CCNA 2 v7.0 Curriculum: Module 10 – LAN Security Concepts

itexamanswers.net/ccna-2-v7-0-curriculum-module-10-lan-security-concepts.html

June 5, 2020

10.0 Introduction

10.0.1 Why should I take this module?

Welcome to LAN Security Concepts!

If your career path is in IT, you won't just be building or maintaining networks. You will be responsible for the security of your network. For today's network architects and administrators, security is not an afterthought. It is a top priority for them! In fact, many people in IT now work exclusively in the area of network security.

Do you understand what makes a LAN secure? Do you know what threat actors can do to break network security? Do you know what you can do to stop them? This module is your introduction to the world of network security, so don't wait, click Next!

10.0.2 What will I learn in this module?

Module Title: LAN Security Concepts

Module Objective: Explain how vulnerabilities compromise LAN security.

Topic Title	Topic Objective
Endpoint Security	Explain how to use endpoint security to mitigate attacks.
Access Control	Explain how AAA and 802.1X are used to authenticate LAN endpoints and devices.
Layer 2 Security Threats	Identify Layer 2 vulnerabilities.
MAC Address Table Attack	Explain how a MAC address table attack compromises LAN security.
LAN Attacks	Explain how LAN attacks compromise LAN security.

10.1 Endpoint Security

10.1.1 Network Attacks Today

The news media commonly covers attacks on enterprise networks. Simply search the internet for “latest network attacks” to find up-to-date information on current attacks. Most likely, these attacks will involve one or more of the following:

- **Distributed Denial of Service (DDoS)** – This is a coordinated attack from many devices, called zombies, with the intention of degrading or halting public access to an organization’s website and resources.
- **Data Breach** – This is an attack in which an organization’s data servers or hosts are compromised to steal confidential information.
- **Malware** – This is an attack in which an organization’s hosts are infected with malicious software that cause a variety of problems. For example, ransomware such as WannaCry, shown in the figure, encrypts the data on a host and locks access to it until a ransom is paid.

10.1.2 Network Security Devices

Various network security devices are required to protect the network perimeter from outside access. These devices could include a virtual private network (VPN) enabled router, a next-generation firewall (NGFW), and a network access control (NAC) device.

Click each network security device for more information.

- VPN-Enabled Router
- NGFW
- NAC

VPN-Enabled Router

A VPN-enabled router provides a secure connection to remote users across a public network and into the enterprise network. VPN services can be integrated into the firewall.

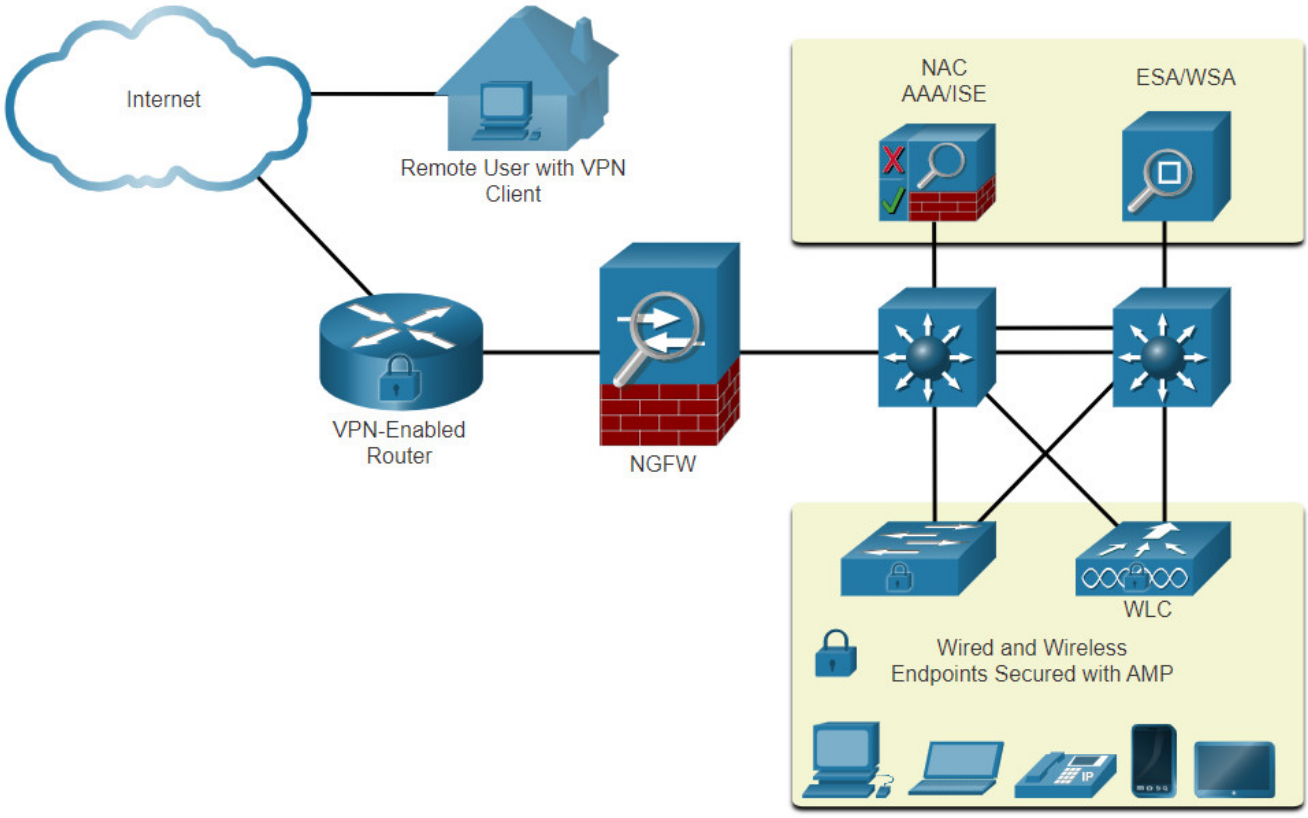
10.1.3 Endpoint Protection

LAN devices such as switches, wireless LAN controllers (WLCs), and other access point (AP) devices interconnect endpoints. Most of these devices are susceptible to the LAN-related attacks that are covered in this module.

But many attacks can also originate from inside the network. If an internal host is infiltrated, it can become a starting point for a threat actor to gain access to critical system devices, such as servers and sensitive data.

Endpoints are hosts which commonly consist of laptops, desktops, servers, and IP phones, as well as employee-owned devices that are typically referred to as bring your own devices (BYODs). Endpoints are particularly susceptible to malware-related attacks that originate through email or web browsing. These endpoints have typically used traditional host-based security features, such as antivirus/antimalware, host-based firewalls, and host-based intrusion prevention systems (HIPSs). However, today endpoints are best protected by a combination of NAC, host-based AMP software, an email security appliance (ESA), and a web security appliance (WSA). Advanced Malware Protection (AMP) products include endpoint solutions such as Cisco AMP for Endpoints.

The figure is a simple topology representing all the network security devices and endpoint solutions discussed in this module.



10.1.4 Cisco Email Security Appliance

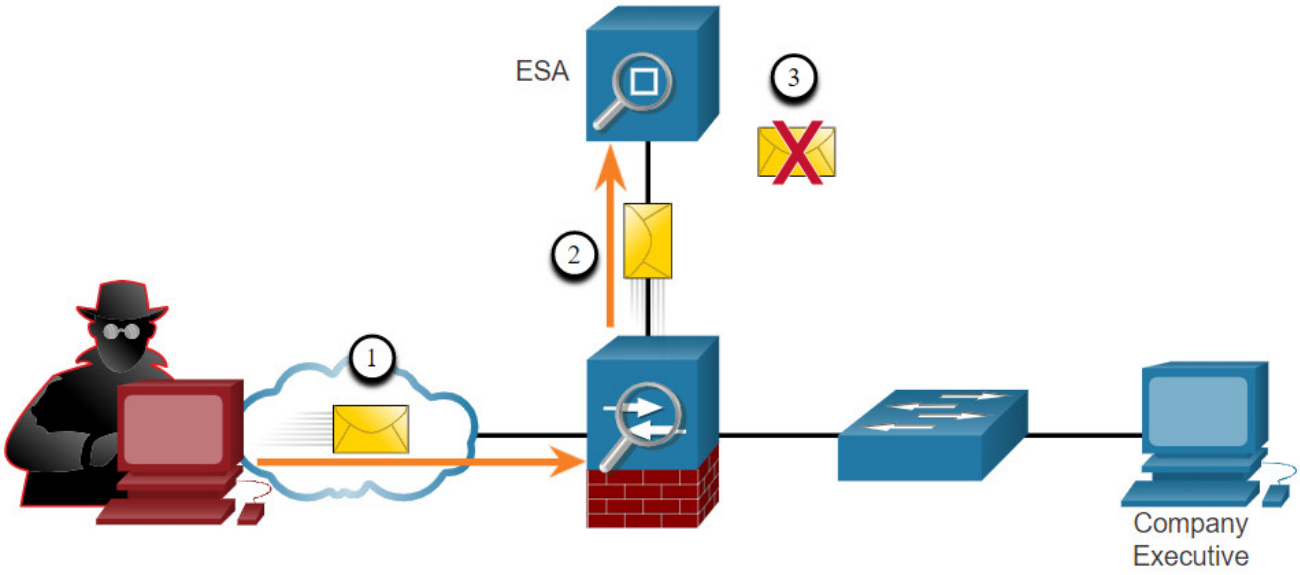
Content security appliances include fine-grained control over email and web browsing for an organization's users.

According to the Cisco's Talos Intelligence Group, in June 2019, 85% of all email sent was spam. Phishing attacks are a particularly virulent form of spam. Recall that a phishing attack entices the user to click a link or open an attachment. Spear phishing targets high-profile employees or executives that may have elevated login credentials. This is particularly crucial in today's environment where, according to the SANS Institute, 95% of all attacks on enterprise networks are the result of a successful spear phishing attack.

