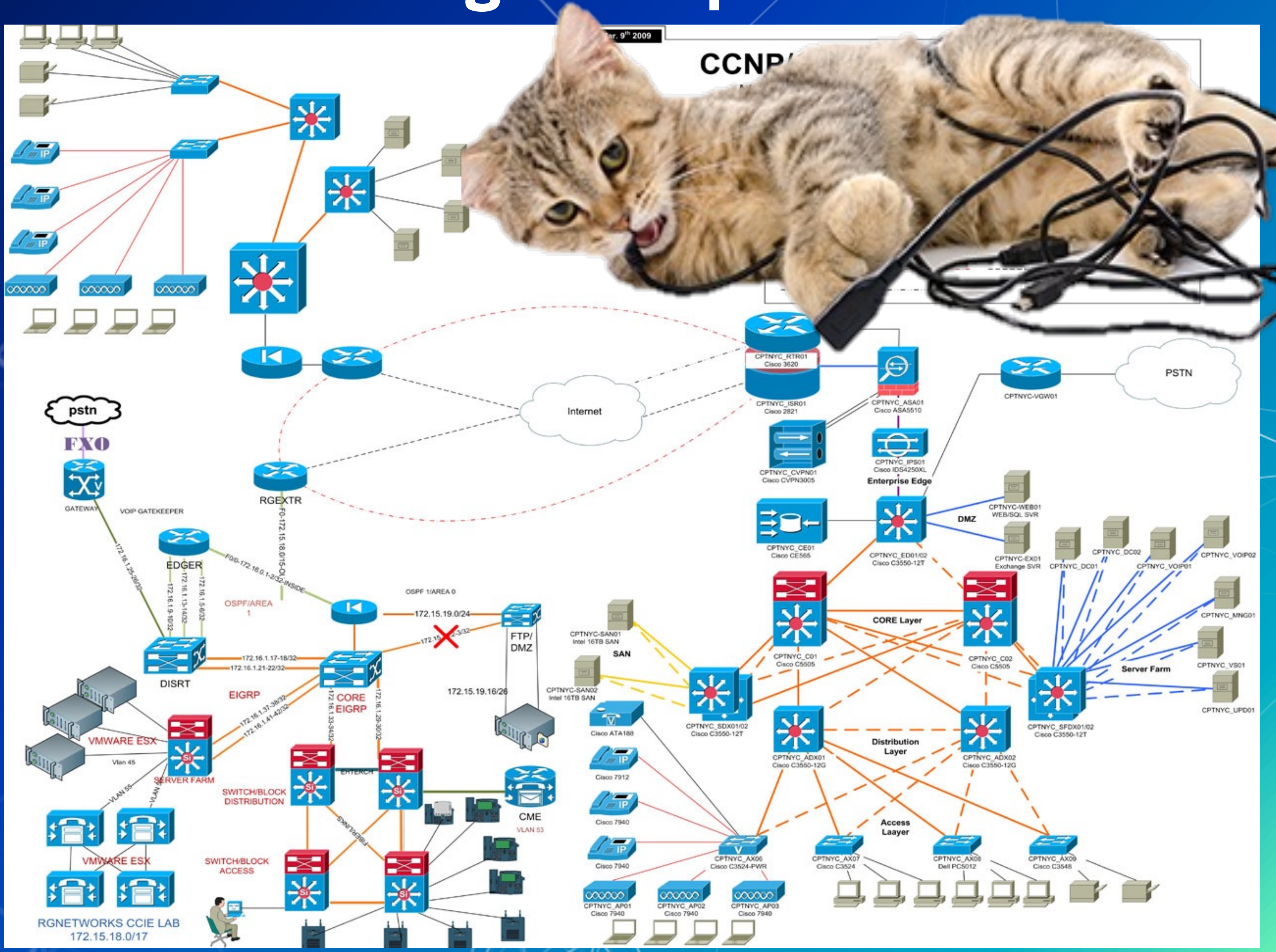
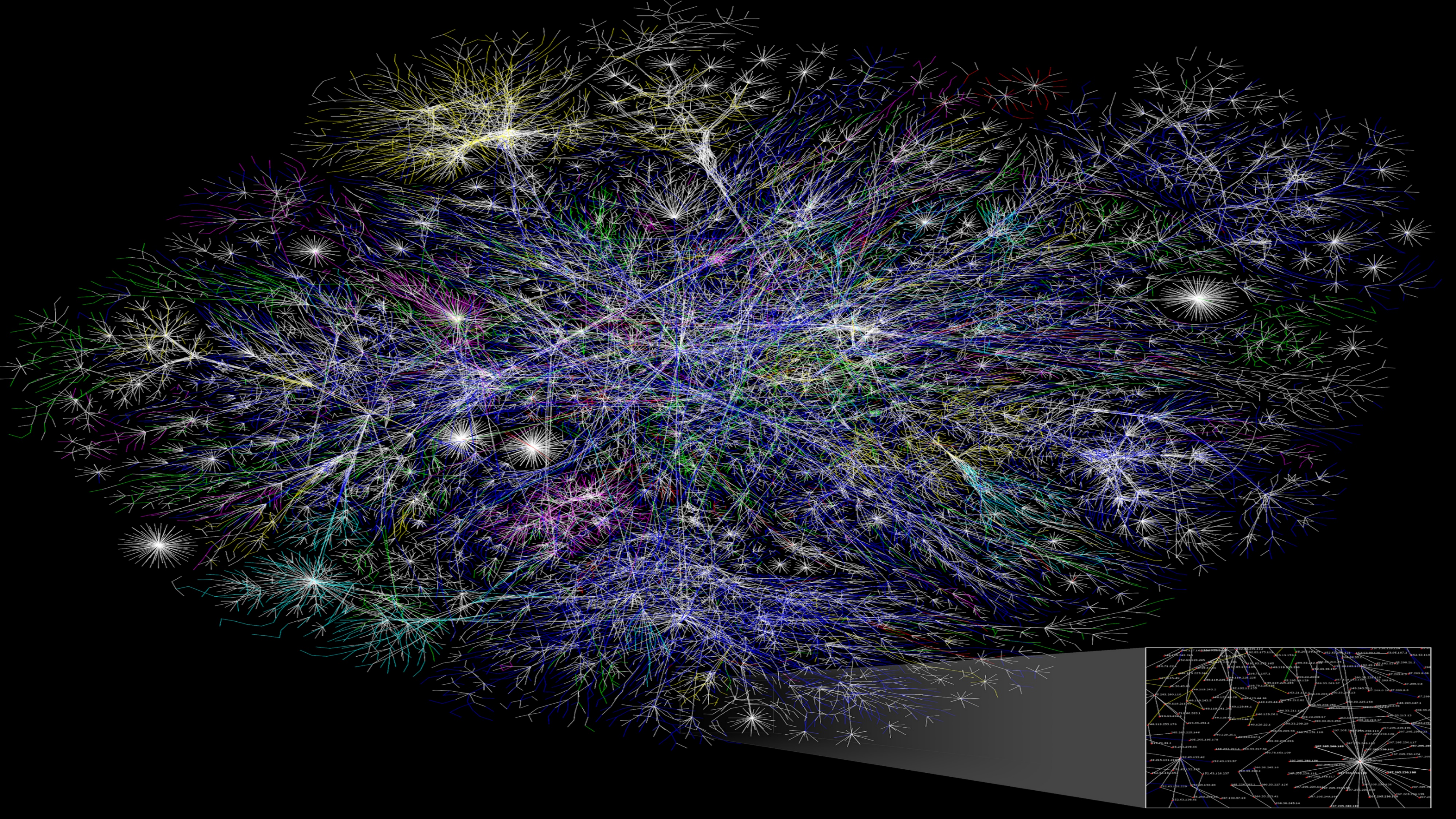
Advanced Networking Concepts

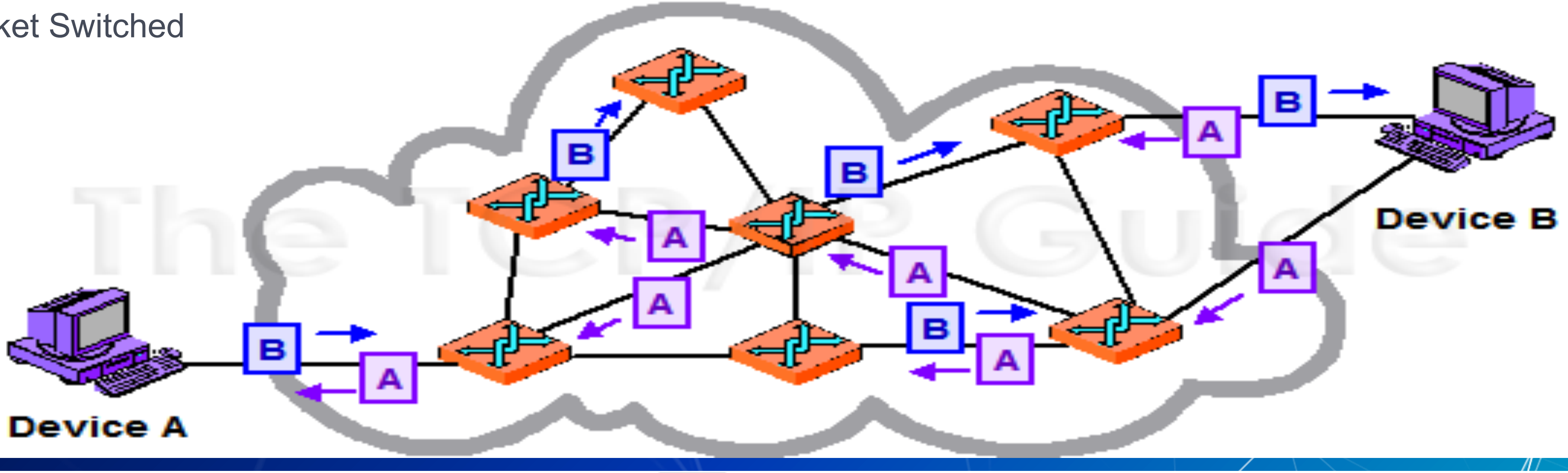


- Systems Security
- Kevin Cleary
- Thursday, April 6, 2023

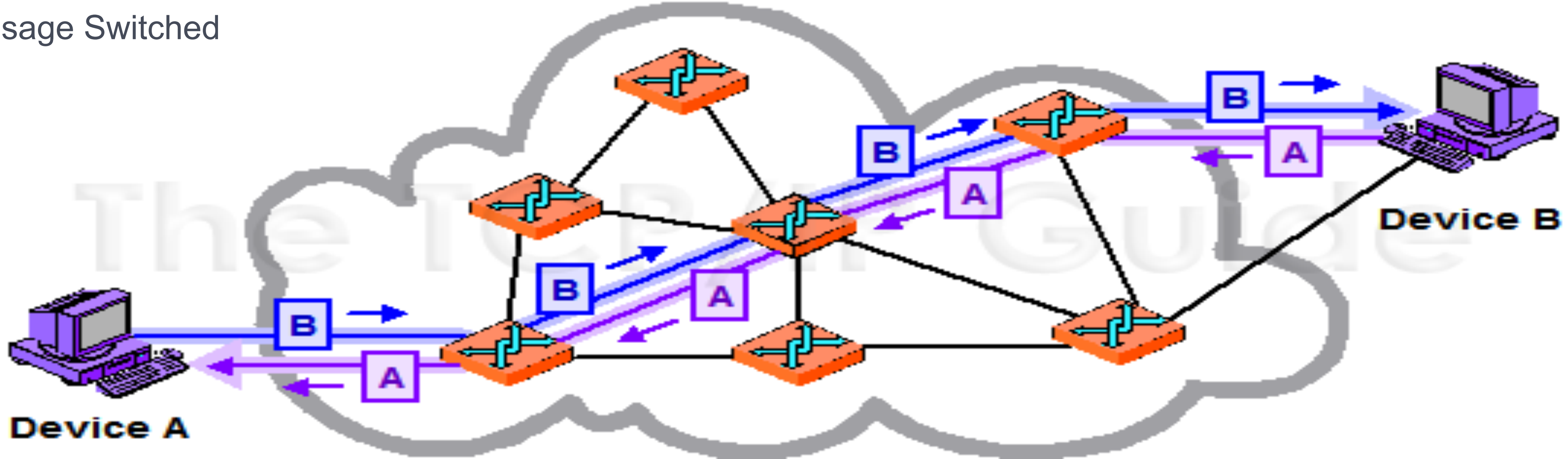

152.63.128.245
210.71.22.1
192.83.175.119
192.83.175.165
140.119.225.236
200.33.209.9
200.33.209.37
67.209.0.8
67.209.0.6
63.95.187.1
65.200.21.1
140.119.225.225
210.71.107.1
65.205.99.129
210.70.129.105
140.119.225.245
192.192.12.135
140.119.243.2
65.203.200.118
140.119.243.5
140.129.44.20
140.129.44.60
140.129.44.45
140.129.44.1
140.119.241.241
200.33.212.82
200.33.208.250
200.33.225.158
148.243.50.1
148.243.147.1
200.33.211.132
140.129.26.1
216.66.203.1
216.66.201.1
140.119.253.170
140.129.22.1
200.33.209.17
200.33.210.250
200.33.213.13
200.33.213.37
200.33.209.29
200.33.209.33
200.78.151.110
205.205.195.178
140.129.25.1
148.243.137.1
200.33.230.206
65.203.200.66
148.243.216.1
200.33.217.34
200.78.151.109
207.205.230.105
207.205.230.110
207.205.230.128
207.205.230.117
207.205.230.174
152.63.133.42
152.63.133.57
200.33.245.10
152.63.132.155
152.63.128.237
207.205.230.118
207.205.249.117
152.63.128.229
152.63.130.69
148.224.208.1
200.33.227.126
207.205.230.112
207.205.230.155
200.33.223.41
207.205.249.101
207.139.97.10
152.63.130.60
200.33.245.14

Packet Vs Circuit Switching

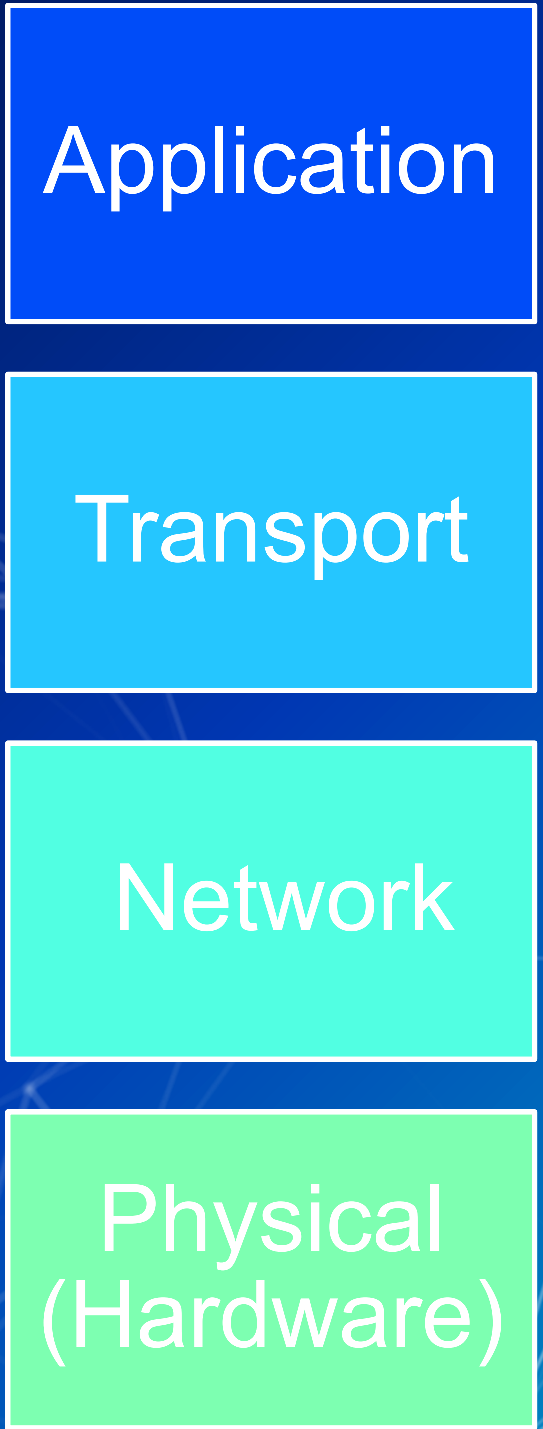
Packet Switched



Message Switched



The TCP/IP Protocol Stack



Application

Transport

Network

Physical (Hardware)

