

Chapter 2

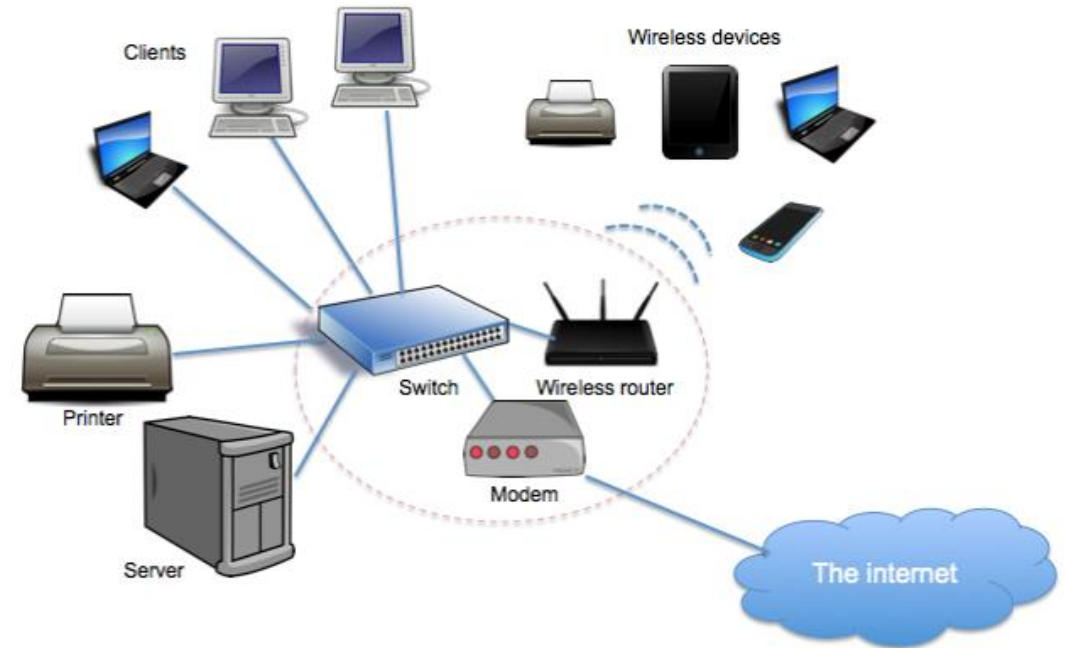
Network and Security

Outline

- Need for Network
- Importance of Networking in Cybersecurity
- Cyber Attribution
- Network Security Concern
- Understanding Network Basics
 - node, server, client, circuit, cabling, NIC, protocols, hubs, switches, routers,
- Types of network
- IP, Port, socket, localhost
- OSI and TCP/IP model
- Network Protocols
 - ARP, TCP, UDP, DNS, DHCP, NAT, IPv4/v6, TCP
- Using TCP Utilities
 - Ping, Ipconfig, Traceroute, netstat
- Understand and Analyze Packet
 - Pcap file, Wireshark, tshark, tcpdump

What is Network?

- A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data and resources
- An example of a network is the Internet, which connects millions of people all over the world



Why do we Need Networks?

- Enhance Communication

- Information can be sent to a larger audience in an extremely fast and efficient manner. e.g., emails, instant messaging, video-conferencing

- Enable users to share resources

- Using network-connected peripheral devices like printers, scanners and copiers, or sharing software between multiple users, saves money

- Facilitate centralized management

- More control on network, user authentication and management

- Backup

- Storing information in one centralized database to improve data security



Importance of Networking in Cybersecurity

- Secure and reliable network infrastructure is the foundation for secure digital communication
- Identifying Threat Source
 - Networks are common entry points for cyberattacks (e.g., phishing, DDoS, MITM)
 - Understanding protocols (TCP/IP, DNS, etc.) helps pinpoint weaknesses
- Configuring and Managing Network Security Tools
 - Firewalls, intrusion detection/prevention systems (IDS/IPS), and routers
 - Proper setup minimizes risk from external and internal threats
- Monitoring and Incident Response
 - Understanding network traffic patterns helps detect anomalies
 - Faster identification and mitigation of attacks like malware and ransomware

Importance of Networking in Cybersecurity

➤ Regulatory Compliance

- Many industries require secure network configurations for compliance (e.g., GDPR, HIPAA)
- Ensures organizations meet legal and ethical standards

➤ Emerging Technologies

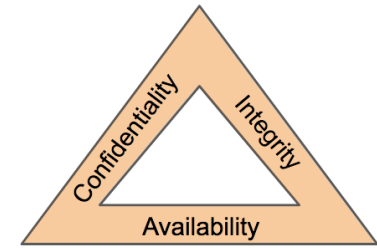
- Networks underpin IoT, cloud computing, and edge computing
- Securing these technologies requires expertise in network dynamics

➤ Career Opportunities

- Cybersecurity professionals often work in roles requiring network expertise
- Roles include Network Security Analyst, Ethical Hacker, and Security Architect

This is where “cool things” happen

Network Concerns



- Cost
 - High Initial Investment (Network cabling, servers, and devices)
 - Ongoing Maintenance (updates, repairs, and monitoring)
- Maintenance and support
 - Requires regular monitoring/maintenance of hardware and software
 - Requires skilled network administrator
 - Downtime Risk
- Security Risk
 - MITM, DoS, DDoS, Phishing, viruses, Social Engineering
- Privacy Concerns
 - Administrator Access, Continues Monitoring
- Scalability Challenges
 - Hardware Limitations, performance bottleneck

1

SECURITY RISKS INVOLVED

DEPENDENCY ON TECHNOLOGY

2

3

POTENTIAL FOR DATA LOSS

NETWORK CONGESTION ISSUES

4

5

INCREASED MAINTENANCE REQUIREMENTS

HIGH INITIAL SETUP COSTS

6

7

DIFFICULTY IN TROUBLESHOOTING

Cyber Attribution

- Cyber attribution is the process which security analysts collect evidence, build timelines, and attempt to piece together evidence in the wake of a cyberattack to identify the responsible organization/individuals
- Networking knowledge is critical to understanding cyber attribution problem
- Why Cyber Attribution is a problem?



Watch: [Accountability in Cyberspace: The Problem of Attribution](#)

Why Cyber attribution is a problem?

- Anonymous Actors
 - Use of anonymity tools
 - Difficulty in identifying true source
- False Flag Operations
 - Deliberate planting of misleading evidence
 - Incorrect attributions due to deception
- Rapidly Evolving Tactics
 - Constantly changing cyber landscape
 - Difficulty in keeping up with new techniques
- Limited Forensic Evidence
 - Effective attacker cover-up
 - Minimal traces for identification



[Source: Homepage - Osservatorio Balcani e Caucaso Transeuropa](#)

Why is Cyber Attribution Important?

Accountability

- Holding the responsible parties accountable for the damage caused by a cyberattack, use legal actions and sanctions

Deterrence

- Identifying attackers acts as a deterrent for future cyberattacks by discouraging attackers from operating with freedom

Response Strategy

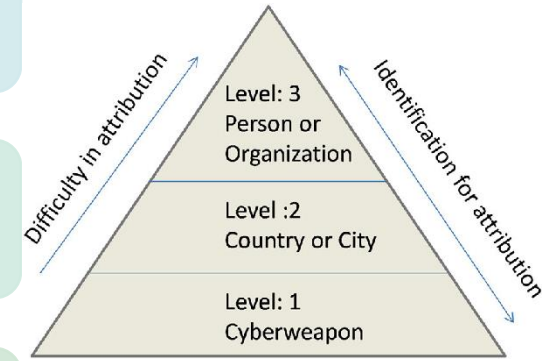
- Knowing who is behind the attack can help determine the appropriate response, whether it's a defensive action, legal action, or retaliation (in cases involving nation-state attacks)

Enhancing Security Measures

- Knowing the identity and tactics of attackers helps organizations refine their security strategies, protect from future threat

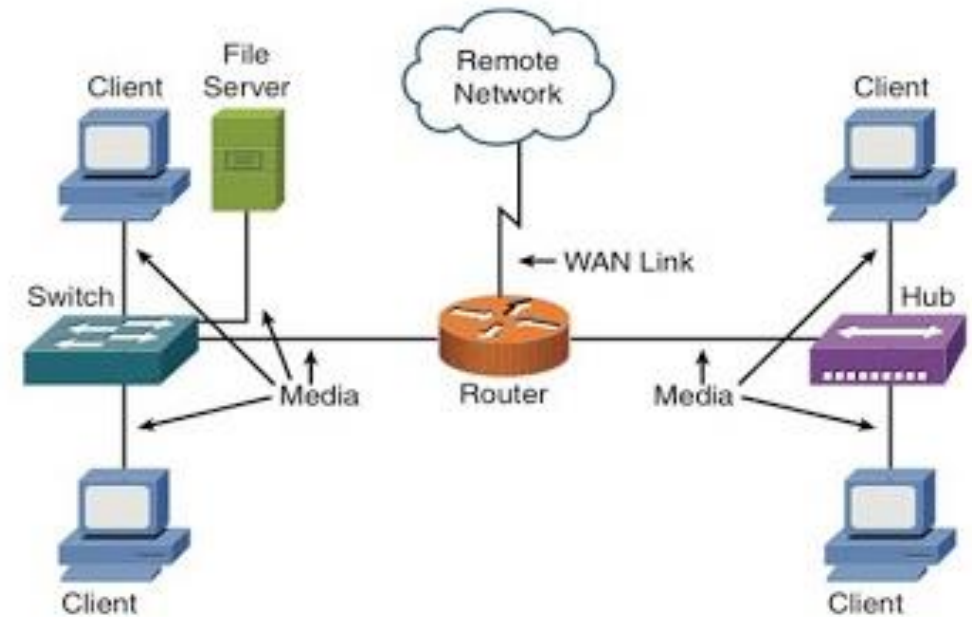
Understanding Threat Actors and Building Trust

- Understanding threat actor, building trust and accountability between stakeholders, including governments, organizations, and the public



Understanding Network Basics

- Network node
 - Any system or device connected to a network is called a node
 - Routers, switches, hubs, servers, and printers
 - Any device connecting over Wi-Fi or Ethernet
 - Nodes must have some form of identification, like an IP address or MAC address
- Network components:
 - Server(s)
 - Includes microcomputers and mainframes
 - Clients
 - PCs
 - A circuit or network system
 - Path over which servers and clients communicate



A Typical Network

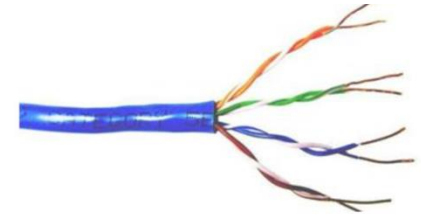
Understanding Network Components

- Circuit components

1. Cable

- **Copper wire:** twisted pair and coaxial cable
- **Fiber-optic:** glass fibers transmit information using light signals

- Unshielded twisted pair (UTP)



- Shielded twisted pair (STP)



- Coaxial cable



- Fiber optic



Fiber-optic is the most secure because it cannot be tapped like the other three copper-based cables; it does not emit EMI

Coaxial Cable



- transmission of signals happens in the electrical form over the inner conductor of the cable
- higher noise immunity than twisted-pair cable
- moderate cost
- moderately high bandwidth
- low attenuation
- easy to install
- get disturbed by external magnetic field

Twisted-Pair Cable



- transmission of signals happens in the electrical form over the metallic conducting wires
- low noise immunity
- cheapest
- low bandwidth
- very high attenuation
- easy to install
- get disturbed by external magnetic field

Fiber-Optic Cable



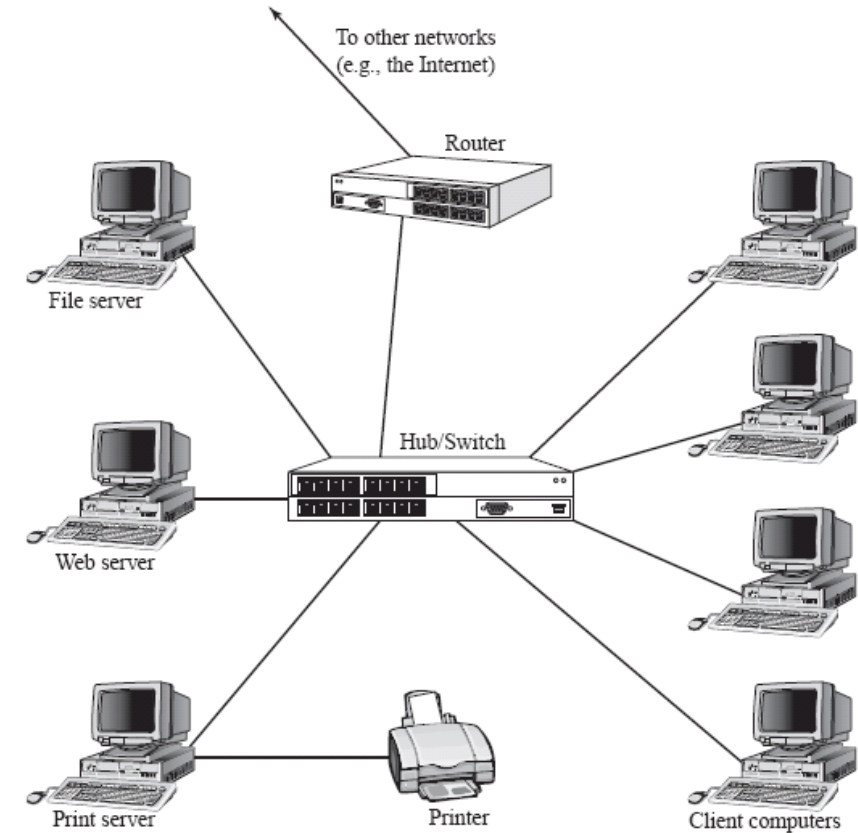
- signal transmission happens in optical forms over a glass fiber
- highest noise immunity
- expensive
- very high bandwidth
- very low attenuation
- difficult to install
- not affected by the external magnetic field
- most efficient
- glass fiber

Understanding Network Components



2. Router

- Device that routes data packets based on their IP addresses
- Shares information with other routers in network
- Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets
- **Forwarding**: process of moving packets from input to output port
- **Fragmentation**: break up or divide larger packets into smaller ones called fragments

