

WELCOME TO ARUBA NETWORK SECURITY ESSENTIALS!

QUICK LINKS:

Aruba Certification & Training:
arubanetworks.com/certification

Airheads Community:
community.arubanetworks.com/

HPE Press Study Guides:
hpepress.hpe.com

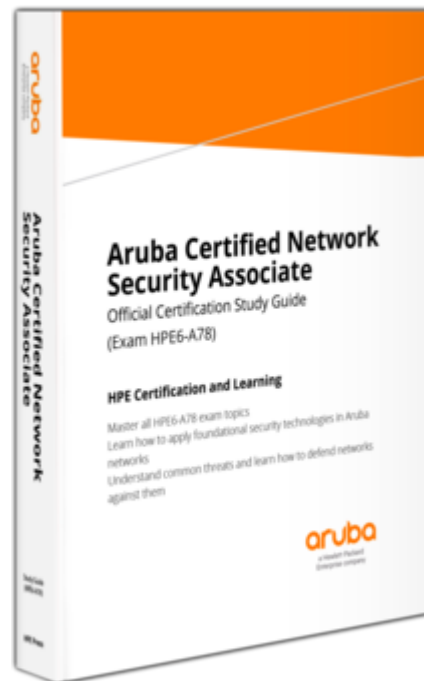
Contact us: arubatraining@hpe.com

Part 1: January 25

Part 2: February 1

You are here!

Next Step: Get certified on Aruba Security!



Aruba Network Security Essentials for the Intelligent Edge!

What to expect

ENGLISH | Presenter: Tyler McMinn

SPANISH | Presenter: Alvaro Tellez

- Thank you for choosing to learn with us, we can't wait to get started!
- To start learning Aruba's network security technologies you need some basic network security knowledge- and that's what you'll get here.
- If you attend both sessions, you will get a certificate of course completion!

Aruba Mobility Essentials for the Intelligent Edge!

What to expect

ENGLISH | Presenter: Tyler McMinn

PART 1: January 25th, 2021 | 8AM-10AM PST

PART 2: February 1st, 2021 | 8AM-10AM PST

- Part 1 Introduces malware and threat assessment while covering how to defend networks and harden switch devices.
- Part 2 Hardening wireless devices. Explain the use of security protocols, user authentication, and data encryption technologies.

SPANISH | Presenter: Alvaro Tellez

PARTE 1: Enero 25th, 2021 | 11AM-1PM PST

PARTE 2: Febrero 1st, 2021 | 11AM-1PM PST



aruba

a Hewlett Packard
Enterprise company

Aruba Network Security Essentials

Re 20.31



a Hewlett Packard
Enterprise company

Security Threats and the Aruba Security Strategy

Aruba Network Security Fundamentals

Rev 20.21



EDUCATION
SERVICES

Security Fundamentals

Confidentiality, Integrity, and Availability (CIA)



Confidentiality (privacy)

- No one can read a message except the intended recipient(s)



Integrity

- The message received matches the message sent
- Related to authenticity

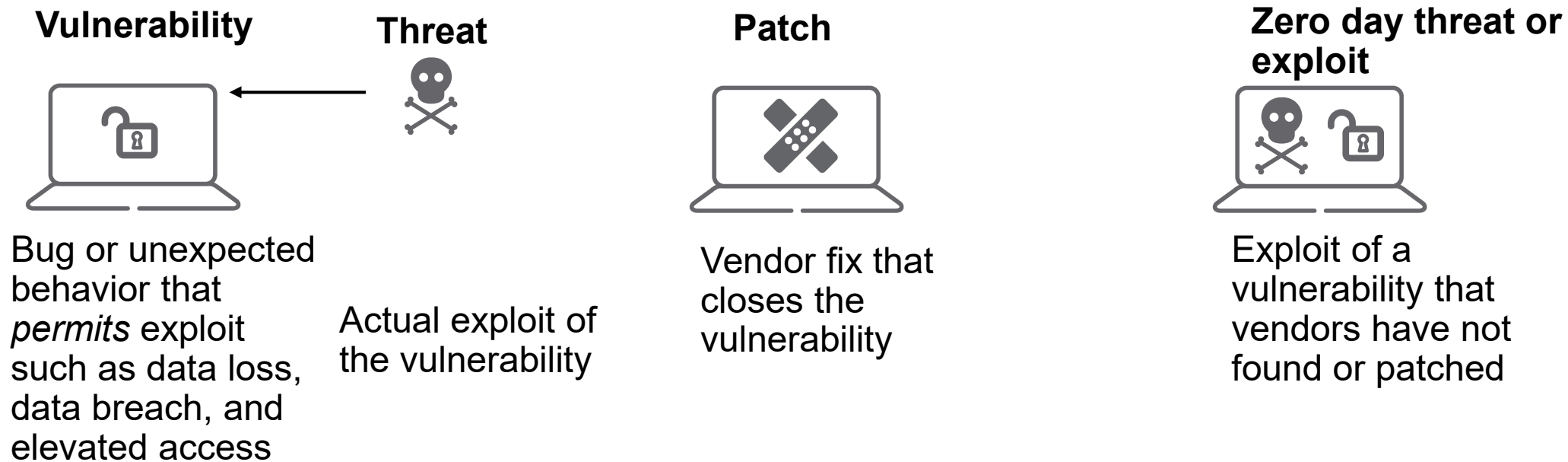


Availability

- Network services are available for legitimate users

Threat Overview

Vulnerabilities versus Threats



Actors

Bad actors (“black hat”)

- Outside hackers
 - Someone seeking to cause general mischief
 - Criminal
 - Government
- Inside hackers
 - Disgruntled employees or contractors
 - Self-serving employees or contractors



Non-malicious actors

- Careless employees or admins who expose the network to threat
- Inexperienced admins
- Users behaving badly or breaking rules, but without malicious intent



Ethical hackers (“white hat”) and “pen” testers

- Security researchers: Discover vulnerabilities so that they can responsibly disclose and inform vendors
- Pen testers: Perform penetration testing to help companies find and close vulnerabilities



What Is Malware?

- Malicious code that executes unauthorized actions on a device
 - Examples: Steal data or lock up the device
- Key component of many exploits

Malware-infected device

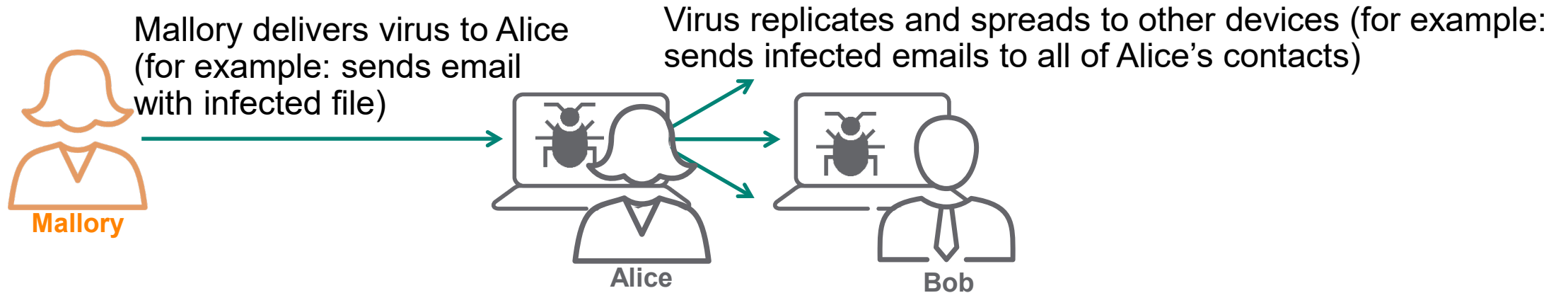


- Many types of malware, often classified by
- How the malware infects the system
 - What the malware does

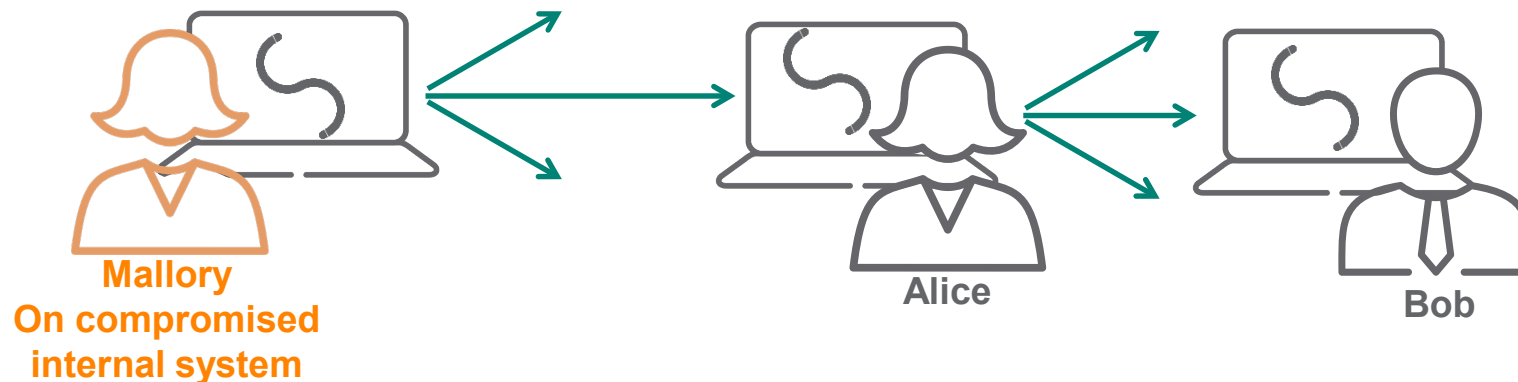
Malware

How It Infects a System

Virus—Infection requires user to do something (such as run a file)



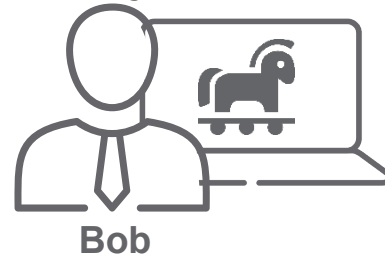
Worm—Spreads on its own



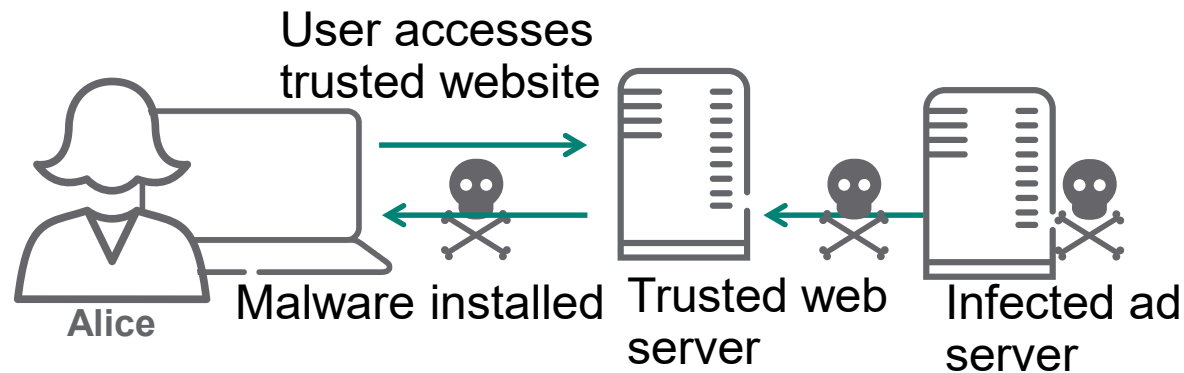
Malware

How It Infects a System (Cont.)

Trojan—User voluntarily installs software that includes hidden malware



Malvertising and driveby downloads



Malware

What It Does

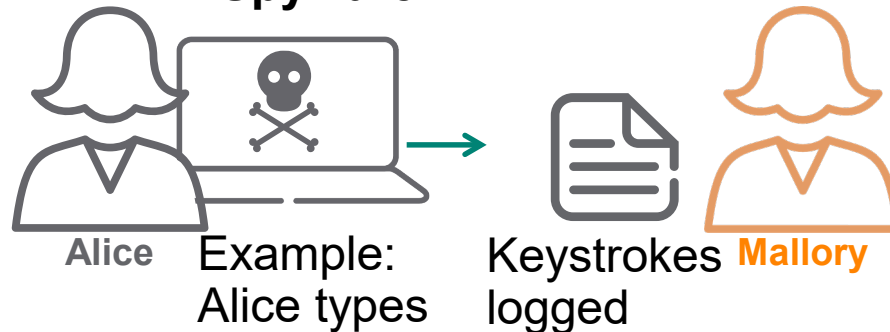
Adware (sometimes classified as Potentially Unwanted Program, PUP)



Ransomware



Spyware



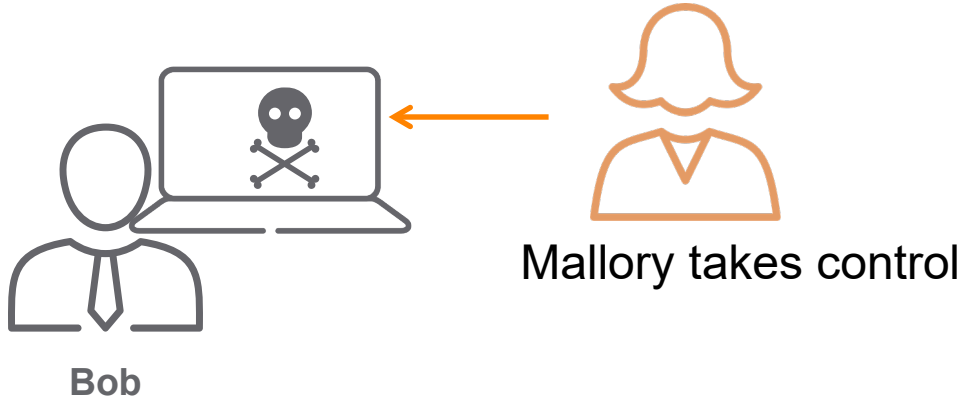
Crypto-mining malware



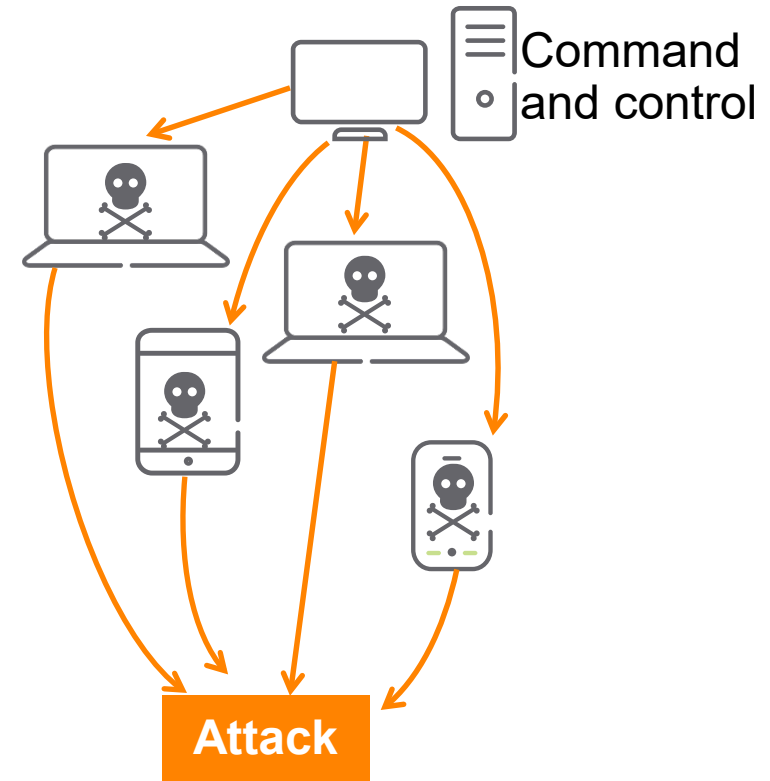
Malware

What It Does (Cont.)

