COMP482
Cybersecurity
Week 3 - Monday

Dr. Nicholas Polanco
(he/him)

KALAMAZOO COLLEGE

Attendance

https://forms.office.com/r/BtVc9FH95i

CSE482 - Attendance

Important Notes

1. The TryHackMe activities for today cover a large amount of background in networking if you are interested.
   a. **I am only covering some basic elements to help us look at threats and defenses!**
   b. I tried to stress this at the beginning of the term, but network cybersecurity is **a lot** and my goal is to cover as many topics as we can
2. I have split this into a two-class lecture, so it isn't too long or too much information in one day.
   a. I created a stopping point and shifted the schedule so we can work on our Activity from Friday and cover the rest of this Wednesday.

Important Dates (Week 3)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
				Reflection: Week 2 Project Deliverable: Meeting with Dr. Polanco Topic Deliverable: Topic Selection Activity: Keylogger or Buffer Overflow		

Outline

1. Networking Basics
2. Man-in-the-Middle (MitM)
3. Denial of Service
4. Spoofing
5. Activity

Outline

1. Session Hijacking
2. Port Scanning
3. Firewall
4. IDS
5. VPN

Networking Basics

Networking Basics

A computer network is a system of interconnected devices that can communicate with each other to share resources, such as data, applications, or hardware.

These devices—like computers, servers, routers, and other networking equipment—are linked together using physical cables (like Ethernet) or wireless technologies (such as Wi-Fi).

Image Credit

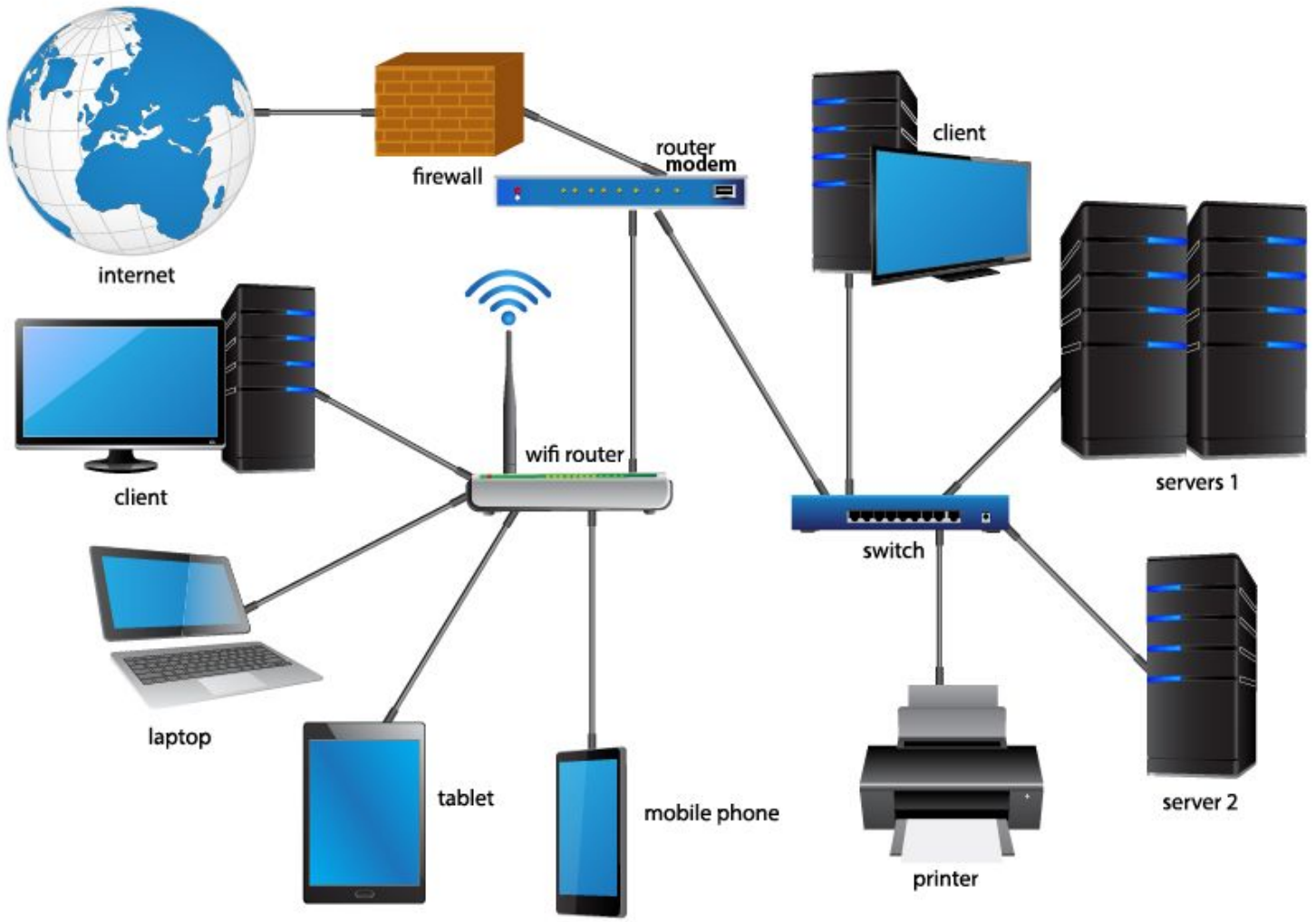


Image Credit
https://integrinetit.com/what-is-a-computer-network/

KALAMAZOO COLLEGE

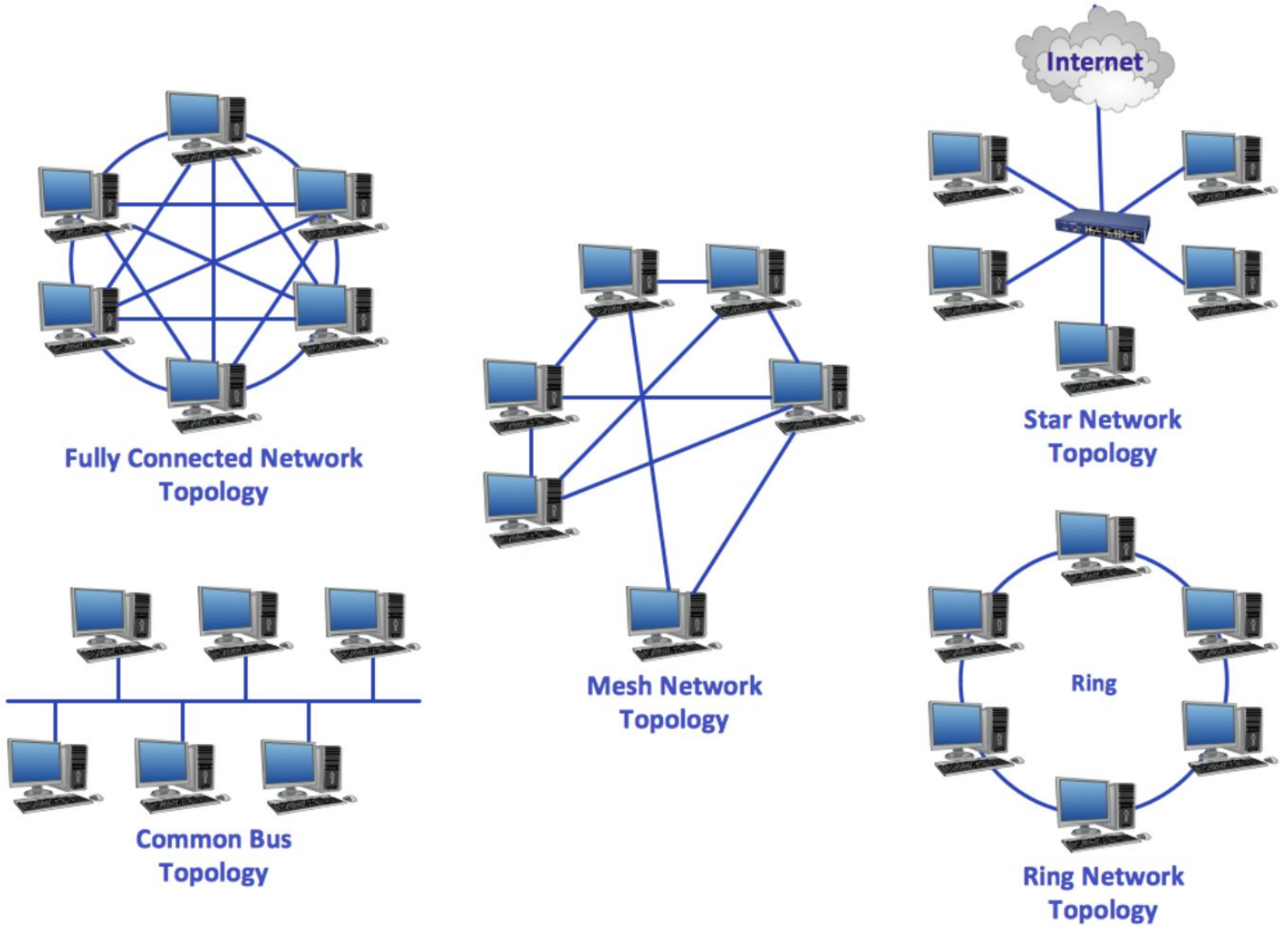


Image Credit
https://www.swissns.ch/site/2017/06/the-various-types-of-network-topologies/

KALAMAZOO COLLEGE

Networking Basics (continued)

The Open Systems Interconnection model, or OSI model, is a conceptual framework that breaks down network communication into seven abstract layers.

This model helps **standardize how computer systems communicate across networks**, promoting interoperability between different vendors and technologies.

Image Credit

The seven layers of the OSI model

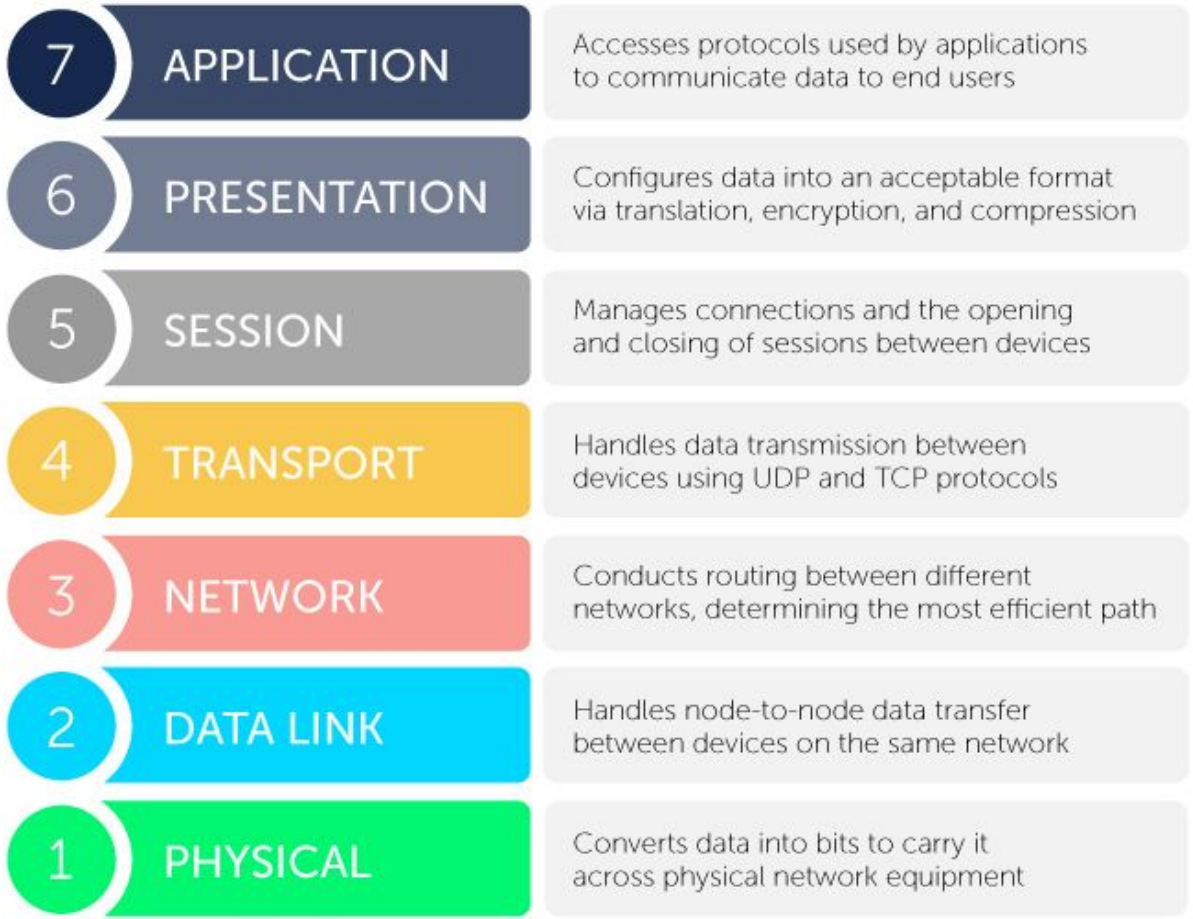


Image Credit
https://bluecatnetworks.com/glossary/what-is-the-osi-model/

KALAMAZOO COLLEGE

Networking Basics (continued)