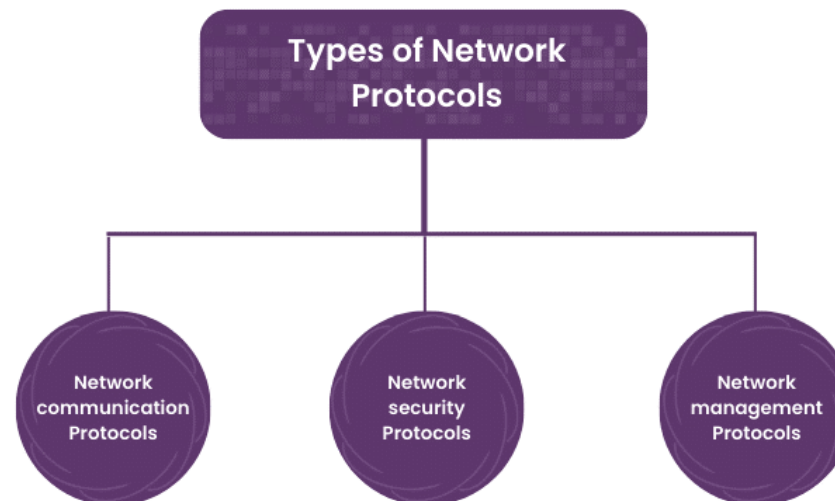


Understanding Network Components

3. Switches, Hubs, Bridges, Gateways

4. Protocols

- A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network
- HTTP, IP, FTP, SMTP, DNS, TCP, UDP
- IPsec, TLS
- ICMP, DHCP, SNMP



Types of Networks (categorized by size)

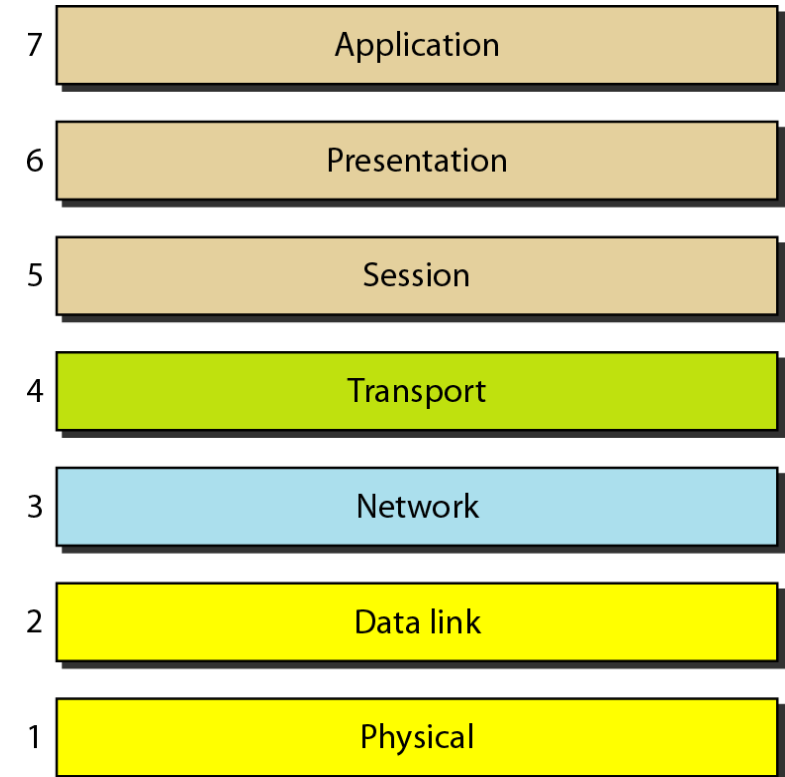
- Personal area network (PAN)
- Local area network (LAN)
- Campus area network (CAN)
- Metropolitan Area area network (MAN)
- Wide area network (WAN)



OSI Model

- Conceptual framework that describes networking
- Seven-layer reference model
- Developed by ISO subcommittee in 1947 and released in 1984
- Networks rarely based strictly on OSI model
- OSI Model was devised before OSI protocols were specified which makes it very general
- Used to describe other models

Please Do Not Tell Secret Password to Anyone



7. Application

- Provides a user interface

6. Presentation

- Presents Data
- Handles encryption and decryption

5. Session

- Maintains distinction between data of separate applications
- Provides dialog control between hosts

4. Transport

- Provides End-to-End connections
- Provides reliable or unreliable delivery and flow control

3. Network

- Provides Logical Addressing
- Provides Path determination using logical addressing

2. Data Link

- Provides media access and physical addressing

1. Physical

- Converts digital data so that it can be sent over the physical medium
- Moves data between hosts

Read more: <https://www.freeccnastudyguide.com/study-guides/ccna/ch1/1-3-osi-reference-model/>

Watch: https://www.youtube.com/watch?v=-6Uoku-M6oY&ab_channel=JKennethLim

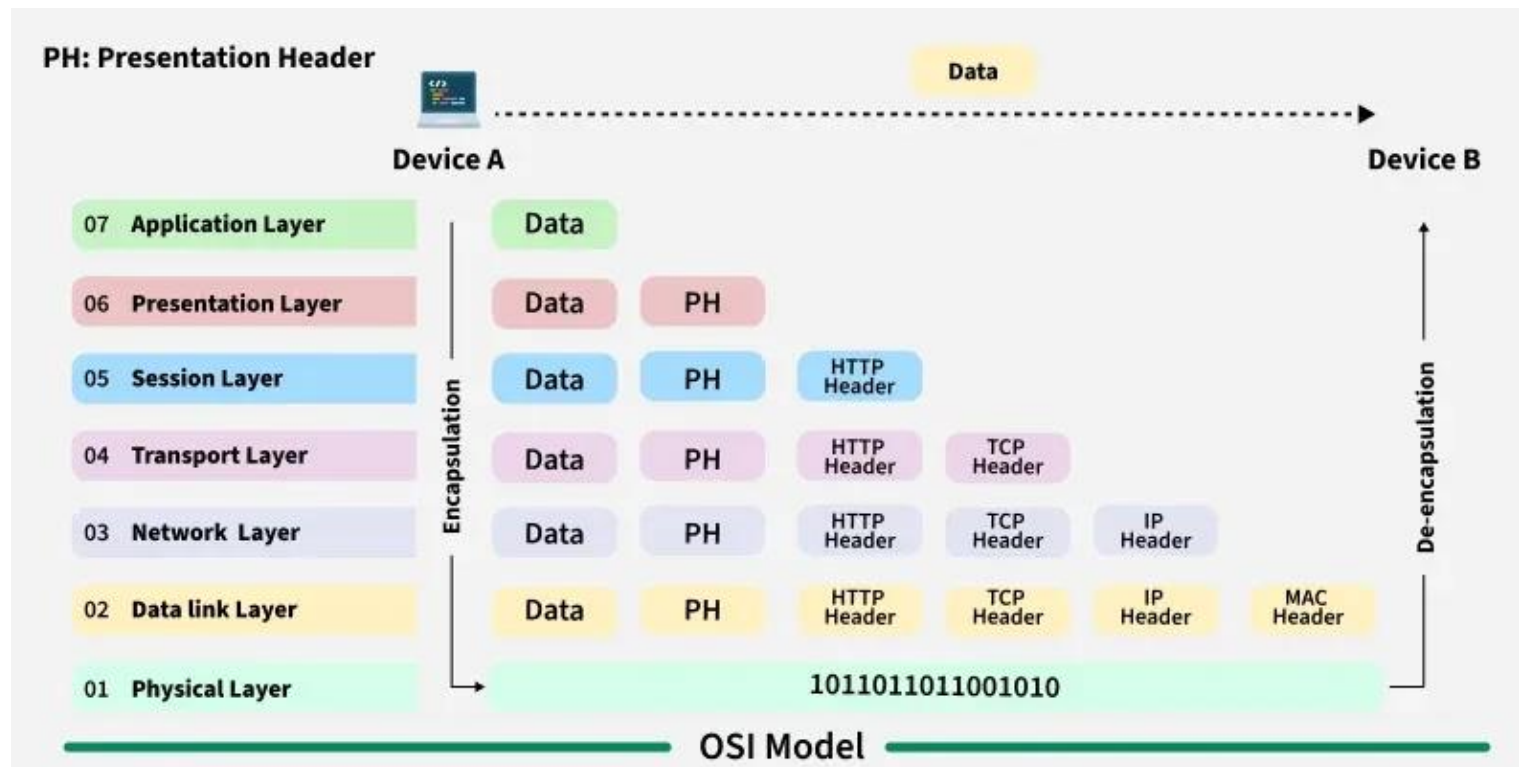
Data Flow in OSI Model

- **Application Layer:** Applications create the data
- **Presentation Layer:** Data is formatted and encrypted
- **Session Layer:** Connections are established and managed
- **Transport Layer:** Data is broken into segments for reliable delivery
- **Network Layer:** Segments are packaged into packets and routed
- **Data Link Layer:** Packets are framed and sent to the next device
- **Physical Layer:** Frames are converted into bits and transmitted physically

Each layer adds specific information to ensure the data reaches its destination correctly, and these steps are reversed upon arrival.

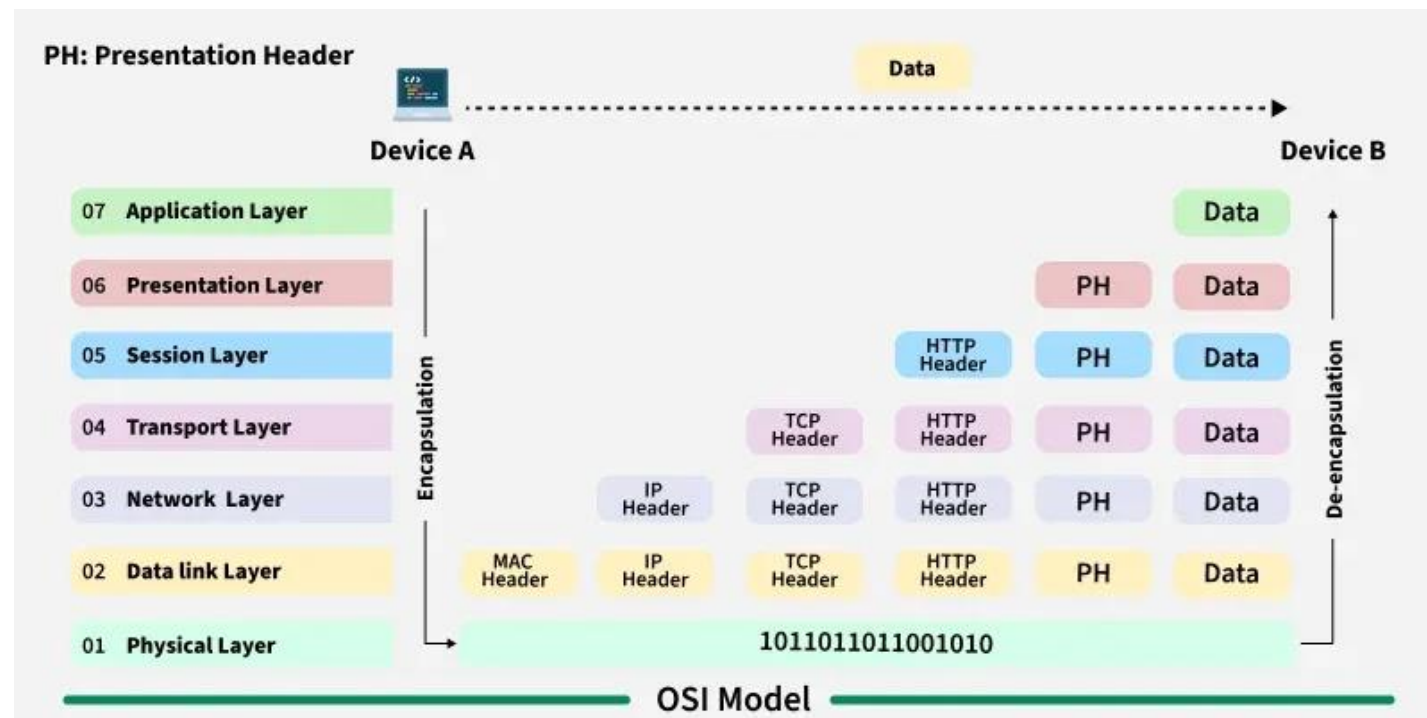
Encapsulation/Decapsulation

- Encapsulation is the process of adding protocol information to data as it travels to its destination
 - Ensures that data is correctly formatted, addressed, and delivered as it travels across multiple layers of the network



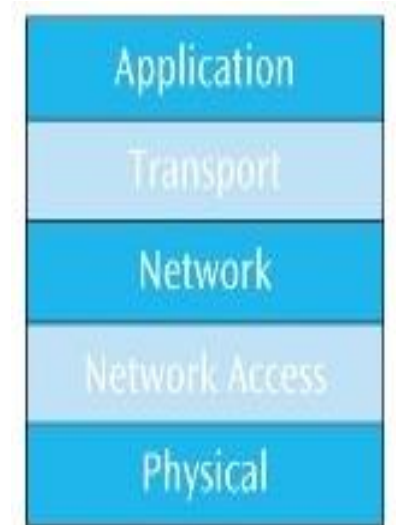
Encapsulation/Decapsulation

- Decapsulation is the process of removing that information so the destination device can read the original data
 - Ensures that the receiver can interpret and use the data by reversing the process and unpacking it layer by layer

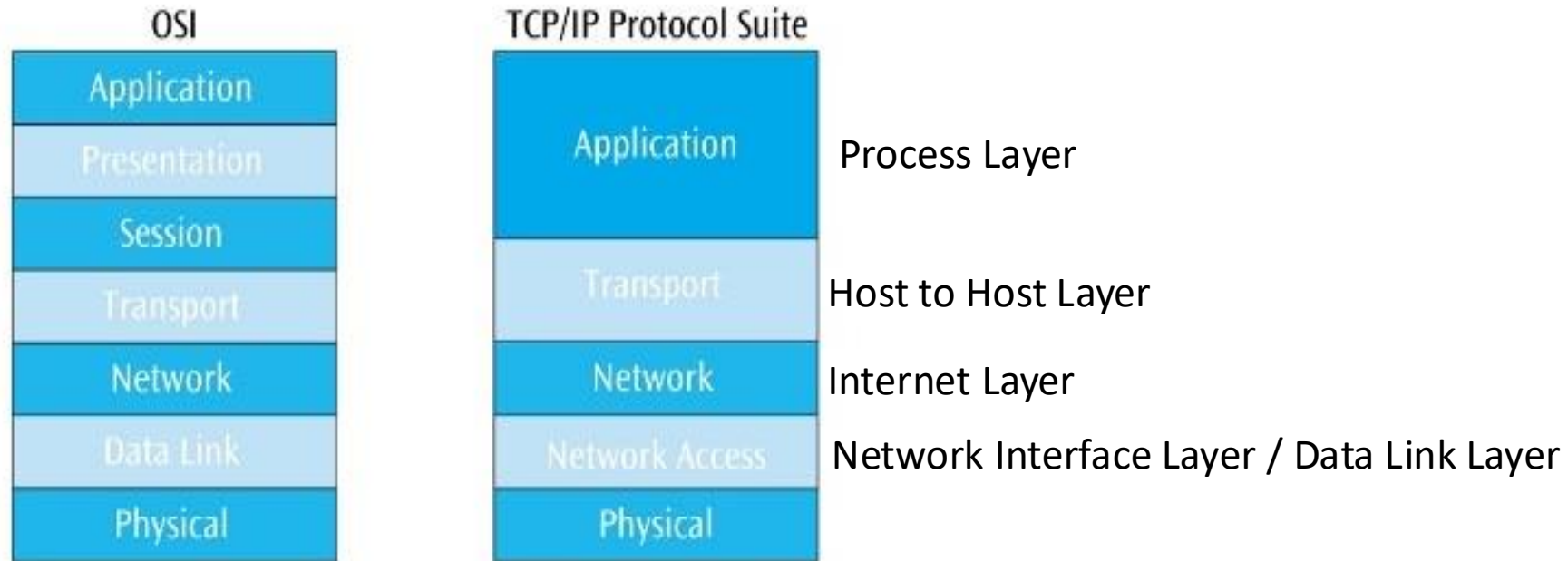


TCP/IP Model

- Stands for Transmission Control Protocol/ Internet Protocol, used for Internet and similar networks (Created in 1974 by DoD)
- Two DARPA scientists, Vint Cerf and Bob Kahn; “Fathers of the Internet”
- Originally there were only four layers in TCP/IP combining the two bottom layers (**DoD model**)
- Layers in the TCP/IP protocol suite do not exactly match those in the OSI model
- TCP/IP protocol suite is made of five layers (**Internet Model**)