The Cisco ESA is a device that is designed to monitor Simple Mail Transfer Protocol (SMTP). The Cisco ESA is constantly updated by real-time feeds from the Cisco Talos, which detects and correlates threats and solutions by using a worldwide database monitoring system. This threat intelligence data is pulled by the Cisco ESA every three to five minutes. These are some of the functions of the Cisco ESA:

- Block known threats.
- Remediate against stealth malware that evaded initial detection.
- Discard emails with bad links (as shown in the figure).
- Block access to newly infected sites.
- Encrypt content in outgoing email to prevent data loss.

In the figure, the Cisco ESA discards the email with bad links.



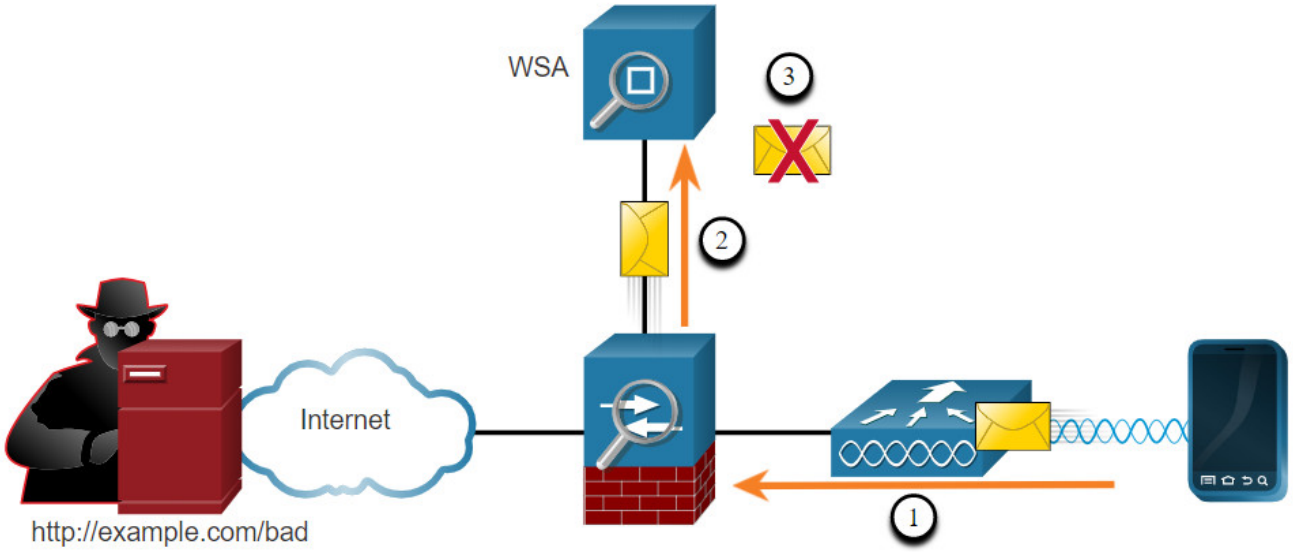
1. Threat actor sends a phishing attack to an important host on the network.
2. The firewall forwards all email to the ESA.
3. The ESA analyzes the email, logs it, and if it is malware discards it.

10.1.5 Cisco Web Security Appliance

The Cisco Web Security Appliance (WSA) is a mitigation technology for web-based threats. It helps organizations address the challenges of securing and controlling web traffic. The Cisco WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, and reporting.

Cisco WSA provides complete control over how users access the internet. Certain features and applications, such as chat, messaging, video and audio, can be allowed, restricted with time and bandwidth limits, or blocked, according to the organization's requirements. The WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, Web application filtering, and encryption and decryption of web traffic.

In the figure, an internal corporate employee uses a smartphone to attempt to connect to a known blacklisted site.



1. A user attempts to connect to a website.
2. The firewall forwards the website request to the WSA.
3. The WSA evaluates the URL and determines it is a known blacklisted site. The WSA discards the packet and sends an access denied message to the user.

10.2 Access Control

10.2.1 Authentication with a Local Password

In the previous topic, you learned that a NAC device provides AAA services. In this topic, you will learn more about AAA and the ways to control access.

Many types of authentication can be performed on networking devices, and each method offers varying levels of security. The simplest method of remote access authentication is to configure a login and password combination on console, vty lines, and aux ports, as shown in the vty lines in the following example. This method is the easiest to implement, but it is also the weakest and least secure. This method provides no accountability and the password is sent in plaintext. Anyone with the password can gain entry to the device.

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

SSH is a more secure form of remote access:

- It requires a username and a password, both of which are encrypted during transmission.
- The username and password can be authenticated by the local database method.
- It provides more accountability because the username is recorded when a user logs in.

The following example illustrates SSH and local database methods of remote access.

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

The local database method has some limitations:

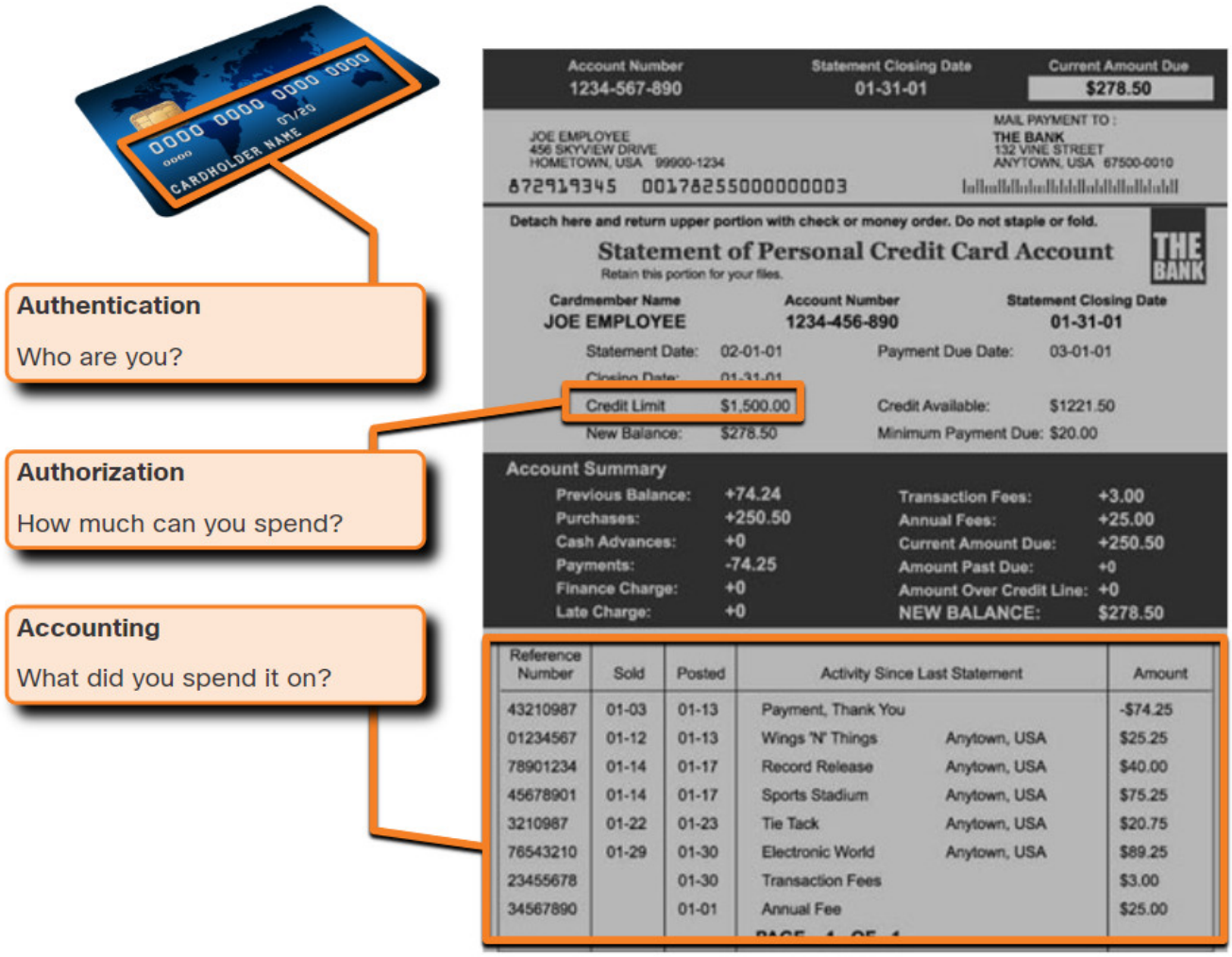
- User accounts must be configured locally on each device. In a large enterprise environment with multiple routers and switches to manage, it can take time to implement and change local databases on each device.
- The local database configuration provides no fallback authentication method. For example, what if the administrator forgets the username and password for that device? With no backup method available for authentication, password recovery becomes the only option.

A better solution is to have all devices refer to the same database of usernames and passwords from a central server..

10.2.2 AAA Components

AAA stands for Authentication, Authorization, and Accounting. The AAA concept is similar to using a credit card, as shown in the figure. The credit card identifies who can use it, how much that user can spend, and keeps an account of what items or services the user purchased.

AAA provides the primary framework to set up access control on a network device. AAA is a way to control who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting).

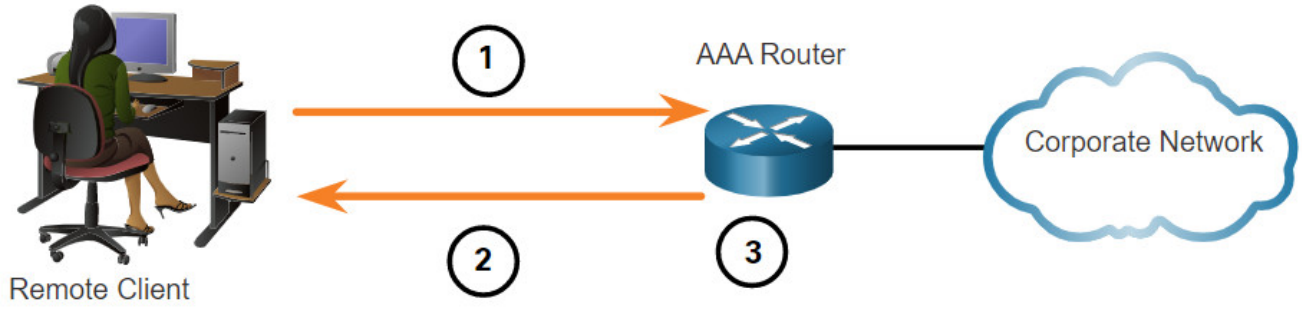


10.2.3 Authentication

Local and server-based are two common methods of implementing AAA authentication.

