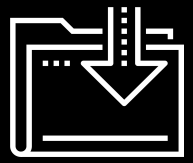
Introduction to Networking

Cybersecurity

Networking 101, Day 1



Class Objectives

By the end of today's class, you will be able to:

Identify clients, servers, requests, and responses in network communications.

Identify network topologies and compare their advantages and disadvantages.

Design a conceptual network made of various network and network security devices.

Convert binary numeric representations into readable IP addresses and determine which servers the IP addresses belong to.

Modify host file to circumvent DNS and redirect access of a website.

Introduction to Networks and Network Security


Today, we will be switching gears to focus on one of the most important topics in cybersecurity: **networking**.

Computer Networks

A computer network consists of multiple devices connected together to share resources and services.

Services:
Online order processing, GPS, online gaming, video streaming

Resources:
Web pages, email images, data files

Devices (nodes):
Computers, laptops, cell phones, printers, servers

Computer Networking

Knowledge of computer networking is essential for the following technical roles:

Security operations center (SOC) staff	Network security engineer	Penetration tester
Commonly diagnose and troubleshoot network-related security issues and attacks. Understanding network devices and design can help them quickly resolve and identify these issues.	May work on the design of a company's network architecture to protect their organization from security risks.	Test for vulnerabilities within a company's network. Understanding network design and common network vulnerabilities is core knowledge for penetration testers.

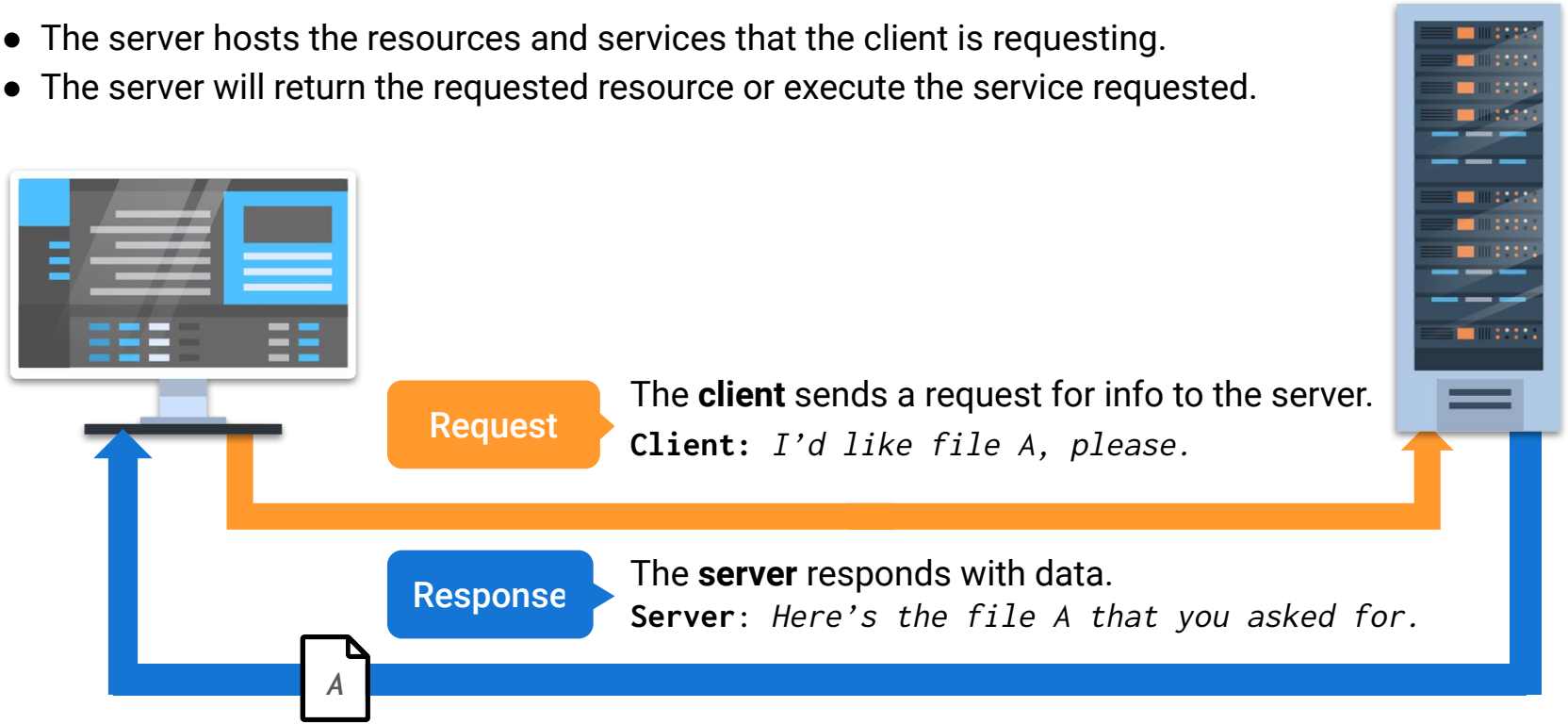
The Client-Server Model

The **client-server model** is a network computing model that defines how resources and services are shared across a network.

Client-Server Model

The client requests a resource or a service.

- The server hosts the resources and services that the client is requesting.
- The server will return the requested resource or execute the service requested.



Client and Server Example

Let’s take the example of a webpage.

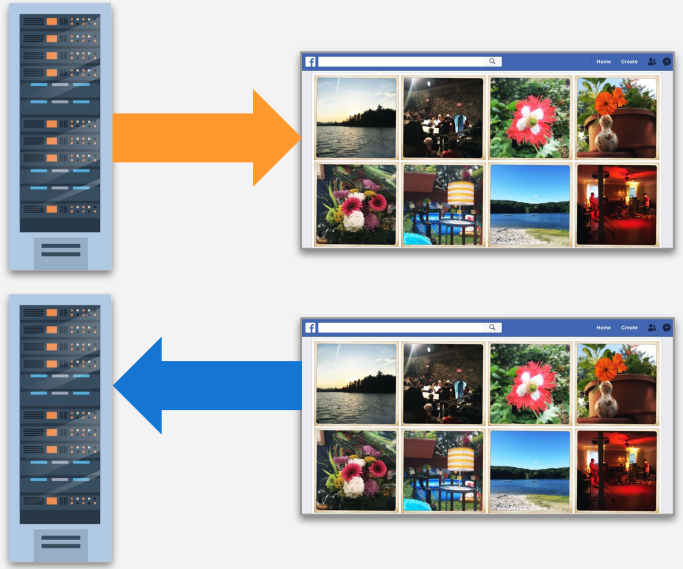
You want to view the vacation photos your friend posted on Facebook. When you view them...

Request

..the browser is making a request: ***“Facebook, can you please get me my friend’s vacation photos?”***

Return

Facebook’s web server provides a response: ***“Yes, here are your friend's vacation photos.”***



This two-way conversation between the client and server is known as the request and response method of device communication.

Client-Server Model

01

The **request** is the process in which the client sends a message to a server asking for a resource or to run a service.

02

The **response** is sent back to the client after the server receives and processes the request.

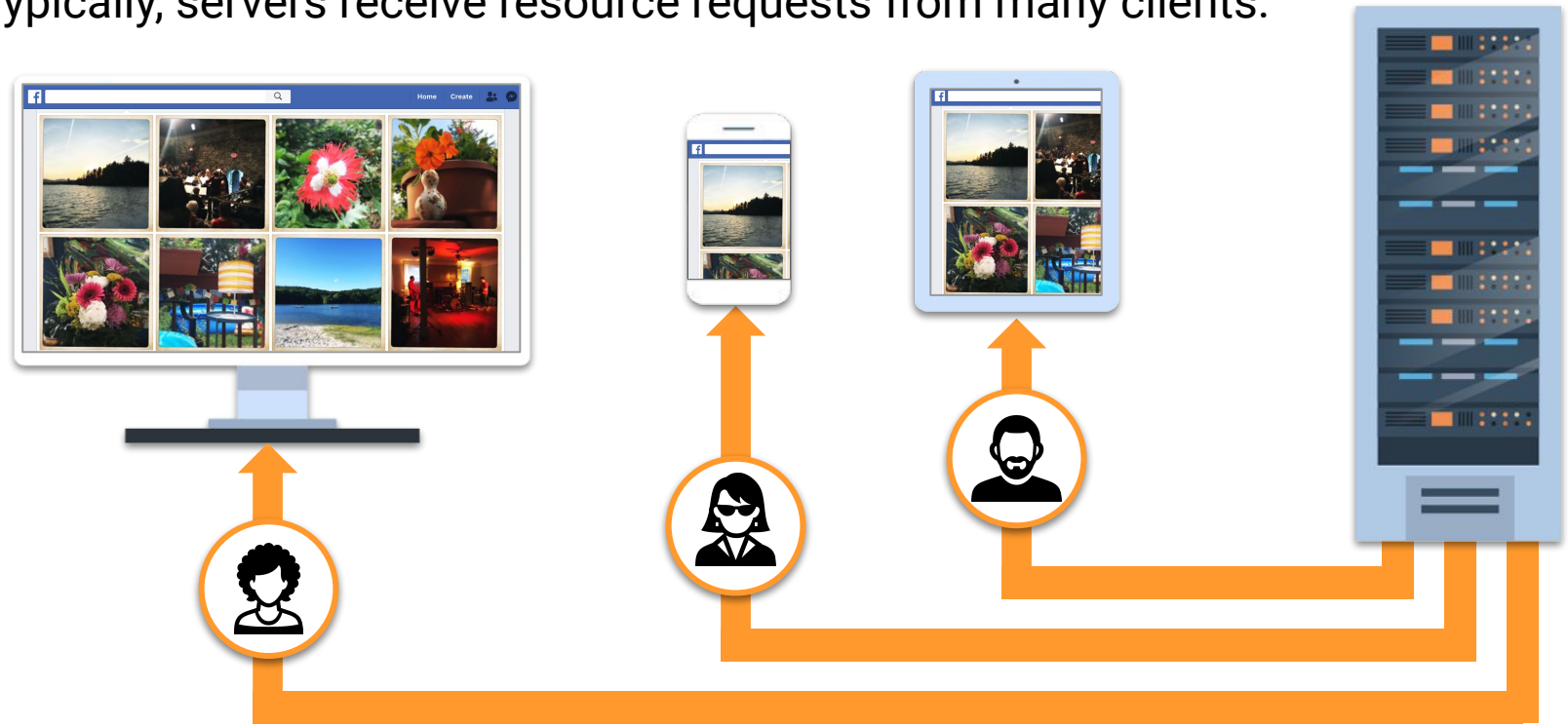
03

The **response message** could be:

- An acknowledgement of the request.
- A requested resource.
- An error message.

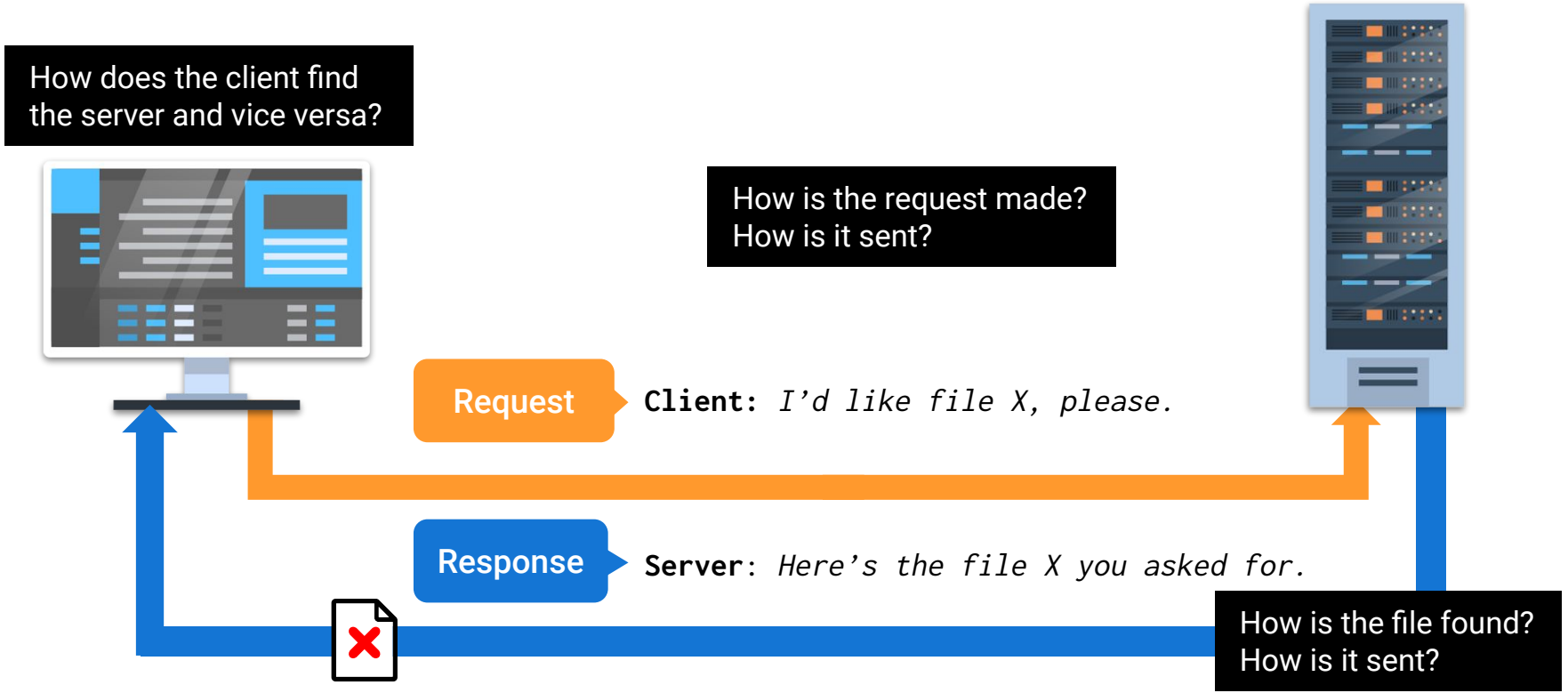
One Server, Many Clients

The client-server model is not a “one client, one server” relationship.
Typically, servers receive resource requests from many clients.



