IPs and Protocols

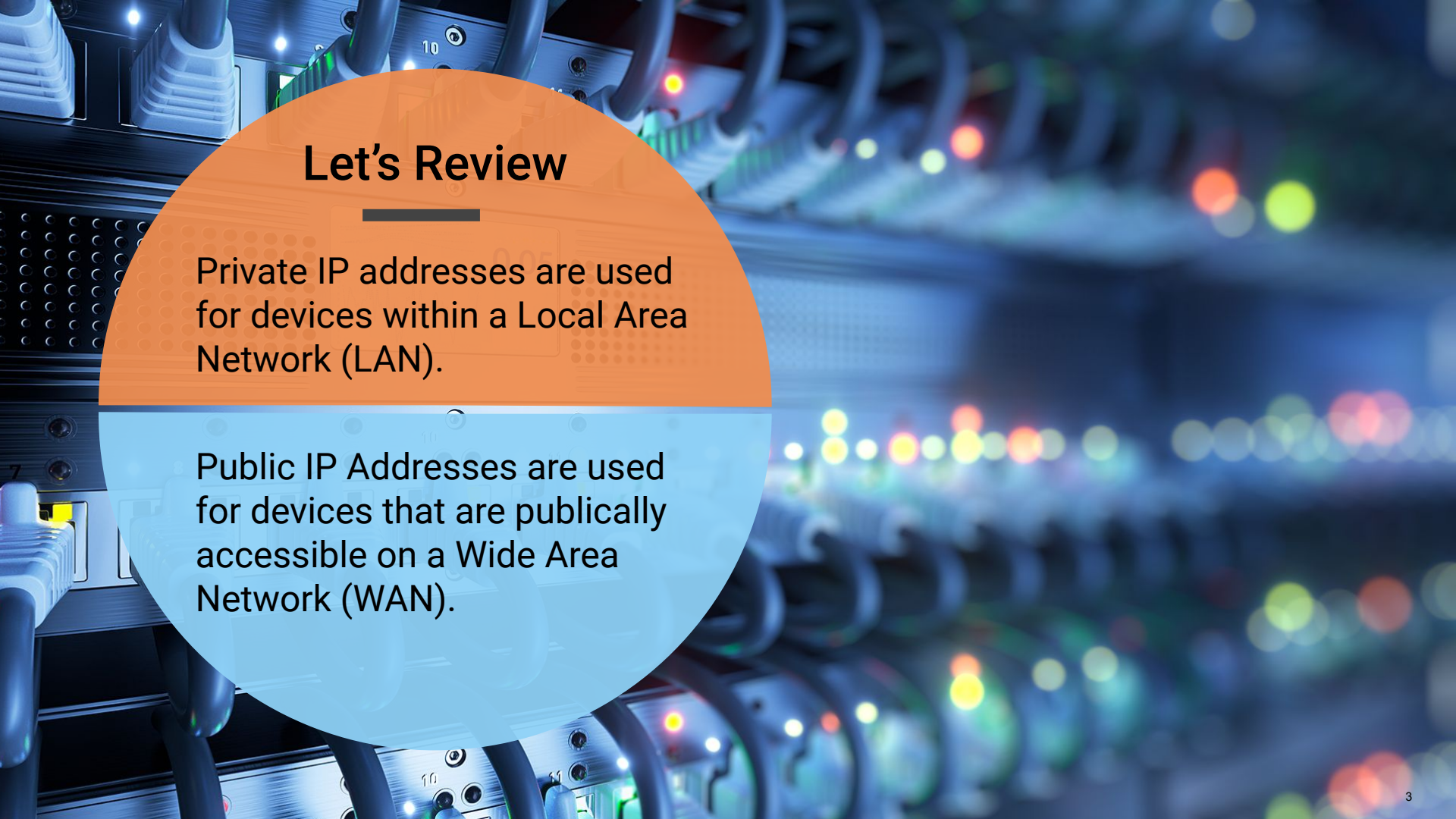
Cybersecurity

Networking 2, Day 1

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.



Let's 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)

Several processes are taking place when we connect to the internet…

LAN

?

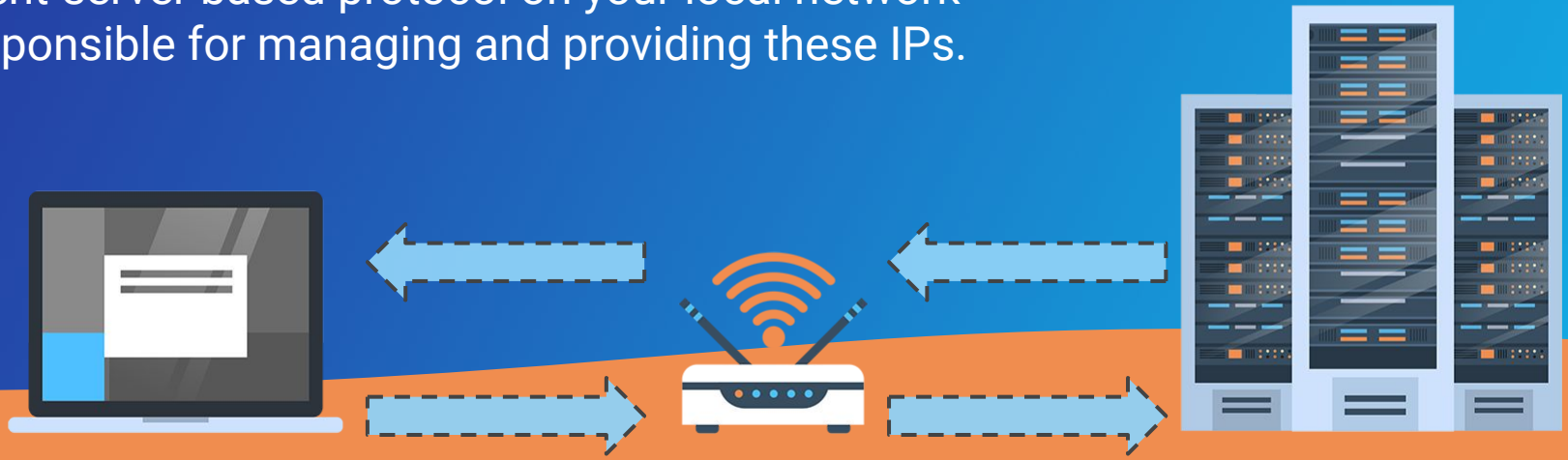
?

WAN

Dynamic Host Configuration Protocol (DHCP)

For a computer on a LAN to connect to a webpage, it first needs to be assigned a private IP Address.

The **Dynamic Host Configuration Protocol (DHCP)** is a client-server based protocol on your local network responsible for managing and providing these IPs.



