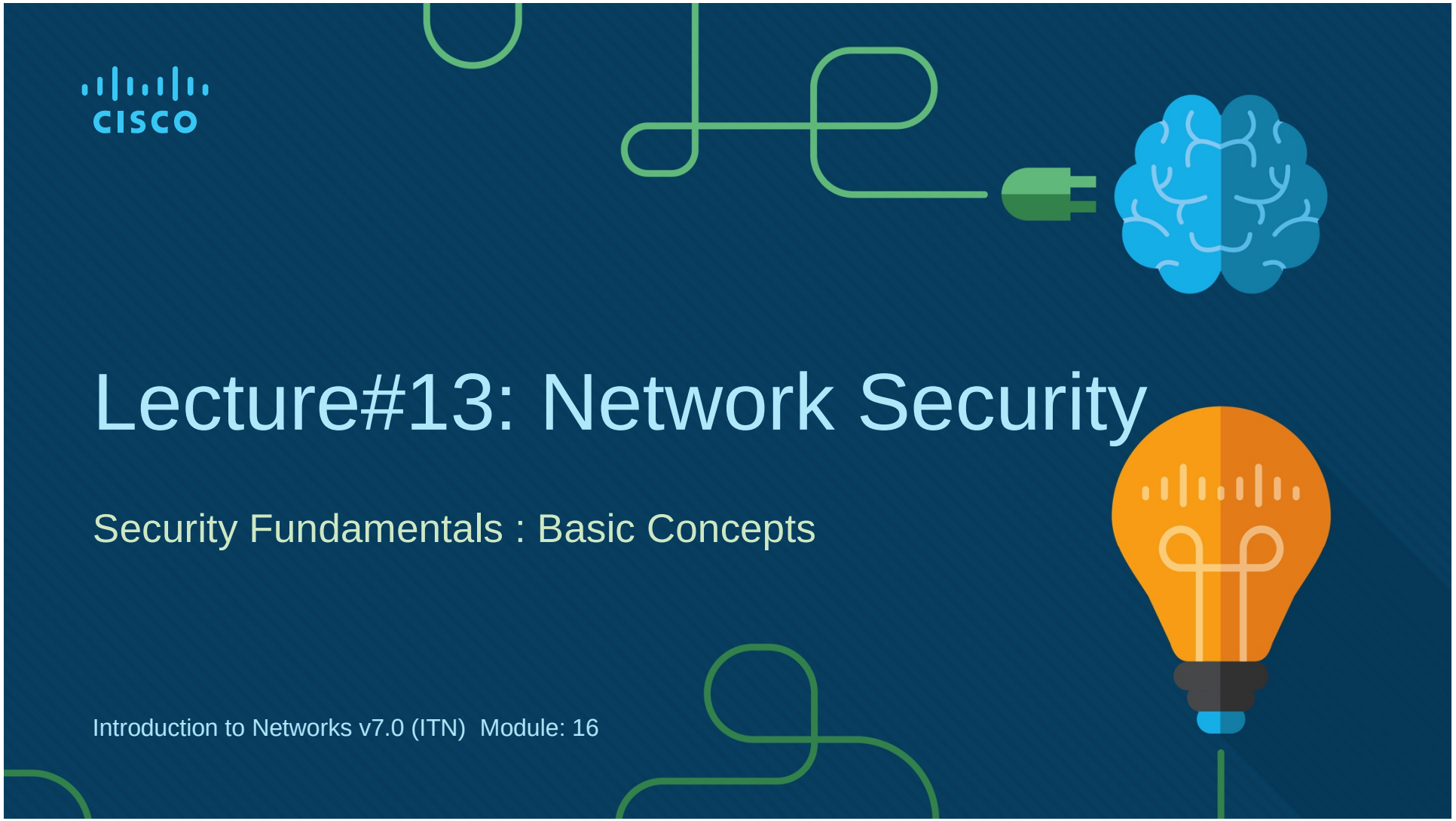

Lecture#13: Network Security
Security Fundamentals : Basic Concepts
Introduction to Networks v7.0 (ITN) Module: 16

13.1.1 Security Threats

Types of Threats

Attacks on a network can be devastating and can result in a loss of time and money due to damage, or theft of important information or assets.

- Intruders can gain access to a network through software vulnerabilities, hardware attacks, or through guessing someone's username and password.
- Intruders who gain access by modifying software or exploiting software vulnerabilities are called threat actors.

After the threat actor gains access to the network, four types of threats may arise:

- Information Theft
- Data Loss and manipulation
- Identity Theft
- Disruption of Service

Types of Vulnerabilities

Vulnerability is the **degree of weakness** in a network or a device. Some degree of vulnerability is inherent in routers, switches, desktops, servers, and even security devices. Typically, the network devices under attack are the endpoints, such as servers and desktop computers.