**Remote Administration
Tool/Remote Access
Trojan (RAT) and rootkit**

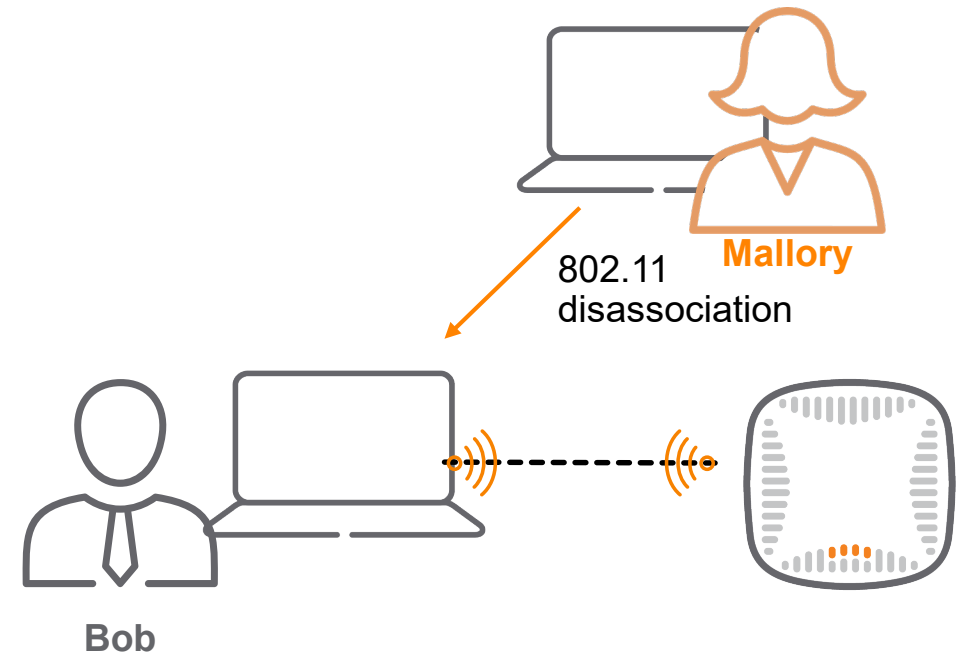


Bots and botnets



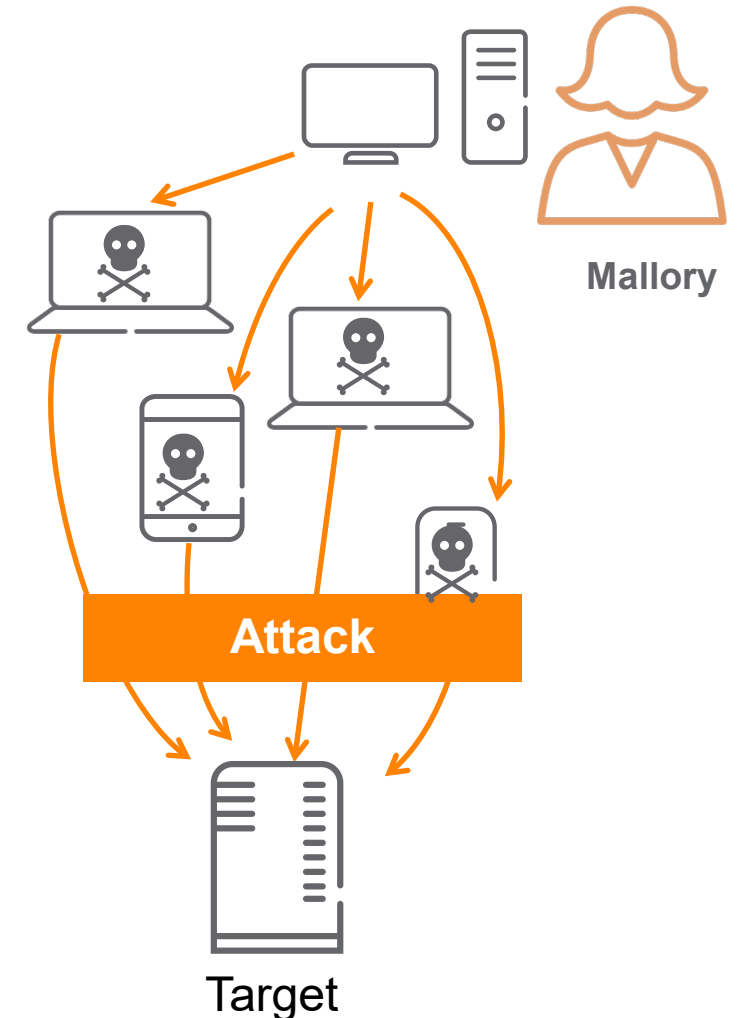
Denial of Service (DoS)

- Any attack that prevents users from accessing a network or network services
- Many ways to launch
- Examples include:
 - Services DoS
 - Targeting a vulnerability to freeze a server
 - Tying up sessions and overwhelming a server
 - Network DoS
 - Inserting invalid routes
 - Overwhelming ARP tables
 - Wireless DoS
 - Sending 802.11 disassociation or de-authentication frames to clients
 - RF jamming

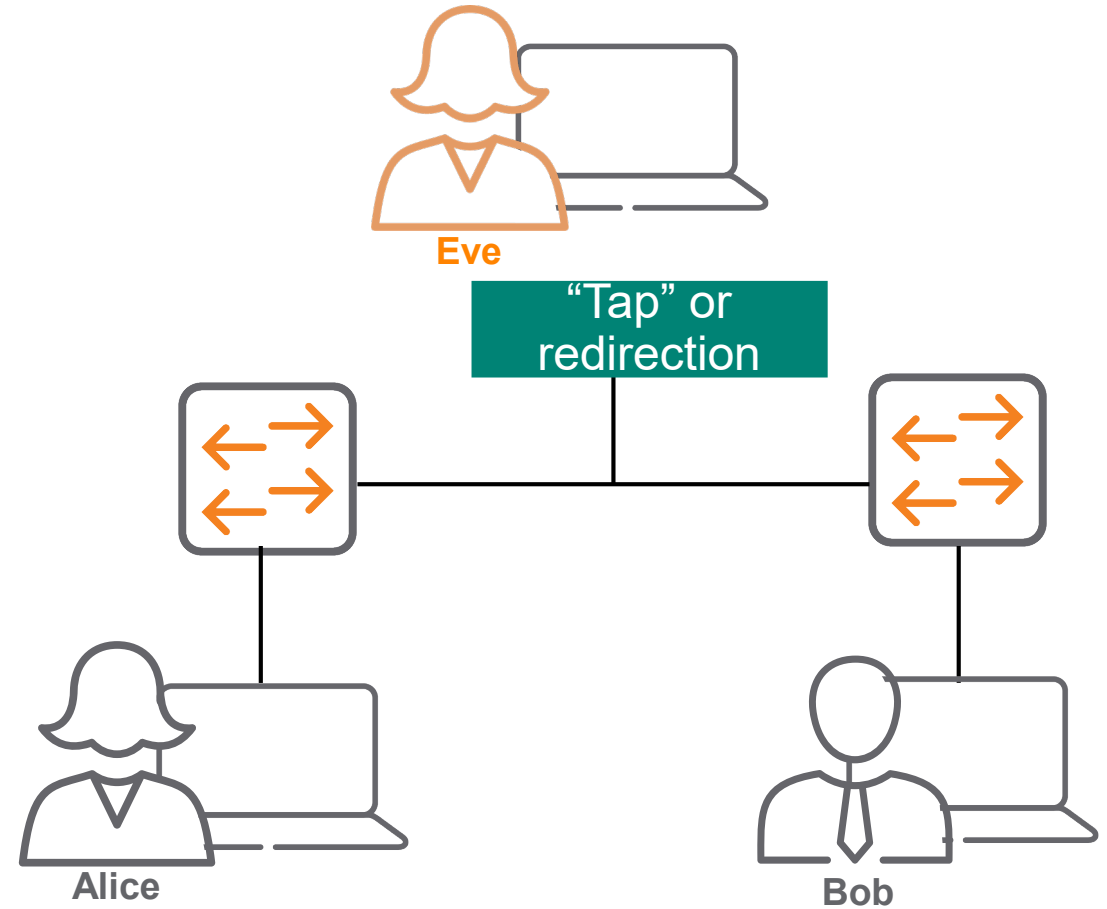
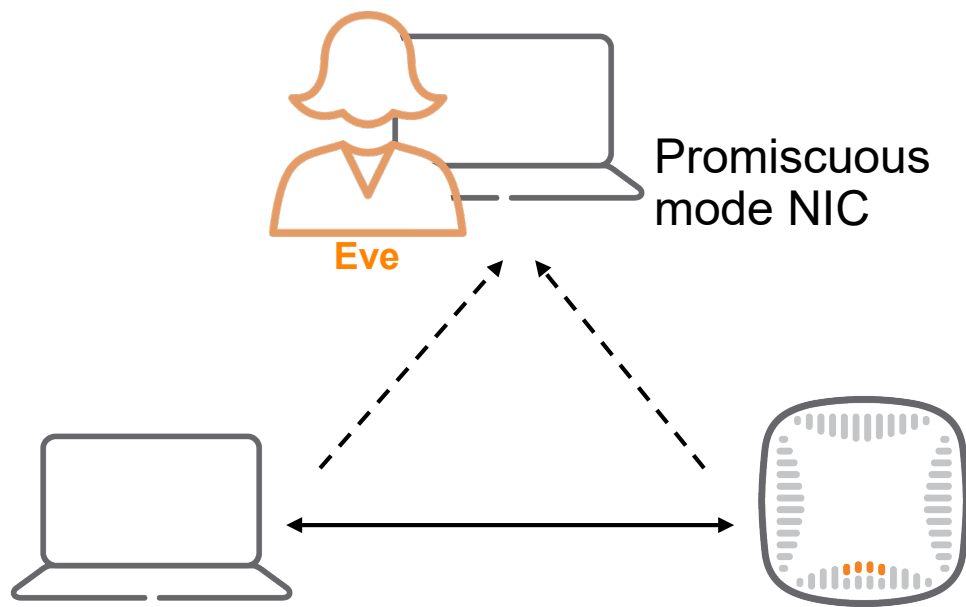


Distributed Denial of Service (DDoS)

- DoS attack launched by many devices to overwhelm a system
 - One common method: Botnet
- Typically launched through the Internet
- But your internal security controls can:
 - Help prevent endpoints from becoming bots launching DDoS attacks against other systems
 - Help detect and rate limit endpoints that are acting like bots