Comparing OSI with the TCP/IP Model



Seven layers of the OSI model competed to the five layers of the TCP/IP protocol suite

Devices used in each layer of TCP/IP model

- **Physical Layer:** Hubs, Cables, Modem, Repeater, Amplifiers
- **Data Link (Network Access) Layer:** Switch, NIC
- **Network Layer:** Routers, L3 switches
- **Transport layer:** Gateway/Firewall, load Balancers
- **Application layer:** PCs, Phones, Servers

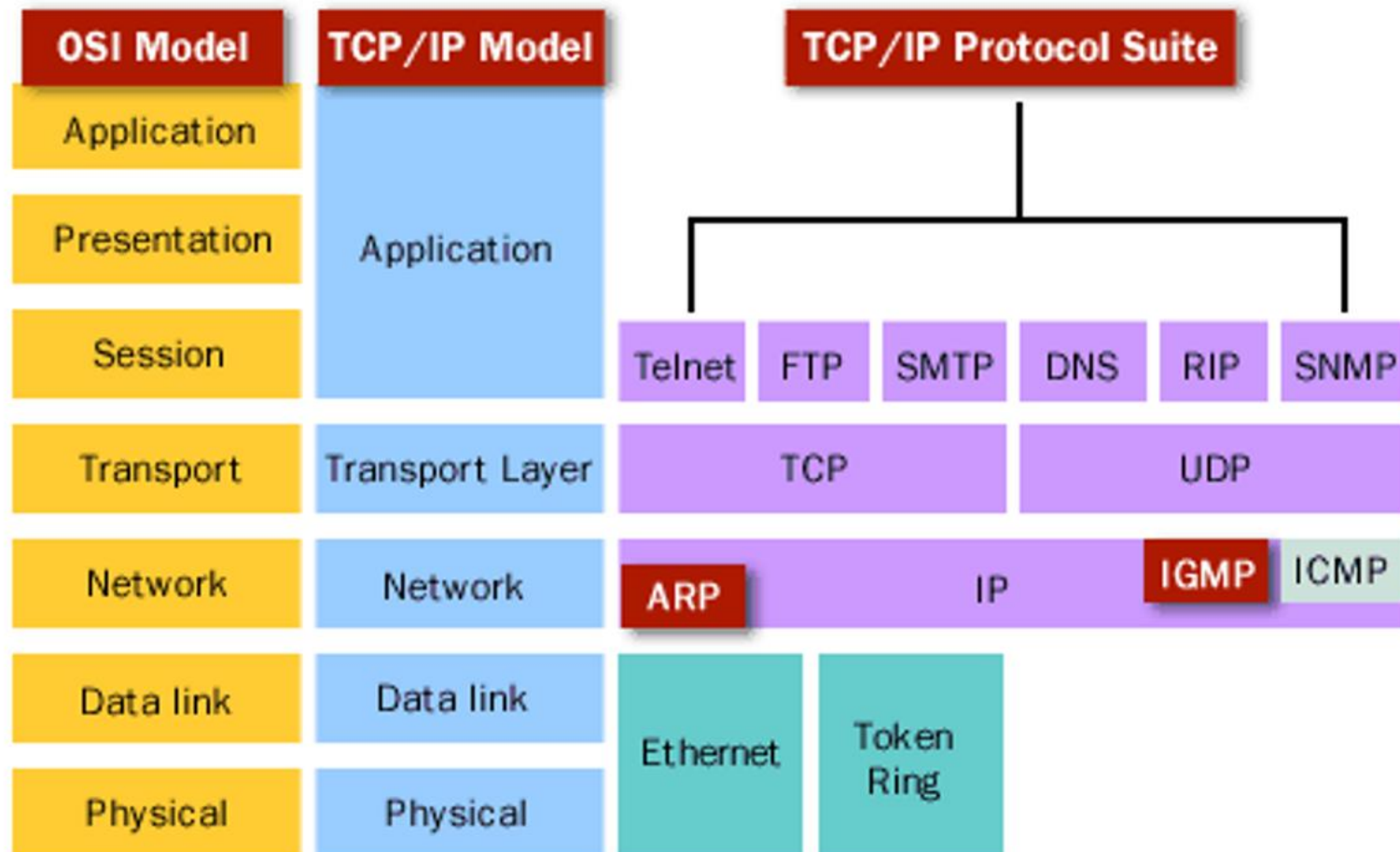
Reminders

- Quiz1 Today
- Cyber Threat Presentation (Due Feb 9)
 - Pick your topic
 - Box submission link will be available soon
 - Everyone in the class will have access to the folder
 - This is part of your Assignment#2
- Office hour change today
 - 4:00 PM – 5:00 PM

Cyber Attack Presentation

- Due Feb 09
- **Group Formation:**
 - Students will be paired into teams of two. Each team will select one type of cyberattack from the list provided.
 - One student will focus on **explaining and demonstrating the attack**.
 - The other student will focus on **explaining and demonstrating a defense strategy** against the attack
- Each team will create a video presentation (5 minutes) where:
 - attack is clearly explained
 - defense is explained with techniques, or strategies to counteract or mitigate the attack

Protocols at Different Layers



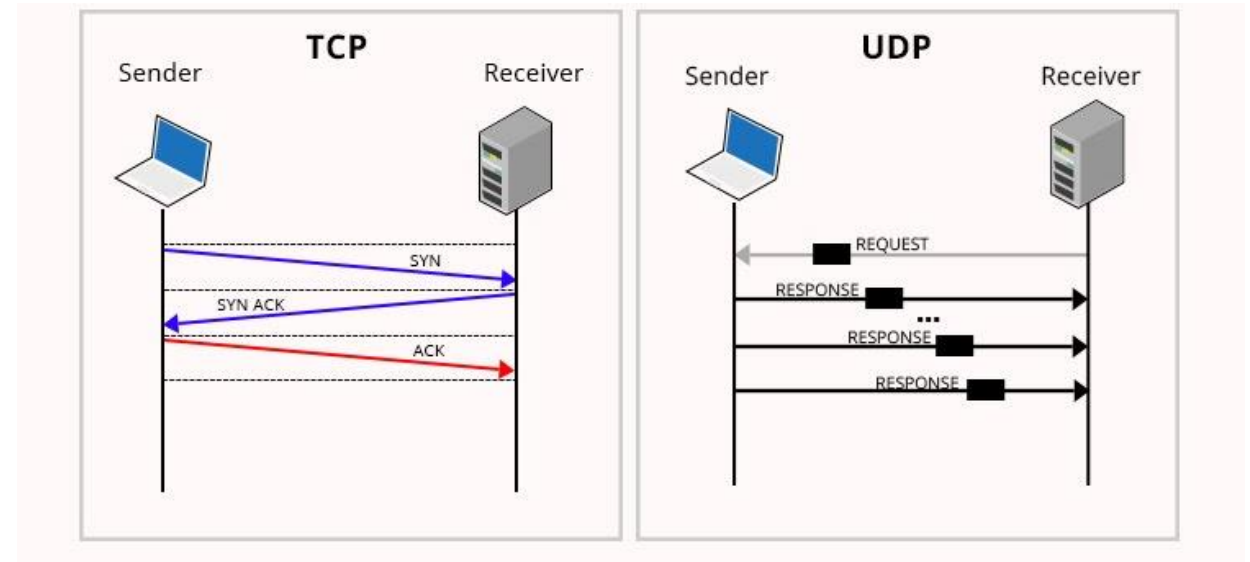
Transport Layer protocols

- **TCP**

- Protocol: Connection Oriented
- Data Sending : Slower
- Keeps track of lost packet arrival order
- Header Size: 20 Bytes
- Acknowledgment segments
- Application: Email, HTTP, HTTPS, FTP

- **UDP**

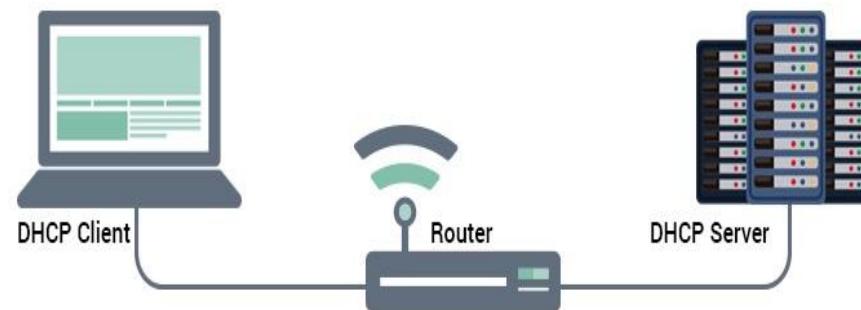
- Protocol: Connectionless
- Data Sending : Faster
- Doesn't care about packet arrival order
- Header Size: 8 Bytes
- No Acknowledgment segments
- Application: VoIP, Computer games



Dynamic Host Configuration Protocol (DHCP)

DHCP runs at application layer of TCP/IP and allow host to dynamically obtain its IP address from network server when it joins network

- reduces the amount of time you spend configuring computers on your network
- conserves IP addresses, only assigns them when a client requests one
- client can renew its lease on address in use
- support for mobile users who want to join network (more shortly)
- only one DHCP can become a single point of failure for your network

