CHAPTER 6

Securing the Local Area Network

6.0 Introduction

6.0.1.1 Securing the Local Area Network

A secure network is only as strong as its weakest link. For this reason, in addition to securing the network edge, it is also important to secure the end devices that reside on the network. Endpoint security includes securing the network infrastructure devices on the local-area network (LAN) and end systems, such as workstations, servers, IP phones, access points, and storage area networking (SAN) devices. There are several endpoint security applications and devices available to accomplish this, including Cisco Advanced Malware Protection, Email and Web Security appliances, and Network Admission Control (NAC).

Endpoint security also encompasses securing Layer 2 of the network infrastructure to guard against Layer 2 attacks such as MAC address spoofing and STP manipulation attacks. Layer 2 security configurations include enabling port security, BPDU guard, Root guard, and PVLAN Edge.

Refer to Online Course for Illustration

6.1 Endpoint Security

6.1.1 Introducing Endpoint Security

6.1.1.1 Securing LAN Elements

News media commonly cover external network attacks on enterprise networks. These are some examples of such attacks:

- DoS attacks an organization's network to degrade or even halt public access to it
- Breach of an organization's Web server to deface their web presence
- Breach of an organization's data servers and hosts to steal confidential information

Various network security devices are required to protect the network perimeter from outside access. As shown in the figure, these devices could include a hardened ISR that is providing VPN services, an ASA firewall appliance, an IPS appliance, and a AAA ACS server.

Many attacks can, and do, originate from inside the network. Therefore, securing an internal LAN is just as important as securing the outside network perimeter. Without a secure LAN, users within an organization are still susceptible to network threats and outages that can

directly affect an organization's productivity and profit margin. After an internal host is infiltrated, it can become a starting point for an attacker to gain access to critical system devices, such as servers and more sensitive information.

Specifically, there are two internal LAN elements to secure:

- **Endpoints** - Hosts commonly consist of laptops, desktops, servers, and IP phones which are susceptible to malware-related attacks.
- **Network infrastructure** - LAN infrastructure devices interconnect endpoints and typically include switches, wireless devices, and IP telephony devices. Most of these devices are susceptible to LAN-related attacks including MAC address table overflow attacks, spoofing attacks, DHCP related attacks, LAN storm attacks, STP manipulation attacks, and VLAN attacks.

This section focuses on securing endpoints.

Refer to **Online Course** for Illustration

6.1.1.2 Traditional Endpoint Security

Historically, employee endpoints were company-issued computers which resided within a clearly defined LAN perimeter. These hosts were protected by firewalls and IPS scanning devices which worked well with hosts that were connected to the LAN and behind the firewall.

The endpoints also used traditional host-based security features, as shown in the figure.

Refer to **Online Course** for Illustration

6.1.1.3 The Borderless Network

The network has evolved to include traditional endpoints and new, lightweight, portable, consumerized endpoints such as iPhones, iPads, Android devices, tablets, and more. These new endpoints have blurred the network border because access to network resources can be initiated by users from many locations using various connectivity methods.

There are some problems with the traditional method of securing endpoints. In many networks, the network-based devices are disparate and typically do not share information among themselves. Additionally, new endpoint devices are not good candidates for the traditional host-based endpoint security solutions because of the variety of devices and the variety of operating systems available on those devices.

The challenge is allowing these heterogeneous devices to connect to enterprise resources securely.

Refer to **Online Course** for Illustration

6.1.1.4 Securing Endpoints in the Borderless Network

Larger organizations now require protection before, during, and after an attack. IT administrators must be able to answer the questions shown in Figure 1.

Organizations must also protect their endpoints from new threats and provide the protection outlined in Figure 2.

Refer to **Online Course** for Illustration

6.1.1.5 Modern Endpoint Security Solutions

New security architectures for the borderless network address these challenges by having endpoints use network scanning elements. These devices provide many more layers of

scanning than a single endpoint possibly could. They are also capable of sharing information among themselves to make better informed decisions.

Protecting endpoints in a borderless network can be accomplished using the following modern security solutions:

- Antimalware Protection (AMP)
- Email Security Appliance (ESA)
- Web Security Appliances (WSA)
- Network Admission Control (NAC)

These technologies work in concert with each other to give more protection than host-based suites can provide.

The next section will highlight these technologies.

Refer to Online Course for Illustration

6.1.1.6 Hardware and Software Encryption of Local Data

Endpoints are also susceptible to data theft. For instance, if a corporate laptop is lost or stolen, a thief could scour the hard drive for sensitive information, contact information, personal information, and more.

The solution is to locally encrypt the disk drive with a strong encryption algorithm such as 256-bit AES encryption. The encryption protects the confidential data from unauthorized access. The encrypted disk volumes can only be mounted for normal read/write access with the authorized password.

Some operating systems such as MAC OSX natively provide encryption options. The Windows operating system supports encryption software such as BitLocker, TrueCrypt, Credant, VeraCrypt, and others.

Refer to Interactive Graphic in online course

6.1.1.7 Activity – Identify Endpoint Security Terminology (DND)

Refer to Online Course for Illustration

6.1.2 Antimalware Protection

6.1.2.1 Advanced Malware Protection

Malware knows no boundaries and the most common and pervasive threat to endpoints is malware. For this reason, in 2013, Cisco acquired Sourcefire, the leading antimalware company. Sourcefire provides a variety of security-related resources which are now being integrated into Cisco products.

Specifically, Cisco added Sourcefire's Advanced Malware Protection (AMP) technology to protect endpoints and networks more effectively than traditional host-based malware protection. As shown in the figure, AMP provides organizations with continuous visibility and control to defeat malware across the extended network before, during, and after an attack.

The AMP solution can enable malware detection and blocking, continuous analysis and retrospective alerting with:

- **File Reputation** – Analyze files inline and block or apply policies
- **File Sandboxing** – Analyze unknown files to understand true file behavior
- **File Retrospection** – Continue to analyze files for changing threat levels.

Refer to Video in online course

6.1.2.2 AMP and Managed Threat Defense

AMP uses the vast cloud security intelligence networks of both Cisco and Sourcefire to provide advanced protection.

Specifically, AMP accesses the collective security intelligence of the Cisco Talos Security Intelligence and Research Group (Talos). Talos is the result of merging the Cisco Security Intelligence Operation (SIO) team and the Sourcefire Vulnerability Research Team (VRT) team. Talos detects and correlates threats in real time using the largest threat-detection network in the world.