Local AAA Authentication

Local AAA stores usernames and passwords locally in a network device such as the Cisco router. Users authenticate against the local database, as shown in figure. Local AAA is ideal for small networks.

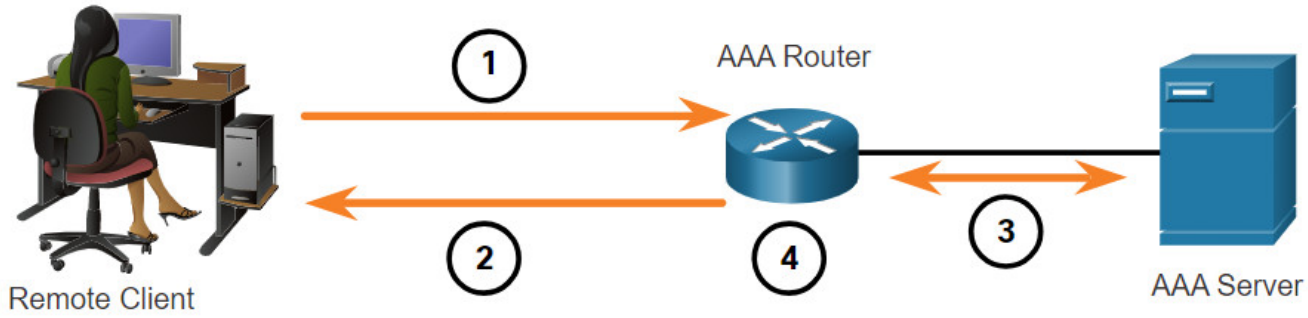


1. The client establishes a connection with the router.

2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is provided access to the network based on information in the local database.

Server-Based AAA Authentication

With the server-based method, the router accesses a central AAA server, as shown in figure. The AAA server contains the usernames and password for all users. The router uses either the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) protocols to communicate with the AAA server. When there are multiple routers and switches, server-based AAA is more appropriate.

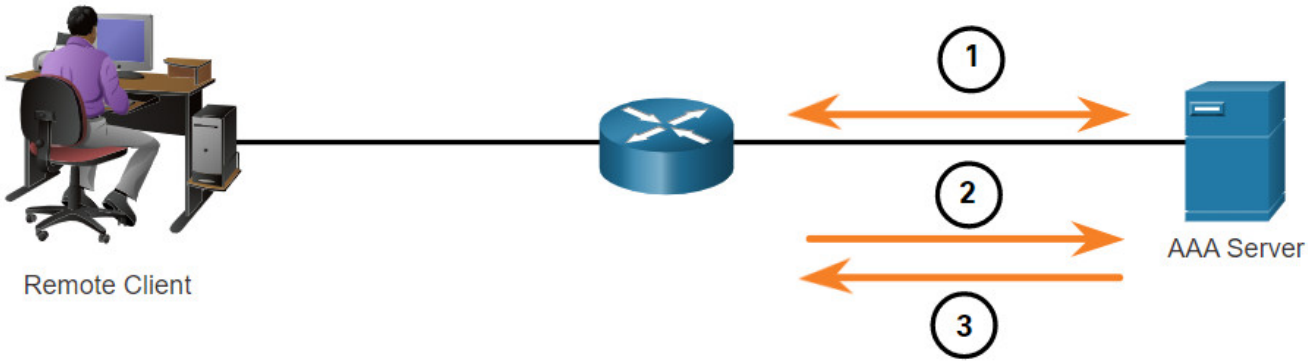


1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a AAA server.
4. The user is provided access to the network based on information in the remote AAA server.

10.2.4 Authorization

AAA authorization is automatic and does not require users to perform additional steps after authentication. Authorization governs what users can and cannot do on the network after they are authenticated.

Authorization uses a set of attributes that describes the user's access to the network. These attributes are used by the AAA server to determine privileges and restrictions for that user, as shown in the figure.

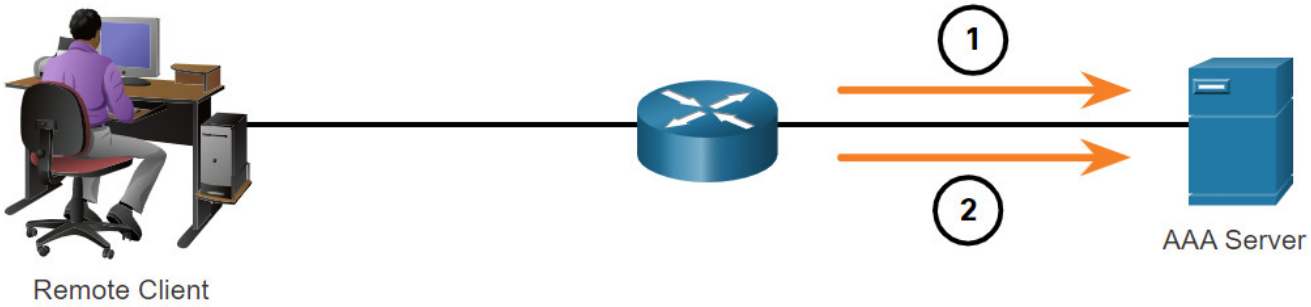


1. When a user has been authenticated, a session is established between the router and the AAA server.
2. The router requests authorization from the AAA server for the client's requested service.
3. The AAA server returns a PASS/FAIL response for authorization.

10.2.5 Accounting

AAA accounting collects and reports usage data. This data can be used for such purposes as auditing or billing. The collected data might include the start and stop connection times, executed commands, number of packets, and number of bytes.

A primary use of accounting is to combine it with AAA authentication. The AAA server keeps a detailed log of exactly what the authenticated user does on the device, as shown in the figure. This includes all EXEC and configuration commands issued by the user. The log contains numerous data fields, including the username, the date and time, and the actual command that was entered by the user. This information is useful when troubleshooting devices. It also provides evidence for when individuals perform malicious acts.

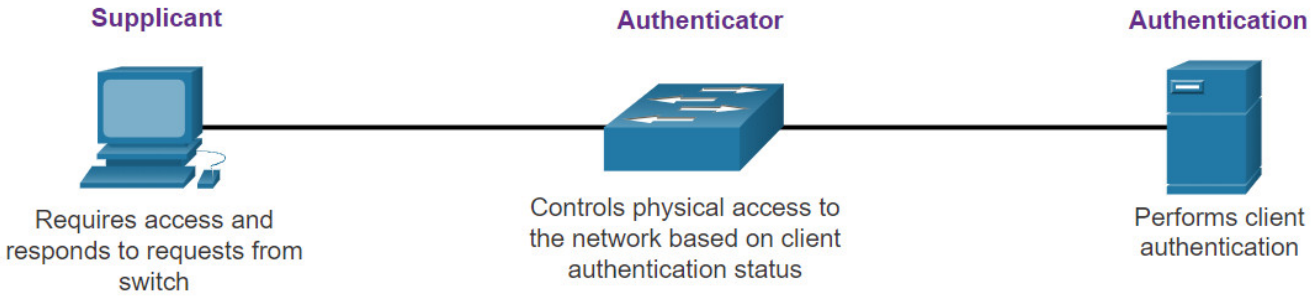


1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded and the accounting process ends.

10.2.6. 802.1X

The IEEE 802.1X standard is a port-based access control and authentication protocol. This protocol restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports. The authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN.

With 802.1X port-based authentication, the devices in the network have specific roles, as shown in the figure.



- **Client (Supplicant)** – This is a device running 802.1X-compliant client software, which is available for wired or wireless devices.
- **Switch (Authenticator)** –The switch acts as an intermediary between the client and the authentication server. It requests identifying information from the client, verifies that information with the authentication server, and relays a response to the client. Another device that could act as authenticator is a wireless access point.
- **Authentication server** –The server validates the identity of the client and notifies the switch or wireless access point that the client is or is not authorized to access the LAN and switch services.