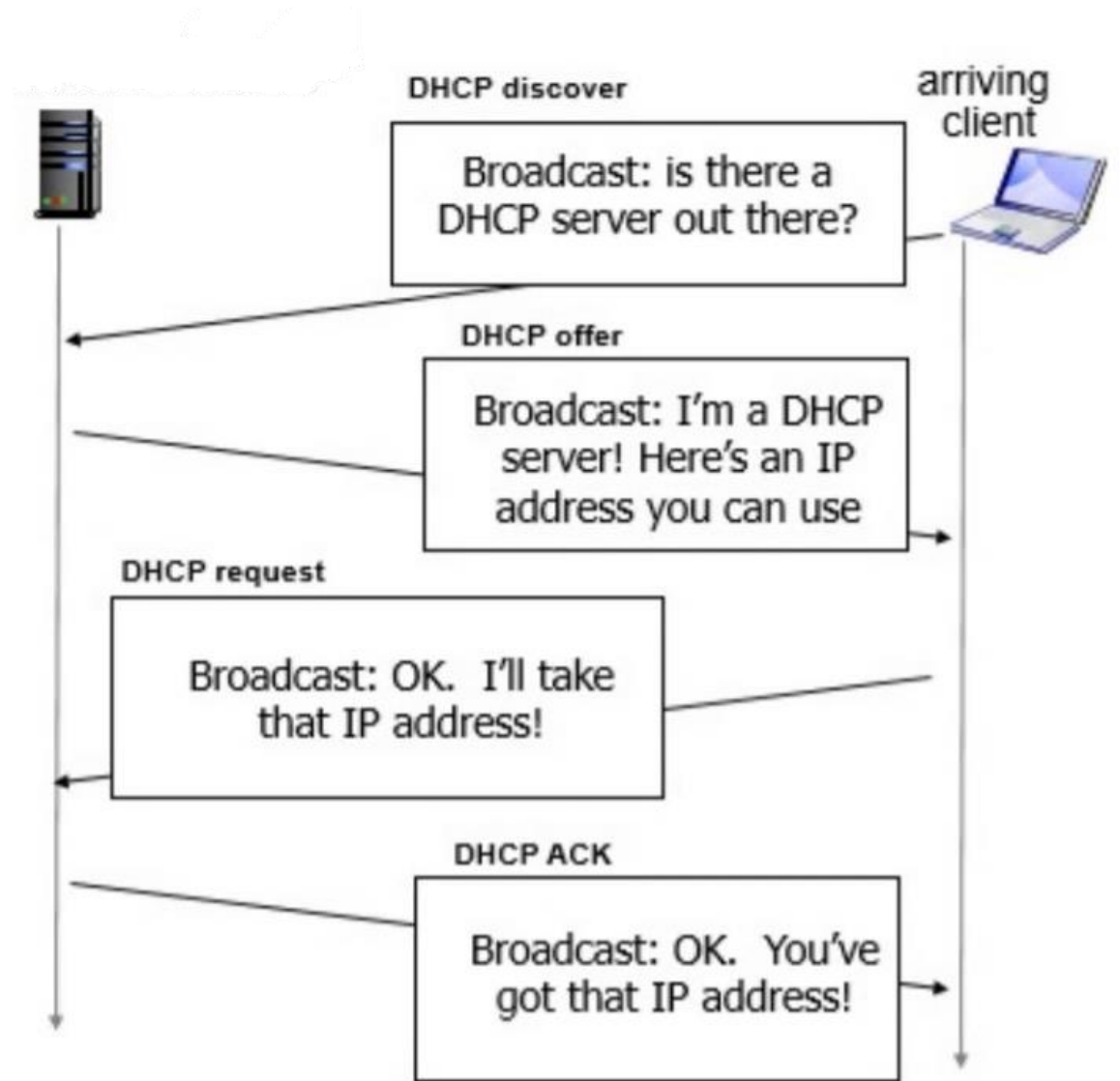


Dynamic Host Configuration Protocol

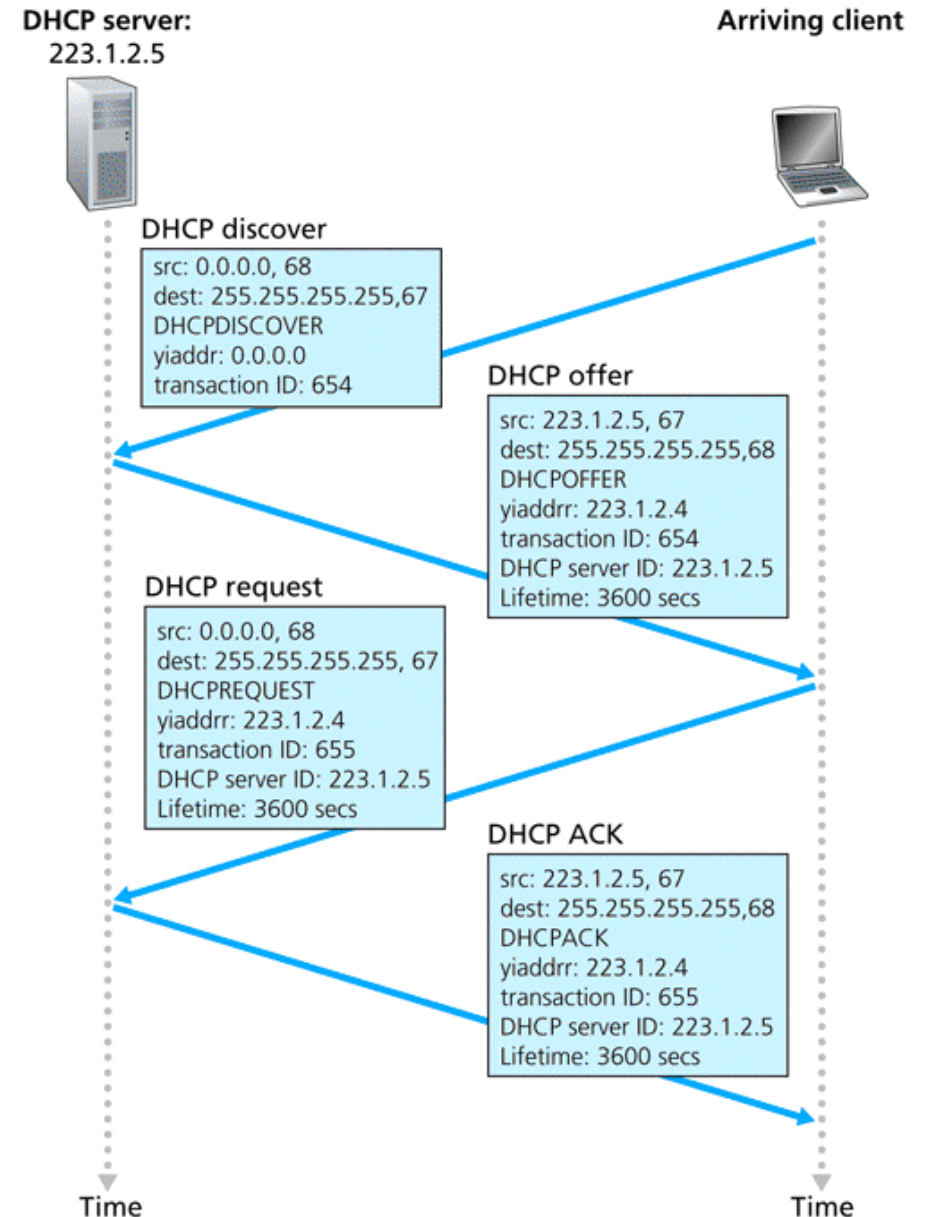
DORA process

DHCP Overview

- host broadcasts “DHCP discover” msg
- DHCP server responds with “DHCP offer” msg
- host requests IP address: “DHCP request” msg
- DHCP server sends address: “DHCP ack” msg



1. Client broadcasts a DHCPDISCOVER message from the port 68 (UDP), to the port 67(UDP) of the server
2. Then, each DHCP server available in the network may respond from its port 67 to the port 68 of the client with a DHCPOFFER message, which includes an available network address and other configuration parameters
3. Then the client selects a server, and broadcasts a DHCPREQUEST message to request a specific IP address. It does also do this from its own port 68, to the port 67 (still broadcasting).
4. Server responds with a DHCPACK message with the requested parameters, from its port 67 to the port 68 of the client, who will now have an assigned IP with a lease time



```
Command Prompt
Microsoft Windows [Version 10.0.16299.1087]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\forev>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-19ULK5G
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

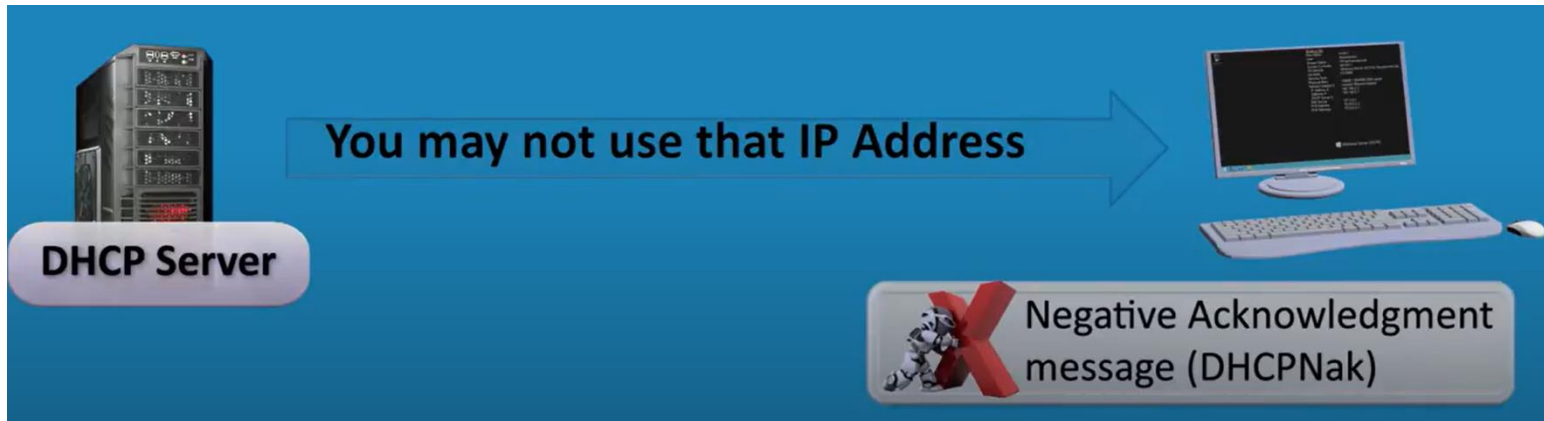

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-83-F4-B6
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::cd10:bb32:6572:face%7(Preferred)
IPv4 Address. . . . . : 192.168.253.128(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, July 13, 2020 10:43:58 AM
Lease Expires . . . . . : Monday, July 13, 2020 11:29:00 AM
```

```
Last login: Tue Feb 13 14:57:11 on ttys000
robinchataut@MBP-CRF92J2253 ~ % sudo su
Password:
sh-3.2# cat /var/db/dhclient/leases
cat: /var/db/dhclient/leases: Is a directory
sh-3.2# cat /var/db/dhclient/leases/*
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>ClientIdentifier</key>
  <data>DNS Suffix . : localdomain
  </data>
  <key>IPV4Address</key>
  <string>10.0.0.162</string>
  <key>LeaseLength</key>
  <integer>172800</integer>
  <key>LeaseStartDate</key>
  <date>2024-02-13T00:29:28Z</date>
```


DHCPNAK

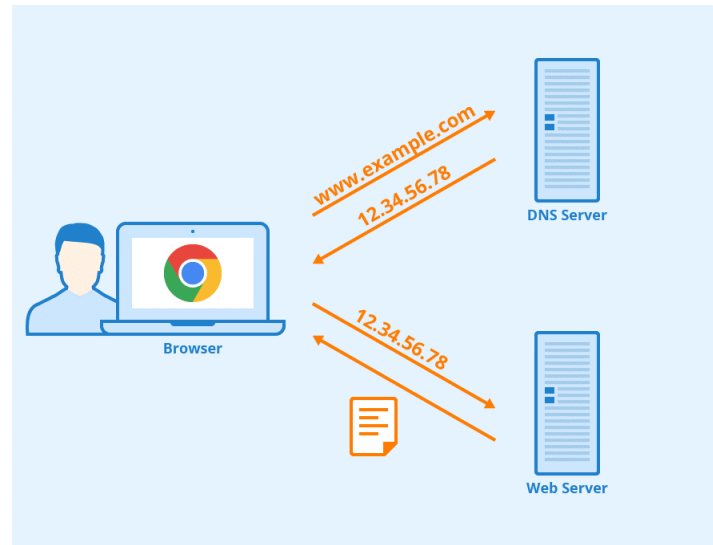
- Negative ACK (NAK) message
 - Server declines the offer made by client
 - When you start a DHCP client, it tries to renew its lease on an existing IP address
 - IP address is no longer available



Domain Name System (DNS)

DNS: Application Layer Protocol

- Locating a Document on the Internet
- When a user, running a Web browser, enters a URL, how is URL translated into an IP address?
- DNS – large, distributed database of URLs and IP addresses
- Like a phonebook of the Internet, helps you to find IP address for a specific name
- Created in 1983



c:\windows\system32\drivers\etc\hosts
sudo nano /private/etc/hosts

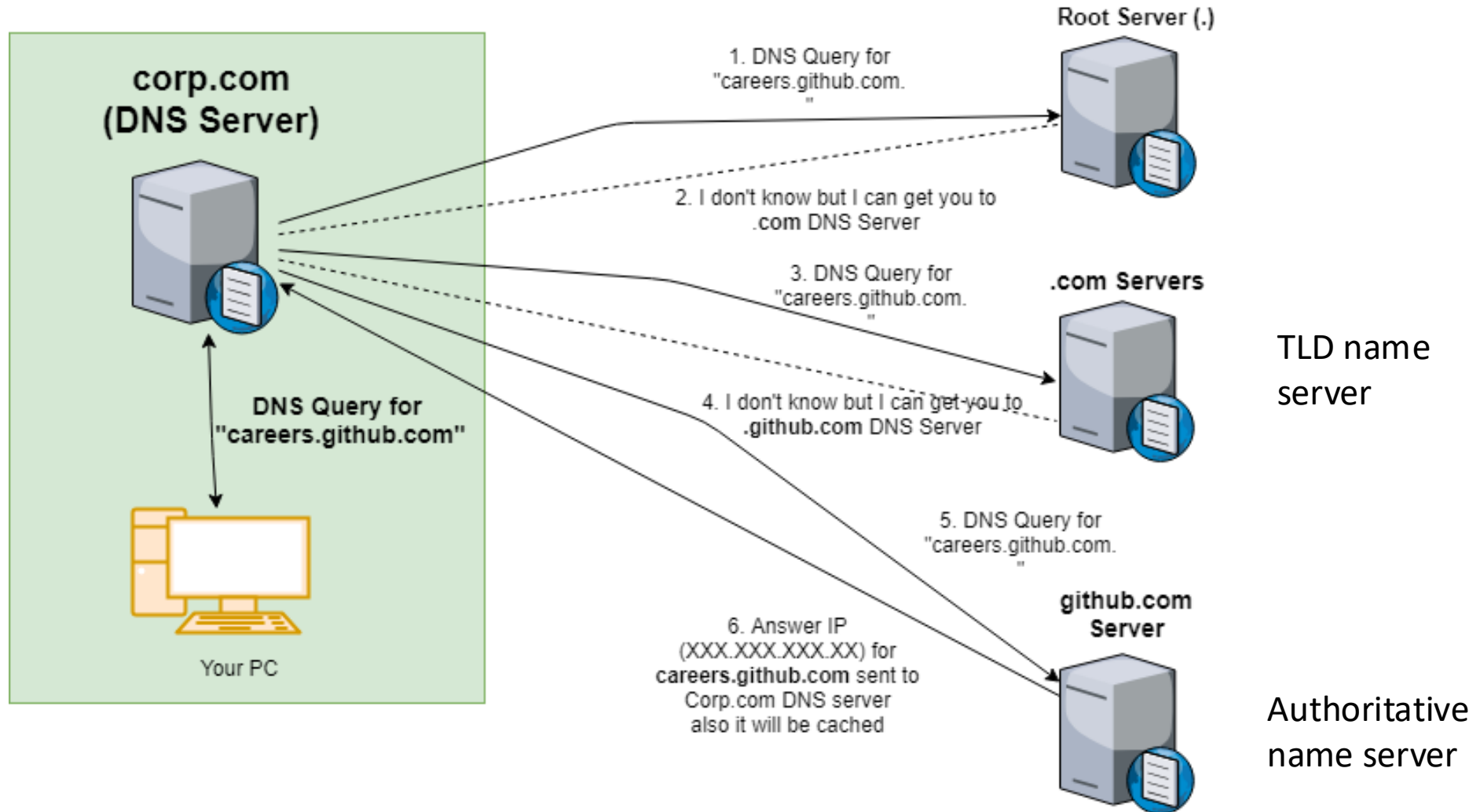
Example of a hosts file

```
File  Edit  Format  View  Help
app.thousandeyes.com    192.150.160.193
www.google.com    172.217.2.36
www.evernote.com    204.154.94.81
www.atlassian.net    104.192.136.171
en.wikipedia.org    198.35.26.96|
twitter.com    199.59.149.230
www.sfsymphony.org    66.40.15.115
www.netflix.com    50.112.250.71
www.linkedin.com    108.174.10.10
www.amazon.com    54.239.17.6
```