Layer 1: Physical - The purpose is to transmits raw bitstream over the physical medium. The data is moved using bits (0 and 1) across components like physical cables (e.g., fiber, copper) and radio frequencies (e.g., Wi-Fi, Bluetooth)

The Physical Layer

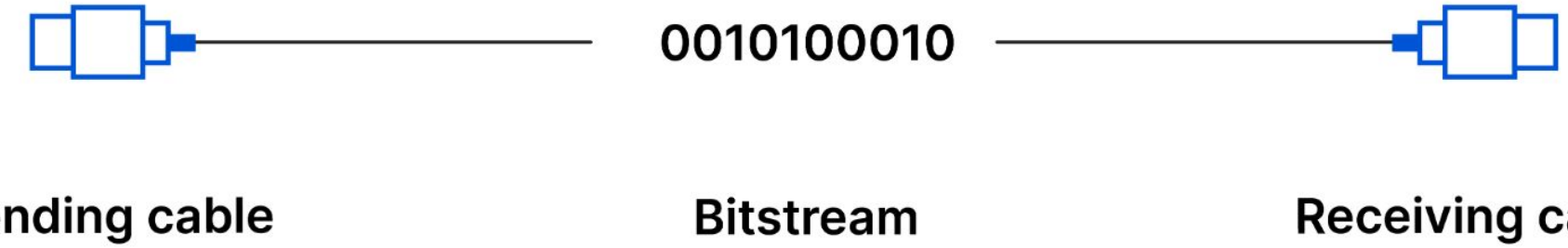


Image Credit
https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

KALAMAZOO COLLEGE

Networking Basics (continued)

Layer 2: Data Link - Its main role is to provide reliable transmission of data across a physical network link.

It breaks down the raw data into frames, which are manageable chunks, and adds headers/trailers for processing. It also uses devices Media Access Control address (MAC) to identify devices on the same local network.

Image Credit

The Data Link Layer

Image Credit
http://cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

KALAMAZOO COLLEGE

Pause: MAC Address

A MAC address is a unique identifier assigned to a network interface card (NIC) of a device, like a computer, smartphone, or router.

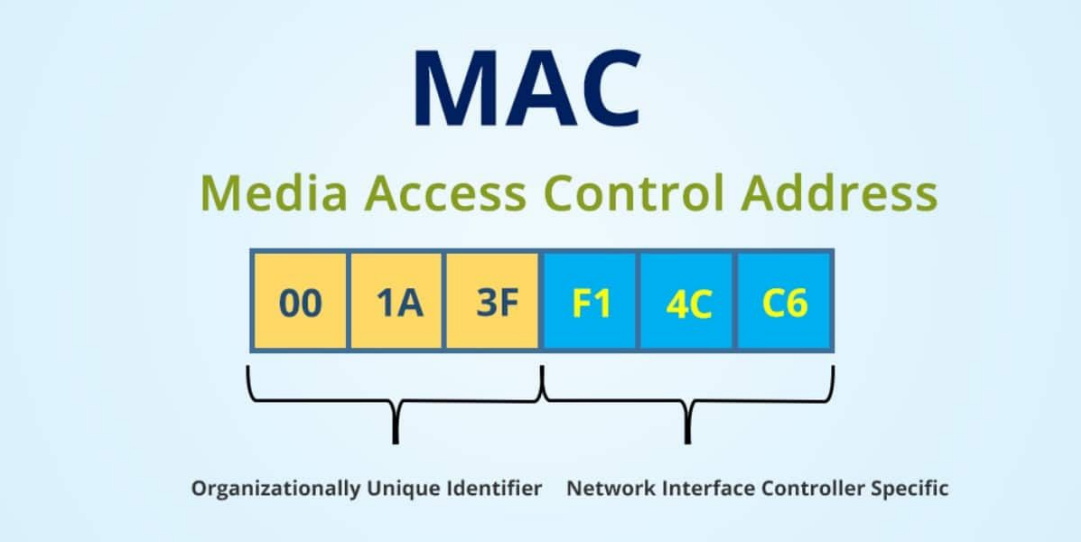


Image Credit: https://eshop.macsales.com/blog/85737-how-to-find-your-macs-mac-address-in-macos-ventura/

KALAMAZOO COLLEGE

Networking Basics (continued)

Layer 3: Network Layer - Its main responsibility is to route data packets across *different networks* and ensure that data is transferred from the source to the destination system.

It makes decisions based on the destination IP address in the packet. The routers of a network operate at the Network Layer, and they use routing tables to determine where to send data packets next.

Image Credit

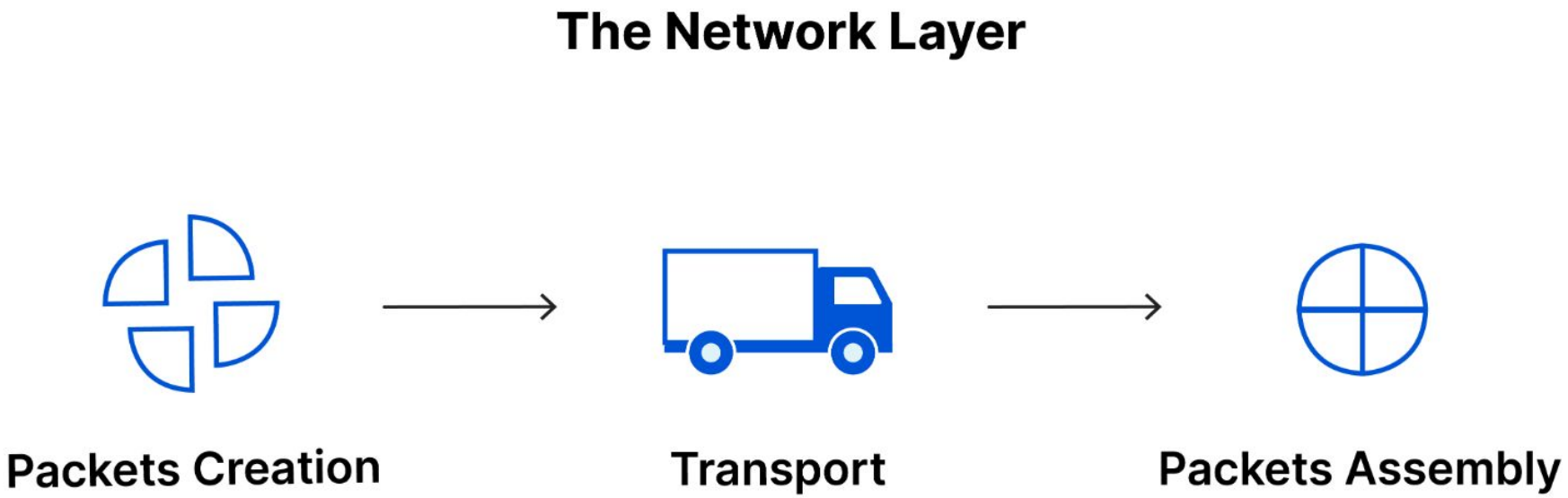


Image Credit
http://cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

KALAMAZOO COLLEGE

Pause: Protocols

A protocol in computer networking is a fundamental set of rules that dictate how data is exchanged over a network. Whether it's ensuring reliable delivery, routing packets correctly, or providing secure communication, protocols are essential for modern digital communication.

The examples can include: TCP, IP, HTTP, FTP, SMTP.

Image Credit

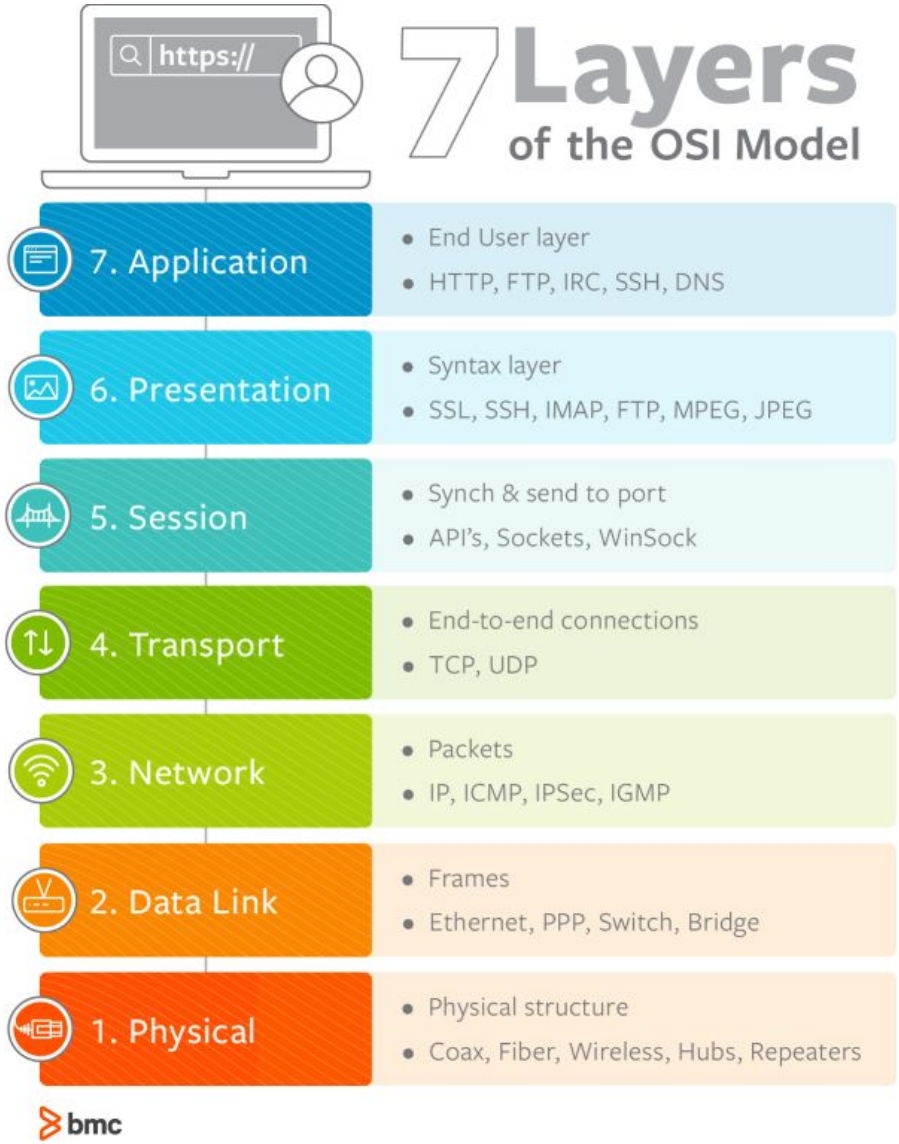


Image Credit
https://www.bmc.com/blogs/osi-model-7-layers/

KALAMAZOO COLLEGE

Pause: IP Address

An Internet Protocol address (IP) is an identifier assigned to devices connected to a network that uses the IP for communication.