Talos employs more than 600 engineers, technicians, and researchers that work around the clock, 365 days a year, in more than 40 languages, to analyze this information, as well as public and private threat feeds.

These teams gather real-time threat intelligence from a variety of sources:

- 1.6 million deployed security devices, including firewall, IPS, web, and email appliances
- 150 million endpoints

They then analyze this data:

- 100 TB of security intelligence daily
- 13 billion web requests per day
- 35% of the world's enterprise email traffic

Click here to read the transcript of this video.

Refer to Video in online course

6.1.2.3 AMP for Endpoints

AMP protects before, during, and after an attack. AMP is available in a variety of formats:

- **AMP for Endpoints** - AMP for Endpoints integrates with Cisco AMP for Networks to deliver comprehensive protection across extended networks and endpoints.
- **AMP for Networks** - Provides a network-based solution and is integrated into dedicated Cisco ASA Firewall and Cisco FirePOWER network security appliances.
- **AMP for Content Security** – This is an integrated feature in Cisco Cloud Web Security or Cisco Web and Email Security Appliances to protect against email and web-based advanced malware attacks.

Cisco AMP for Endpoints runs a FireAMP agent and becomes a FireAMP connector. AMP for Endpoints integrates with Cisco AMP for Networks to deliver comprehensive protection through a single pane of glass and across extended networks and endpoints. It uses continuous analysis, retrospective security, and multisource indications of compromise. This helps an administrator identify stealthy attacks that manage to traverse from the endpoint to inline at the network level, correlate those events for faster response, and achieve greater visibility and control.

Click here to read the transcript of this video.

Refer to Online Course for Illustration

6.1.3 Email and Web Security

6.1.3.1 Securing Email and Web

Over the past 25 years, email has evolved from a tool used primarily by technical and research professionals to become the backbone of corporate communications. Each day, more than 100 billion corporate email messages are exchanged. As the level of use rises, security becomes a greater priority.

Mass spam campaigns are no longer the only concern. Today, spam and malware are just part of a complex picture that includes inbound threats and outbound risks. For this reason, Cisco acquired IronPort Systems in 2007. IronPort appliances are now part of the Cisco Email Security Appliance (ESA) and Cisco Web Security Appliance (WSA) product lines.

Refer to Video in online course

6.1.3.2 Cisco Email Security Appliance

To defend mission-critical email systems, Cisco offers a variety of email security solutions, including the ESA as well as virtual, Cloud, and hybrid solutions. These solutions provide:

- Fast, comprehensive, email protection that can block spam and threats before they reach your network.
- Flexible Cloud, virtual and physical deployment options to meet changing business needs.
- Outbound message control through on-device data-loss prevention (DLP) and email encryption.

The Cisco ESA fights spam, viruses, and blended threats for organizations of any size. It enforces compliance and protects reputation and brand assets, reduces downtime, and simplifies administration of corporate mail systems.

The Cisco ESA is constantly updated by real-time feeds from the Cisco Talos, which detects and correlates threats using a worldwide database monitoring system. The solution then automatically forwards security updates to the Cisco Talos. This threat intelligence data is pulled by the Cisco ESAs every three to five minutes.

Cisco ESA defends mission-critical email systems with appliance, virtual, cloud, and hybrid solutions. These are some of the main features and benefits of Cisco Email Security solutions:

- **Global threat intelligence** - Cisco Talos provides a 24-hour view into global traffic activity. It analyzes anomalies, uncovers new threats, and monitors traffic trends.

- **Spam blocking** - A multilayered defense combines an outer layer of filtering based on the reputation of the sender and an inner layer of filtering that performs a deep analysis of the message.
- **Advanced malware protection** – Includes AMP that takes advantage of the vast cloud security intelligence network of Sourcefire. It delivers protection across the attack continuum: before, during, and after an attack.
- **Outbound message control** - Controls outbound messages through DLP and email encryption to help ensure that important messages comply with industry standards and are protected in transit.

Click Play in the figure to see a video about how the Cisco ESA protects an organization.

Click here to read the transcript of this video.

Refer to **Online Course** for Illustration

6.1.3.3 Cisco Web Security Appliance

The Cisco WSA is a mitigation technology for web-based threats that helps organizations address the growing challenges of securing and controlling web traffic. The Cisco WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, reporting, and secure mobility to provide an all-in-one solution on a single platform.

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, URL-filtering, malware scanning, URL categorization, Web application filtering, and TLS/SSL encryption and decryption.

These are some of the main features and benefits of Cisco Web Security Appliance solutions:

- **Talos Security Intelligence** - Fast and comprehensive web protection backed by a large threat detection network.
- **Cisco Web Usage Controls** - Combines traditional URL filtering with dynamic content analysis to mitigate compliance, liability, and productivity risks.
- **Advanced Malware Protection (AMP)** - AMP is an additionally licensed feature available to all Cisco WSA customers.
- **Data Loss Prevention (DLP)** - Prevent confidential data from leaving the network by creating context-based rules for basic DLP.

To help illustrate how the WSA interacts with other devices, refer to Figures 1 through 3. In Figure 1, the user initiates a web request for abc.com and sends it to the ASA firewall. The ASA redirects the request to the WSA for it to check the request. If the request violates the security policy, the WSA forwards a denial to the host. If the request is acceptable, the WSA initiates a web request to the destination Web server as shown in Figure 2. In Figure 3, the reply from the Web server is forwarded by the ASA to the WSA. The WSA again checks the content for objectionable content and if no issues are encountered, it then forwards the Web content to the host.

Note Cisco Web Security Virtual Appliance (WSAV) is a software version of the Cisco WSA that runs on top of a VMware ESXi or KVM hypervisor and Cisco Unified Computing System (UCS) servers.

Refer to Online Course for Illustration

6.1.3.4 Cisco Cloud Web Security

Cisco Cloud Web Security (CWS) is a cloud-based security service that uses web proxies in Cisco's cloud environment to scan traffic for malware and policy enforcement. CWS provides the following benefits:

- Granular web use policies can be set and enforced across the entire environment for applications, websites, and specific webpage content.
- Cisco CWS is easy to integrate into your existing infrastructure.
- Real-time threat intelligence is continuously updated to protect against the latest threats.
- Centralized management and reporting provides visibility into web usage and threat information.