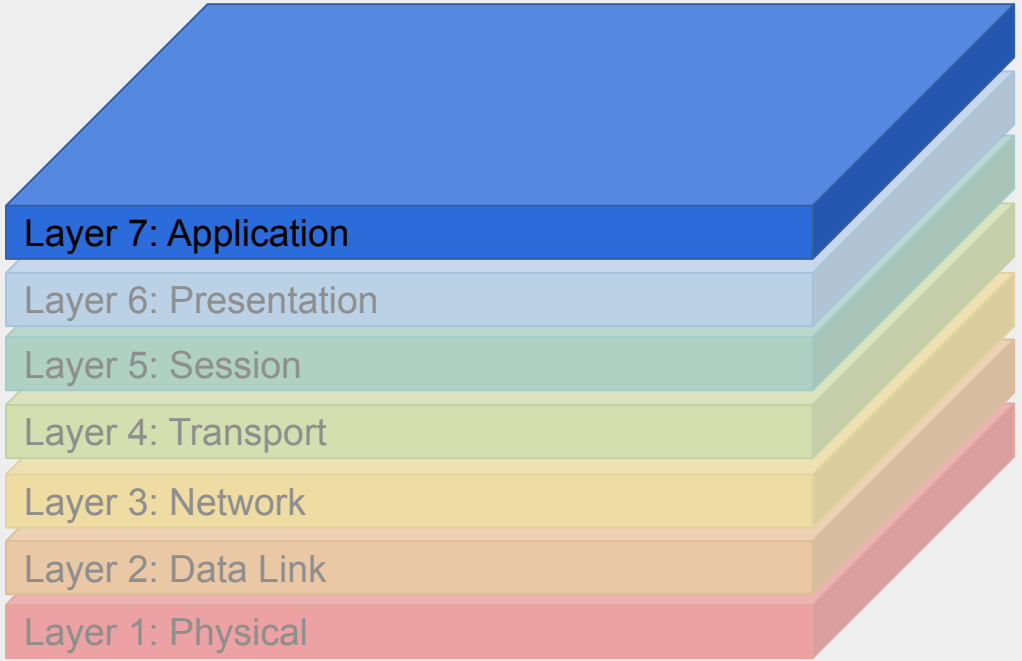
DHCP Fact List

DHCP is **dynamic**, because most devices do not have fixed IP addresses.

DHCP serves the DHCP clients—all devices needing a dynamic IP address.

DHCP is a **Layer 7: Application** 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

1 DHCP Discover

Client finds the server.

2 DHCP Offer

The server checks available IPs, selects one, and sends it back over the network.

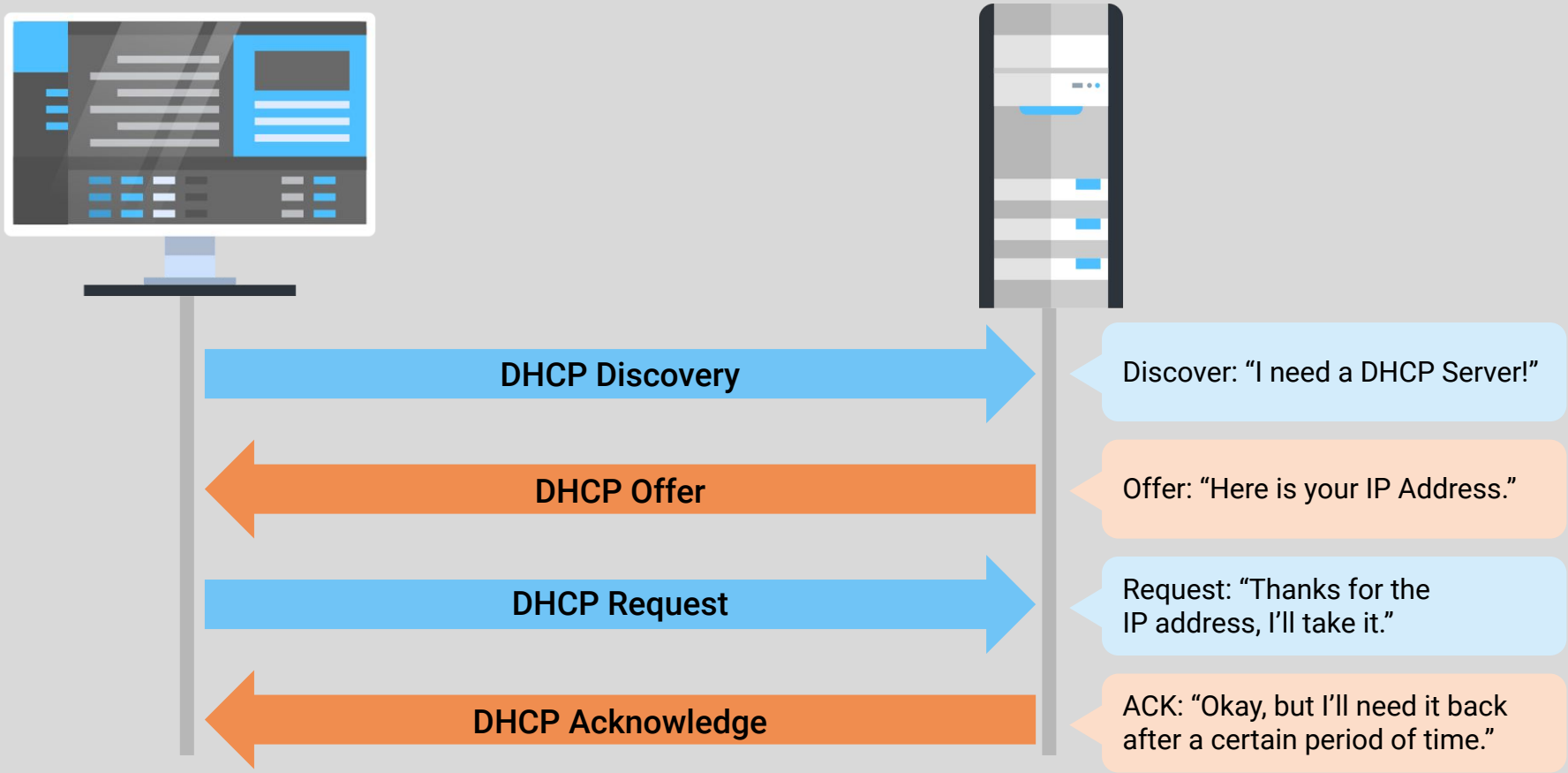
3 DHCP Request

Client sends a message accepting the IP.