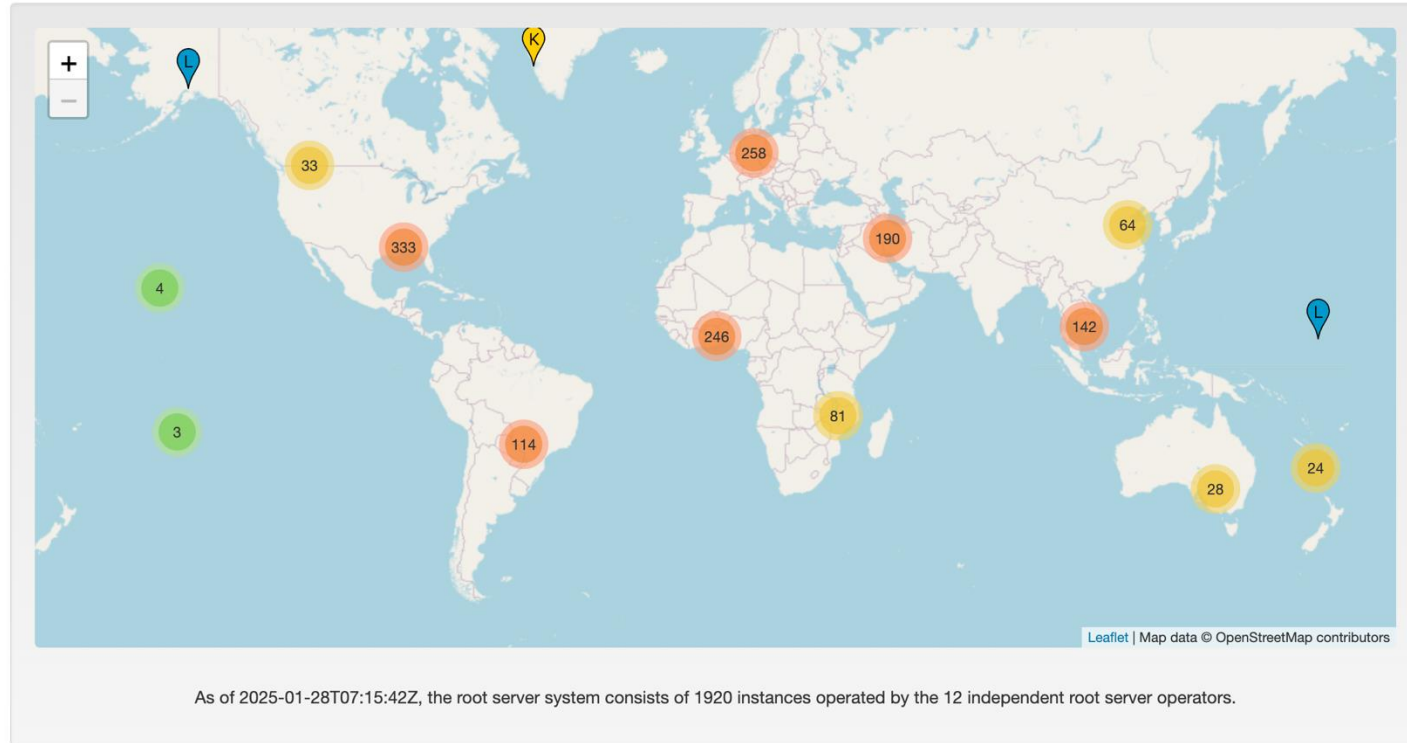
Locating a Document on the Internet

- For the web browser, the DNS lookup occurs "behind the scenes" and requires no interaction from the user's computer apart from the initial request
 - First operation performed by DNS is to **query local database (local DNS server)** for URL/IP address information
 - If local server does not recognize address, the **server at next level** will be queried
 - First **root server** for URL/IP addresses will be queried
 - If root server recognizes domain name but not extension in front of domain name, root server will query **server at domain name's location (TLD name server)**
 - If not found, request is sent to **Authoritative name servers**

Locating a Document on the Internet



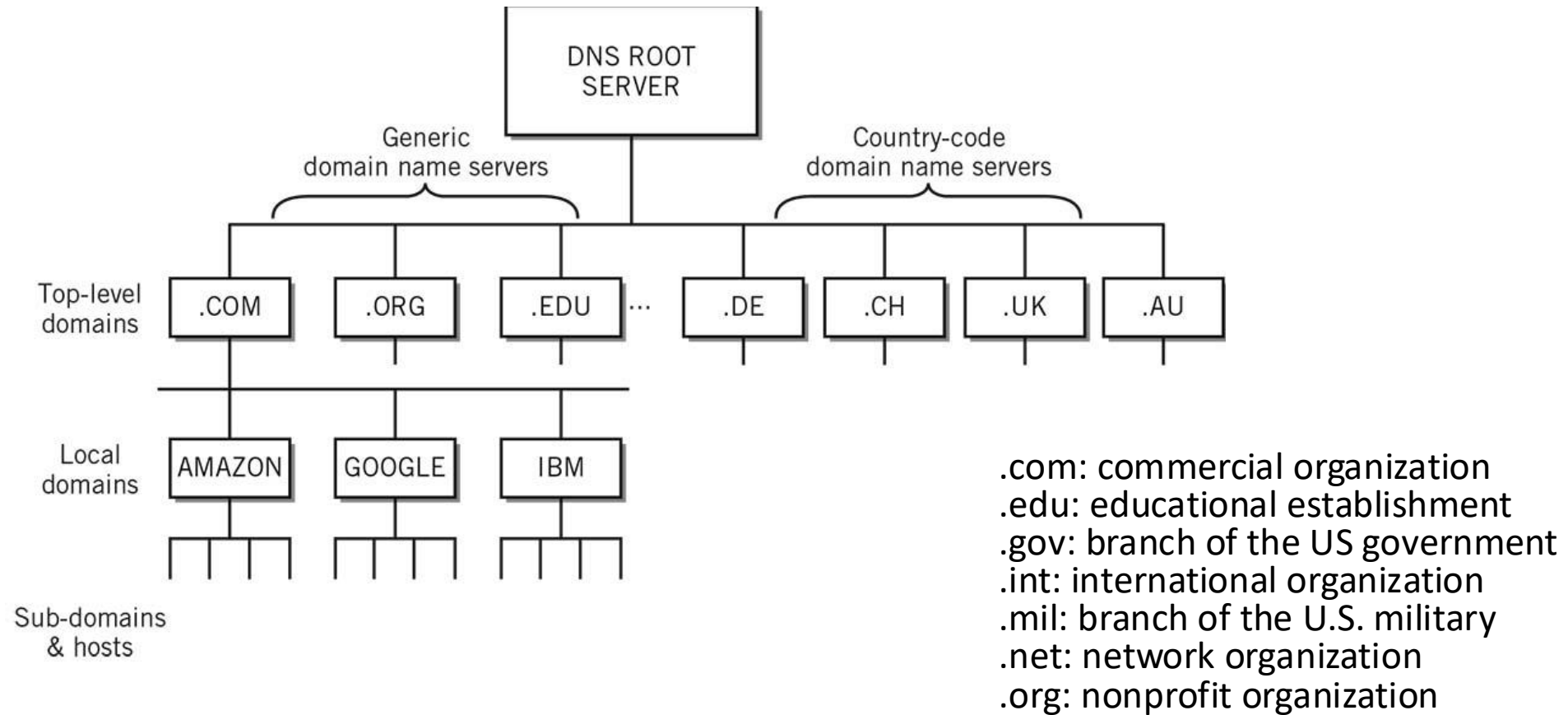
<https://root-servers.org/>



13 root server systems (managed by 12 different entities) all have the **same data** but are managed separately for reasons of **resilience, redundancy, scalability, and governance**

List of Root Servers

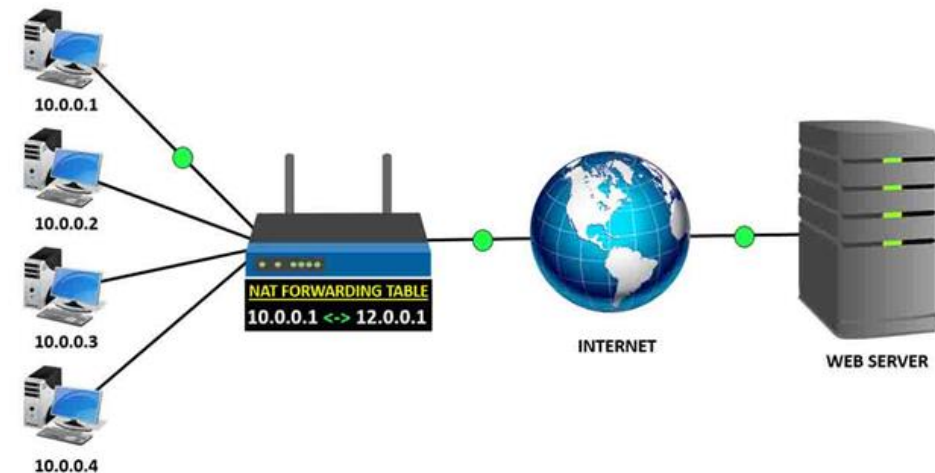
HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	170.247.170.2, 2801:1b8:10::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project



Domain Name System Server Hierarchy

Network Address Translation (NAT)

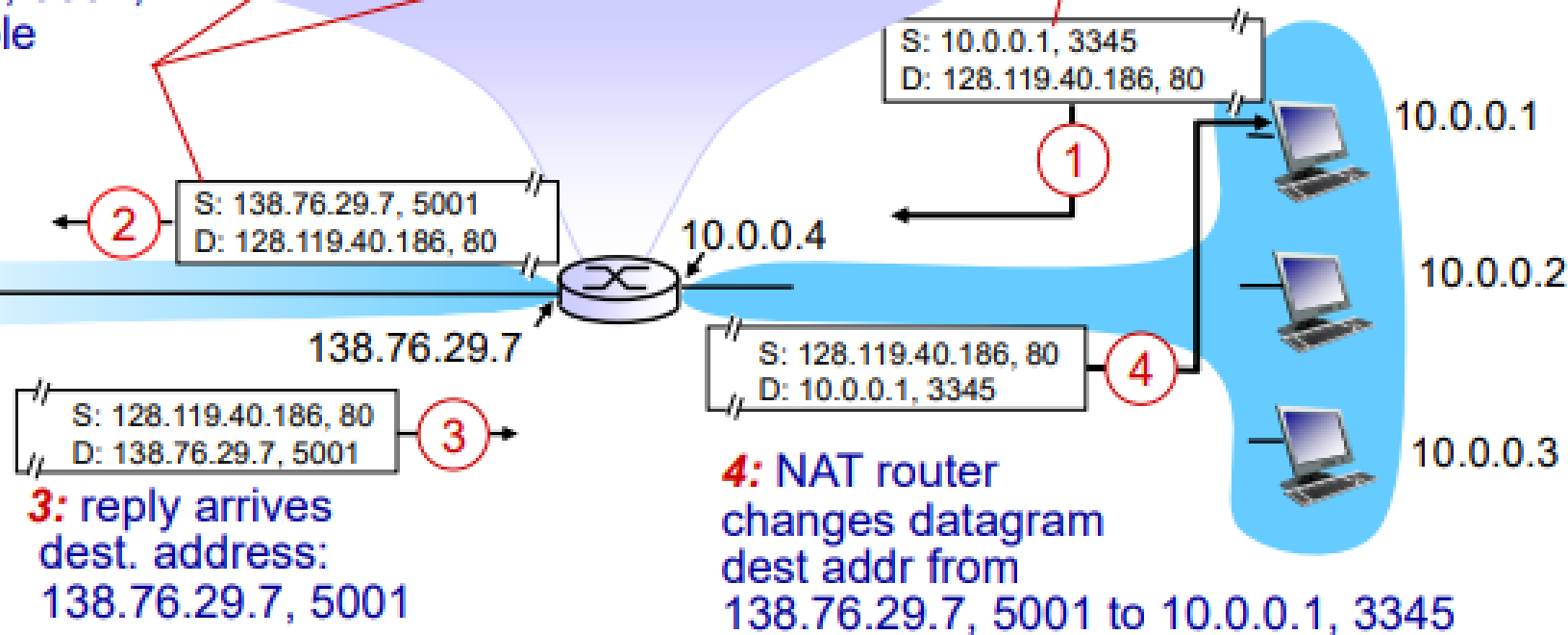
- NAT lets router represent entire LAN to Internet as a single IP address
 - Network layer protocol (Layer 3)
 - All traffic leaving LAN appears as originating from global IP address
 - All traffic coming into this LAN uses this global IP address
- Features:
 - Allows a LAN to hide all the workstation IP addresses from the Internet (*security*)
 - Conserves public IP address (saves money)
 - Introduces small amount of delay
 - End-End IP traceability is lost
- Blocks of addresses for private use:
 - 10.0.0.0 – 10.255.255.255
 - 172.16.0.0 – 172.31.255.255
 - 192.168.0.0 – 192.168.255.255



2: NAT router changes datagram source addr from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table

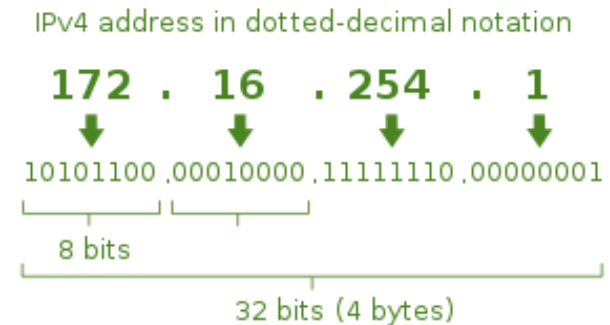
NAT translation table	
WAN side addr	LAN side addr
138.76.29.7, 5001	10.0.0.1, 3345
.....