Client-Server Model Continued

There's a lot to learn about this *"simple"* process.



Introduction to Network Security

As we cover the tools and processes within the wide scope of networking, we will also discuss threats and risks.

Network security is the practices and policies used to protect and monitor a computer network's resources against threats and risks.

Network Security

These risks and threats can include:

- Unauthorized access into networks
- Denial of service (DoS) attacks
- Eavesdropping
- Data modification


As security professionals, you will often be asked to not only monitor and identify potential network security threats and risks, but also to determine the best way to mitigate them.

Activity: Network Security

In this activity, you will play the role of a security analyst at Acme Corp.

- Several suspicious activities have occurred on Acme's products and systems.
- For each suspicious activity, you must list out the client and servers, and then describe the request and response in simple terms.

Suggested Time:

10 Minutes

Time's Up! Let's Review.

Questions?

Network Structure

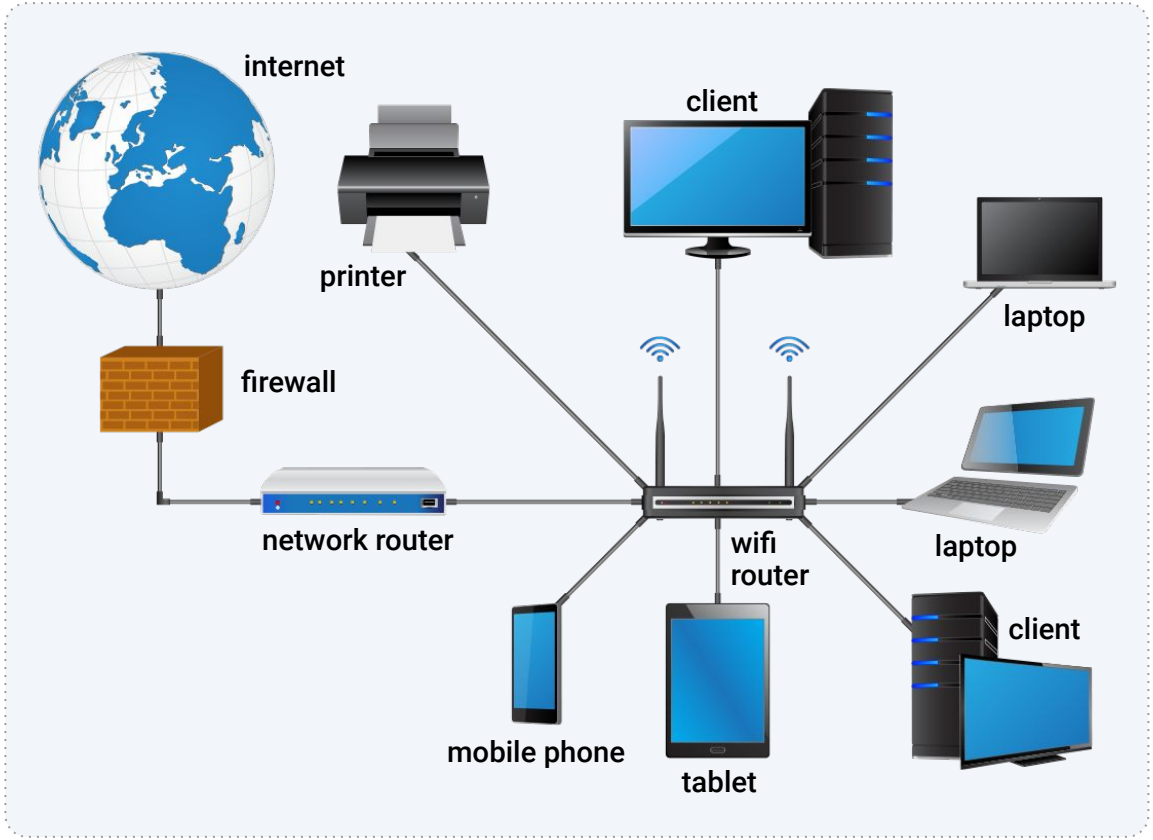
As mentioned, a computer network consists of multiple devices (nodes) connected to each other.

But how exactly are they connected?

Local Area Network

When computer networks were first created, they were smaller private networks designed to connect devices within the same room or building.

This type of network is a **local area network (LAN)**.



A **Local Area Network (LAN)** is a private computer network that connects devices in smaller physical areas.

Advantages of using a LAN

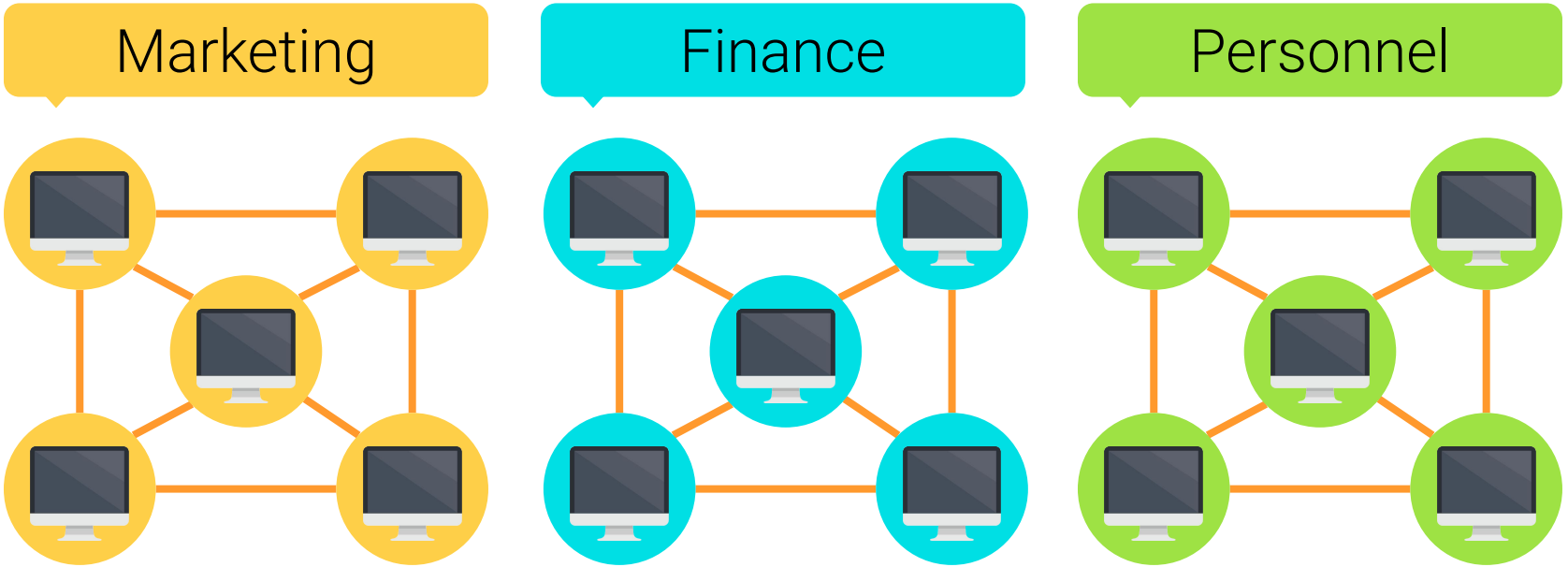
Network speed and performance:
Since the devices are physically near each other, connections are significantly faster and perform better.

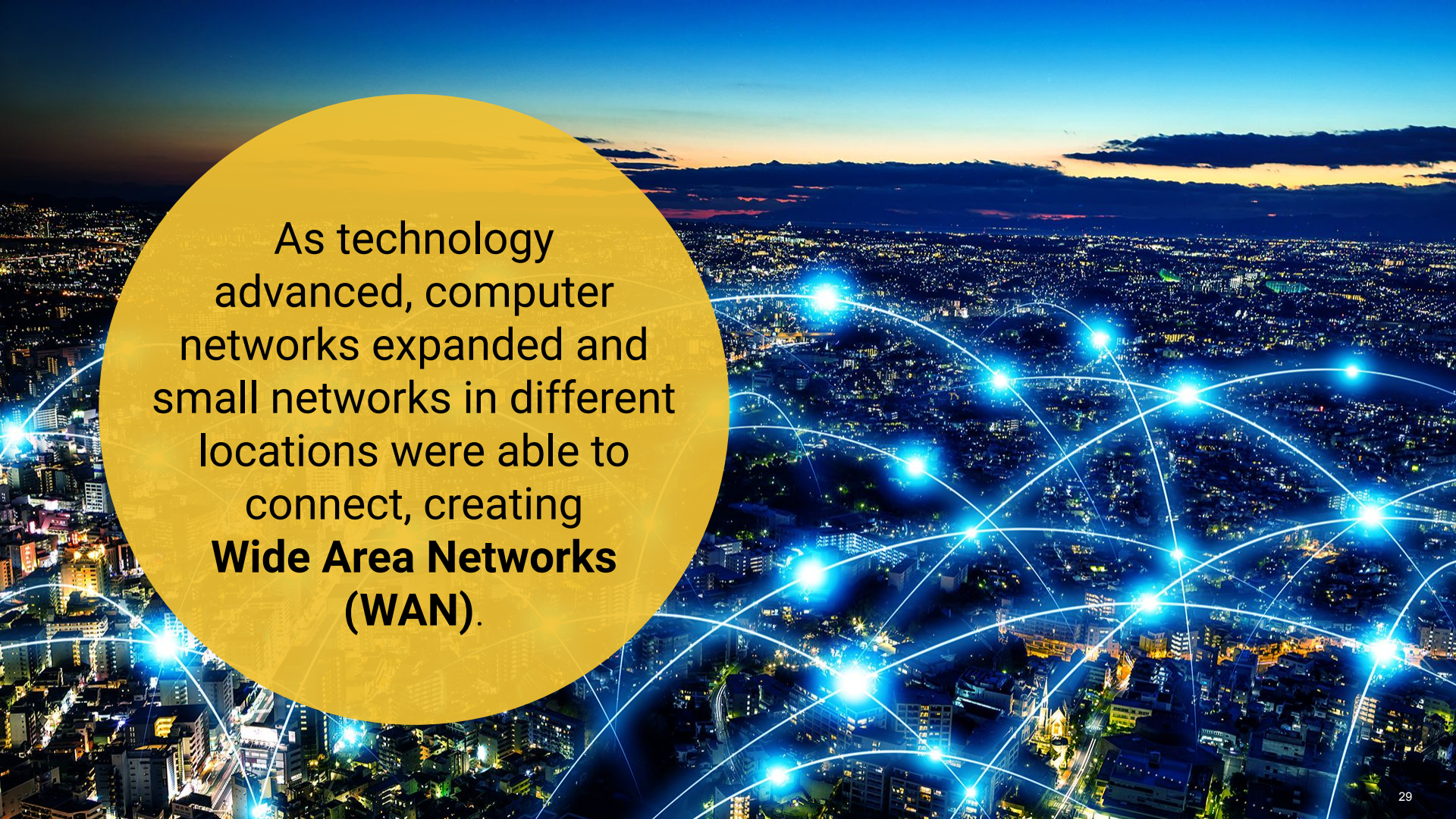
Network security:
With security devices, a business can control what data comes in and out of their local network as well as who has access to resources.

Versatility:
New network devices can be easily added or removed inside a LAN due to the proximity of the devices within the network.