Cisco customers can connect to the Cisco CWS service directly by using a proxy auto-configuration (PAC) file in the user's end device or through connectors integrated into four Cisco products:

- Cisco ISR G2 routers
- Cisco ASA
- Cisco WSA
- Cisco AnyConnect Secure Mobility Client

In the figure, the Cisco ASA is enabled with the Cisco CWS connector. The following explains how Cisco CWS protects corporate users through a four-step process:

1. An internal user makes an HTTP request to an external website (www.example.com).
2. The Cisco ASA forwards the HTTP request to Cisco CWS global cloud infrastructure.
3. Cisco CWS notices that www.example.com has web content, possibly a banner ad, that is redirecting the user to a known malicious site (www.malicious.com).
4. Cisco CWS blocks the request to the malicious site, but continues to allow access to the rest of the content at www.example.com.

Refer to Online Course for Illustration

6.1.4 Controlling Network Access

6.1.4.1 Cisco Network Admission Control

The purpose of Cisco Network Admission Control (NAC) is to allow only authorized and compliant systems, whether managed or unmanaged, to access the network. Cisco NAC is also designed to enforce network security policy. NAC helps maintain network stability by providing authentication, authorization, and posture assessment (evaluating an incoming device against the policies of the network). NAC also quarantines noncompliant systems and manages the remediation of noncompliant systems.

As displayed in the table in Figure 1, there are two categories of Cisco NAC products:

- **NAC framework** - The NAC framework uses the existing Cisco network infrastructure and third-party software to enforce security policy compliance on all endpoints. As shown in Figure 2, different devices in the network, not necessarily one device, can provide the features of NAC.
- **Cisco NAC appliance** - As part of the Cisco TrustSec solution, the Cisco NAC Appliance incorporates NAC functions into an appliance and provides a solution to control network access.

The Cisco NAC Appliance can be used to:

- Recognize users, their devices, and their roles in the network
- Evaluate whether machines are compliant with security policies
- Enforce security policies by blocking, isolating, and repairing noncompliant machines
- Provide easy and secure guest access
- Simplify non-authenticating device access
- Audit and report who is on the network

Cisco NAC Appliance extends NAC to all network access methods, including access through LANs, remote-access gateways, and wireless access points. It also supports posture assessment for guest users.

Note NACs are evolving away from basic security protection to more sophisticated **endpoint visibility, access, and security (EVAS)** controls. Unlike older NAC technologies, EVAS use more granular information to enforce access policies, such as data about user role, location, business process considerations, and risk management. EVAS controls also help grant access beyond computers, allowing network administrators to provide access through mobile and IoT devices.

Refer to Online Course for Illustration

6.1.4.2 Cisco NAC Functions

The goal of both the NAC framework and the Cisco NAC Appliance is to ensure that only hosts that are authenticated and have had their security posture examined and approved are permitted onto the network. For example, company laptops used offsite for a period of time might not have received current security updates or could have become infected from other systems. Those systems cannot connect to the network until they are examined, updated, and approved.

Network access devices function as the enforcement layer, as shown in the figure. They force the clients to query a RADIUS server for authentication and authorization. The RADIUS server can query other devices, such as a Trend Micro antivirus server, and reply to the network enforcers.

Refer to Online Course for Illustration

6.1.4.3 Cisco NAC Components

Cisco Secure Access Control products are part of the NAC Appliance-based Cisco TrustSec solution. TrustSec is a core component of the Secure Borderless Networks architecture. In the NAC Appliance-based TrustSec approach, Cisco NAC Manager (NAM) is a policy server that works with Cisco NAC Server (NAS) to authenticate users and assess their devices over LAN, wireless, or VPN connections, as shown in the figure. Access to the network and resources is based on user credentials and their roles in the organization, as well as the policy compliance of endpoint devices:

- **Cisco NAC Manager (NAM)** - The policy and management center for an appliance-based NAC deployment environment, Cisco NAC Manager defines role-based user access and endpoint security policies.
- **Cisco NAC Server (NAS)** - Assesses and enforces security policy compliance in an appliance-based NAC deployment environment.
- **Cisco NAC Agent (NAA)** - An optional lightweight agent running on an endpoint device. It performs deep inspection of the device's security profile by analyzing registry settings, services, and files.

These are two additional TrustSec Policy enforcement tools:

- **Cisco NAC guest server** - Manages guest network access, including provisioning, notification, management, and reporting of all guest user accounts and network activities.
- **Cisco NAC profiler** - Helps to deploy policy-based access control by providing discovery, profiling, policy-based placement, and post-connection monitoring of all endpoint devices.

Refer to Online Course for Illustration

6.1.4.4 Network Access for Guests

Cisco NAC Guest Server provides guest policy enforcement to either the Cisco NAC Appliance or the Cisco Wireless LAN Controller, where guest policies are enforced. Cisco NAC Guest Server, a component of the Cisco TrustSec solution, provides full guest access lifecycle support, including provisioning, notification, management, and reporting.

Cisco NAC Guest Server provides the ability for sponsors, such as employees of the company, to create guest accounts. Sponsors are authenticated on the guest server and are granted permissions based upon their roles. Sponsors can be given role-based permissions to create accounts, edit accounts, suspend accounts, and run reports.

There are three ways to grant sponsor permissions to:

- Only those accounts created by the sponsor
- All accounts
- No accounts (i.e., they cannot change any permissions)

After a guest account is created, guests can log onto the network with the details provided to them by the sponsor.

Creating a user account on a Cisco NAC Guest Server is shown in Figures 1 through 8.

Refer to Online Course for Illustration

6.1.4.5 Cisco NAC Profiler

Cisco NAC Profiler enables the dynamic discovery, identification, and monitoring of all network-attached endpoints within an enterprise network. It manages these devices intelligently, based on user-defined security policies.

When deployed as part of a broader NAC implementation, Cisco NAC Profiler facilitates deployment and management of Cisco NAC systems. It discovers and tracks the location and type of all LAN-attached endpoints, including those that cannot authenticate.

Cisco NAC Profiler enables security administrators to:

- Simplify deployment of Cisco NAC by automating device identification and authentication and easing administrative tasks.
- Facilitate deployment and management of the Cisco ACS 802.1X-based infrastructure or Cisco NAC overlay solutions.
- Gather endpoint device profiling information and maintain a real-time, contextual inventory of networked devices.
- Monitor and manage device behavior anomalies, such as port swapping, MAC address spoofing, and profile changes.
- Secure all company-owned endpoints, including non-authenticating devices such as printers and IP phones.

