IPs and Routing

Cybersecurity

Networking 2, Day 1


Recap

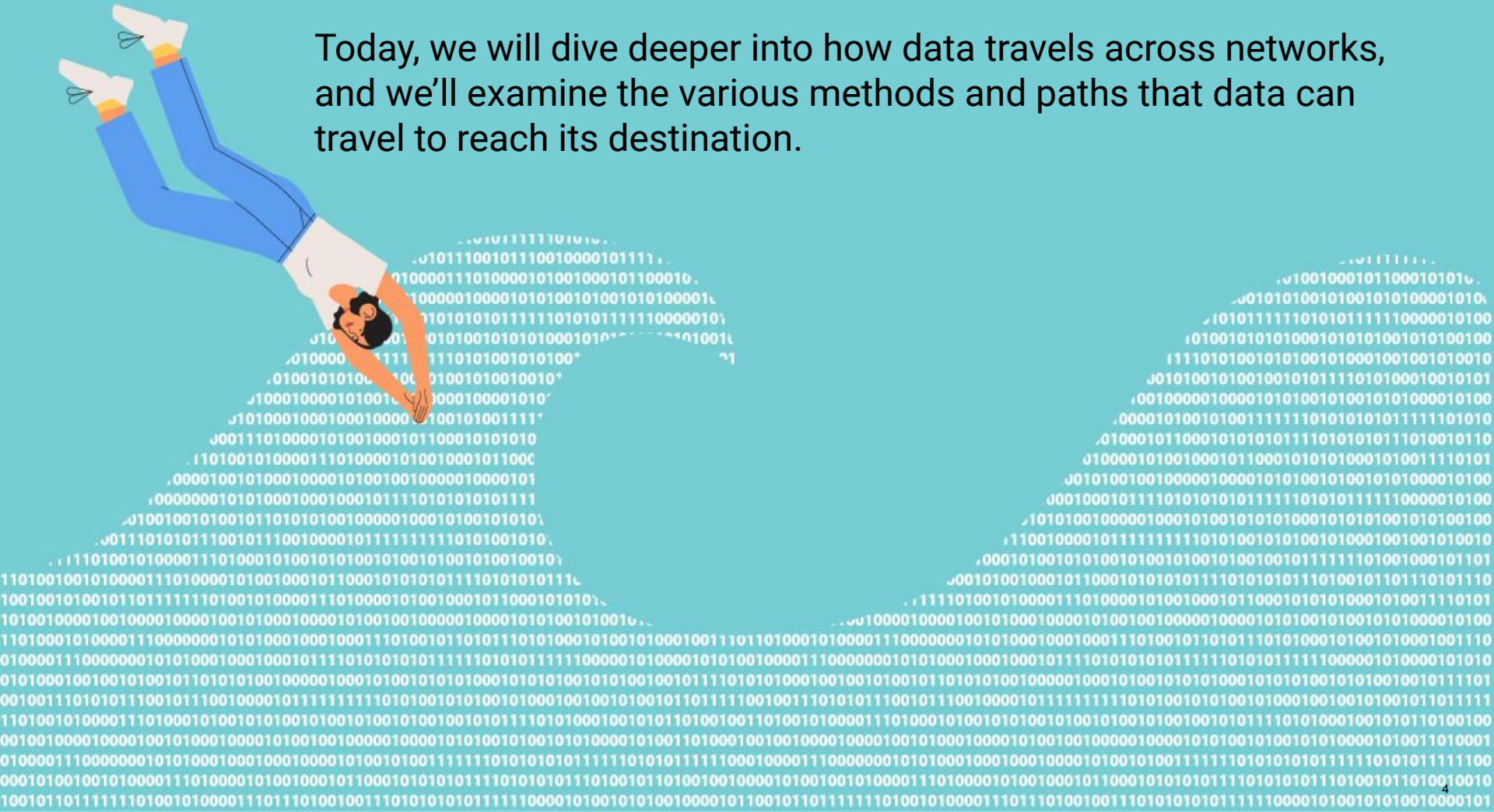
Recap

We've covered many of the devices and technologies that build networks and assist in getting data from source to destination.

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

Resources:
Webpages, email images, data files

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



Today, we will dive deeper into how data travels across networks, and we'll examine the various methods and paths that data can travel to reach its destination.

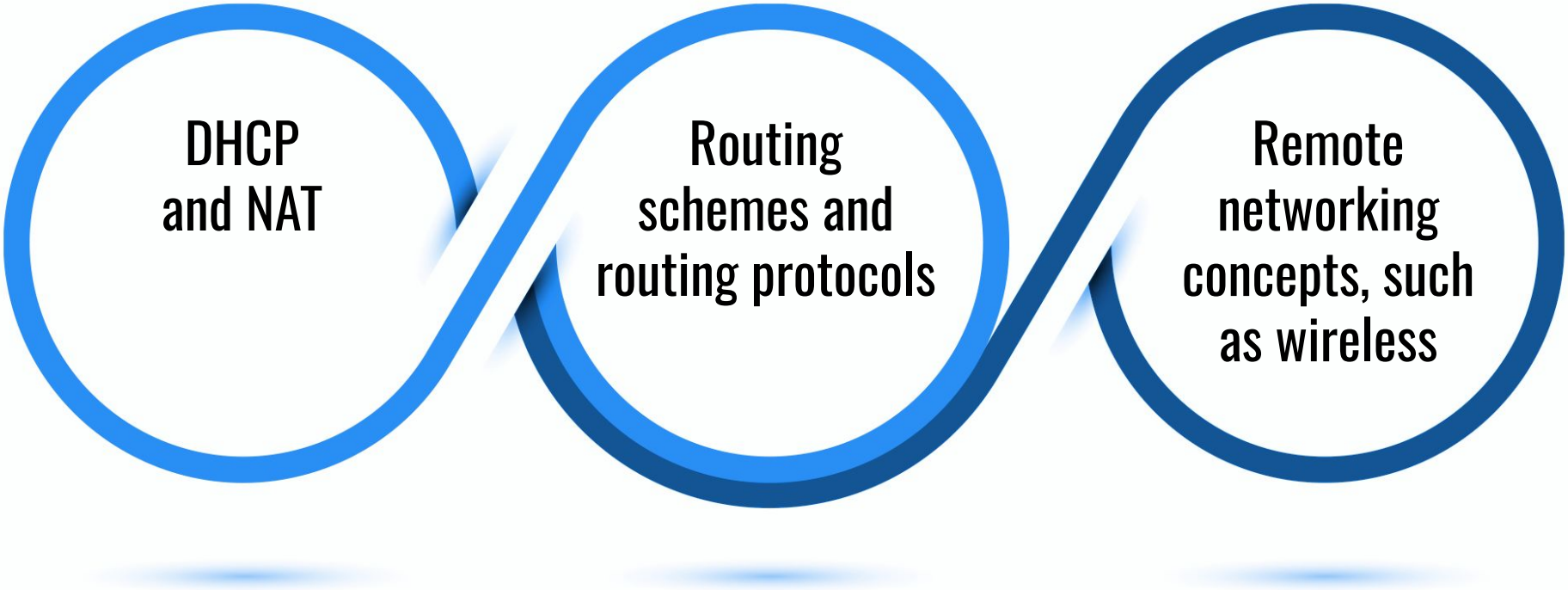
Class Objectives

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

- Explain how DHCP and NAT assist with the transmission of data from private to public networks and from public to private networks.
- Analyze packet captures to diagnose potential DHCP issues on a network.
- Optimize routing schemes by determining the shortest or quickest paths between multiple servers.
- Use Wireshark to visualize wireless beacon signals, capture BSSIDs and SSIDs, and determine the type of wireless security being used by WAPs.
- Use Aircrack-ng to obtain a wireless key and decrypt wireless traffic to determine security risks.

Today's Class

We will cover:



DHCP and NAT

Let’s Review

To understand the first concept of the day, we'll need to quickly review:

Private IP addresses

Are used for devices within a Local Area Network (LAN).

Public IP Addresses

Are used for devices that are publically accessible on a Wide Area Network (WAN).

Dynamic Host Configuration Protocol (DHCP)

When you turn on your laptop and connect to the internet, several processes are taking place.

- If you're on a LAN and want to connect to the internet and visit a webpage, your computer needs to be assigned a private IP address.
- However, most computers do not have pre-assigned private IP addresses, so you'll need to obtain one before you can connect.
- A networking device known as a **DHCP server** is responsible for managing and providing these private IP addresses.

A **Dynamic Host Configuration Protocol (DHCP)** is a client-server based protocol on your local network that is responsible for managing and assigning IP addresses to individual machines.

Dynamic Host Configuration Protocol (DHCP)

DHCP is **dynamic**, because most devices don't have fixed IP addresses.