1: host 10.0.0.1 sends datagram to 128.119.40.186, 80



Internet Protocol (IP)

- IP operates at the Network layer of the TCP/IP model
- Using IP, router makes:
 - Routing decisions based on address portion of IP datagram
 - Fragment the datagram into smaller if the next router has smaller packet size than the current packet size, using fragment offset
 - May determine that current datagram has been hopping around the network too long and delete it (Time to Live)
- There are currently two versions of IP:
 - Version 4, which has been in existence for many years
 - Version 6, which has been available for several years but is only now starting to see a substantial move towards replacing version 4



IPv4 Header

Version	Hlen	Service Type	Total Length	Identification	Flags	
4 bits	4 bits	8 bits	16 bits	16 bits	3 bits	
Fragment Offset		Time to Live	Protocol	Header Checksum	Source IP Address	
13 bit		8 bits	8 bits	16 bits	32 bits	
	Destination IP Address			IP Options		
32 bits				Variable Length		
Padding	Data					
Optional	Variable Length					

Example of an IP packet in Wireshark where you can see how these fields are used

```
[-] Internet Protocol Version 4, Src: 192.168.82.147 (192.168.82.147), Dst: 192.243.232.2 (192.243.232.2)
  Version: 4
  Header Length: 20 bytes
  [-] Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 1155
  Identification: 0x69de (27102)
  [-] 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: 128
  Protocol: TCP (6)
  [-] Header checksum: 0xd064 [validation disabled]
    [Good: False]
    [Bad: False]
  Source: 192.168.82.147 (192.168.82.147)
  Destination: 192.243.232.2 (192.243.232.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  [+] Transmission Control Protocol, Src Port: 57487 (57487), Dst Port: 80 (80), Seq: 1102, Ack: 883, Len: 1115
```

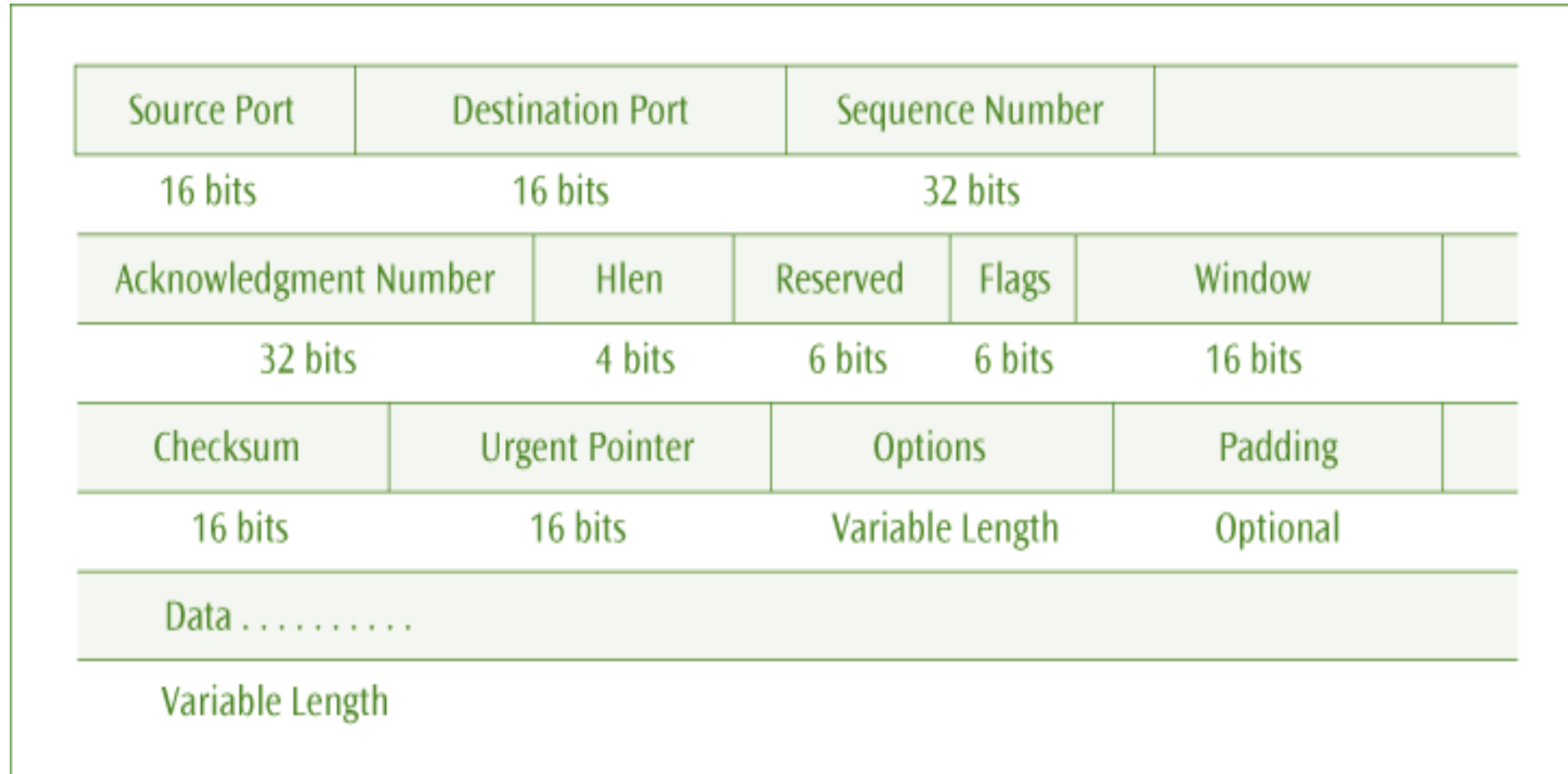
IPv6

- Deployed in 1999
- Main features include:
 - Simpler header
 - 128-bit IP addresses
 - Priority levels and quality of service parameters
 - No fragmentation (intermediate nodes cannot fragment IPv6 fragments)
 - No checksum
- IPv6 addresses are 128-bits in size (2^{128} is a very large number!)
- Binary addresses are written using the short-hand hexadecimal form:

<https://ipv6test.google.com/>

0110 1010 0011 1110 1011 1010 ... 1110 1111
6A3E : BA91 : 7221 : 0000 : 01FC : 922C : 877B : FFEF


TCP Header




Address Resolution Protocol (ARP)

- When an IP packet has traversed the Internet and encounters the destination LAN, how does the packet find the destination workstation?
- Even though destination workstation may have an IP address, a LAN does not use IP addresses to deliver frames
 - LAN are programmed to communicate using MAC address
- ARP translates IP address into MAC layer address so frame can be delivered to proper workstation
- RARP does MAC to IP address translation

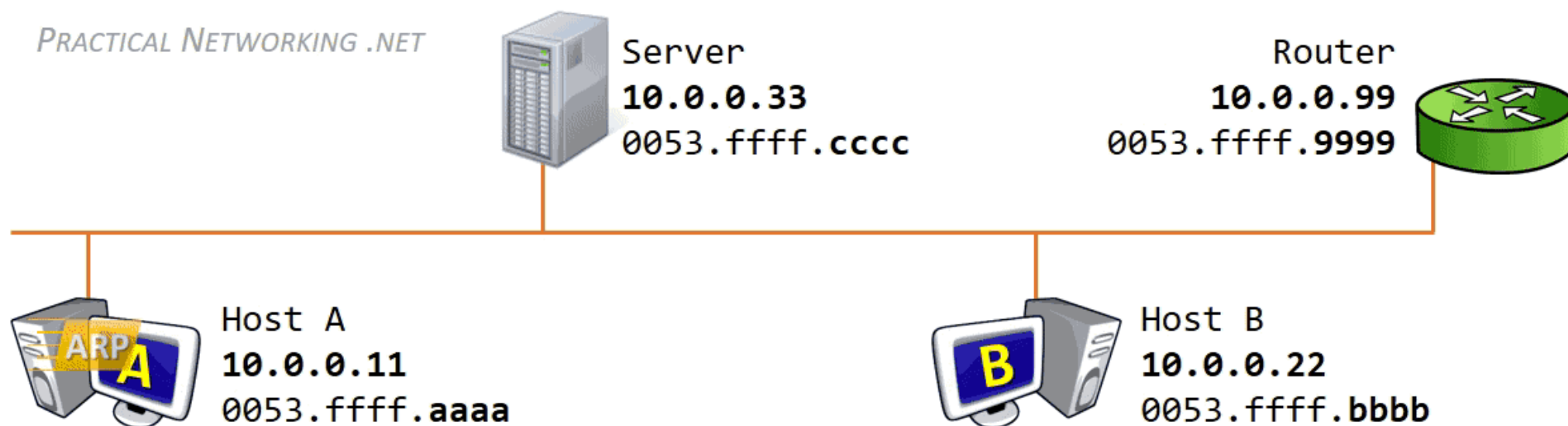


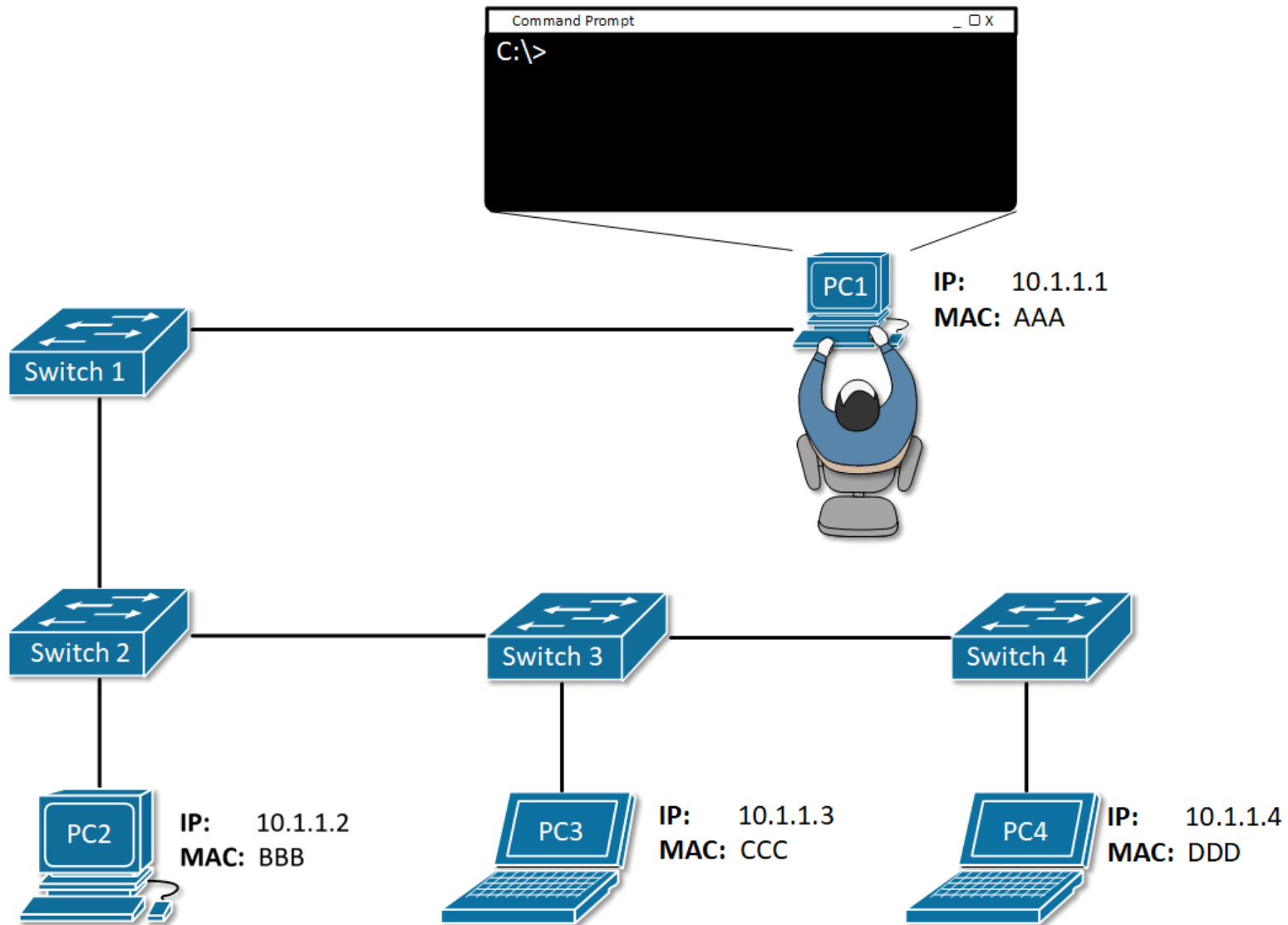
R1's ARP Table			
<u>IP Address</u>		<u>MAC Address</u>	
11.11.11.77	<--->	aaaa	
22.22.22.2	<--->	bb22	
22.22.22.88	<--->	bbbb	

Address Resolution Protocol (ARP)

R1's ARP Table			
IP Address		MAC Address	
11.11.11.77	<--->	aaaa	
22.22.22.2	<--->	bb22	
22.22.22.88	<--->	bbbb	

- Address Resolution itself is a two step process – a request and a response
- **ARP request is a broadcast, and an ARP response is a Unicast**






Address Resolution Protocol (ARP)

- Execute **arp -a** in command line to see existing ARP entry
- Delete ARP entry. Execute **arp -d** command (may need admin rights)


```
C:\Users\lenovo>arp -a
```