10.3 Layer 2 Security Threats

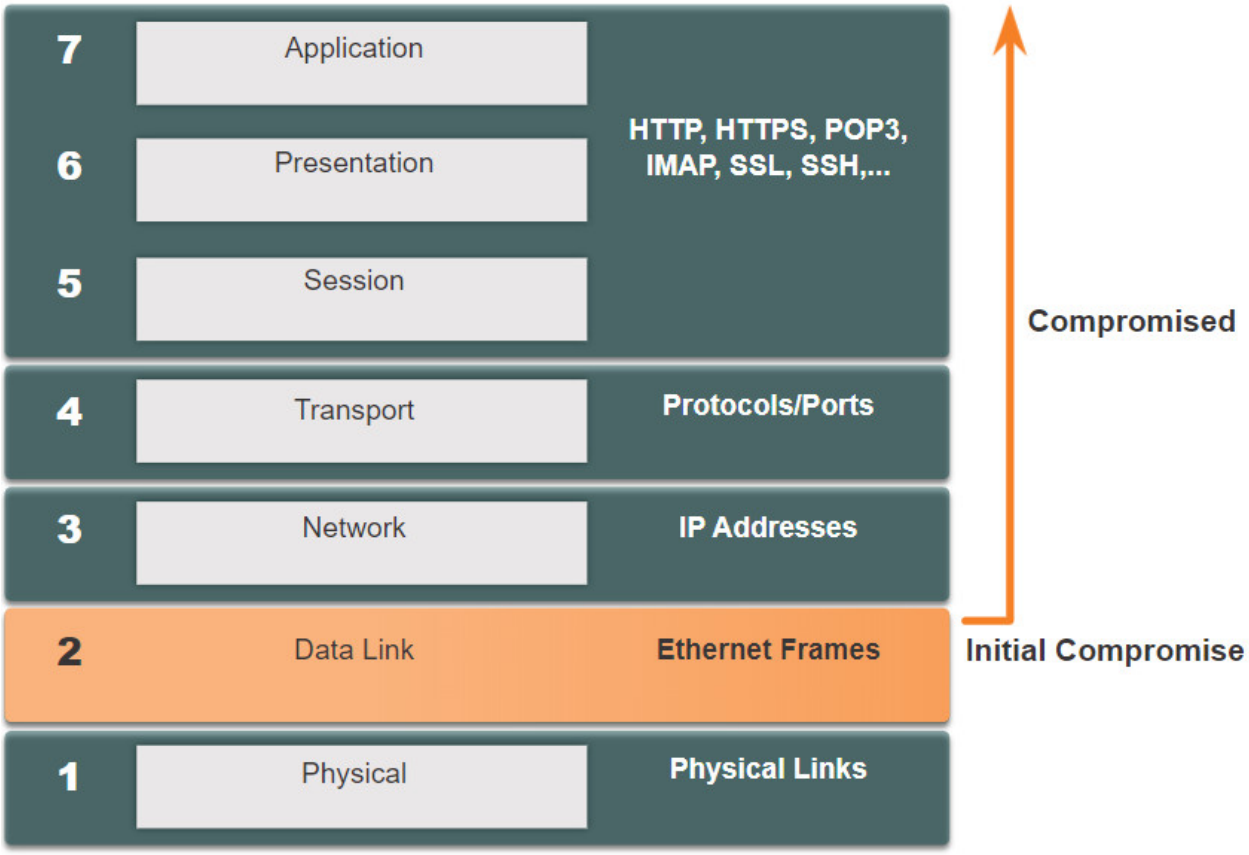
10.3.1 Layer 2 Vulnerabilities

The previous two topics discussed securing endpoints. In this topic, you will continue to learn about ways to secure the LAN by focusing on the frames found in the data link layer (Layer 2) and the switch.

Recall that the OSI reference model is divided into seven layers which work independently of each other. The figure shows the function of each layer and the core elements that can be exploited.

Network administrators routinely implement security solutions to protect the elements in Layer 3 up through Layer 7. They use VPNs, firewalls, and IPS devices to protect these elements. However, if Layer 2 is compromised, then all the layers above it are also affected.

For example, if a threat actor with access to the internal network captured Layer 2 frames, then all the security implemented on the layers above would be useless. The threat actor could cause a lot of damage on the Layer 2 LAN networking infrastructure.



10.3.2 Switch Attack Categories

Security is only as strong as the weakest link in the system, and Layer 2 is considered to be that weak link. This is because LANs were traditionally under the administrative control of a single organization. We inherently trusted all persons and devices connected to our LAN. Today, with BYOD and more sophisticated attacks, our LANs have become more vulnerable to penetration. Therefore, in addition to protecting Layer 3 to Layer 7, network security professionals must also mitigate attacks to the Layer 2 LAN infrastructure.

The first step in mitigating attacks on the Layer 2 infrastructure is to understand the underlying operation of Layer 2 and the threats posed by the Layer 2 infrastructure.

Attacks against the Layer 2 LAN infrastructure are described in the table and are discussed in more detail later in this module.

Layer 2 Attacks

Category	Examples

Category	Examples
MAC Table Attacks	Includes MAC address flooding attacks.
VLAN Attacks	Includes VLAN hopping and VLAN double-tagging attacks. It also includes attacks between devices on a common VLAN.
DHCP Attacks	Includes DHCP starvation and DHCP spoofing attacks.
ARP Attacks	Includes ARP spoofing and ARP poisoning attacks.
Address Spoofing Attacks	Includes MAC address and IP address spoofing attacks.
STP Attacks	Includes Spanning Tree Protocol manipulation attacks.

10.3.3 Switch Attack Mitigation Techniques

The table provides an overview of Cisco solutions to help mitigate Layer 2 attacks.

Layer 2 Attack Mitigation

Solution	Description
Port Security	Prevents many types of attacks including MAC address flooding attacks and DHCP starvation attacks.
DHCP Snooping	Prevents DHCP starvation and DHCP spoofing attacks.
Dynamic ARP Inspection (DAI)	Prevents ARP spoofing and ARP poisoning attacks.
IP Source Guard (IPSG)	Prevents MAC and IP address spoofing attacks

These Layer 2 solutions will not be effective if the management protocols are not secured. For example, the management protocols Syslog, Simple Network Management Protocol (SNMP), Trivial File Transfer Protocol (TFTP), telnet, File Transfer Protocol (FTP) and most other common protocols are insecure; therefore, the following strategies are recommended:

- Always use secure variants of these protocols such as SSH, Secure Copy Protocol (SCP), Secure FTP (SFTP), and Secure Socket Layer/Transport Layer Security (SSL/TLS).
- Consider using out-of-band management network to manage devices.
- Use a dedicated management VLAN where nothing but management traffic resides.
- Use ACLs to filter unwanted access.

10.4 MAC Address Table Attack

10.4.1 Switch Operation Review

In this topic, the focus is still on switches, specifically their MAC address tables and how these tables are vulnerable to attacks.

Recall that to make forwarding decisions, a Layer 2 LAN switch builds a table based on the source MAC addresses in received frames. Shown in the figure, this is called a MAC address table. MAC address tables are stored in memory and are used to more efficiently forward frames.

```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

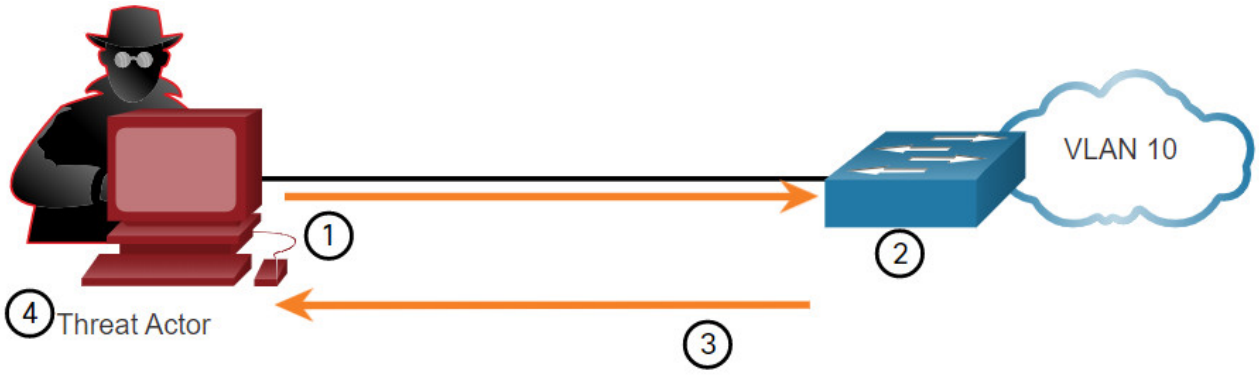
10.4.2 MAC Address Table Flooding

All MAC tables have a fixed size and consequently, a switch can run out of resources in which to store MAC addresses. MAC address flooding attacks take advantage of this limitation by bombarding the switch with fake source MAC addresses until the switch MAC address table is full.

When this occurs, the switch treats the frame as an unknown unicast and begins to flood all incoming traffic out all ports on the same VLAN without referencing the MAC table. This condition now allows a threat actor to capture all of the frames sent from one host to another on the local LAN or local VLAN.

Note: Traffic is flooded only within the local LAN or VLAN. The threat actor can only capture traffic within the local LAN or VLAN to which the threat actor is connected.

The figure shows how a threat actor can easily use the network attack tool **macof** to overflow a MAC address table.



1. The threat actor is connected to VLAN 10 and uses **macof** to rapidly generate many random source and destination MAC and IP addresses.
2. Over a short period of time, the switch's MAC table fills up.
3. When the MAC table is full, the switch begins to flood all frames that it receives. As long as **macof** continues to run, the MAC table remains full and the switch continues to flood all incoming frames out every port associated with VLAN 10.
4. The threat actor then uses packet sniffing software to capture frames from any and all devices connected to VLAN 10.

If the threat actor stops **macof** from running or is discovered and stopped, the switch eventually ages out the older MAC address entries from the table and begins to act like a switch again.

10.4.3 MAC Address Table Attack Mitigation

What makes tools such as **macof** so dangerous is that an attacker can create a MAC table overflow attack very quickly. For instance, a Catalyst 6500 switch can store 132,000 MAC addresses in its MAC address table. A tool such as **macof** can flood a switch with up to 8,000 bogus frames per second; creating a MAC address table overflow attack in a matter of a few seconds. The example shows a sample output of the **macof** command on a Linux host.