DHCP client

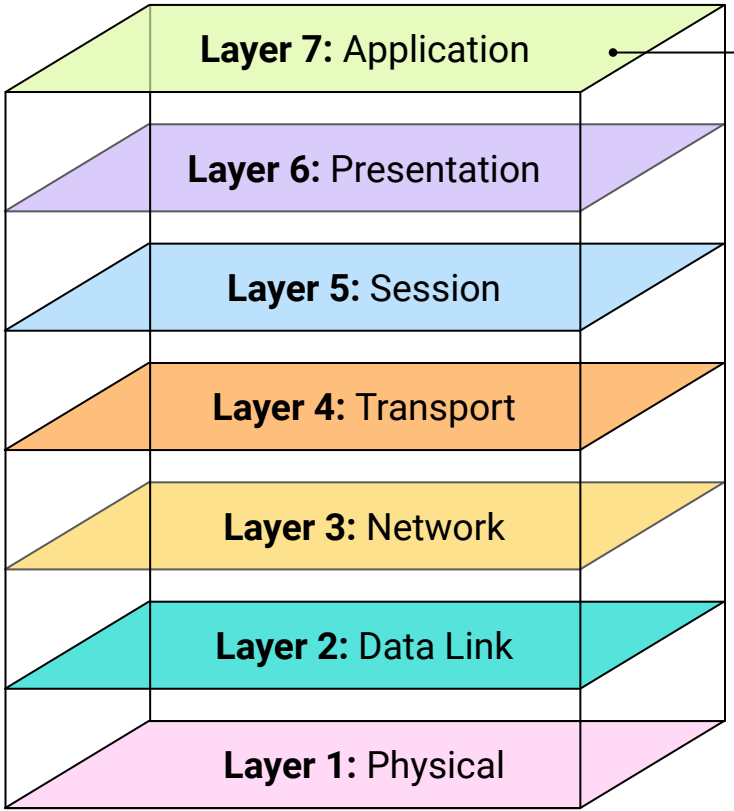
Any device that needs a dynamic IP address, e.g., your computer.

DHCP server

The provider of the IP addresses on your local network.

On a small or home network, the DHCP server is typically located on your router, but at an enterprise level could be on its own server.

Dynamic Host Configuration Protocol (DHCP)

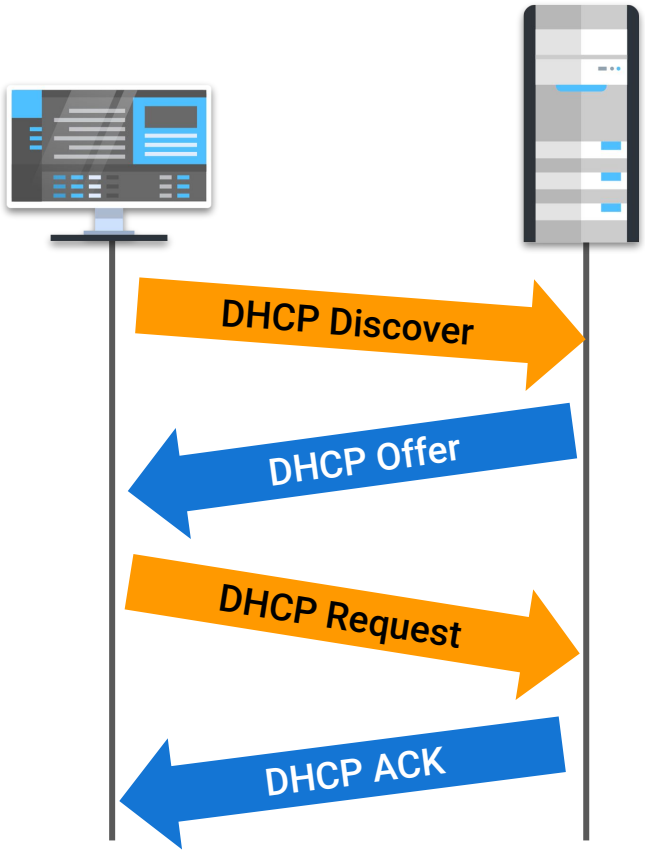


DHCP is a **Layer 7: Application** layer protocol, that uses two UDP ports:

Port 67 is used by the server

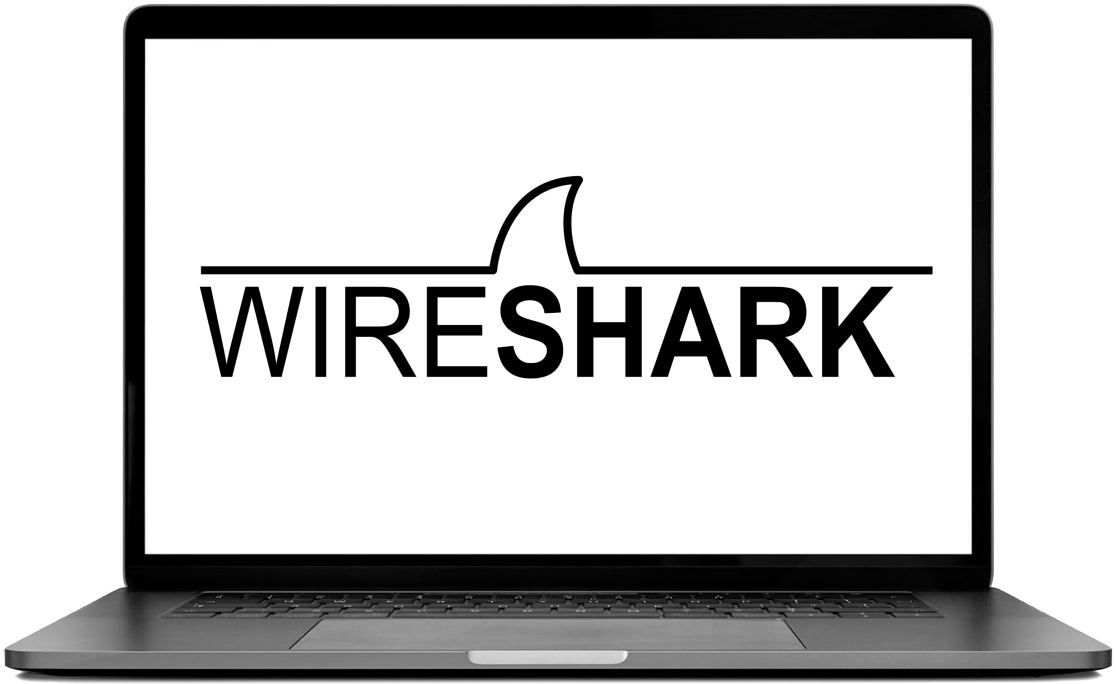
Port 68 is used by the client.

DHCP Request and Receive Four-Step Process



DHCP Discover	Client needs to find the server.	*"I need a DHCP Server!"*
DHCP Offer	The server checks available IPs, selects one, and sends it out to the network.	*"Here is your IP address, DHCP client."*
DHCP Request	Client sends a message message back to the DHCP server.	*"Thanks for the IP address, I'll take it."*
DHCP ACK	Server tells client the IP is valid for a period of time called the **DHCP lease**. Once it expires, the DHCP server can give that IP to another device.	*"Okay, but I'll need it back after a certain period of time."*

Let’s visualize these four steps using PCAP files in Wireshark.



Instructor Demonstration

DHCP

Questions?

Network Address Translation (NAT)

To connect across the internet, you need a public IP address. This allows messages to be sent to your device. Public IP addresses are provided through **Network Address Translation (NAT)**.

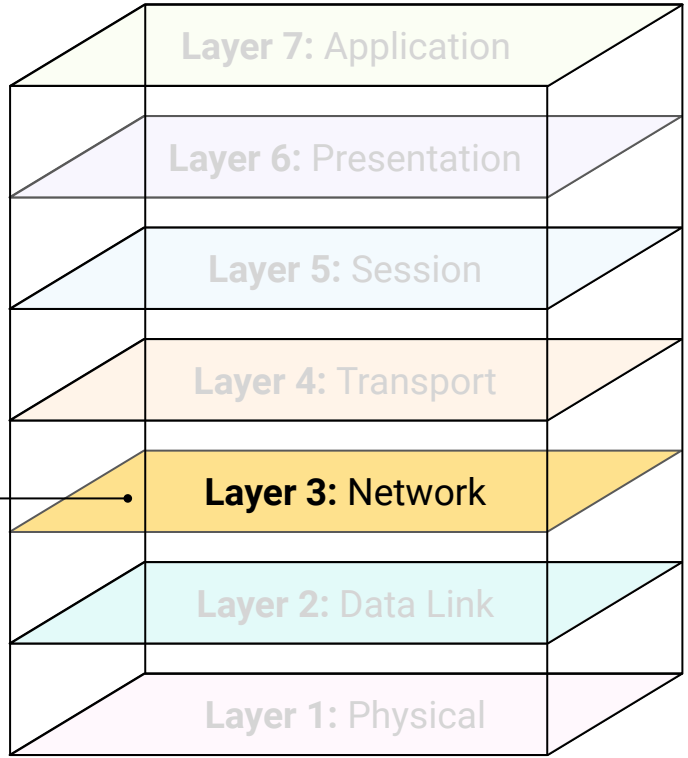
Network Address Translation (NAT) is a method of mapping a private IP address to a public IP address and vice versa.