- An IPv4 (version 4) address consists of 4 numbers (or "octets") separated by dots. Each number ranges from 0 to 255.
  - Example: 192.168.1.1
- An IPv6 (version 6) addresses are written as 8 groups of 4 hexadecimal digits, separated by colons.
  - Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- These can be dynamic (changing over time) or static (fixed, unchanging) and are assigned by network routers or ISPs (Internet Service Providers).

Image Credit

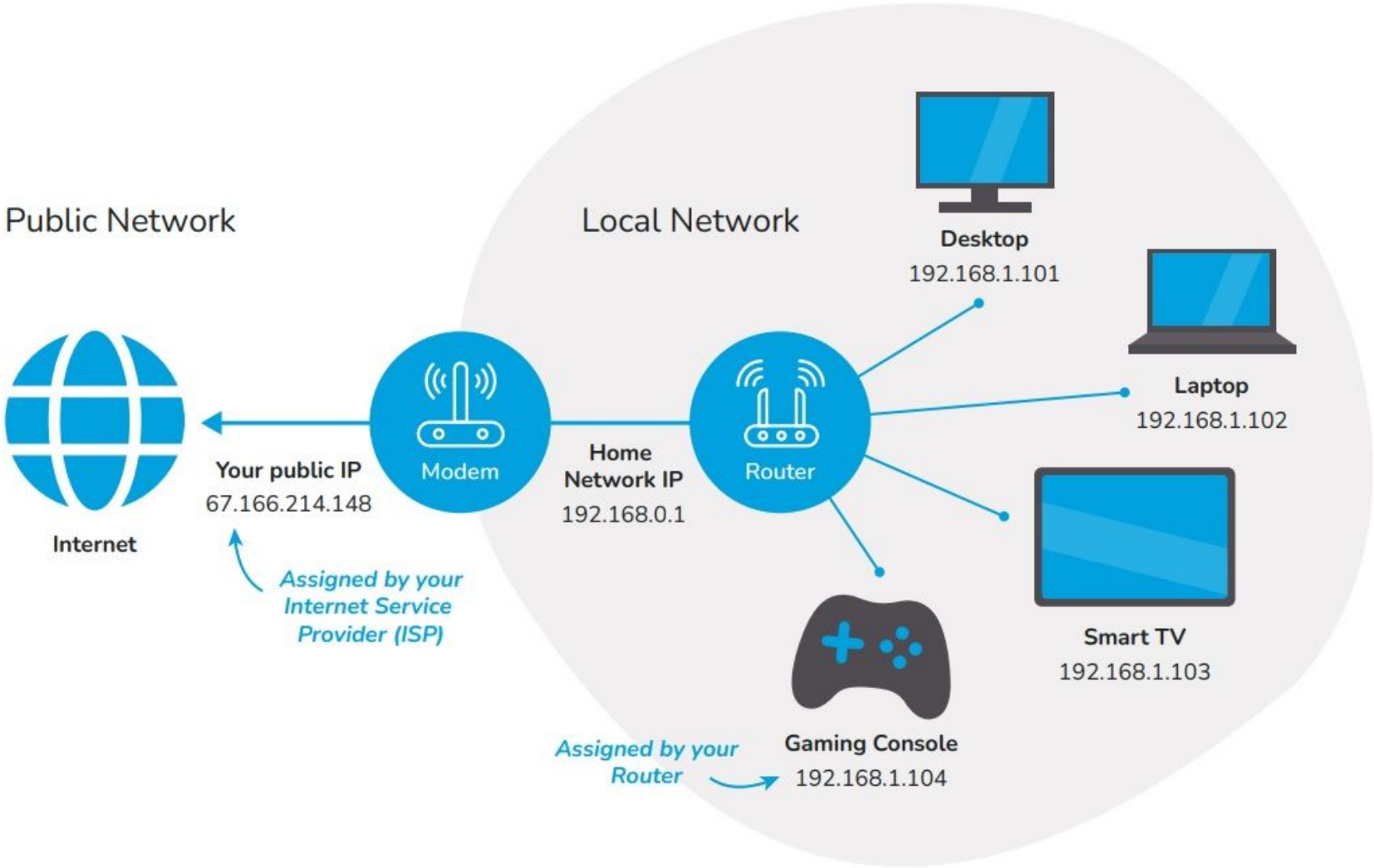


Image Credit
https://www.netgear.com/hub/technology/what-is-router-ip-address/

KALAMAZOO COLLEGE

Pause: Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).

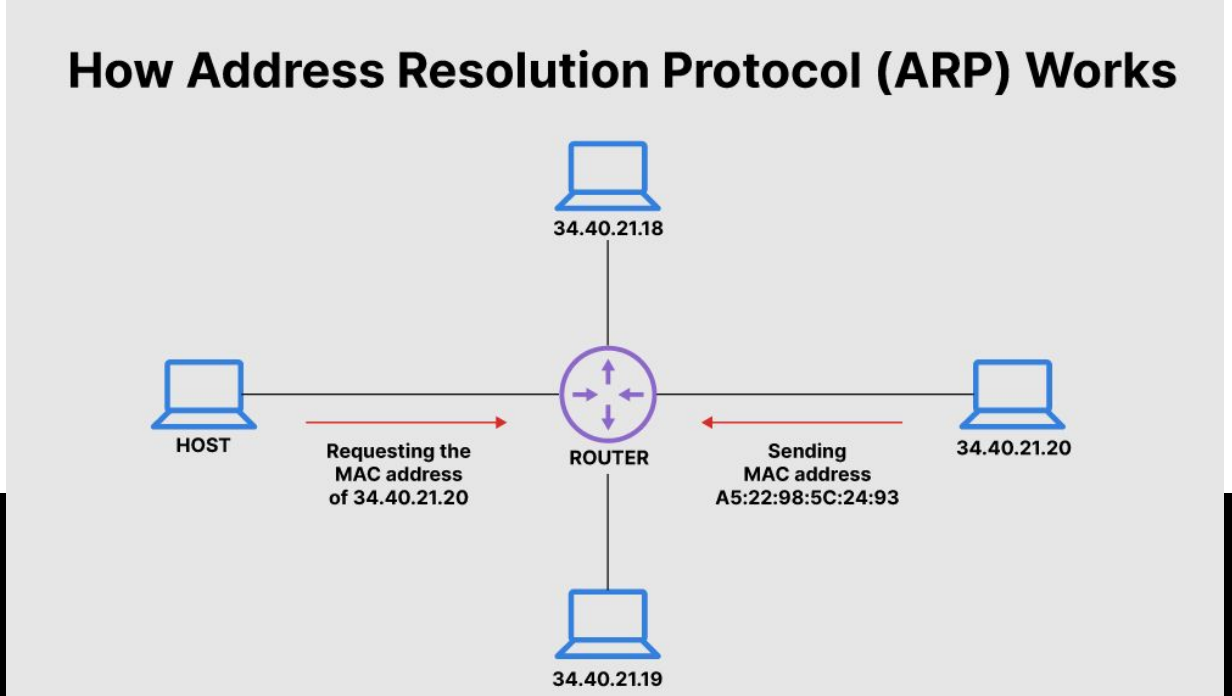


Image Credit: https://www.fortinet.com/resources/cyberglossary/what-is-arp

KALAMAZOO COLLEGE

Networking Basics (continued)

Layer 4: Transport Layer - It is responsible for ensuring reliable data transfer between two devices on a network.

The Transport Layer divides large data from the Application Layer into smaller, manageable chunks (called segments in TCP/IP). At the receiving end, it reassembles these segments back into the original message.

Image Credit

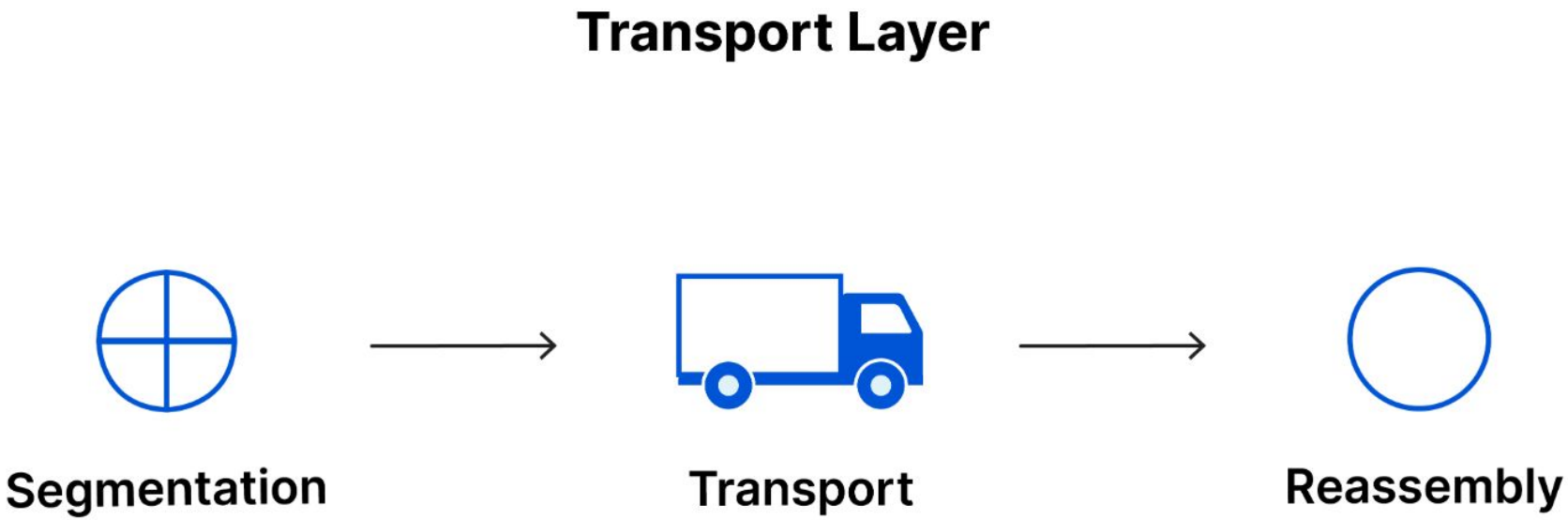


Image Credit
https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

KALAMAZOO COLLEGE

Pause: TCP

The Transmission Control Protocol (TCP) is a protocol in computer networking that ensures reliable, ordered, and error-free delivery of data between devices.

- Before any data transfer happens, TCP establishes a reliable connection between the sender and receiver through a process called the Three-Way Handshake.
- TCP includes a checksum for each packet to verify that the data hasn't been corrupted during transmission. If errors are detected, the data is discarded, and the sender is asked to retransmit it.