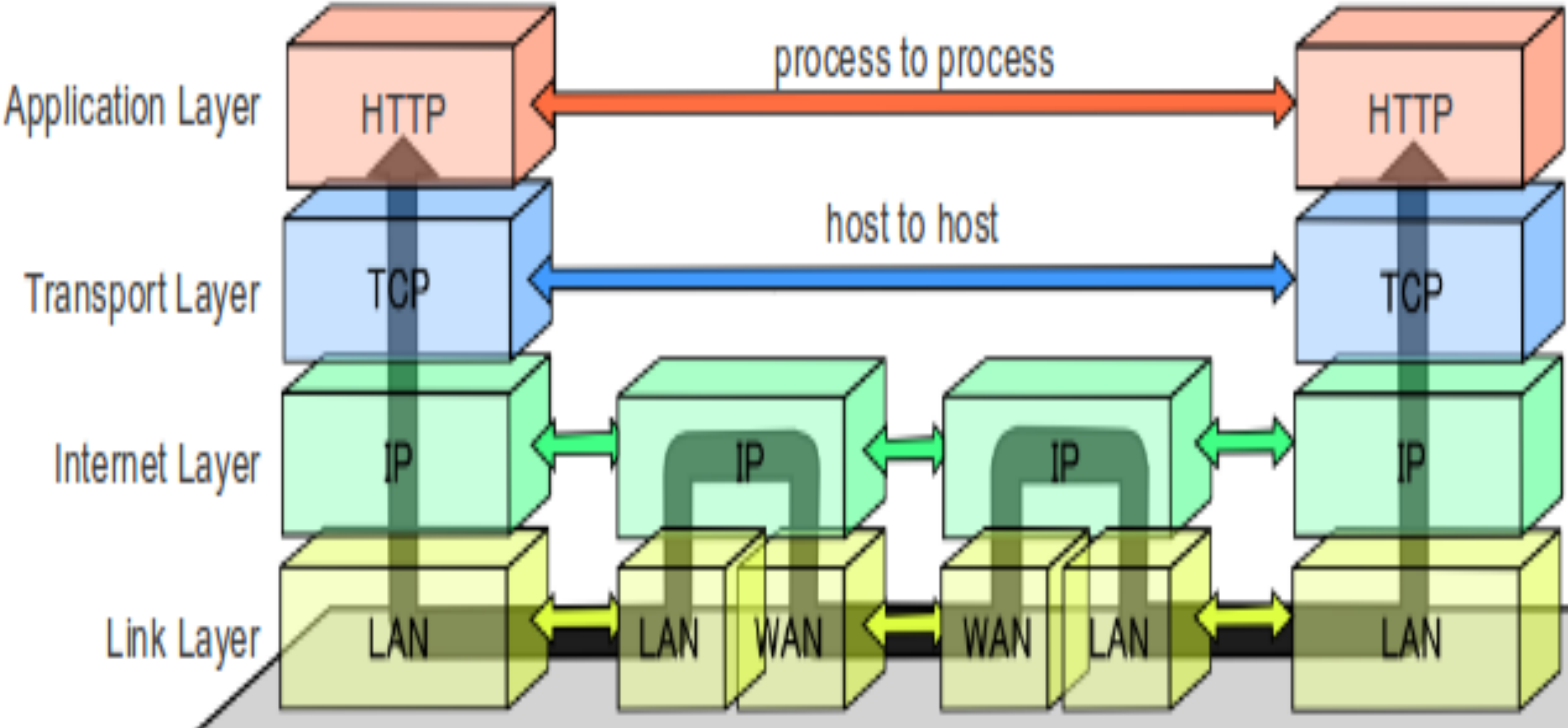
At what layers do we primarily deal with Security?

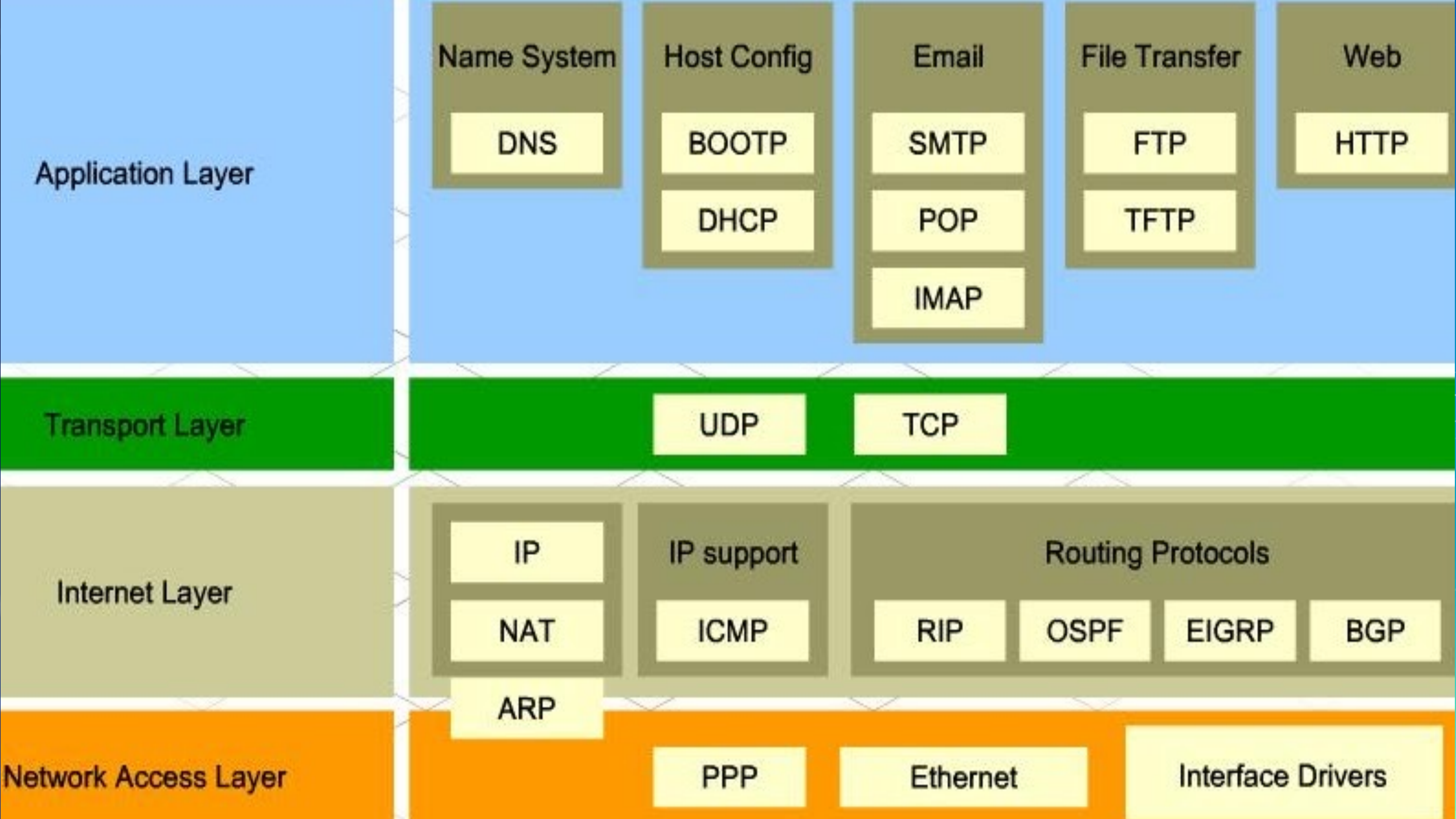
All Layers!

Protocol Stacks

- Protocol stack used by most devices is known as TCP/IP.
  - The stack includes:
    - Network (Internet) - packet switched
    - Transport Layer - circuit switching
- The TCP/IP protocol stack takes care of how computer communications get routed to the correct computer and how packets are reassemble so that they make sense to our applications.
  - Messages travel down and then up the protocol stack.
  - Each protocol within the stack has a set task.
  - transport layer provides management overhead to ensure messages are sent and received in a reliable way, ensuring integrity and authenticity.
  - The IP layer takes care of steering these packets in an efficient, redundant way across many multiple, heterogeneous networks.
- The Hardware layer physical transmits packets wrapped in frames.