NAT

A mapping gets stored in a **Network Address Translation** table.

- The router is considered the **gateway** between private and public networks.
- Traffic needing to go from private to public networks and public to private networks (or even private to private networks), needs to go through the gateway.

While NAT touches several OSI layers, it's main task is IP address translation, so it primarily works on **Layer 3: Network**.



NAT: Step-by-Step

We'll move through the steps of NAT using the following scenario:

- Your computer, with the private IP `10.0.0.5`, is trying to access the webpage google.com, which has the public IP `74.0.0.1`.
- Your network's public IP address is `32.0.0.1`.

Step One: Create the Packet

First, your computer creates a packet with the following info (among other data):

Packet	
Destination IP and Port	`74.0.0.1:80`
Source IP and Port	`10.0.0.5:49200`

Step Two: Packet to NAT Table

The packet is sent to the internal router, which creates a record in the NAT table.

Packet from Private IP	
Destination IP and Port	74.0.0.1:80
Source IP and Port	10.0.0.5:49200

NAT Table	
LAN Address	10.0.0.5:49200
WAN Address	32.0.0.1:49200

Step Three: Going Public

The router modifies the packet and replaces the source IP with the **network's public IP address**.

Packet from Private IP	
Destination IP and Port	74.0.0.1:80
Source IP and Port	10.0.0.5:49200

NAT Table	
LAN Address	10.0.0.5:49200
WAN Address	32.0.0.1:49200

Packet Going Public	
Destination IP and Port	74.0.0.1:80
Source IP and Port	32.0.0.1:49200

Step Four: Source Receives and Responds

When google.com receives the packet, it creates a response packet.

Incoming Packet	
Destination IP and Port	74.0.0.1:80
Source IP and Port	**32.0.0.1**:49200

Responding Packet	
Destination IP and Port	32.0.0.1:49200
Source IP and Port	74.0.0.1:80

Google Server: IP 74.0.0.1

Step Five: Back to NAT

When the router receives the packet, it checks the NAT table to see exactly which device is expecting this packet.

It will update the packet and **translate** the IP to include the following new packet details:

Private Packet	
Destination IP and Port	10.0.0.5:49200
Source IP and Port	74.0.0.1:80

NAT Table	
LAN Address	10.0.0.5:49200
WAN Address	32.0.0.1:49200

Responding Packet	
Destination IP and Port	32.0.0.1:49200
Source IP and Port	74.0.0.1:80

Step Six: Return of the Packet

Your device, with private IP `10.0.0.5`, receives the packet. You can now view google.com.

Incoming Packet	
Destination IP and Port	10.0.0.5:49200
Source IP and Port	74.0.0.1:80

NAT Table	
LAN Address	10.0.0.5:49200
WAN Address	32.0.0.1:49200

Responding Packet	
Destination IP and Port	32.0.0.1:49200
Source IP and Port	74.0.0.1:80

Questions?

DHCP Attacks

DHCP Attacks

DHCP servers have a limited number of IP addresses that they can distribute to devices on a LAN.

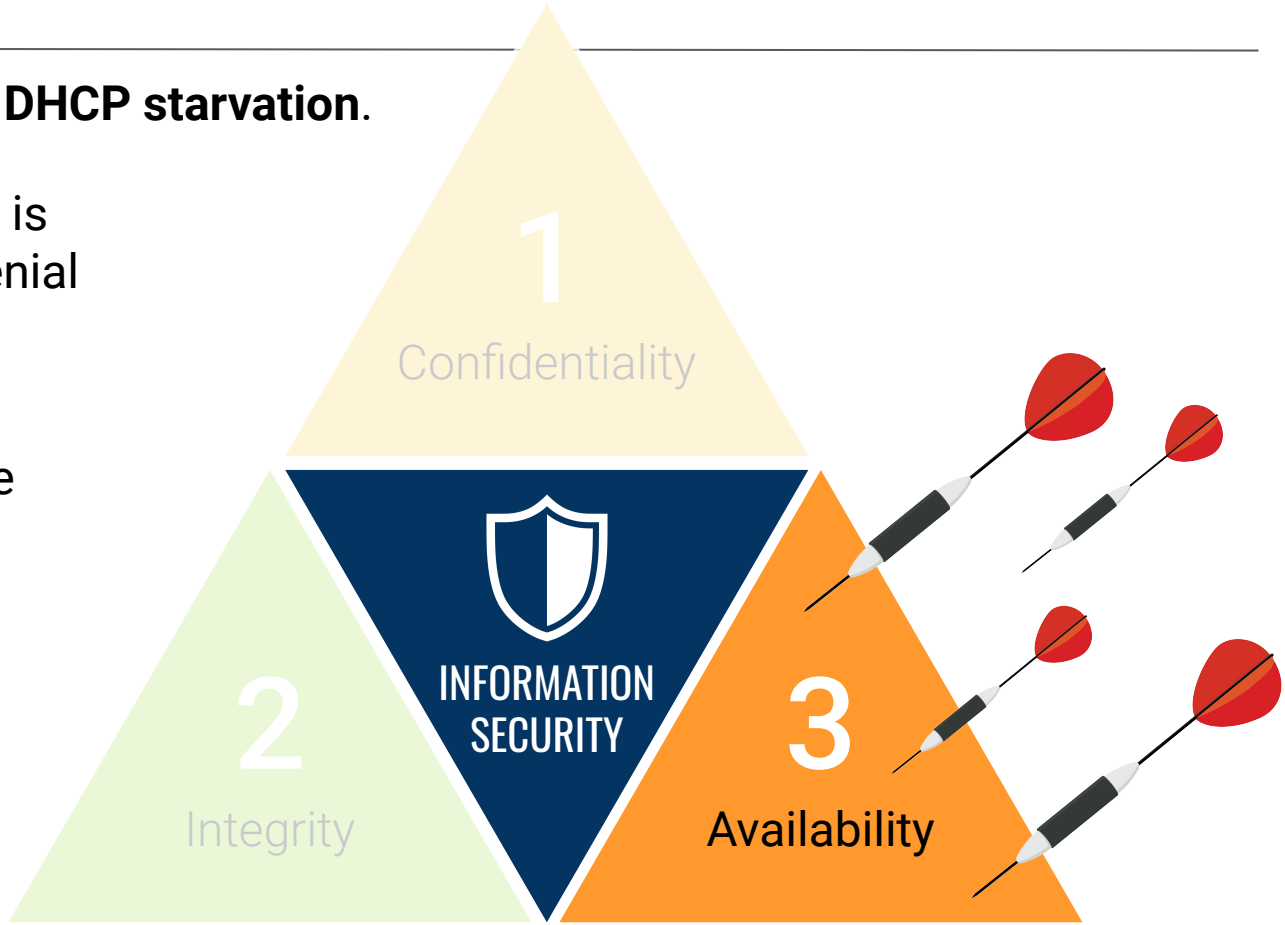
- If an attacker is able to access the LAN, they can send a large number of DHCP messages over the network requesting IP addresses from the DHCP server.
- If they send enough, the DHCP server may run out of IP addresses to distribute.
- If the DHCP server runs out of IPs, new, legitimate users won't be able to receive a private address.

DHCP Attacks

This attack is known as **DHCP starvation**.

If it sounds familiar, this is because it's a type of denial of service (DoS) attack.

This attack impacts the **availability** aspect of the CIA triad.



Instructor Demonstration

Visualizing DHCP Starvation

Visualizing DHCP Starvation

Now, we'll visualize a DHCP starvation attack:

No.	Time	Source Port	Source	Destination	Protocol	SSID	Length	Info
1	0.000000		0.0.0.0	255.255.255.255	DHCP		286	DHCP Discover - Transaction ID 0x7bcbc32c
2	0.000064		0.0.0.0	255.255.255.255	DHCP		286	DHCP Discover - Transaction ID 0x7bcbc32c
3	0.000133		0.0.0.0	255.255.255.255	DHCP		286	DHCP Discover - Transaction ID 0x7bcbc32c
4	0.000198		0.0.0.0	255.255.255.255	DHCP		286	DHCP Discover - Transaction ID 0x7bcbc32c
5	0.000271		0.0.0.0	255.255.255.255	DHCP		286	DHCP Discover - Transaction ID 0x7bcbc32c
6	0.000335		0.0.0.0	255.255.255.255	DHCP		286	DHCP Discover - Transaction ID 0x7bcbc32c
7	0.000403		0.0.0.0	255.255.255.255	DHCP		286	DHCP Discover - Transaction ID 0x7bcbc32c
8	0.000467		0.0.0.0	255.255.255.255	DHCP		286	DHCP Discover - Transaction ID 0x7bcbc32c
9	0.000539		0.0.0.0	255.255.255.255	DHCP		286	DHCP Discover - Transaction ID 0x7bcbc32c
10	0.000604		0.0.0.0	255.255.255.255	DHCP		286	DHCP Discover - Transaction ID 0x7bcbc32c

One way to prevent DHCP starvation is to set a maximum threshold.