Image Credit

Working of the TCP protocol

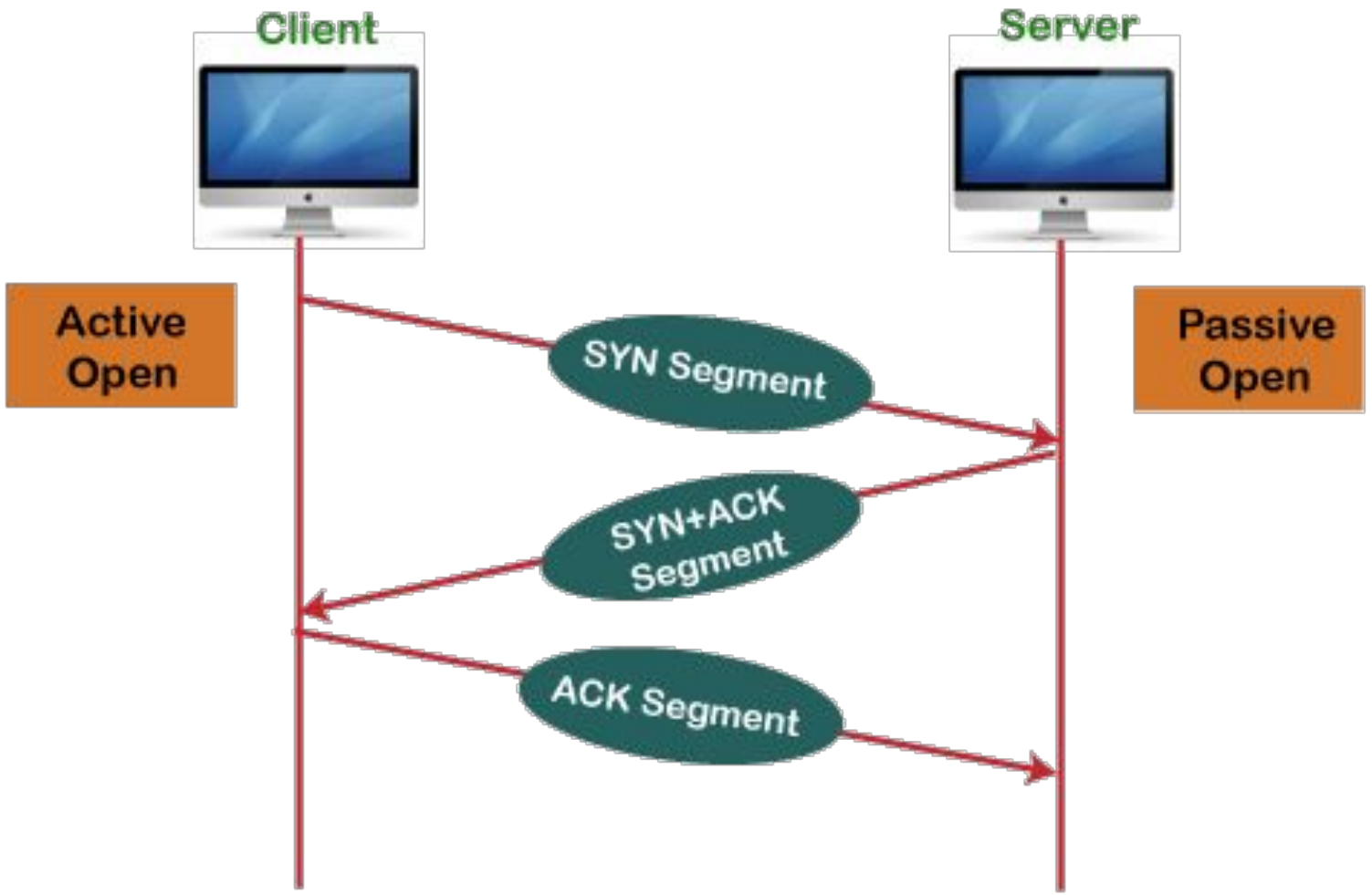


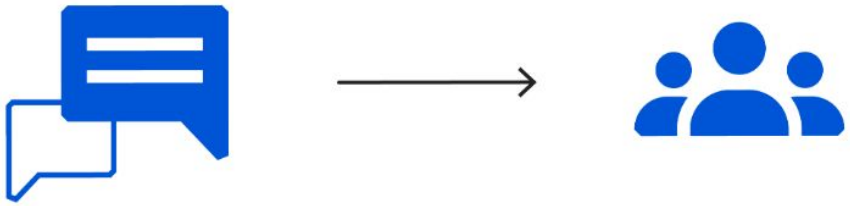
Image Credit
https://www.tpointtech.com/tcp

KALAMAZOO COLLEGE

Networking Basics (continued)

Layer 5: Session Layer - It is responsible for managing sessions or connections between two communicating devices or applications on a network. A session refers to the ongoing communication between two devices for the duration of a transaction or exchange of data.

The Session Layer



Session of communication

Image Credit
https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

KALAMAZOO COLLEGE

Networking Basics (continued)

Layer 6: Presentation Layer - It is responsible for ensuring that the data sent from the Application Layer (Layer 7) is in a format or syntax that can be understood by the receiving system. Essentially, it acts as a translator between the application layer and the transport layer by ensuring that data is properly formatted, compressed, and encrypted for transmission.

Image Credit

The Presentation Layer

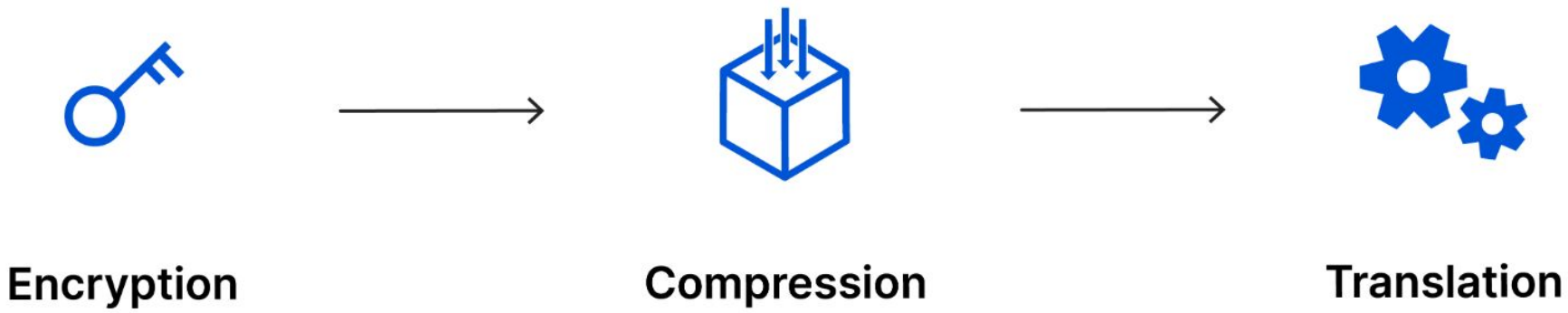


Image Credit
https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

KALAMAZOO COLLEGE

Networking Basics (continued)

Layer 7: Application Layer - It is the layer that directly interacts with end-user applications and provides the interface for communication between the user and the underlying network.

The Application Layer is responsible for providing network services and application protocols that allow programs to communicate over the network.

Networking Basics (continued)

Layer 7: Application Layer
This layer uses various application-level protocols to manage communication between devices. These include:

- HTTP/HTTPS: The web browsing (HyperText Transfer Protocol).
- FTP: The file transfers (File Transfer Protocol).
- SMTP: The Simple Mail Transfer Protocol, used for email sending.
- DNS: The Domain Name System, used to resolve domain names to IP addresses.
- IMAP/POP3: The email retrieval protocols.
- Telnet/SSH: The use of remote login to other systems.

Application Layer

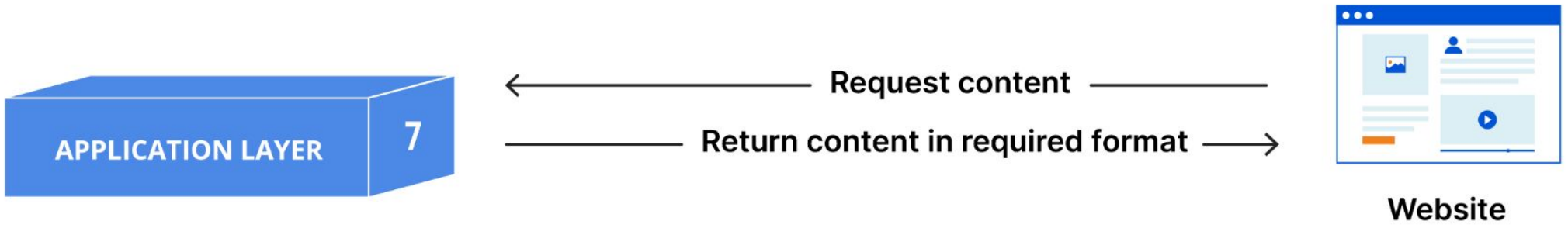


Image Credit
https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

KALAMAZOO COLLEGE

The seven layers of the OSI model

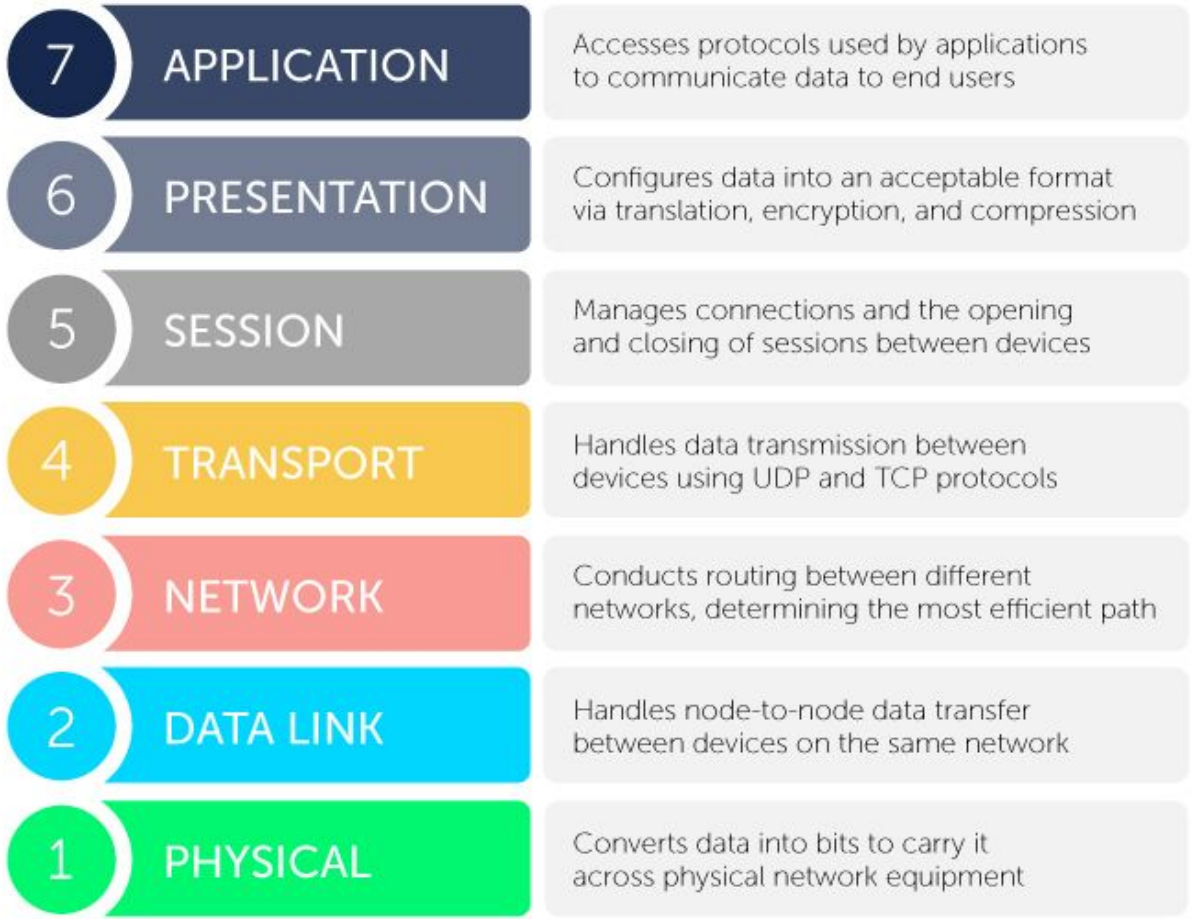


Image Credit
https://bluecatnetworks.com/glossary/what-is-the-osi-model/

KALAMAZOO COLLEGE

Pause: TPC/IP Model

The TCP/IP model (Transmission Control Protocol/Internet Protocol) is a conceptual framework used to understand and implement network communication between different devices over the internet. It's the foundational model for most modern networking systems, including the Internet.

The TCP/IP model is simpler and more focused on real-world protocols and communication methods, specifically for the internet.

- This is what you see implemented in most systems today.

Image Credit

Pause: TPC/IP Model (continued)

TCP/IP Model Layers:

Application Layer (TCP/IP) = Combines OSI's Application, Presentation, and Session Layers.