Local Area Network

Larger companies often have multiple LANs for different departments or offices within their organization. While these local area networks are great for sharing resources, they are limited to sharing only within their own network.




As technology advanced, computer networks expanded and small networks in different locations were able to connect, creating **Wide Area Networks (WAN)**.

A **Wide Area Network (WAN)** is a network used to connect multiple LANs.

The most widely-known example of a WAN is the Internet.

Wide Area Network

Advantage

You are able to share or access resources across a much larger geographic area.

Disadvantages

Security issues: Traffic that travels from your LAN and into a WAN needs to be encrypted and never captured.

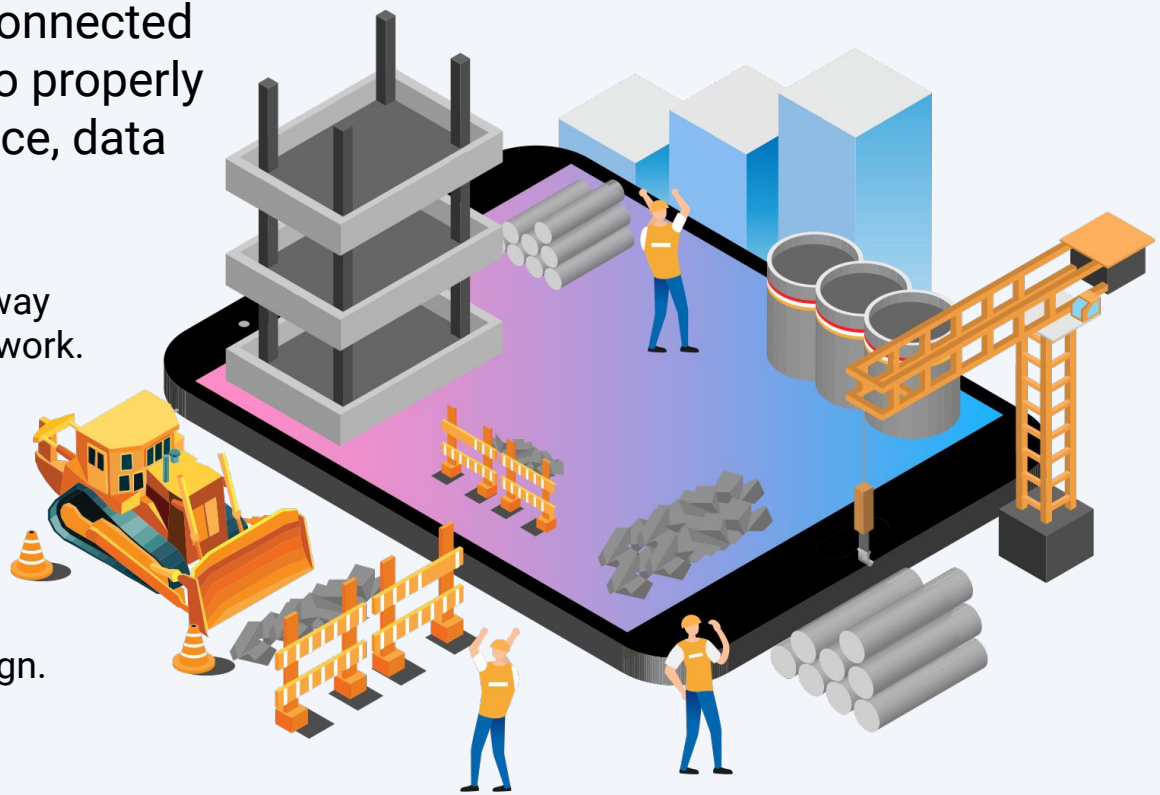
Troubleshooting: Traffic issues outside of your LAN can be challenging to troubleshoot and resolve.

Network topology is the design or technique with which computers are set up on a network.

Network Topology

Machines on a network are connected in a specific design in order to properly serve the required performance, data flow, and security factors.

- The topology can determine the way data flows within a local area network.
- The topology can also impact the performance and speed of a network.
- There are a variety of network topologies, with names based on the geometric shape of their design.



Network Topologies: Ring

In a **ring** topology, each device is connected to the next device in the chain.

Network Topologies: Ring

There are two sub-types of ring topologies:

01 Bidirectional

The topology allows traffic to move in either direction.

02 Unidirectional

The traffic flows in a single direction.

For this lesson, we will be referring to the **Unidirectional** Ring Topology.

Network Topologies: Ring

Advantages

- Simple to build.
- Does not require a central node to manage data transmission.
- Adding devices to the network is easy.

Disadvantages

- If any one device goes down, the entire network is affected. In other words, every device is a point of failure.
- Latency (how long it takes for data to travel between devices) is variable between devices on the network. For example, one-way communication between two devices will be relatively quick from device A to device B, but it will be relatively high for communication when B needs to communicate back to A.

Network Topologies: Linear

In a **linear** topology, each device is connected to the adjacent device by a two-way link.

The two devices at the “ends” of the network are not connected to one another (unlike a ring topology).

Network Topologies: Linear

Advantages

Adding devices to the network is easy.

Disadvantages

- A single device failure can interrupt the entire network.
- Latency is variable between devices on the network. For example, devices near one another will trade data quickly, but devices far away will experience high communication delay.

Network Topologies: Star

In a star topology, all devices in the network are attached to a central node.

Devices transmit data by sending it to the central node, which then determines which other device on the network to forward it to.

Network Topologies: Star

Advantages

- Communication delay is consistent between devices, since every node is the same distance from the central manager, which is ultimately responsible for forwarding data.
- Failure of an end device doesn't endanger the entire network—the node is the only point of failure.
- Extending the network is easy.

Disadvantages

- The number of devices on the network is constrained by the number of connections available on the central node.
- Can be difficult to set up if the central node is physically far away from any of the end devices.

Network Topologies: Bus

In a **bus** topology, every device is attached to a central data link. When a device transmits data, it sends it on the link, at which point every device on the network can receive it simultaneously.

Network Topologies: Bus

Advantages

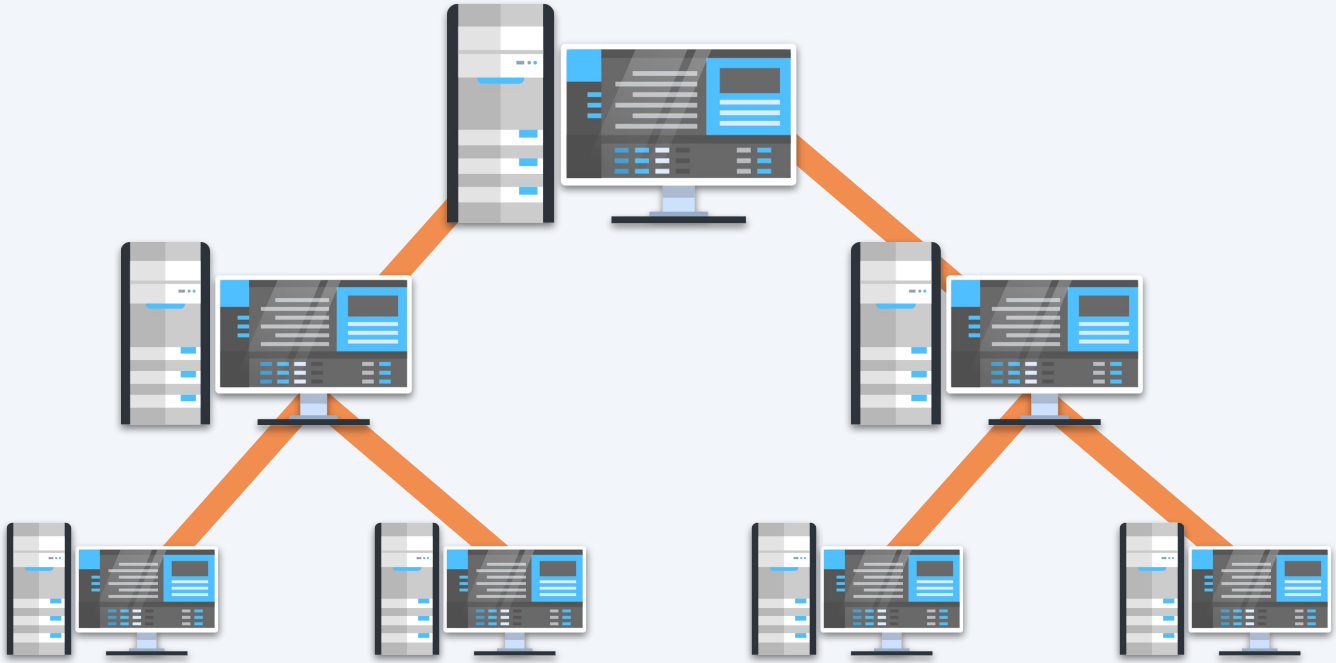
- Data transmission is fast between all devices.
- Easy to expand the network.

Disadvantages

- Sending data to every device on a network wastes bandwidth.
- Two devices cannot transmit data simultaneously.

Network Topologies: Tree

A **tree** topology is a special type of topology in which many connected devices are arranged like the branches of a tree. In a tree, there can be only one connection between any two connected devices.



Network Topologies: Tree

Advantages

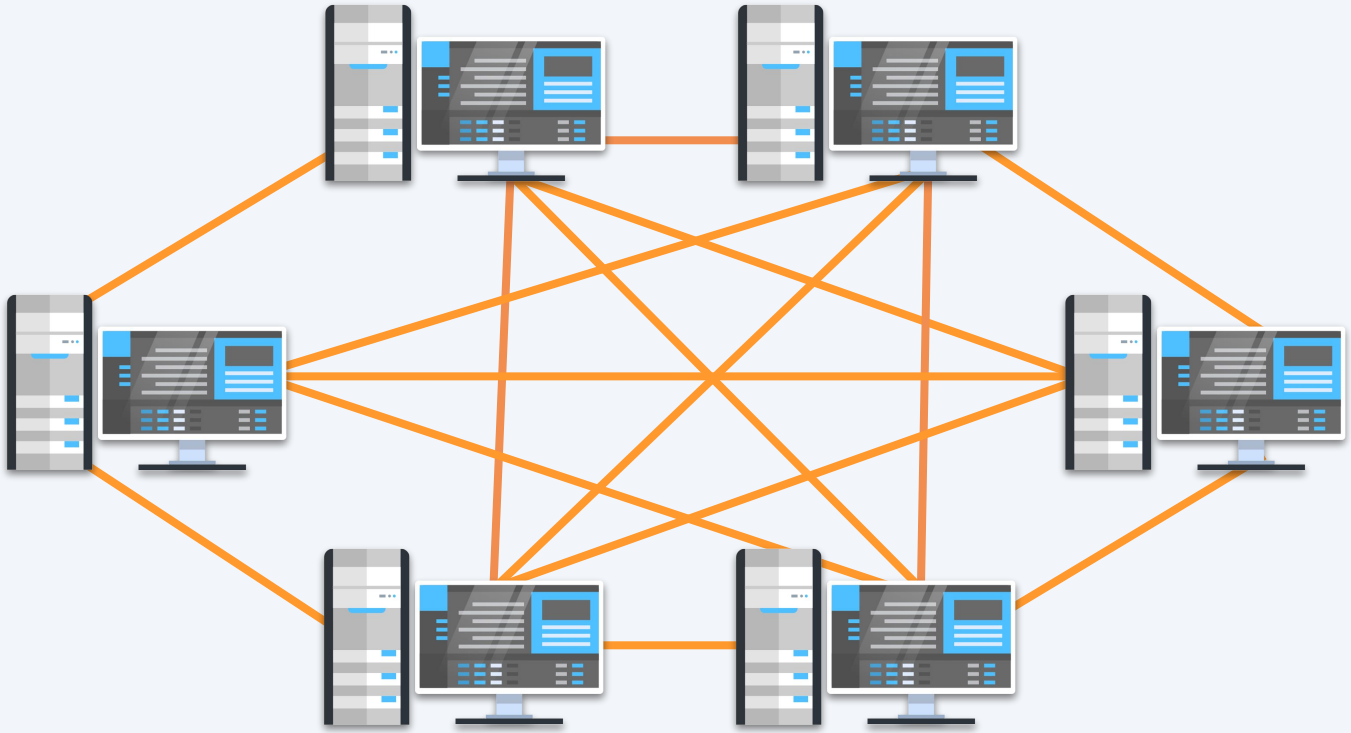
Easy to expand the network.

Disadvantages

If the top node is impacted, all devices below are impacted.

Network Topologies: Fully Connected

In a **fully connected** topology, every device on the network is directly connected to every other.



Network Topologies: Fully Connected

Advantages

- Highly redundant: If a single link between devices fails, both devices can still communicate with the rest of the network.
- Data transmission is point-to-point between directly connected devices. Since all devices are directly connected, transmission is fast.