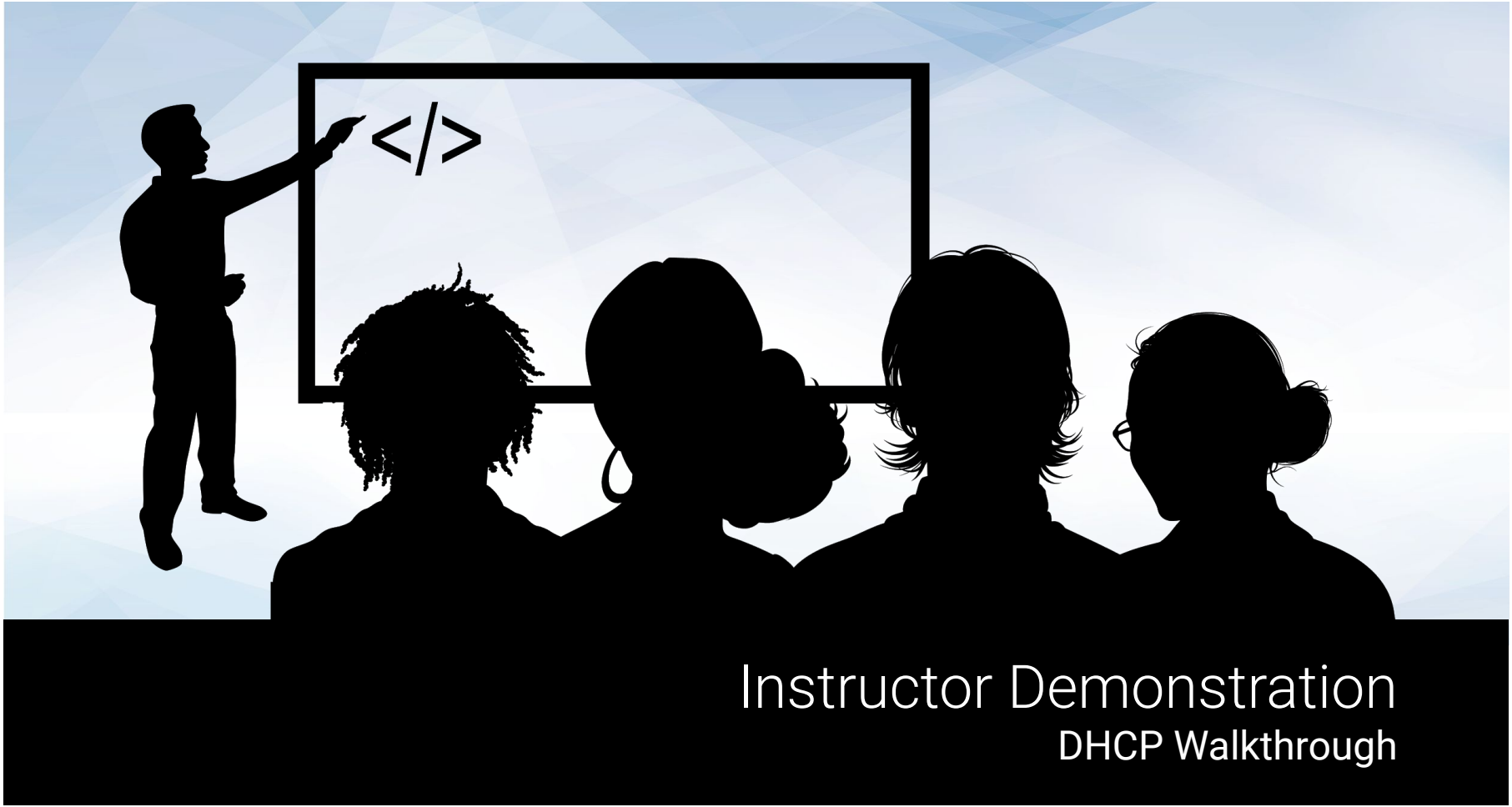
4 DHCP ACK

Server tells client the IP is valid for the **DHCP lease** time, after which it can be sent to another machine.

Four-Step Process



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

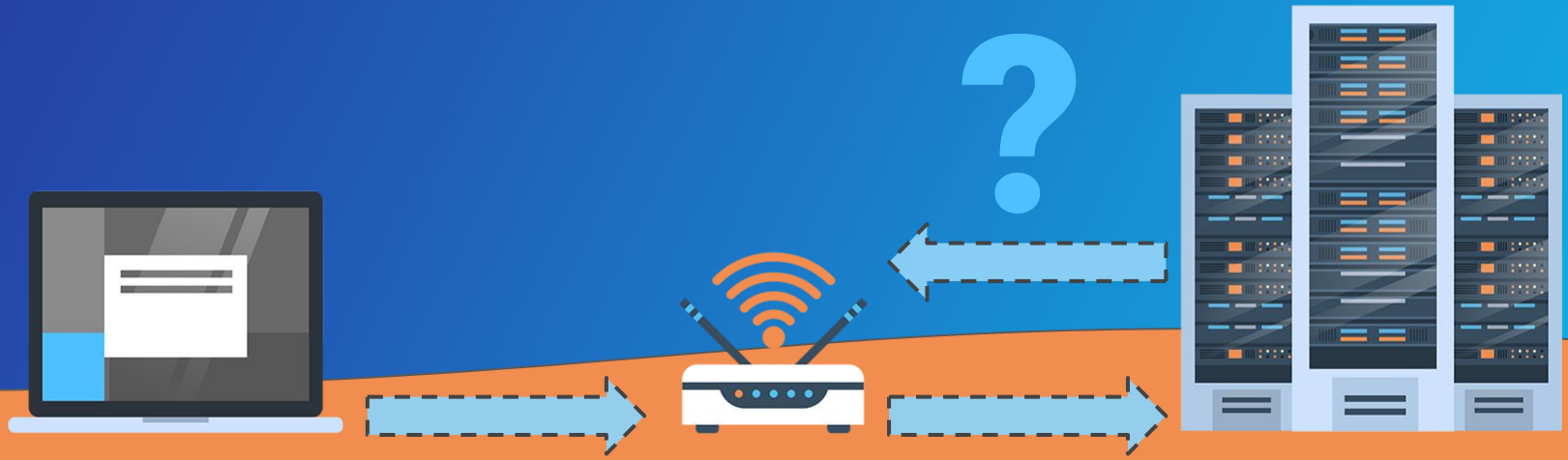


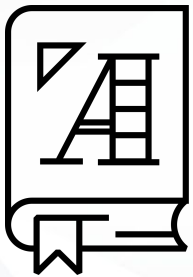
Instructor Demonstration

DHCP Walkthrough

NAT

The device now has a private IP address, but it still needs to connect to a WAN in order to access public data like websites.





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

NAT

Mappings gets stored in a **Network Address Translation Table**.

NAT tables are managed by the router, considered the gateway between private and public networks.

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

Step-by-Step Walkthrough

We'll walk 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: Creating the Packet

First, your computer creates a packet with the following info:

- Destination IP and port: `74.0.0.1:80`
- Source IP and port: `10.0.0.5:49200`

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 will be 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 Translation Table	
LAN Address	**WAN Address**
`10.0.0.5:49200`	`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 Translation Table	
LAN Address	WAN Address
10.0.0.5:49200	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

Google.com receives the packet and then responds with the another packet:

Incoming Packet	
Destination IP and Port	`74.0.0.1:80`
Source IP and Port	**`32.0.1`**`.5:49200`

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 and knows exactly which device is expecting this packet.
It will update the packet and translate the IP to include the following new packet details:

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

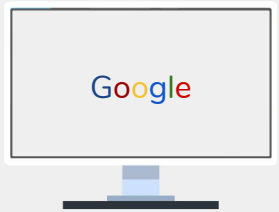
Incoming Packet	
Destination IP and Port	`10.0.5.1:49200`
Source IP and Port	`74.0.0.1:80`

NAT Translation Table	
LAN Address	**WAN Address**
`10.0.0.5:49200`	`32.0.0.1:49200`

Responding Packet	
Destination IP and Port	`32.0.01:49200`
Source IP and Port	`74.0.0.1:80`

Step Six: Return of the Packet

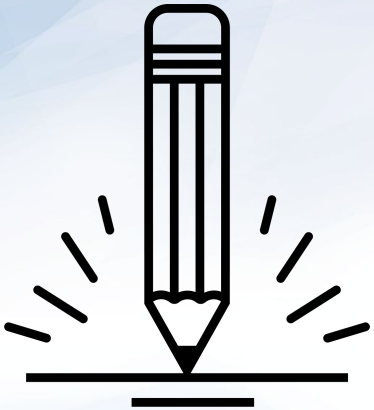
Your device, with private IP `10.0.0.5` receives the packet. You can now view google.com.



Receiving Packet	
Destination IP and Port	`10.0.0.5.1:49200`
Source IP and Port	`74.0.0.1:80`

NAT Translation Table	
LAN Address	**WAN Address**
`10.0.0.5:49200`	`32.0.0.1:49200`

Responding Packet	
Destination IP and Port	`32.0.01:49200`
Source IP and Port	`74.0.0.1:80`



Activity: Analyzing NAT

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

You will add message routes provided by Acme Corp to the NAT table.

Suggested Time:
10 minutes

DHCP Attacks

DHCP Attacks

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

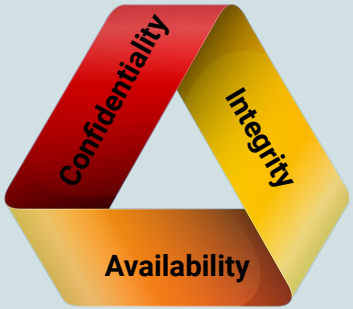
- If an attacker is able to access the LAN, they can send a large number of DHCP messages over the network requesting IP addresses from the DHCP server.
- If the number of requests is large enough, the DHCP server can run out of IPs, and new, legitimate users won't be able to receive an IP.