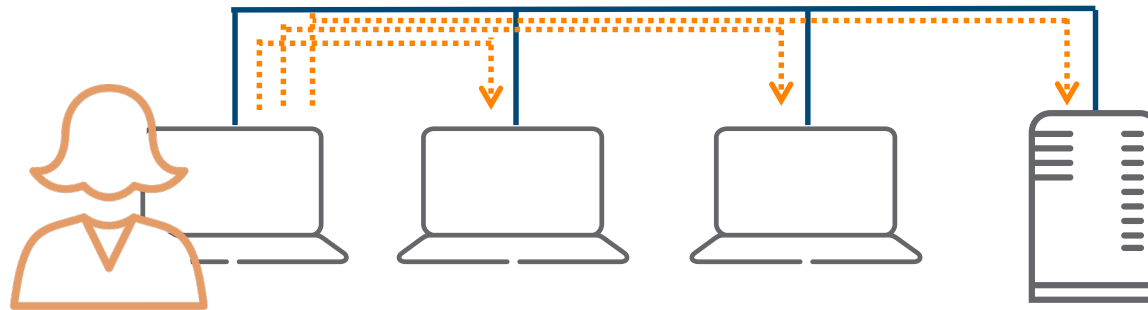


Eavesdropping



Network Reconnaissance

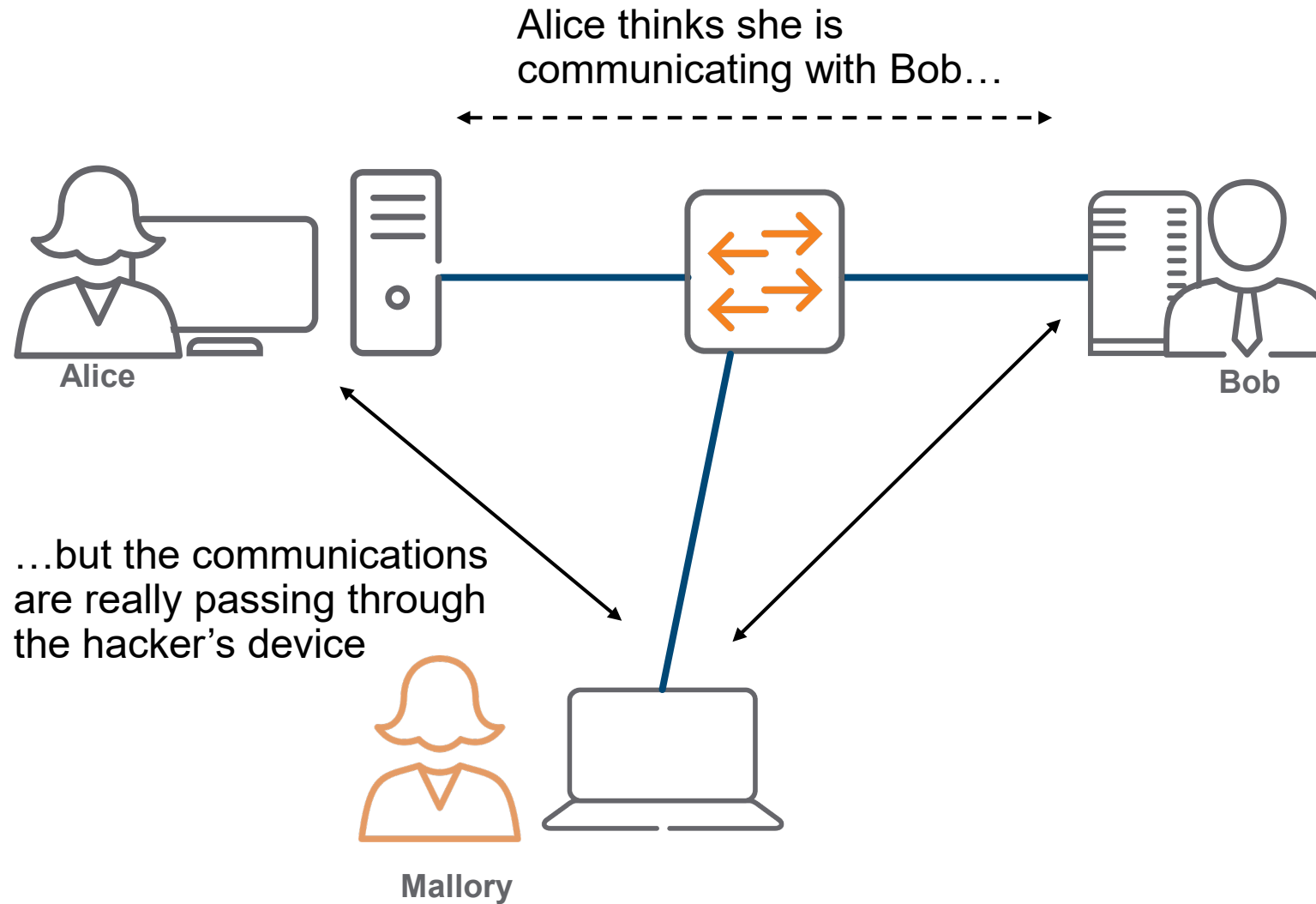
Port scanners such as Nmap



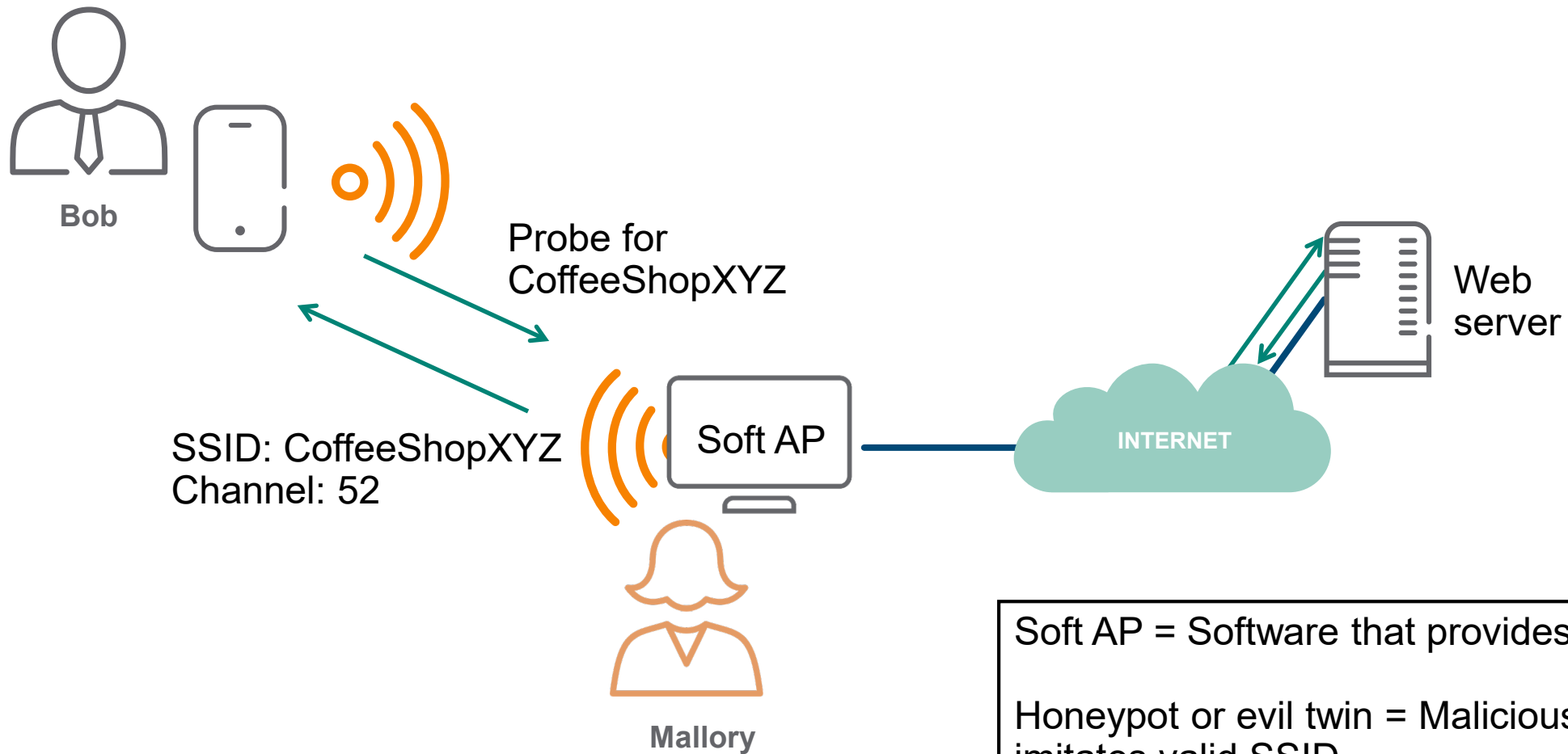
List of IP addresses
List of open TCP/UDP ports
OS on each device
Potential vulnerabilities ->

Exploits to try and where to try them

Man-in-the-Middle (MITM) Attack



Some Methods for Launching MITM Attacks



Soft AP = Software that provides AP functions

HoneyPot or evil twin = Malicious AP that imitates valid SSID

Address Resolution Protocol (ARP) and ARP Vulnerabilities

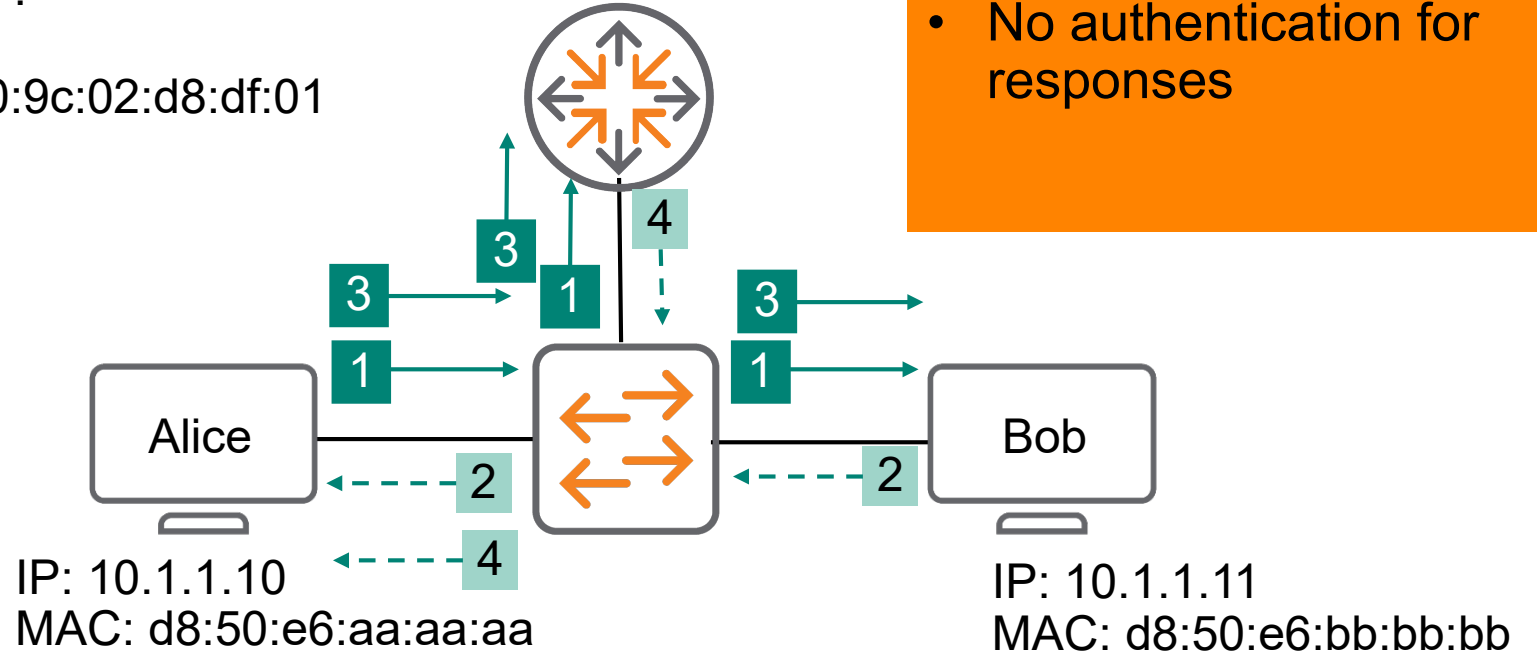
- 1 ARP request—Who has 10.1.1.11?
- 2 ARP response—10.1.1.11 is at d8:50:e6:bb:bb:bb IP: 10.1.1.1
MAC:00:9c:02:d8:df:01
- 3 ARP request—Who has 10.1.1.1?
- 4 ARP response—10.1.1.1 is at 00:9c:02:d8:df:01

Vulnerabilities

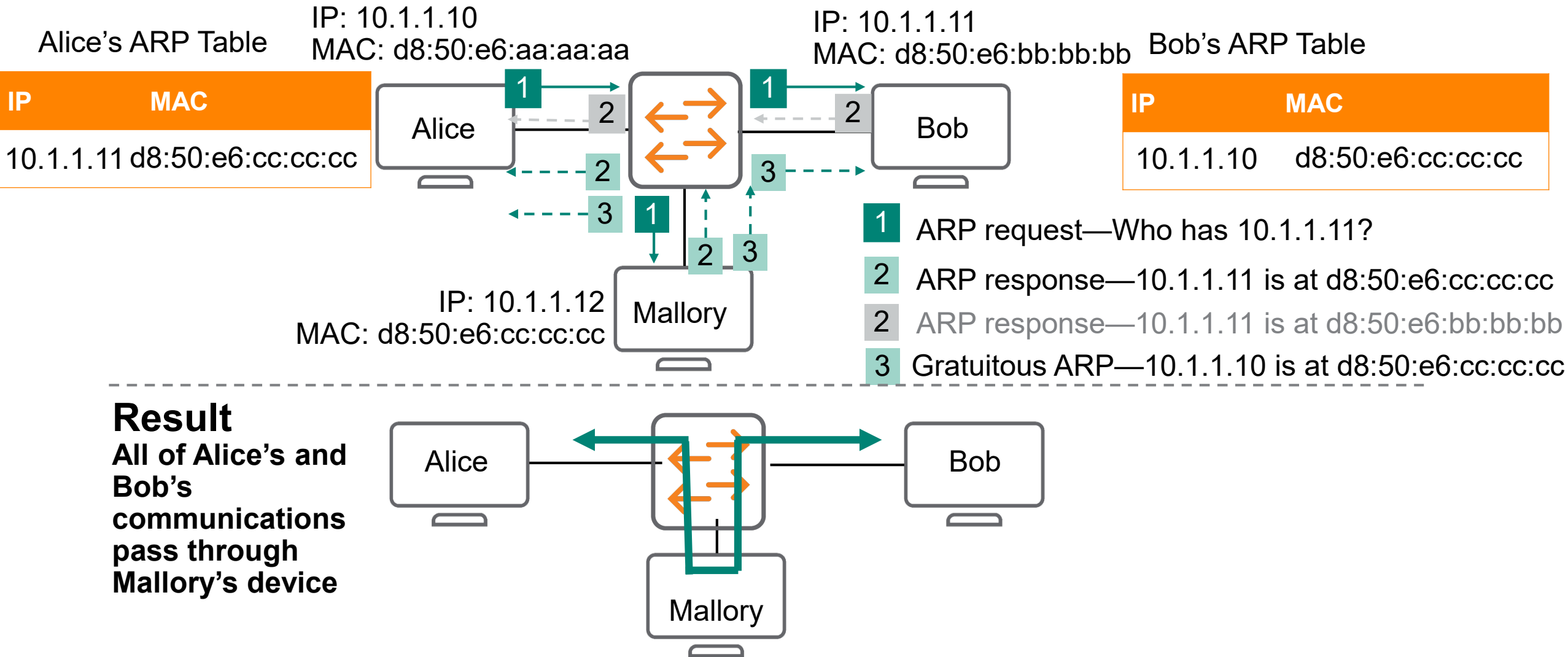
- Requests broadcast everywhere
- No authentication for responses

Alice's ARP table

IP	MAC
10.1.1.1	00:9c:02:d8:d:01
10.1.1.11	d8:50:e6:bb:bb:bb



Using ARP Poisoning to Implement an MITM Attack



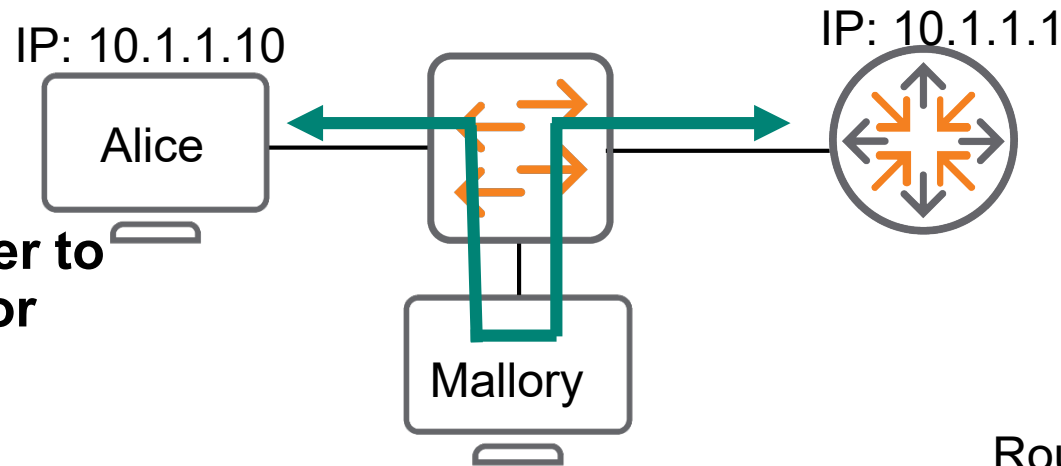
Using ARP Poisoning to Implement an MITM Attack (Cont.)