Data Flow of the Internet Protocol Suite





Application Layer

Name System
DNS

Host Config
BOOTP
DHCP

Email
SMTP
POP
IMAP

File Transfer
FTP
TFTP

Web
HTTP

Transport Layer

UDP
TCP

Internet Layer

IP
NAT
ARP

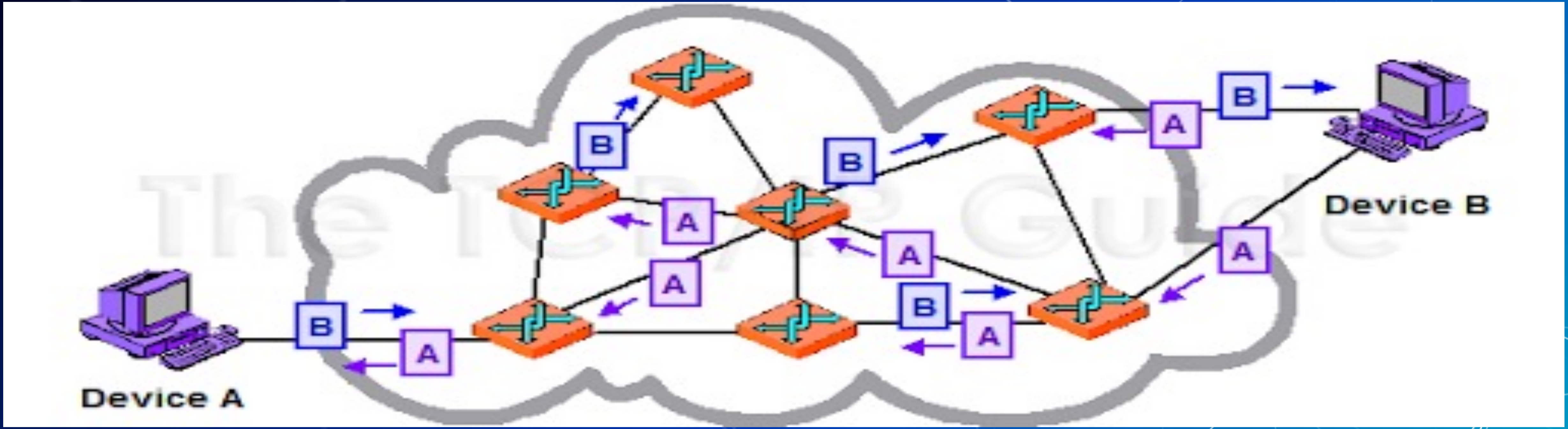
IP support
ICMP

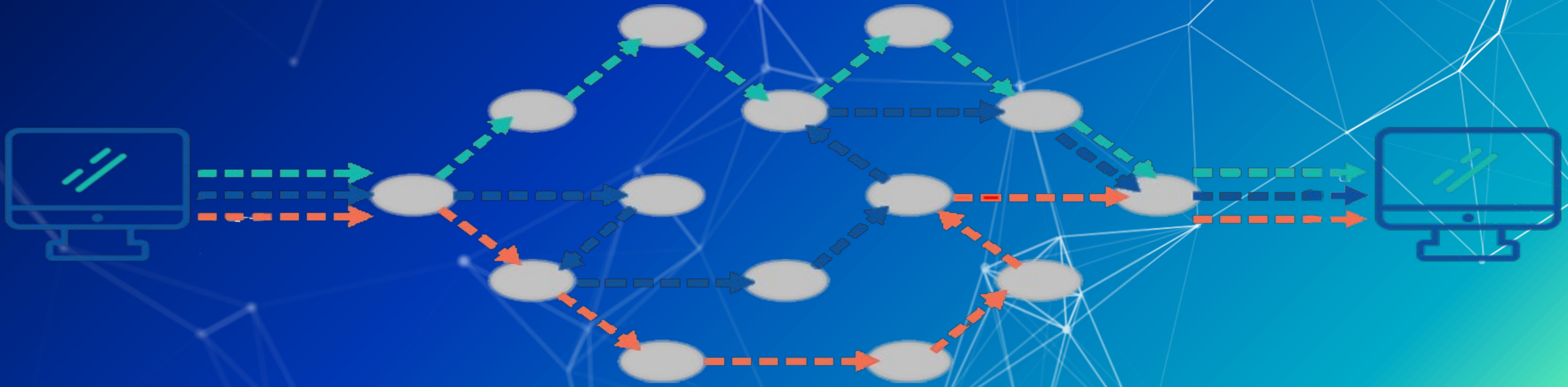
Routing Protocols
RIP
OSPF
EIGRP
BGP

Network Access Layer

PPP
Ethernet
Interface Drivers

The Flow of Internet Data at the Transport Layer

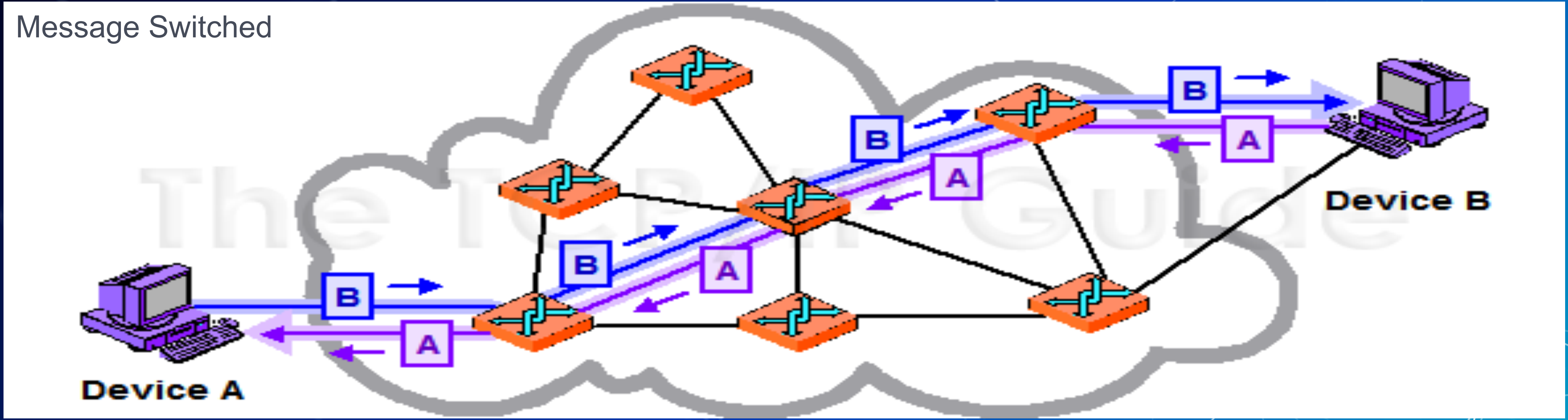




The Flow of Internet Data at the Transport Layer

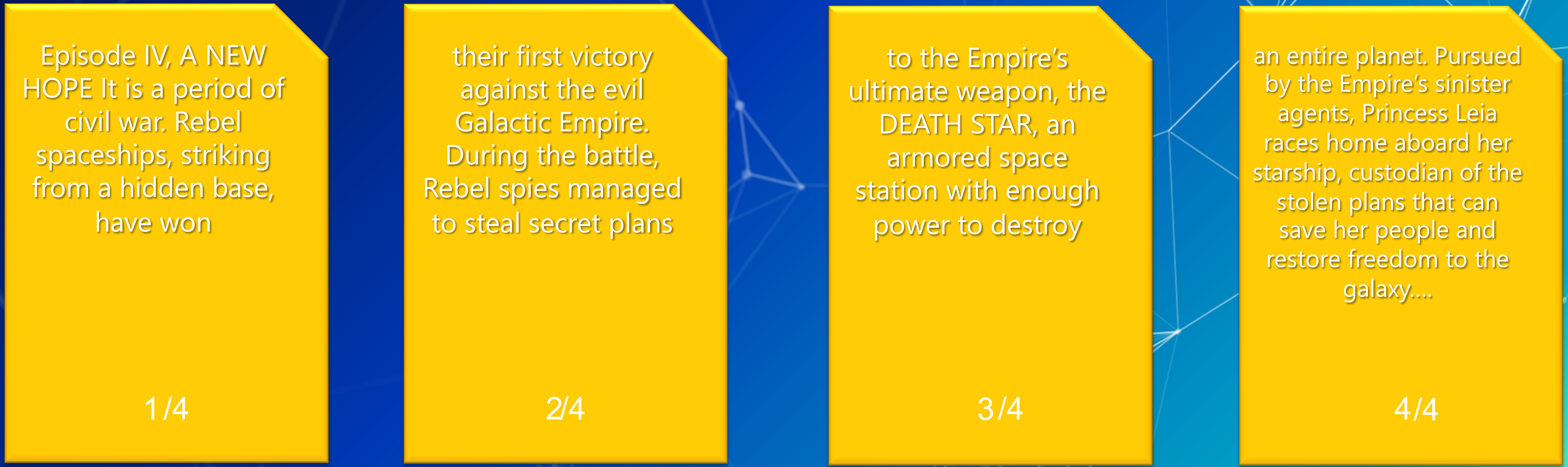
- Network layer protocol is known as the “Internet Protocol” or IP
- IP is an unreliable, connectionless, packet switched protocol.
  - IP's job is to send and route packets to other routers / computers.
  - IP packets are independent entities and may arrive out of order or not at all.
  - IP does not guarantee packet delivery.
  - A series of diagnostic tools exist at the IP layer, the Internet Control Messaging Protocol ICMP. (“ping” and “traceroute”.)
- Advantages:
  - More tolerant to failures
  - Better utilization of an internet connection
- Disadvantages:
  - Packets may arrive out of order
  - Packets may not arrive at all!
  - Controlled chaos from a messaging perspective
- What about Encryption

The Flow of Internet Data at the Transport Layer



Breaking a Message Down Into Packets

Episode IV, A NEW HOPE It is a period of civil war. Rebel spaceships, striking from a hidden base, have won their first victory against the evil Galactic Empire. During the battle, Rebel spies managed to steal secret plans to the Empire's ultimate weapon, the DEATH STAR, an armored space station with enough power to destroy an entire planet. Pursued by the Empire's sinister agents, Princess Leia races home aboard her starship, custodian of the stolen plans that can save her people and restore freedom to the galaxy….



Episode IV, A NEW HOPE It is a period of civil war. Rebel spaceships, striking from a hidden base, have won

1 /4

their first victory against the evil Galactic Empire. During the battle, Rebel spies managed to steal secret plans

2/4

to the Empire's ultimate weapon, the DEATH STAR, an armored space station with enough power to destroy

3 /4

an entire planet. Pursued by the Empire's sinister agents, Princess Leia races home aboard her starship, custodian of the stolen plans that can save her people and restore freedom to the galaxy….

4 /4

The Transport Layer

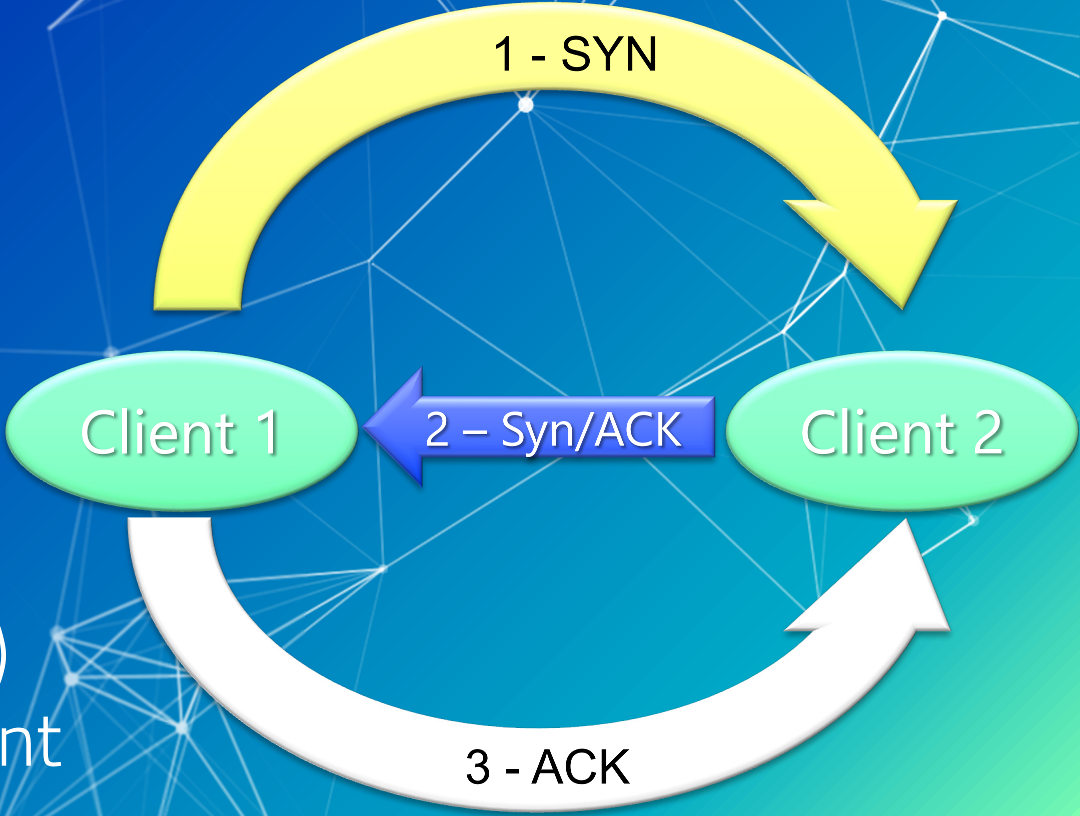
- Your application passes information on to the Transport layer to be broken up in to manageable chunks called packets.
  - Information is added to the packet headers for re-assembly.
    - Sequencing numbers
    - Session IDs
- The Transport layer is a connection-oriented, message switched, reliable, byte stream service.
  - Connection-oriented means:
    - semi-permanent connection is established before any useful data can be transferred
    - a stream of data is delivered in the same order as it was sent
  - TCP must first establish a connection before exchanging data (a handshake).
  - For each packet received, an acknowledgement is sent to the sender.
- Three way handshake to establish a connection
  - TCP SYN, SYN ACK, ACK / SYN-ACK-ACK

The Transport Layer

- The Transport layer, using the Transmission Control Protocol (TCP) takes care of breaking application messages into chunks, known as **packets** and assigning information such as:
  - Port number - help to separate what data is destined to which applications.
    - Email and Web browsers have a specific, unique port number
    - The builds a socket. Ex – 192.168.100.2:25
  - Number of packets sent.
  - The number the packet in the series being sent.
  - Packet sequencing numbers.
  - On the receiving end the TCP protocol helps to arrange packets as they arrive in the correct order for the applications.
  - Provides SSL for whole-session encryption
- A cousin of TCP, User Datagram Protocol (UDP) is commonly used for streaming. A connectionless, unreliable protocol

The Transport Layer

- TCP header flags:
  - Three way handshake to establish a connection
    - SYN – requests synchronization with new sequencing numbers
    - SYN ACK
    - ACK / SYN-ACK-ACK – acknowledges synchronization or shutdown request.
  - RST causes immediate disconnection
  - FIN requests graceful shutdown
- Security Implications:
  - Headers can be used:
    - To perpetrate attacks
    - Provide telemetry for monitoring tools such as Intrusion detection systems (IDS)
  - First layer in the TCP/IP stack to implement Encryption



The TCP/IP Protocol Stack

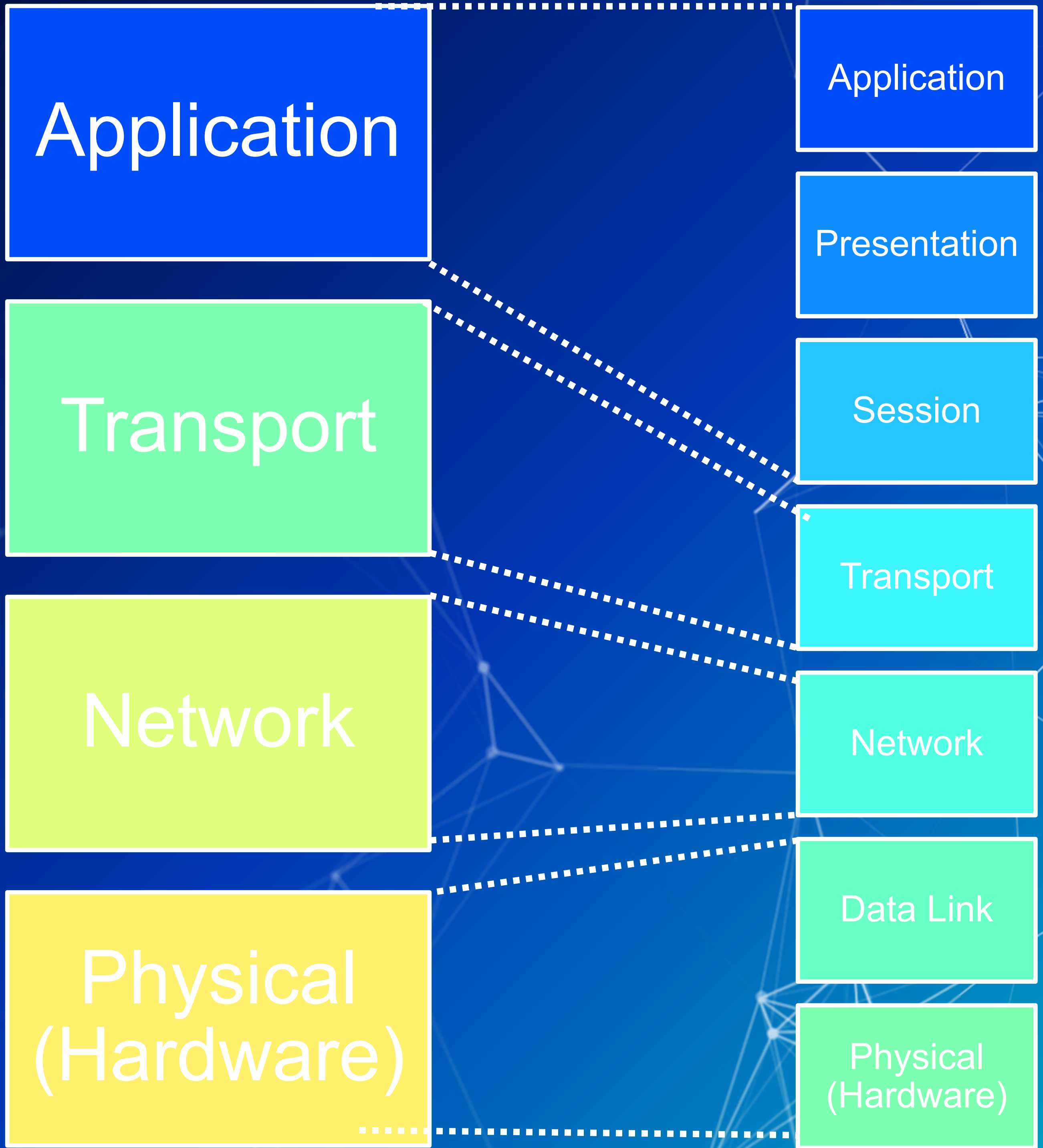
“Please do not throw sausage pizza away”

- Application
- Transport
- Network
- Physical (Hardware)

The OSI Model

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical (Hardware)