Cisco NAC Profiler has two components: the NAC Profiler Collector, shown in Figures 1 and 4, and the NAC Profiler Server application, shown in Figure 2 and 3. Figures 1 through 4 illustrate sequentially how the Cisco NAC Profiler collects, aggregates, filters, and updates device data.

Refer to Online Course for Illustration

6.2 Layer 2 Security Considerations

6.2.1 Layer 2 Security Threats

6.2.1.1 Describe Layer 2 Vulnerabilities

The OSI reference model is divided into seven layers which work independently of each other. As shown in Figure 1, each layer performs a specific function and has core elements that can be exploited.

Network administrators routinely implement security solutions to protect the elements in Layer 3 up through Layer 7 using VPNs, firewalls, and IPS devices. However, as shown in Figure 2, if Layer 2 is compromised, then all layers above it are also affected. For example, if an employee or visitor with access to the internal network could capture Layer 2 frames, then all of the security implemented on the layers above would be useless. The employee could also wreak havoc on the Layer 2 LAN networking infrastructure.

Refer to Online Course for Illustration

6.2.1.2 Switch Attack Categories

Security is only as strong as the weakest link in the system, and Layer 2 is considered to be that weakest link. This is because traditionally LANs were 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 highlighted in Figure 1.

Note The focus of this section is on common Layer 2 attacks.

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

These Layer 2 solutions will not be effective if the management protocols are not secured. An example would be if attackers can easily telnet into a switch. Syslog, SNMP, TFTP, telnet, FTP and most other common network management protocols are insecure. Therefore, the following strategies are recommended:

- Always use secure variants of these protocols such as SSH, SCP, and SSL.
- Consider using out-of-band (OOB) management.
- Use a dedicated management VLAN where nothing but management traffic resides.
- Use ACLs to filter unwanted access.

Refer to **Interactive Graphic** in online course

6.2.1.3 Activity – Identify Switch Attack Types

Refer to **Online Course** for Illustration

6.2.2 CAM Table Attacks

6.2.2.1 Basic Switch Operation

To make forwarding decisions, a Layer 2 LAN switch builds a table of MAC addresses that is stored in its Content Addressable Memory (CAM). A CAM table is the same thing as a MAC address table. In this course, we will use the term CAM table. One important exception to this is that the syntax to show what addresses are stored in a switch uses "mac address table", as shown in the figure.

The CAM table binds and stores MAC addresses and associated VLAN parameters that are connected to the physical switch ports. Switches then compare the destination MAC unicast addresses of incoming frames to the entries in the CAM table to make port forwarding decisions. If the destination MAC address is in the CAM table, the switch forwards the frame accordingly. However, if the destination MAC address is not in the CAM table, the switch will flood the frame out of all ports except for the frame's port of ingress. This is called an unknown unicast flood.

The output in the figure displays the content of a sample CAM table.

Refer to **Online Course** for Illustration

6.2.2.2 CAM Table Operation Example

Refer to the sample topology in Figure 1, consisting of a Layer 2 switch interconnecting four hosts. The CAM table is currently empty because switch S1 has been rebooted and is now operational. To view the content of a CAM table, use the **show mac-address-table** privileged EXEC command, as shown in Figure 2.

In this scenario, the user on PC-A is pinging the IP address of PC-B. Therefore, PC-A will first reference its locally stored Address Resolution Protocol (ARP) cache to discover the MAC address of PC-B. If that the entry is not cached, PC-A must discover the MAC address of PC-B using ARP.

PC-A sends an ARP request to S1 containing the destination broadcast MAC address, PC-A MAC Address, PC-A IP address and PC-B IP address, as shown in Figure 3. When S1 receives the frame on port F0/1, it immediately records the source MAC address of PC-A to port F0/1 in its CAM table. Because the destination MAC address is a broadcast, S1 then floods the ARP request frame out of all ports except for the frame's port of ingress (F0/1).

PC-B recognizes that the frame destination contains its IP address and responds by sending an ARP Reply containing the destination MAC address of PC-A, its own MAC Address, PC-B IP address and the destination IP address of PC-A as shown in Figure 4. When S1 receives the frame, it immediately records the source MAC address of PC-B to port F0/2. Figure 5 displays the resulting content of the CAM table on S1.

S1 then references the ARP Reply destination MAC address in its CAM table and discovers that it is connected to port F0/1. S1 forwards the ARP reply only to PC-A. PC-A now has the complete information and can successfully ping PC-B.

If PC-C pings PC-D, then the preceding scenario is repeated, and the resulting CAM table is displayed in Figure 6.

Refer to **Online Course** for Illustration

6.2.2.3 CAM Table Attack

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

If enough entries are entered into the CAM table before older entries expire, the table fills up to the point that no new entries can be accepted. When this occurs, the switch treats the frame as an unknown unicast and begins to flood all incoming traffic to all ports without referencing the CAM table. The switch, in essence, acts as a hub. As a result, the attacker can capture all of the frames sent from one host to another.

Note Traffic is flooded only within the local VLAN, so the intruder sees only traffic within the local VLAN to which the intruder is connected. In the previous page, the attacker would only be able to capture traffic on the default (VLAN 1).

For example, macof is a network attack tool capable of generating a large number of random source and destination MAC and IP addresses very quickly, as shown in Figure 1. Over a short period of time, the CAM table fills up (Figure 2), and when full, the switch begins to flood all frames that it receives (Figure 3). As long as the attack tool continues the attack, the CAM table remains full, and the switch continues to flood all incoming

frames out of every port. This allows the attacker to capture various frames and to send packets to devices that would otherwise be unreachable (Figure 4).

If the intruder does not maintain the flood of invalid source MAC addresses, the switch eventually ages out the older MAC address entries from the table and begins to act like a switch again. If the attack is not discovered quickly before the entries age out, the cause of the problem may be difficult to determine, and the attacker would remain anonymous.

Note Another network attack tool is Yersinia which was designed to exploit weaknesses in protocols including Spanning Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), Dynamic Host Configuration Protocol (DHCP), Hot Standby Router Protocol (HSRP), IEEE 802.1Q, IEEE 802.1X, and VLAN Trunking Protocol (VTP).

Refer to Online Course for Illustration

6.2.2.4 CAM Table Attack Tools

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

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 CAM table of a switch is full, it starts broadcasting out all ports including those connecting to other Layer 2 switches.

To mitigate CAM table overflow attacks, network administrators must implement port security.