```
# macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S
1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S
446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S
105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S
1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S
1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S
1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S
727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S
605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S
2128143986:2128143986(0) win 512
```

Another reason why these attack tools are dangerous is because they not only affect the local switch, they can also affect other connected Layer 2 switches. When the MAC address table of a switch is full, it starts flooding out all ports including those connected to other Layer 2 switches.

To mitigate MAC address table overflow attacks, network administrators must implement port security. Port security will only allow a specified number of source MAC addresses to be learned on the port. Port security is further discussed in another module.

10.5 LAN Attacks

10.5.1 Video – VLAN and DHCP Attacks

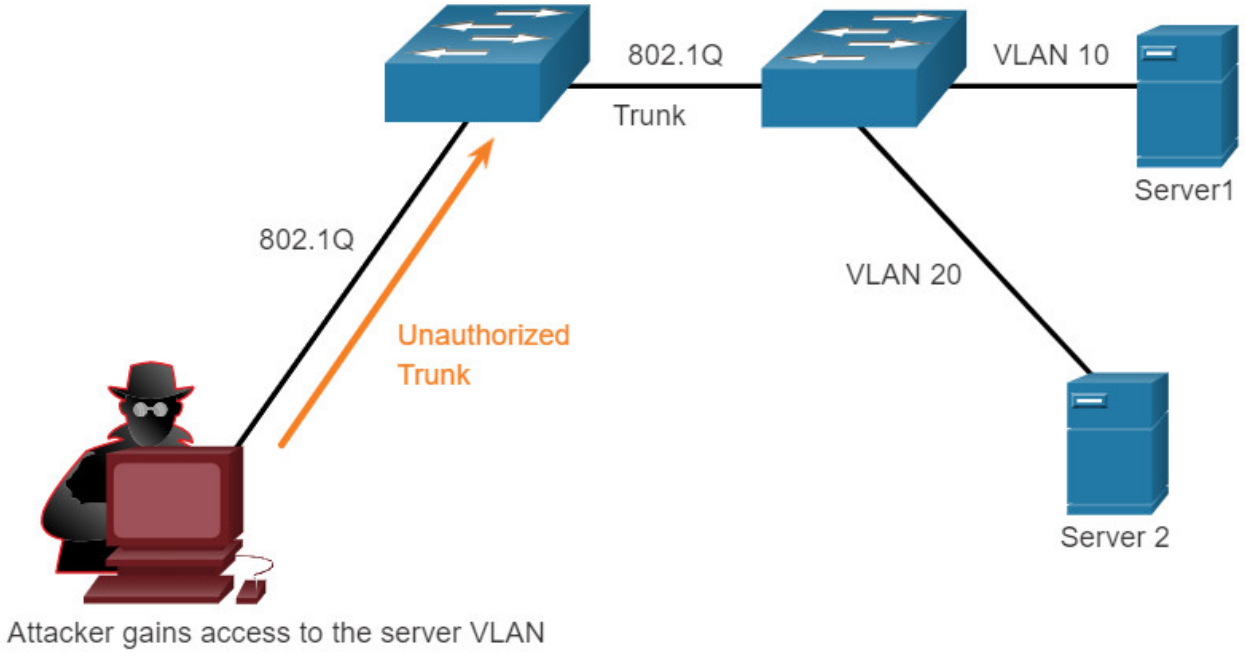
This topic investigates the many different types of LAN attacks and their mitigation techniques. Like the previous topics, these attacks tend to be specific to switches and Layer 2.

Click Play in the figure to view a video about VLAN and DHCP attacks.

10.5.2 VLAN Hopping Attacks

A VLAN hopping attack enables traffic from one VLAN to be seen by another VLAN without the aid of a router. In a basic VLAN hopping attack, the threat actor configures a host to act like a switch to take advantage of the automatic trunking port feature enabled by default on most switch ports.

The threat actor configures the host to spoof 802.1Q signaling and Cisco-proprietary Dynamic Trunking Protocol (DTP) signaling to trunk with the connecting switch. If successful, the switch establishes a trunk link with the host, as shown in the figure. Now the threat actor can access all the VLANs on the switch. The threat actor can send and receive traffic on any VLAN, effectively hopping between VLANs.



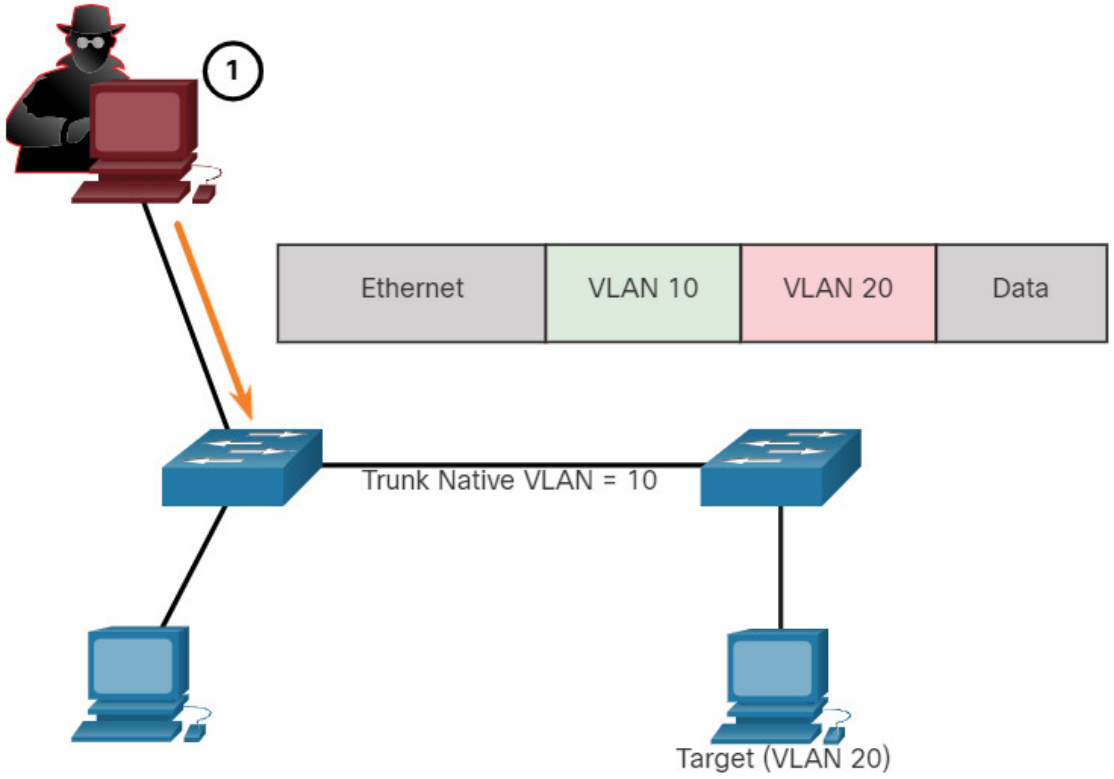
10.5.3 VLAN Double-Tagging Attack

A threat actor in specific situations could embed a hidden 802.1Q tag inside the frame that already has an 802.1Q tag. This tag allows the frame to go to a VLAN that the original 802.1Q tag did not specify.

Click each step for an example and explanation of a double-tagging attack.

- Step 1
- Step 2
- Step 3

The threat actor sends a double-tagged 802.1Q frame to the switch. The outer header has the VLAN tag of the threat actor, which is the same as the native VLAN of the trunk port. For the purposes of this example, assume that this is VLAN 10. The inner tag is the victim VLAN, in this example, VLAN 20.



A VLAN double-tagging attack is unidirectional and works only when the attacker is connected to a port residing in the same VLAN as the native VLAN of the trunk port. The idea is that double tagging allows the attacker to send data to hosts or servers on a VLAN that otherwise would be blocked by some type of access control configuration. Presumably the return traffic will also be permitted, thus giving the attacker the ability to communicate with devices on the normally blocked VLAN.

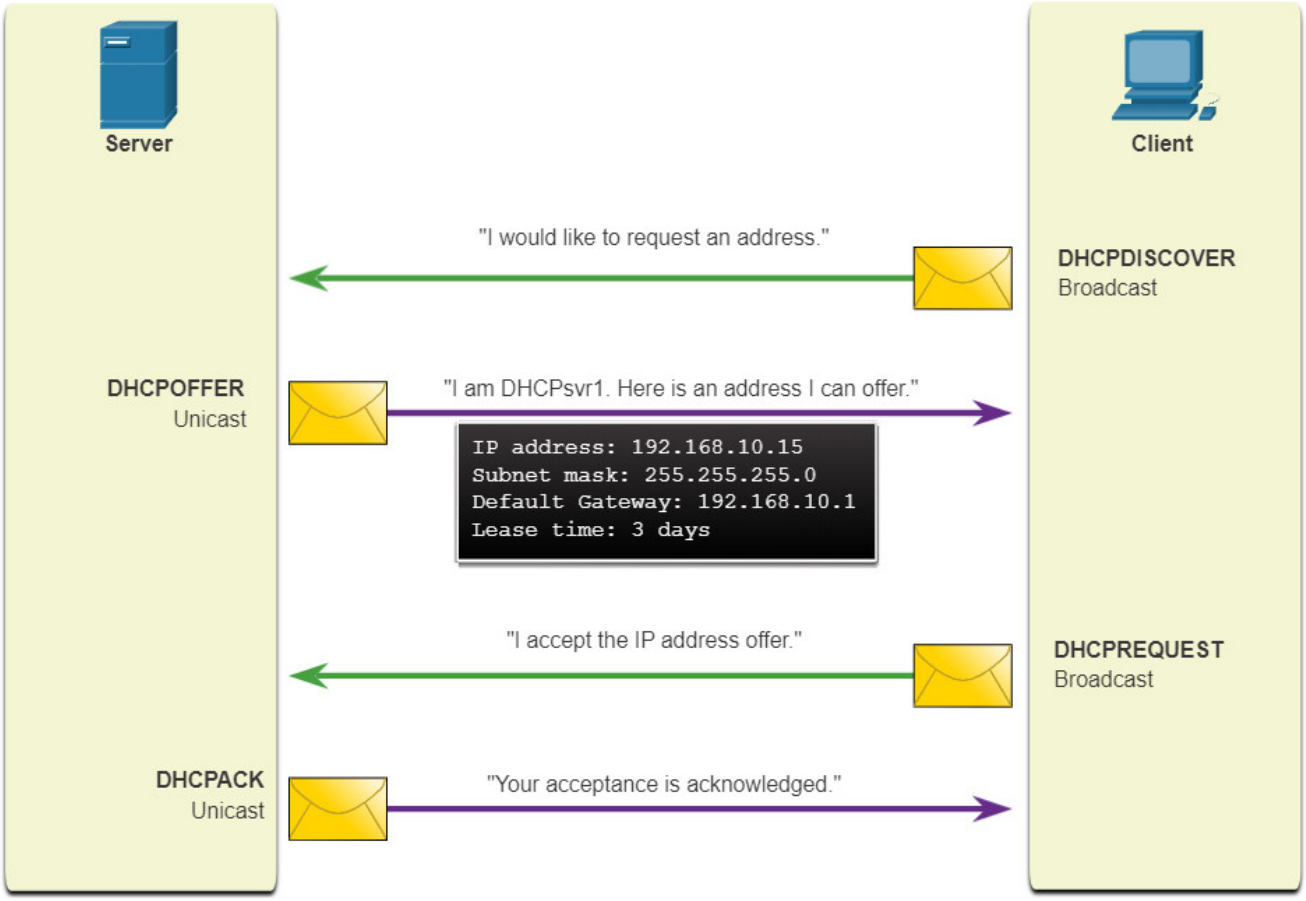
VLAN Attack Mitigation

VLAN hopping and VLAN double-tagging attacks can be prevented by implementing the following trunk security guidelines, as discussed in a previous module:

- Disable trunking on all access ports.
- Disable auto trunking on trunk links so that trunks must be manually enabled.
- Be sure that the native VLAN is only used for trunk links.

10.5.4 DHCP Messages

DHCP servers dynamically provide IP configuration information including IP address, subnet mask, default gateway, DNS servers, and more to clients. A review of the sequence of the DHCP message exchange between client and server is shown in the figure.



10.5.5 DHCP Attacks

Two types of DHCP attacks are DHCP starvation and DHCP spoofing. Both attacks are mitigated by implementing DHCP snooping.

DHCP Starvation Attack

The goal of the DHCP Starvation attack is to create a DoS for connecting clients. DHCP starvation attacks require an attack tool such as Gobbler.