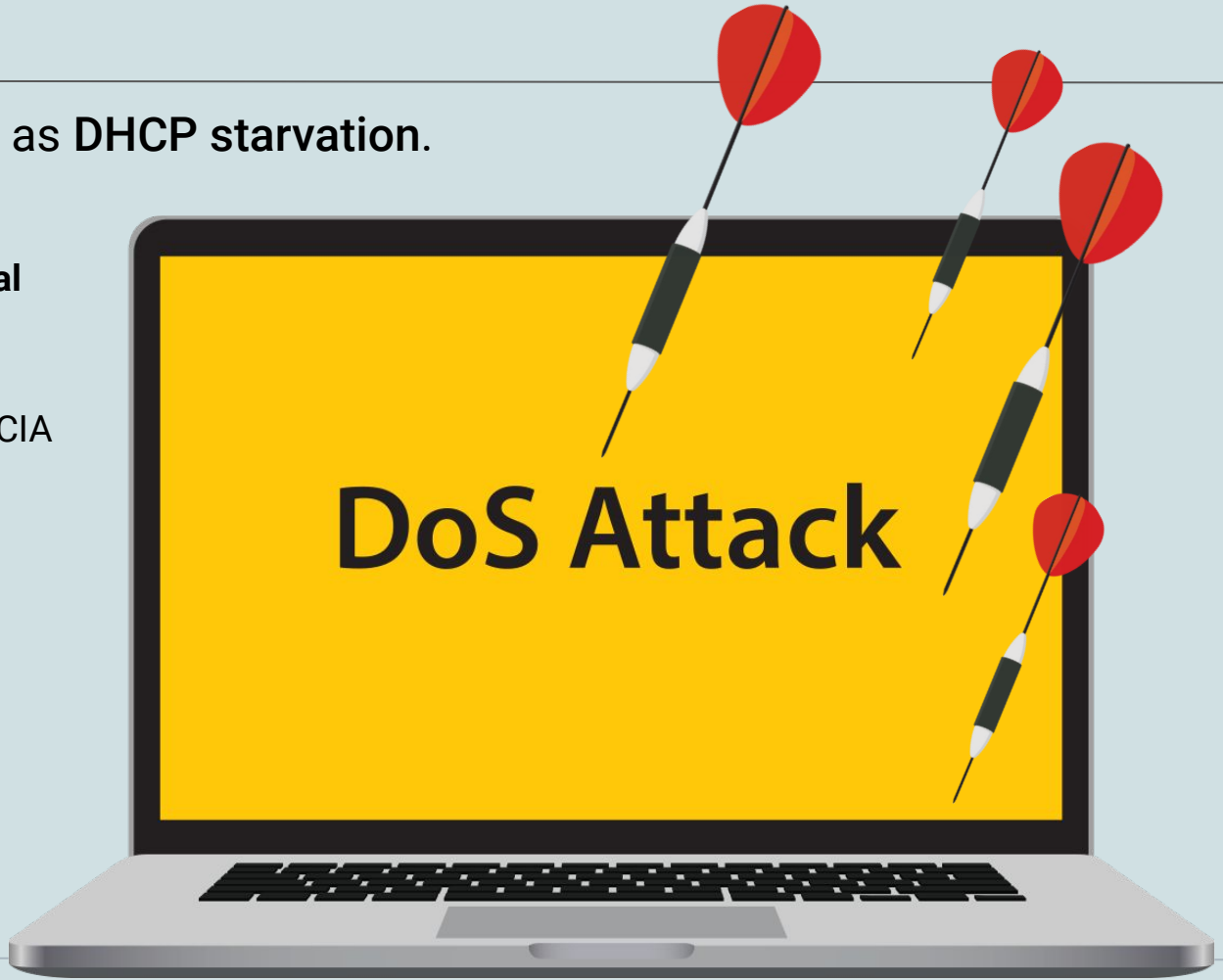
DHCP Attacks

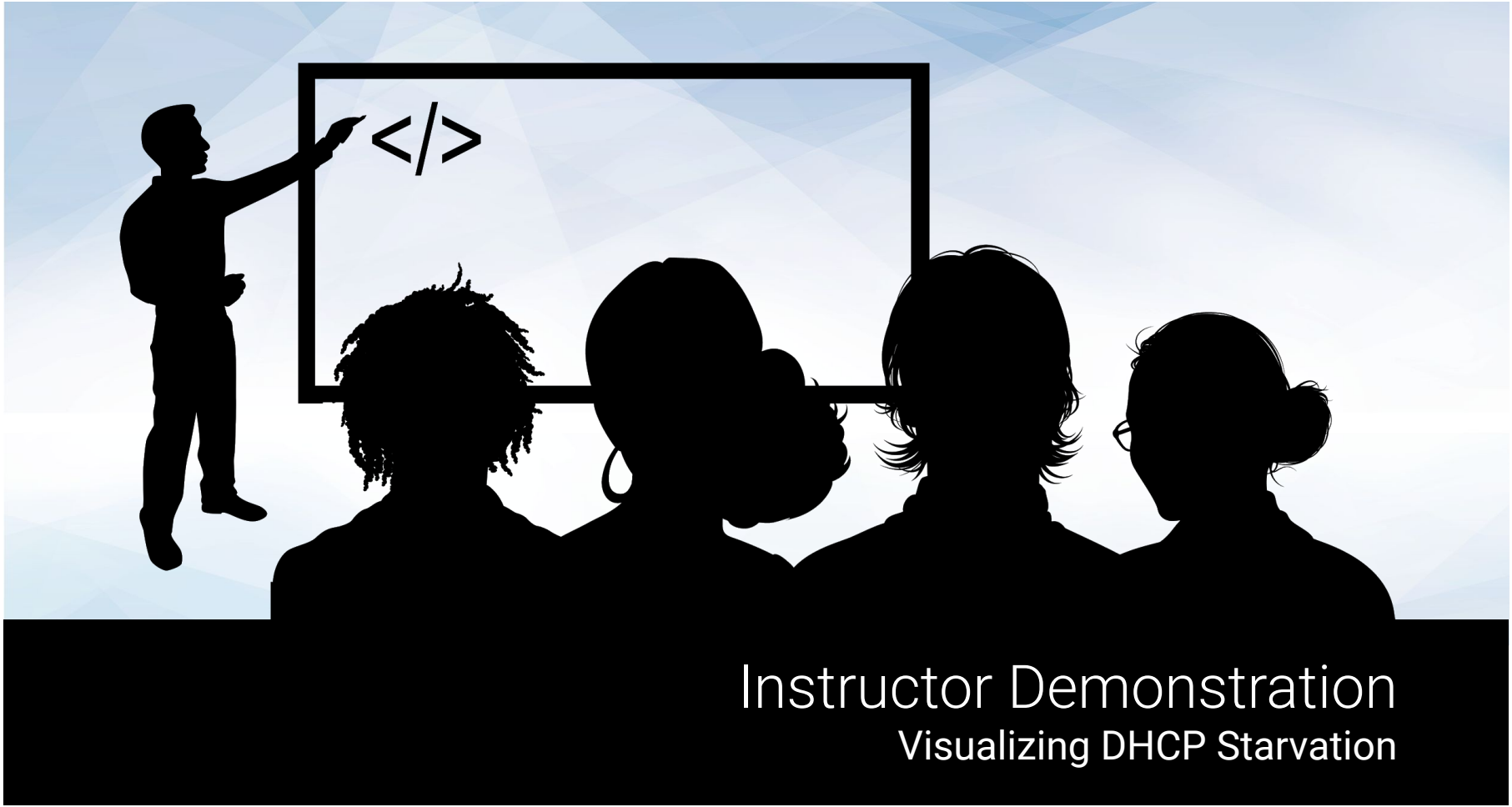
This attack is known as **DHCP starvation**.