Refer to Online Course for Illustration

6.2.3 Mitigating CAM Table Attacks

6.2.3.1 Countermeasure for CAM Table Attacks

The simplest and most effective method to prevent CAM table overflow attacks is to enable port security. Port security allows an administrator to statically specify MAC addresses for a port or to permit the switch to dynamically learn a limited number of MAC addresses. By limiting the number of permitted MAC addresses on a port to one, port security can be used to control unauthorized expansion of the network, as shown in the figure.

When MAC addresses are assigned to a secure port, the port does not forward frames with source MAC addresses outside the group of defined addresses. When a port configured with port security receives a frame, the source MAC address of the frame is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port.

Refer to Online Course for Illustration

6.2.3.2 Port Security

To enable port security, use the **switchport port-security** interface configuration command on an access port, as shown in the example in Figure 1. Notice in the example, the port must be configured as an access port before port security can be enabled. This is

because port security can only be configured on access ports and, by default, Layer 2 switch ports are set to dynamic auto (trunking on). Therefore, the port must be initially configured with the **switchport mode access** interface configuration command.

Figure 2 is displaying the default port security settings of interface FastEthernet 0/1. Notice how the port security is enabled, the violation mode is shutdown, and how the maximum number of MAC addresses is 1.

Once port security is enabled, other port security specifics can be configured as shown in the output of Figure 3.

Note Available configuration parameters are dependent on the switch model and IOS version.

Refer to **Online Course** for Illustration

6.2.3.3 Enabling Port Security Options

To set the maximum number of MAC addresses allowed on a port use the **switchport port-security maximum** *value* command shown in Figure 1. The default port security value is 1.

Note The actual maximum number of secure MAC addresses that can be configured is set by the maximum number of available MAC addresses allowed by the active Switch Database Management (SDM) template. Use the **show sdm prefer** command to view the current template settings.

Figure 2 displays a sample configuration changing the default maximum MAC addresses to four.

The switch can be configured to learn about MAC addresses on a secure port in one of two ways:

- **Manually configured** - The administrator manually configures the MAC address(es) using the **switchport port-security mac-address** interface configuration command shown in Figure 3.
- **Dynamically learned** - The administrator enables the switch to dynamically learn the MAC address using the **switchport port-security mac-address sticky** interface configuration command shown in Figure 4.

Figure 5 displays a sample configuration of manually configuring a MAC address and enabling dynamic learning for the remainder of the total allowed as configured by the maximum value.

Figure 6 shows the use of the **show port-security [interface** *interface-id*] address command to view all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.

Refer to **Online Course** for Illustration

6.2.3.4 Port Security Violations

If a MAC address of a device attached to the port differs from the list of secure addresses, then a port violation occurs, and the port enters the error-disabled state. A security violation is created when a station with a MAC address that is not in the address table attempts

to access the interface when the table is full. Another example of a situation that creates a security violation is when an address is being used on two secure interfaces in the same VLAN.

How a switch behaves depends on the configured violation. There are three security violation modes, as shown in Figure 1. The table in Figure 2 differentiates between these three modes.

To set the port security violation mode, use the **switchport port-security violation {protect | restrict | shutdown | shutdown vlan}** interface configuration command.

Figure 3 displays a sample configuration of changing the security violation to "restrict". The output of the **show port-security interface** command confirms that the change has been made.

To re-enable an error-disable port, manually re-enable the disabled port by entering the **shutdown** and **no shutdown** interface configuration commands.

Note Alternatively, the switch could be configured to automatically re-enable an error-disabled port using the **errdisable recovery cause psecure-violation global** configuration mode command.

Use the Syntax Checker in Figure 4 to configure port security on the S1 interface FastEthernet 0/19.

Refer to **Online Course** for Illustration

6.2.3.5 Port Security Aging

Port security aging can be used to set the aging time for static and dynamic secure addresses on a port. Two types of aging are supported per port:

- **Absolute** - The secure addresses on the port are deleted after the specified aging time.
- **Inactivity** - The secure addresses on the port are deleted only if they are inactive for the specified aging time.

Use aging to remove secure MAC addresses on a secure port without manually deleting the existing secure MAC addresses. Aging time limits can also be increased to ensure past secure MAC addresses remain, even while new MAC addresses are added. Keep in mind the maximum number of secure addresses per port can be configured. Aging of statically configured secure addresses can be enabled or disabled on a per-port basis.

Use the **switchport port-security aging** command shown in Figure 1 to enable or disable static aging for the secure port, or to set the aging time or type.

Figure 2 displays a sample configuration of changing the aging type to 10 minutes of inactivity.

Refer to **Online Course** for Illustration

6.2.3.6 Port Security with IP Phones

An access port connecting an IP phone and a computer, as shown in Figure 1, typically requires two secure MAC addresses. However, on some switches this number should be set to three because when the port is connected to a Cisco IP phone, the IP phone requires up to two MAC addresses. The IP phone address is learned on the voice VLAN and might

also be learned on the access VLAN. Connecting a PC to the IP phone requires an additional MAC address.

The addresses are usually learned dynamically. However, when configuring port security with an IP phone, the voice addresses cannot be made sticky.

As shown in Figure 2, a maximum of 3 MAC addresses can be learned on this port. Violations of this policy result in the port being shut down. The aging timeout for the learned MAC addresses is set to two hours.

Refer to Online Course for Illustration

6.2.3.7 SNMP MAC Address Notification

Network managers need a way of monitoring who is using the network and what their location is. For example, if port F0/1 is secure on a switch, an SNMP trap is generated when a MAC address entry for that port disappears from the CAM table.

The MAC address notification feature sends SNMP traps to the network management station (NMS) whenever a new MAC address is added to, or an old address is deleted from the forwarding tables. MAC address notifications are generated only for dynamic and secure MAC addresses.

MAC address notification allows the network administrator to monitor MAC addresses that are learned, as well as MAC addresses that age out and are removed from the switch. For example, in the figure the laptop with MAC C has disconnected from the network. The switch will eventually timeout port F0/3 and send an SNMP trap notification to the NMS Server.

Use the **mac address-table notification** global configuration command to enable the MAC address notification feature on a switch.

Refer to Online Course for Illustration

6.2.4 Mitigating VLAN Attacks

6.2.4.1 VLAN Hopping Attacks

The VLAN architecture simplifies network maintenance and improves performance, but it also opens the door to abuse.