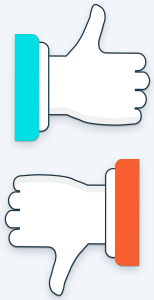
Disadvantages

- Very complicated to set up and manage.
- The number of links in the network scales exponentially with each single device added to the network, making fully connected topologies very expensive to establish.

Network Topologies: Mesh

A mesh topology is similar to a fully connected topology. However, not every device is directly connected.

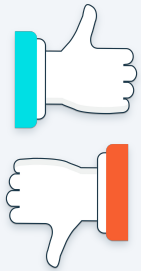
Rather, many of them are connected and devices on the network cooperate to find the shortest path to forward data to one another.



The advantages and disadvantages are the same as a fully connected topology.

Network Topologies: Hybrid

A **hybrid** topology is any combination of the above topologies.



The advantages and disadvantages depend on the types of networks combined.

Topologies and Network Security

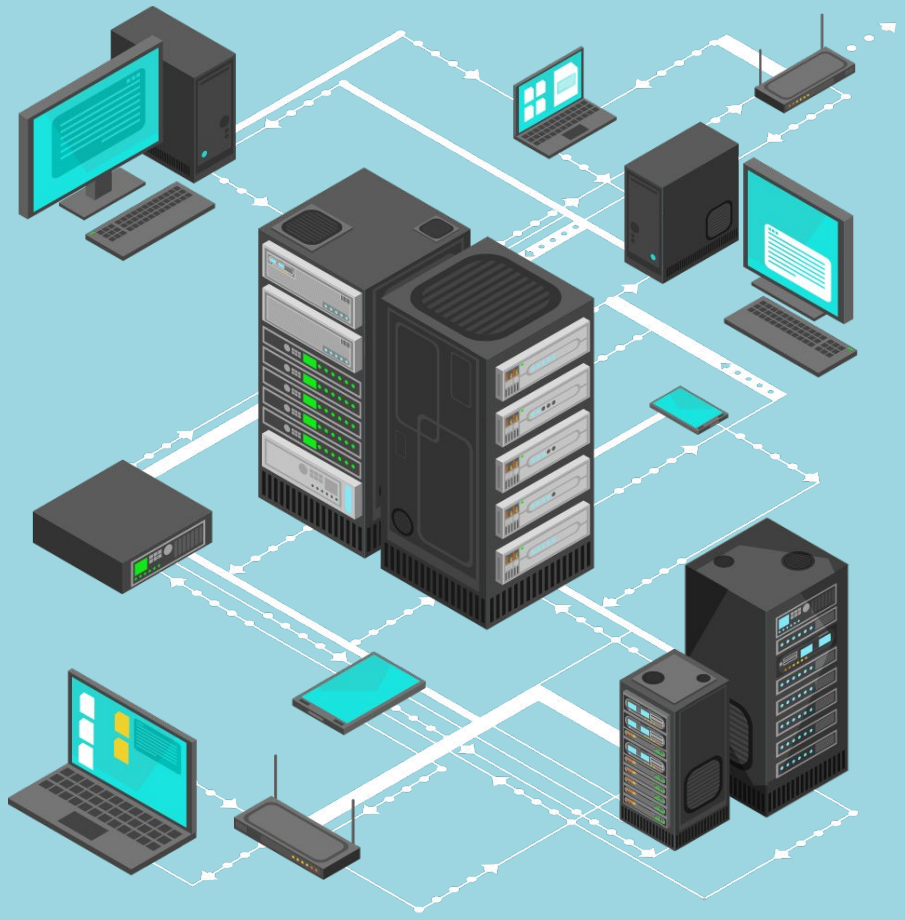
If an attacker takes down a device that is a “point of failure,” that local area network will be impacted.

If an attacker takes control of a device on a topology in which that device is connected to other devices, the attacker may also be able to move from the compromised device to any other device on the network, which would have considerably more impact on the business.

Questions?

Network Devices

The nodes that connect a network are actually many different devices, each with complex responsibilities.



We will now cover the primary network devices found on LANs and WANs.

Network Devices: Router

A **router** is a networking device that forwards (routes) resources to other networks.

A router can connect:

- two different LANs
- two different WANs, or
- a LAN to a WAN

Routers are commonly used to connect your home network (a LAN) to the internet (a WAN).

Network Devices: Switch

A **switch** is a networking device that forwards resources within a network.
In other words, switches connect devices within a LAN.

Switches:

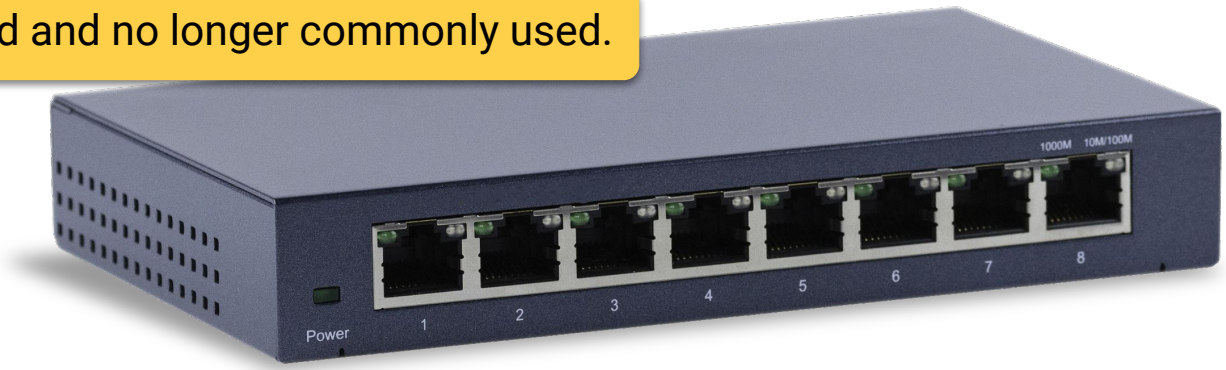
- Are typically used in large businesses that have many computers.
- Typically feed into routers.
- Are intelligent devices, which means they can be programmed to direct resources to certain computers.

Network Devices: Hub

A **hub** serves the exact same purpose as a switch, except it is not an intelligent device. Therefore, hubs cannot be programmed.

- Instead, they direct a copy of the exact same resource to all computers they are connected to.
- Hubs are less secure than switches because they direct resources to all computers, even those that do not need them.

Hubs are outdated and no longer commonly used.



Network Devices: Bridge

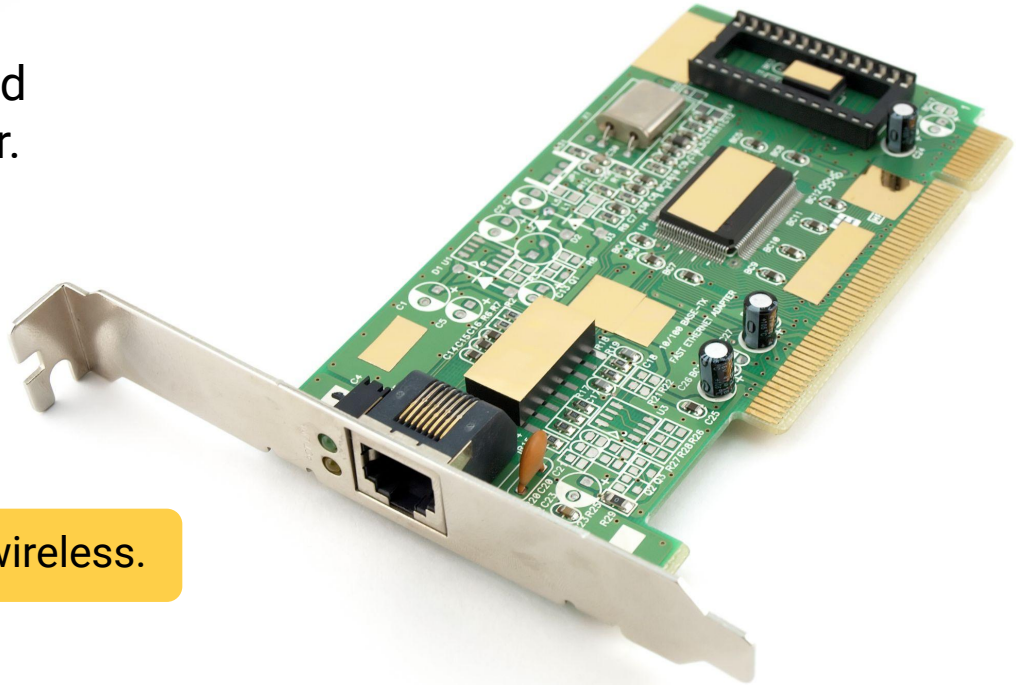
A **bridge** is basically a switch that only has two connections, one in and one out.

Bridges are often used to tie two LANs together.

Network Devices: Network Interface Controller (NIC)

An **NIC** is a type of computer hardware that connects a computer to a computer network.

- An NIC is usually a circuit board or chip installed on a computer.
- Each computer must have an NIC in order to receive or send resources.



NICs can either be wired or wireless.

Network Devices: Modem

A **modem** converts resource data into a format that the next type of connection can understand.

In simple terms:

Your computer and your internet service provider speak different languages.

- Your computer speaks “digital”
- Your internet service provider speaks “analog.”

A modem translates between your computer and the internet service provider so they can understand each other.

Modem is short for *modulator-demodulator*.

Network Devices: Wireless Access Point (WAP)

WAPs give wireless devices the ability to connect to a wired network.

Network Devices: All-in-One Device

All-in-one devices can have modems, WAPs, routers, and more all built into a single device. All-in-one devices are very common household devices.

Advantage

They are easy to use, as less equipment needs to be set up and maintained.

Disadvantages

They are a single point of failure, and it can be difficult to troubleshoot where an issue is in a network transmission.

The previous devices work to transfer data **across networks**.

There are also network security devices used to protect resources **on the network**.

Network Security Devices: Firewall

A **firewall** is an intelligent network security device that monitors incoming and outgoing traffic based on security rules.

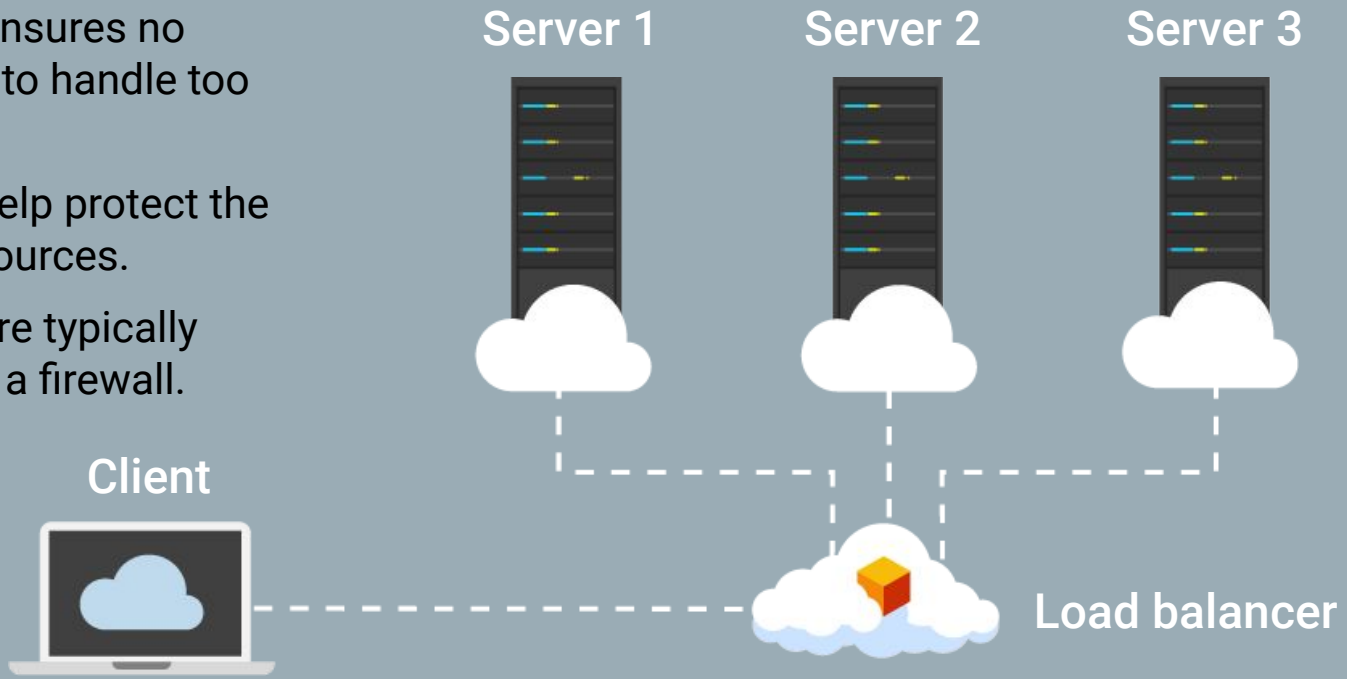
- Firewalls are typically placed right at the entry point of a LAN.
- This placement protects the confidentiality and integrity of resources within that LAN.