There are **three primary vulnerabilities** or weaknesses:

- **Technological Vulnerabilities** might include TCP/IP Protocol weaknesses, Operating System Weaknesses, and Network Equipment weaknesses.
- **Configuration Vulnerabilities** might include unsecured user accounts, system accounts with easily guessed passwords, misconfigured internet services, unsecure default settings, and misconfigured network equipment.
- **Security Policy Vulnerabilities** might include lack of a written security policy, politics, lack of authentication continuity, logical access controls not applied, software and hardware installation and changes not following policy, and a nonexistent disaster recovery plan.

All three of these **sources of vulnerabilities** can leave a network or device **open to** various attacks, including malicious code attacks and network attacks.

Physical Security

If network resources can be **physically compromised**, a threat actor can deny the use of network resources. The four classes of physical threats are as follows:

- **Hardware threats -** This includes physical damage to servers, routers, switches, cabling plant, and workstations.
- **Environmental threats -** This includes temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry).
- **Electrical threats -** This includes voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss.
- **Maintenance threats -** This includes poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling.

A good plan for physical security must be created and implemented to address these issues.

13.1.2 Network Attacks

Types of Malware

Malware is short for malicious software. It is code or software specifically designed to damage, disrupt, steal, or inflict “bad” or illegitimate action on data, hosts, or networks. The following are types of malware:

- **Viruses -** A computer virus is a type of malware that propagates by inserting a copy of itself into, and becoming part of, another program. It spreads from one computer to another, leaving infections as it travels.
- **Worms -** Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate.
- **Trojan Horses -** It is a harmful piece of software that looks legitimate. Unlike viruses and worms, Trojan horses do not reproduce by infecting other files. They self-replicate. Trojan horses must spread through user interaction such as opening an email attachment or downloading and running a file from the internet.

Network Attacks

Reconnaissance Attacks

In addition to malicious code attacks, it is also possible for networks to fall prey to various network attacks.

Network attacks can be classified into three major categories:

- **Reconnaissance attacks** - The discovery and mapping of systems, services, or vulnerabilities.
- **Access attacks** - The unauthorized manipulation of data, system access, or user privileges.
- **Denial of service** - The disabling or corruption of networks, systems, or services.

For reconnaissance attacks, external threat actors can use internet tools, such as the **nslookup** and **whois** utilities, to easily determine the IP address space assigned to a given corporation or entity. After the IP address space is determined, a threat actor can then ping the publicly available IP addresses to identify the addresses that are active.

Network Attacks

Access Attacks

Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information.

Access attacks can be classified into four types:

- **Password attacks -** Implemented using brute force, trojan horse, and packet sniffers
- **Trust exploitation -** A threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target.
- **Port redirection**: - A threat actor uses a compromised system as a base for attacks against other targets. For example, a threat actor using SSH (port 22) to connect to a compromised host A. Host A is trusted by host B and, therefore, the threat actor can use Telnet (port 23) to access it.
- **Man-in-the middle -** The threat actor is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties.

Denial of Service Attacks

Denial of service (DoS) attacks are the most publicized form of attack and among the most difficult to eliminate. However, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators.

- DoS attacks take many forms. Ultimately, they prevent authorized people from using a service by consuming system resources. To help prevent DoS attacks it is important to stay up to date with the latest security updates for operating systems and applications.
- DoS attacks are a major risk because they interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled threat actor.
- A DDoS is similar to a DoS attack, but it originates from multiple, coordinated sources. For example, a threat actor builds a network of infected hosts, known as zombies. A network of zombies is called a botnet. The threat actor uses a command and control (CnC) program to instruct the botnet of zombies to carry out a DDoS attack.

Network Attacks

Lab – Research Network Security Threats

In this lab, you will complete the following objectives:

- Part 1: Explore the SANS Website
- Part 2: Identify Recent Network Security Threats
- Part 3: Detail a Specific Network Security Threat

13.1.3 Network Attack Mitigations

Network Attack Mitigations

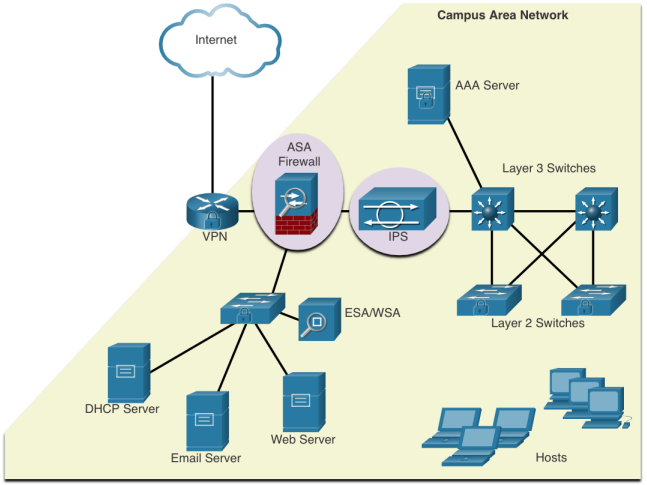
The Defense-in-Depth Approach

To **mitigate network attacks**, you must first secure devices including routers, switches, servers, and hosts. Most organizations employ a **defense-in-depth approach** (also known as a layered approach) to security.