A specific type of VLAN threat is a VLAN hopping attack. 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 attacker takes advantage of the automatic trunking port feature enabled by default on most switch ports. The network attacker configures a host to spoof a switch to use 802.1Q signaling and Cisco-proprietary Dynamic Trunking Protocol (DTP) signaling to trunk with the connecting switch. If successful and the switch establishes a trunk link with the host, then the attacker can access all the VLANS on the switch and hop (i.e., send and receive) traffic on all the VLANs.

Click Play in the figure to view an animation that illustrates a VLAN hopping attack.

A VLAN hopping attack can be launched in one of two ways:

- Spoofing DTP messages from the attacking host to cause the switch to enter trunking mode. From here, the attacker can send traffic tagged with the target VLAN, and the switch then delivers the packets to the destination.
- Introducing a rogue switch and enabling trunking. The attacker can then access all the VLANs on the victim switch from the rogue switch.

Refer to Online Course for Illustration

6.2.4.2 VLAN Double-Tagging Attack

Another type of VLAN hopping attack is a double-tagging (or double-encapsulated) attack. This attack takes advantage of the way hardware on most switches operates.

Most switches perform only one level of 802.1Q de-encapsulation. This can allow an attacker in specific situations to embed a hidden 802.1Q tag inside the frame. This tag allows the frame to go to a VLAN that the original 802.1Q tag did not specify. An important characteristic of the double-encapsulated VLAN hopping attack is that it works even if trunk ports are disabled, as a host typically sends a frame on a segment that is not a trunk link.

A double-tagging attack follows three steps:

- In Figure 1, the attacker sends a double-tagged 802.1Q frame to the switch. The outer header has the VLAN tag of the attacker, 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.
- In Figure 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 VLAN 10, which is the native VLAN. The switch forwards the packet out on all VLAN 10 ports after stripping the VLAN 10 tag. On the trunk port, the VLAN 10 tag is stripped, and the packet is not retagged because it is part of the Native VLAN. At this point, the VLAN 20 tag is still intact and has not been inspected by the first switch.
- In Figure 3, the frame arrives at the second switch but has no knowledge that it was supposed to be for VLAN 10. 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 attacker sent and sees that the frame is destined for VLAN 20, the target VLAN. The second switch sends the frame on to the victim port or floods it, depending on whether there is an existing MAC address table entry for the victim host.

This type of 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.

Refer to Online Course for Illustration

6.2.4.3 Mitigating VLAN Hopping Attacks

Figure 1 shows the best way to prevent basic VLAN hopping attacks:

- Disable DTP (auto trunking) negotiations on non-trunking ports by using the **switchport mode access** interface configuration command.
- Manually enable the trunk link on a trunking port using the **switchport mode trunk** interface configuration command.
- Disable DTP (auto trunking) negotiations on trunking ports using the **switchport nonnegotiate** interface configuration command.

- Set the native VLAN to be something other than VLAN 1 and to be set on an unused VLAN using the **switchport trunk native vlan** *vlan_number* interface configuration mode command.
- Disable unused ports and put them in an unused VLAN.

For example, in the configuration shown in Figure 2:

- FastEthernet ports 0/1 to 0/16 are access ports and therefore trunking is disabled by explicitly making them access ports.
- FastEthernet ports 0/1 to 0/16 are unused ports and are disabled and assigned to an unused VLAN.
- FastEthernet ports 0/21 to 0/24 are trunk links and are manually enabled as trunks with DTP disabled. The native VLAN is also changed from the default VLAN 1 to an unused VLAN 999.

Use the Syntax Checker in Figure 3 to configure trunk links to mitigate VLAN attacks.

Refer to **Online Course** for Illustration

6.2.4.4 PVLAN Edge Feature

Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor.

In such an environment, the use of the PVLAN (Private VLAN) Edge feature ensures that there is no exchange of unicast, broadcast, or multicast traffic between PVLAN edge ports on the switch, as shown in the figure. The PLVAN Edge feature is also called Protected Ports.

The PVLAN Edge feature has the following characteristics:

- A protected port does not forward any traffic, such as unicast, multicast, or broadcast, to any other port that is also a protected port. Data traffic cannot be forwarded between protected ports at Layer 2; only control traffic is forwarded because these packets are processed by the CPU and forwarded in software. All data traffic passing between protected ports must be forwarded through a Layer 3 device.
- Forwarding behavior between a protected port and a non-protected port proceeds as usual.
- The default is to have no protected ports defined.

Refer to **Online Course** for Illustration

6.2.4.5 PVLAN Edge

To configure the PVLAN Edge feature, enter the **switchport protected** interface configuration mode command.

The PVLAN Edge feature can be configured on a physical interface or an EtherChannel group. When the PVLAN Edge feature is enabled for a port channel, it is enabled for all ports in the port-channel group. To disable protected port, use the **no switchport protected** interface configuration mode command.

To verify the configuration of the PVLAN Edge feature, use the **show interfaces interface-id switchport** global configuration mode command, as shown in the figure.

The PVLAN edge is a feature that has only local significance to the switch, and there is no isolation provided between two protected ports located on different switches. A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port on the same switch. Traffic cannot be forwarded between protected ports at Layer 2 (L2); all traffic passing between protected ports must be forwarded through a Layer 3 (L3) device.

Refer to Online Course for Illustration

6.2.4.6 Private VLANs

VLANs are broadcast domains. However, in some situations, it may useful to break this rule and allow only the minimum required L2 connectivity within the VLAN.

PVLANs provide Layer 2 isolation between ports within the same broadcast domain. There are three types of PVLAN ports:

- **Promiscuous** - A promiscuous port can talk to everyone. It can communicate with all interfaces, including the isolated and community ports within a PVLAN.
- **Isolated** - An isolated port can only talk to promiscuous ports. An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic from an isolated port is forwarded only to promiscuous ports.
- **Community** - Community ports can talk to other community and promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

The example in Figure 1 illustrates which ports can interconnect. The security provided by a PVLAN can be bypassed by using the router as a proxy. For example, in Figure 2 PC-A and PC-B are isolated from each other. However, PC-A can initiate an attack against PC-B by sending packets that have the source IP address and MAC address of PC-A, the destination IP address of PC-B, but the destination MAC address of R1. S1 will forward the frame to R1 because F0/5 is configured as a promiscuous port. R1 rebuilds the frame with PC-B's MAC address and forwards it to S1. S1 then forwards the frame to PC-B. To mitigate this type of attack, configure an ACL that will deny traffic with a source and destination IP address that belongs to the same subnet, as shown in Figure 2.