Gobbler has the ability to look at the entire scope of leasable IP addresses and tries to lease them all. Specifically, it creates DHCP discovery messages with bogus MAC addresses.

DHCP Spoofing Attack

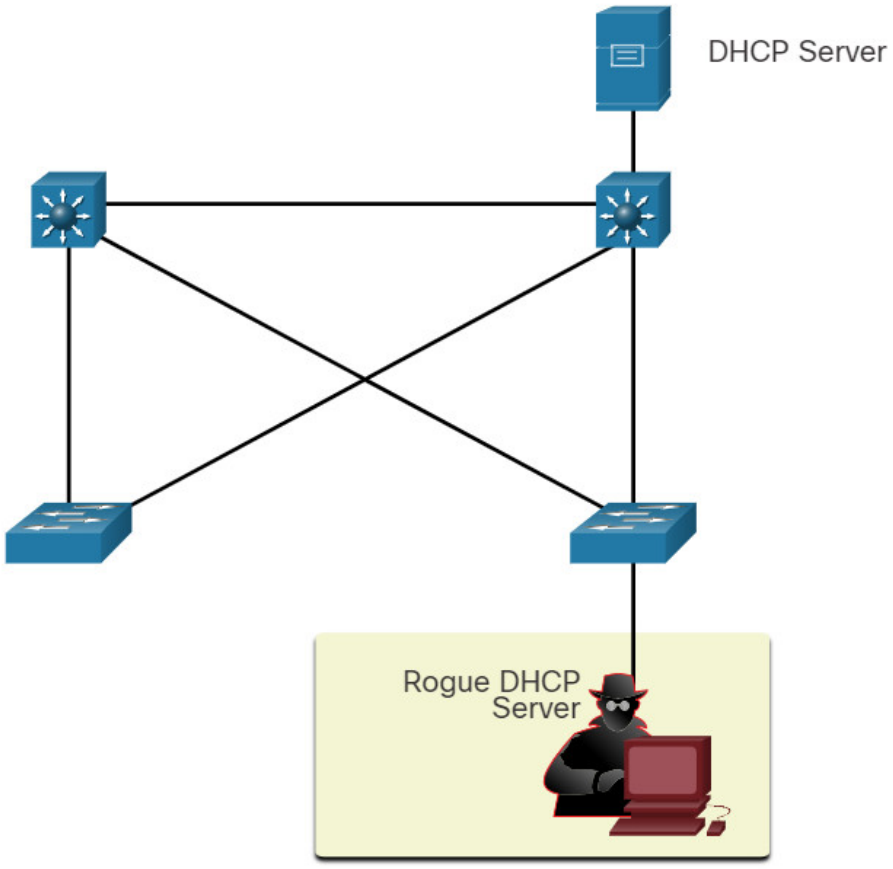
A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. A rogue server can provide a variety of misleading information:

- **Wrong default gateway** – The rogue server provides an invalid gateway or the IP address of its host to create a man-in-the-middle attack. This may go entirely undetected as the intruder intercepts the data flow through the network.

- **Wrong DNS server** – The rogue server provides an incorrect DNS server address pointing the user to a nefarious website.
- **Wrong IP address** – The rogue server provides an invalid IP address effectively creating a DoS attack on the DHCP client.

Click each step for an example and explanation of a DHCP spoofing attack.

Threat Actor Connects Rogue DHCP Server
A threat actor successfully connects a rogue DHCP server to a switch port on the same subnet and VLANs as the target clients. The goal of the rogue server is to provide clients with false IP configuration information.



10.5.6 Video – ARP Attacks, STP Attacks, and CDP Reconnaissance

Click Play in the figure to view a video about VLAN and DHCP attacks.

10.5.7 ARP Attacks

Recall that hosts broadcast ARP Requests to determine the MAC address of a host with a particular IP address. This is typically done to discover the MAC address of the default gateway. All hosts on the subnet receive and process the ARP Request. The host with the matching IP address in the ARP Request sends an ARP Reply.

According to the ARP RFC, a client is allowed to send an unsolicited ARP Reply called a "gratuitous ARP." When a host sends a gratuitous ARP, other hosts on the subnet store the MAC address and IP address contained in the gratuitous ARP in their ARP tables.

The problem is that an attacker can send a gratuitous ARP message containing a spoofed MAC address to a switch, and the switch would update its MAC table accordingly. Therefore, any host can claim to be the owner of any IP and MAC address combination they choose. In a typical attack, a threat actor can send unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway.

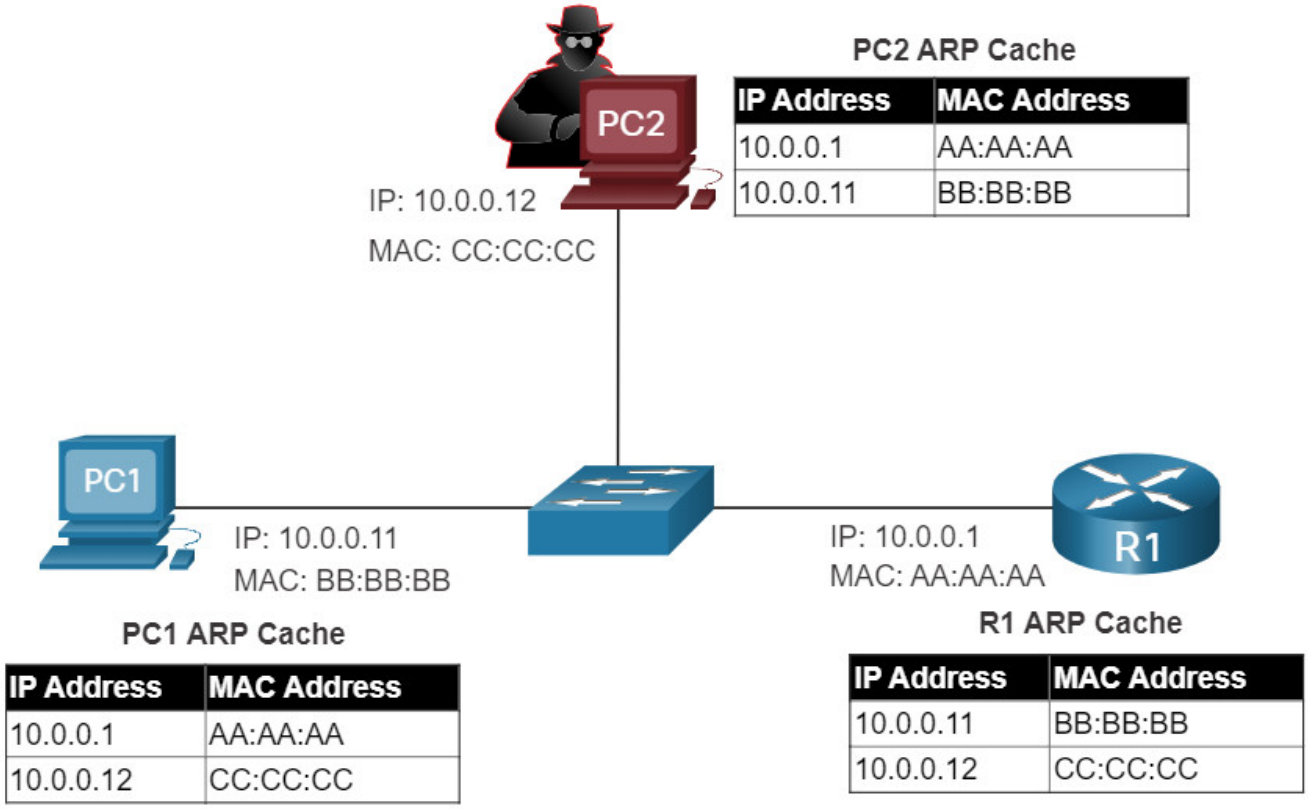
There are many tools available on the internet to create ARP man-in-the-middle attacks including dsniff, Cain & Abel, ettercap, Yersinia, and others. IPv6 uses ICMPv6 Neighbor Discovery Protocol for Layer 2 address resolution. IPv6 includes strategies to mitigate Neighbor Advertisement spoofing, similar to the way IPv6 prevents a spoofed ARP Reply.

ARP spoofing and ARP poisoning are mitigated by implementing DAI.

Click each step for an example and explanation of ARP spoofing and ARP poisoning.

- Step 1
- Step 2
- Step 3

Normal State with Converged MAC Tables
Each device has an accurate MAC table with the correct IP and MAC addresses for the other devices on the LAN.

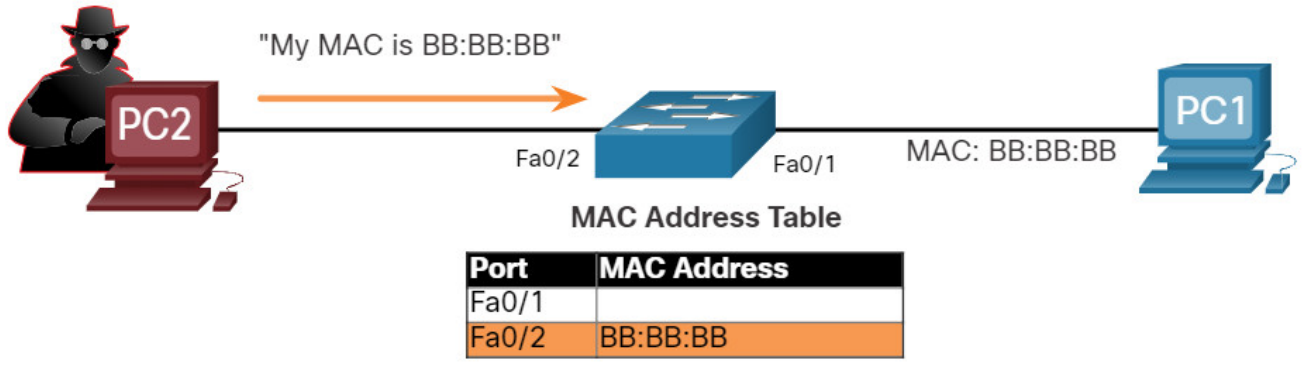


Note: MAC addresses are shown as 24 bits for simplicity.

10.5.8 Address Spoofing Attack

IP addresses and MAC addresses can be spoofed for a variety of reasons. IP address spoofing is when a threat actor hijacks a valid IP address of another device on the subnet, or uses a random IP address. IP address spoofing is difficult to mitigate, especially when it is used inside a subnet in which the IP belongs.

MAC address spoofing attacks occur when the threat actors alter the MAC address of their host to match another known MAC address of a target host. The attacking host then sends a frame throughout the network with the newly-configured MAC address. When the switch receives the frame, it examines the source MAC address. The switch overwrites the current MAC table entry and assigns the MAC address to the new port, as shown in the figure. It then inadvertently forwards frames destined for the target host to the attacking host.



Note: MAC Addresses are shown as 24 bits for simplicity

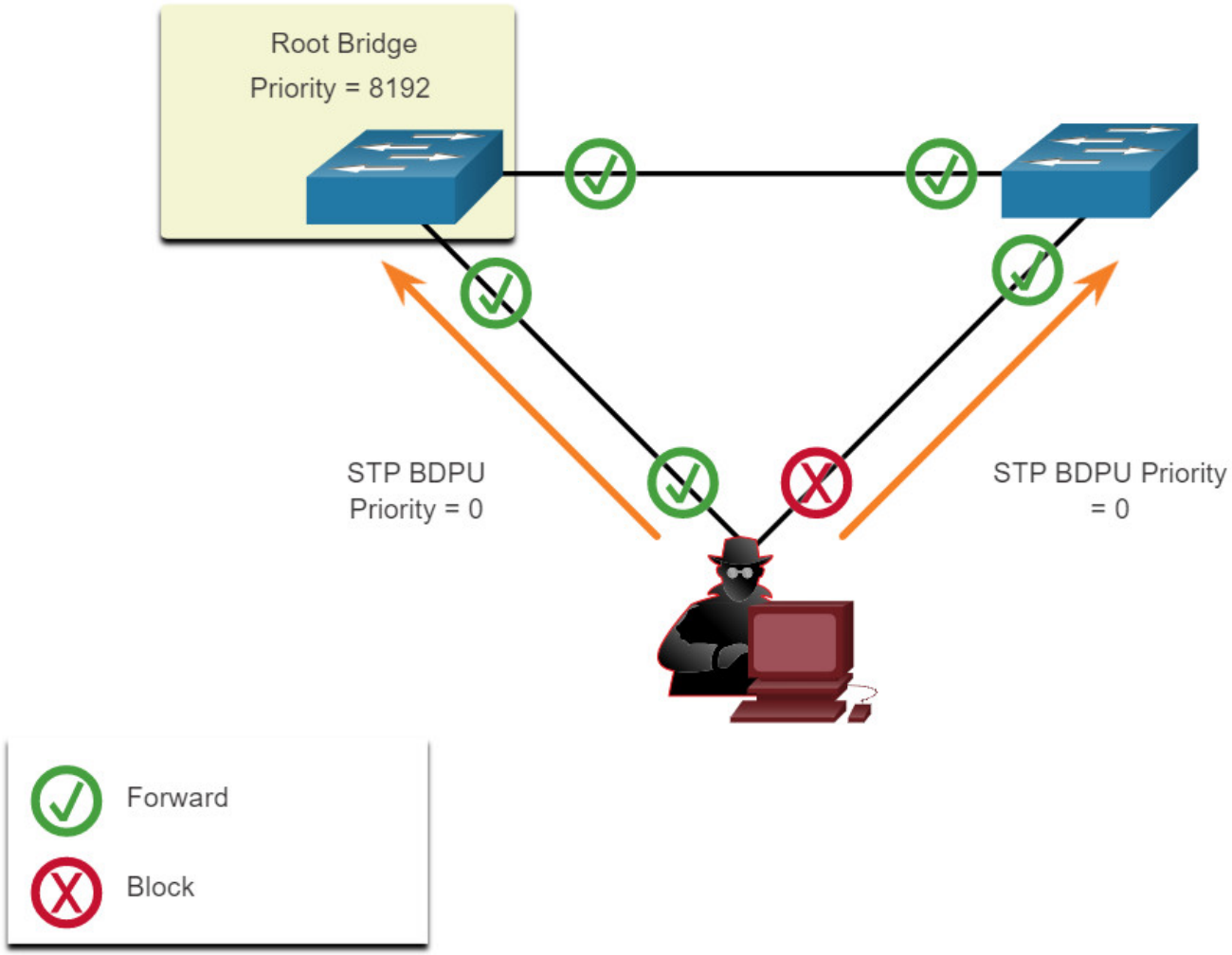
When the target host sends traffic, the switch will correct the error, realigning the MAC address to the original port. To stop the switch from returning the port assignment to its correct state, the threat actor can create a program or script that will constantly send frames to the switch so that the switch maintains the incorrect or spoofed information. There is no security mechanism at Layer 2 that allows a switch to verify the source of MAC addresses, which is what makes it so vulnerable to spoofing.