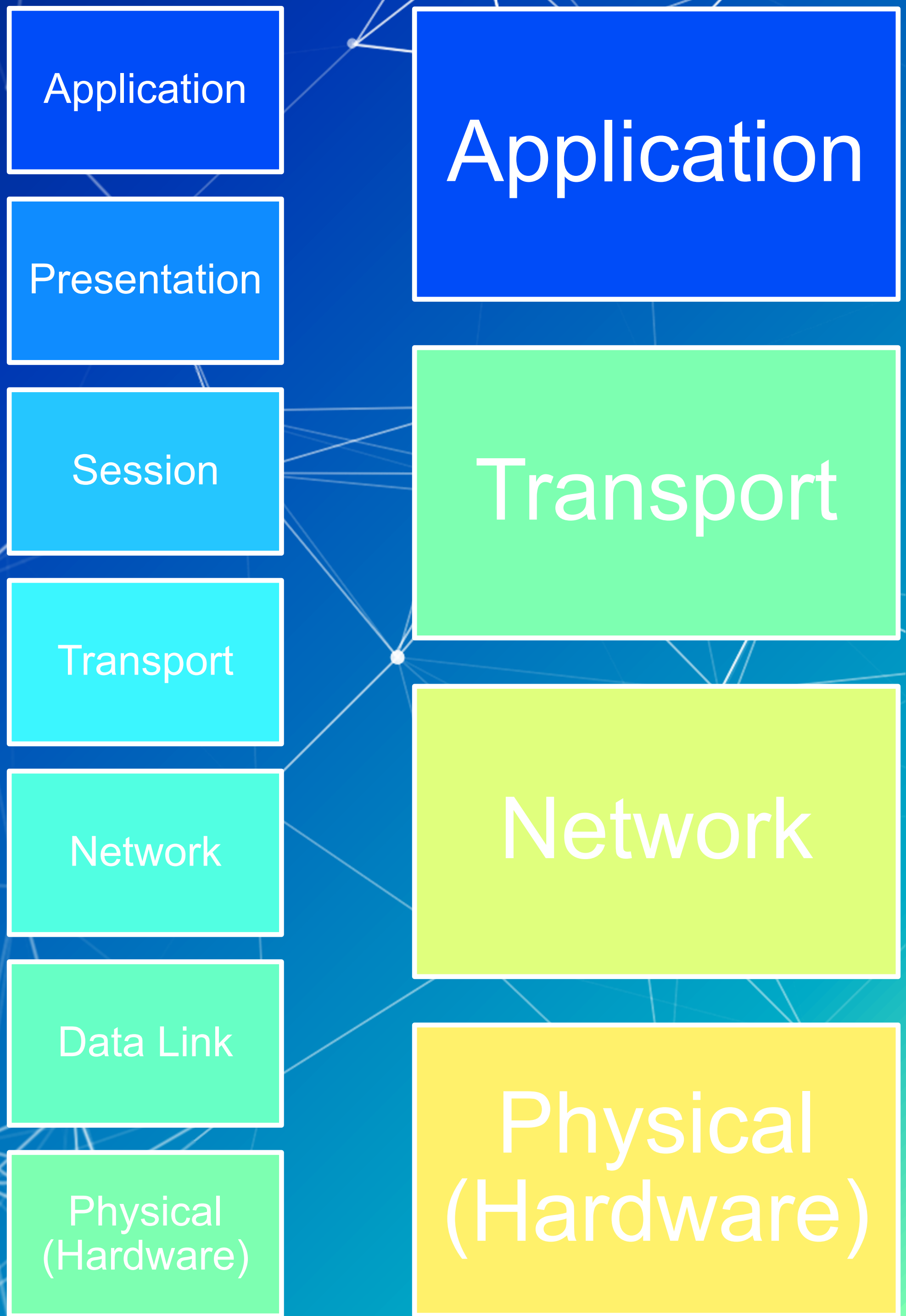
The TCP/IP Protocol Stack



The OSI Model

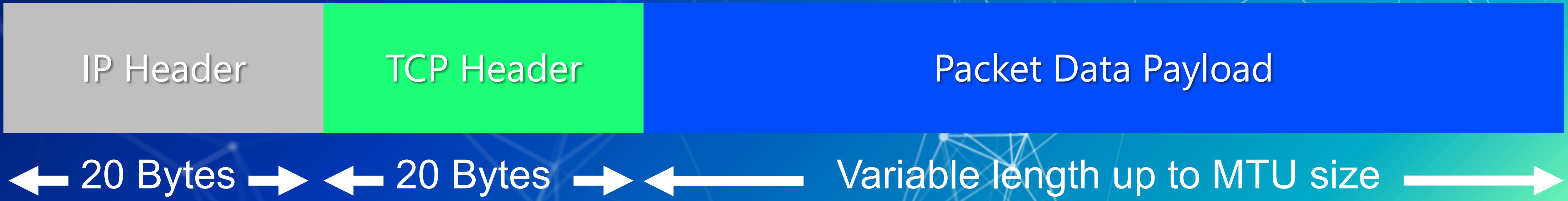
A Word on TLS Encryption and OSI

- Transport Layer Security (TLS) has replaced Secure Sockets Layer (SSL) to provide end to end encrypted connections.
- This all happens at:
  - OSI - the *Session*, *Presentation* and *Application* layers
  - TCP/IP – the *Transport / Application* Layers.
    - HTTP(s), FTP(s), SMTP(s), IMAP(s)
- OSI is just a model! – TLS does not fit neatly inside of it.
- What does this mean for things like firewalls?
- Encryption can happen at (nearly) every layer!



Headers

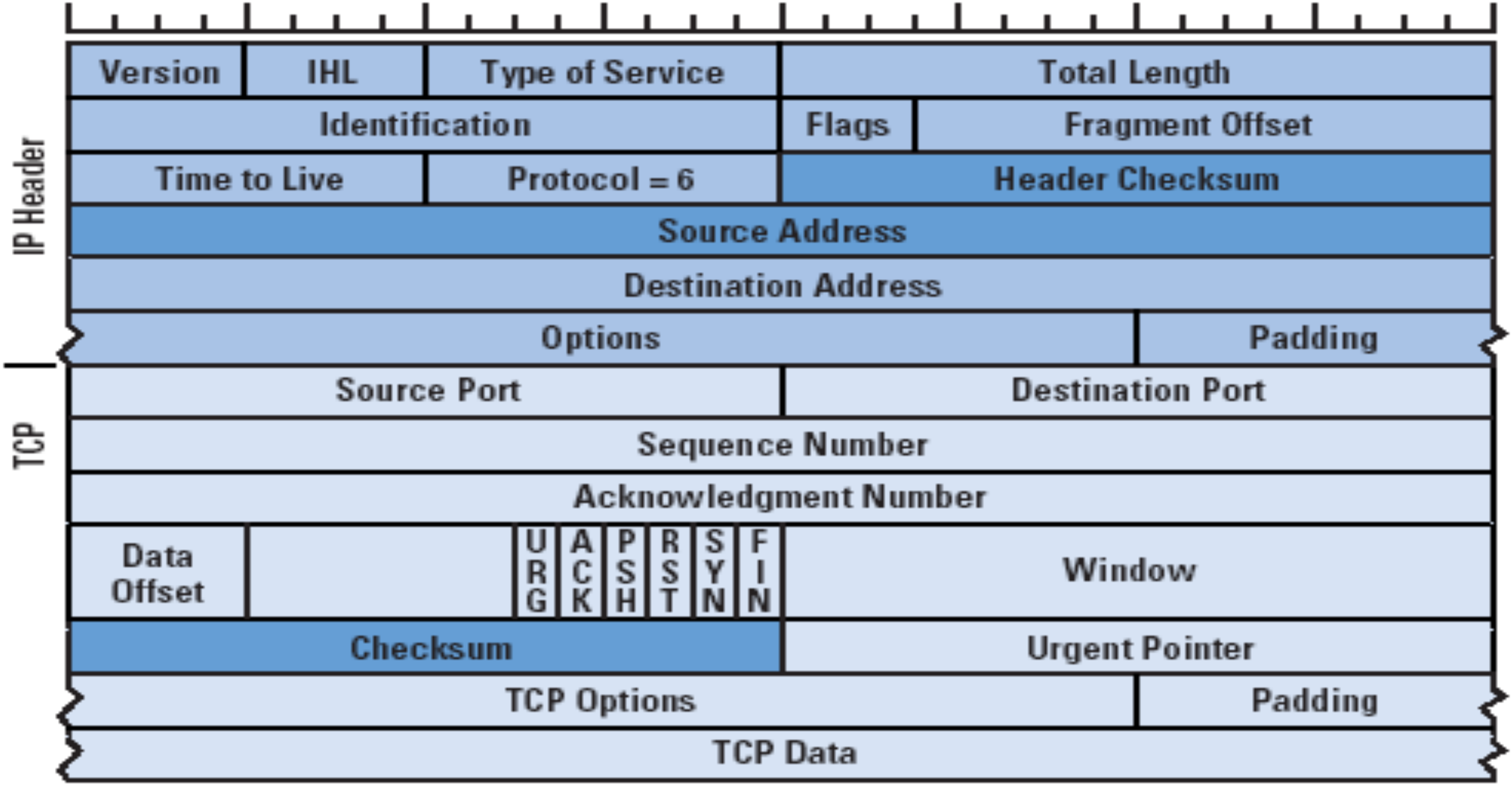
- Each layer of the protocol stack places information and metadata into “packet headers”.
  - This is information needed to deliver and re-order the packet once it has arrived to its destination.
  - Packet data payload is variable length up to the maximum allowable size of a packet. Maximum allowable size is known as the Maximum transmission unit (MTU)
    - Not to be confused with the frame size at the data link layer.
    - Commonly 1500 bytes – 40 bytes of header and 1460 bytes for data
    - “Jumbo” frame MTU can grow as large as 9000 bytes.
  - Header information is very important when it comes to packet capture and analysis done by intrusion detection systems.



IP Header | TCP Header | Packet Data Payload

20 Bytes | 20 Bytes | Variable length up to MTU size

32 bit word size



IP Header

Version | IHL | Type of Service | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol = 6 | Header Checksum

Source Address

Destination Address

Options | Padding

TCP

Source Port | Destination Port

Sequence Number

Acknowledgment Number

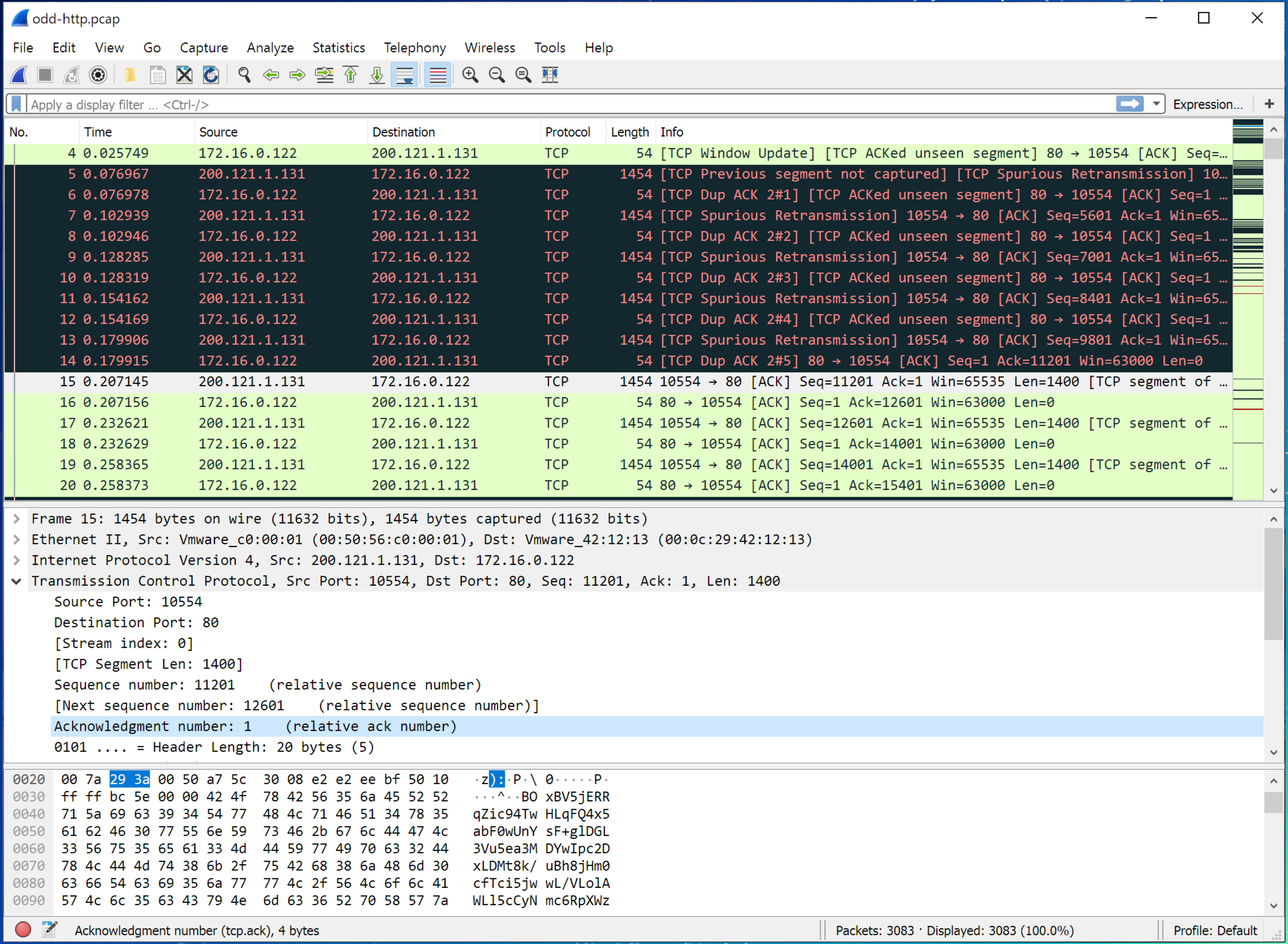
Data Offset | URG | ACK | PSH | RST | SYN | FIN | Window

Checksum | Urgent Pointer

TCP Options | Padding

TCP Data

Wireshark



```
No.  Time      Source        Destination   Protocol Length Info
   4 0.025749  172.16.0.122  200.121.1.131 TCP        54 [TCP Window Update] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=…
   5 0.076967  200.121.1.131 172.16.0.122  TCP      1454 [TCP Previous segment not captured] [TCP Spurious Retransmission] 10…
   6 0.076978  172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#1] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
   7 0.102939  200.121.1.131 172.16.0.122  TCP      1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=5601 Ack=1 Win=65…
   8 0.102946  172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#2] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
   9 0.128285  200.121.1.131 172.16.0.122  TCP      1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=7001 Ack=1 Win=65…
  10 0.128319  172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#3] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
  11 0.154162  200.121.1.131 172.16.0.122  TCP      1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=8401 Ack=1 Win=65…
  12 0.154169  172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#4] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
  13 0.179906  200.121.1.131 172.16.0.122  TCP      1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=9801 Ack=1 Win=65…
  14 0.179915  172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
  15 0.207145  200.121.1.131 172.16.0.122  TCP      1454 10554 → 80 [ACK] Seq=11201 Ack=1 Win=65535 Len=1400 [TCP segment of …
  16 0.207156  172.16.0.122  200.121.1.131 TCP        54 80 → 10554 [ACK] Seq=1 Ack=12601 Win=63000 Len=0
  17 0.232621  200.121.1.131 172.16.0.122  TCP      1454 10554 → 80 [ACK] Seq=12601 Ack=1 Win=65535 Len=1400 [TCP segment of …
  18 0.232629  172.16.0.122  200.121.1.131 TCP        54 80 → 10554 [ACK] Seq=1 Ack=14001 Win=63000 Len=0
  19 0.258365  200.121.1.131 172.16.0.122  TCP      1454 10554 → 80 [ACK] Seq=14001 Ack=1 Win=65535 Len=1400 [TCP segment of …
  20 0.258373  172.16.0.122  200.121.1.131 TCP        54 80 → 10554 [ACK] Seq=1 Ack=15401 Win=63000 Len=0
```