Note PVLANs are used mainly in service provider co-location sites. Another typical application can be found in hotels where each room would be connected on its own isolated port.

Refer to Video in online course

6.2.4.7 Video Demonstration - Private VLAN Tutorial and Demonstration

This video and tutorial demonstrates Private VLAN configuration and includes the following:

- Advantages of Private VLANs
- Examples of Private VLAN implementation
- Types of Private VLAN ports

- Configuration of Private VLANS on a 3560 Multilayer switch
- Use of the switchport protected command on a 2960 switch

Click here to read the transcript of this video.

Refer to Online Course for Illustration

6.2.5 Mitigating DHCP Attacks

6.2.5.1 DHCP Spoofing Attack

DHCP servers dynamically provide IP configuration information including IP address, subnet mask, default gateway, DNS servers, and more to clients. The sequence of DHCP message exchange between client and server is displayed in Figure 1.

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** - Attacker 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** - Attacker provides an incorrect DNS server address pointing the user to a nefarious website.
- **Wrong IP address** - Attacker provides an invalid default gateway IP address and creates a DoS attack on the DHCP client.

A DHCP spoofing attack is explained in the following figures:

- In Figure 2, an attacker successfully connects a rogue DHCP server to a switch port on the same subnet as the clients. The goal of the rogue server is to provide clients with false IP configuration information.
- In Figure 3, a legitimate client connects to the network and requires IP configuration parameters. Therefore, the client broadcasts a DHCP Discovery request looking for a response from a DHCP server. Both servers will receive the message and respond.
- In Figure 4, the legitimate DHCP server responds with valid IP configuration parameters. However, the rogue server also responds with DHCP offers containing attacker-defined IP configuration parameters. The client will reply to the first offer received.
- In Figure 5, the rogue offer was received first, and therefore, the client broadcasts a DHCP request accepting the attacker-defined parameters from the rogue server. The legitimate and rogue server will receive the request.
- In Figure 6, the rogue server unicasts a reply to the client to acknowledge its request. The legitimate server will cease communicating with the client.

Refer to Online Course for Illustration

6.2.5.2 DHCP Starvation Attack

Another DHCP attack is the 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.

A DHCP starvation attack is explained in the following figures:

- In Figure 1, an attacker launches the Gobbler tool. Gobbler identifies the size of the DHCP scope and sends a DHCP discovery message for every leasable IP address in the scope.
- In Figure 2, the DHCP provides offers for every received discovery message.
- In Figure 3, Gobbler requests all the DHCP offers.
- In Figure 4, the server acknowledges every request.

Refer to Online Course for Illustration

6.2.5.3 Mitigating DHCP Attacks

It is easy to mitigate DHCP starvation attacks using port security. However, mitigating DHCP spoofing attacks requires more protection.

For instance, Gobbler uses a unique MAC address for each DHCP request and port security. Port security could be configured to mitigate this. However, Gobbler can also be configured to use the same interface MAC address with a different hardware address for every request. This would render port security ineffective.

DHCP spoofing attacks can be mitigated using DHCP snooping on trusted ports. DHCP snooping also helps mitigate against DHCP starvation attacks by rate limiting the number of DHCP discovery messages that an untrusted port can receive. DHCP snooping builds and maintains a DHCP snooping binding database that the switch can use to filter DHCP messages from untrusted sources. The DHCP snooping binding table includes the client MAC address, IP address, DHCP lease time, binding type, VLAN number, and interface information on each untrusted switchport or interface.

Note In a large network, the DHCP binding table may take time to build after it is enabled. For example, it could take 2 days for DHCP snooping to complete the table if DHCP lease time is 4 days.

When DHCP snooping is enabled on an interface or VLAN, and a switch receives a packet on an untrusted port, the switch compares the source packet information with that held in the DHCP snooping binding table. The switch will deny packets containing specific information:

- Unauthorized DHCP server messages from an untrusted port
- Unauthorized DHCP client messages not adhering to the snooping binding table or rate limits
- DHCP relay-agent packets that include option-82 information on an untrusted port

Note To counter Gobbler using the same MAC address, DHCP snooping also makes the switch check the Client Hardware Address (CHADDR) field in the DHCP request. This ensures that it matches the hardware MAC address in the DHCP snooping binding table and the MAC address in the CAM table. If there is no match, the request is dropped.

Note Similar mitigation techniques are available for DHCPv6 and IPv6 clients. Because IPv6 devices can also receive their addressing information from the router's Router Advertisement (RA) message, there are also mitigation solutions to prevent any rogue RA messages.

Refer to **Online Course** for Illustration

6.2.5.4 Configuring DHCP Snooping

As shown in the figure, DHCP snooping recognizes two types of ports:

- **Trusted DHCP ports** - Only ports connecting to upstream DHCP servers should be trusted. These ports that are expected to reply with DHCP offer and DHCP Ack messages. Trusted ports must be explicitly identified in the configuration.
- **Untrusted ports** - These ports connect to hosts that should not be providing DHCP server messages. By default, all switch ports are untrusted.

The general rule when configuring DHCP snooping is to "trust the port and enable DHCP snooping by VLAN". Therefore, the following steps should be used to enable DHCP snooping:

Step 1. Enable DHCP snooping using the **ip dhcp snooping** global configuration command.

Step 2. On trusted ports, use the **ip dhcp snooping trust** interface configuration command.

Step 3. Enable DHCP snooping by VLAN, or by a range of VLANs.

Untrusted ports should also rate limit the number of DHCP discovery messages they can receive per second using the **ip dhcp snooping limit rate** interface configuration command.

Note Rate limiting further mitigates the risk of DHCP starvation attacks.

Refer to **Online Course** for Illustration

6.2.5.5 Configuring DHCP Snooping Example

Examine the reference topology in Figure 1.

Figure 2 displays the commands configured on S1 to enable DHCP snooping. Notice how DHCP snooping is first enabled. Then the upstream interface to the DHCP server is explicitly trusted. Next, the range of FastEthernet ports from F0/5 to F0/24 are untrusted, and therefore, are rate limited to six packets per second. Finally, DHCP snooping is enabled on VLANS 5, 10, 50, 51, and 52.

Note To provide more information about the actual client that generated the DHCP request, enable DHCP option 82 with the **ip dhcp snooping information option** global configuration command. This adds the switch port identifier into the DHCP request.

Figure 3 displays the resulting output of the **show ip dhcp snooping** privileged EXEC command. While Figure 4 displays the resulting output of the **show ip dhcp snooping binding** command. Another way to verify is with the **show ip dhcp snooping database** command.