There are many types of firewalls and specific firewall functionalities, which will be covered in more detail in future lessons.

Network Security Devices: Load Balancers

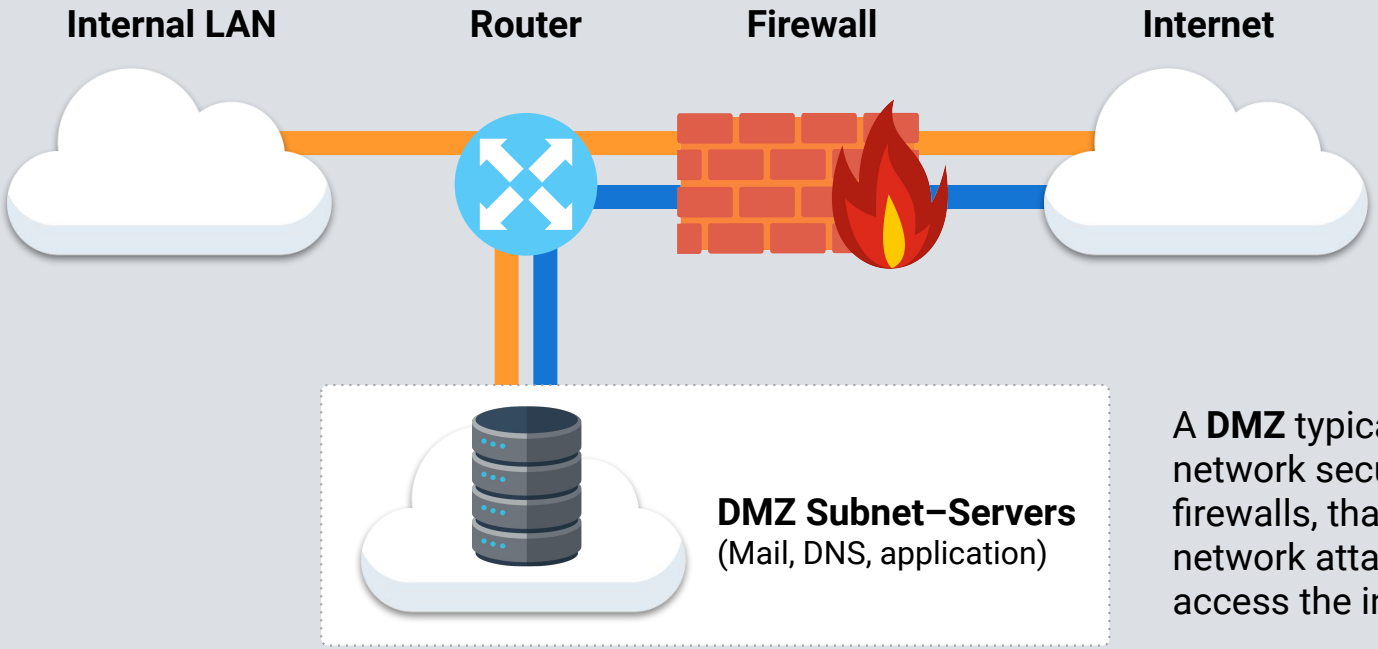
A **load balancer** is an intelligent network security device that distributes that incoming network traffic across multiple servers.

- A load balancer ensures no single server has to handle too much traffic.
- Load balancers help protect the availability of resources.
- Load balancers are typically placed right after a firewall.



Network Security Devices: Demilitarized Zone (DMZ)

A **DMZ** is a smaller subnetwork within a LAN used to add an additional layer of security to an organization's LAN, protecting secure data within the internal networks.



A **DMZ** typically has its own network security devices, such as firewalls, that attempt to detect network attacks before they access the internal networks.

A common task for network and security professionals is to visually design a setup before purchasing, installing, and configuring a network with these devices.

Network Visualization

Designing your network visually can assist with the following:

01

Making networks more efficient, since proximity of certain devices can reduce latency.

02

Avoiding the creation of a “single point of failure.”

03

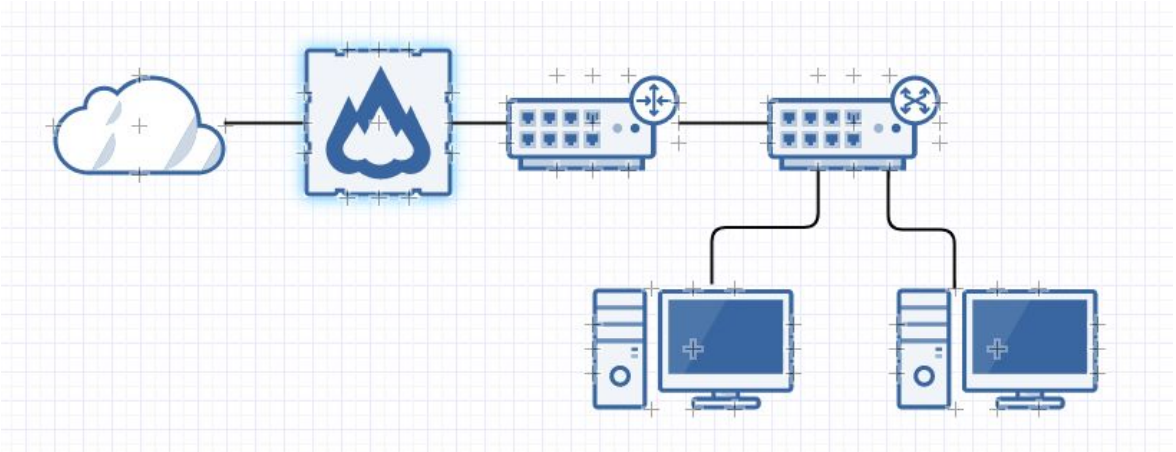
Ensuring private resources are protected from unauthorized sources.

Network Design Demo

We will use the free web tool Gliffy to design a basic network incorporating the following devices:

Draw.io

- 2 Computers
- 1 Switch
- 1 Router
- 1 Firewall
- 1 Representation of the internet



Draw.io

gliffy

Instructor Demonstration

Cliffy Draw.io

Activity: Network Devices

In this activity, you will continue to play the role of a security analyst at Acme Corp. Acme Corp just opened a new office in Shanghai, China and has a list of employee computers and network devices they want to have in the office.

- Your task is to design the network layout for the Shanghai office using Gliffy.
- Additionally, you need to add network security devices to the design to protect against a network attack.

Suggested Time:

25 Minutes

Time's Up! Let's Review.

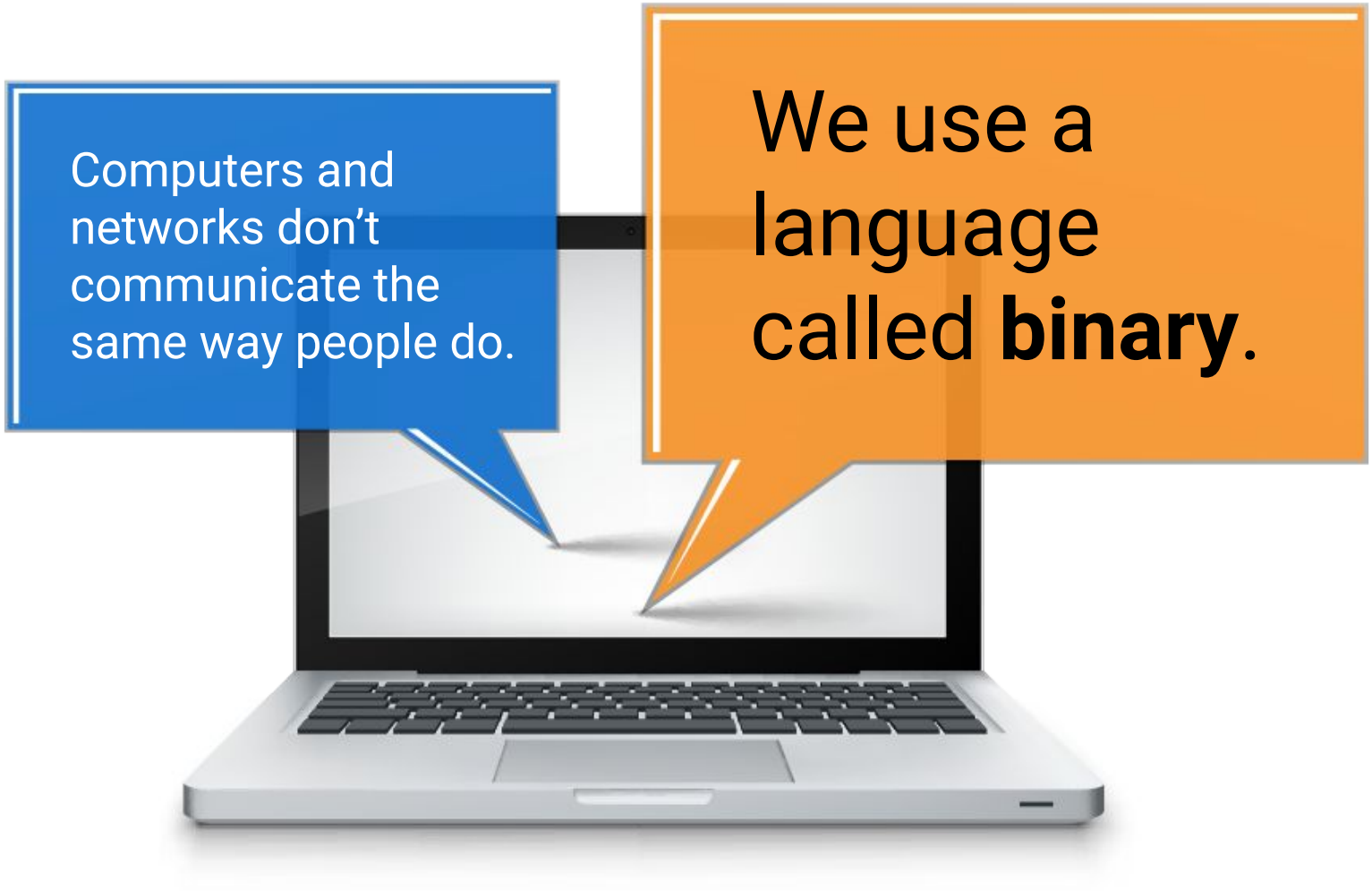
Questions?

Countdown timer

15:00

(with alarm)

What’s my (Network) Address?


Computers and networks don’t communicate the same way people do.
We use a language called **binary**.

Everything we see on our computers, whether it's numbers, words, images, videos, or music, is all a representation of binary data.

Binary Data

At the lowest level, computers communicate with electrical signals, which have two states: **on** and **off**.

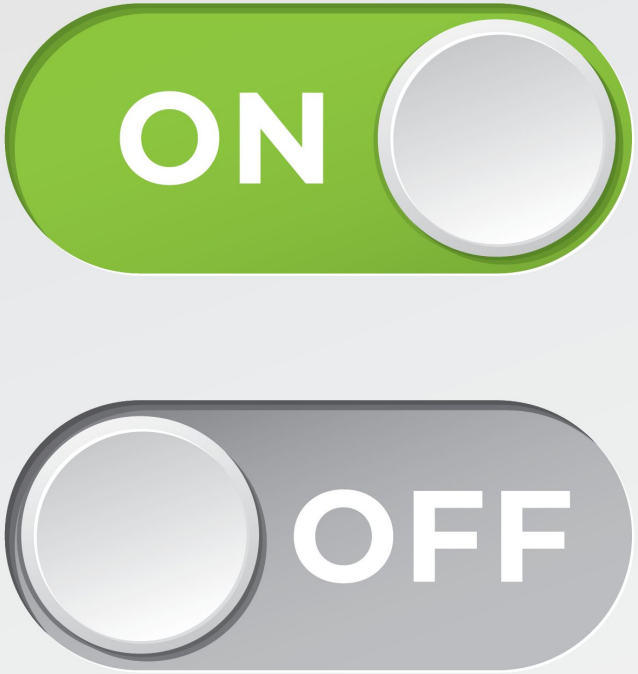
Binary is a **two-digit** numerical system that computers use to communicate:

`1` signifies an **on** signal.

`0` signifies an **off** signal.

Computers transmit these electrical signals from one computer to another, and the electrical signals get converted into binary data.