The layered approach requires a combination of networking devices and services working in tandem.

Several security devices and services are implemented to protect an organization's users and assets against TCP/IP threats:

- VPN, ASA Firewall, IPS, ESA/WSA, AAA Server



Network Attack Mitigations

Keep Backups

Backing up device configurations and data is one of the most effective ways of protecting against data loss. Backups should be performed on a regular basis as identified in the security policy. Data backups are usually stored offsite to protect the backup media if anything happens to the main facility.

The table shows backup considerations and their descriptions.

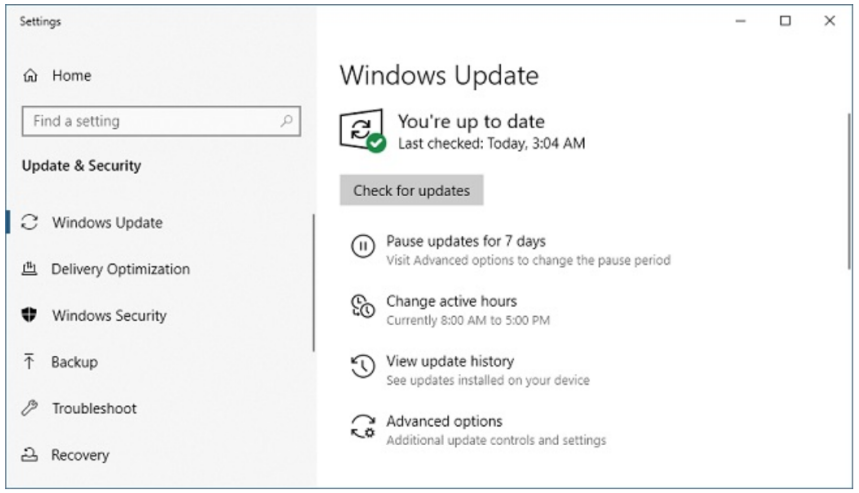
Consideration	Description
Frequency	• Perform backups on a regular basis as identified in the security policy. • Full backups can be time-consuming, therefore perform monthly or weekly backups with frequent partial backups of changed files.
Storage	• Always validate backups to ensure the integrity of the data and validate the file restoration procedures.
Security	• Backups should be transported to an approved offsite storage location on a daily, weekly, or monthly rotation, as required by the security policy.
Validation	• Backups should be protected using strong passwords. The password is required to restore the data.

Network Attack Mitigations

Upgrade, Update, and Patch

As new malware is released, enterprises need to keep current with the latest versions of antivirus software.

- The most effective way to mitigate a worm attack is to download security updates from the operating system vendor and patch all vulnerable systems.
- One solution to the management of critical security patches is to make sure all end systems automatically download updates.



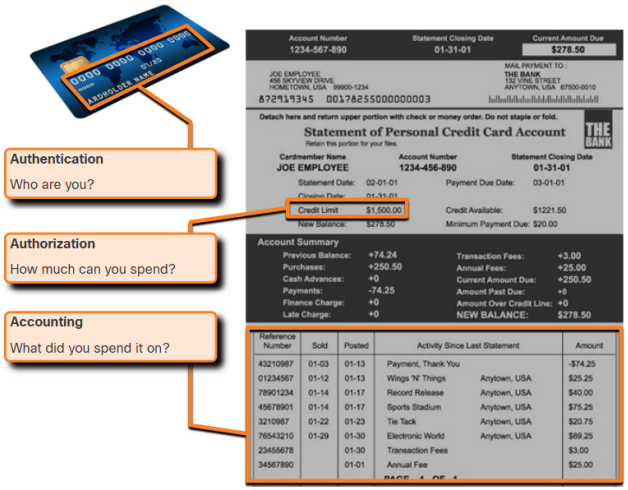
Network Attack Mitigations

Authentication, Authorization, and Accounting

Authentication, authorization, and accounting (AAA, or “triple A”) network security services provide the primary framework to set up access control on network devices.

- AAA is a way to control who is permitted to access a network (authenticate), what actions they perform while accessing the network (authorize), and making a record of what was done while they are there (accounting).