IP and MAC address spoofing can be mitigated by implementing IPSG.

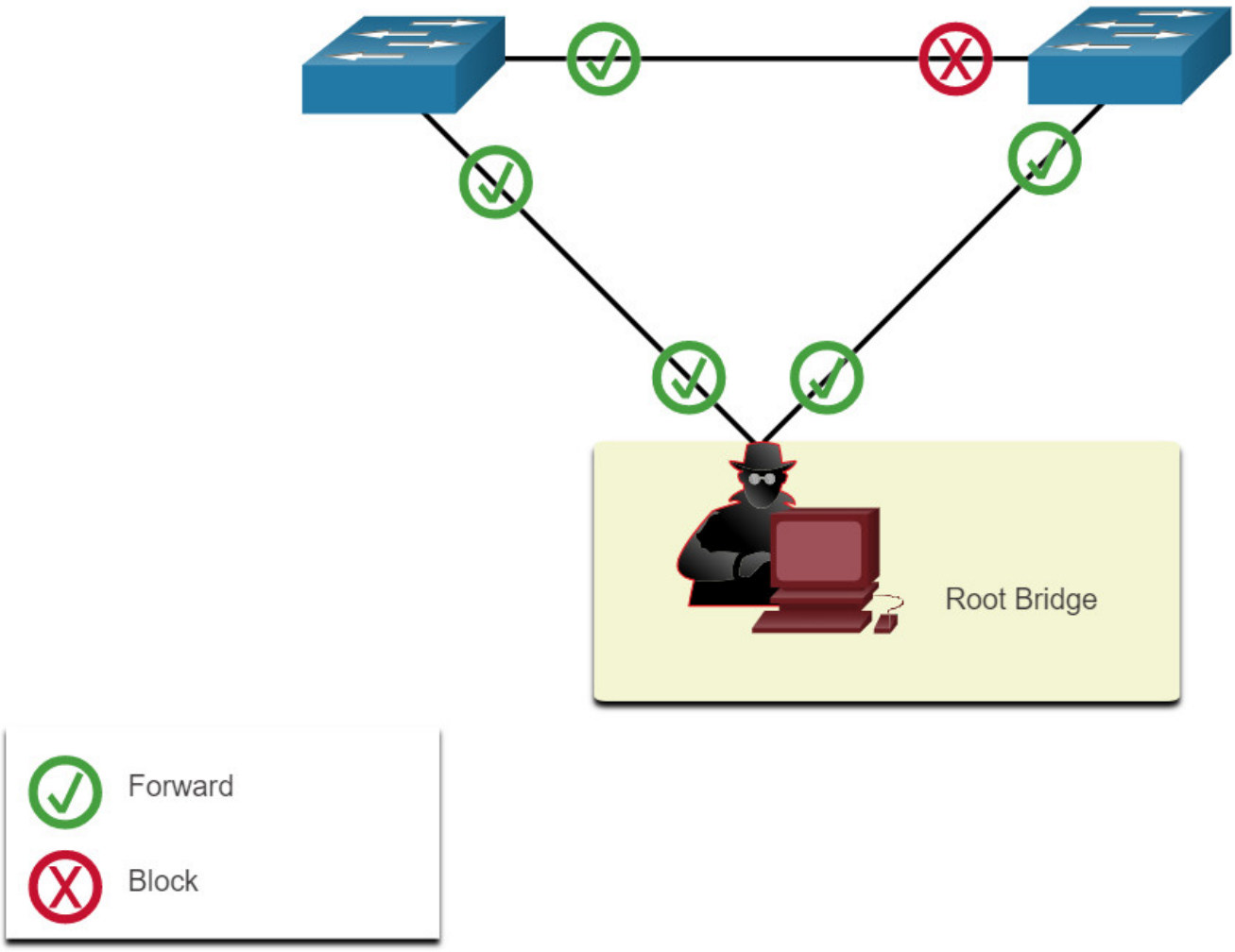
10.5.9 STP Attack

Network attackers can manipulate the Spanning Tree Protocol (STP) to conduct an attack by spoofing the root bridge and changing the topology of a network. Attackers can make their hosts appear as root bridges; and therefore, capture all traffic for the immediate switched domain.

To conduct an STP manipulation attack, the attacking host broadcasts STP bridge protocol data units (BPDUs) containing configuration and topology changes that will force spanning-tree recalculations, as shown in the figure. The BPDUs sent by the attacking host announce a lower bridge priority in an attempt to be elected as the root bridge.



If successful, the attacking host becomes the root bridge, as shown in the figure, and can now capture a variety of frames that would otherwise not be accessible.



This STP attack is mitigated by implementing BPDU Guard on all access ports. BPDU Guard is discussed in more detail later in the course.

10.5.10 CDP Reconnaissance

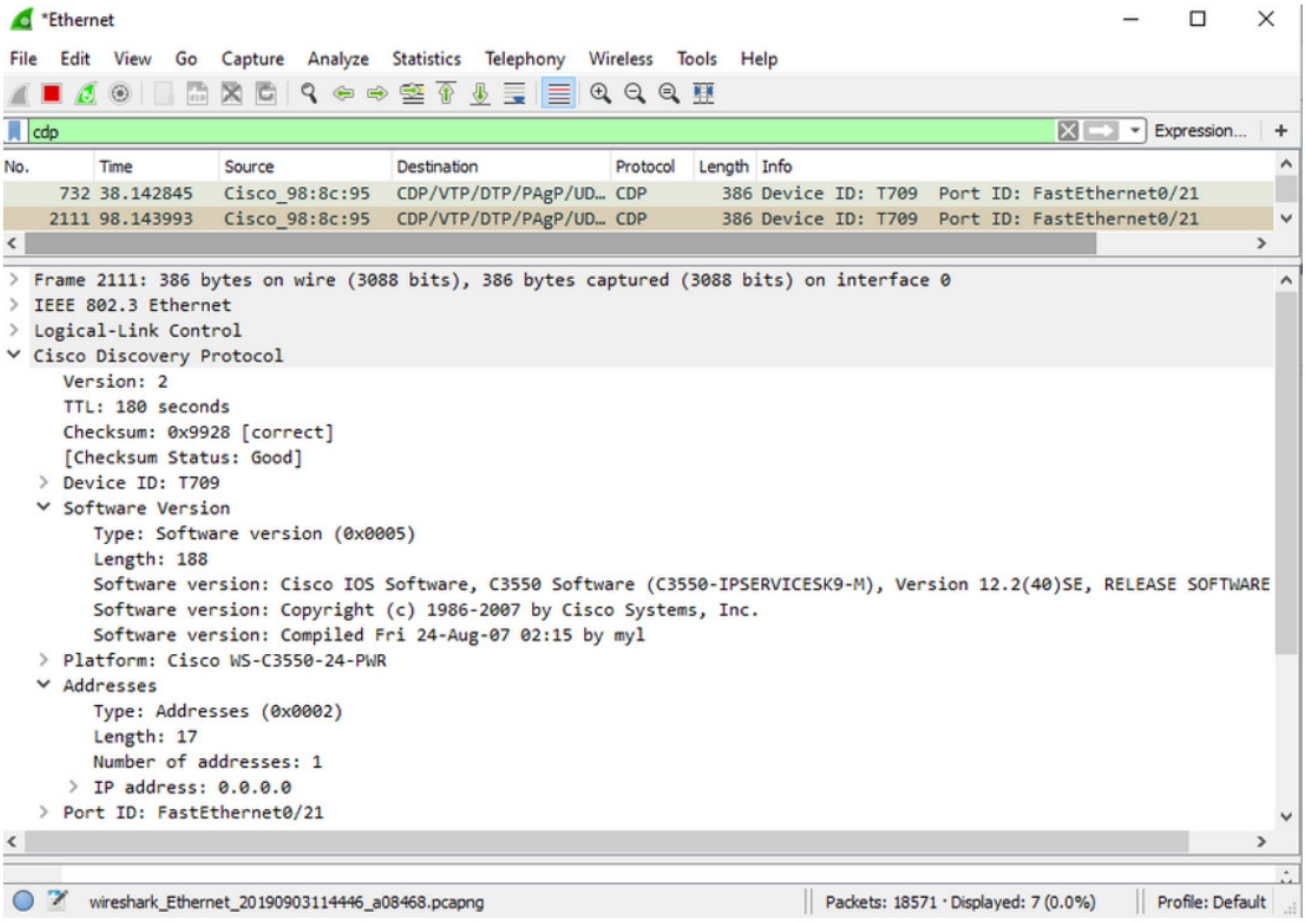
The Cisco Discovery Protocol (CDP) is a proprietary Layer 2 link discovery protocol. It is enabled on all Cisco devices by default. CDP can automatically discover other CDP-enabled devices and help auto-configure their connection. Network administrators also use CDP to help configure and troubleshoot network devices.

CDP information is sent out CDP-enabled ports in periodic, unencrypted broadcasts. CDP information includes the IP address of the device, IOS software version, platform, capabilities, and the native VLAN. The device receiving the CDP message updates its CDP database.

CDP information is extremely useful in network troubleshooting. For example, CDP can be used to verify Layer 1 and 2 connectivity. If an administrator cannot ping a directly connected interface, but still receives CDP information, then the problem is most likely related to the Layer 3 configuration.

However, the information provided by CDP can also be used by a threat actor to discover network infrastructure vulnerabilities.

In the figure, a sample Wireshark capture displays the contents of a CDP packet. The attacker is able to identify the Cisco IOS software version used by the device. This allows the attacker to determine whether there were any security vulnerabilities specific to that particular version of IOS.



CDP broadcasts are sent unencrypted and unauthenticated. Therefore, an attacker could interfere with the network infrastructure by sending crafted CDP frames containing bogus device information to directly-connected Cisco devices.

To mitigate the exploitation of CDP, limit the use of CDP on devices or ports. For example, disable CDP on edge ports that connect to untrusted devices.

To disable CDP globally on a device, use the **no cdp run** global configuration mode command. To enable CDP globally, use the **cdp run** global configuration command.

To disable CDP on a port, use the **no cdp enable** interface configuration command. To enable CDP on a port, use the **cdp enable** interface configuration command.

Note: Link Layer Discovery Protocol (LLDP) is also vulnerable to reconnaissance attacks. Configure **no lldp run** to disable LLDP globally. To disable LLDP on the interface, configure **no lldp transmit** and **no lldp receive.**

10.6 Module Practice and Quiz

10.6.1 What did I learn in this module?

Endpoints are particularly susceptible to malware-related attacks that originate through email or web browsing, such as DDOS, date breaches, and malware. These endpoints have typically used traditional host-based security features, such as antivirus/antimalware, host-based firewalls, and host-based intrusion prevention systems (HIPSs). Endpoints are best protected by a combination of NAC, host-based AMP software, an email security appliance (ESA), and a web security appliance (WSA). Cisco WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, Web application filtering, and encryption and decryption of web traffic.