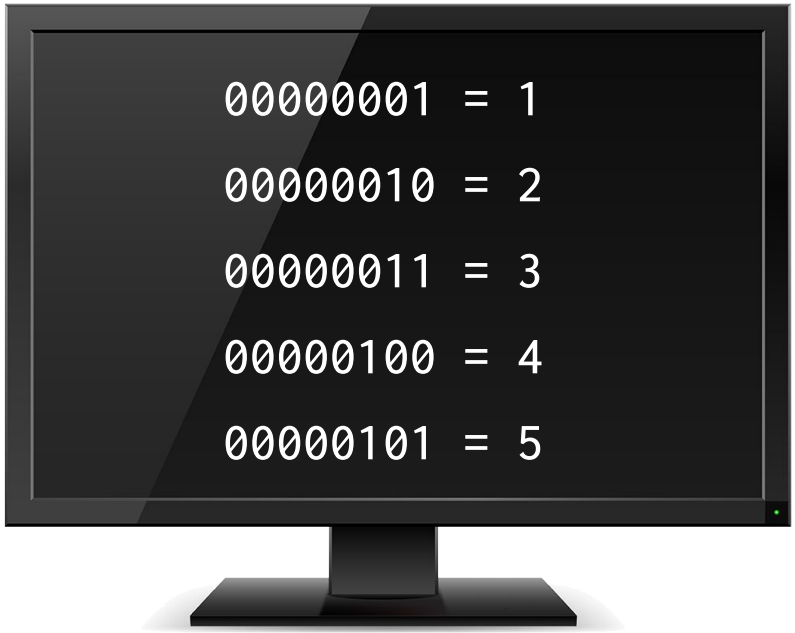
Once the receiving computer receives the binary data, it gets translated into a form that humans can understand.



Binary Data

For example: If one computer wants to transmit 1 2 3 4 5 to another computer, it can't simply transmit these five numbers as we read them, since computers only speak in binary.

The computer would transmit the binary data:



The conversion of this binary data into a numerical representation of

1 2 3 4 5

is one type of conversion called **binary to decimal**.

Receiving Computers Use Other Conversions, Such As:

Binary to ASCII	ASCII is primarily used to convert binary to readable text that humans understand. **Example:** `01101000 01101001` represents `hi`.
Binary to hexadecimal	Hexadecimal, or hex, shortens binary data to letters and numbers. **Example:** `11000111 00000110 10100110 11100110 11110110 01000110` represents `C7 06 A6 E6 F6 46`.
Binary to octal	Octal is another way to shorten binary data with numbers. **Example:** `11000111 00000110` represents `307 6`.

Octal isn't as widely used as the others, but it is important to understand that binary can be converted into multiple formats.

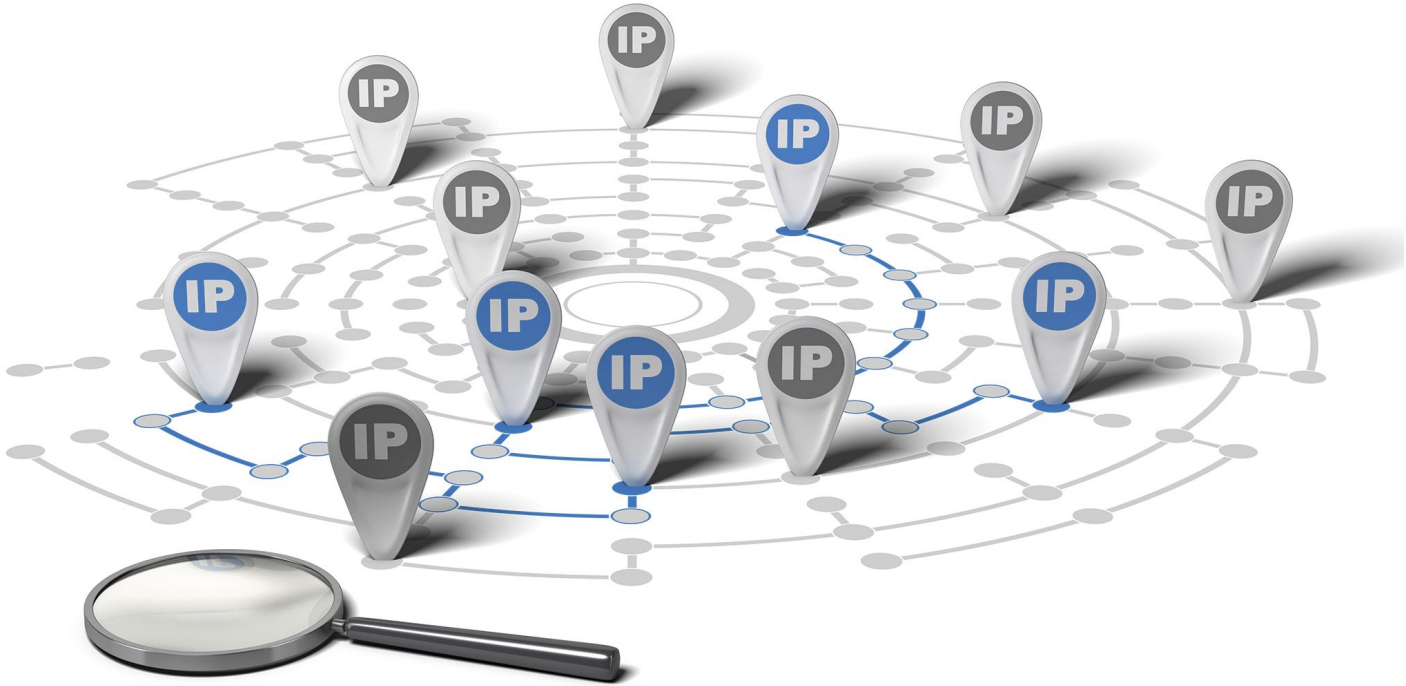
Binary data is used by networks to identify network addresses to determine where to send data.

Binary and Network Addresses

A **network address** is similar to a mailing address. Without a mailing address, we wouldn't know where to send mail. Likewise, we need a specific address to send our data over networks.

An **Internet Protocol (IP) address** is a numerical network address associated with a device such as a computer, printer, router or server.

Each of our computers has an IP address.
Let’s check them at: www.whatsmyip.org.



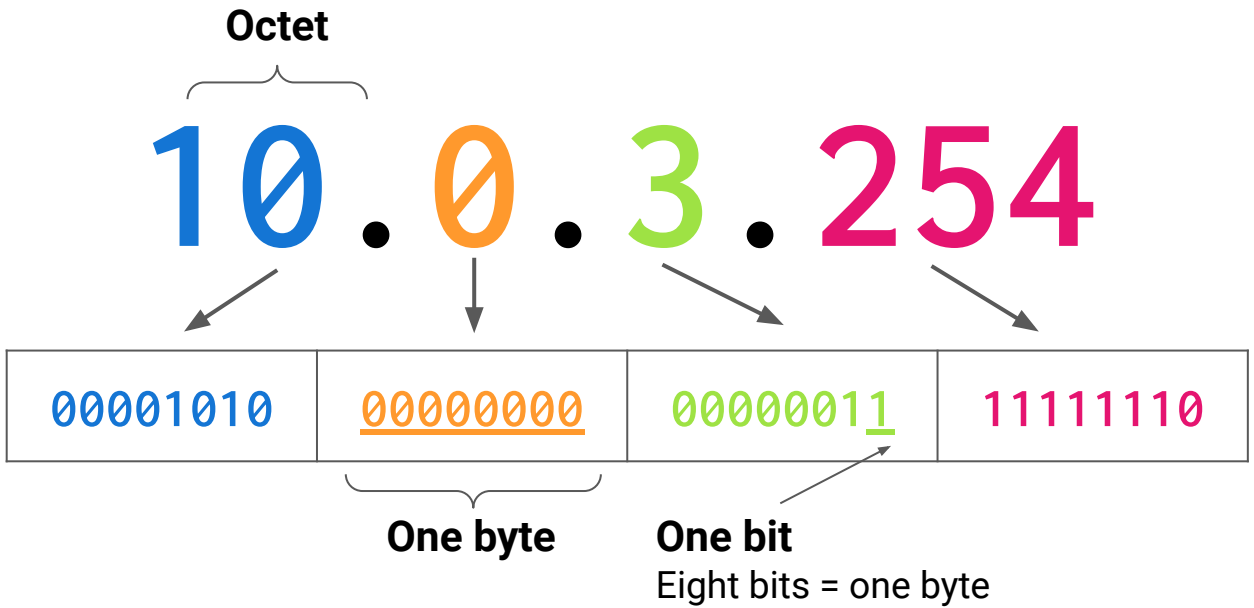
IP Addresses

IP addresses are managed by a global organization known as the **Internet Assigned Numbers Authority (IANA)**.

- The IANA has sub-organizations responsible for the distribution of IP addresses.
- Two primary versions of IP addresses are distributed today.
- The main version is IPv4 (IP version 4).

IPv4

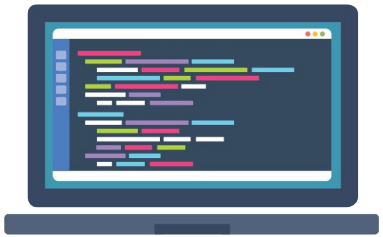
IPv4 IP addresses are made up of four **octets** separated by decimals. These octets are the conversion of eight binary **bits** or one **byte** to standard decimal numbers.



IP Example

10.0.3.254

00001010	00000000	00000011	11111110



What computers read:

`00001010.00000000.00000011.11111110`

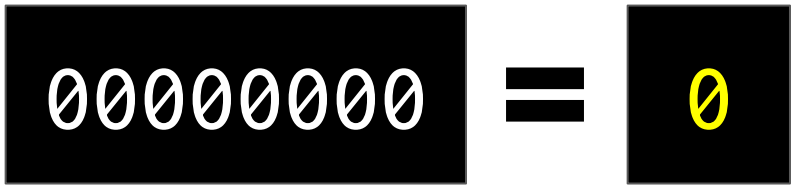
What we read:

`10.0.3.254`

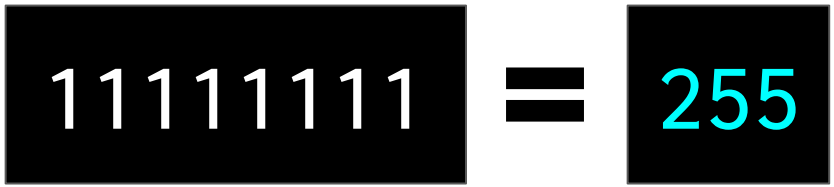
IPv4

Each octet can range from zero to 255. This is because:

Lowest value of eight bits



Highest value of eight bits



Converting IP

Converting IP addresses can be tricky. Fortunately, there is a web tool that can easily convert binary to IP and IP to binary.

IPv6

There is another version of IP addresses called **IPv6** (IP version 6).

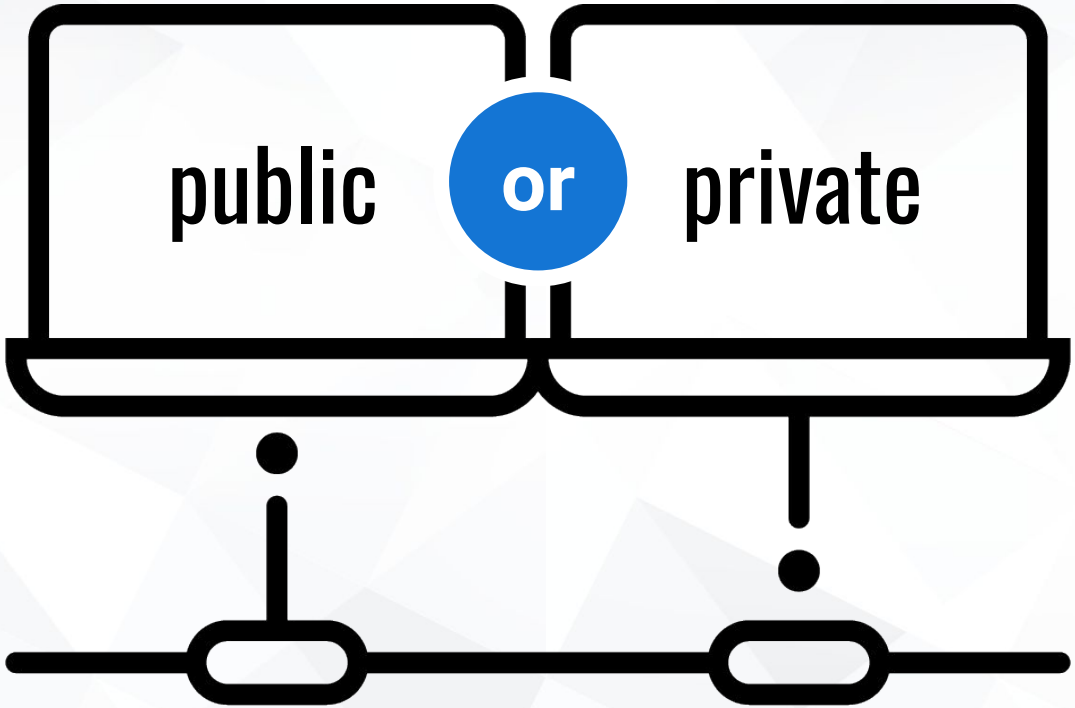
- IPv6 was created due to concern about the lack of possible addresses provided by IPv4.
- IPv6 addresses are divided into eight groups of two bytes. However, these bytes are not binary or decimal. They use letters and numbers in hexadecimal (or, hex) format. We will cover this number format in greater detail later.