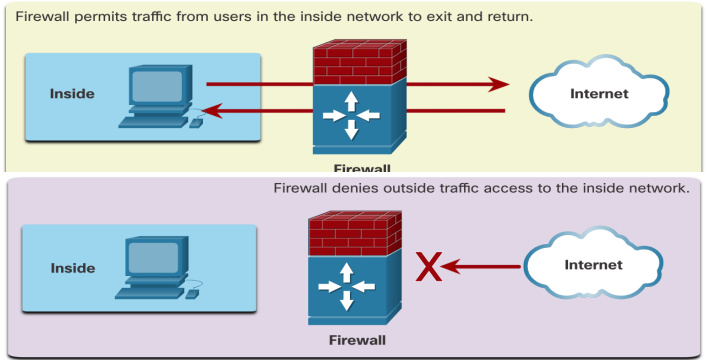
- The concept of AAA is similar to the use of a credit card. The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on.

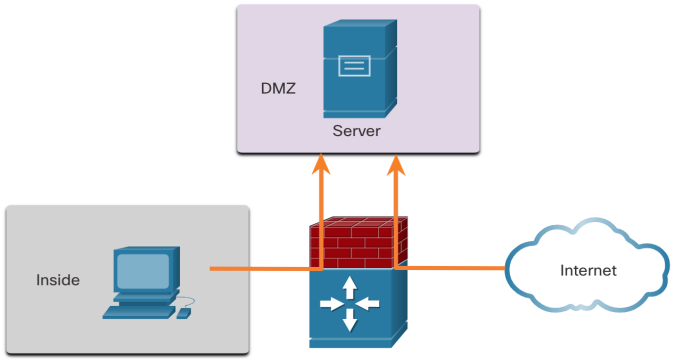


Firewalls

Network firewalls reside between two or more networks, control the traffic between them, and help prevent unauthorized access.

A **firewall** could allow outside users controlled access to specific services. For example, servers accessible to outside users are usually located on a special network referred to as the demilitarized zone (DMZ). The DMZ enables a network administrator to apply specific policies for hosts connected to that network.





Types of Firewalls

Firewall products come packaged in various forms. These products use different techniques for determining what will be permitted or denied access to a network. They include the following:

- **Packet filtering** - Prevents or allows access based on IP or MAC addresses
- **Application filtering** - Prevents or allows access by specific application types based on port numbers
- **URL filtering** - Prevents or allows access to websites based on specific URLs or keywords
- **Stateful packet inspection (SPI)** - Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS).

Network Attack Mitigations

Endpoint Security

An endpoint, or host, is an individual computer system or device that acts as a network client. Common endpoints are laptops, desktops, servers, smartphones, and tablets.

- Securing **endpoint devices** is one of the most challenging jobs of a network administrator because it involves human nature. A company must have well-documented policies in place and employees must be aware of these rules.

- Employees need to be **trained on proper use** of the network. Policies often include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control.

13.1.4 Device Security

Device Security

Cisco AutoSecure

The **security settings** are set to the **default values** when a new operating system is installed on a device. In most cases, this level of security is inadequate. For Cisco routers, the **Cisco AutoSecure** feature can be used to assist securing the system.

In addition, there are some simple steps that should be taken that apply to most operating systems:

- Default usernames and passwords should be changed immediately.
- Access to system resources should be restricted to only the individuals that are authorized to use those resources.
- Any unnecessary services and applications should be turned off and uninstalled when possible.
- Often, devices shipped from the manufacturer have been sitting in a warehouse for a period of time and do not have the most up-to-date patches installed. It is important to update any software and install any security patches prior to implementation.

Device Security
Passwords

To protect network devices, it is important to use strong passwords. Here are standard guidelines to follow:

- Use a password length of at least eight characters, preferably 10 or more characters.
- Make passwords complex. Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces, if allowed.
- Avoid passwords based on repetition, common dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, such as birthdates, ID numbers, ancestor names, or other easily identifiable pieces of information.
- Deliberately misspell a password. For example, Smith = Smyth = 5mYth or Security = 5ecur1ty.

Device Security

Passwords (Cont.)

To protect network devices, it is important to use strong passwords. Here are standard guidelines to follow:

- Change passwords often. If a password is unknowingly compromised, the window of opportunity for the threat actor to use the password is limited.
- Do not write passwords down and leave them in obvious places such as on the desk or monitor.

On Cisco routers, leading spaces are ignored for passwords, but spaces after the first character are not. Therefore, one method to create a strong password is to use the space bar and create a phrase made of many words. This is called a passphrase. A passphrase is often easier to remember than a simple password. It is also longer and harder to guess.

Network Attack Mitigations

Additional Password Security

There are several steps that can be taken to help ensure that passwords remain secret on a Cisco router and switch including these:

- Encrypt all plaintext passwords with the **service password-encryption** command
- Set a minimum acceptable password length with the **security passwords min-length** command.
- Deter brute-force password guessing attacks with the **login block-for # attempts # within #** command.
- Disable an inactive privileged EXEC mode access after a specified amount of time with the **exec-timeout** command.