This threshold is the number of DHCP requests a server can accept per second.

DHCP Spoofing

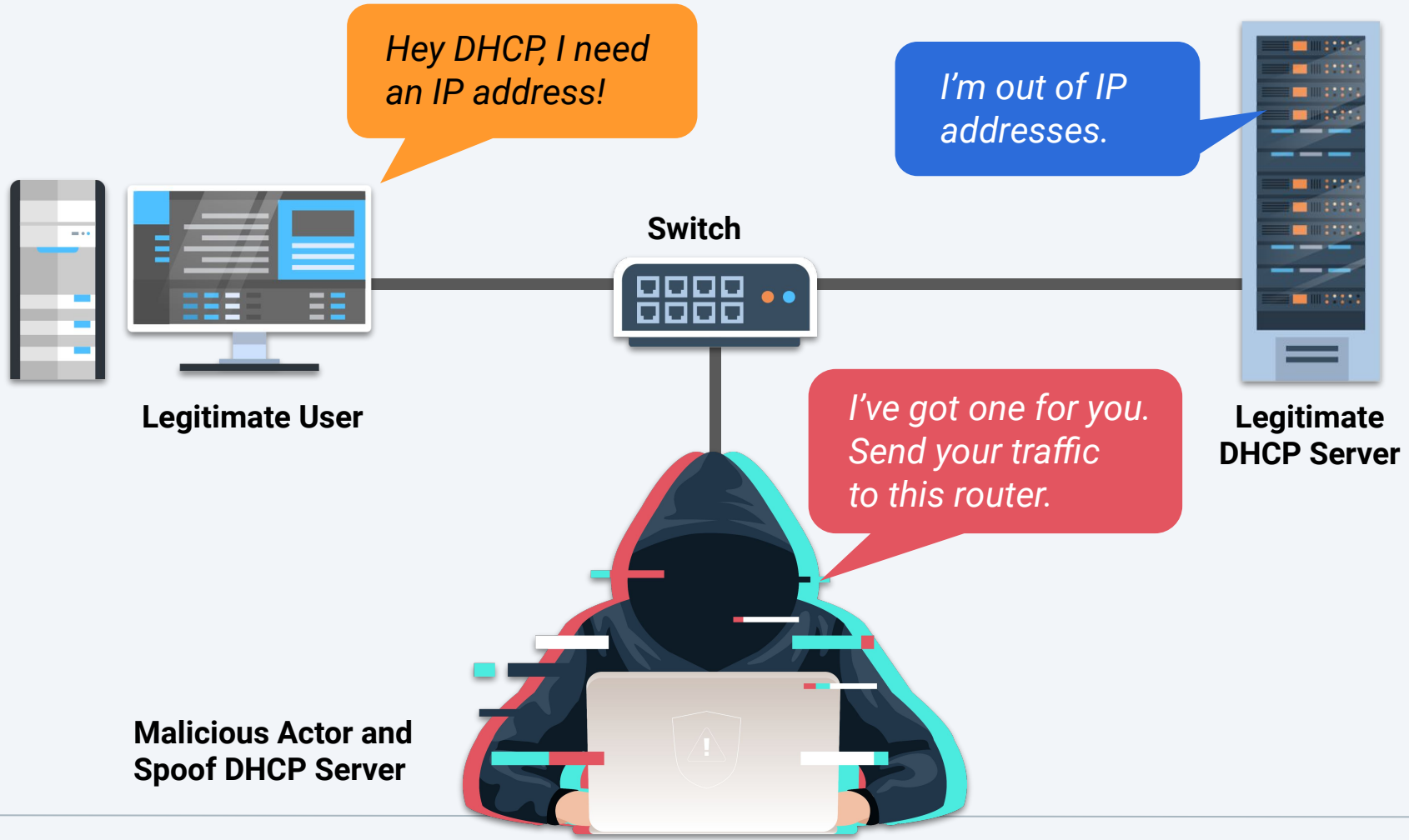
After a DHCP starvation attack occurs, an attacker can potentially set up a fraudulent DHCP server.

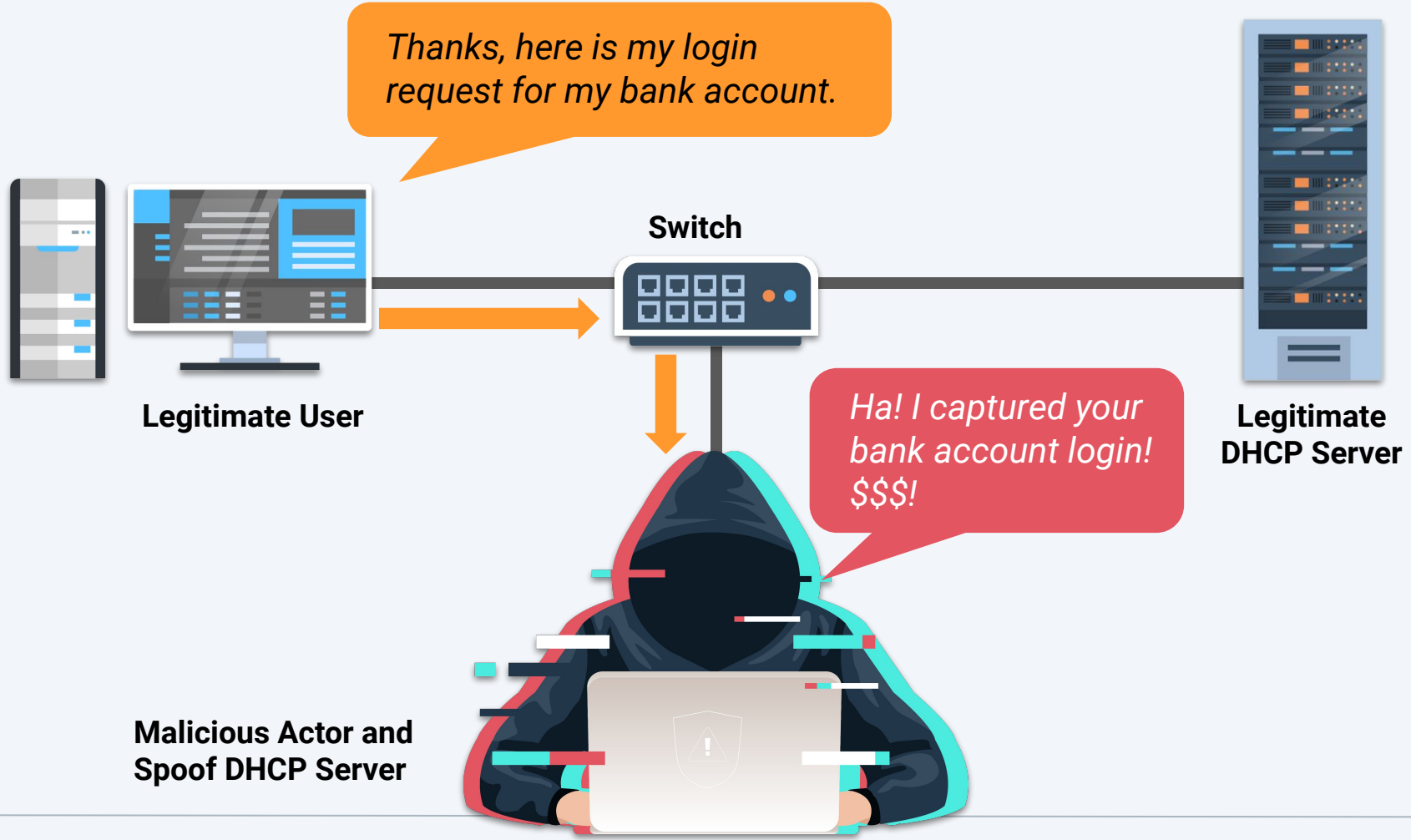
This fraudulent DHCP server can falsely send out spoof messages to the DHCP clients, identifying a malicious router that clients should direct traffic to.

Once the DHCP clients make this change, they will start sending out their traffic to the malicious router.

The attacker can then use the router to capture sensitive data.

This attack is known as DHCP spoofing.