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

- IPv6 has not yet been widely adopted. Many devices need to be updated before accepting and sending traffic with IPv6.

For this reason, we won't be discussing IPv6 in more detail.
But it is still important to know that there are two possible IP versions.

IP addresses are categorized as



Public IPs

Public IP addresses are addresses that can be accessed over the internet.

Advantages:
Public IPs' resources are accessible over the internet.

Disadvantages:
Not all devices should be accessed over the internet, as this potentially exposes these devices to malicious actors.

Public IP addresses are typically assigned out in **IP ranges** by an Internet Service Provider.

- **IP ranges** are groups of IP addresses in which the numbers are typically sequential.
- For example, the IP range `108.0.0.1 - 108.0.0.3` would include the IPs:
  - `108.0.0.1`
  - `108.0.0.2`
  - `108.0.0.3`

Private IPs

Private IP addresses are addresses that are not exposed to the internet. Instead, they are typically located within a LAN.

Advantages:

- Private IP addresses aren't publicly accessible, and therefore more secure.
- They can also be reused, as long as they are within different LANs.
- Private IPs can't conflict across different networks.

Disadvantages:

- Private IP addresses are not directly accessible over the public internet.
- They are assigned by a network administrator of the LAN they belong to.

Private IPs

Three IPv4 ranges are saved as private IP addresses and used only for private addressing.

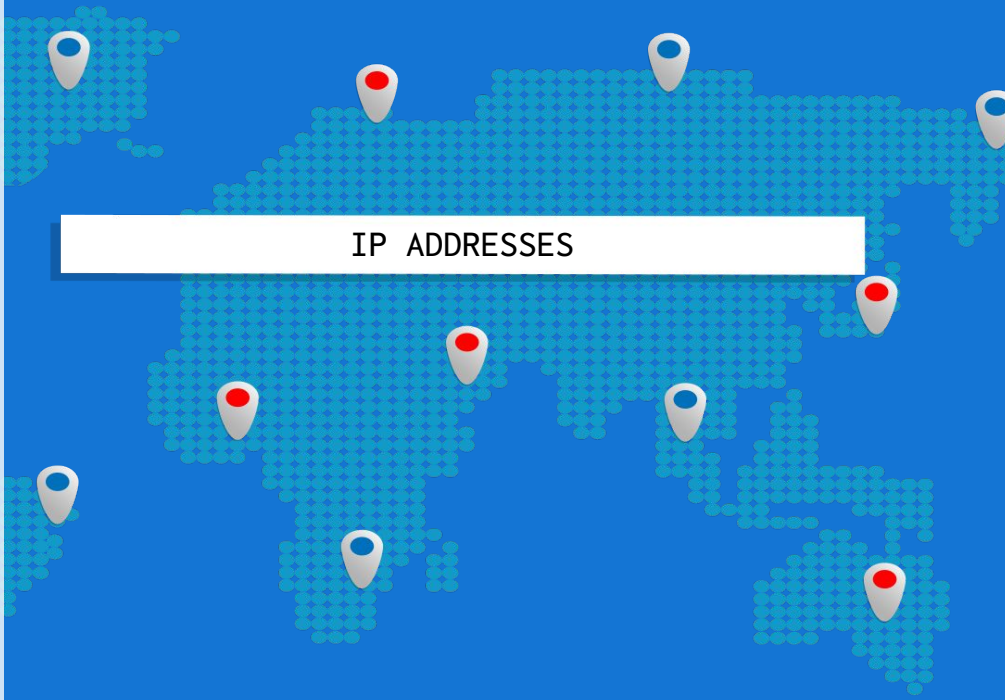
Starting IP	Ending IP	IP Addresses Available
10.0.0.0	10.255.255.255	16,777,216
172.16.0.0	172.31.255.255	1,048,576
192.168.0.0	192.168.255.255	65,536

All addresses not in these three ranges are considered public.

Subnetting

IP addresses are assigned manually by the user or organization that manages their local network.

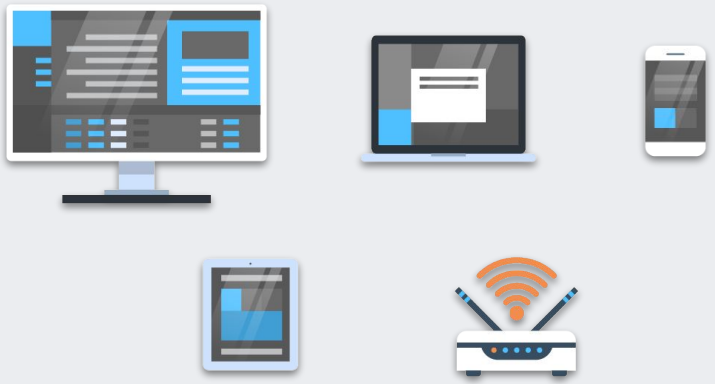
But how do organizations decide what IP addresses are assigned?



Subnetting

Organizations will often group their devices together on a network for organizational and efficiency reasons. For example:

Organizations are typically provided a range of IP addresses that they will distribute across departments and devices.

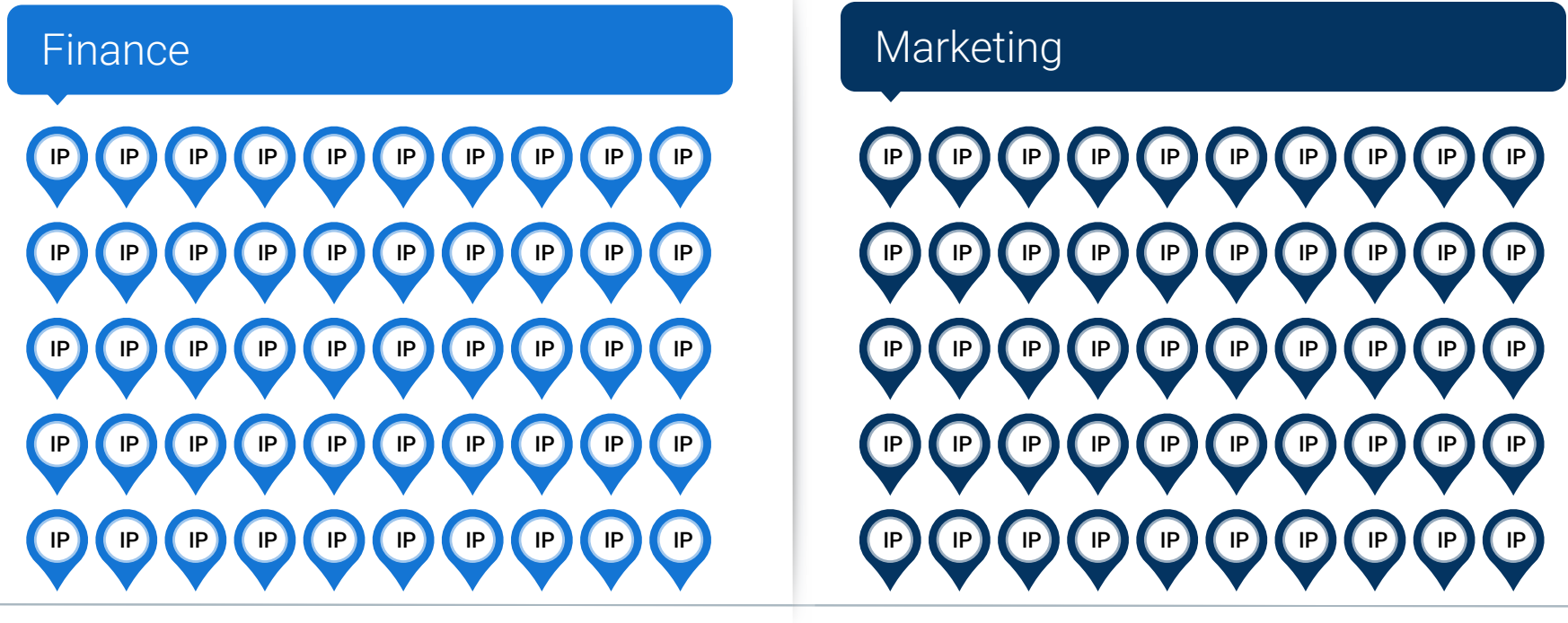


An organization would group together servers designated for Finance, and servers designated for Marketing.

This process of breaking up an IP address range into smaller, more specific networks of grouped devices is called **subnetting**.

Subnetting

For example: If a company has 100 new IP addresses to distribute, they can assign 50 to the Finance department and 50 to the Marketing department by subnetting their provided IP range.

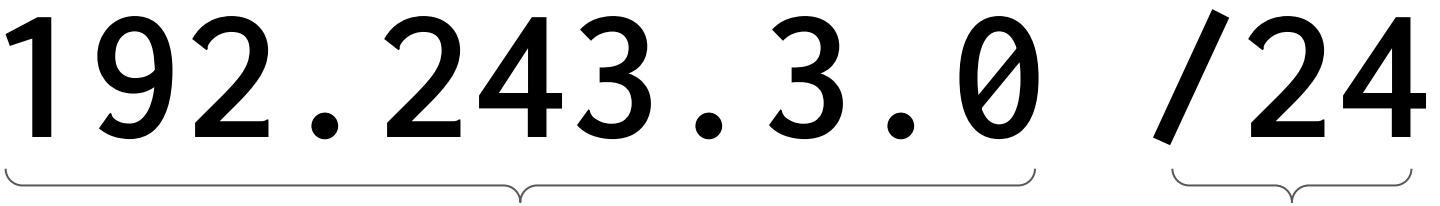


To subnet, we don't have to list and assign IP addresses one by one.

Instead, we use a format known as Classless Inter-Domain Routing (CIDR).

CIDRs

CIDRs are made up of two sets of numbers:
an IP address (the prefix) and a range of available IP addresses (the suffix).



Prefix:
The IP address.
The first 3 octets would be the Network ID.

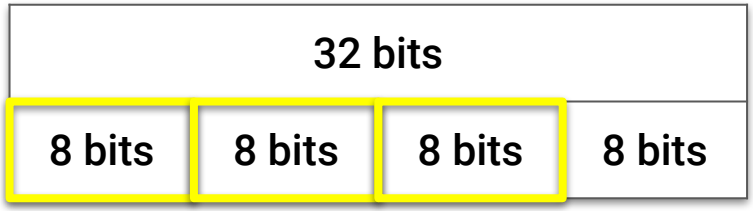
Suffix:
The range of IPs and the number of IPs available.

24 means everything after the first 24 bits is **variable**.

CIDRs

CIDRs are made up of two sets of numbers:
an IP address and a range of available IP addresses.

192.243.3.0 /24

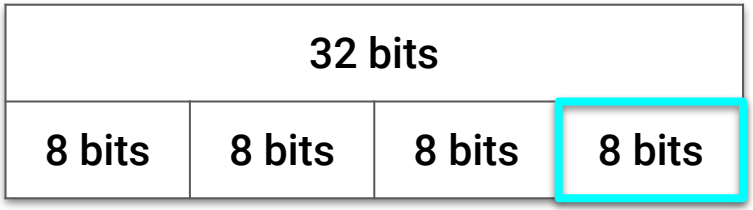


24 means the first 24 bits (three octets) are **static** for a given network.

CIDRs

CIDRs are made up of two sets of numbers:
an IP address and a range of available IP addresses.