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

This attack impacts the availability concept of the CIA triad.







Instructor Demonstration

Visualizing DHCP Starvation

Visualizing DHCP Starvation

Now, we'll visualize a DHCP starvation attack by opening up the following pcap file in Wireshark.

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

Preventing DHCP Starvation

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.

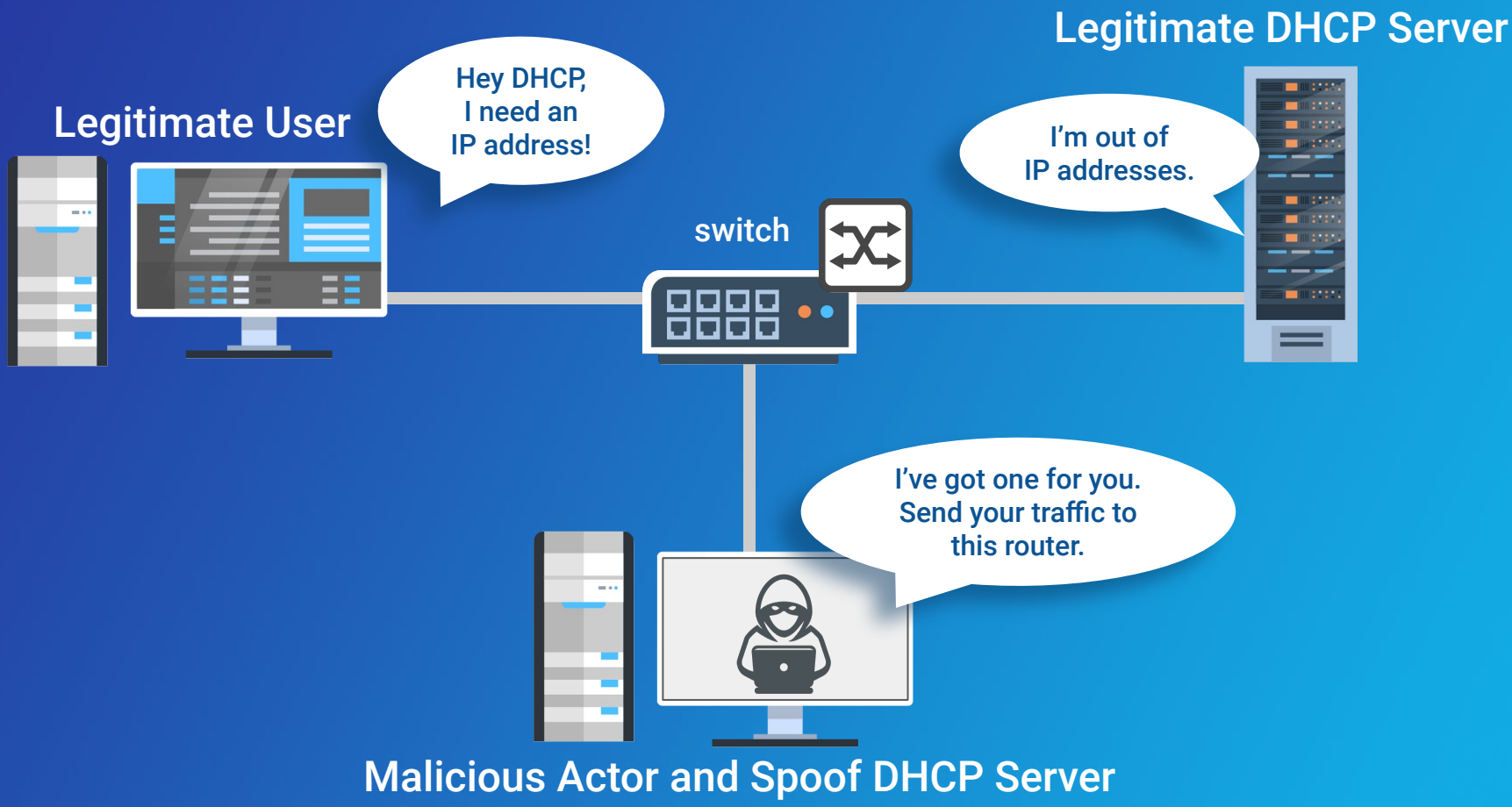
DHCP Spoofing

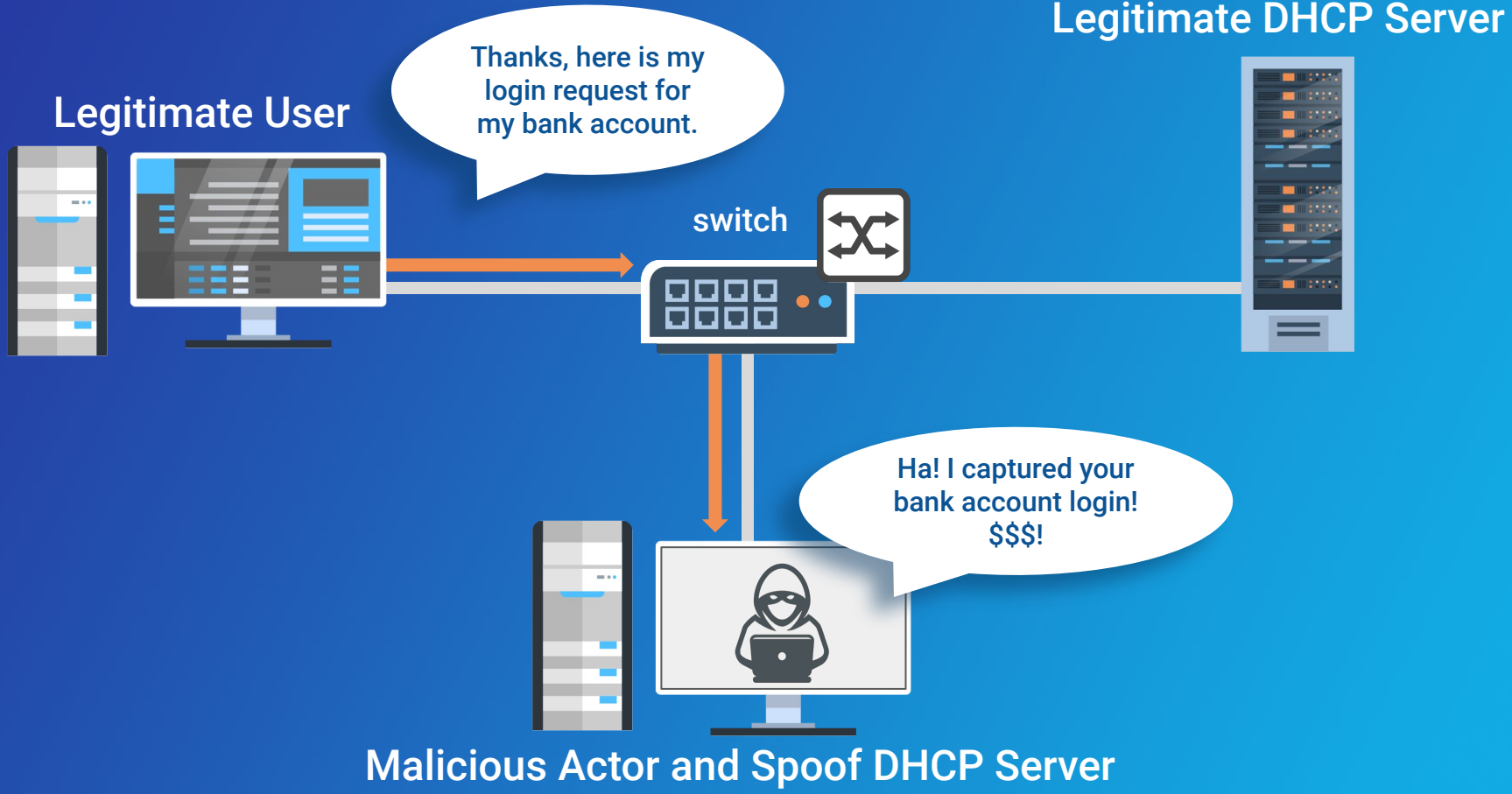
After a DHCP starvation attack occurs, an attack can potentially set up a fraudulent **DHCP server**.