Hey DHCP, I need an IP address!
I'm out of IP addresses.
Switch
Legitimate User
Legitimate DHCP Server
I've got one for you. Send your traffic to this router.
Malicious Actor and Spoof DHCP Server


Thanks, here is my login request for my bank account.
Switch
Legitimate User
Legitimate DHCP Server
Ha! I captured your bank account login! $$$!
Malicious Actor and Spoof DHCP Server

DHCP snooping is a process implemented on a network switch that inspects packets to confirm that they're legitimate DHCP offers, and block those it determines to be unauthorized.

Activity: DHCP Attacks

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

You will analyze a packet capture to determine what type of attack may be causing network issues for Acme employees.

Suggested Time:

15 Minutes

Time’s Up! Let’s Review.

Questions?

Routing Schemes and Protocols

Routes

Data takes a **route** from source to destination.

Routing is the act of choosing the path that traffic takes in or across networks.

Routing Schemes

Network devices have several routing schemes to choose from:

Unicast

A single device delivers a message to another single, specific device.

Broadcast

A single device broadcasts a message to all devices on that same network.

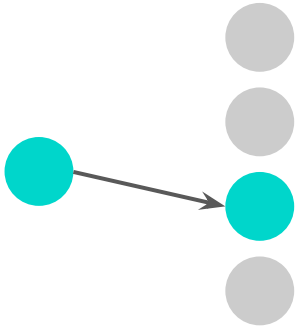
Multicast

A device sends a message to devices that have expressed interest in receiving the message.

Routing Scheme Examples

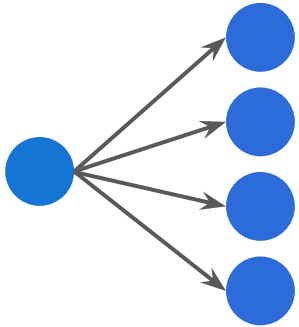
Unicast

A phone call between two people.



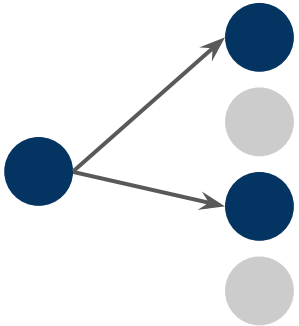
Broadcast

DHCP offer message that is broadcast across an entire LAN.



Multicast

A subscription-based service sends network traffic to its subscribers.



Devices choose their routing scheme based on the protocol used, as well as the intended recipients of the traffic.

Comparing the Schemes

Disadvantages of each:

Unicast

If the message has to reach multiple destinations, many unicast messages must be sent.

Broadcast

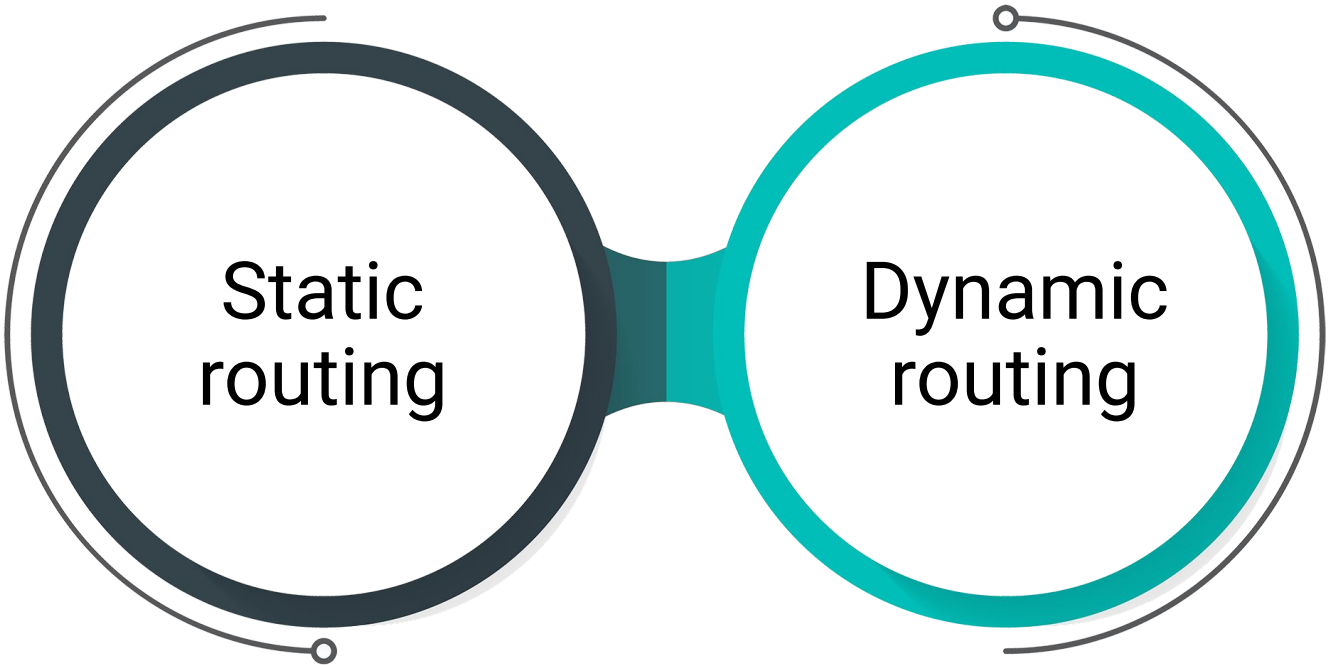
Since broadcast messages are sent to everyone on a network, they can cause unnecessary traffic.

Multicast

Intended recipients will need to be updated and maintained to make sure they're accurate.

Routing Techniques

Networks need to select an optimal route to make sure network traffic is delivered efficiently. Networks use two primary routing techniques to determine the path for transmitting their network traffic:



Static routing is the manual configuration of a network route, typically done by a network administrator.

Static Routing

Usually used on smaller networks.

Advantages

Lower CPU on the router, network administrator has full control of their network's routing behavior.

Disadvantages

Fault tolerance, meaning if a device on a manually created path fails, the route has to be manually deleted and redefined.

Dynamic routing solves the fault tolerance issue by allowing the network to act on its own to avoid network blockages.

Dynamic Routing

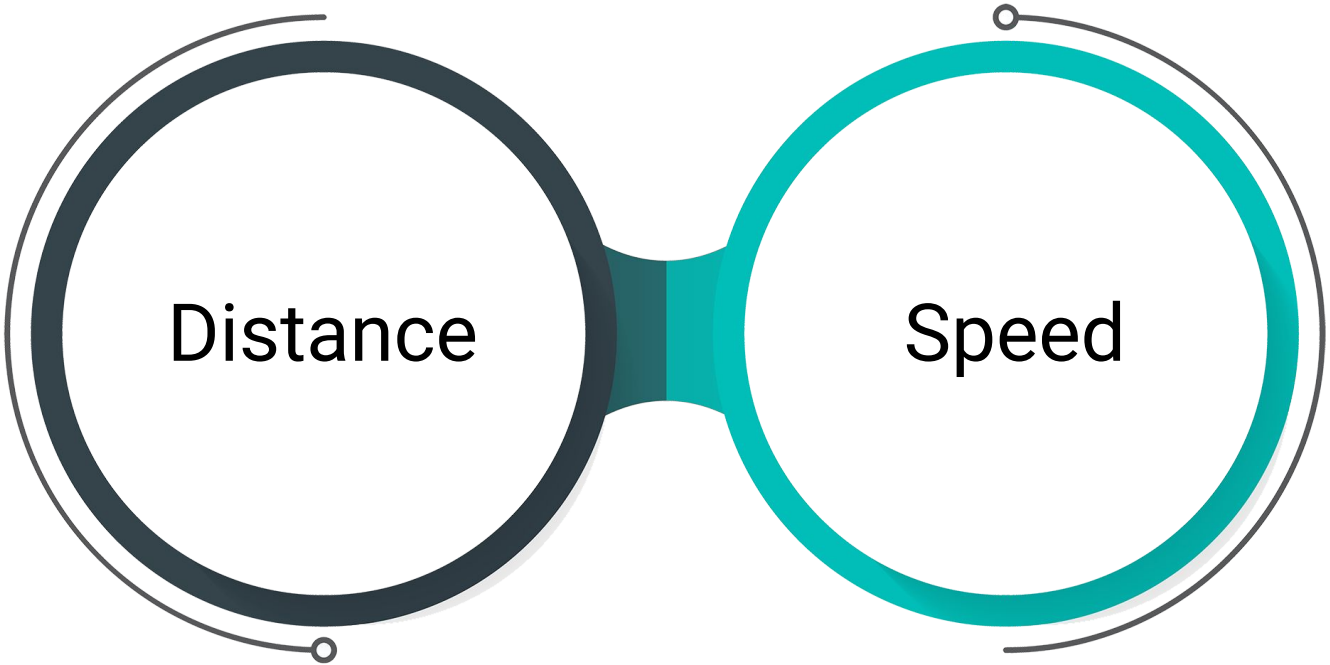
The network is adaptive and data gets forwarded on a different route depending on the network conditions.