- This handles end-user applications and network services like HTTP, FTP, DNS, etc. It deals with things like data formatting, encryption, and session management.

Transport Layer (TCP/IP) = Same as OSI's Transport Layer.

- This ensures reliable data transmission and error control. This is where protocols like TCP (reliable, connection-based) and UDP (unreliable, connectionless) come into play.

Pause: TPC/IP Model (continued)

TCP/IP Model Layers (continued):

Internet Layer (TCP/IP) = Corresponds to OSI's Network Layer.

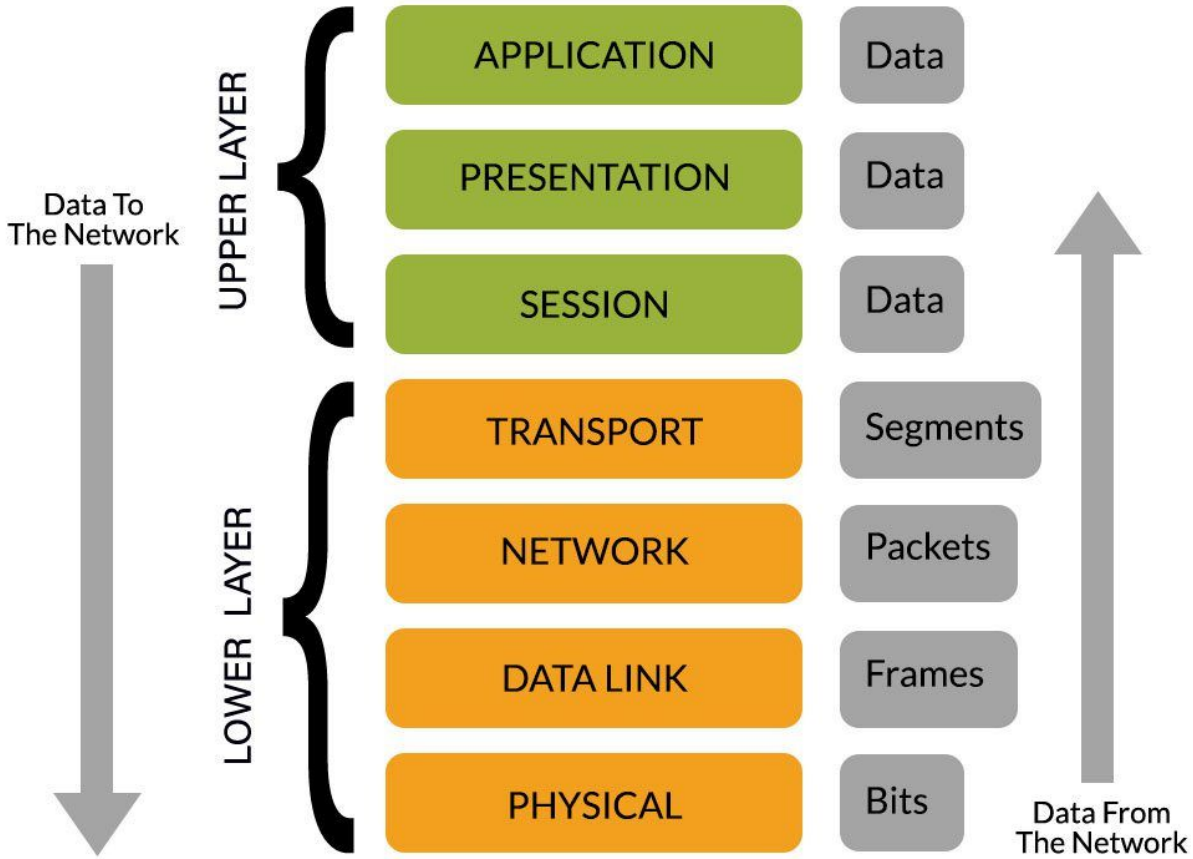
- This is responsible for routing and addressing data packets. It includes IP (Internet Protocol) for logical addressing and routing.

Network Access Layer (TCP/IP) = Combines OSI's Data Link Layer and Physical Layer.

- This deals with the actual transmission of data over physical mediums like Ethernet or Wi-Fi. It manages hardware addressing (e.g., MAC addresses) and the physical transmission of data.

Image Credit

OSI MODEL vs TCP/IP MODEL



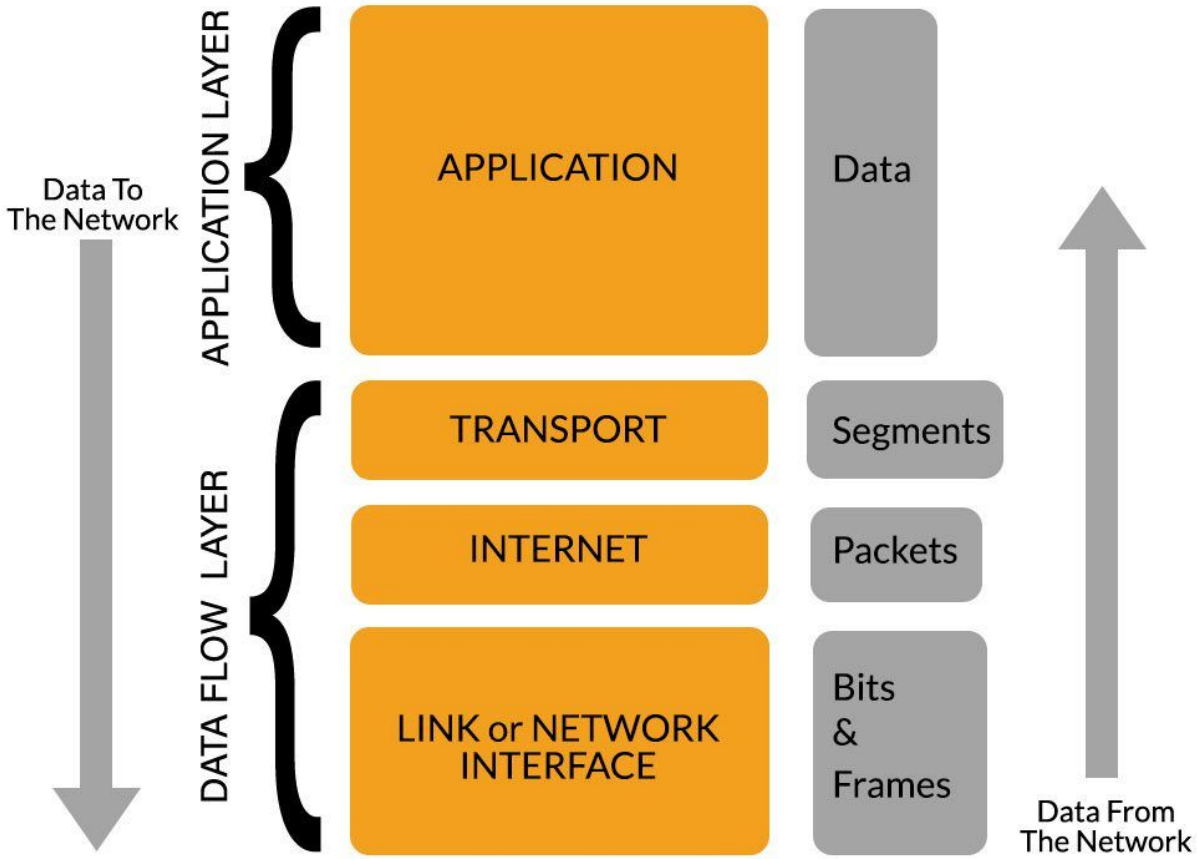


Image Credit
https://www.rtautomation.com/rtas-blog/a-refresher-course-on-osi-tcp-ip/

KALAMAZOO COLLEGE

Man-in-the-Middle (MitM)

Man-in-the-Middle (MitM)

A Man-in-the-Middle (MitM) attack is a type of cybersecurity breach where an attacker secretly intercepts and potentially alters communication between two parties (typically a client and a server) without either party knowing.

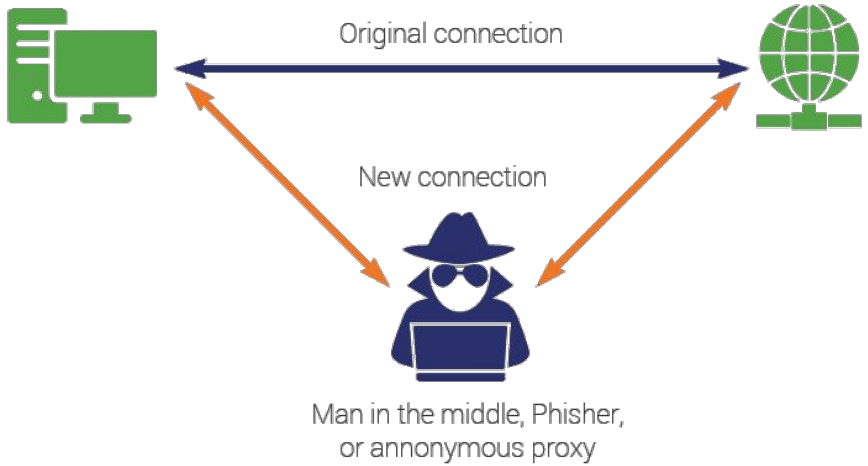


Image Credit
https://www.thesslstore.com/blog/man-in-the-middle-attack-2/

KALAMAZOO COLLEGE

OSI Layer	MITM Attack Type
Application	Cookie Injection, MITB
Presentation	SSL Hijack
Transport	IP Spoofing
Data Link	ARP Poisoning, ICMP MITM

Image Credit

Man-in-the-Middle (MitM) (continued)

The MitM attack can be categorized as any of the following ways:

1. Interception of Communication
2. Eavesdropping
3. Data Modification or Injection
4. Impersonation
5. Decryption of Traffic (If Encrypted)
6. Session Hijacking

Man-in-the-Middle (MitM) (continued)

The MitM examples of attacks are:

- Secure Sockets Layer (SSL) Stripping
  - The attacker intercepts the initial secure connection request, replaces it with an HTTP version, and then forwards it to the destination. Any communication thereafter is unencrypted and can be intercepted or manipulated.