Often implemented against default router to intercept all of one or more users' traffic

Alice's ARP Table

IP	MAC
10.1.1.1	d8:50:e6:cc:cc:cc

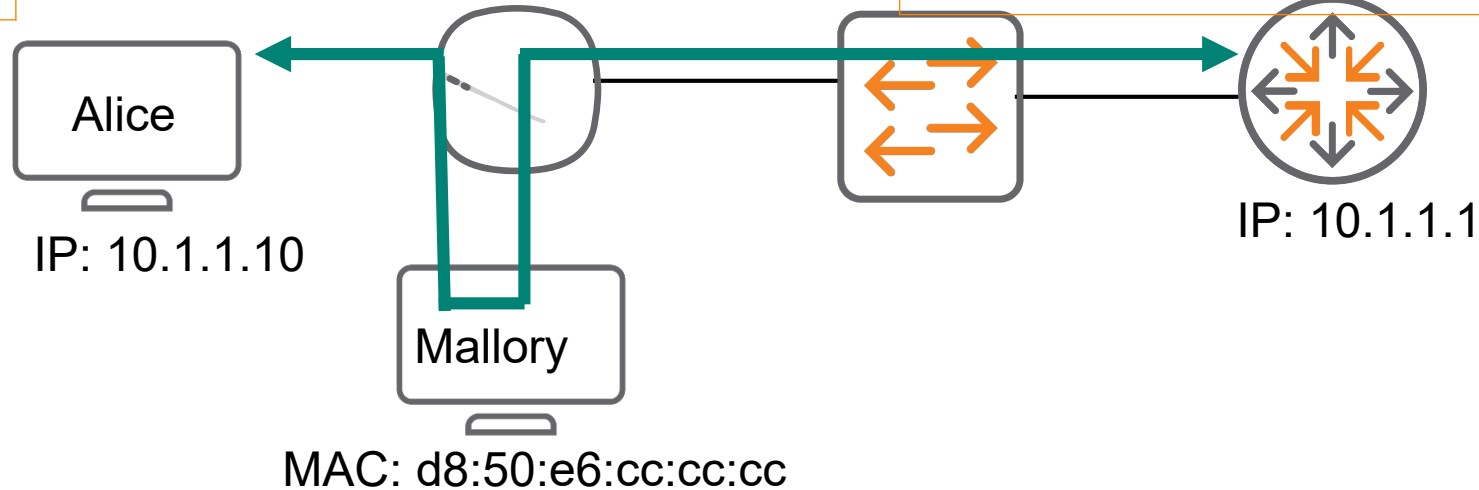
Used in wired and wireless environments



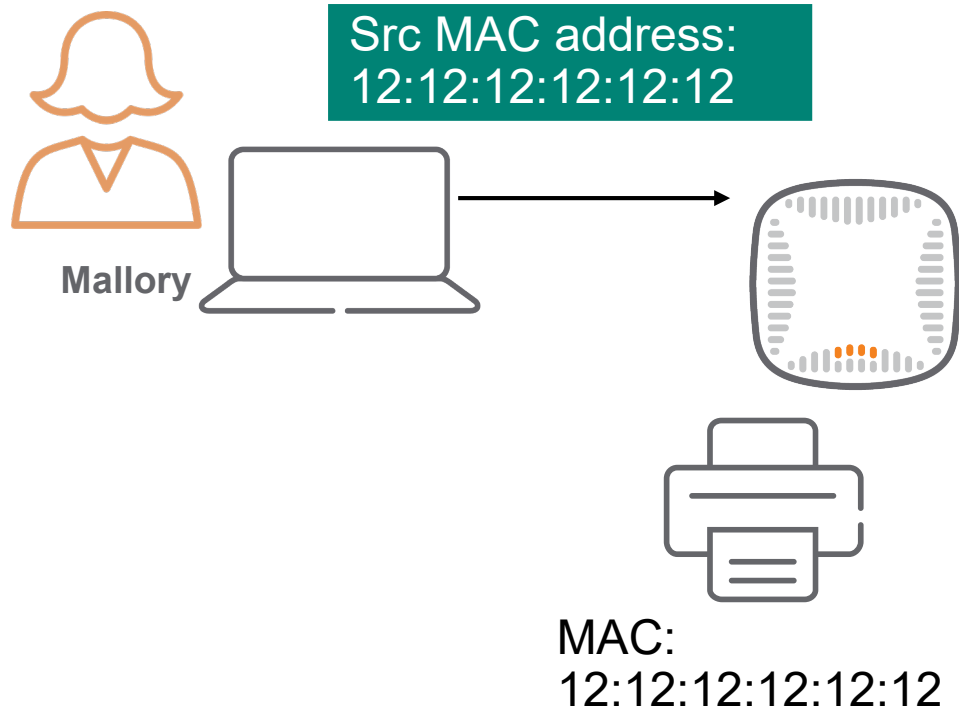
MAC: d8:50:e6:cc:cc:cc

Router's ARP Table

IP	MAC
10.1.1.10	d8:50:e6:cc:cc:cc



MAC and IP Spoofing



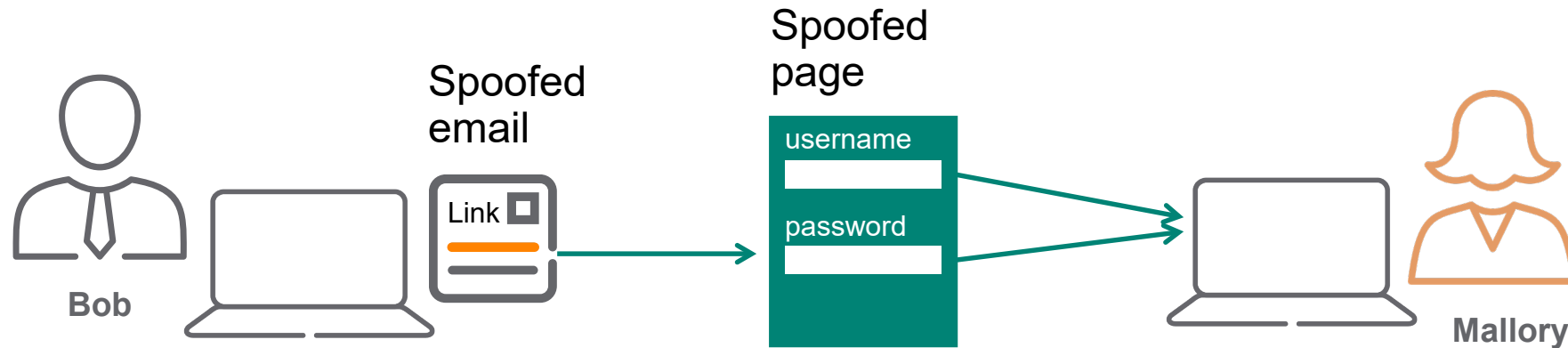
Spoofing a MAC is trivial

Changing addresses to pose as another device for purposes such as:

- Hiding the source of an attack with MAC or IP spoofing
- Gaining unauthorized access with MAC spoofing
- Launching an MITM attack
- Launching a DoS attack by posing as gateway

Email Spoofing and Phishing

phishing = Sending a spoofed email, typically with a malicious link for collecting sensitive information
spear phishing = Phishing that is targeted to a specific user, often using social networking info



32% of breaches in 2019 involved phishing¹

¹ "2019 Data Breach Investigations Report," Verizon

Social Engineering

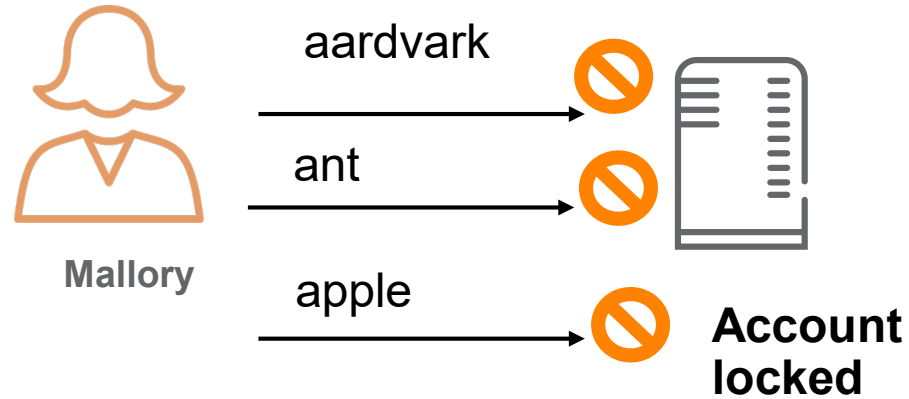


- Using human behavior to get around security measures
- Example: Posing as an IT staff member and asking for an employee's password

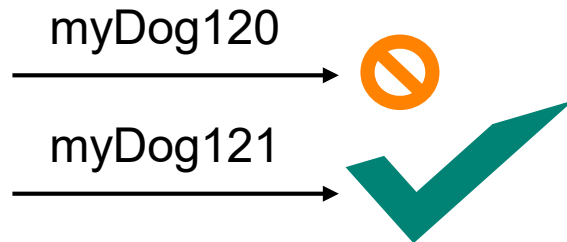
- Teach employees best practices
 - Do not share password with anyone
 - Be wary of unsolicited emails with links or requests for sensitive information
 - Hover over the link to see where it actually goes
 - Instead of clicking on links, navigate to the site yourself
 - Do **not** click past security warnings
 - Call supposed sender and verify the source was not spoofed

Additional Attacks Against Passwords

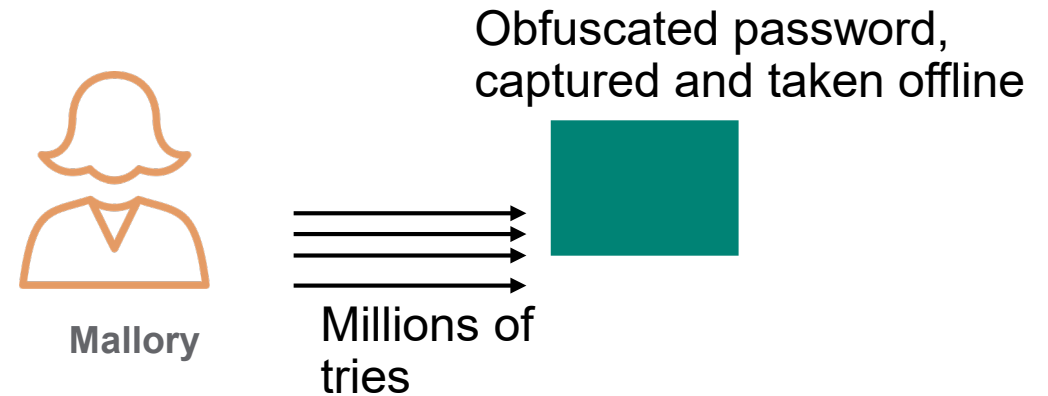
Online dictionary attack = Less effective



Unless the hacker has info from another data breach



Offline dictionary/brute force attack = More effective



Dictionary attack = Try all dictionary words
Brute force attack = Try all possible character combinations; takes longer than dictionary attack and can be infeasible for long enough password (more than 8 characters)

What Makes a Good Password

1

Never repeated and no simple variations (i.e. incrementing number)

2

8 or more characters (NIST), but preferably much longer

3

Random characters preferred, but if not feasible, 4 or more words

4

Mix of different character types (less important than length)

Password management solutions

- Advantages
 - No repeated passwords
 - Stronger passwords
 - Ease of use
- Disadvantages
 - Must trust the solution

Best can be avoiding passwords and using credentials like digital certificates (discussed in next module)

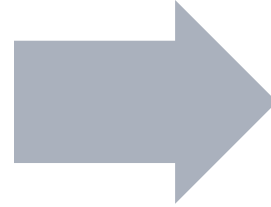
Lab Activity 1

Bad emails?

Tasks

1 – Analyze Emails

- Look at several emails
- Flag potential phishing attempts and explain your reasoning



2 – Create a Plan to Educate Users

- Prepare a presentation to explain ways that employees can minimize their exposure to common threats

See Lab Guide for instructions

Review tasks

Complete lab(s)

Complete debrief

Email 1

From: **Order Confirmation** <nooreply@o64.onechanges.com>

Date: Sat, May 30, 2020 at 6:33 PM

Subject: Ian, Please Confirm Your \$10 Paypal Gift Card

To: <ian.mcgregor@organizationabc.com>



RECEIVE A PAYPAL GIFT CARD

**Tell us what you like about Paypal,
and get a \$10 Gift Card!**

Thank you for your feedback.