The fraudulent server can send **spoof** messages, assigning clients to a malicious router.

The attacker can use this router to capture sensitive data.

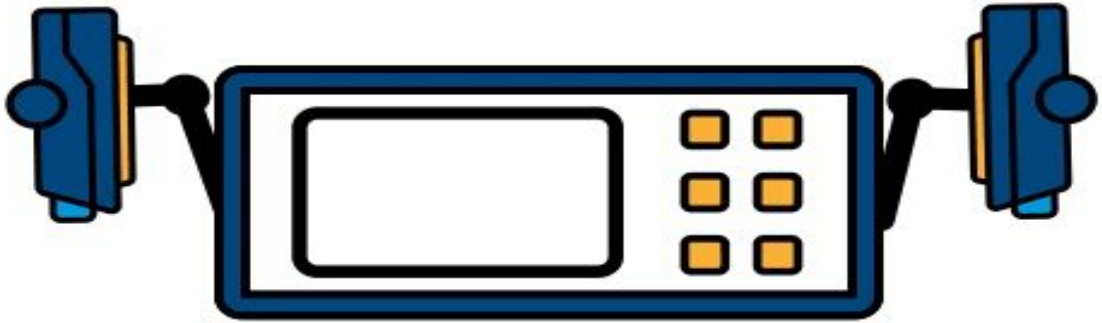
This attack is known as **DHCP spoofing**.

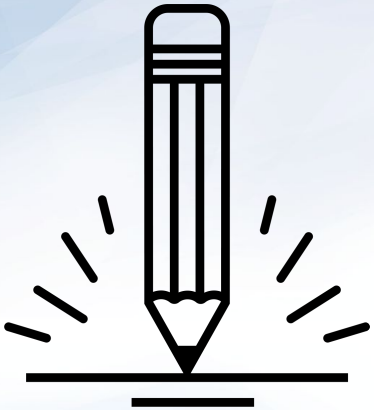

Legitimate DHCP Server
Legitimate User
Hey DHCP, I need an IP address!
I'm out of IP addresses.
switch
I've got one for you. Send your traffic to this router.
Malicious Actor and Spoof DHCP Server


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

Preventing DHCP Spoofing

DHCP snooping is a process implemented on a network switch that inspects packets to confirm that they're legitimate DHCP offers.





Activity: DHCP Attacks

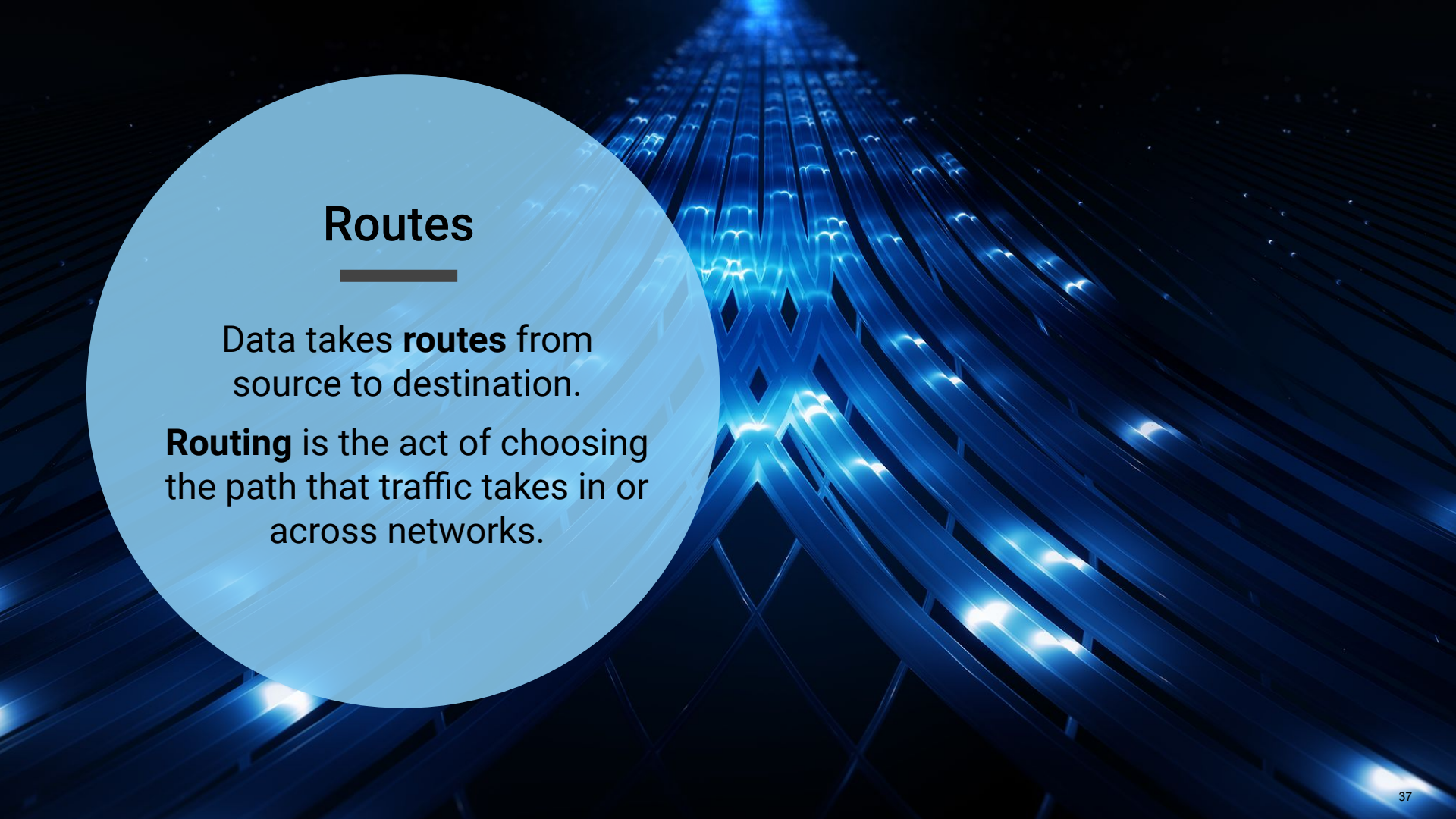
In this activity, you will continue to play the role of a security analyst at Acme Corp.

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.

Routing Schemes and Protocols



Routes

Data takes **routes** 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.

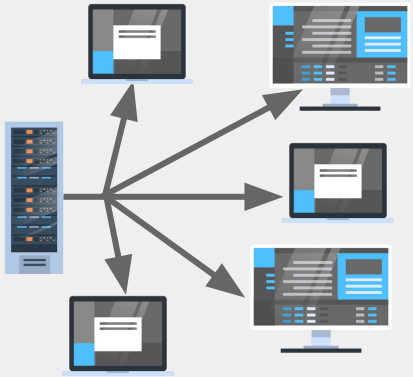
Routing Scheme Examples

Unicast

A phone call between two people.