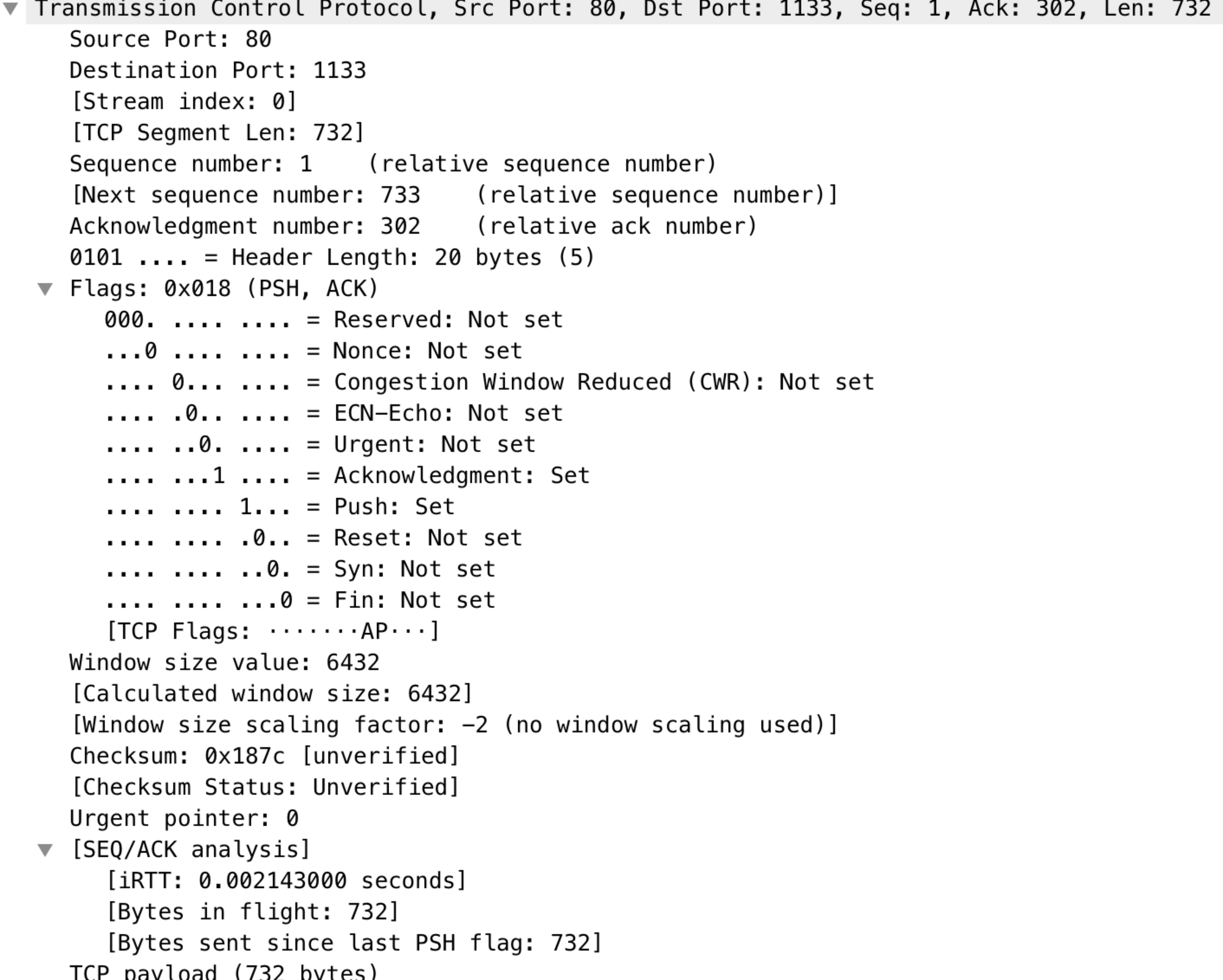
```
> Frame 15: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
> Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
> Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
v Transmission Control Protocol, Src Port: 10554, Dst Port: 80, Seq: 11201, Ack: 1, Len: 1400
    Source Port: 10554
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 1400]
    Sequence number: 11201    (relative sequence number)
    [Next sequence number: 12601    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
```

```
0020  00 7a 29 3a 00 50 a7 5c  30 08 e2 e2 ee bf 50 10   ·z):·P·\ 0·····P·
0030  ff ff bc 5e 00 00 42 4f  78 42 56 35 6a 45 52 52   ···^··BO xBV5jERR
0040  71 5a 69 63 39 34 54 77  48 4c 71 46 51 34 78 35   qZic94Tw HLqFQ4x5
0050  61 62 46 30 77 55 6e 59  73 46 2b 67 6c 44 47 4c   abF0wUnY sF+glDGL
0060  33 56 75 35 65 61 33 4d  44 59 77 49 70 63 32 44   3Vu5ea3M DYwIpc2D
0070  78 4c 44 4d 74 38 6b 2f  75 42 68 38 6a 48 6d 30   xLDMt8k/ uBh8jHm0
0080  63 66 54 63 69 35 6a 77  77 4c 2f 56 4c 6f 6c 41   cfTci5jw wL/VLolA
0090  57 4c 6c 35 63 43 79 4e  6d 63 36 52 70 58 57 7a   WLl5cCyN mc6RpXWz
```

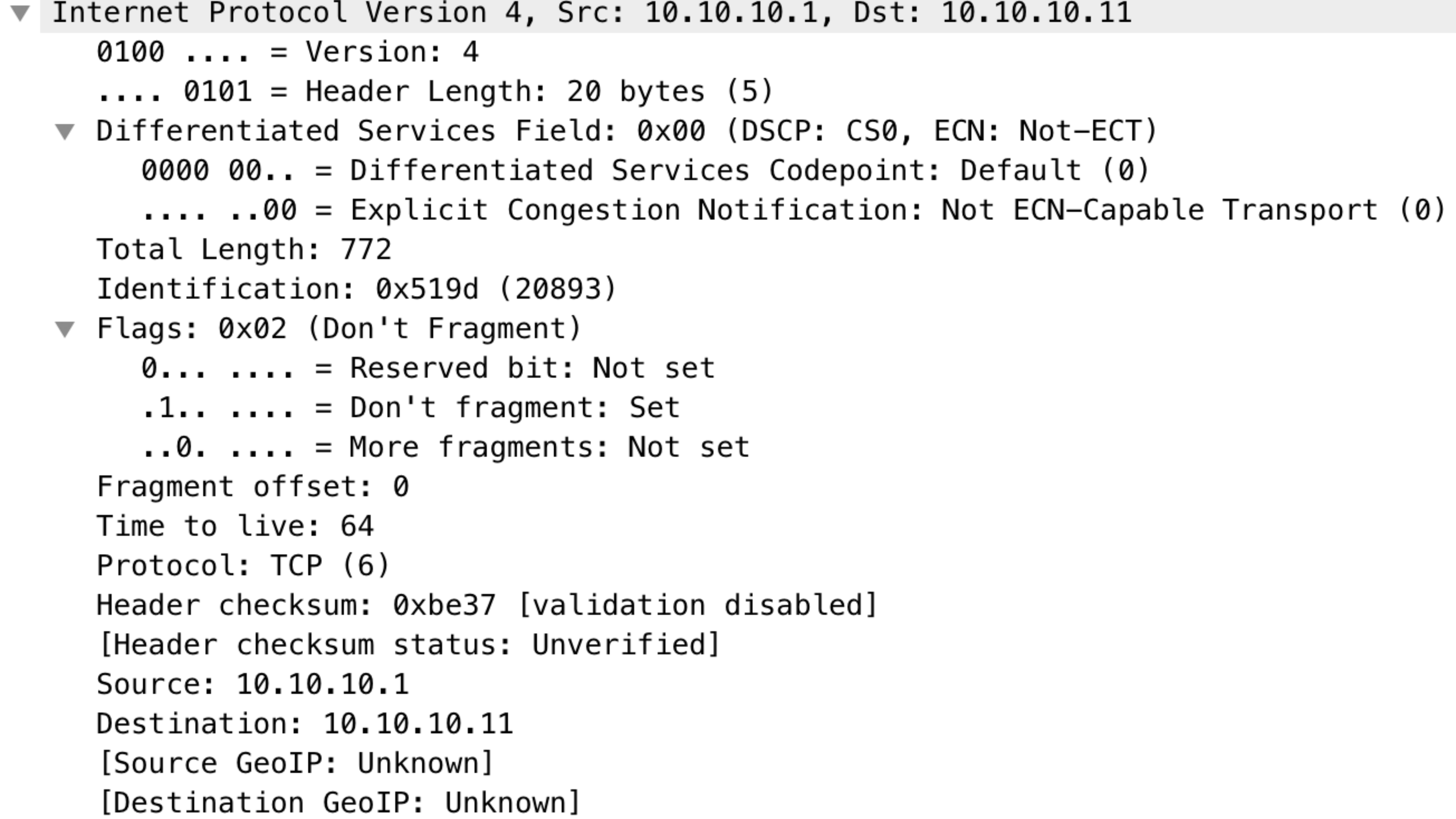
Acknowledgment number (tcp.ack), 4 bytes

Packets: 3083 · Displayed: 3083 (100.0%)