Claim Now

The advertiser does not manage your subscription.
If you prefer not to receive further communication please unsubscribe [here](#)
Or write to: 11310 E 21st St N ,#518, Wichita, KS, 67206

Email 2

From: **Drivefact** <zxisibnqyzbzmz@mgheda.drivefact.org>

Date: Thu, May 21, 2020 at 8:35 PM

Subject: Client #9809790 To STOP Receiving These Emails From Us Hit reply And Let Us Know.

To: <ian.mcgregor@organizationabc.com>

Please confirm you Unsubscribe

To confirm your Unsubscribe, please [click here](#) or on the link below.



Thank you!

Email 3

From: **BGXYZ BANK** <nooreply@byxz.com>
Date: Tue, May 26, 2020 at 4:04 PM
Subject: Urgent Request
To: <ian.mcgregor@organizationabc.com>



Dear Valued Customer,

We believe your account may have been compromised. Please click the link below to change your password to prevent any unauthorized individuals from accessing your account.

Click here

Thank you for your quick action.
BGXYZ BANK



©2020 BGXYZ BANK

Debrief

1 – Analyze Emails

- Look at several emails
- Flag potential phishing attempts and explain your reasoning

- Which emails were phishing attempts?
- What signs did you see?
- How can you protect yourself against such attempts?

2 – Create a Plan to Educate Users

- Prepare a presentation to explain ways that employees can minimize their exposure to common threats

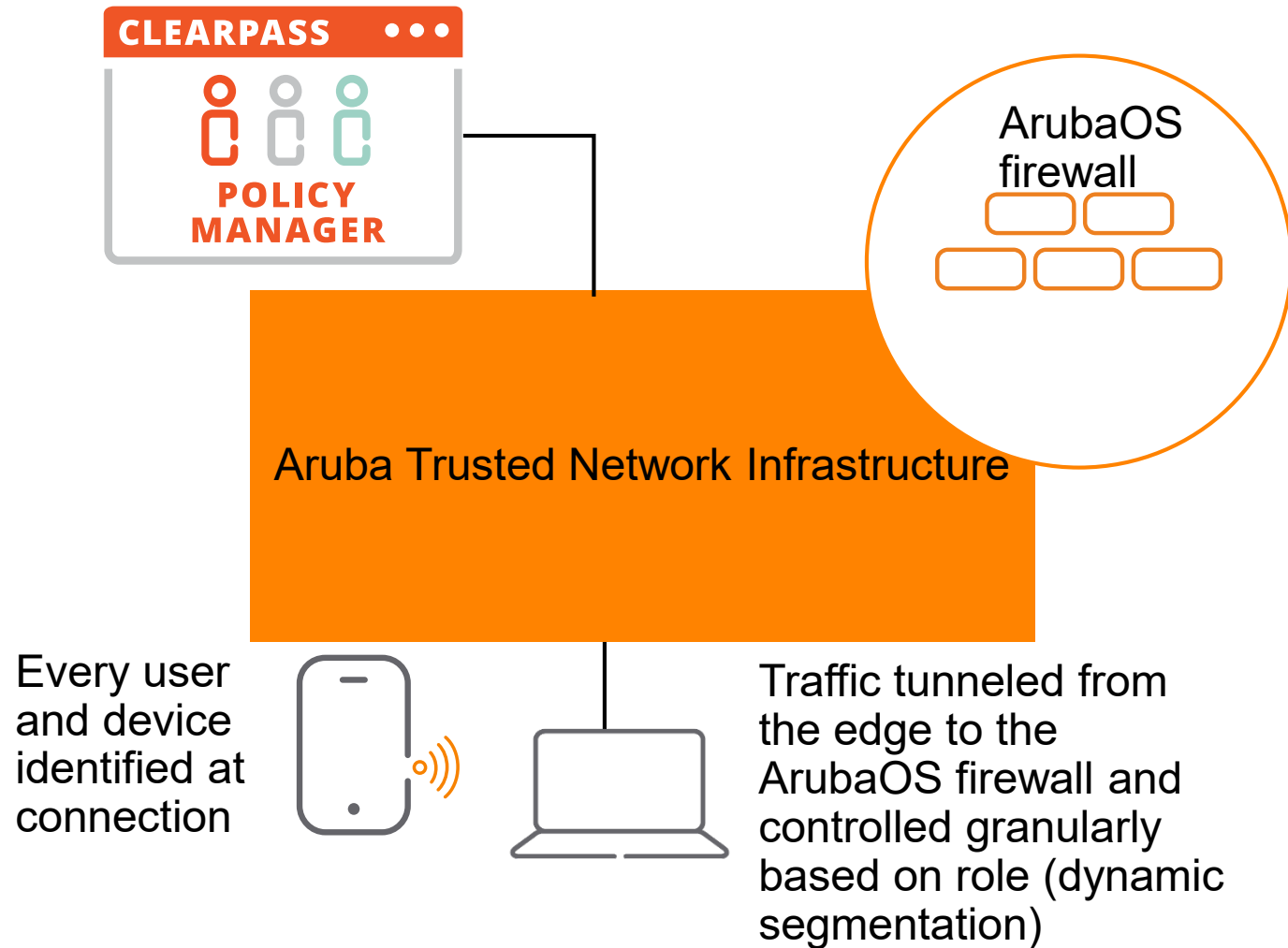
Review tasks

Complete lab(s)

Complete debrief

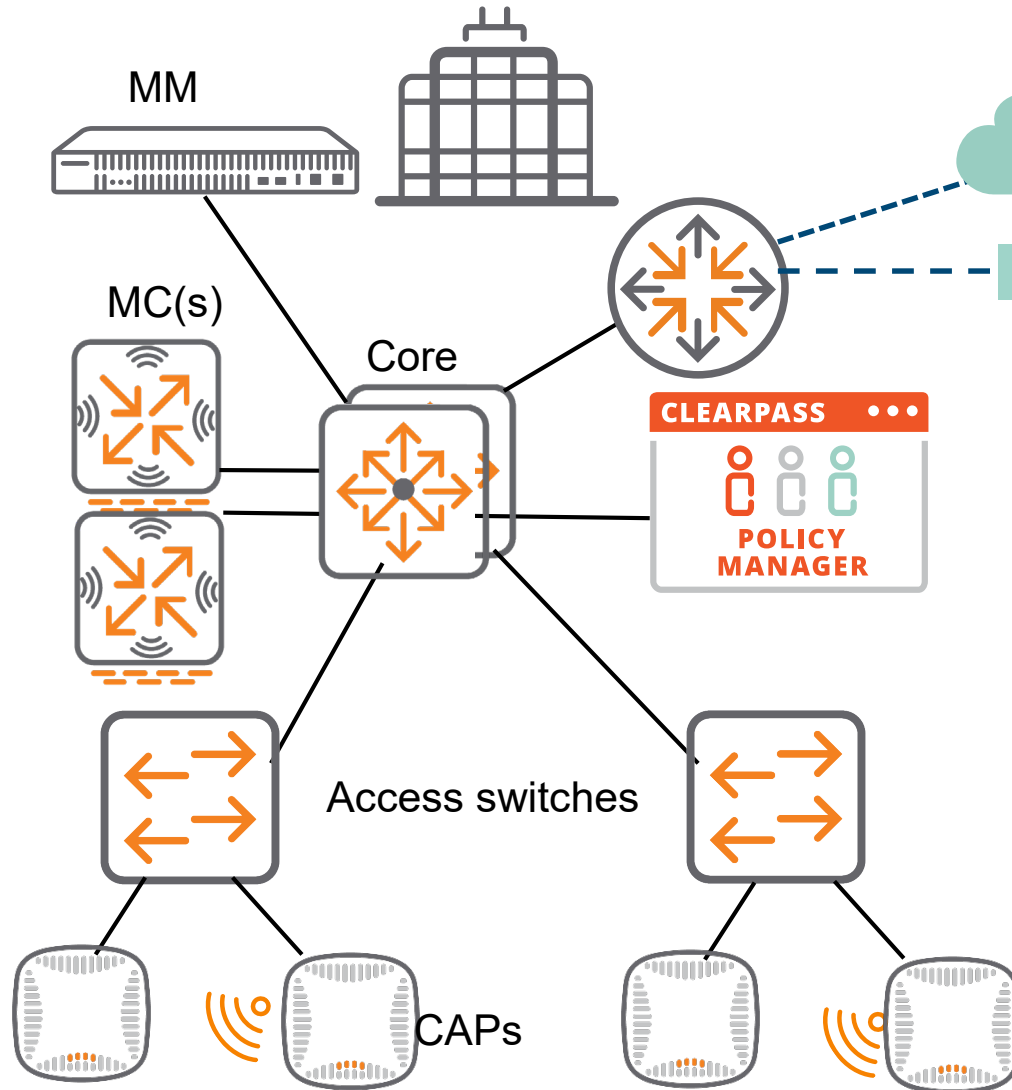
Aruba Security Strategy

Enforce Micro-Segmentation with Aruba ClearPass, ArubaOS Firewall, and Dynamic Segmentation

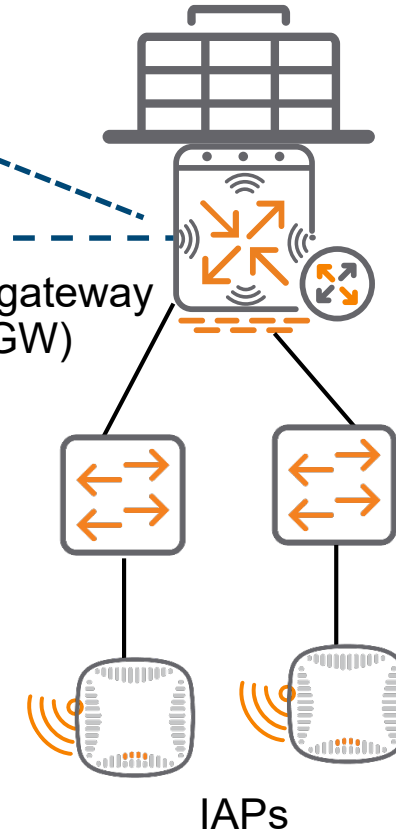


Implement Same Security Everywhere

Main campus/data center



Branches



Aruba security:

- Trusted network infrastructure
- Role-based access control and micro-segmentation
- Logging and inspection
- Continuous monitoring and enforcement

Aruba SD-Branch:

- Same security capabilities
- LAN, WLAN, SD-WAN, and security integrated under a single framework

Rev 20.31

aruba

a Hewlett Packard
Enterprise company

Security Technologies

Aruba Network Security Fundamentals



Regulatory Compliance

aruba

a Hewlett Packard
Enterprise company

Regulatory Requirements

Good security practices can protect the company from:

- Legal fines
- Damaged reputation
- Lost revenue
- Downtime

Region	Data protection regulations
US	Privacy Act Safe Harbor Act Health Insurance Portability and Accountability Act (HIPAA) Health Information Technology for Economic and Clinical Health (HITECH) Act Federal Information Processing Standards (FIPS) 140-2 (140-3 is emerging)
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)
European Union (EU)	General Data Protection Regulation (GDPR)
Japan	Act on the Protection of Personal Information (APPI)
Multiple regions	Payment Card Industry (PCI) Data Security Standard (DSS) 3.2

Applies to all companies that process, store, or manage data about EU citizens



Understand Your Company's Policies



Work with legal and security teams to understand your responsibilities

Implement security best practices AND prove it

- Documentation trails for audits



a Hewlett Packard
Enterprise company

Hardening Switches

Aruba Network Security Fundamentals

Rev 20.21



EDUCATION
SERVICES



Why Harden Devices?



Protect against attacks such as:

- DoS
- MITM
- Eavesdropping
- Reconnaissance

Comply with regulations

Best Practices Checklist

Set up out-of-band management network

Authenticate managers securely

Enable secure protocols and disable insecure ones

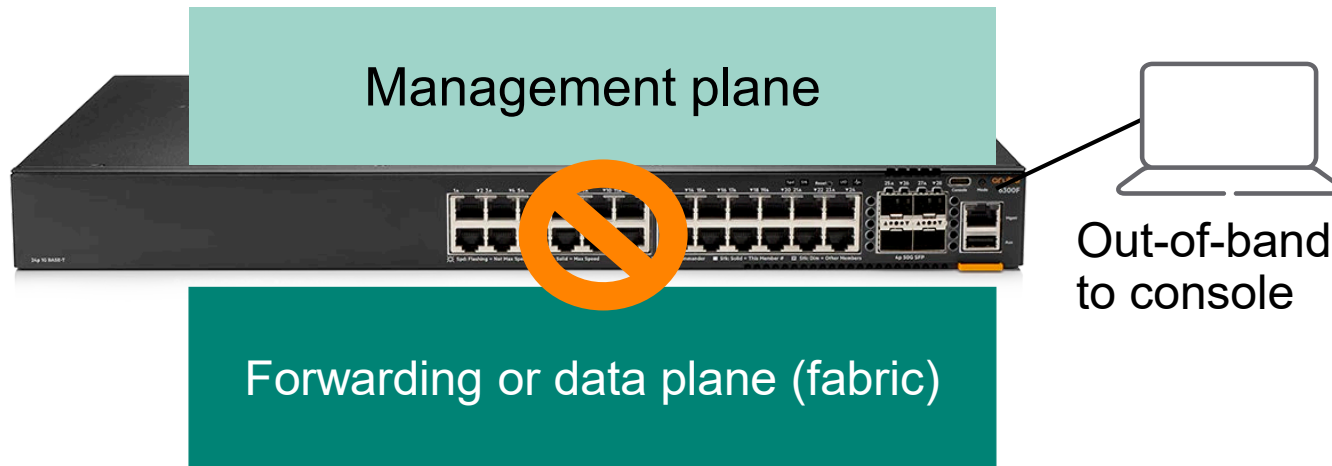
Ensure physical security and implement other security measures such as Control Plane Policing (CPP)

Download Aruba
Hardening Guides

<https://asp.arubanetworks.com/downloads>

Set Up Out-of-Band Management

Out-of-Band Management to a Console Port



Connection	Protocol	Interface
console	serial	CLI (or Menu)

Advantages:

- Complete separation of management and data planes
- Very difficult to lock yourself out

Disadvantages:

- Less flexibility
- Remote access possible, but can be complex to establish

Ethernet Out-of-Band Management

Select which protocols are enabled on which side

ArubaOS-Switch = Listen on OOBM, data, or both

ArubaOS-CX = Enable on a VRF

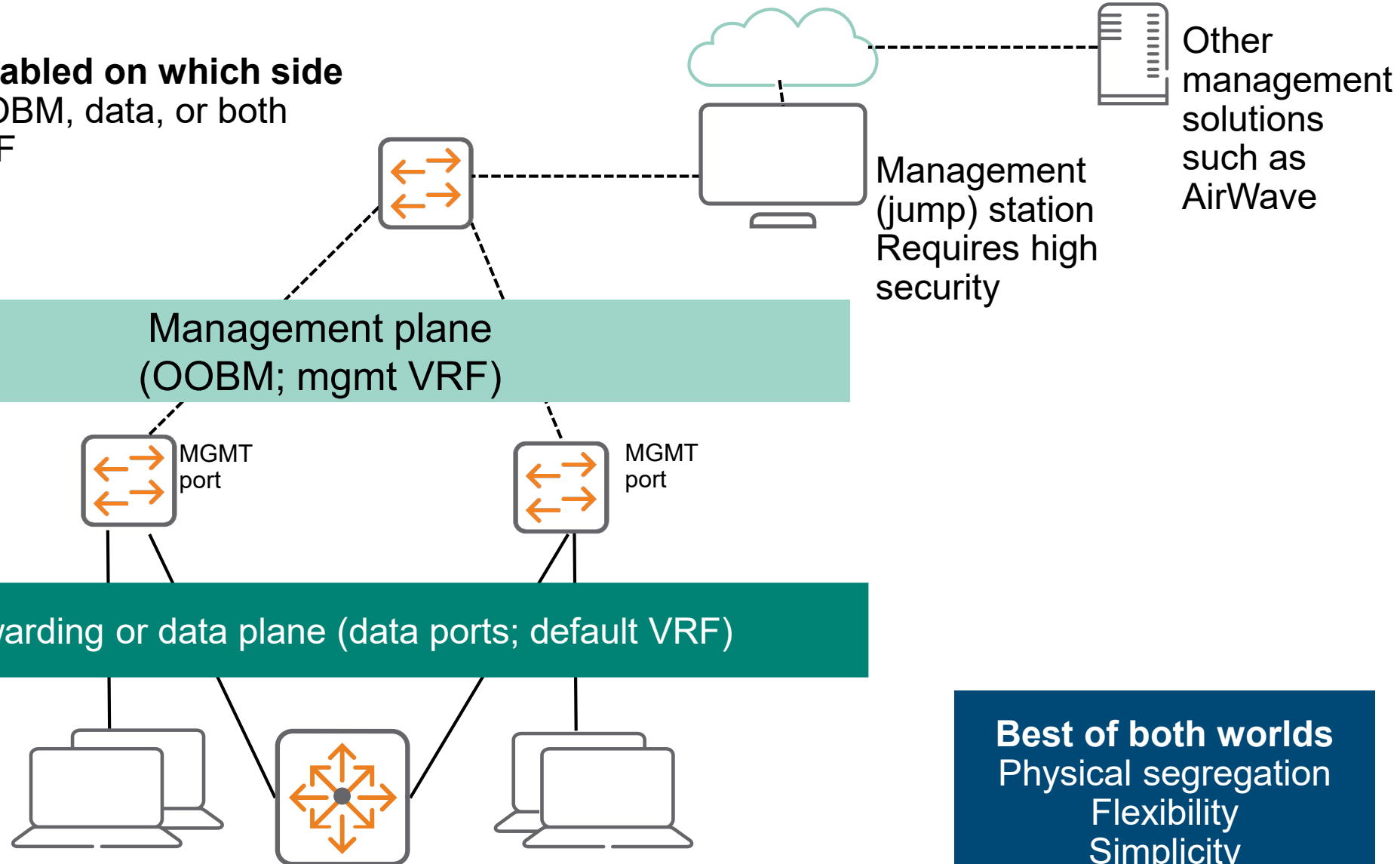
Examples

SSH
SNMP
HTTPS

Management plane
(OOBM; mgmt VRF)

RADIUS
HTTPS

Forwarding or data plane (data ports; default VRF)



Best of both worlds
Physical segregation
Flexibility
Simplicity

Authenticate Managers Securely

Manager Roles

ArubaOS-Switch

– Operators:

- Limited show commands
- Can view statistics and some config information

– Managers:

- Complete read-write access
- Can view all information and change configurations



ArubaOS-CX

– Operators:

- No config privileges
- Display-only CLI access

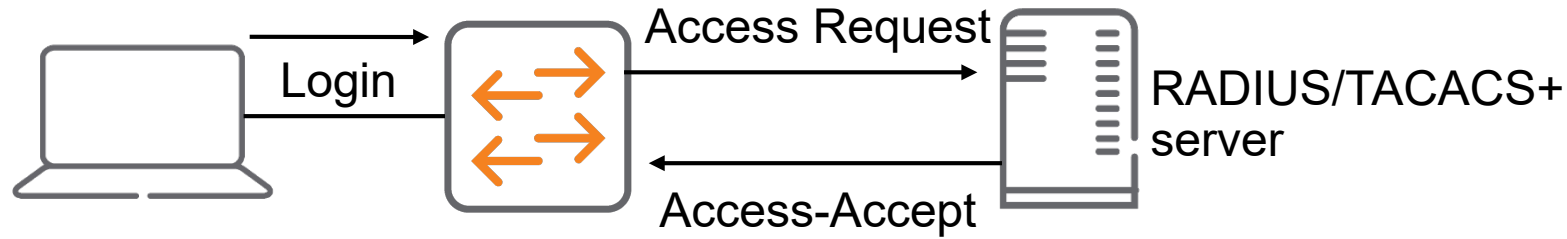
– Administrators:

- Full CLI access
- Can add/remove user accounts

– Auditors:

- CLI commands in the auditor context
- Through Web UI can access only
 - System > Log page

Setting up External Authentication for Management Access



Overview

1. Specify one or more external servers and optionally place them in different groups
2. Specify RADIUS or TACACS authentication for specific access types
3. Communicate with the external server admin to set the correct AVPs or VSAs for placing users in the correct groups

Specifying External Access Methods

<code>aaa authentication</code>	access level	access type	1 st auth method	2 nd auth method*
Options: (can mix and match)	login, enable	telnet, console, ssh, web, rest	none, local, radius [server- group <name>] tacacs	authorized, none, local

Example:

```
aaa authentication login ssh tacacs local
aaa authentication enable ssh tacacs local
```

aaa authentication login		access type	1 st auth method	2 nd auth method*	n auth method*
Options (can mix and match)	login, enable	console, ssh, https-server, default	local, group <name>	local, group <name>	local, group <name>

Example:

```
aaa authentication login ssh group tacacs local
```

*Use 1st auth method unless all requests to all servers in group timeout, then proceed to 2nd
For AOS-CX, then proceed to 3rd, and so on

Use Secure Protocols

Use Secure Protocols

Access type	Insecure Do not use	Secure Recommended use
CLI	Telnet ArubaOS-Switch: Enabled by default ArubaOS-CX: Not supported	SSH ArubaOS-Switch: Enabled by default ArubaOS-CX: Enabled by default on VRFs mgmt and default
File transfer through terminal	TFTP ArubaOS-Switch: Enabled by default ArubaOS-CX: Not supported	SFTP ArubaOS-Switch: Enabled ArubaOS-CX: Enabled
Web	HTTP ArubaOS-Switch: Enabled by default ArubaOS-CX: Not supported	HTTPS ArubaOS-Switch: Disabled by default (requires certificate) ArubaOS-CX: Enabled by default on VRFs mgmt and default (self-signed cert)
SNMP	SNMPv1/v2c ArubaOS-Switch: Enabled by default; public community = manager ArubaOS-CX: Not enabled on any VRFs by default; public community = read-only	SNMPv3 ArubaOS-Switch: Disabled by default ArubaOS-CX: Not enabled on any VRFs; no SNMPv3 users by default

Disable SNMPv1/v2

–ArubaOS-Switch:

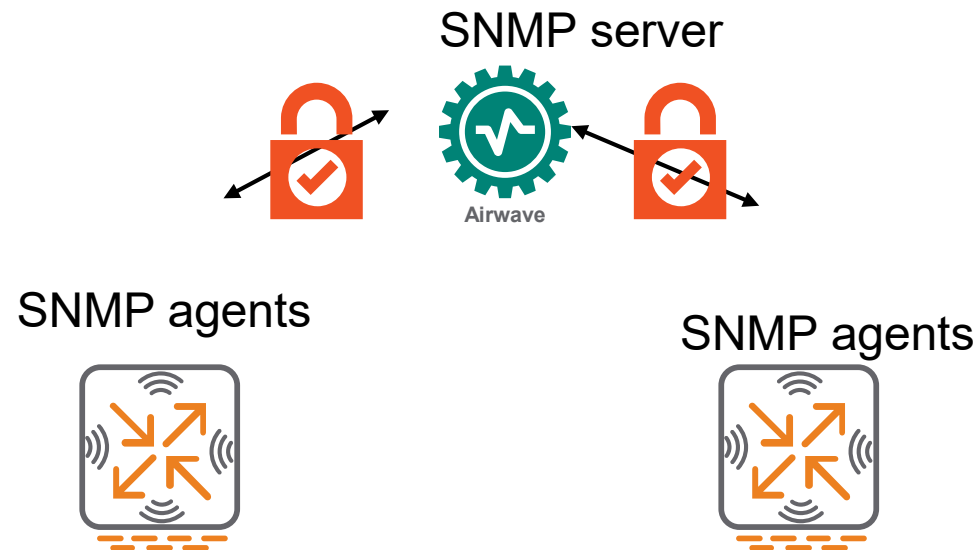
- Remove “public” community
- Disable SNMP-server to disable SNMPv1/v2c entirely

–ArubaOS-CX:

- Remove “public” community and any other configured communities

Security vulnerabilities of SNMPv1/v2c

- Plaintext passwords
- Susceptibility to eavesdropping
- Susceptibility to unauthorized reading and writing to switch settings

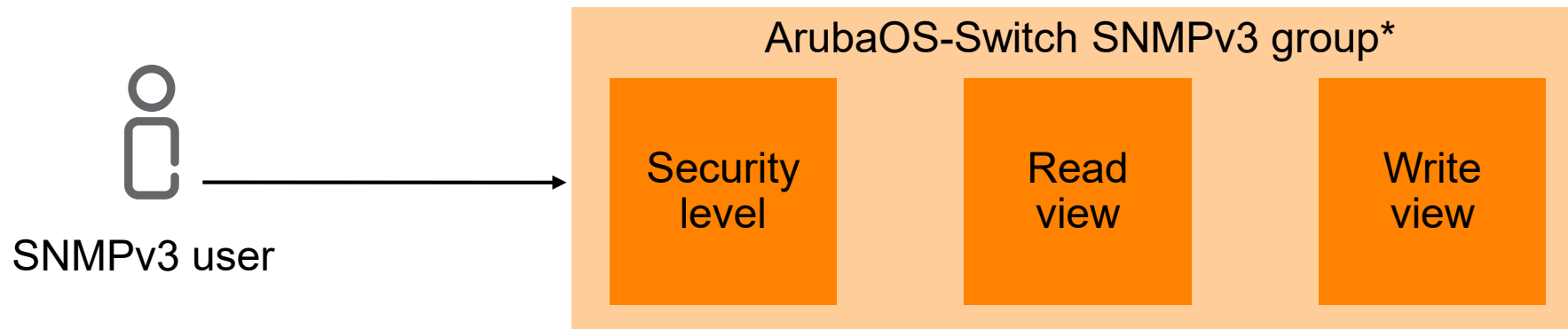


Set Up SNMPv3

- ArubaOS-Switch: Enable SNMPv3
 - Delete initial user
- Create SNMPv3 users with secure algorithms and long passwords
 - Auth = SHA
 - Priv = AES
- ArubaOS-Switch: Assign the user to a group
- ArubaOS-CX: Enable SNMP on a VRF

Create matching SNMPv3 users on the server (such as AirWave) and Aruba switches:

- Username
- Authentication protocol (SHA)
- Authentication password
- Privacy protocol (AES)
- Privacy password



*Typical groups for ArubaOS-Switch:

- managerpriv
- operatorauth

ArubaOS-CX security level set globally

Ensure Physical Security and Other Measures

Ensure Physical Security

–Physical security recommendations:

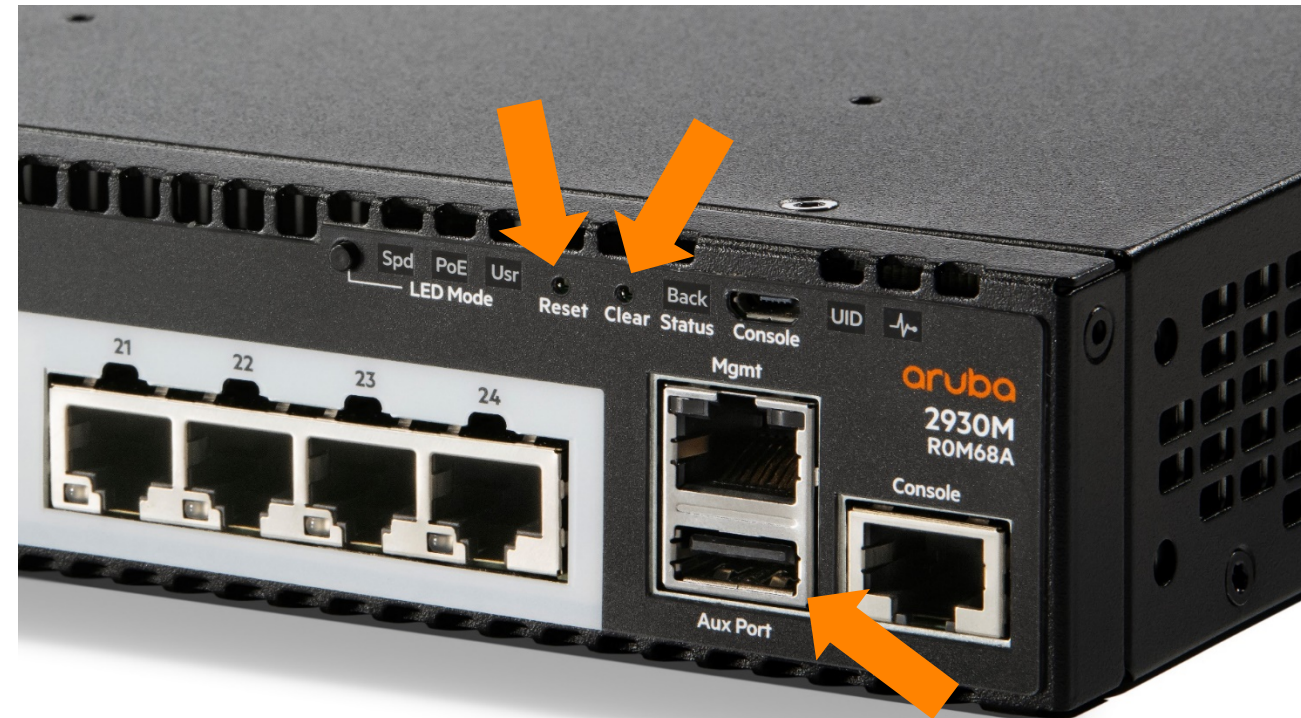
- Locked closets
- Possibly biometrics (data center)
- Disable unused ports (or ensure authentication enabled on them)