192.243.3.0 /24

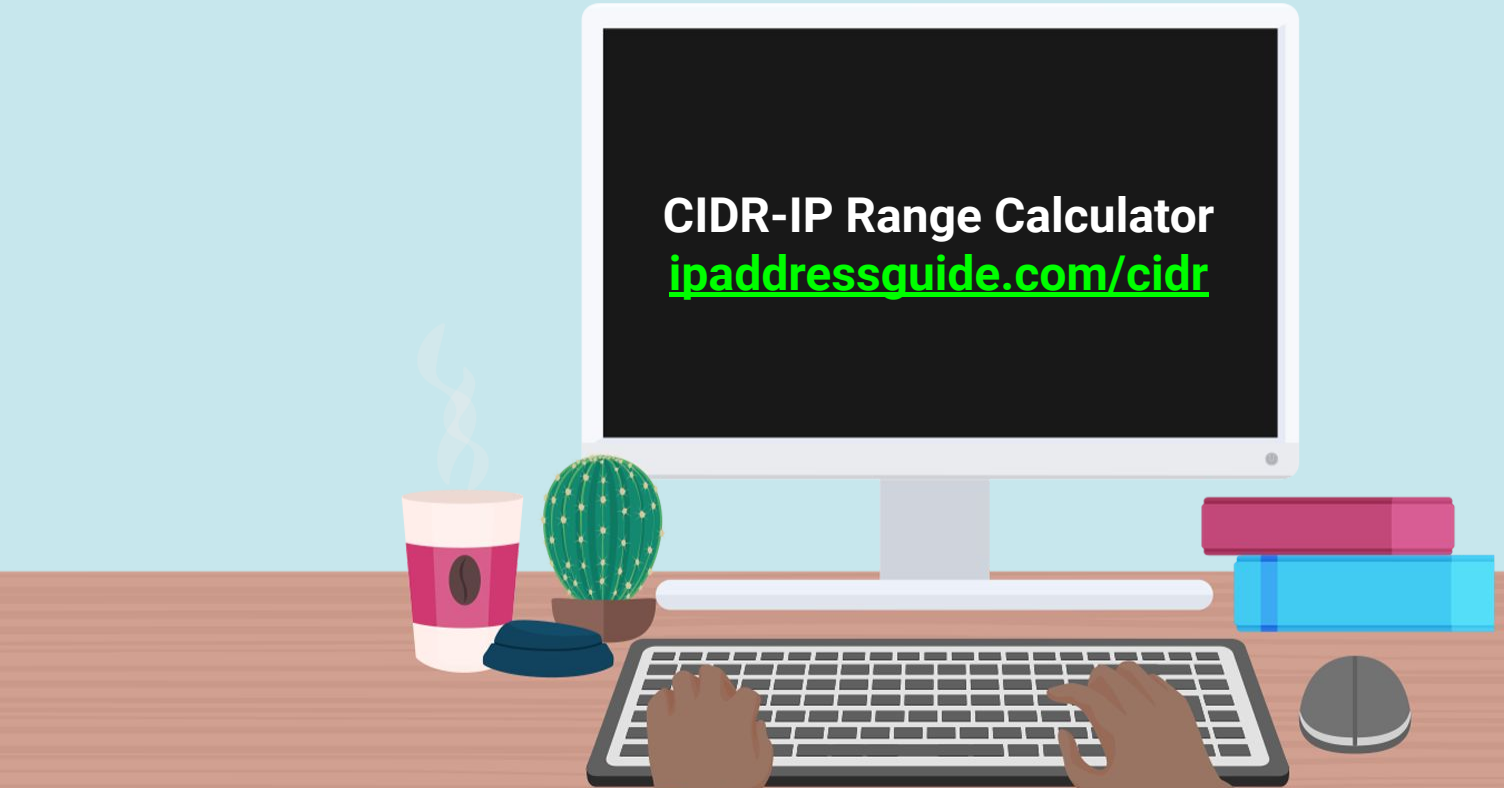


The last 8 bits (.0) is **variable**.

- The range of each octet is 0–255.
- There are 256 available IP addresses in the range 192.243.3.0/24.
- 0 and 255 are reserved. 0 is reserved for the subnet ID and that 255 is reserved for the broadcast.

Range Calculator

We can use online tools to easily calculate an IP address range.



MAC Address

Another important network address utilized *within* a LAN is the **Media Access Control Address (MAC address)**.

- MAC addresses are burned-in addresses assigned to network interface cards (NICs) and must be unique to each NIC located on the same network
- A MAC address is a string of six sets of alphanumeric characters, separated by colons.
- The first 24-bits identify the vendor, manufacturer, or organization associated with the NIC.

Example: 00:0a:95:9d:68:16

Activity: Network Addressing

In this activity, you will continue to play the role of a security analyst at Acme Corp.

Your task is to convert binary traffic into an IP address, determine if it is public or private, and compare the IP to a list of Acme's servers to see which systems the hacker is trying to access.

Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?

Addresses and the Internet

Accessing data from the internet applies similar network addressing concepts.

Domain Name System (DNS)

Domain Name System

Domain Name System allows us to navigate to *facebook.com* instead of having to type *31.13.65.36*.

DNS lookup

Using a process called **DNS lookup**, our browser searches a series of caches to find the IP address associated to the webpage we type.

Lookups and Caches

When a website is entered in a browser, the browser will check DNS caches to see if they already have the DNS translation of the domain's IP address stored.

Layers of Cache

The caches are searched in an ascending order of scope, starting at your browser's DNS cache and ending, if necessary, at the top-level domain DNS cache.

The DNS lookup process searches caches in the following order:

01 Browser's cache.

02 The operating system's cache, stored in the hosts file.

03 Internet Service Provider's (ISP) cache.

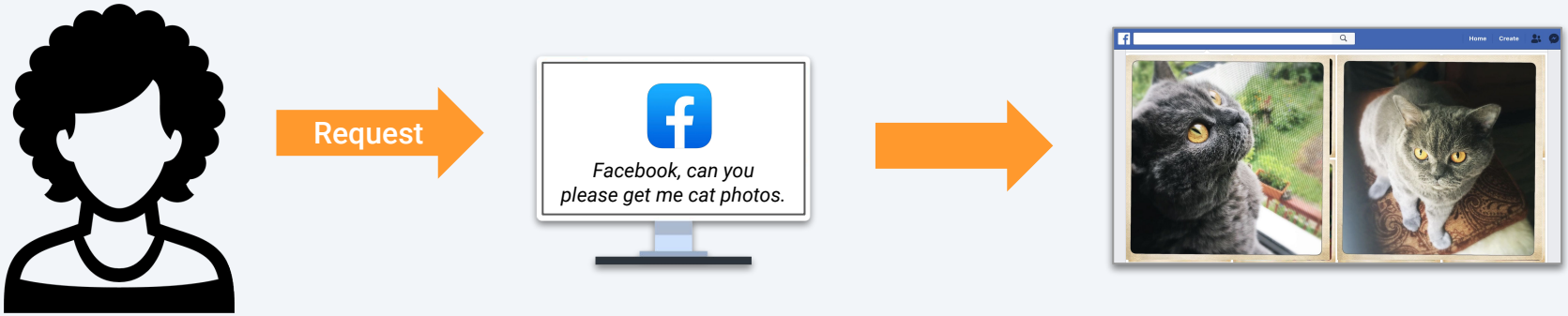
04 Finally, the top-level domain's (TLD) cache.

URLs

A domain is the website we access for resources. The resources we're requesting are typically at a specific location within that domain.

For example:

If we are viewing a picture from Facebook, the picture likely isn't located at the URL *www.facebook.com*. It is likely at a specific location, such as *www.facebook.com/photos/catpicture.jpg*.



URLs

This resource is located in the **URL (Uniform Resource Locator)**.

A URL is the full address of a resource on the internet.

Similar to file structures, URLs have a syntax indicating where to obtain the specific resource being requested.

The syntax is: `[scheme]://[subdomain].[domain].[TLD][/path/][filename]`

URL Syntax

https
(Hypertext Transfer Protocol) is a scheme indicating a file on the internet.

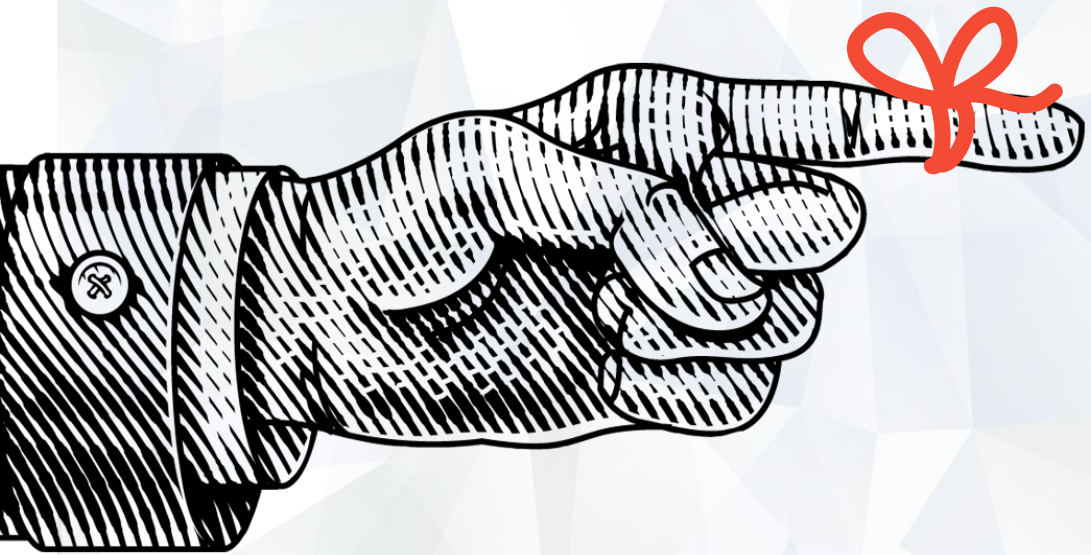
facebook
is the primary domain.

/photos/
is the path where the resource is located.

www
is a subdomain of facebook.com.

.com
is the TLD, or top-level domain.

catpicture.jpg
is the resource or file being requested.



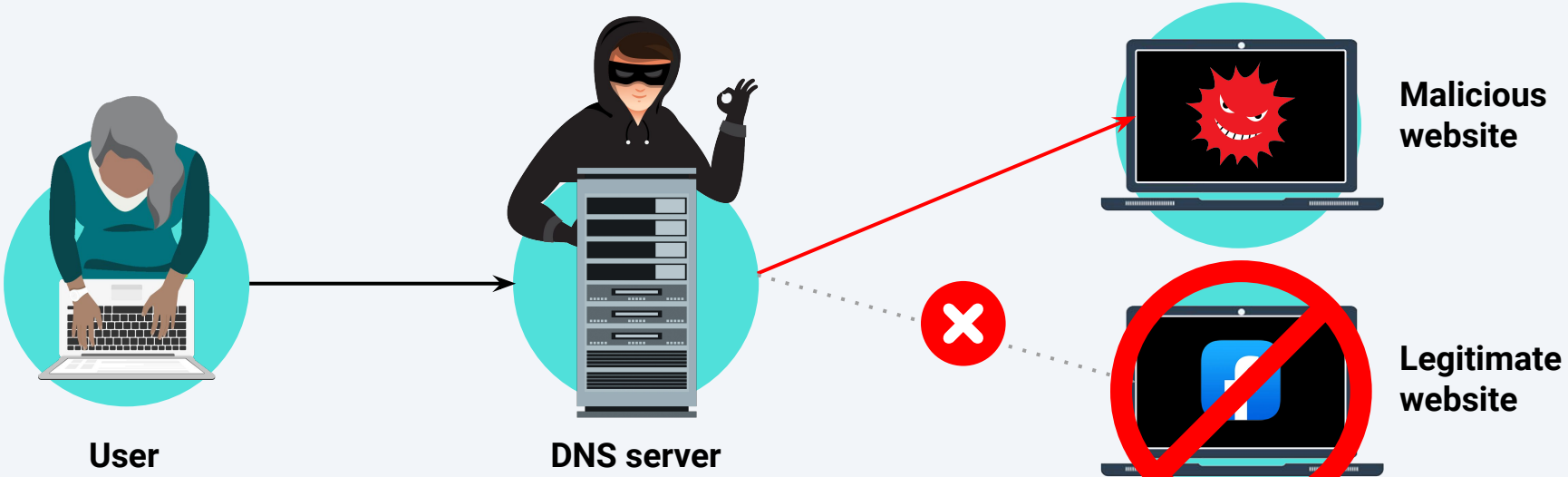
Remember,

- DNS caches indicate where to request the resources from, based on the domain being accessed.
- If a hacker is able to manipulate the DNS cache, they can trick and exploit a user's request by returning a domain or resource that was not originally requested.

DNS hijacking is a type of network attack that exploits DNS vulnerabilities to divert web traffic away from legitimate servers and towards fake or malicious servers.

DNS, URLs, and Security

Example: A hacker owns a malicious site located at the IP `137.74.187.102`.



The hacker accesses your hosts file DNS cache and updates a record that makes browser requests for facebook.com go instead to `137.74.187.102`.

Now, every time you go to facebook.com, you are redirected to the hacker's malicious website.

Instructor Demonstration

DNS Hijacking

Activity: DNS Hijackings

In this activity, you will continue to play the role of a security analyst at Acme Corp.

Your task is to create and test out a DNS spoof record that will redirect any hacker trying to visit acmetradesecrets.com to another website.

Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?


The End