Image Credit
https://www.rapidsslonline.com/ssl/what-is-ssl-stripping-attack/

KALAMAZOO COLLEGE

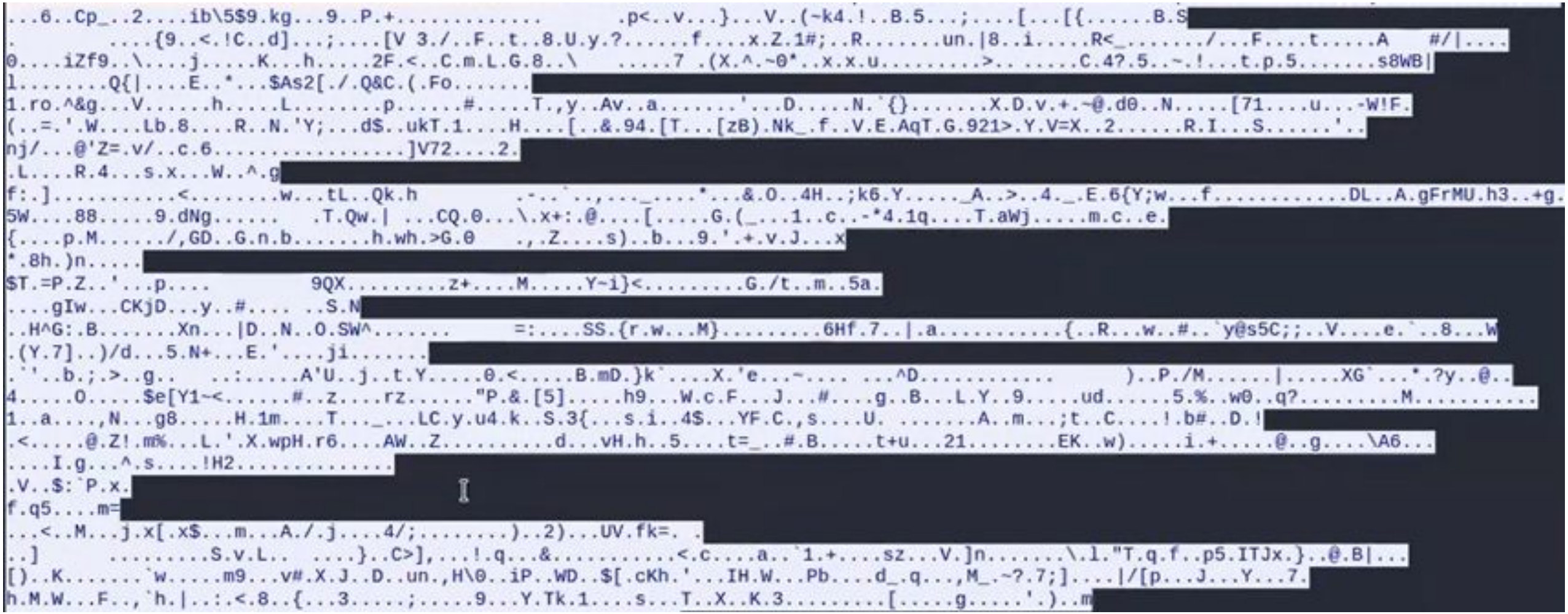


Image Credit

KALAMAZOO COLLEGE

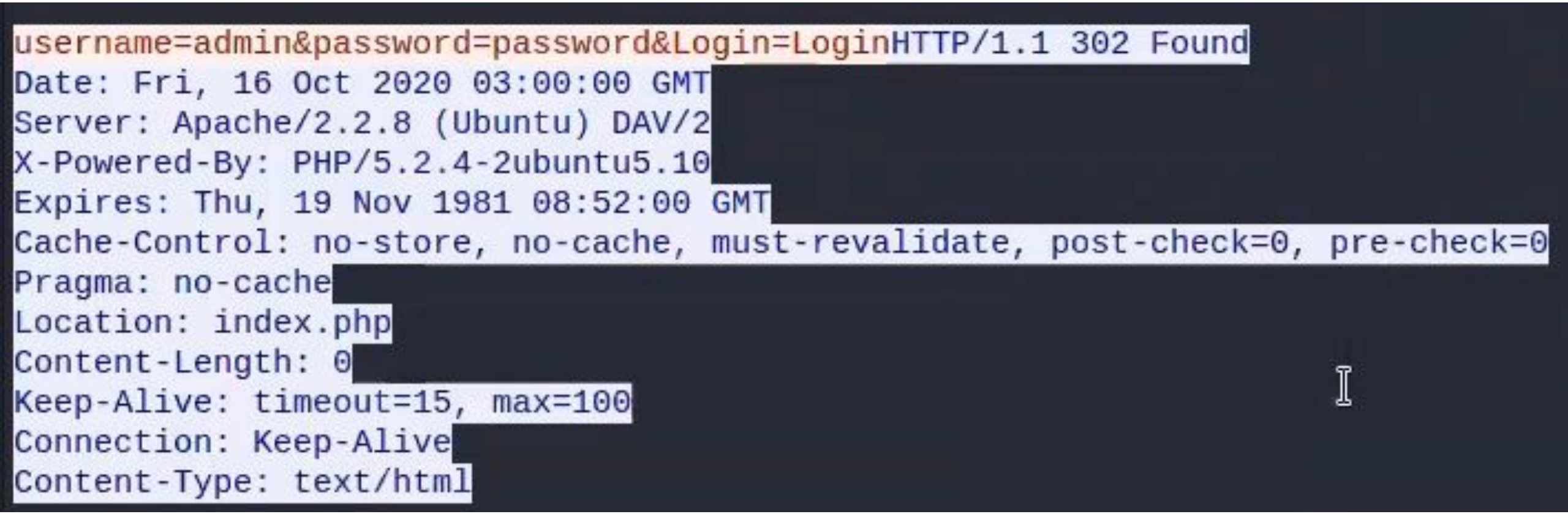


Image Credit

Man-in-the-Middle (MitM) (continued)

- Session Fixation:
  - The attacker forces the victim's web browser to use a session identifier (ID) that the attacker knows. The attacker then waits for the victim to authenticate, and once the session is active, the attacker can hijack it by using the same session ID.

Session Fixation Attack

Image Credit
https://www.thesslstore.com/blog/the-ultimate-guide-to-session-hijacking-aka-cookie-hijacking/

KALAMAZOO COLLEGE

Denial of Service

Denial of Service

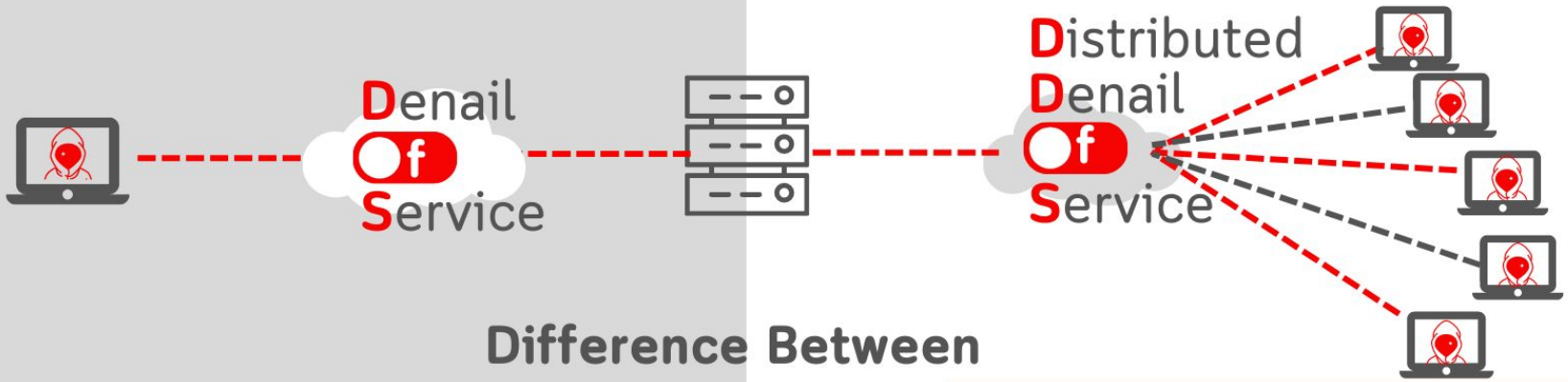
A denial-of-service (DoS) attack is an attempt to make a machine or network unavailable to its legitimate users. Attackers achieve this by overwhelming the target with traffic or malicious requests, causing it to crash or become unresponsive. This can make websites, online services, or entire networks inaccessible.

Pause: Distributed Denial of Service

A Distributed Denial-of-Service (DDoS) attack is a cyberattack where multiple systems flood a target server or network with malicious traffic, making it unavailable to legitimate users.

Unlike a simple DoS attack, which uses one source, DDoS attacks utilize a network of compromised devices (a botnet) to amplify the attack's scale and make it harder to trace back to the source.

Image Credit



Difference Between

It transmits less amounts of traffic.	**Volume of Traffic**	It may transmits much higher amounts of traffic.
Often carried out from a single machine using a script or tool.	**Manner of Execution**	Employs a (C&C) server to coordinate numerous hosts infected with malware (bots), resulting in a botnet.
Tracking the true origin is significantly less difficult .	**Tracing of Source**	Tracking the true origin is significantly more difficult .
It is simple to identify and terminate the connection.	**Ease of Detection**	A DDoS attack, on the other hand, emanates from several locations, hiding its origins.
DDoS attack may be deployed less quicker.	**Speed of Attack**	DDoS attack may be deployed much quicker.

zenarmor

Image Credit
https://www.zenarmor.com/docs/network-security-tutorials/dos-vs-ddos-attacks

KALAMAZOO COLLEGE

Denial of Service (continued)

We have a lot of different types of Denial of Service attacks, a few are listed here:

1. Internet Control Message Protocol (ICMP) Flood
   a. This floods the target with ICMP echo requests (pings), overwhelming its processing power.
2. SYN Flood
   a. This sends a large number of TCP-SYN packets to the target, preventing legitimate connections
3. User Datagram Protocol (UDP) Flood
   a. This sends a flood of UDP packets to the target, exhausting its resources. This doesn't require a connection to be maintained.