–Recommendations when physical security is impossible:

- Disable clear and reset buttons

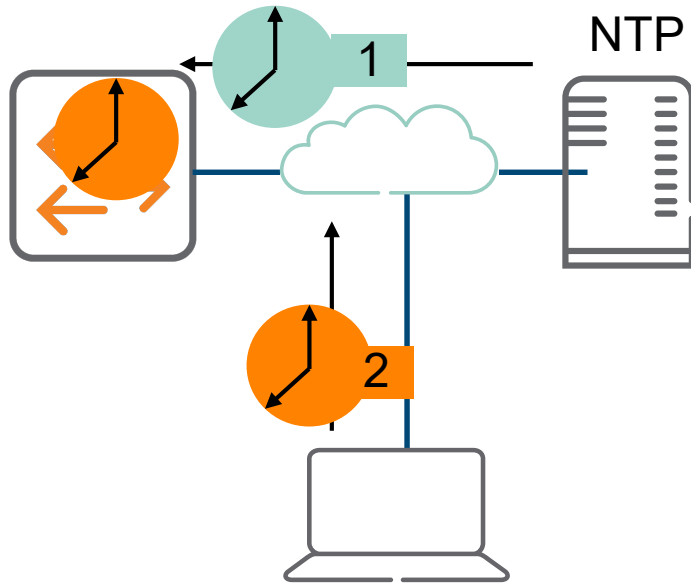
Hacker with physical access can clear the config (Reset) or password (Clear):

- Launch DoS
- Gain unauthorized access

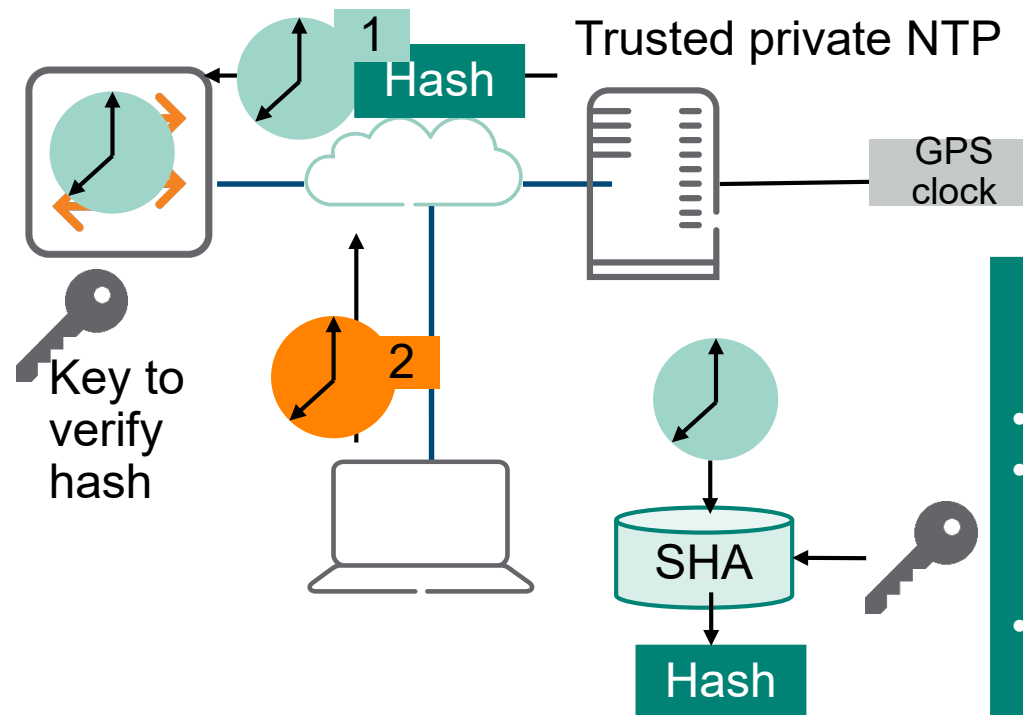


Authenticated Network Time Protocol (NTP)

Without authentication—Hacker can tamper with time




With authentication—Only valid time accepted




Why care?

- Prevent replay attacks
- Ensure technologies like RADIUS and certificates work
- Ensure log accuracy for forensics and audits

Take Additional Hardening Actions

- Set non-zero idle session timeout
- Configure a banner
 - Exec = post-login
 - Login = 
 - Informs you about login attempts
 - Alerts you to issues
 - Message of the day = Allows admins to alert each other
- Set lockouts
 - Protect from dictionary attacks
 - But be aware of lockout-based DoS
 - Use non-default names
 - Set reasonable lockout times (minutes)

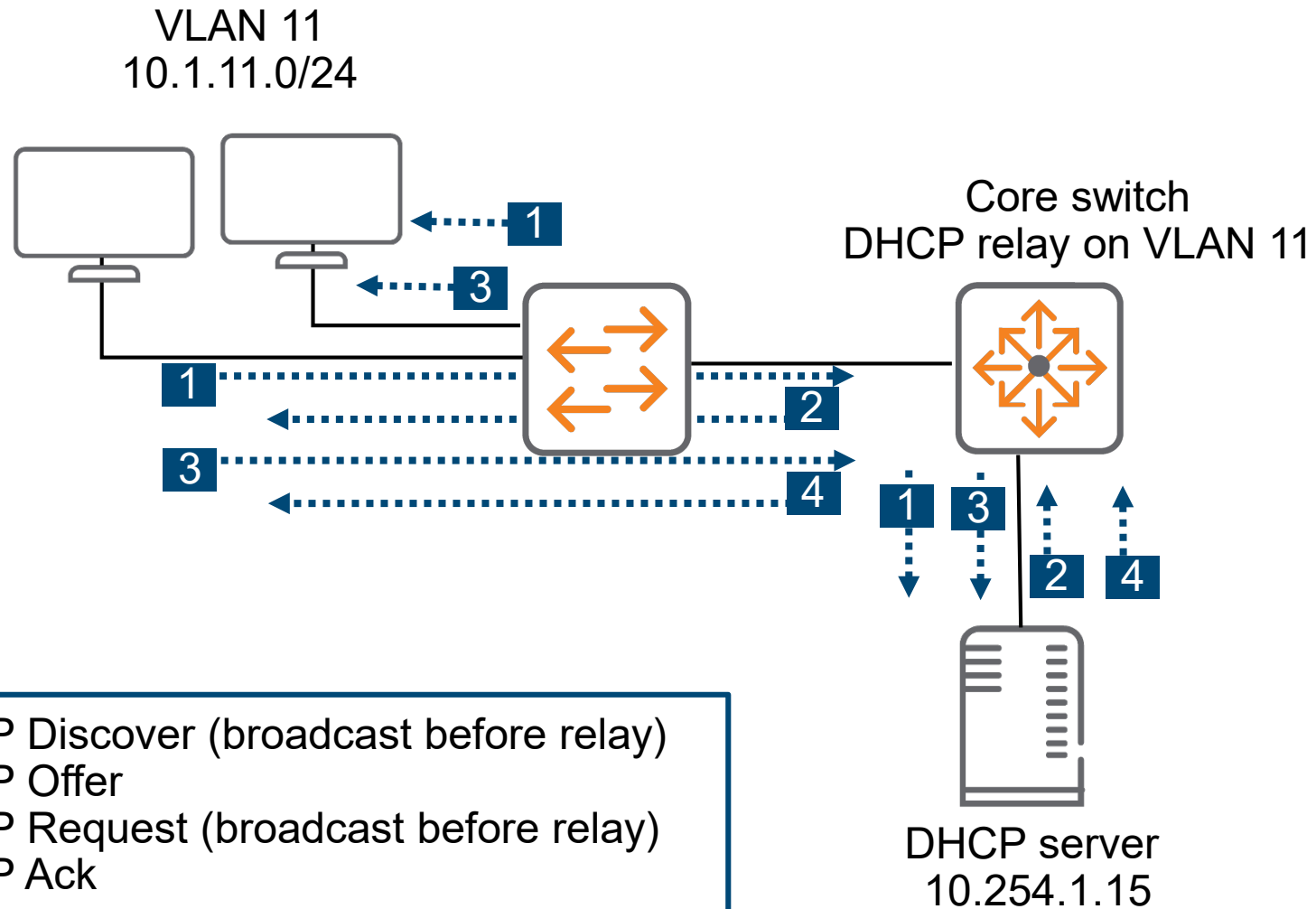


```
The device you have accessed belongs to example.com. Only authorized users are allowed to access this device.'

Your previous successful login (as manager) was on 2020-02-16 16:47:32 from the console
```


Use DHCP Snooping and ARP Protection

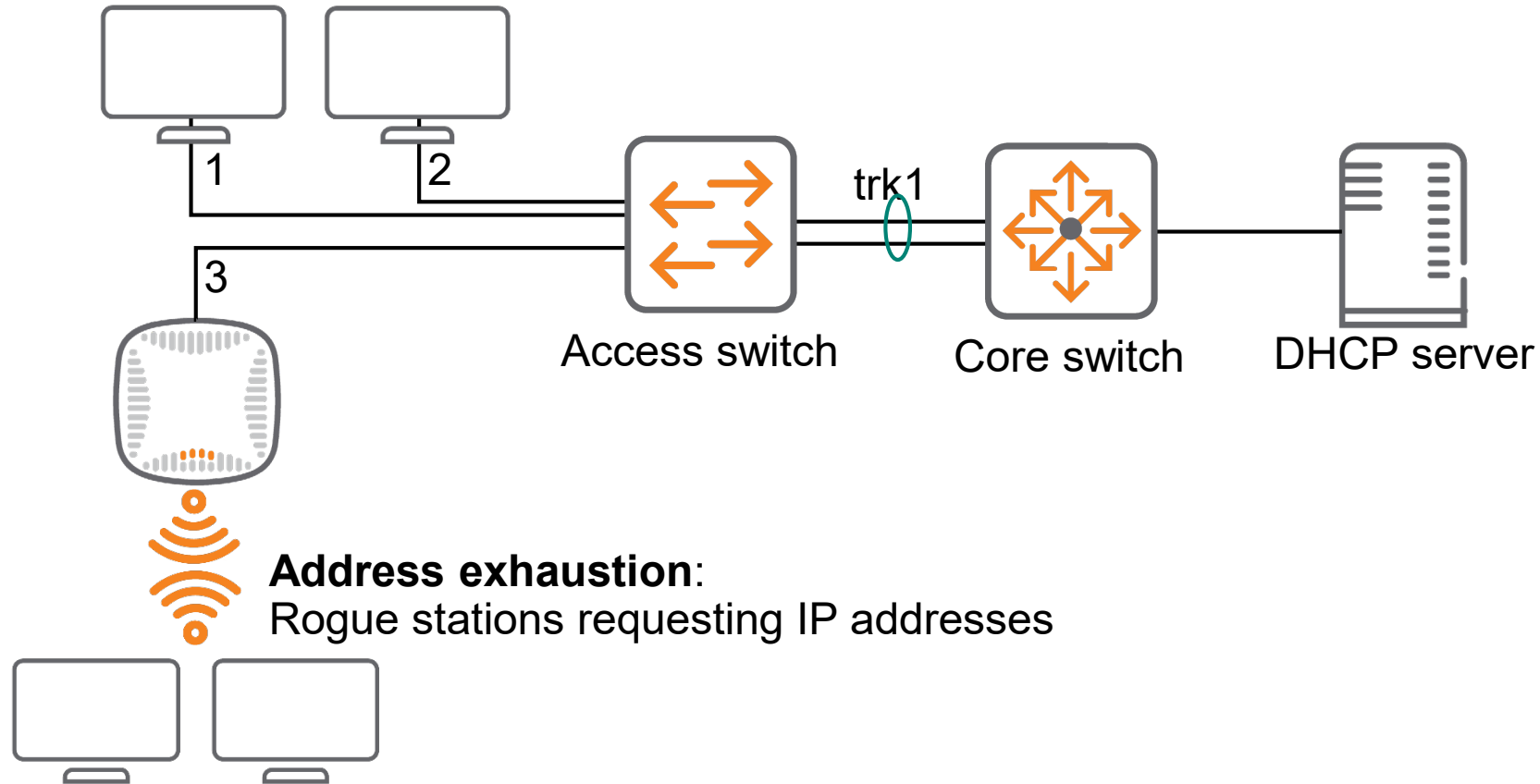
DHCP Review



DHCP Attacks

Address spoofing:

Rogue DHCP servers provide legitimate stations with invalid IP addresses or gateway addresses