The primary routing technique used over the internet.

Uses **routing protocols** to determine the best route to direct the traffic.

Routing Protocols

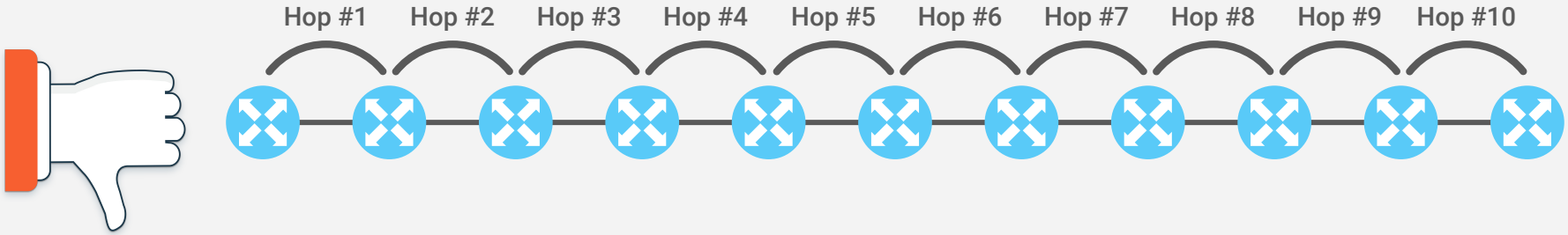
Dynamic routing protocols look at two primary criteria to determine the optimal path:

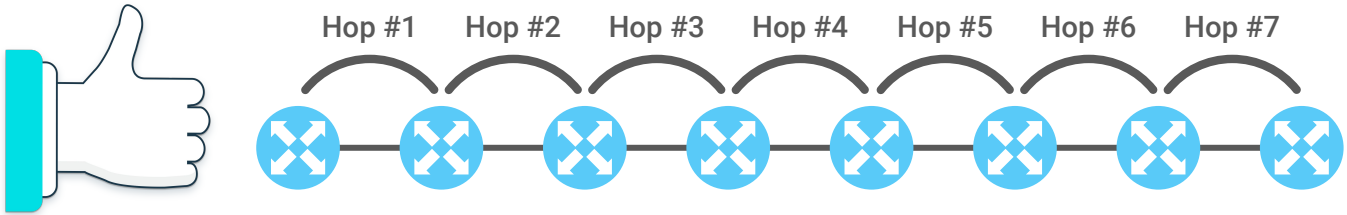


Distance is the amount of devices or hops used to get the data from the source to the destination.

Routing Protocols: Distance

If one route has 10 hops, and another has seven hops, the protocol will choose the route with seven hops.





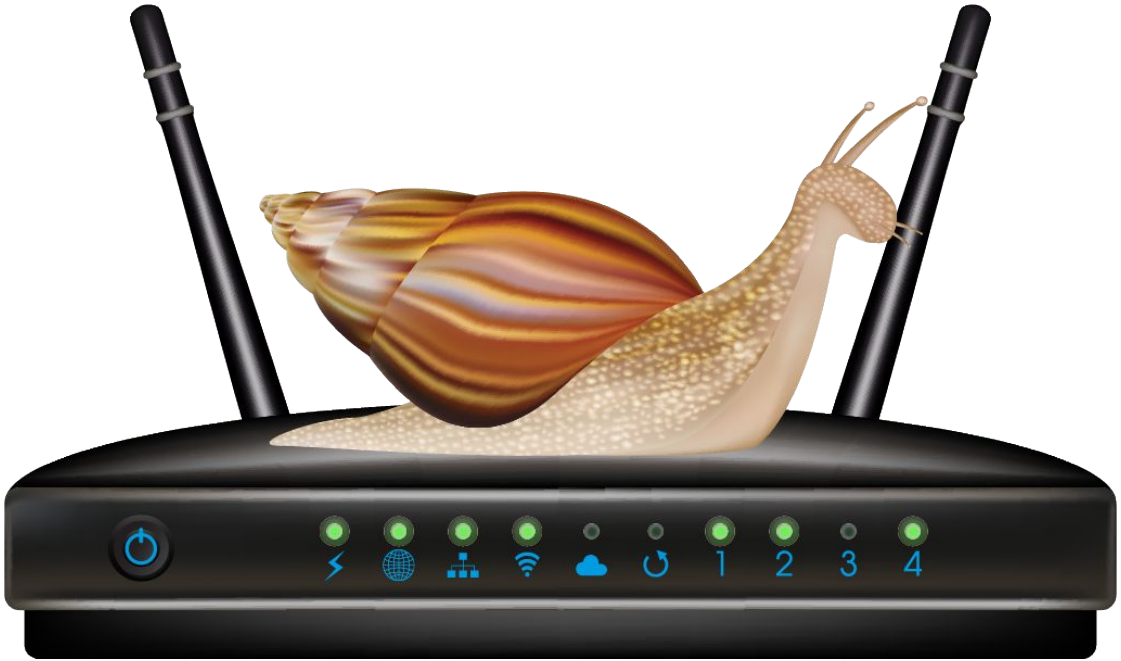
Distance-Vector Routing Protocols

Dynamic routing protocols that use distance as criteria are **distance-vector routing protocols**, which include:

Routing Information Protocol (RIP)	One of the oldest dynamic protocols. It uses the hops count as its main criteria for choosing the route.
Enhanced Interior Gateway Routing Protocol (EIGRP)	A more efficient distance-vector routing protocol than RIP.

Speed: The route is determined by the time it takes to move from source to destination.

Just because a route has more hops, doesn't mean it's always slower. For example, the path with more hops might be faster if there's network congestion on the path with fewer hops.



Dynamic routing protocols that use speed as criteria are called link-state routing protocols.

Routing Protocols: OSPF

One link-state routing protocol is **Open Shortest Path First (OSPF)**.
In this example, Device A needs to send data to Device C.

If both are using a **distance-vector routing protocol**, such as RIP, the path would be:

A > C = one hop, the minimum number of hops.

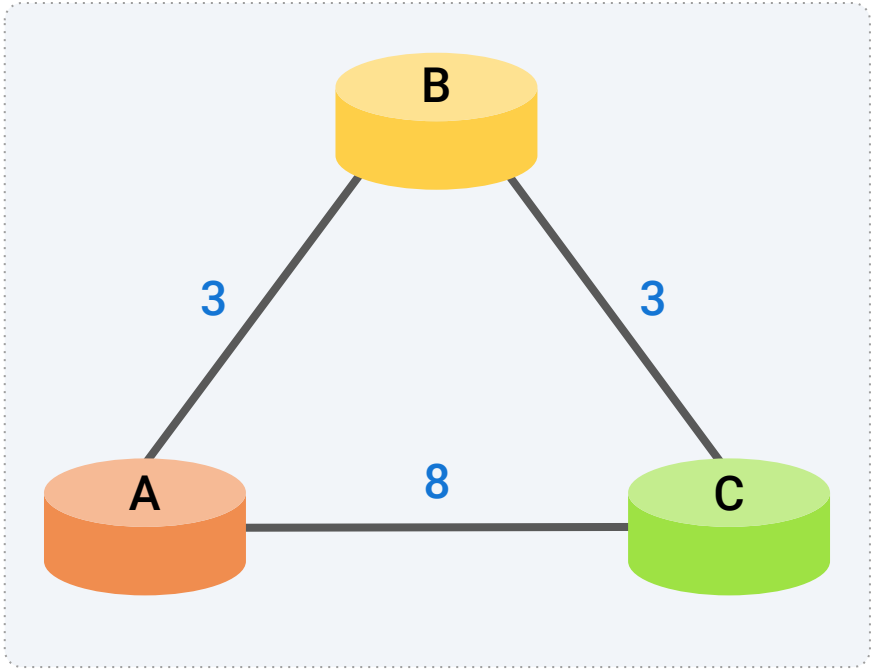
If using a link-state routing protocol such as **OSPF**, speed would be the key factor.

The numbers between the devices indicate the time to get from one device to the next.

A > B > C = 6

A > C = 8

OSPF would choose the path of **A > B > C**.



Questions?

Activity: Routing Schemes and Protocols

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

Your task is to analyze a network diagram and identify the shortest “Time-Wise” path between the servers provided.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?