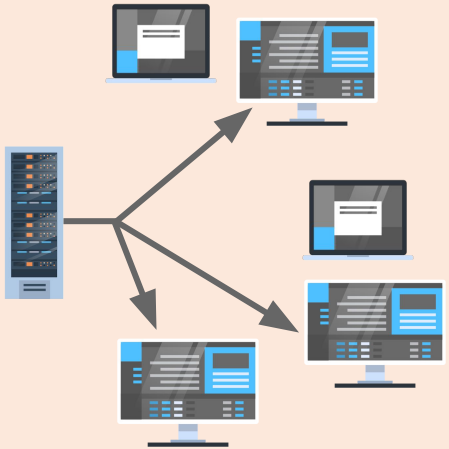
Broadcast

DHCP offer message that is broadcast across an entire LAN.



Multicast

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



Comparing the Schemes

Disadvantages of each:

Unicast	Broadcast	Multicast
If the message has to reach multiple destinations, many unicast messages must be sent.	Since broadcast messages are sent to everyone on a network, they can cause unnecessary traffic.	Intended recipients will need to be updated and maintained to make sure they're accurate.

Routing Techniques

Devices want to make sure traffic is sent as efficiently as possible.

Networks use two primary routing techniques to determine the path: **static** and **dynamic** routing.

Static Routing

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

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 can't be adjusted.

Dynamic Routing

Dynamic Routing prevents fault tolerance issues by allowing the network to act autonomously in order to avoid network blockages.

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

Primary routing technique used over the internet.

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

Routing Protocols

There are several **dynamic routing protocols** used to determine the path traffic takes to reach its final destination.

The two primary criteria are **distance** and **speed**.

Distance

Distance is the number of **hops** (devices) it takes to get from the source to the destination.

Dynamic routing protocols that use distance as criteria are **distance-vector routing protocols**.

Protocols include:

- **Routing Information Protocol (RIP)**
- **Enhanced Interior Gateway Routing Protocol (EIGRP)**

Speed

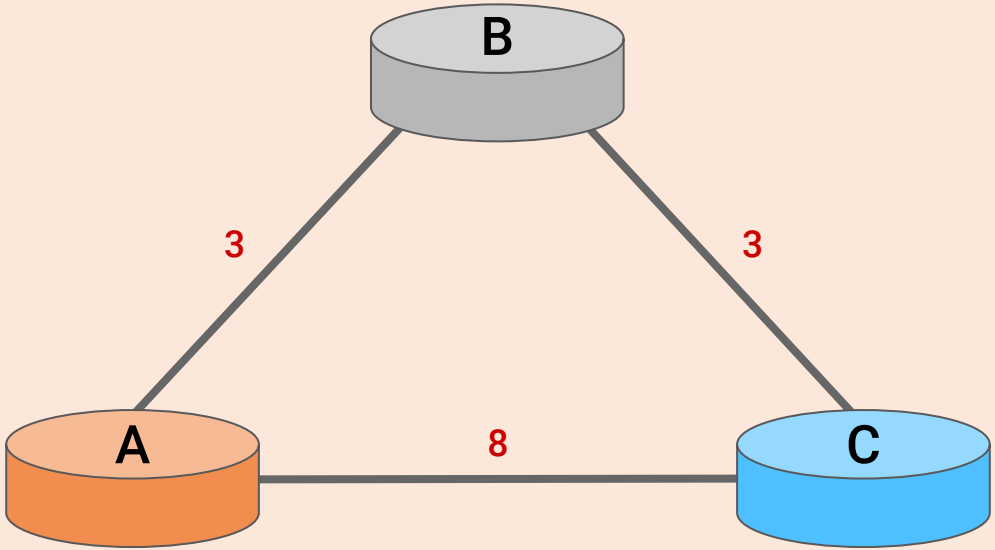
The route is determined by the time it takes to move from source to destination.

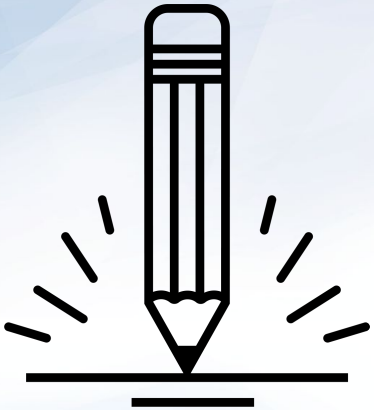
Dynamic routing protocols that use speed as criteria are **link-state routing protocols**.

One protocol is **Open Shortest Path First (OSPF)**.

Distance vs. Speed

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.





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.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Countdown timer

15:00

(with alarm)

Going Wireless


You may
already know that
wireless technologies
communicate data through
air and space without
using wires.

Wireless Networking

WiFi is a wireless technology that uses radio waves to provide wireless internet and network connections.

Devices that use WiFi have a standard called `802.11`.

Connecting to WiFi Networks

Wireless access points (WAPs) broadcast a signal called a **beacon** that computers detect and tune into.

Wireless Networking

When a WAP needs to broadcast its signal, it must identify itself with a **Basic Service Set Identifier (BSSID)**.

These BSSIDs are not easily recognizable. For example: `00-A4-22-01-53-45`. So WAPs also broadcast **Service Set Identifiers (SSID)**. For example:

- Austin Public Library
- Airport Wifi
- Starbucks_Public
- New England Clam Router
- This LAN is my LAN
- Abraham Linksys

Wireless Security

Can an attacker capture and view private wireless network traffic?

(Yes!)

How Do We Secure WiFi?

WEP

First, there was **Wired Equivalent Privacy (WEP)**, a security protocol using encryption to provide protection and privacy to wireless traffic.