Profile: Default



```
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 1133, Seq: 1, Ack: 302, Len: 732
    Source Port: 80
    Destination Port: 1133
    [Stream index: 0]
    [TCP Segment Len: 732]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 733    (relative sequence number)]
    Acknowledgment number: 302    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▼ Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······AP···]
    Window size value: 6432
    [Calculated window size: 6432]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x187c [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▼ [SEQ/ACK analysis]
      [iRTT: 0.002143000 seconds]
      [Bytes in flight: 732]
      [Bytes sent since last PSH flag: 732]
    TCP payload (732 bytes)
```



```
▼ Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.11
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 772
    Identification: 0x519d (20893)
  ▼ Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xbe37 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.1
    Destination: 10.10.10.11
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

Packet Routing at the Network Layer

- IP packet routing is similar to mailing a letter.
- The steps you take in mailing a letter include…
  - Sealing your message in to an envelope.
  - Looking up the address to write on the envelope.
  - Determine if you can hand deliver your message or if it needs to be given to the mail person.
  - If the mailman must deliver the message you must hand the message off to them. The mailman works with other mailmen to then deliver your envelope.
  - Wait for a response.

STILLWATER MUNICIPAL AIRPORT
Stillwater, Oklahoma
Home of Oklahoma A. and M. College

Dedication October 13, 1930
By Hon. Patrick J. Hurley, Secretary of War

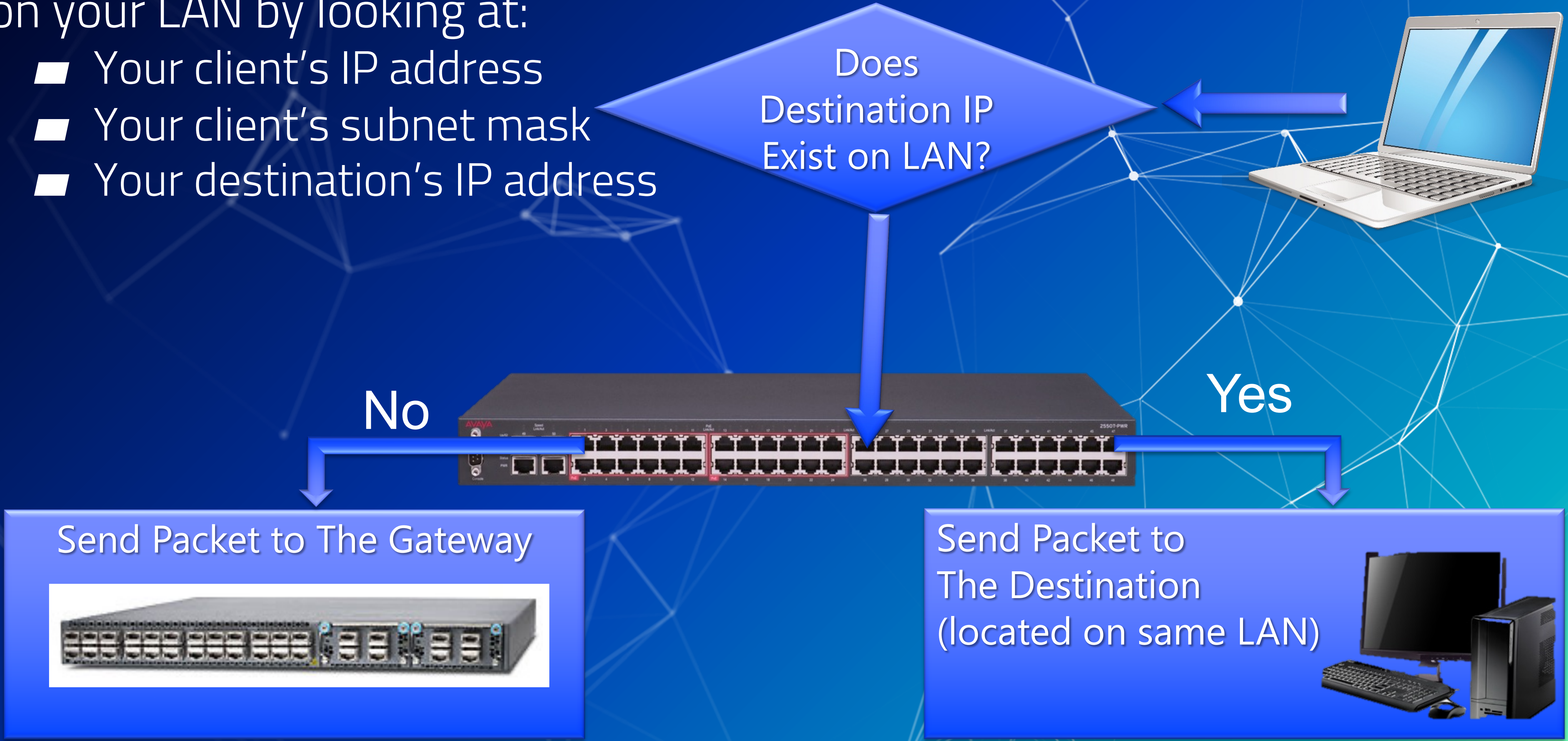
STILLWATER
OCT 13
12 AM
1930
OKLA.

UNITED STATES POSTAGE
5 CENTS 5

IRAS BUNN
250 Rieg Avenue
Conneaut, Ohio.

The Flow of Internet Data

- The IP layer determines if the client you're sending a packet to resides on your LAN by looking at:
  - Your client's IP address
  - Your client's subnet mask
  - Your destination's IP address



Does Destination IP Exist on LAN?

No

Yes

Send Packet to The Gateway

Send Packet to
The Destination
(located on same LAN)

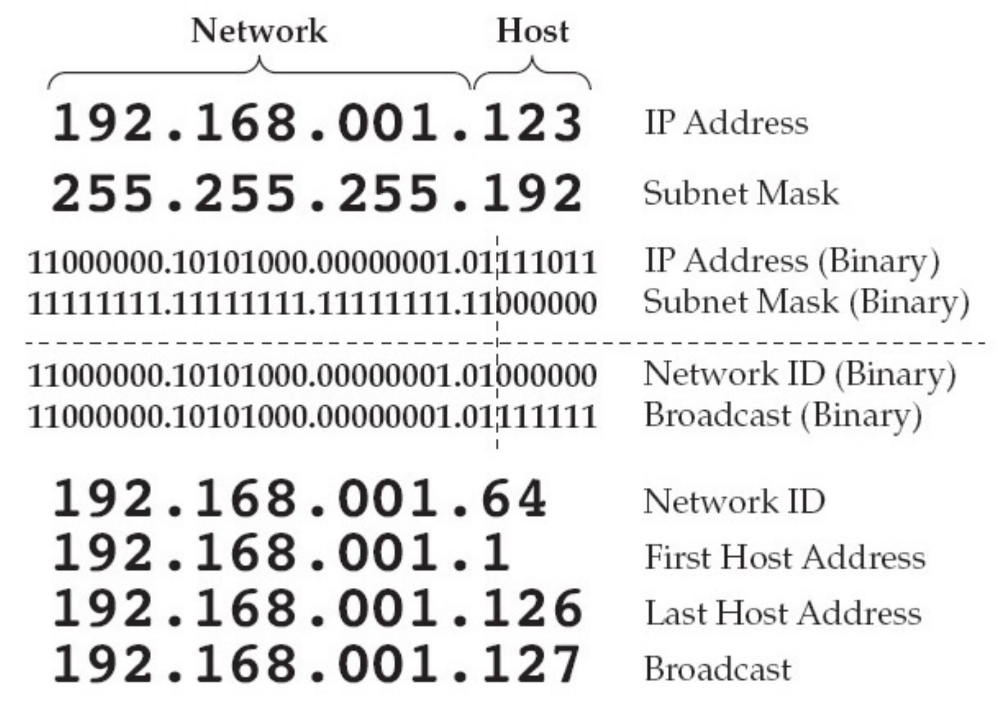
Network – IP Client Information

- To route packets correctly, a device must be configured with:
  - IP address: Every IP address on the internet is unique*:
    - IPV4 - 4 x 8 bit (32 bit) numbers represented in decimal notation separated by '.'s.
      - Ex: 128.205.34.66.
    - IPV6 - 8 x 16 bit (128 bit) alphanumeric addresses in decimal notation separated by '.'s.
      - Ex: 2001:0000:3238:DFE1:63:0000:0000:FEFB
    - IP addresses (To and From) are placed in packet headers, similar to an envelop.
  - Subnet Mask – used to determine the boundaries of a Local Area Network.
    - A subnet mask resembles an IP address. Ex 255.255.255.0
  - Gateway IP Address – where packets destined outside LAN are handed off.
- Some IP ranges are designated as **internal** ranges and are **repeatable**
  - 192.168.0.0 - 192.168.255.255 (65,536 IP addresses) - private
  - 172.16.0.0 - 172.31.255.255 (1,048,576 IP addresses) - private
  - 10.0.0.0 - 10.255.255.255 (16,777,216 IP addresses) – private
  - 127.0.0.1 -127.255.255.255 – loopback (testing and troubleshooting)

Network – Subnetwork Ranges

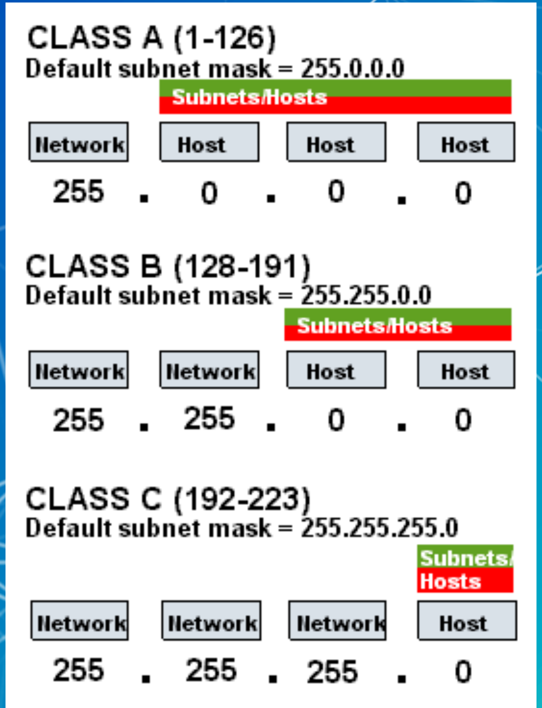
- Networks usually come in several sizes (number of addresses that can be assigned to hosts)

Class	Range	Network Address	Host Address	Number of Hosts
A	1.0.0.0 – 126.0.0.0	xxx	xxx.xxx.xxx	16,777,214
B	128.0.0.0 - 191.255.0.0	xxx.xxx	xxx.xxx	65,534
C	192.0.1.0- 223.255.255.255	xxx.xxx.xxx	xxx	254



Network	Host

192.168.001.123	IP Address
255.255.255.192	Subnet Mask
11000000.10101000.00000001.01111011	IP Address (Binary)
11111111.11111111.11111111.11000000	Subnet Mask (Binary)
11000000.10101000.00000001.01000000	Network ID (Binary)
11000000.10101000.00000001.01111111	Broadcast (Binary)
192.168.001.64	Network ID
192.168.001.1	First Host Address
192.168.001.126	Last Host Address
192.168.001.127	Broadcast



CLASS A (1-126)
Default subnet mask = 255.0.0.0
Subnets/Hosts

Network	Host	Host	Host
255 .	0 .	0 .	0

CLASS B (128-191)
Default subnet mask = 255.255.0.0
Subnets/Hosts

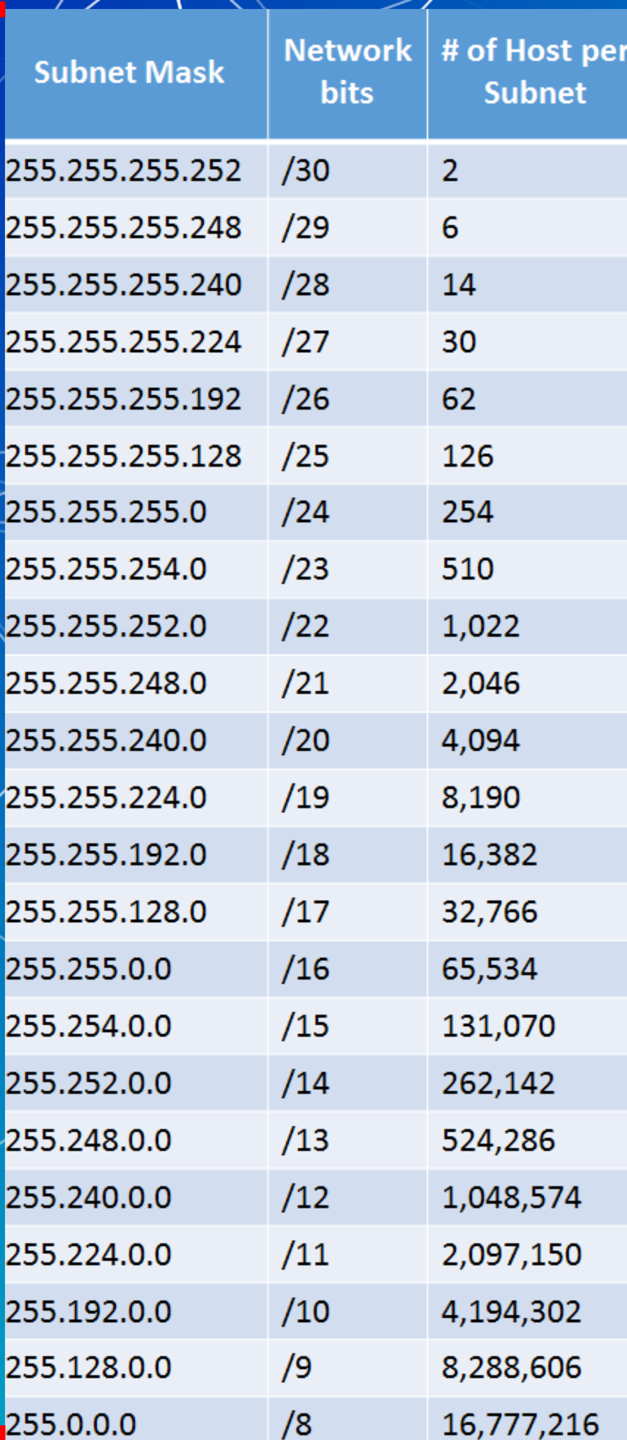
Network	Network	Host	Host
255 .	255 .	0 .	0

CLASS C (192-223)
Default subnet mask = 255.255.255.0
Subnets/Hosts

Network	Network	Network	Host
255 .	255 .	255 .	0

Subnetwork Ranges

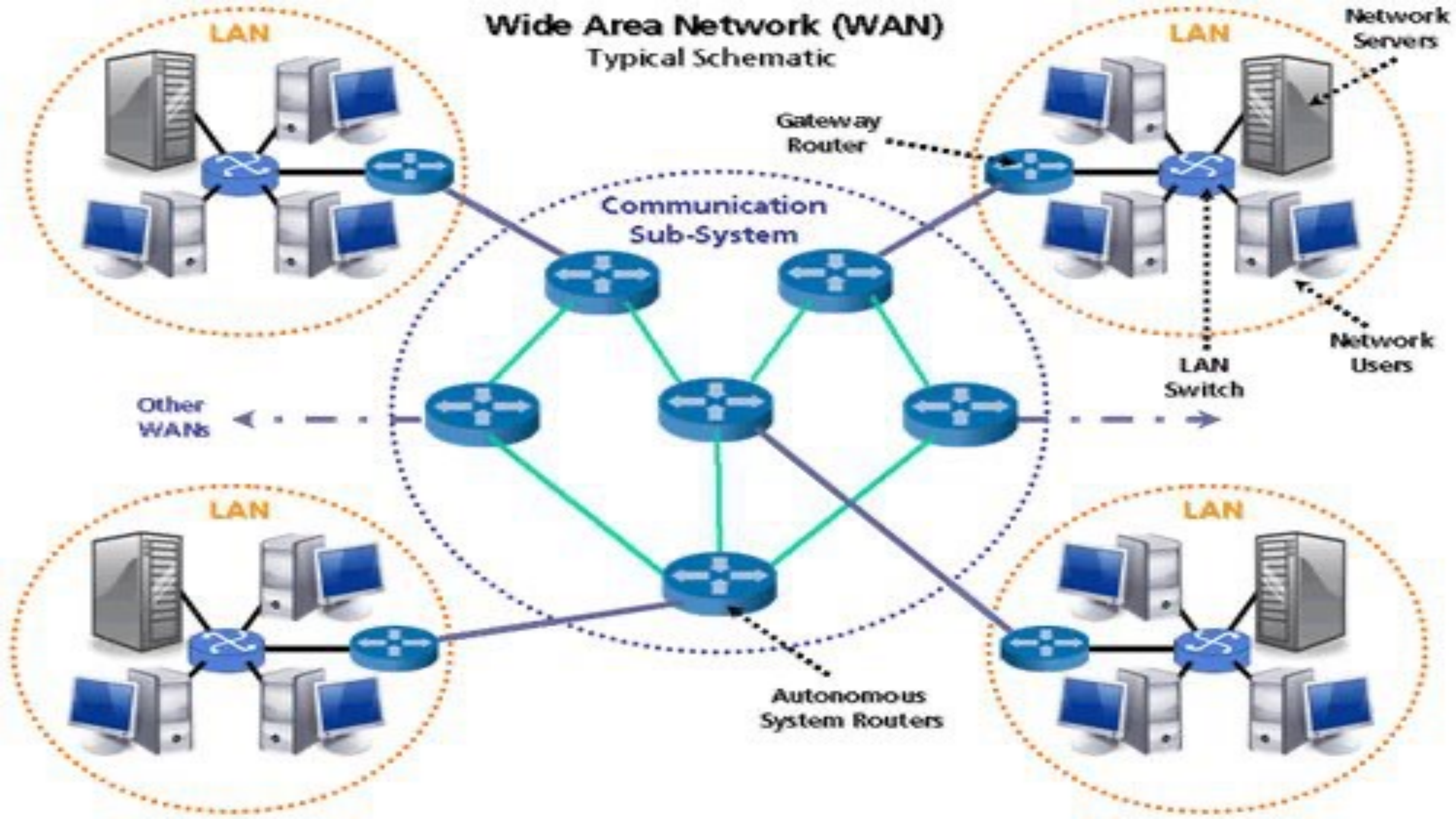
- But… subnet defaults can be adjusted!
  - https://www.calculator.net/ip-subnet-calculator.html