Countdown timer

15:00

(with alarm)

Wireless Networking

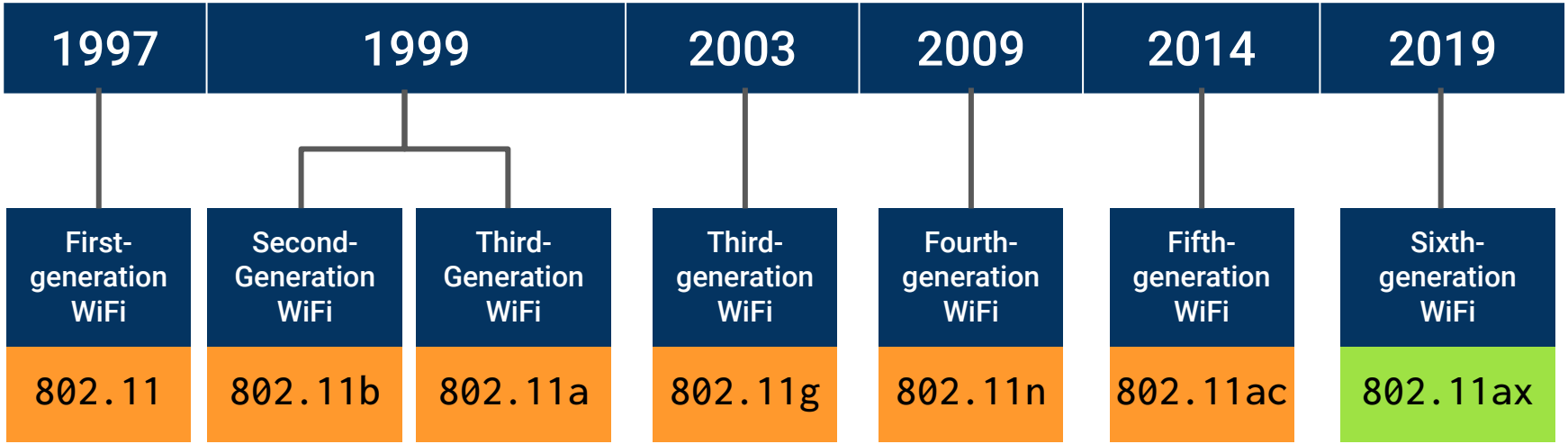
Wireless technologies are those that communicate data without wires through air and space.

WiFi is the type of wireless technology that uses radio waves to provide wireless internet and network connections.

Wireless Networking

Devices that use WiFi use a standard called `802.11`, developed by the Institute of Electrical and Electronics Engineers (IEEE), to talk to each other in an agreed-upon format.

`802.11` has different versions that allow different speeds, functionalities, and security protections.



(Source 1) (Source 2)

A **wireless access point (WAP)** is a networking hardware device that connects a wireless network to a wired network.

Wireless Networking

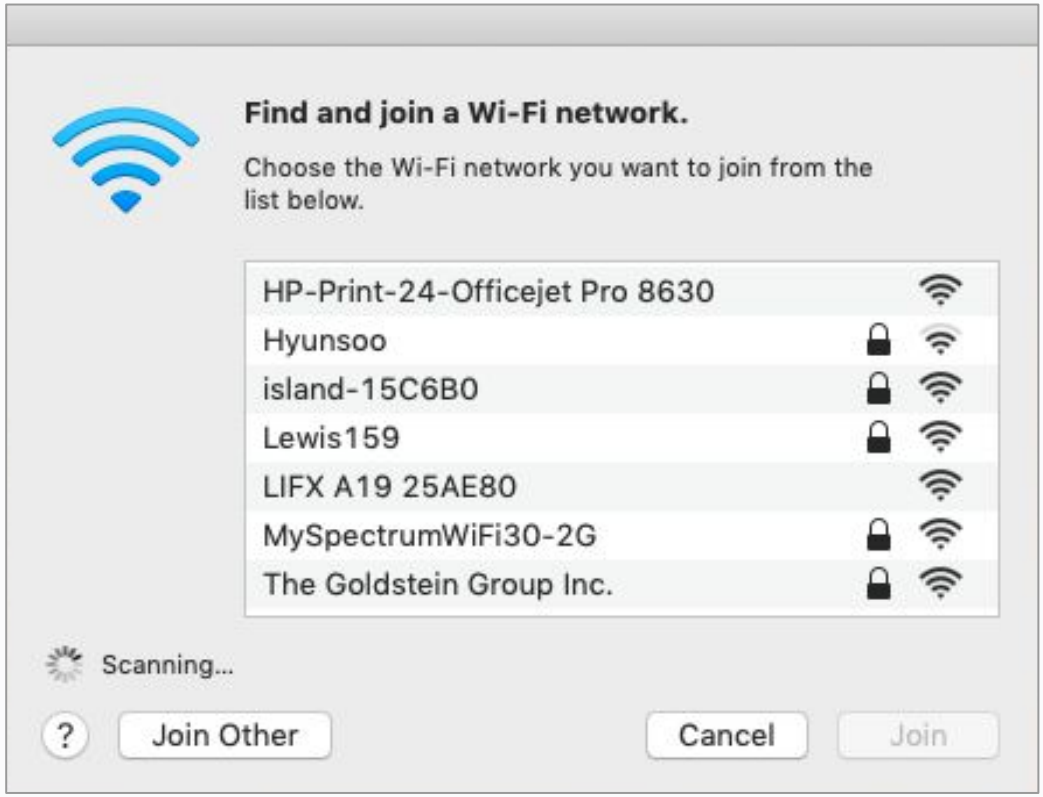
WAPs broadcast a signal called a **beacon** that computers detect and tune into.

When you select “View Available Wireless Networks," on your computer or your mobile device, these devices are detecting the beacon signals.

Connecting to WiFi Networks

When a WAP needs to broadcast its signal, it must identify itself.

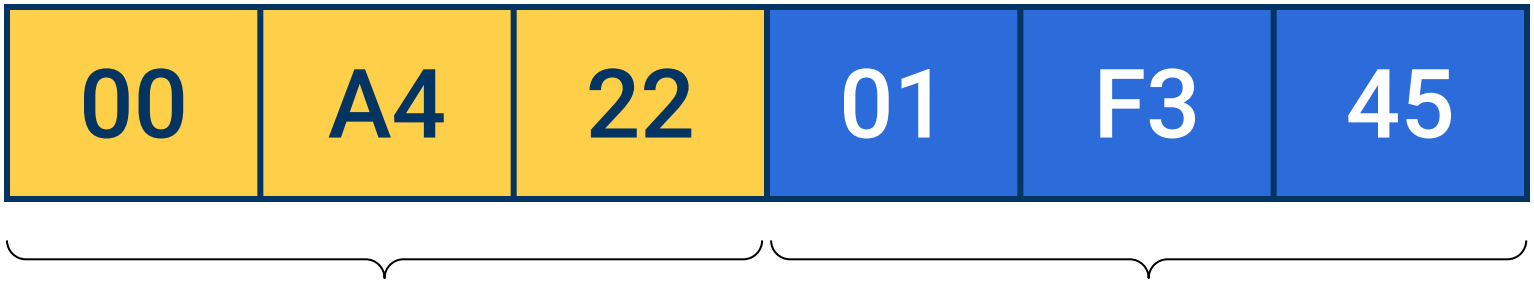
A WAP uses a **Basic Service Set Identifier (BSSID)** to identify its MAC address in a beacon signal.



Wireless Networking

When you're looking for the wireless signal to connect to your computer, MAC addresses are not easy to recognize.

MAC addresses use six hexadecimal octets, such as:

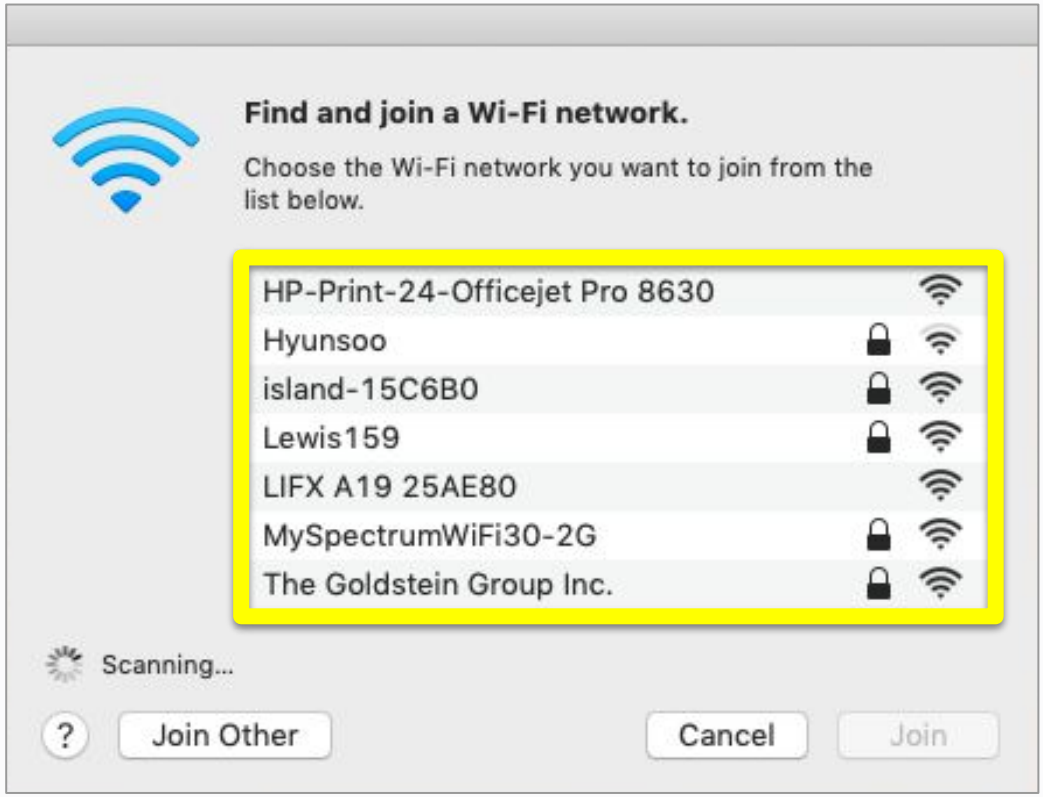


Connecting to WiFi Networks

For this reason, WAPs also broadcast a **Service Set Identifier (SSID)** using a more recognizable format.