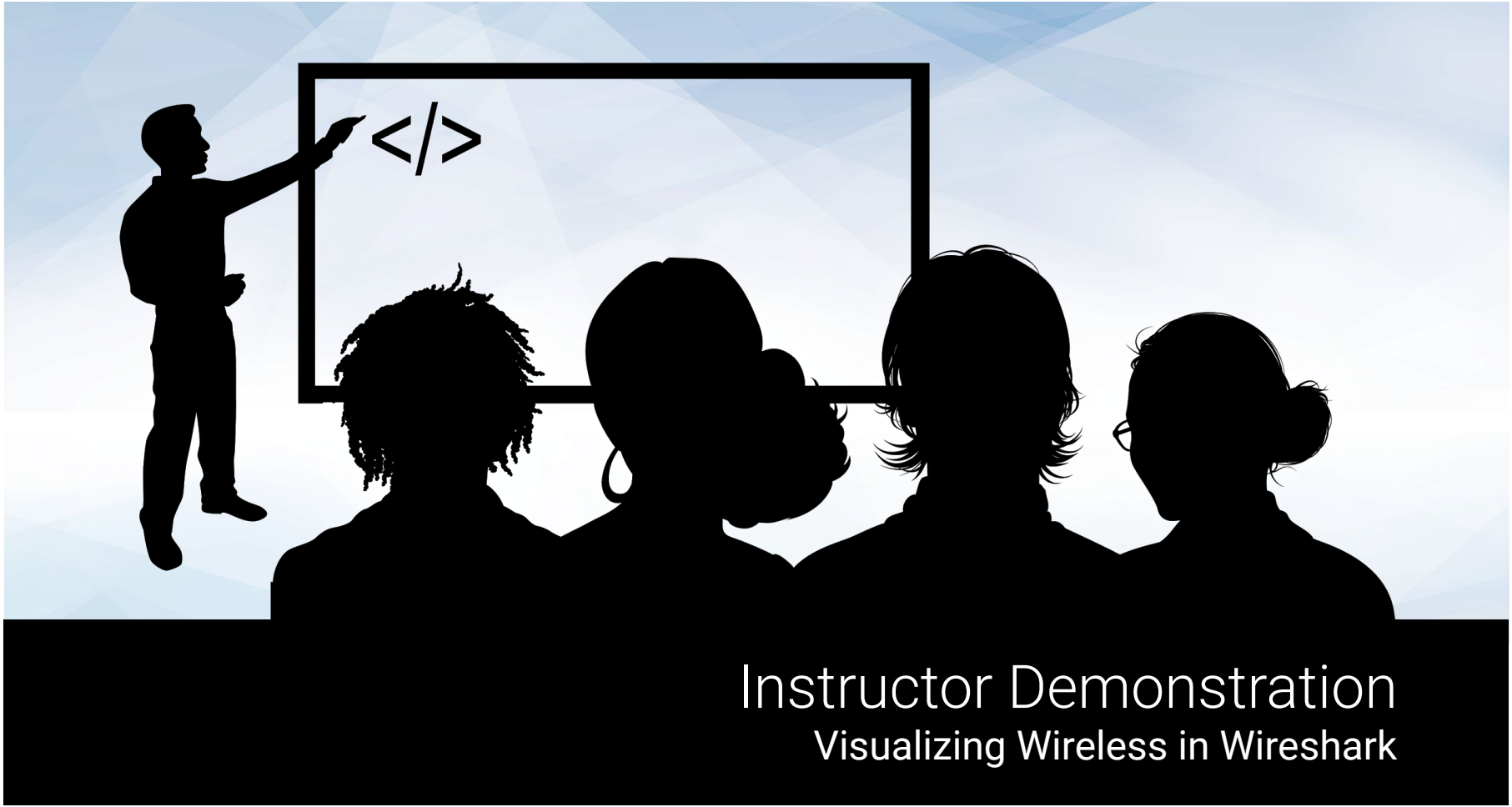
WPA

Major vulnerabilities made WEP obsolete, replaced by a more secure, sophisticated protocol called **WiFi Protected Access (WPA)**.

WPA2

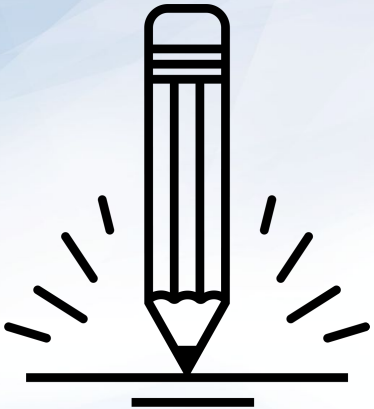
Finally, an even more secure protocol, **WPA2**, came along. This is currently the most commonly used protocol.

In the following demo, we will use Wireshark to visualize wireless beacon signals, capture BSSID and SSIDs, and determine which wireless security protocol is being used by the WAPs.



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.

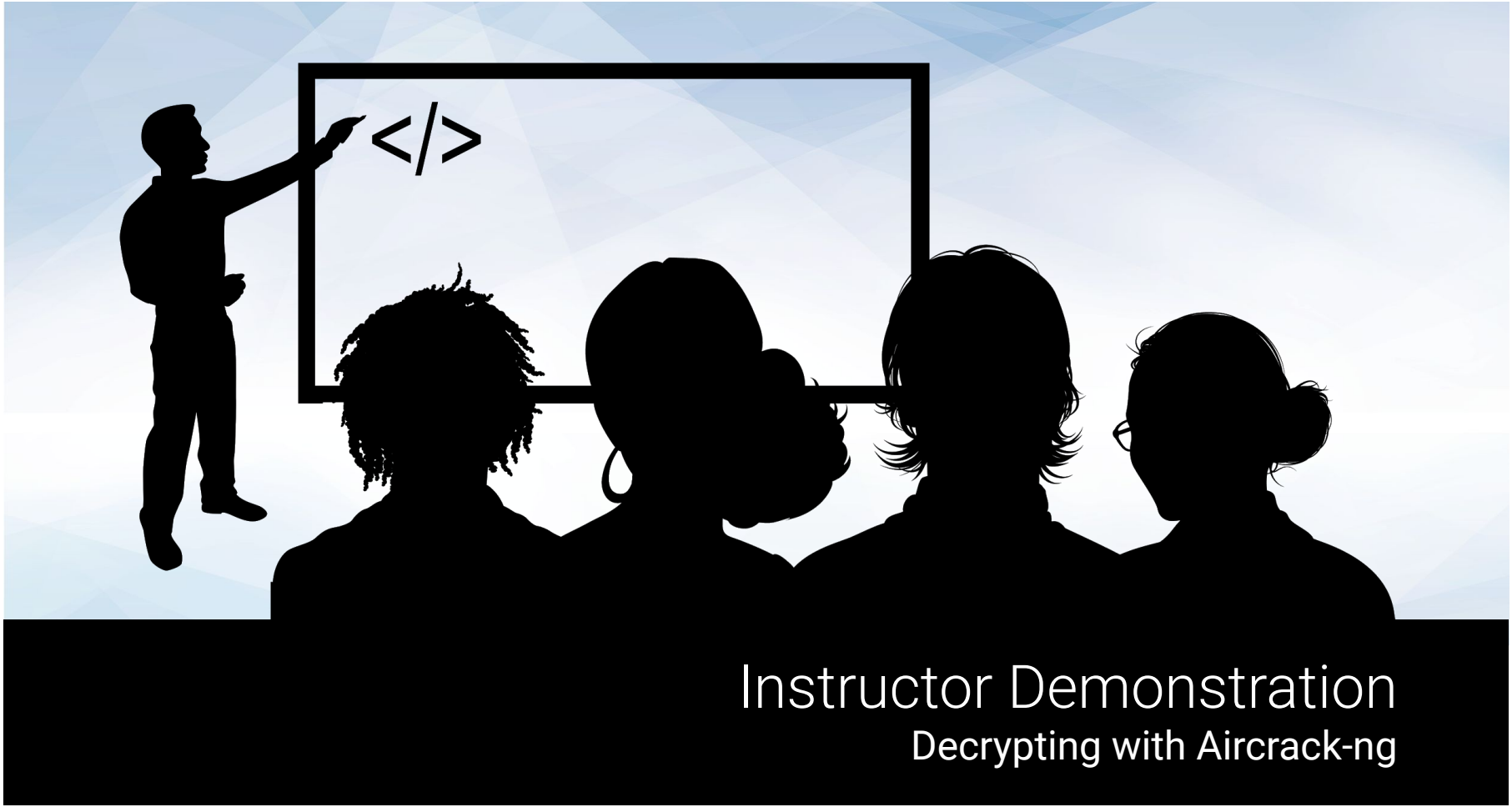
You will analyze your traffic capture from the Kansas City office, determine which wireless routers are in the office, and the routers' SSIDs, BSSIDs, and type of security.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Wireless Attacks

In the following walkthrough,
we will demonstrate how to use a tool
called **Aircrack-ng** to decrypt
WEP-encrypted wireless traffic.



Instructor Demonstration

Decrypting with Aircrack-ng

Cybercriminal Tactics

How cyber criminals can find weak wireless security routers that are available for exploit:

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.

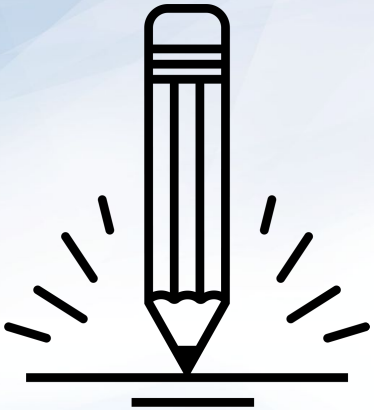
Warflying: Using drones to find vulnerable access points.

Look up: *warchalking symbols*

Cybercriminal Tactics

Cybercriminals can also create a fake WAP called an **evil twin**:

When using an evil twin, an attacker can make a fake SSID to trick unsuspecting users into connect to the attacker's wireless access point.



Activity: Wireless Attacks

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:
15 Minutes

Time’s Up! Let’s Review.

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.