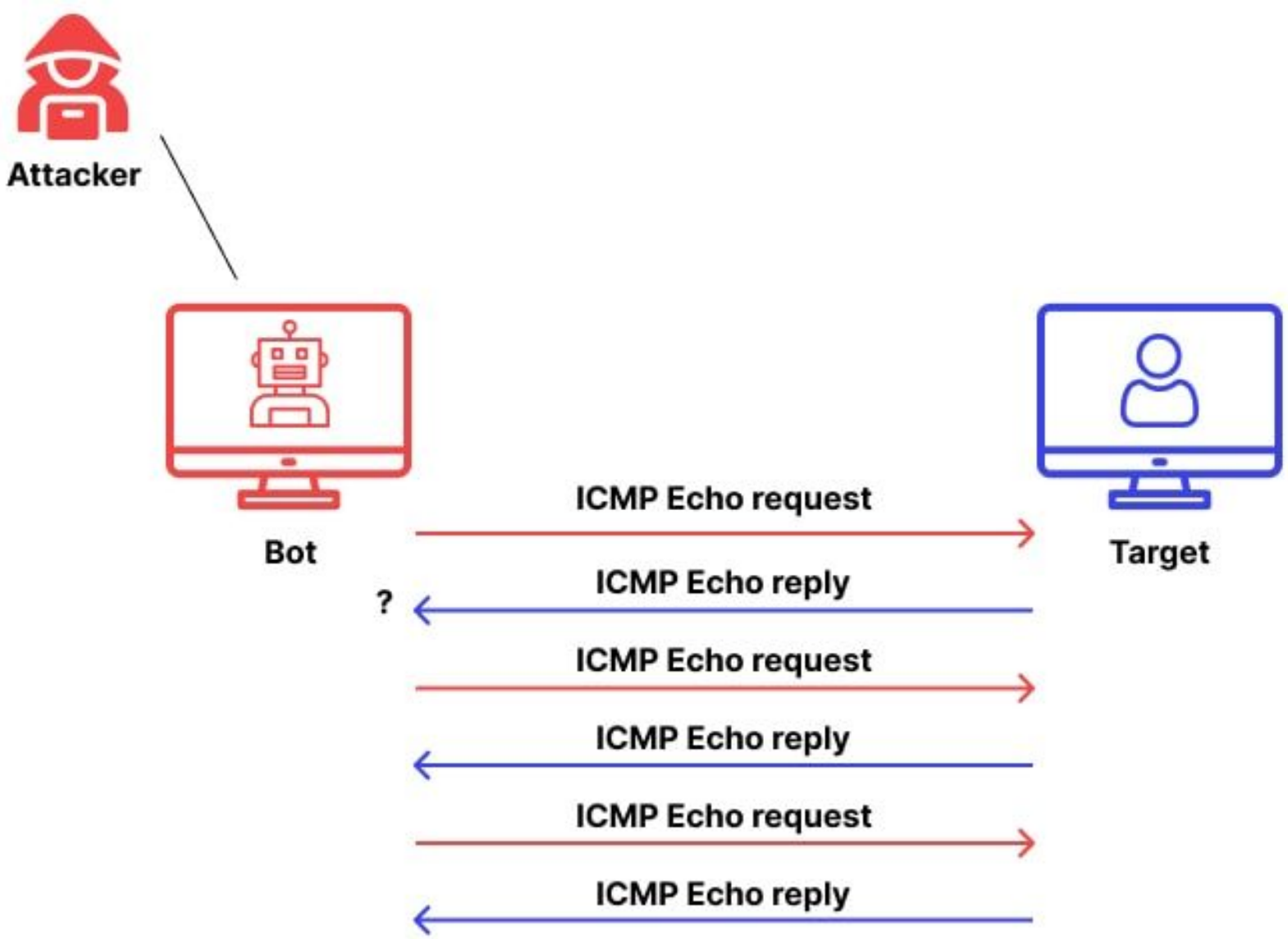


Image Credit
https://www.wallarm.com/what/what-is-a-ping-flood-dos-attack

KALAMAZOO COLLEGE

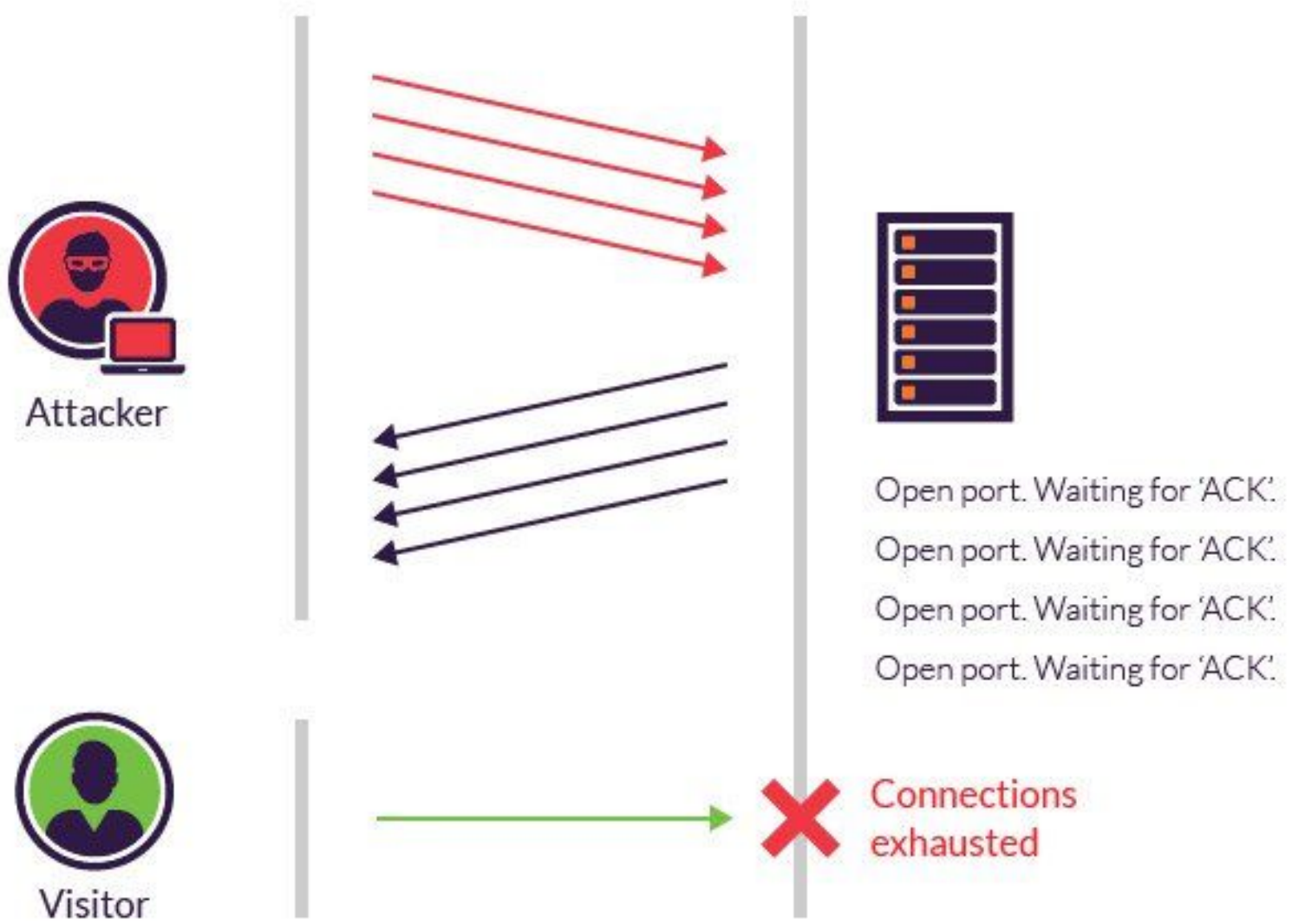
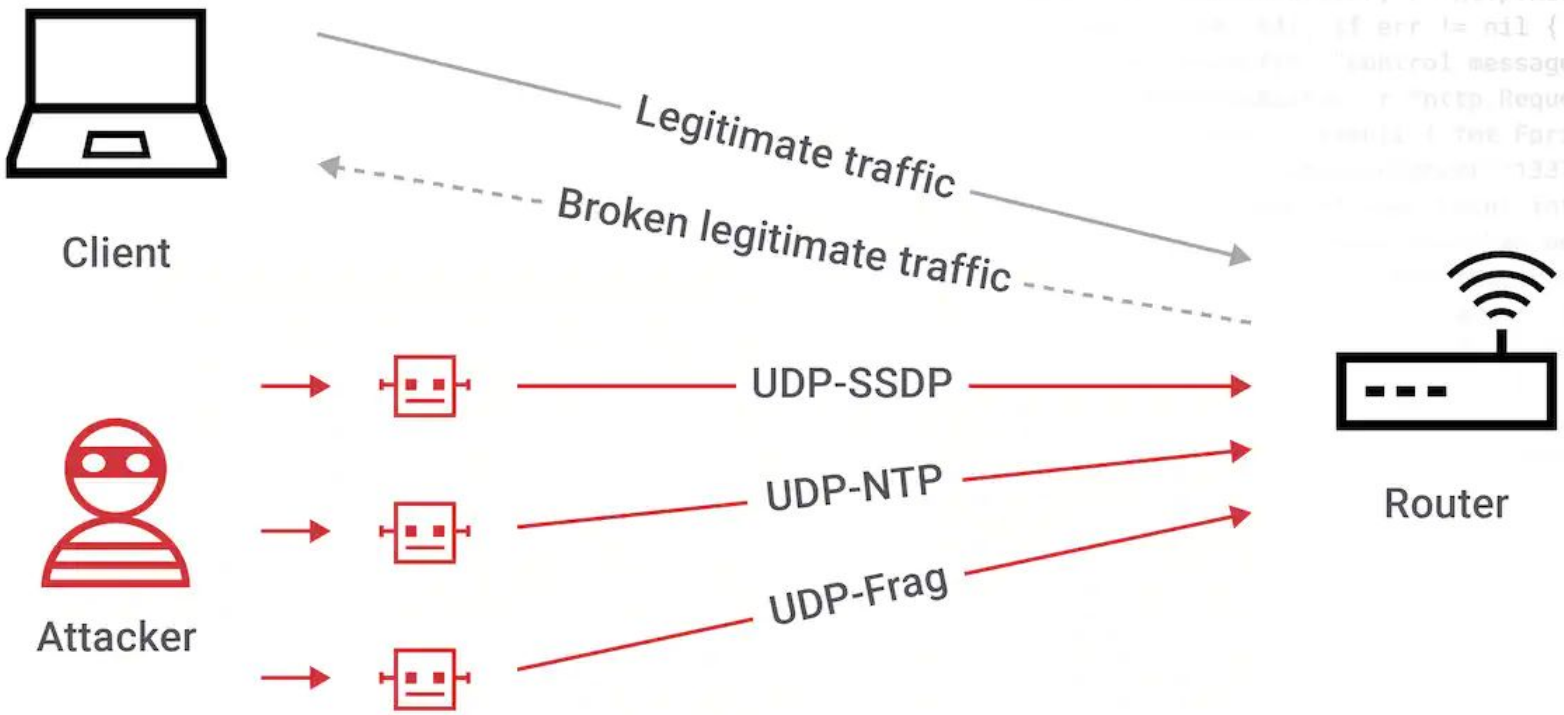


Image Credit
https://www.wallarm.com/what/what-is-a-ping-flood-dos-attack

KALAMAZOO COLLEGE



What is a UDP flood attack?

Akamai

Image Credit
https://www.akamai.com/glossary/what-is-udp-flood-ddos-attack

KALAMAZOO COLLEGE

Spoofing

Spoofing

Spoofing is a cybercrime where someone disguises their identity to appear as a trusted source, often for malicious purposes like gaining access to systems, stealing data, or distributing malware.

Image Credit
https://www.terranovasecurity.com/solutions/security-awareness-training/what-is-spoofing

KALAMAZOO COLLEGE

Spoofing (continued)

We have many different types of spoofing, a few of these types of attacks can be seen below:

- DNS Spoofing (DNS Cache Poisoning)
  - The attacker poisons the DNS cache of a target system, redirecting them to a fake server.
  - The attacker might change the victim's DNS cache so that when they try to visit a legitimate website, they are instead redirected to a malicious website.

Pause: Domain Name System (DNS)

This is a system that translates domain names into IP addresses. It's often called the "phonebook of the internet"