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

Device Security
Enable SSH

It is possible to configure a Cisco device to support SSH using the following steps:

1) **Configure a unique device hostname**. A device must have a unique hostname other than the default.
2) **Configure the IP domain name**. Configure the IP domain name of the network by using the global configuration mode command **ip-domain name**.
3) **Generate a key to encrypt SSH traffic**. SSH encrypts traffic between source and destination. However, to do so, a unique authentication key must be generated by using the global configuration command **crypto key generate rsa general-keys modulus** *bits*.
   - The modulus *bits* determines the size of the key and can be configured from 360 bits to 2048 bits. The larger the bit value, the more secure the key. However, larger bit values also take longer to encrypt and decrypt information. The minimum recommended modulus length is 1024 bits.

Enable SSH (Cont.)

It is possible to configure a Cisco device to support SSH using the following steps:

4) **Verify or create a local database entry**. Create a local database username entry using the **username** global configuration command.
5) **Authenticate against the local database**. Use the **login local** line configuration command to authenticate the vty line against the local database.
6) **Enable vty inbound SSH sessions**. By default, no input session is allowed on vty lines. You can specify multiple input protocols including Telnet and SSH using the **transport input [ssh | telnet]** command.

Device Security

Disable Unused Services

Cisco routers and switches start with a list of active services that may or may not be required in your network. Disable any unused services to preserve system resources, such as CPU cycles and RAM, and prevent threat actors from exploiting these services.

- The type of services that are on by default will vary depending on the IOS version. For example, IOS-XE typically will have only HTTPS and DHCP ports open. You can verify this with the **show ip ports all** command.
- IOS versions prior to IOS-XE use the **show control-plane host open-ports** command.

Device Security

Packet Tracer – Configure Secure Passwords and SSH

In this Packet Tracer, you will configure passwords and SSH:

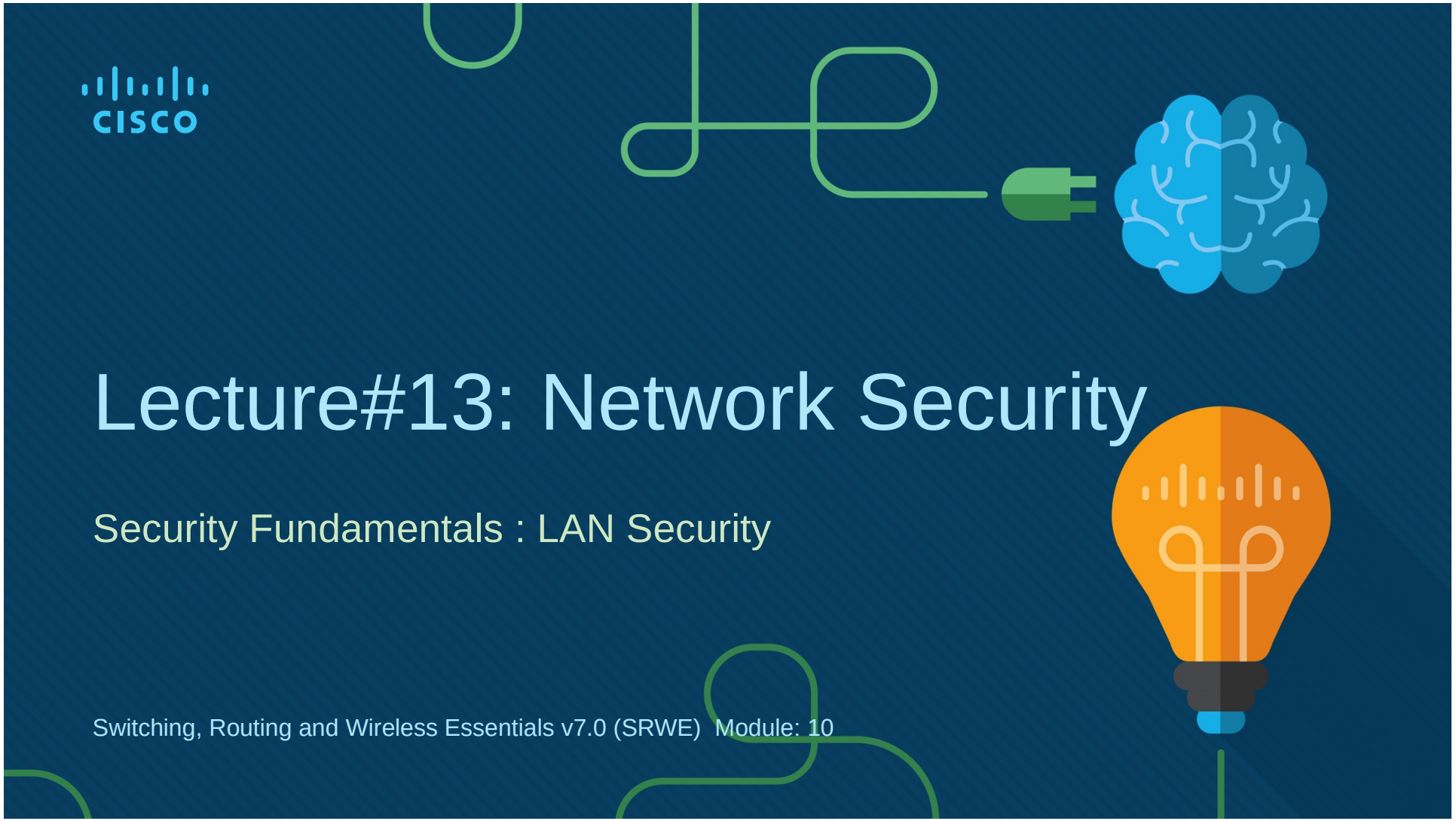
- The network administrator has asked you to prepare RTA and SW1 for deployment. Before they can be connected to the network, security measures must be enabled.

