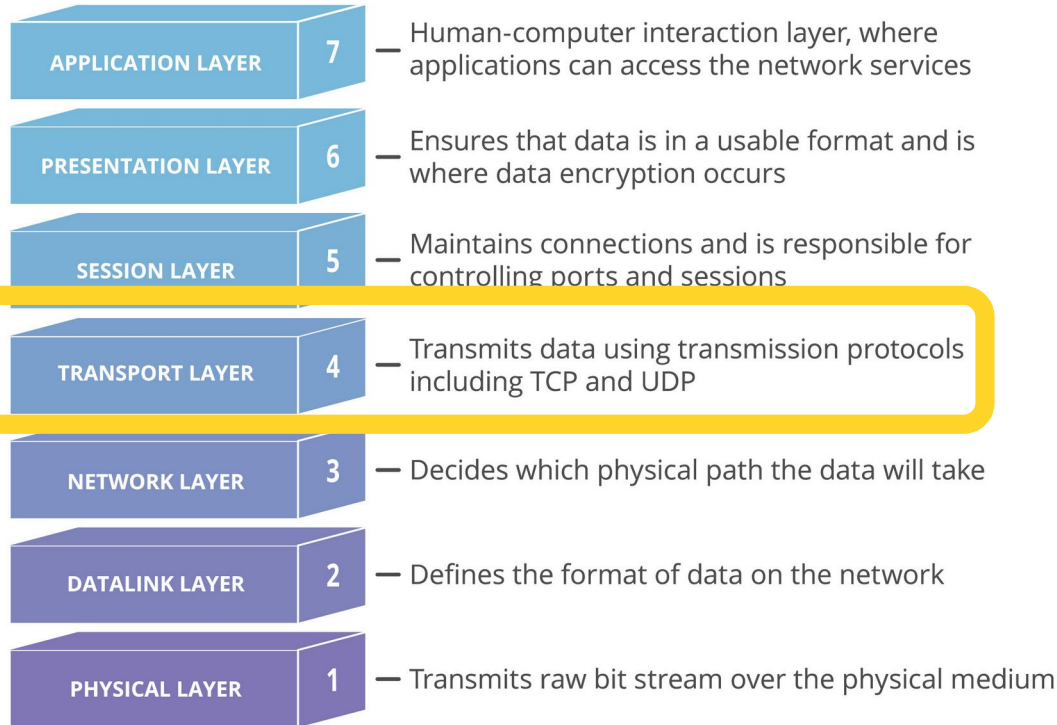
A QUIC ending to a 56-slide presentation.




QUIC



What layer of the OSI Model are we on?





What does QUIC do?

- QUIC is a transport protocol developed by Google that runs on top of the UDP protocol. 
- ◆ • QUIC is designed to reduce latency and improve performance for web applications, especially for high-latency connections and mobile networks.
- QUIC uses features such as encryption and congestion control to improve reliability and security over unreliable networks.



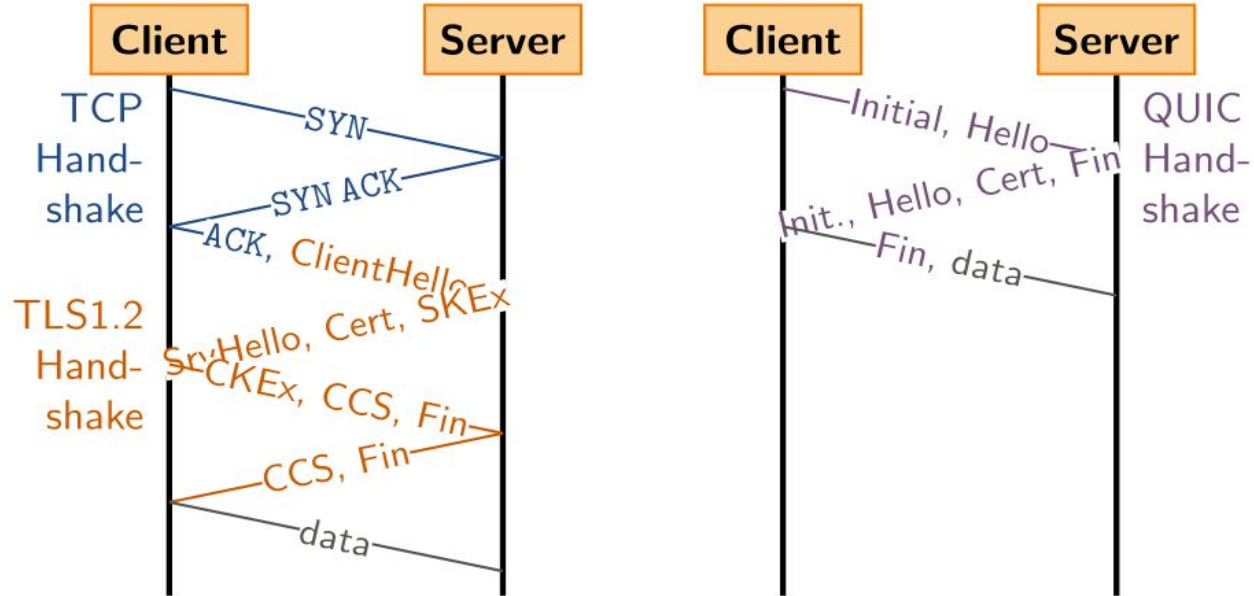
Who uses QUIC?



- HTTP/3 is based on QUIC 
- SSH over QUIC has a Proof-Of-Concept 
- YouTube uses QUIC to speed up video streaming.
- Apple has implemented QUIC in some of its software products to improve network performance.
- Cloudflare supports QUIC for its content delivery network (CDN) services.



QUIC vs TCP/TLS Handshake



You don't have to go home, but you can't stay here.



Questions?