The administrator of the WAP can configure this SSID.

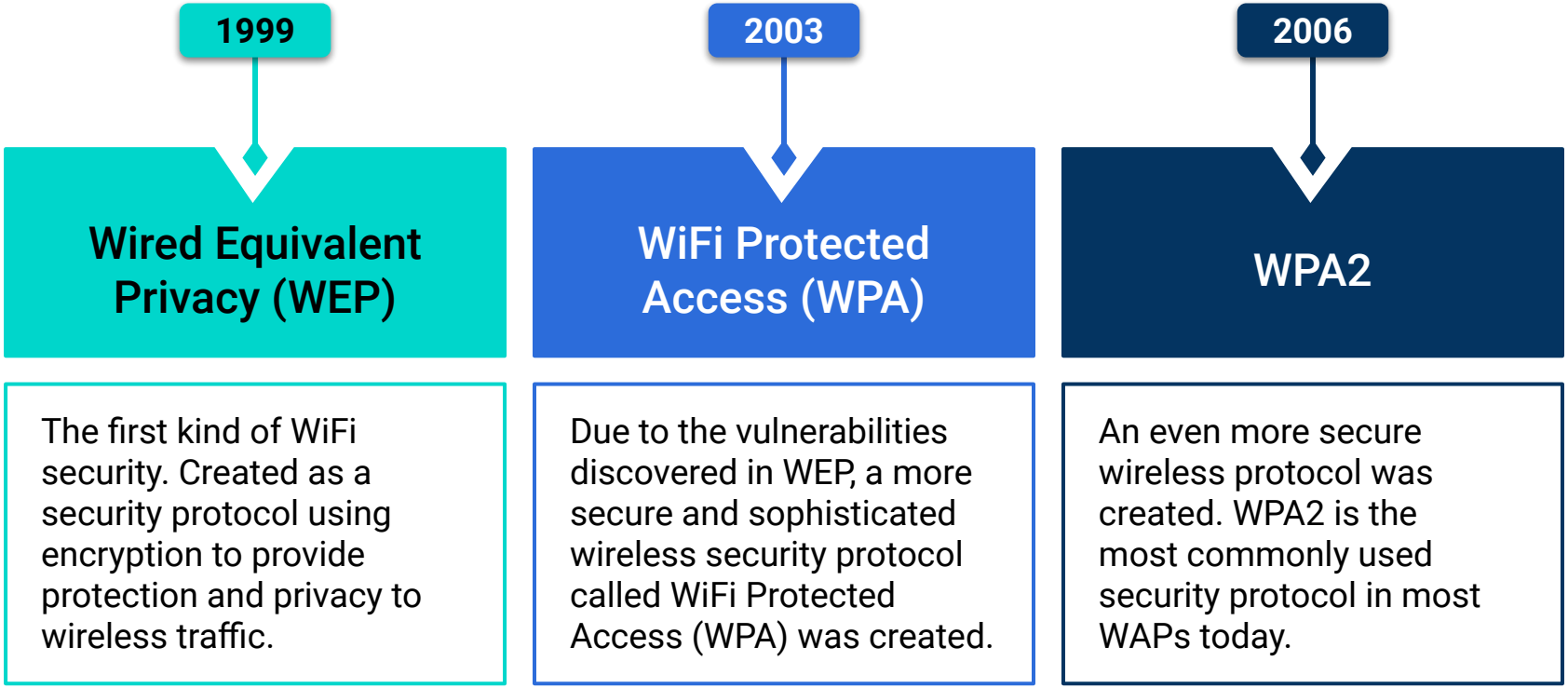
When you select "View Available Wireless Networks" on your device, the **SSIDs** are the names listed, such as "Airport WiFi," "Cafe_Public," etc.



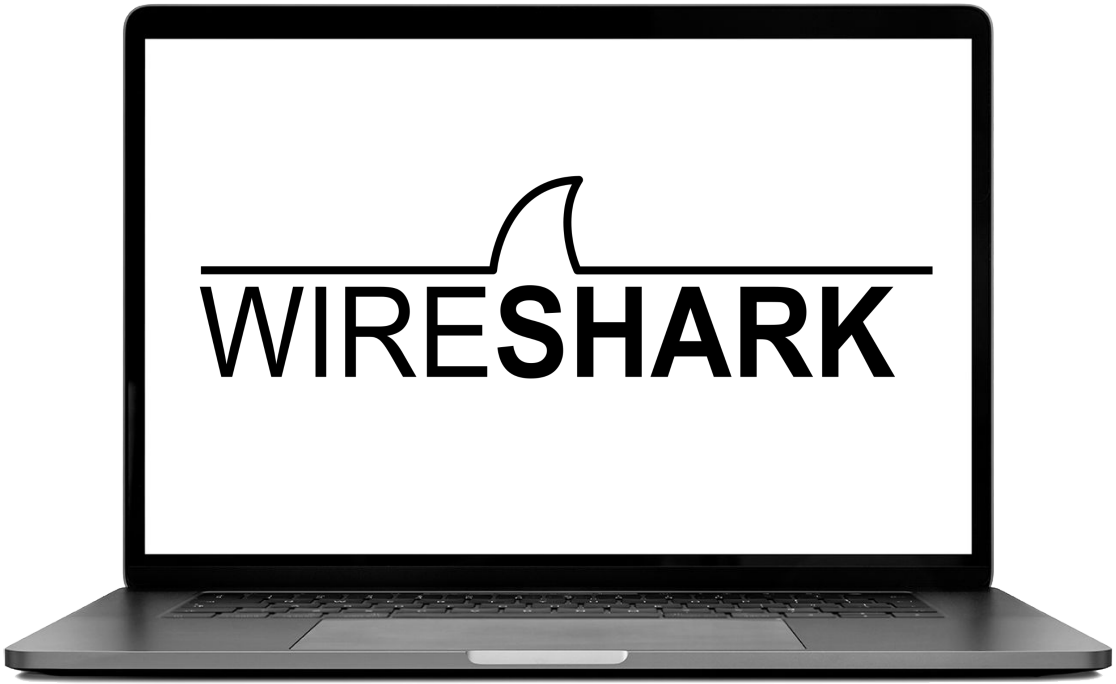
Connecting to WiFi Networks

WiFi provides great advantages by allowing users to connect their devices to the internet wirelessly. However, it’s possible for attackers to capture and view private wireless network traffic.

Wireless Security



Now we will now use Wireshark to visualize wireless beacon signals, capture BSSIDs and SSIDs, and determine which wireless security is being used by the wireless access points.



Instructor Demonstration

Visualizing Wireless in Wireshark

Activity: Analyzing Wireless Security

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

You will analyze your traffic capture from the Kansas City office and determine which wireless routers they have in the office, as well as the routers' SSIDs, BSSIDs, and the type of security they use.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?

Wireless Attacks

Cybercriminal Tactics

Cybercriminals have several methods of finding weak wireless security routers:

Wardriving

Driving around an area with a computer and a wireless antenna to find wireless LANs that may be vulnerable.

Warchalking

Marking locations with chalk so sites can be exploited these access points at a later time.

Warflying

Using drones to find vulnerable access points.

Cybercriminal Tactics

Cybercriminals can also create a fake wireless access point, called an **evil twin**. An attacker can make a fake SSID to trick unsuspecting users into connecting to the attacker's wireless access point.

For example:

An attacker can set up a fake WAP with the SSID Starbucks_FreeWifi in a Starbucks coffee shop.

Once the user is connected, the attacker can capture and view their traffic.

We will demonstrate how to use a free wireless decryption tool called Aircrack-ng to decrypt WEP-encrypted wireless traffic.

Instructor Demonstration

Decrypting with Aircrack-ng

Activity: Wireless Attacks - Optional

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

You must analyze a packet capture, obtain a wireless key, and decrypt wireless traffic in order to determine the associated security risks.

Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?


The End