Device Security

Lab – Configure Network Devices with SSH

In this lab, you will complete the following objectives:

- Part 1: Configure Basic Device Settings
- Part 2: Configure the Router for SSH Access
- Part 3: Configure the Switch for SSH Access
- Part 4: SSH from the CLI on the Switch



Lecture#13: Network Security

Security Fundamentals : LAN Security

Switching, Routing and Wireless Essentials v7.0 (SRWE) Module: 10

13.2.1 Endpoint Security

Endpoint Security

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 encrypts the data on a host and locks access to it until a ransom is paid.

Endpoint Security

Network Security Devices

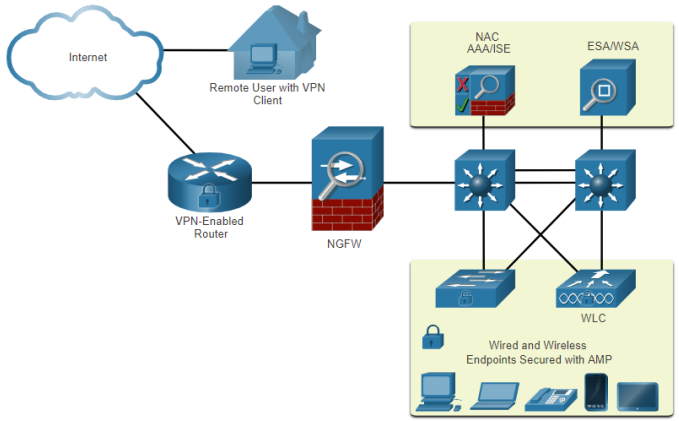
Various network security devices are required to protect the network perimeter from outside access. These devices could include the following:

- **Virtual Private Network** (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.
- **Next-Generation Firewall** (NGFW) - provides stateful packet inspection, application visibility and control, a next-generation intrusion prevention system (NGIPS), advanced malware protection (AMP), and URL filtering.
- **Network Access Control** (NAC) - includes authentication, authorization, and accounting (AAA) services. In larger enterprises, these services might be incorporated into an appliance that can manage access policies across a wide variety of users and device types. The Cisco Identity Services Engine (ISE) is an example of a NAC device.

Endpoint Security

Endpoint Protection

- Endpoints are hosts which commonly consist of laptops, desktops, servers, and IP phones, as well as employee-owned devices. Endpoints are particularly susceptible to malware-related attacks that originate through email or web browsing.
- Endpoints have typically used traditional host-based security features, such as antivirus/antimalware, host-based firewalls, and host-based intrusion prevention systems (HIPSs).
- Endpoints today are best protected by a combination of NAC, AMP software, an email security appliance (ESA), and a web security appliance (WSA).



Endpoint Security

Cisco Email Security Appliance

The Cisco ESA device 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
- Block access to newly infected sites.
- Encrypt content in outgoing email to prevent data loss.

Endpoint Security

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.

13.2.2 Access Control

Access Control

Authentication with a Local Password

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.

```
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.
- Authentication can be checked locally.

```
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:

- The method provides no fallback authentication method.
- User accounts must be configured locally on each device which is not scalable.

Access Control

AAA Components

AAA stands for **Authentication**, **Authorization**, and **Accounting**, and 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).

AAA authentication can be implemented in two ways :

1) Local AAA Authentication:

- Stores usernames and passwords locally in a network device (e.g., Cisco router).
- Users authenticate against the local database.
- Local AAA is ideal for small networks.

AAA Components (Cont.)

2) Server-Based AAA Authentication:

- With the server-based method, the router accesses a central AAA server.
- 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.

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

Access Control

AAA Components (Cont.)

- 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

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.