- In practice, by adjusting the subnet mask, we can have much more granular control over the size, number and topology of our networks.
- More subnets means more segmentation!!! (more to come on that)
- Most enterprise networks will use combinations of:
  - Public addresses (For Servers)
  - Private addresses (For endpoints, IoT, printers, etc)
  - NAT'ing (For endpoints, IoT, printers, etc)



Subnet Mask	Network bits	# of Host per Subnet
255.255.255.252	/30	2
255.255.255.248	/29	6
255.255.255.240	/28	14
255.255.255.224	/27	30
255.255.255.192	/26	62
255.255.255.128	/25	126
255.255.255.0	/24	254
255.255.254.0	/23	510
255.255.252.0	/22	1,022
255.255.248.0	/21	2,046
255.255.240.0	/20	4,094
255.255.224.0	/19	8,190
255.255.192.0	/18	16,382
255.255.128.0	/17	32,766
255.255.0.0	/16	65,534
255.254.0.0	/15	131,070
255.252.0.0	/14	262,142
255.248.0.0	/13	524,286
255.240.0.0	/12	1,048,574
255.224.0.0	/11	2,097,150
255.192.0.0	/10	4,194,302
255.128.0.0	/9	8,288,606
255.0.0.0	/8	16,777,216

Wide Area Network (WAN)

Typical Schematic

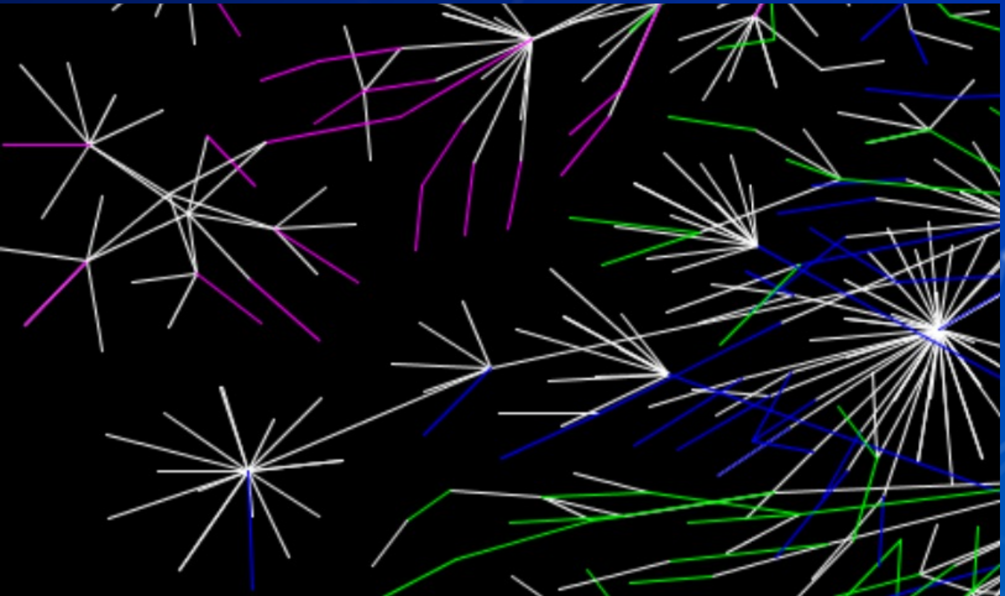


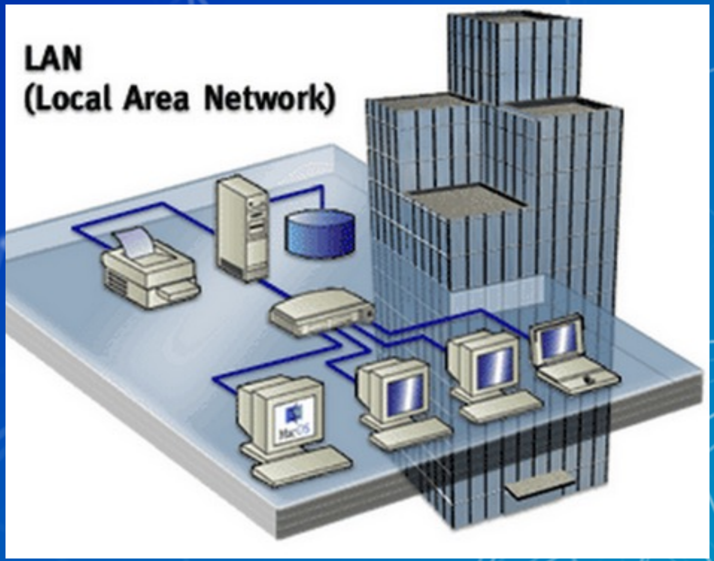
The Flow of Internet Data at the Network Layer

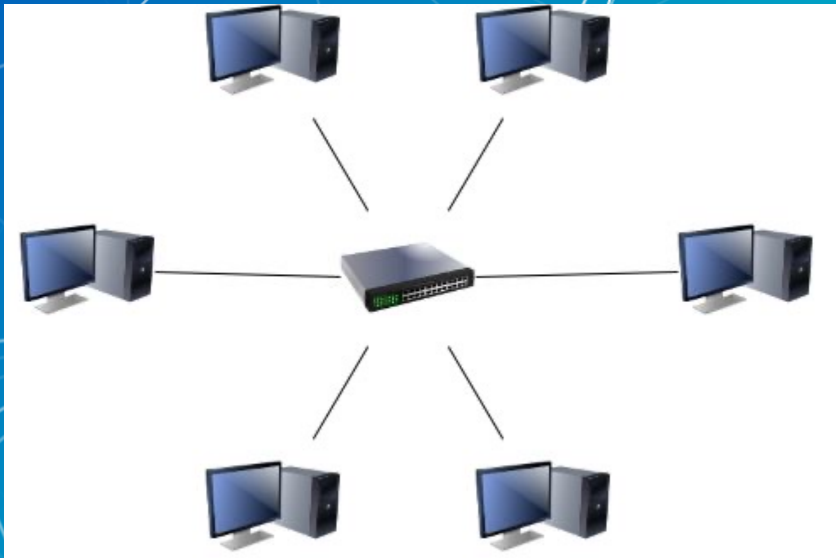
- Gateways will communicate with one or more other gateways and devices called “routers”.
  - Routers are usually connected between subnets and take care of handing off massive amounts of packets.
  - Gateways make convenient locations for Firewall and Monitoring measures.
- Routers maintain multiple connections to one another.
  - Use the following protocols – RIP, OSPF, IS-IS, IGRP, BGP.
- Routers constantly keep track of other routers around them.
  - They will look at things like link speeds, delay times, network congestion.
  - Routers are connected to “backbones”. Backbones are the information super highways of the internet.
- Routers have a role in security but are not security devices.
- Key security controls at network layer:
  - Firewalls!
  - IDS Sensors

Local Area Networks (Subnets)

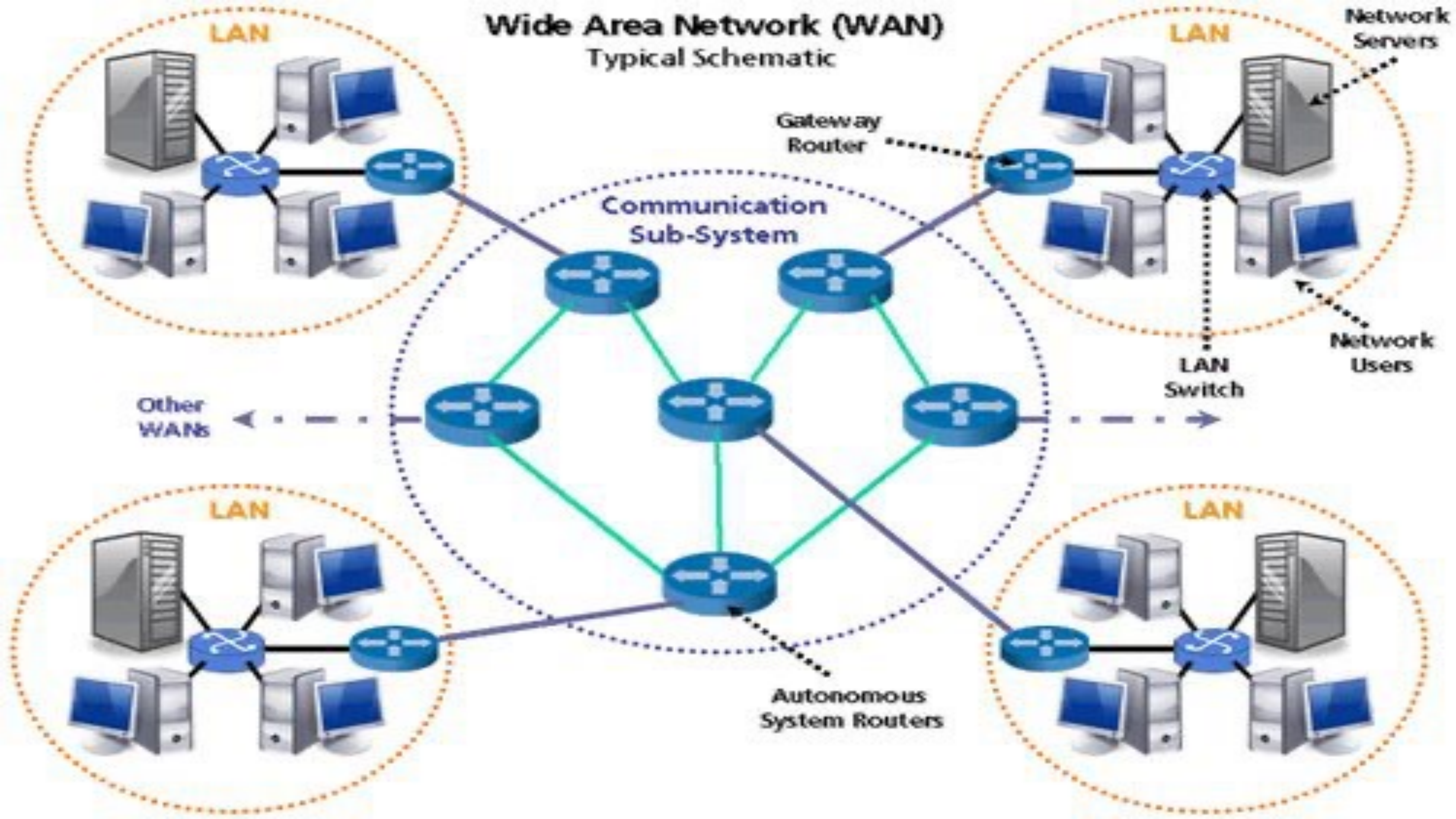
- LANs are the most basic type of network.
  - These small networks are the building blocks of the Internet!
  - Can be thought of as a "local neighborhood" of computers or devices.
  - All devices on the same LAN communicate directly with one another across a "switch" (collision domain).
  - LAN communication DOES NOT require a gateway.
  - Tend to be more "local"







Lockdown
Fall’ 2023

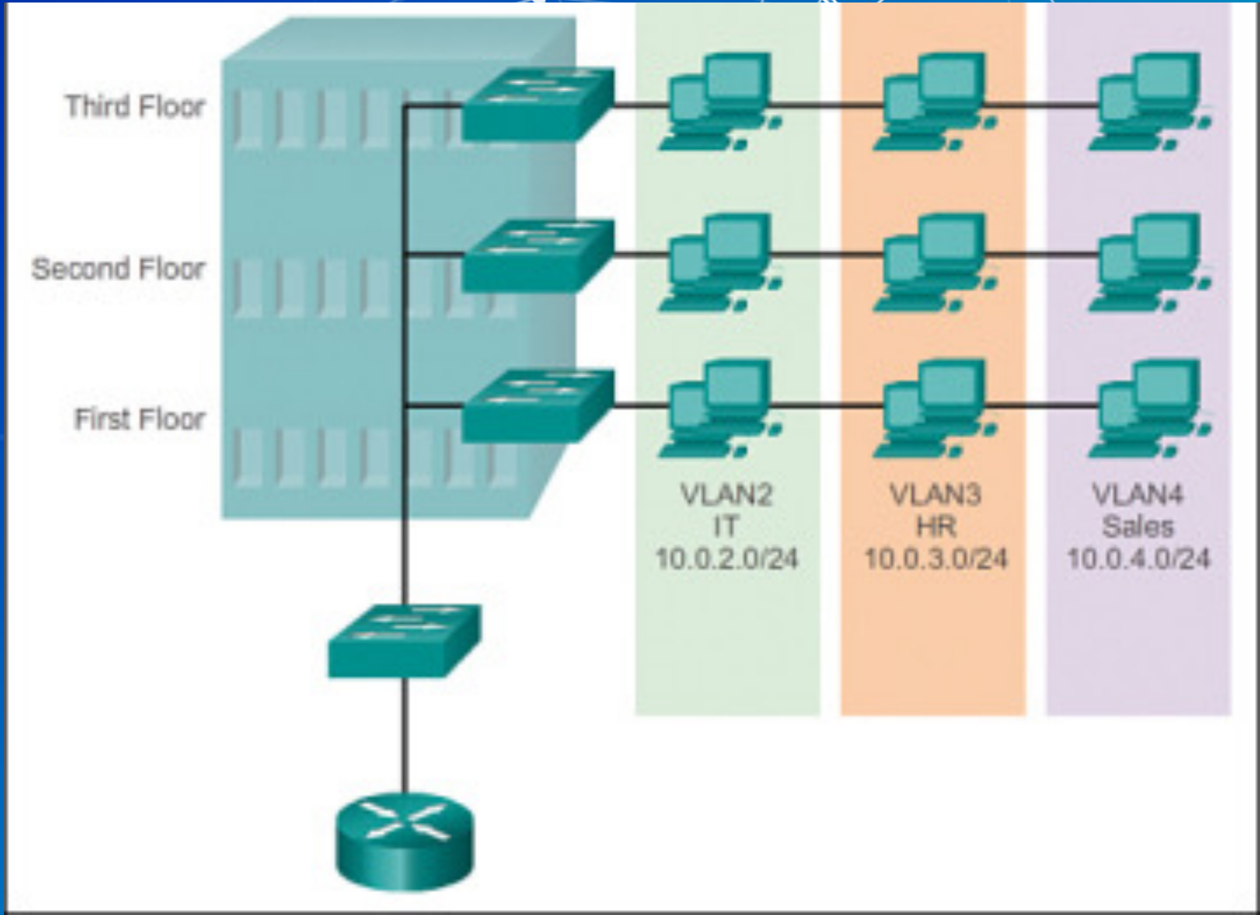

Wide Area Network (WAN)
Typical Schematic
LAN
LAN
Network Servers
Gateway Router
Communication Sub-System
Network Users
LAN Switch
Other WANs
LAN
LAN
Autonomous System Routers

Wide Area Networks

- LANs are interconnected together to form WANs
- LANs get connected to WANs through routers and gateways.
  - Which make them ore expensive to configure and manage.
- The "Internet" is one big WAN.
- We can connect LANs to WANs through both wireless and Wired Connections.
- WANs can span much larger geographic distances than LANs.
- WANs typically boast higher speed connections for each LAN member.
- It's typical and necessary for enterprise IT operations to have many LANs interconnected.
- WANs may be defined by their geographic reach
  - CAN – Campus Area Network
  - PAN – Personal Area Network
  - MAN – Metropolitan Area Network
  - * but these are just fancy names for WANs.

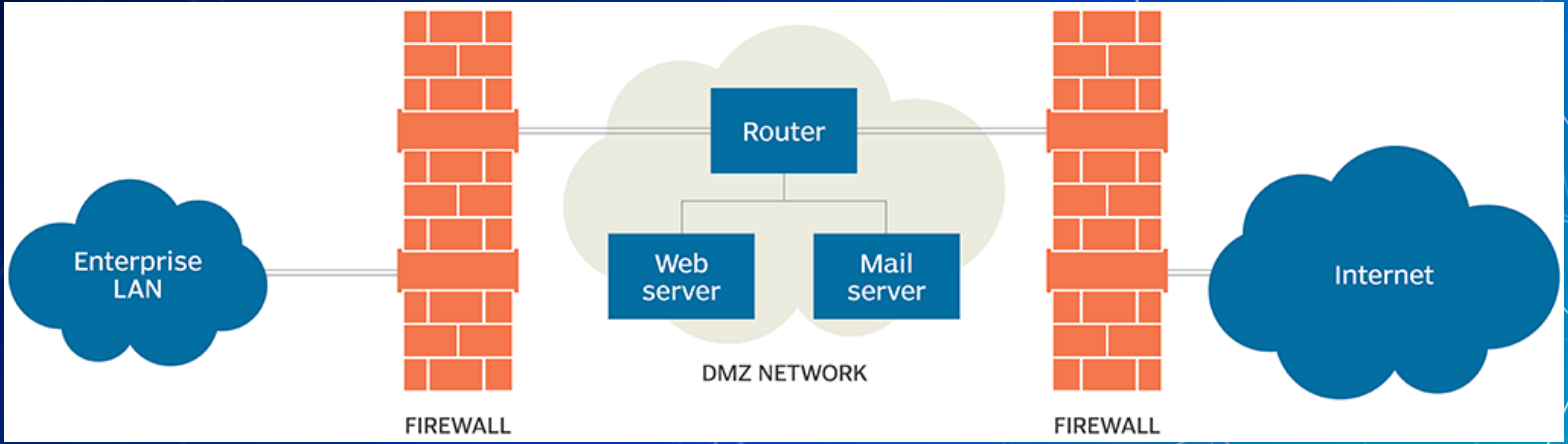
Network Segmentation and Topology

- Network and LAN segmentation is a fundamental security concept.
- Segmenting a network:
  - Limits the broadcast reach of devices on a subnetwork
  - Enables additional firewalls to be placed at the boundary of each network
- LANs can be organized by :
  - Geographic area
  - Device type / Function
  - Administrative boundary
  - Data or work classification
  - Department or entity
  - Type of service.
- Air-Gapping is the ultimate in Network segmentation!



Network Segmentation and Topology

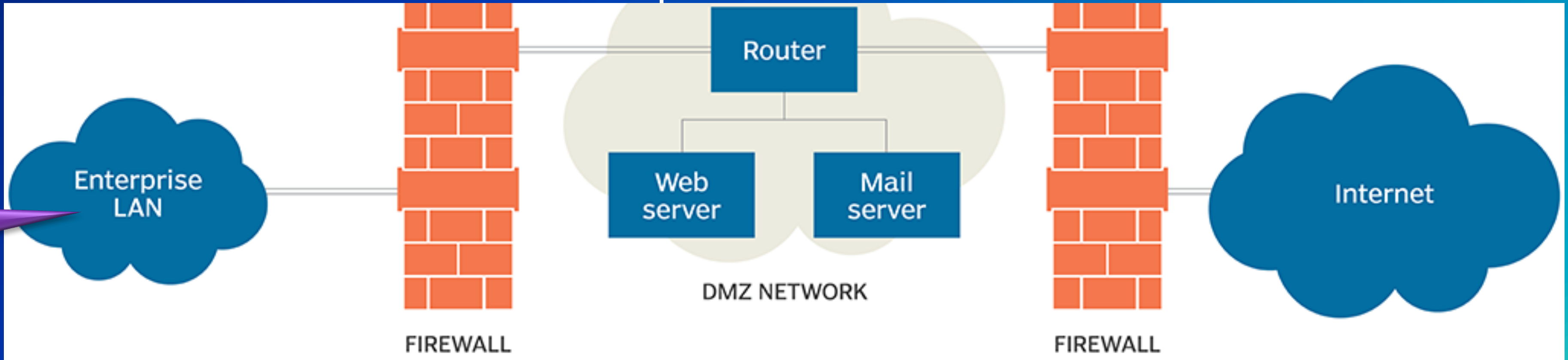
- Demilitarized Zone (DMZ) - Networks considered less secure but not totally insecure land in the DMZ



- DON’T DO THIS

Network Segmentation and Topology

- Demilitarized Zone (DMZ) - a perimeter or screened subnetwork
  - Allows an organization to expose external facing services to untrusted networks (The internet) while ensuring protected networks remains secure.
  - What actually is a “DMZ”? Networks:
    - with external-facing services and resources, accessible from the Internet
    - that are isolated and given limited access to other internal networks.
    - considered less secure but not totally insecure land in the “DMZ”?
    - that proxy services and requests to internal, more secure, networks.