Command to see arp entry

```
Interface: 169.254.199.29 --- 0xb
Internet Address      Physical Address      Type
169.254.255.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

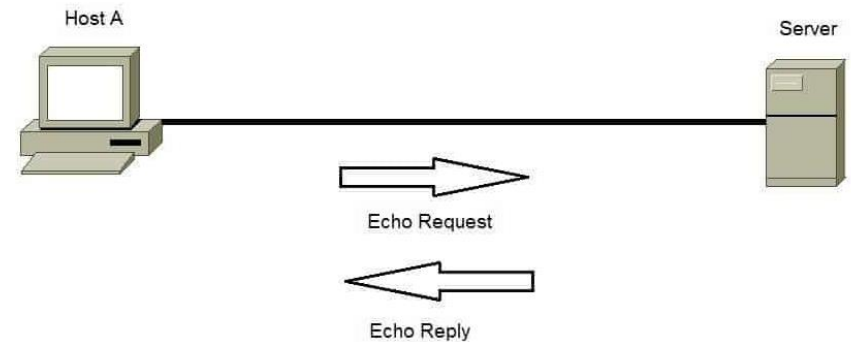
Interface: 192.168.1.6 --- 0x10
Internet Address      Physical Address      Type
192.168.1.1           00-1e-a6-56-14-c0    dynamic
192.168.1.5           fc-f8-ae-a7-80-eb    dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```



Existing ARP entry on interface
whose IP is 192.168.1.6

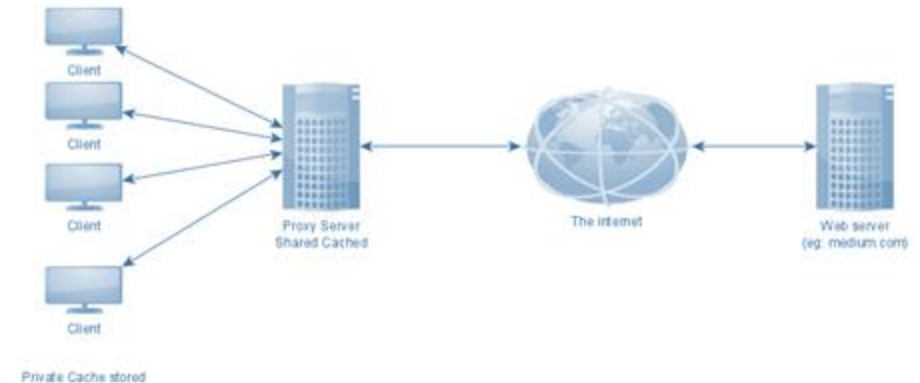
Internet Control Message Protocol

- ICMP: Network layer protocol used by routers and nodes
- Communicates information about network connectivity issues back to the source of the compromised transmission
- Performs error reporting for the Internet Protocol
- ICMP reports errors such as
 - invalid IP address
 - invalid port address
 - the packet has hopped too many times
- A secondary use of ICMP protocol is to perform network diagnostics
 - Commonly used terminal utilities traceroute and ping both operate using ICMP
 - Traceroute utility is used to display the routing path between two Internet devices



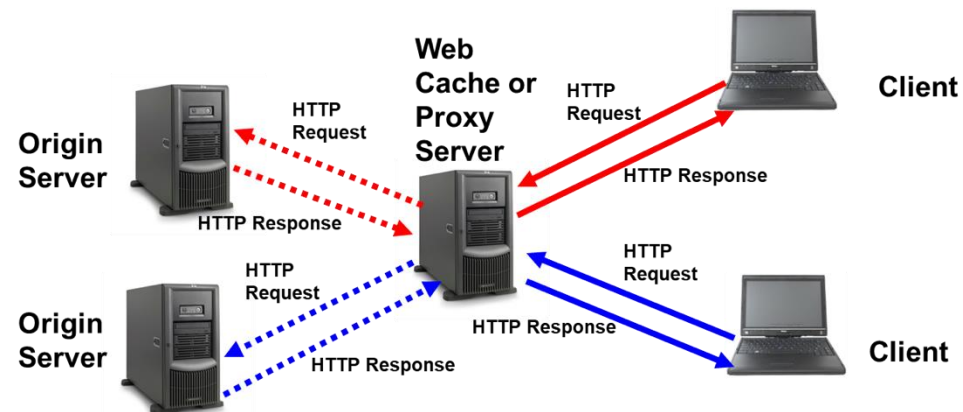
Proxy server

- Proxy server (Web Cache) –satisfies HTTP requests on the behalf of the origin web server
 - Own disk storage
 - Keeps copies of recently requested objects
- Typically installed at ISP or larger institutions
- Advantages:
 - Decreases network congestion
 - Reduces access latency
 - Reduces work load on the original server
- Disadvantages
 - Access latency may increase in case of cache miss
 - Object in the cache is not the most recent version committed to the data source



Proxy server

1. Client/browser sends HTTP Request to Web cache (Proxy server)
2. Proxy server checks to see if it has a local copy of the object
 - 2a. Local recent copy: Proxy server sends object to client's browser
 - 2b. If the local copy is old, the **proxy** fetches a new copy from the source
 - 2c. No Local copy: Proxy server sends HTTP request to origin server
3. Origin server sends object to Proxy server
4. Proxy server stores a local copy of the object
5. Proxy server forwards copy of the object to the client browser

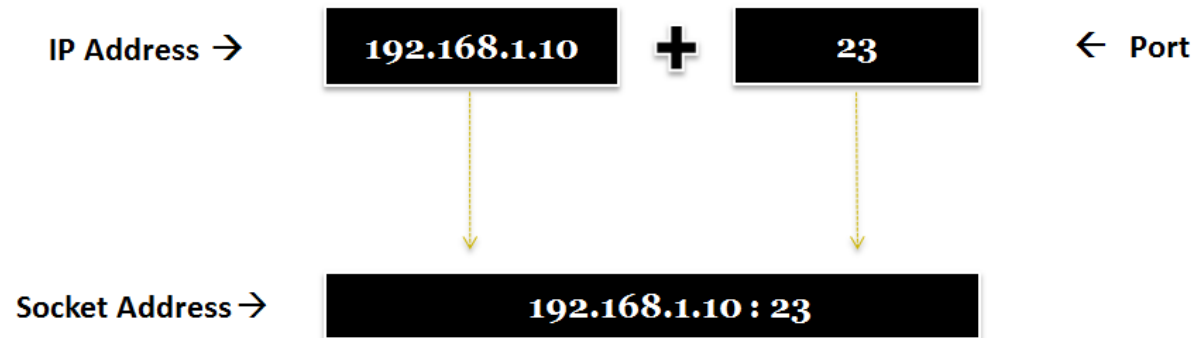


Using Ports and Sockets

- **Port number** is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server
- A port number (port address) identifies:
 - applications associated with data
 - source port for the source application
 - destination port for the destination application
- Two types of TCP/IP ports: UDP ports, TCP ports
- Ports operate at the Transport layer of the OSI
- Each port is assigned a unique 16-bit number
- Many standardized server-side ports;
 - client applications know which port to connect to for a specific service

Using Ports and Sockets

- A socket is a combination of IP address and port number
 - Identifies computer as well as program within the computer uniquely
(a program running in different computer may have same port number)
 - Two sockets required for connection-oriented protocols



Well-known Port Numbers

<i>Port</i>	<i>Protocol</i>
UDP port 15	Netstat
TCP port 20	FTP data
TCP port 21	FTP control
TCP port 22	SSH
TCP port 23	Telnet
TCP port 25	SMTP
TCP port 53	DNS zone transfers
UDP port 53	DNS queries
UDP port 69	TFTP
TCP port 70	Gopher
TCP port 79	Finger
TCP port 80	HTTP
TCP port 110	POP3
UDP port 111	RPC
TCP port 119	NNTP
TCP port 123	NTP
UDP port 137	NetBIOS name service
TCP port 143	IMAP4
UDP port 161	SNMP
TCP port 443	HTTPS
UDP port 520	RIP
UDP port 2049	NFS

TCP/IP Utilities- critical tools in cybersecurity for troubleshooting

- Help network administrators troubleshoot network connections
 - In addition to their direct uses, these tools are often integrated into network monitoring and security information and event management (SIEM) systems to provide real-time alerts and data for security analysis
-
- a. **PING** (Packet Internet Groper) uses the ICMP to test the reachability of a host on an Internet Protocol (IP) network
 - b. **IPCONFIG** displays the current information about your network such as your IP, MAC address, IP address of your router, information about your DHCP and DNS servers. (Note that the equivalent command for Linux/Unix systems is IFCONFIG.)
 - c. **TRACEROUTE** is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination
 - d. **Netstat, nslookup, nmap**

PING

- Ping (latency is the technically more correct term) means the time it takes for a small data set to be transmitted from your device to a server on the Internet and back to your device again
- Sends out four packets of 32 bytes (windows default) to the destination and the destination responds back with the same four packets
- From this we see that the device is alive and see the connection stability (4 of 4 packets received)

```
Command Prompt
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=15ms TTL=113
Reply from 8.8.8.8: bytes=32 time=14ms TTL=113
Reply from 8.8.8.8: bytes=32 time=16ms TTL=113
Reply from 8.8.8.8: bytes=32 time=15ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 16ms, Average = 15ms

C:\>
```

```
robinchataut@MBP-CRF92J2253 ~ % ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=113 time=32.931 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=34.637 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=25.468 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=31.507 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 25.468/31.136/34.637/3.455 ms
```

PING

- What might be other reasons of not getting ping response?
- PING a device that does not exist, we get a “Request timed out” response
- Sent four packets and received zero, so it was a hundred percent lost
 - That means the system you’re trying to reach is not connected to the network

Command Prompt

```
J:\>ping 10.10.10.10
```

```
Pinging 10.10.10.10 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 10.10.10.10:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PING

```
C:\>ping www.in.gov
```

```
Pinging www.in.gov [208.40.244.65] with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 208.40.244.65:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Go to your browser and type www.in.gov, what might be the reason for No response

PING: A few possible reasons of not getting response:

- ❑ **Saving of resources:** The sites might be trying to minimize the number of services on its web site so that the system can focus on serving web requests
- ❑ **Security:** By providing fewer services, fewer security "holes" are likely to exist. People have been known to use ping to send very large packets to hosts. These packets cause the servers' buffers to overflow and crash the system
- ❑ **Firewall:** Host machine could be hidden behind a firewall which only allows http requests to pass. Hence ICMP packets never make it to the host machine
- ❑ **Crash:** System on the other end might have crashed
- ❑ **Temporary Congestion:** Network may be dropping packets because of congestion
- ❑ **Network failure:** Network connection to or from a host may have failed
- ❑ **Hacked Machine:** A machine was modified to behave by dropping packets

More options with ping

```
C:\>ping
```

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
          [-4] [-6] target_name
```

Options:

-t	Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet (IPv4-only).
-i TTL	Time To Live.
-v TOS	Type Of Service (IPv4-only. This setting has been deprecated and has no effect on the type of service field in the IP Header).
-r count	Record route for count hops (IPv4-only).
-s count	Timestamp for count hops (IPv4-only).
-j host-list	Loose source route along host-list (IPv4-only).
-k host-list	Strict source route along host-list (IPv4-only).
-w timeout	Timeout in milliseconds to wait for each reply.
-R	Use routing header to test reverse route also (IPv6-only). Per RFC 5095 the use of this routing header has been deprecated. Some systems may drop echo requests if this header is used.
-S srcaddr	Source address to use.
-c compartment	Routing compartment identifier.
-p	Ping a Hyper-V Network Virtualization provider address.
-4	Force using IPv4.
-6	Force using IPv6.

More options with ping

```
C:\>ping -l 128 127.0.0.1
```

```
Pinging 127.0.0.1 with 128 bytes of data:
```

```
Reply from 127.0.0.1: bytes=128 time<1ms TTL=128
```

```
Reply from 127.0.0.1: bytes=128 time<1ms TTL=128
```

```
Reply from 127.0.0.1: bytes=128 time<1ms TTL=128
```

```
Reply from 127.0.0.1: bytes=128 time<1ms TTL=128
```

```
Ping statistics for 127.0.0.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>
```

```
C:\>ping -a 8.8.8.8
```

```
Pinging dns.google [8.8.8.8] with 32 bytes of data:
```

```
Reply from 8.8.8.8: bytes=32 time=15ms TTL=118
```

```
Reply from 8.8.8.8: bytes=32 time=12ms TTL=118
```

```
Reply from 8.8.8.8: bytes=32 time=12ms TTL=118
```

```
Reply from 8.8.8.8: bytes=32 time=11ms TTL=118
```

```
Ping statistics for 8.8.8.8:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 11ms, Maximum = 15ms, Average = 12ms
```

IPCONFIG

ipconfig /all (ifconfig -a)

- Displays the current information about your network such as your IP and MAC address, and the IP address of your router. It can also display information about your DHCP and DNS servers

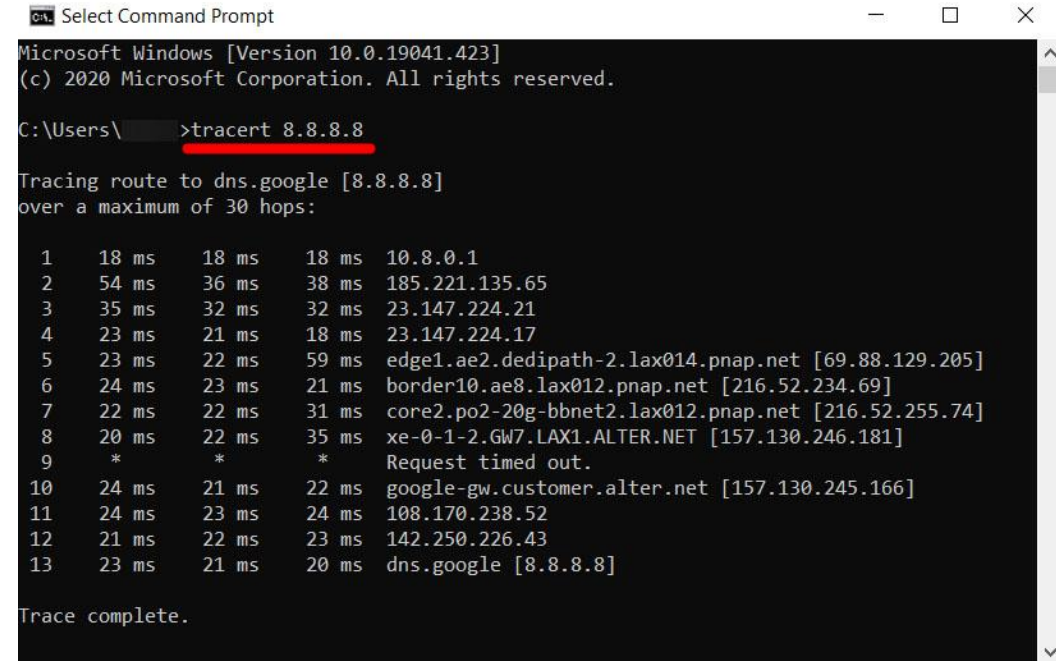
```
Connection-specific DNS Suffix  . : fsc.int
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : E4-5E-37-E0-A0-79
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b044:2499:28fe:97d%24(Preferred)
IPv4 Address. . . . . : 10.65.60.20(Preferred)
Subnet Mask . . . . . : 255.255.248.0
Lease Obtained. . . . . : Monday, February 22, 2021 3:17:32 PM
Lease Expires . . . . . : Saturday, March 6, 2021 11:33:12 PM
Default Gateway . . . . . : 10.65.56.1
DHCP Server . . . . . : 172.20.168.10
DHCPv6 IAID . . . . . : 367287863
DHCPv6 Client DUID. . . . . : 00-01-00-01-26-F5-4B-BE-58-82-A8-8C-02-25
DNS Servers . . . . . : 172.20.168.253
                        172.20.168.254
Primary WINS Server . . . . . : 172.20.168.11
Secondary WINS Server . . . . . : 172.20.168.10
NetBIOS over Tcpip. . . . . : Enabled
```

```
robinchataut@MBP-CRF92J2253 ~ % ipconfig getpacket en0
op = BOOTREPLY
[htype = 1
flags = 0
hlen = 6
hops = 0
xid = 0x889ee9be
secs = 0
ciaddr = 10.0.0.162
yiaddr = 10.0.0.162
siaddr = 10.0.0.1
giaddr = 0.0.0.0
chaddr = 5c:e9:1e:6a:29:fc
sname =
file =
options:
Options count is 10
dhcp_message_type (uint8): ACK 0x5
server_identifier (ip): 10.0.0.1
lease_time (uint32): 0x2a300
renewal_t1_time_value (uint32): 0x14431
rebinding_t2_time_value (uint32): 0x24151
subnet_mask (ip): 255.255.255.0
broadcast_address (ip): 10.0.0.255
router (ip_mult): {10.0.0.1}
domain_name_server (ip_mult): {75.75.75.75, 75.75.76.76}
end (none):
```

TRACERT

- Follows the route (Trace Route) a data packet takes from the source device to the destination
- Traceroute results show you the IP addresses for different points in the route
- Addresses in the first few rows are from your source network, the middle hops are from internet service providers (ISPs), while the last ones are those near the destination
- Used to troubleshoot bottlenecks (areas of the network where data flow is slow due to congestion or lack of adequate resources)

traceroute is equivalent to tracert in Unix systems



```
Select Command Prompt
Microsoft Windows [Version 10.0.19041.423]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1  18 ms  18 ms  18 ms  10.8.0.1
  2  54 ms  36 ms  38 ms  185.221.135.65
  3  35 ms  32 ms  32 ms  23.147.224.21
  4  23 ms  21 ms  18 ms  23.147.224.17
  5  23 ms  22 ms  59 ms  edge1.ae2.dedipath-2.lax014.pnap.net [69.88.129.205]
  6  24 ms  23 ms  21 ms  border10.ae8.lax012.pnap.net [216.52.234.69]
  7  22 ms  22 ms  31 ms  core2.po2-20g-bbnet2.lax012.pnap.net [216.52.255.74]
  8  20 ms  22 ms  35 ms  xe-0-1-2.GW7.LAX1.ALTER.NET [157.130.246.181]
  9      *      *      *      Request timed out.
 10  24 ms  21 ms  22 ms  google-gw.customer.alter.net [157.130.245.166]
 11  24 ms  23 ms  24 ms  108.170.238.52
 12  21 ms  22 ms  23 ms  142.250.226.43
 13  23 ms  21 ms  20 ms  dns.google [8.8.8.8]

Trace complete.
```