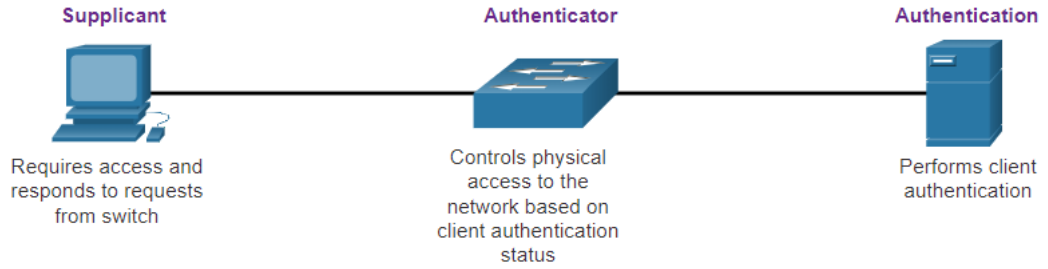
A **primary use of accounting** is to combine it with AAA authentication.

- 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

Access Control
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.



Access Control

802.1X (Cont.)

With 802.1X port-based authentication, the devices in the network have specific roles:

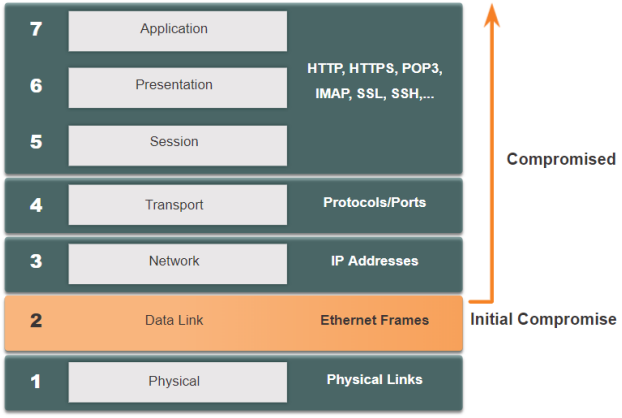
- **Client (Supplicant)** - This is a device running 802.1X-compliant client software, which is available for wired or wireless devices.
- **Switch (Authenticator)** –The switch acts as an intermediary between the client and the authentication server. It requests identifying information from the client, 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.

13.2.3 Layer 2 Security Threats

Layer 2 Vulnerabilities

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.



Layer 2 Security Threats

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.

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.

Layer 2 Security Threats

Switch Attack Mitigation Techniques

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. The following strategies are recommended:

- Always use secure variants of management protocols (SSH, SCP, SFTP, 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.

13.2.4 MAC Address Table Attack

MAC Address Table Attack

Switch Operation Review

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

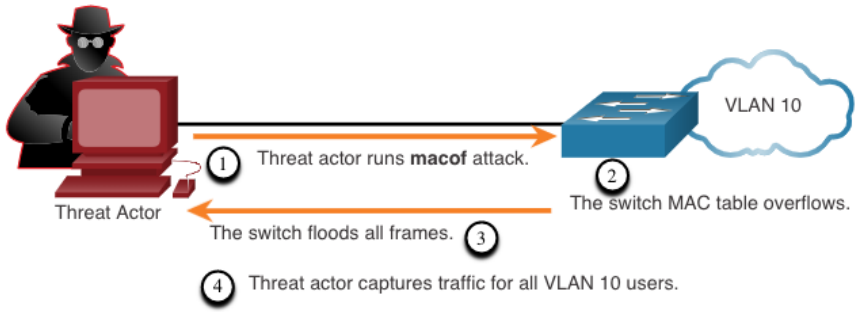
MAC Address Table Attack

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.



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.

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.

13.2.5 LAN Attacks

Video – VLAN and DHCP Attacks

This video will cover the following:

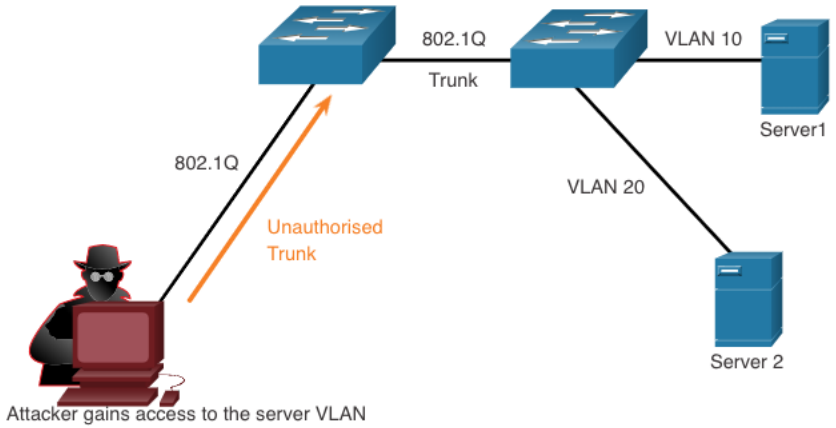
- VLAN Hopping Attack
- VLAN Double-Tagging Attack
- DHCP Starvation Attack
- DHCP Spoofing Attack

LAN Attacks

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.