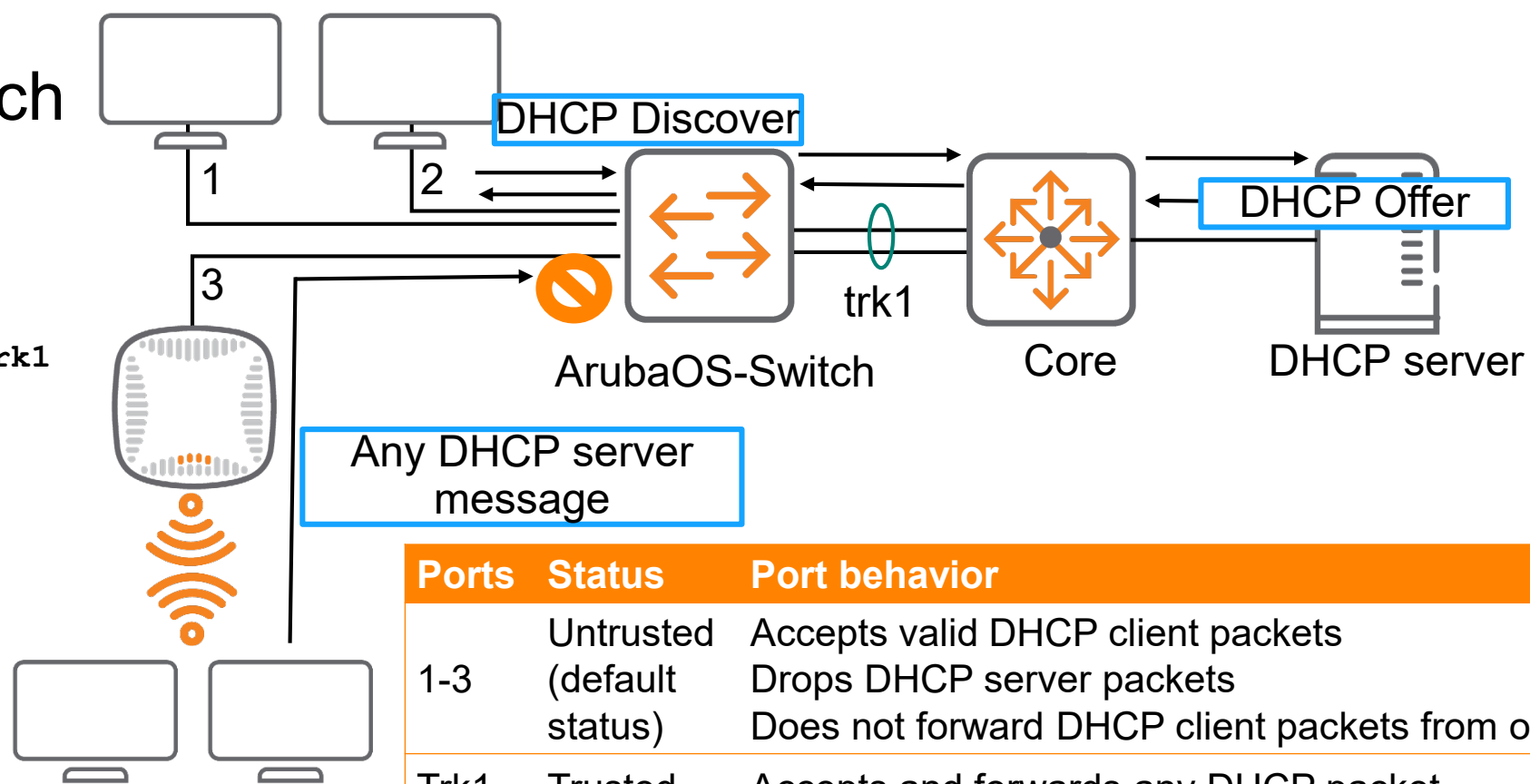
Address exhaustion:

Rogue stations requesting IP addresses

ArubaOS-Switch: Using DHCP Snooping to Protect Against DHCP Attacks

Access layer ArubaOS-Switch config

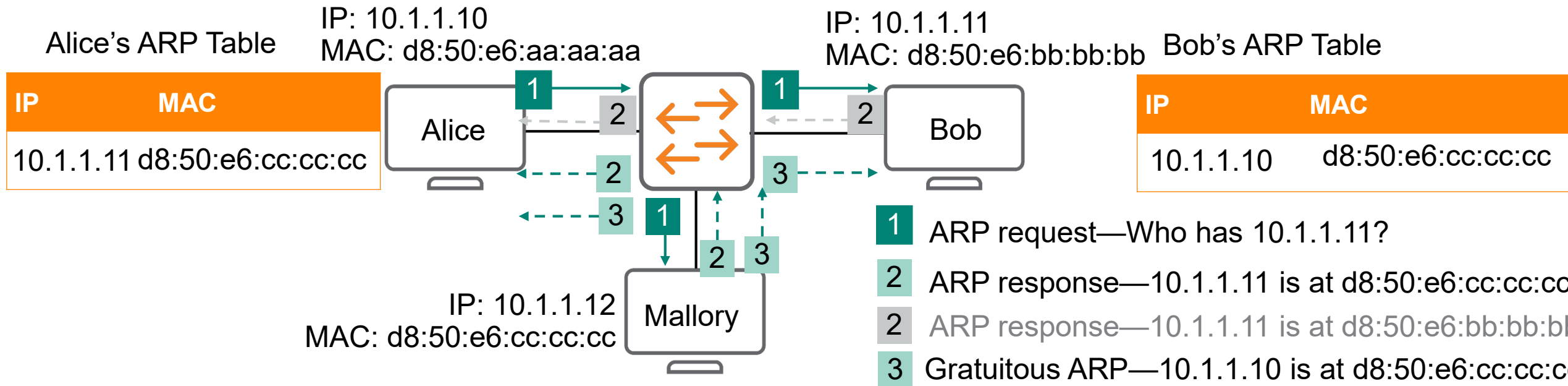
```
dhcp-snooping vlan 11
dhcp-snooping trust trk1
dhcp-snooping max-binding 1
dhcp-snooping
```



Ports	Status	Port behavior
1-3	Untrusted (default status)	Accepts valid DHCP client packets Drops DHCP server packets Does not forward DHCP client packets from other ports
Trk1	Trusted	Accepts and forwards any DHCP packet

Review ARP Snooping and Poisoning

- ARP has no security mechanisms, making it vulnerable to:
 - ARP poisoning
 - ARP snooping
 - DoS attacks

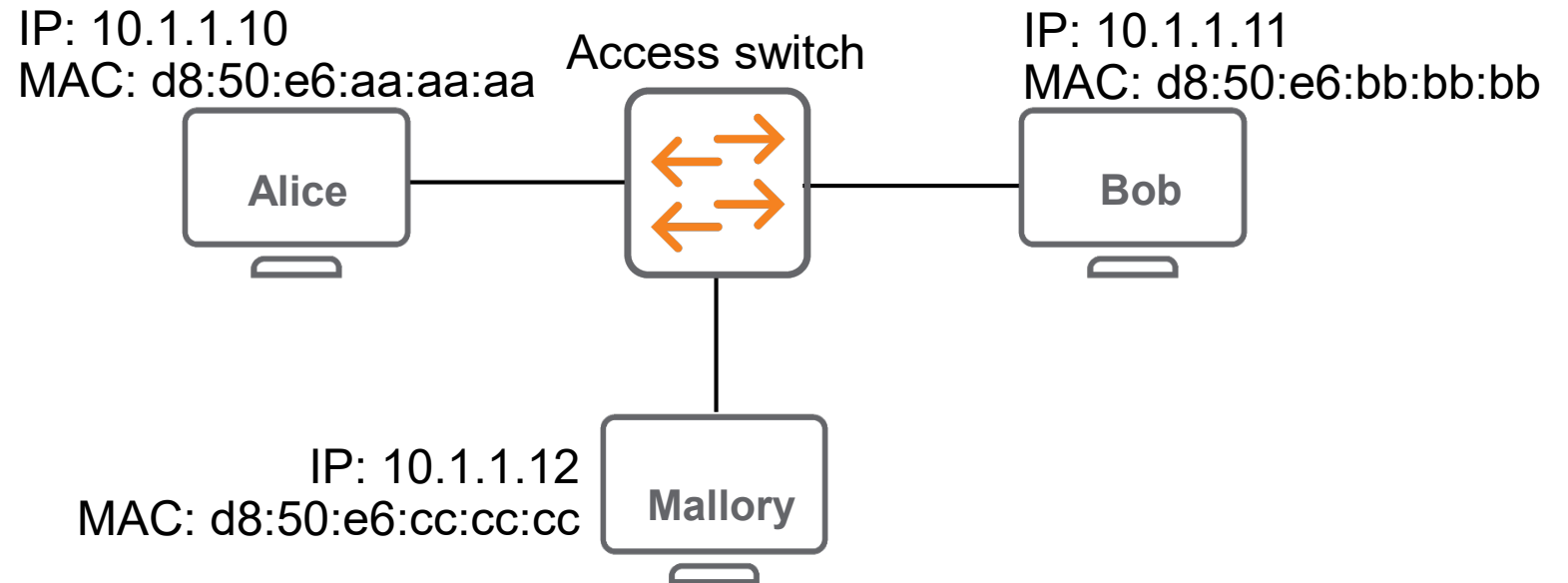


ArubaOS-Switch: ARP Protection

- Enabled globally and per-VLAN
 - Must be enabled in both places
- Switch checks ARP responses on untrusted ports in enabled VLANs*
 - Verifies that ARP responses have valid IP-to-MAC address bindings.
 - Drops ARP responses with invalid bindings
 - Implements optional validity checks

IP-to-MAC binding table

IP	MAC
10.1.10.10	d8:50:e6:aa:aa:aa
10.1.10.11	d8:50:e6:bb:bb:bb
10.1.10.12	d8:50:e6:cc:cc:cc

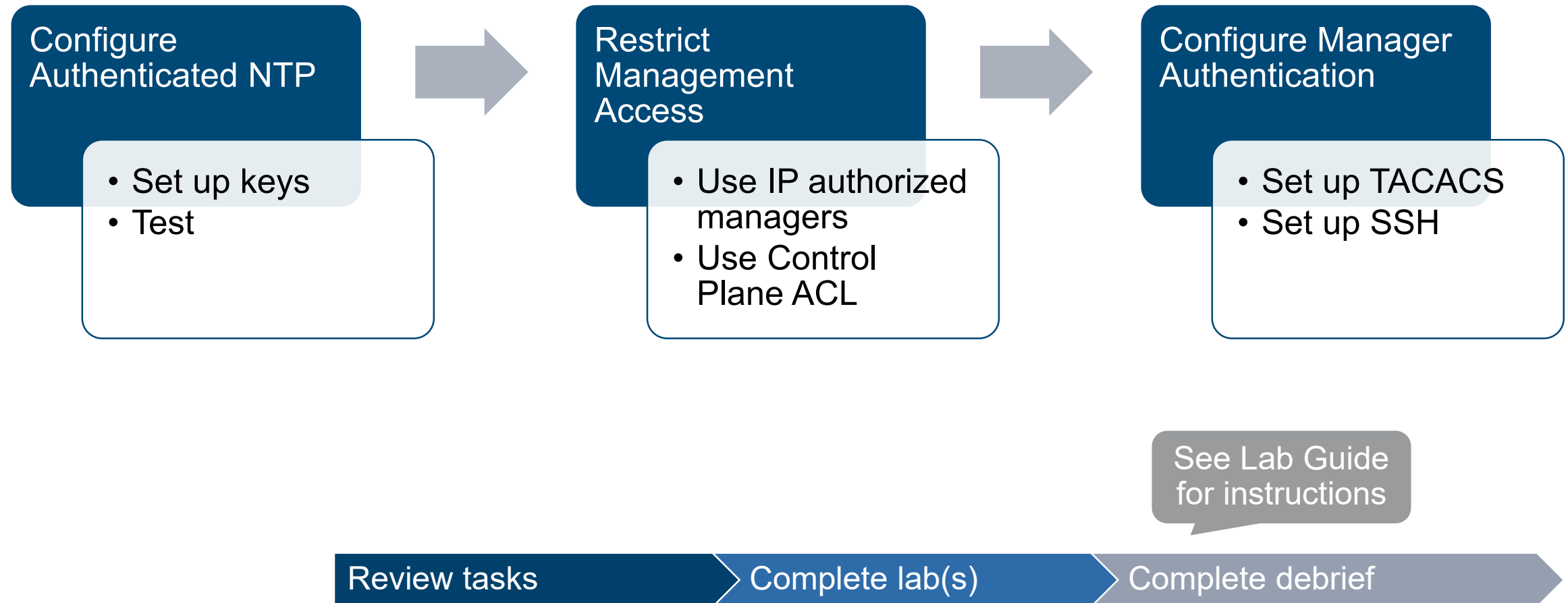


*All ports untrusted by default

Lab Activity 2

Harden Aruba Switches

Tasks



Lab Tasks (Demonstrate)

Lab: Harden Aruba Switches

Task 1: Configure Authenticated NTP	46
Task 2: Restrict Management Access to Aruba Switches	49
Task 3: Configure Manager Authentication for SSH	50

Debrief

Configure Authenticated NTP

- Set up keys
- Test

- What approaches did you take to ensure SSH management clients could authenticate the switches?
- Which device determined the manager's role when you logged into the switches over SSH?

Restrict Management Access

- Use IP authorized managers
- Use Control Plane ACL

- Why was it important to set up NTP?

Configure Manager Authentication

- Set up TACACS
- Set up SSH














Review tasks

Complete lab(s)

Complete debrief

Next Steps...

Recommend completing the ACMA for wireless mobility fundamentals
And the ACSA for switching fundamentals *before* going onto the ACNSA
and ACCA (ClearPass fundamentals)

	MOBILITY	DESIGN	CLEARPASS	SWITCHING	SECURITY	EDGE
Expert	 ACMX	 ACDX	 ACCX			 ACEX
Professional	 ACMP	 ACDP	 ACCP	 ACSP		 ACEP
Associate	 ACMA	 ACDA	 ACCA	 ACSA	 ACNSA	 ACEA

Aruba Mobility Essentials for the Intelligent Edge!

What to expect

ENGLISH | Presenter: Tyler McMinn

PART 1: January 25th, 2021 | 8AM-10AM PST

PART 2: February 1st, 2021 | 8AM-10AM PST

- Part 1 Introduces malware and threat assessment while covering how to defend networks and harden switch devices.

- Part 2 Hardening wireless devices. Explain the use of security protocols, user authentication, and data encryption technologies.

SPANISH | Presenter: Alvaro Tellez

PARTE 1: Enero 25th, 2021 | 11AM-1PM PST

PARTE 2: Febrero 1st, 2021 | 11AM-1PM PST