  - Are more highly monitored with tighter controls
  - Functions as isolated network positioned between the Internet and internal nets.



Only one LAN?

Network Segmentation and Topology

- What about:

Guest Networks

WiFi

Smartphones

0-Trust Architecture?

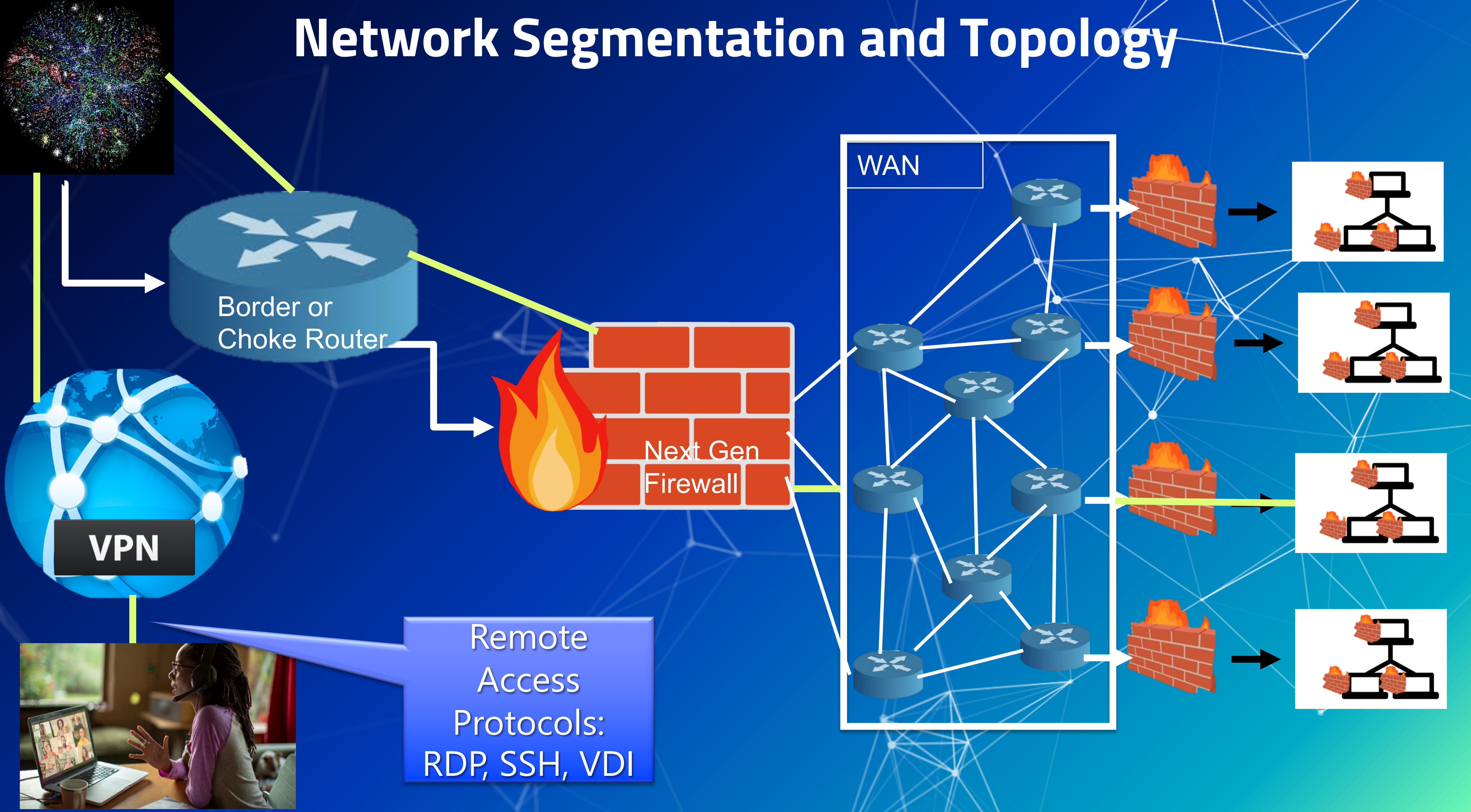
Trust No One!

0-Trust Architectures

0 – Trust Architectures

- Strategic info-sec approach:
  - Eliminate implicit trust relationships (such as your network location)
  - Validate at every stage of an interaction
    - Continual or multiple authentication challenges
  - Never trust, always verify
    - using strong authentication methods (Privileged access management, multifactor)
    - leveraging network segmentation to preventing lateral movement
    - providing Layer 7 (application) threat prevention
    - simplifying and supporting granular, “least access” privileges
- Don’t make the assumption that *everything inside your network is secure*.
- So – What did this mean for our networks?

Network Segmentation and Topology



Remote Access Protocols: RDP, SSH, VDI

Network Segmentation and Topology

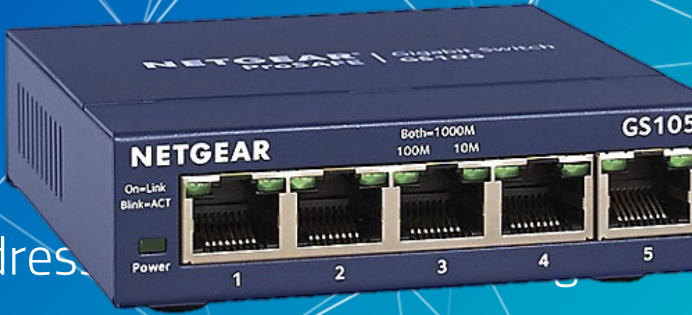
- Multiple "Edge" networks should exist, based on access needs
  - Separate networks (edge and internal) for discrete services.
  - Sensitive servers are not directly open to the world
  - Traffic into a server or service is handled via proxy servers or load balancers which then interact with back-end servers.
  - Provides a layer of security as this restricts the ability of bad actors to directly access internal servers and data via the Internet.
  - Pinhole firewall rules should be leveraged to provide only the minimum requires access – **Remember the importance of "Least Privilege".**
- Enterprise services should be placed on separate subnetworks based on type of service and need for access.
- Disparate WFH clients should tunnel into secure network segments through VPN connections. (Full Tunnel vs Split Tunnel)

The Data Link (Hardware) Layer

- The “hardware“ layer (AKA “Data Link Layer”) is in charge of transmitting data over a physical medium (wired or wireless).
- The physical medium for transmitting data can take on many forms and is implemented with a wide variety of technologies.

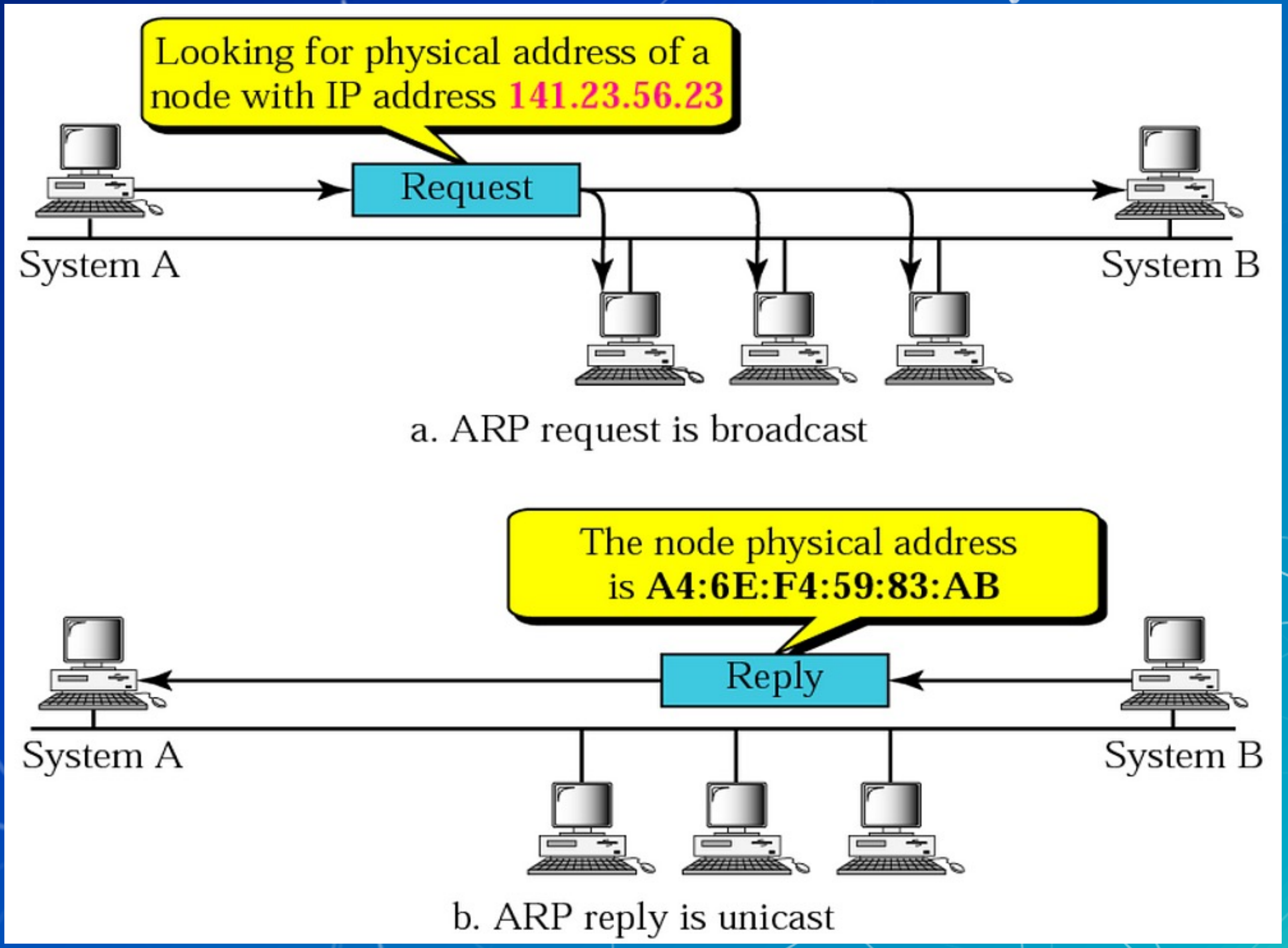
Switches

- Switches - devices that physically connect multiple computers together to form a subnet.
  - Switches join electrical pathways together, so that devices can transmit to each other.
  - Advanced switches support:
    - Virtual Local Area Networks (VLANS)
    - SPANing, TAPing,
    - port filtering
    - Port-based Network Access Control (NAC) for authorized devices
    - Port level security:
      - MAC address flooding (limit # of MACs / port)
      - DHCP spoofing (using trusted ports)
      - Storm control (Broadcast, multicast, unicast)
      - Quality of Service (QoS) queues
      - Dynamic ARP inspection (discard ARP packets with invalid MAC addres
        - Switch loop protection
      - Port activation, deactivation and re-vlan based on IDS monitoring.



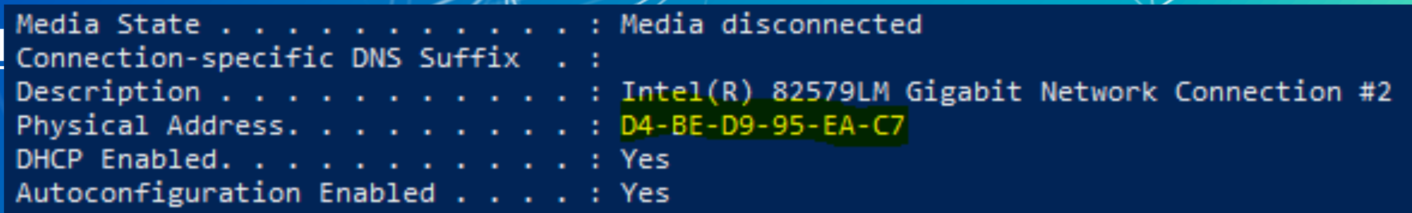
The Data Link (Hardware) Layer

- All network interface cards (NICs) have a hardware address called a “MAC” address, or “Media Access Control Address”.
  - hardcoded on the NIC and *usually* cannot be changed.
  - MAC address is used when delivering messages within subnet, by the switch.
- Possible for a MAC address to have multiple IP addresses bound to it.
- The binding between MAC and IP address is handled through “Address Resolution Protocol” (ARP).
- Your machine will only use ARP to communicate with other devices on you own subnet.


Looking for physical address of a node with IP address 141.23.56.23
Request
System A
System B
The node physical address is A4:6E:F4:59:83:AB
Reply
System A
System B

a. ARP request is broadcast

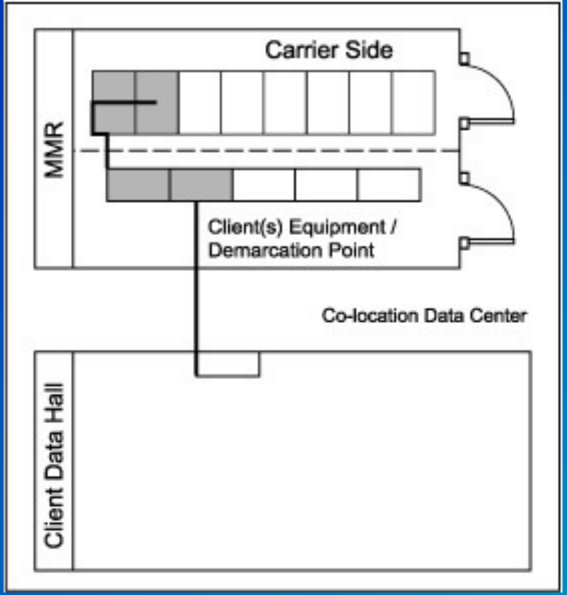
b. ARP reply is unicast

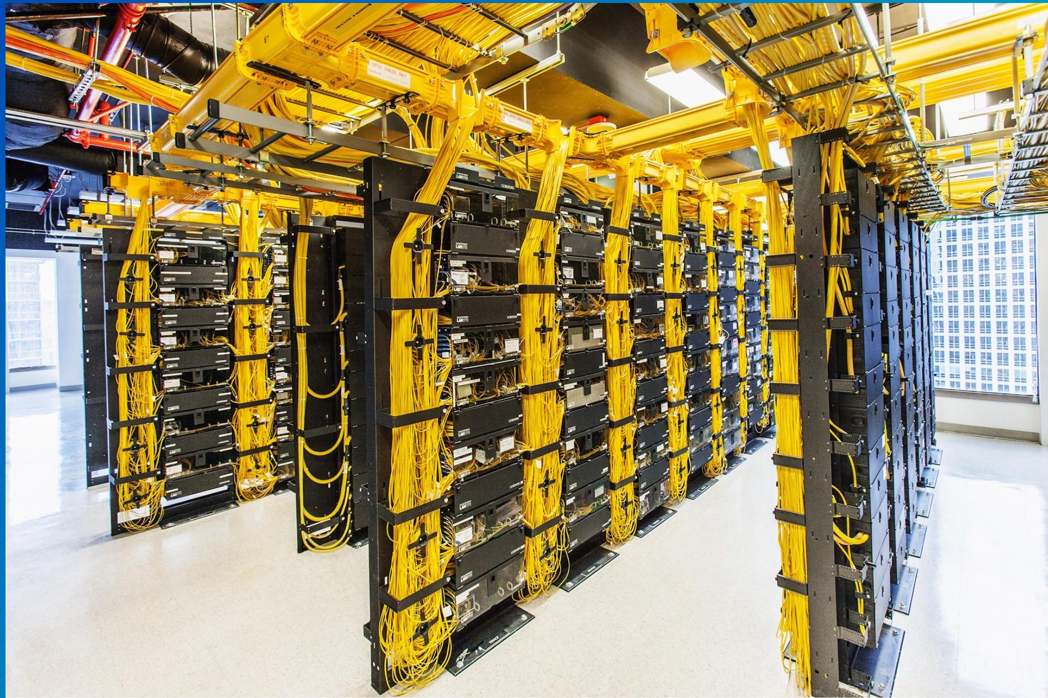


```
Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connection #2
Physical Address. . . . . . . . . : D4-BE-D9-95-EA-C7
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Physical Network Security Management

- Network devices such as routers, firewalls switches should be hardened to standards and configuration baseline.
  - Controlled versioning
  - Automated configuration and management
  - Vulnerability management and patching
  - Change management for config changes
  - Inventory management
  - Account and credential management
  - Secured remote access
- It is important to physically secure:
  - Network cabling
  - Devices and demarcation locations (entrance rooms, distribution areas, wiring





Physical Network Security Management