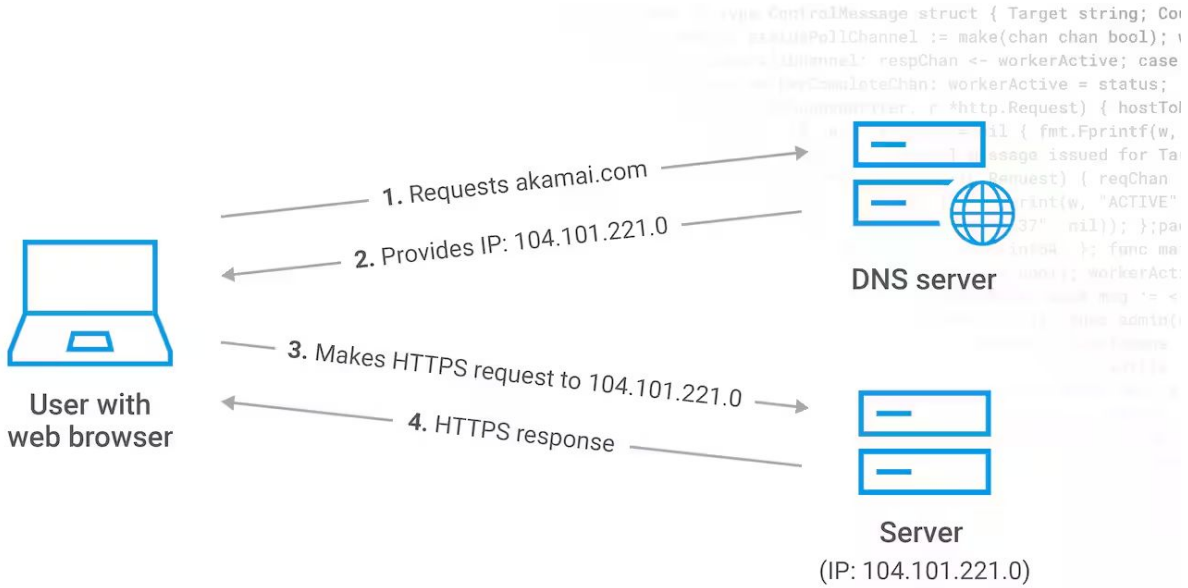


Image Credit
https://www.akamai.com/glossary/what-are-dns-servers

KALAMAZOO COLLEGE

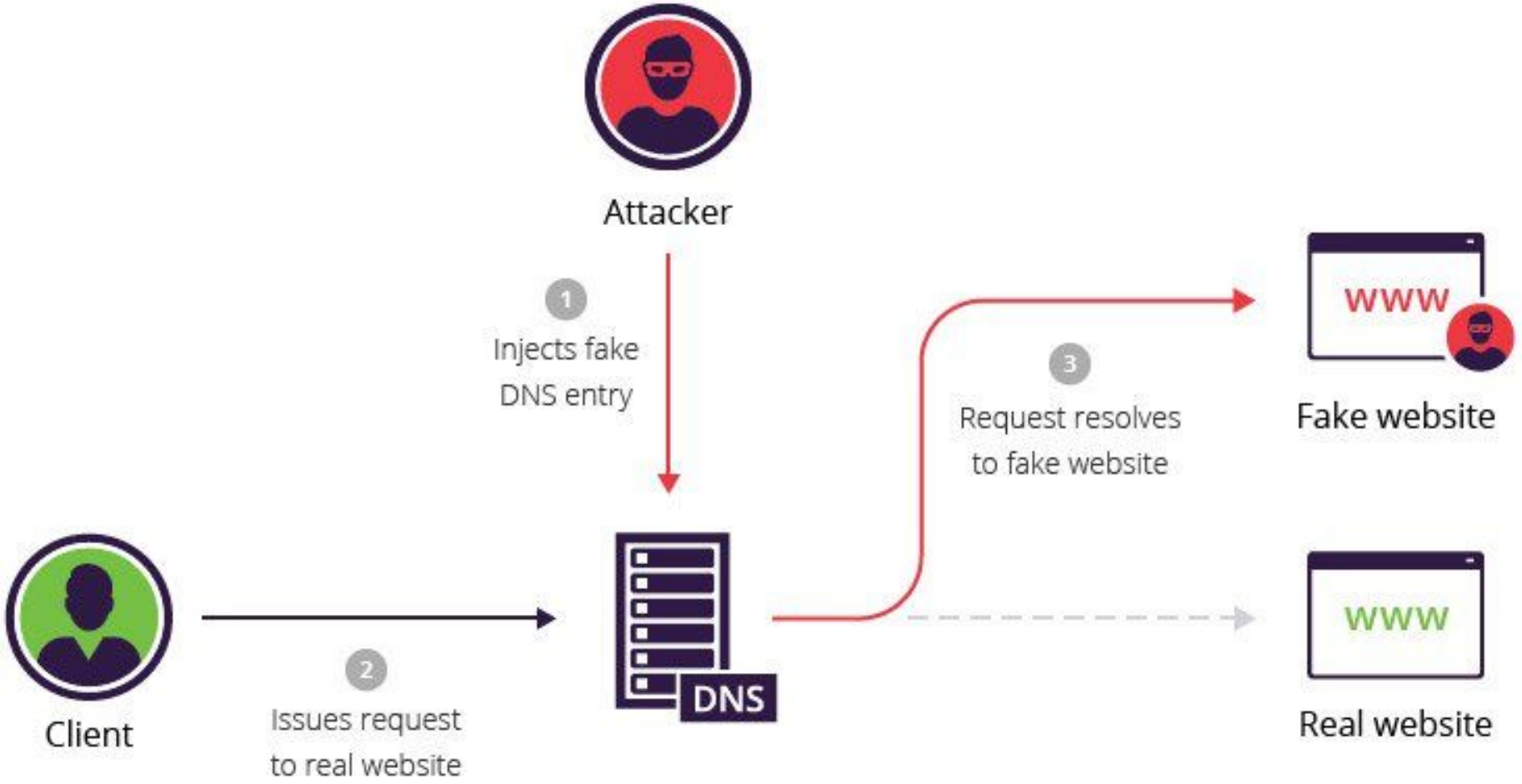


Image Credit
https://www.imperva.com/learn/application-security/dns-spoofing/

KALAMAZOO COLLEGE

Spoofing (continued)

- ARP Spoofing (Address Resolution Protocol)
  - ARP spoofing is commonly used in local area networks (LANs). In this attack, the attacker sends falsified ARP messages over the local network, associating the attacker's MAC address with the IP address of a legitimate device (like a router or server).
  - This allows the attacker to intercept, modify, or block communication between devices on the network.

Image Credit

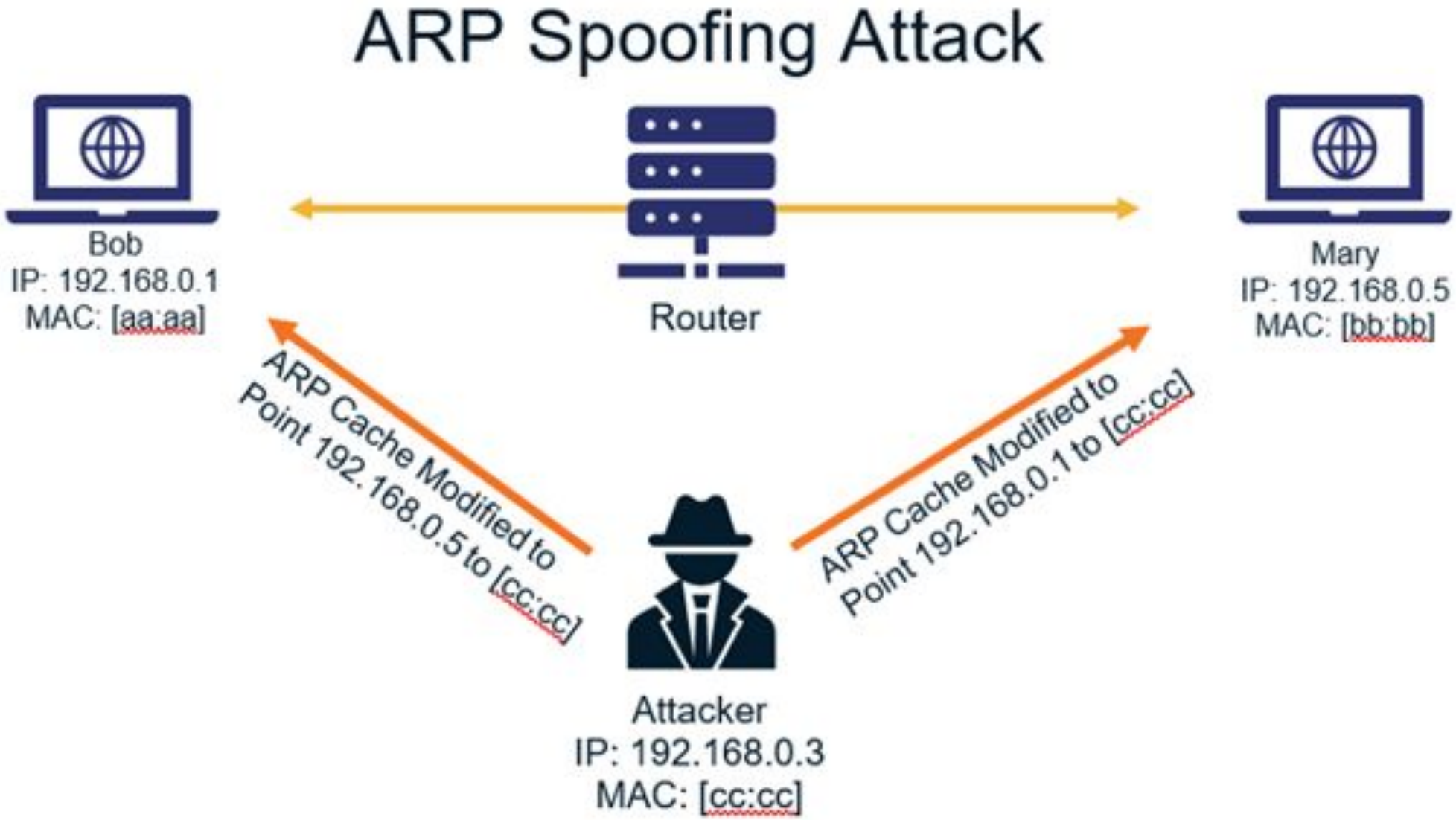


Image Credit
https://www.thesslstore.com/blog/everything-you-need-to-know-about-arp-spoofing/

KALAMAZOO COLLEGE

Spoofing (continued)

- IP Spoofing (Internet Protocol)
  - The creation of IP packets with a false source IP address to impersonate another computer system.
  - This allows cybercriminals to carry out malicious actions, often without detection.

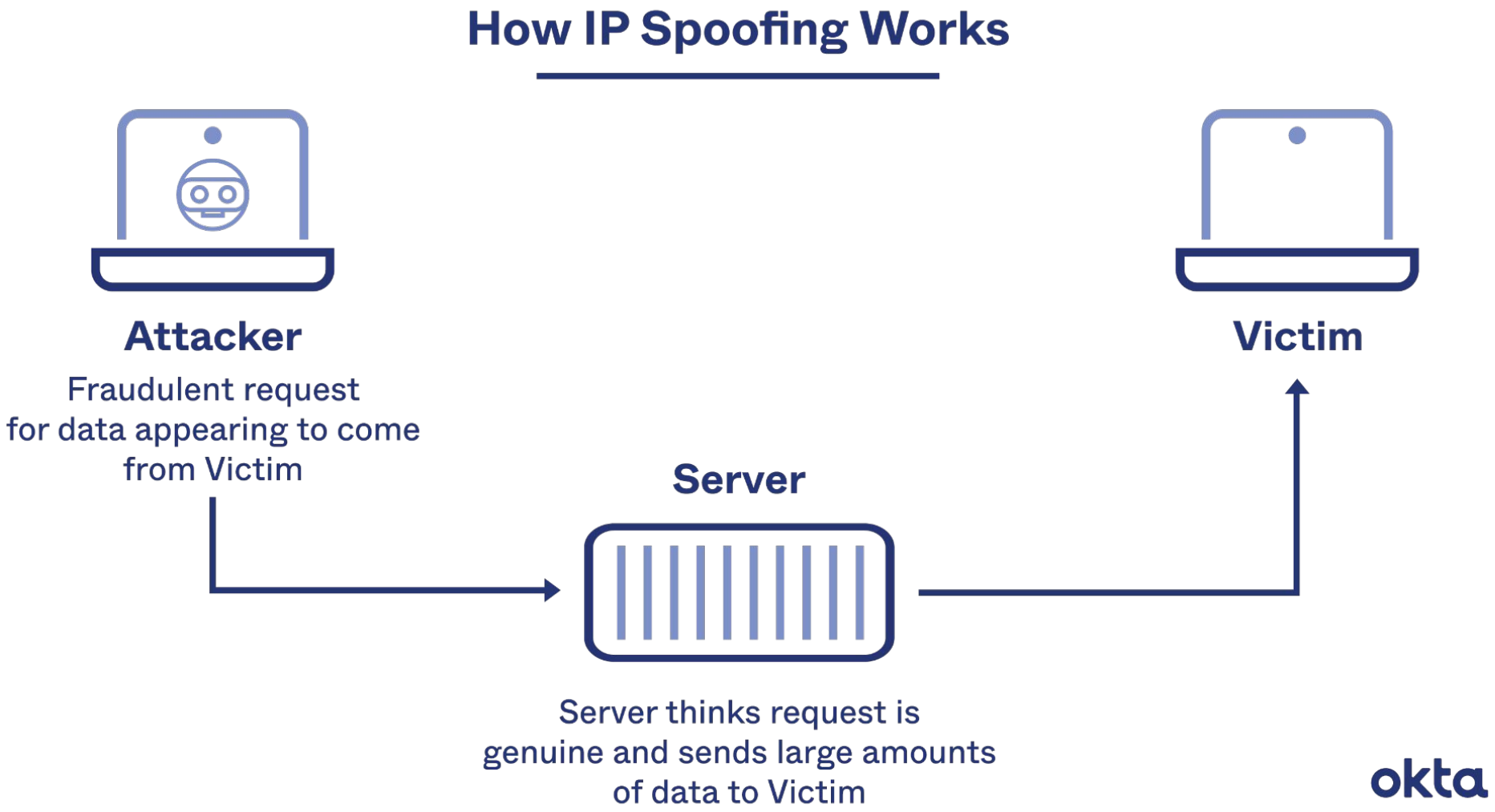


Image Credit
https://www.okta.com/identity-101/ip-spoofing/

KALAMAZOO COLLEGE

Continue Activity/TryHackMe/Ideas

You can use the rest of the time to continue working on your Keylogger and Buffer Overflow. I have posted a few resources on the website.

OR

You can learn more about networks using the TryHackMe resources

OR

You can work on your presentation ideas or project ideas

Questions?