TRACERT

- **Column 1:** represents number of hops that the three data packets were pushed through to reach the destination
- **Columns 2-4:** Shows the round trip time measured in milliseconds
- RTT represents the time it took for a data packet to travel from the source to the destination and back again
- To check for the consistency of the response times, the traceroute command sends three packets to each hop, which is why there are three time values listed per row
- **Column 5:** shows the name or IP address of the routers on every hop from your computer to the destination
- It will also list the domain name of the router, if that information is available

```
Microsoft Windows [Version 10.0.19041.423]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1  18 ms  18 ms  18 ms  10.8.0.1
  2  54 ms  36 ms  38 ms  185.221.135.65
  3  35 ms  32 ms  32 ms  23.147.224.21
  4  23 ms  21 ms  18 ms  23.147.224.17
  5  23 ms  22 ms  59 ms  edge1.ae2.dedipath-2.lax014.pnap.net [69.88.129.205]
  6  24 ms  23 ms  21 ms  border10.ae8.lax012.pnap.net [216.52.234.69]
  7  22 ms  22 ms  31 ms  core2.po2-20g-bbnet2.lax012.pnap.net [216.52.255.74]
  8  20 ms  22 ms  35 ms  xe-0-1-2.GW7.LAX1.ALTER.NET [157.130.246.181]
  9  *      *      *      Request timed out.
 10  24 ms  21 ms  22 ms  google-gw.customer.alter.net [157.130.245.166]
 11  24 ms  23 ms  24 ms  108.170.238.52
 12  21 ms  22 ms  23 ms  142.250.226.43
 13  23 ms  21 ms  20 ms  dns.google [8.8.8.8]

Trace complete.
```

Common Traceroute Error Messages

- If there is an issue within the network, the traceroute results will also show error commands, which include:
- **Request timed out:**
 - means that a firewall or a security device might be blocking your request, or there was a problem in the return route
 - At beginning of a traceroute is very common and can be ignored. This is typically a device that doesn't respond to ICMP or traceroute requests

```
2 * * * Request timed out.
```

- **Destination unreachable:**
 - Means data packets have stopped traveling within the network
 - Most of the time, this is because there is a problem with the router or that the website or IP address you are trying to reach is down

Common Traceroute Error Messages

- *** in RTT columns:**

- means the router did not respond to the request within the maximum allotted time
- could also mean that the router in the hop was not set up to provide a response to a traceroute request
- However, it does not necessarily mean that the packet was dropped
- To verify if there was a packet loss, you can ping the IP address of the router where you see the asterisk

17	*	*	*	Request timed out.
18	*	*	*	Request timed out.
19	*	*	*	Request timed out.

Common Traceroute Error Messages

```
Command Prompt
17  118 ms  82 ms  83 ms  cgcil22crs.ip.att.net [12.122.2.54]
18   94 ms  83 ms  83 ms  cl2oh22crs.ip.att.net [12.122.2.113]
19   86 ms  83 ms  99 ms  phlpa22crs.ip.att.net [12.122.2.230]
20   79 ms  80 ms  94 ms  12.123.237.145
21  *      *      *      Request timed out.
22  *      *      *      Request timed out.
23  *      *      *      Request timed out.
24  *      *      *      Request timed out.
25  *      *      12.118.231.50 reports: Destination net unreachable.
Trace complete.
```


High latency in the beginning hops (first few hops)

Indicates a possible issue on the local network level

You will want to work with your local network administrator to verify and fix it

Timeouts at the beginning of the report

If you have timeouts at the very beginning of the report, say within the first one or two hops, but the rest of the report runs, do not worry. This is perfectly normal as the device responsible likely does not respond to traceroute requests

Timeouts at the very end of the report

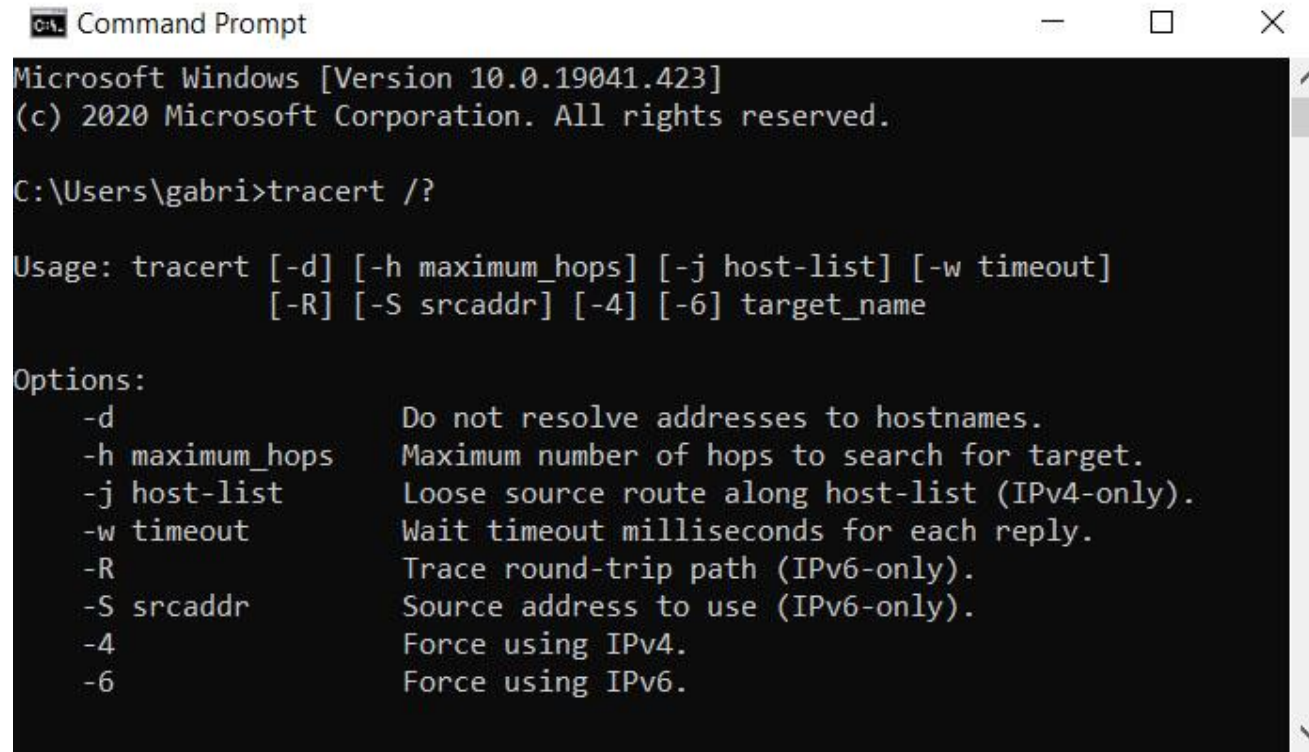
Timeouts at the end may occur for a number of reasons. Not all of them indicate an issue, however:

- target's firewall may be blocking requests (but can be reached with HTTP)
- return path may have an issue from the destination point
- Possible connection problem at the target. This will affect the connection.

Times above 150ms are considered to be long for a trip within the continental United States
(Times over 150ms may be normal if the signal crosses an ocean)

TRACERT

If you are looking for ways to run a traceroute, you can open the terminal/cmd app and type ***tracert*** ***/?*** to see variations you can use



```
Command Prompt
Microsoft Windows [Version 10.0.19041.423]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\gabri>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                Do not resolve addresses to hostnames.
    -h maximum_hops   Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                Force using IPv4.
    -6                Force using IPv6.
```

More Tools

- **Netstat**

- netstat utility displays network statistics and active network connections on a computer. It can show open ports, routing tables, and interface statistics.

- **Nslookup** (Windows) / **dig** (Linux/Unix)

- These tools are used for DNS (Domain Name System) queries. They allow you to look up DNS records for a domain or resolve domain names to IP addresses.

- **Nmap**

- Nmap is a powerful network scanning tool used for discovering hosts and services on a network. It can perform various types of scans, including port scanning and OS fingerprinting.

netstat

- netstat, network statistics, used to display very detailed information about how your computer is communicating with other computers or network devices
- Shows details about individual network connections, interfaces, overall and protocol specific networking statistics

```
robinchataut — -zsh — 90x38
Last login: Tue Aug 29 15:57:21 on ttys000
robinchataut@MBP-CRF92J2253 ~ % netstat
Active Internet connections
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4      0      0 10.0.0.162.63298        server-108-138-1.https  ESTABLISHED
tcp4      0      0 10.0.0.162.63297        server-18-164-96.https ESTABLISHED
tcp6      0      0 2601:18b:8000:7c.63296 2606:4700:20::68.https ESTABLISHED
tcp4      0      0 10.0.0.162.63295        server-18-164-96.https ESTABLISHED
tcp4      0      0 10.0.0.162.63294        aa7557bb34ea5624.https ESTABLISHED
tcp4      0      0 10.0.0.162.63293        93.184.216.86.https   ESTABLISHED
tcp4      0      0 10.0.0.162.63292        179.9.211.130.bc.https ESTABLISHED
tcp4      0      0 10.0.0.162.63291        server-13-35-93-.https ESTABLISHED
tcp4      0      0 10.0.0.162.63289        server-108-139-4.https ESTABLISHED
tcp4      0      0 10.0.0.162.63288        server-108-138-1.https ESTABLISHED
tcp6      0      0 2601:18b:8000:7c.63287 2606:4700:20::68.https ESTABLISHED
tcp6      0      0 2601:18b:8000:7c.63282 bi-in-f157.1e100.https ESTABLISHED
tcp6      0      0 2601:18b:8000:7c.63281 lga34s35-in-x0a..https ESTABLISHED
tcp6      0      0 2601:18b:8000:7c.63280 lga34s38-in-x02..https ESTABLISHED
tcp6      0      0 2601:18b:8000:7c.63279 lga25s78-in-x0e..https ESTABLISHED
tcp6      0      0 2601:18b:8000:7c.63278 lga25s73-in-x08..https ESTABLISHED
tcp4      0      0 10.0.0.162.63277        151.101.130.137.https ESTABLISHED
tcp6      0      0 2601:18b:8000:7c.63276 lga15s49-in-x0e..https ESTABLISHED
```

So far

- ...you have learned about the network basics
- ...you have learned about the OSI model
- .. You have learned about TCP three way handshake
- ...you have seen headers, network protocols, et
- ... You have learned about TCP/IP utilities
- ...There is a lot going on here...

How can you comprehend all this tangibly? How can one visualize what's going on?

- Next steps: packets, PCAPs, and Wireshark

Packet

- *Packet - unit of data*
- *A data stream (e.g., video, a web page) is comprised of many packets*
- *In general, a packet contains the following information:*
 - *Source and destination IP addresses (in IP layer)*
 - *Source and destination port number (in TCP layer)*
 - *MAC address (in Data Link layer)*
 - *Time To Live (TTL; in IP layer)*
 - *Payload*
- *Thus, a packet contains implementations of all the protocol layers (including TCP, IP, application, data link)*
 - *Encapsulation model*

.pcap File

- The common file extension for packet captures and is commonly used in many applications such as Wireshark, ettercap, tcpdump
- A 100 MB PCAP file contains tens of thousands of packets

Wireshark

- *Graphical and extensive packet analyzer*
- *One of the most important tools in the field*
- *Open source and free*
- *Features include filtering, reconstructing conversations, reconstructing files based on packets*
- <https://www.wireshark.org/>

tshark

Dumps and analyzes network traffic

- Command-line-based Wireshark
- Installed with Wireshark
- The manual: `man tshark`

Tool: tcpdump

- *A packet analyzer that runs via command line*
- *To run: `sudo tcpdump -i <INTERFACE>`*
- *The manual: `man tcpdump`*
- *Cheat sheet via SANS Institute: <https://www.sans.org/securityresources/tcpip.pdf>*
- *Example: reading a PCAP file*
 - `tcpdump -r file.pcap`
- *Example: splitting a PCAP file into smaller ones (e.g., 10 MB)*
 - `tcpdump -r old_file.pcap -w new_files -C 10`

References

- *Introduction to Security Cryptography, Ming Chow, Tufts University*
- *CompTIA, Security+*

Review

1. What is the purpose of the Address Resolution Protocol (ARP)?
 - A) To provide encryption across the network
 - B) To compress data for faster transmission
 - C) To translate IP addresses into MAC addresses
 - D) To manage network devices

Review

2. Which OSI layer is responsible for end-to-end connectivity and reliability through error recovery and flow control?

- A) Physical Layer
- B) Transport Layer
- C) Network Layer
- D) Application Layer

Review

3. In the OSI model, at which layer does routing occur?

- A) Session Layer
- B) Presentation Layer
- C) Network Layer
- D) Data Link Layer

Review

4. Which protocol is responsible for assigning IP addresses to devices on a network?

A) DHCP

B) DNS

C) SMTP

D) FTP

Review

5. What is cyber attribution?

- A) The process of assigning a grade to cybersecurity protocols
- B) The process of identifying the perpetrator behind a cyberattack
- C) Adding digital certificates to websites
- D) The distribution of malware via email

Review

6. What role does the Presentation Layer play in the OSI model?

- A) It ensures that data is in a usable format and is where data encryption occurs
- B) It is responsible for physical connectivity between devices
- C) It manages sessions between applications
- D) It controls the reliability of a given link through flow control, segmentation/desegmentation, and error control

Review

7. Which of the following describes the function of NAT (Network Address Translation)?

- A) To translate network addresses into physical addresses
- B) To allow multiple devices on a LAN to share a single IP address to the internet
- C) To convert analog signals into digital signals
- D) To assign static IP addresses to devices on a network

Summary

- Need for Network
- Importance of Networking in Cybersecurity
- Cyber Attribution
- Network Security Concern
- Understanding Network Basics
 - node, server, client, circuit, cabling, NIC, protocols, hubs, switches, routers,
- Types of network
- Networking Scenario Problem
- IP, Port, socket, localhost
- OSI and TCP/IP model
- Network Protocols
 - ARP, TCP, UDP, DNS, DHCP, NAT, IPv4/v6, TCP

Reminders

- Add your name to Cyber Attack Presentation List
 - Presentation Due Feb 9
- Assignment#3 on TCP/IP Utilities
- Prepare for quiz (Chapter 2)
- Install Wireshark (Required for assignment#4)- CTF Challenge
 - Learn how to capture packets

Next Chapter: Cryptography