VLAN Double-Tagging Attacks

A threat actor is 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.

- **Step 1:** 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.
- **Step 2**: The frame arrives on the first switch, which looks at the first 4-byte 802.1Q tag. The switch sees that the frame is destined for the native VLAN. The switch forwards the packet out all native VLAN ports after stripping the VLAN tag. The frame is not retagged because it is part of the native VLAN. At this point, the inner VLAN tag is still intact and has not been inspected by the first switch.
- **Step 3**: The frame arrives at the second switch which has no knowledge that it was supposed to be for the native VLAN. Native VLAN traffic is not tagged by the sending switch as specified in the 802.1Q specification. The second switch looks only at the inner 802.1Q tag that the threat actor inserted and sees that the frame is destined the target VLAN. The second switch sends the frame on to the target or floods it, depending on whether there is an existing MAC address table entry for the target.

VLAN Double-Tagging Attacks (Cont.)

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.

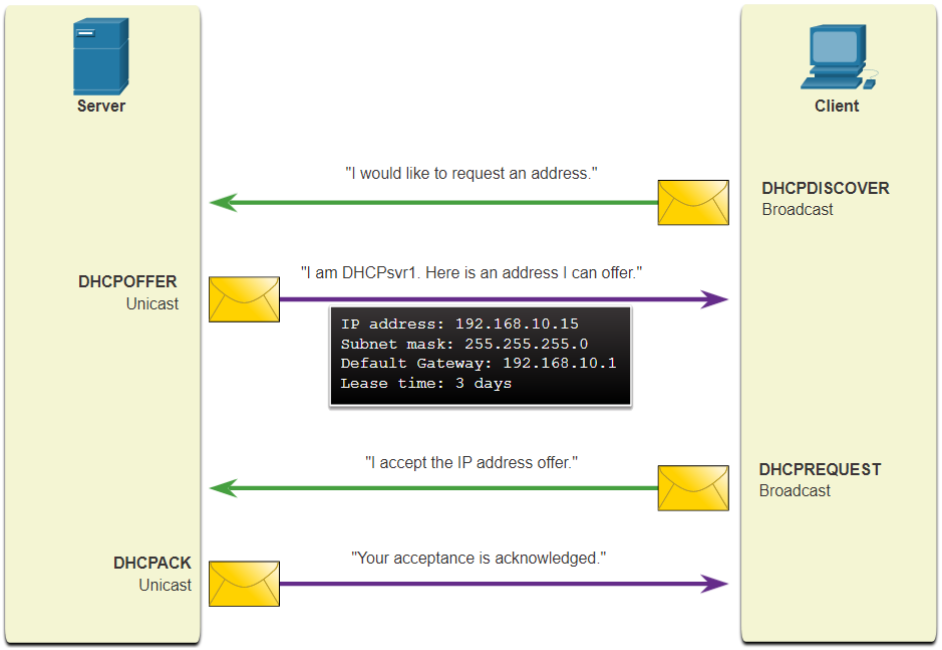
VLAN Attack Mitigation - VLAN hopping and VLAN double-tagging attacks can be prevented by implementing the following trunk security guidelines, as discussed in a previous module:

- 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.

LAN Attacks

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 show in the figure.



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 this 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 –** This 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, including the following:
  - **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.

LAN Attacks

Video – ARP Attacks, STP Attacks, and CDP Reconnaissance

This video will cover the following:

- ARP Spoofing Attack
- ARP Poisoning Attack
- STP Attack
- CDP Reconnaissance

LAN Attacks

ARP Attacks

- Hosts broadcast ARP Requests to determine the MAC address of a host with a destination IP address. 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.
- A client can send an unsolicited ARP Reply called a “gratuitous ARP”. Other hosts on the subnet store the MAC address and IP address contained in the gratuitous ARP in their ARP tables.
- 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. In a typical attack, a 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, effectively setting up a man-in-the-middle attack.
- There are many tools available on the internet to create ARP man-in-the-middle attacks.
- 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 Dynamic ARP Inspection (DAI).

LAN Attacks

Address Spoofing Attacks

- 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 switch overwrites the current MAC table entry and assigns the MAC address to the new port. It then inadvertently forwards frames destined for the target host to the attacking host.
- 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 IP Source Guard (IPSG).

LAN Attacks

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 then 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. The BPDUs sent by the attacking host announce a lower bridge priority in an attempt to be elected as the root bridge.
- This STP attack is mitigated by implementing BPDU Guard on all access ports. BPDU Guard is discussed in more detail later in the course.

CDP Reconnaissance

The Cisco Discovery Protocol (CDP) is a proprietary Layer 2 link discovery protocol. It is enabled on all Cisco devices by default. Network administrators also use CDP to help configure and troubleshoot network devices. CDP information is sent out CDP-enabled ports in periodic, unencrypted, unauthenticated 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.

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**.


CISCO