AAA controls who is permitted to access a network (authenticate), what they can do while they are there (authorize), and to audit what actions they performed while accessing the network (accounting). Authorization uses a set of attributes that describes the user's access to the network. Accounting is combined with AAA authentication. The AAA server keeps a detailed log of exactly what the authenticated user does on the device. The IEEE 802.1X standard is a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports.

If Layer 2 is compromised, then all layers above it are also affected. The first step in mitigating attacks on the Layer 2 infrastructure is to understand the underlying operation of Layer 2 and the Layer 2 solutions: Port Security, DHCP Snooping, DAI, and IPSG. These won't work unless management protocols are secured.

MAC address flooding attacks bombard the switch with fake source MAC addresses until the switch MAC address table is full. At this point, the switch treats the frame as an unknown unicast and begins to flood all incoming traffic out all ports on the same VLAN without referencing the MAC table. The threat actor can now capture all of the frames sent from one host to another on the local LAN or local VLAN. The threat actor uses macof to rapidly generate many random source and destination MAC and IP. To mitigate MAC table overflow attacks, network administrators must implement port security.

A VLAN hopping attack enables traffic from one VLAN to be seen by another VLAN without the aid of a router. The threat actor configures a host to act like a switch to take advantage of the automatic trunking port feature enabled by default on most switch ports.

A VLAN double-tagging attack is unidirectional and works only when the threat actor is connected to a port residing in the same VLAN as the native VLAN of the trunk port. Double tagging allows the threat actor to send data to hosts or servers on a VLAN that otherwise would be blocked by some type of access control configuration. Return traffic will also be permitted, letting the threat actor communicate with devices on the normally blocked VLAN.

VLAN hopping and VLAN double-tagging attacks can be prevented by implementing the following trunk security guidelines:

- Disable trunking on all access ports.
- Disable auto trunking on trunk links so that trunks must be manually enabled.
- Be sure that the native VLAN is only used for trunk links.

DHCP Attack: DHCP servers dynamically provide IP configuration information including IP address, subnet mask, default gateway, DNS servers, and more to clients. Two types of DHCP attacks are DHCP starvation and DHCP spoofing. Both attacks are mitigated by implementing DHCP snooping.

ARP Attack: A threat actor sends a gratuitous ARP message containing a spoofed MAC address to a switch, and the switch updates its MAC table accordingly. Now the threat actor sends unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway. ARP spoofing and ARP poisoning are mitigated by implementing DAI.

Address Spoofing Attack: IP address spoofing is when a threat actor hijacks a valid IP address of another device on the subnet or uses a random IP address. MAC address spoofing attacks occur when the threat actors alter the MAC address of their host to match another known MAC address of a target host. IP and MAC address spoofing can be mitigated by implementing IPSG.

STP Attack: Threat actors manipulate STP to conduct an attack by spoofing the root bridge and changing the topology of a network. Threat actors make their hosts appear as root bridges; therefore, capturing all traffic for the immediate switched domain. This STP attack is mitigated by implementing BPDU Guard on all access ports

CDP Reconnaissance: CDP information is sent out CDP-enabled ports in periodic, unencrypted broadcasts. CDP information includes the IP address of the device, IOS software version, platform, capabilities, and the native VLAN. The device receiving the CDP message updates its CDP database. the information provided by CDP can also be used by a threat actor to discover network infrastructure vulnerabilities. To mitigate the exploitation of CDP, limit the use of CDP on devices or ports.

10.6.2 Module Quiz – LAN Security Concepts

Download Slide Powerpoint (PPT)

CCNA 2 v7.0 Curriculum: Module 10 - LAN Security Concepts.pptx

1 file(s) 1.21 MB

Download

Tags:ccna 2 v7 modules