Note DHCP snooping is also required by Dynamic ARP Inspection (DAI).

Use the Syntax Checker in Figure 5 to configure and verify DHCP snooping.

Refer to Online Course for Illustration

6.2.6 Mitigating ARP Attacks

6.2.6.1 ARP Spoofing and ARP Poisoning Attack

Usually, a host broadcasts an ARP Request to other hosts to determine the MAC address of a host with a particular 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.

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 CAM table accordingly. Therefore, any host can claim to be the owner of any IP/MAC they choose. In a typical attack, a malicious user can send unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the attacker and the IP address of the default gateway.

For example, in Figure 1, PC-A requires the MAC address of its default gateway (R1) and therefore, it sends an ARP Request for the MAC address of 192.168.10.1.

As shown in Figure 2, R1 updates its ARP cache with the IP and MAC addresses of PC-A and sends an ARP Reply to PC-A, which then updates its ARP cache with the IP and MAC addresses of R1.

In Figure 3, the attacker sends two spoofed gratuitous ARP Replies using its own MAC address for the indicated destination IP addresses. PC-A updates its ARP cache with its default gateway now pointing to the attacker's host MAC. R1 also updates its ARP cache with the IP address of PC-A pointing to the attacker MAC address.

The attacker host is now doing an ARP poisoning attack. This is when an attacker uses ARP spoofing to redirect traffic. ARP poisoning leads to various man-in-the-middle attacks, posing a serious security threat to the network.

Note There are many tools available on the Internet to create ARP man-in-the-middle attacks including dsniff, Cain & Abel, ettercap, Yersinia, and others.

Note 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.

Refer to Online Course for Illustration

6.2.6.2 Mitigating ARP Attacks

To prevent ARP spoofing or poisoning, a switch must ensure that only valid ARP requests and replies are relayed.

In a typical attack, a malicious user can send unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the attacker and the IP address of the default gateway.

Dynamic ARP inspection helps prevent such attacks by not relaying invalid or gratuitous ARP Replies out to other ports in the same VLAN. Dynamic ARP inspection intercepts all ARP Requests and all replies on the untrusted ports. Each intercepted packet is verified for valid IP-to-MAC binding. ARP Replies coming from invalid devices are either dropped or logged by the switch for auditing so that ARP poisoning attacks are prevented. DAI can also be rate limited to limit the number of ARP packets, and the interface can be error-disabled if the rate is exceeded.

DAI requires DHCP snooping. DAI determines the validity of an ARP packet based on a valid MAC-address-to-IP-address bindings database that is built by DHCP snooping. In addition, to handle hosts that use statically configured IP addresses, DAI can validate ARP packets against user-configured ARP ACLs.

Refer to **Online Course** for Illustration

6.2.6.3 Configuring Dynamic ARP Inspection

It is generally advisable to configure all access switch ports as untrusted and to configure all uplink ports that are connected to other switches as trusted.

To mitigate the chances of ARP spoofing, these procedures are recommended:

- Implement protection against DHCP spoofing by enabling DHCP snooping globally.
- Enable DHCP snooping on selected VLANs.
- Enable DAI on selected VLANs.
- Configure trusted interfaces for DHCP snooping and ARP inspection (untrusted is default).

The sample topology in the figure identifies trusted and untrusted ports.

Refer to **Online Course** for Illustration

6.2.6.4 Configuring Dynamic ARP Inspection Example

Examine the reference topology in Figure 1. In the example, S1 is connecting two users on VLAN 10. DAI will be configured to mitigate against ARP spoofing and ARP poisoning attacks.

As shown in Figure 2, DHCP snooping is enabled because DAI requires the DHCP snooping table to operate. Next, DHCP snooping and ARP inspection are enabled for the PCs on VLAN10. The uplink port to the router is trusted, and therefore, is configured as trusted for DHCP snooping and ARP inspection.

DAI can also be configured to check for both destination or source MAC and IP addresses:

- **Destination MAC** - Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body.
- **Source MAC** - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.
- **IP address** - Checks the ARP body for invalid and unexpected IP addresses including addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

As shown in Figure 3, the **ip arp inspection validate {[src-mac] [dst-mac] [ip]}** global configuration command is used to configure DAI to drop ARP packets when the IP addresses are invalid. It can be used when the MAC addresses in the body of the ARP packets do not match the addresses that are specified in the Ethernet header. Notice how only one command can be configured. Therefore, entering multiple **ip arp inspection validate** commands overwrite the previous command. To include more than one validation method, enter them on the same command line as displayed in the output.

Use the Syntax Checker in Figure 4 to configure dynamic ARP inspection.

Refer to **Online Course** for Illustration

6.2.7 Mitigating Address Spoofing Attacks

6.2.7.1 Address Spoofing Attack

MAC addresses and IP addresses can be spoofed for a variety of reasons. Spoofing attacks occur when one host poses as another to receive otherwise inaccessible data, or to circumvent security configurations.

The method used by switches to populate the MAC address table leads to a vulnerability known as MAC address spoofing. MAC address spoofing attacks occur when attackers alter the MAC address of their host to match another known MAC address of a target host, as shown in Figure 1. 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 CAM table entry and assigns the MAC address to the new port, as shown in Figure 2. It then inadvertently forwards frames destined for the target host to the attacking host.

When the switch changes the CAM table, the target host does not receive any traffic until it sends traffic. When the target host sends traffic, the switch receives and examines the frame, resulting in the CAM table being rewritten once more, realigning the MAC address to the original port. To stop the switch from returning the spoofed MAC address port assignments to their correct state, the attacking host 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 address spoofing is when a rogue PC hijacks a valid IP address of a neighbor, or a 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.

Refer to **Online Course** for Illustration

6.2.7.2 Mitigating Address Spoofing Attacks

To protect against MAC and IP address spoofing, configure the IP Source Guard (IPSG) security feature. IPSG operates just like DAI, but it looks at every packet, not just the ARP packets. Like DAI, IPSG also requires that DHCP snooping be enabled.

Specifically, IPSG is deployed on untrusted Layer 2 access and trunk ports. IPSG dynamically maintains per-port VLAN ACLs (PVACL) based on IP-to-MAC-to-switch-port bindings. Initially, all IP traffic on the port is blocked, except for DHCP packets that are captured by the DHCP snooping process. A PVACL is installed on the port when a client receives a valid IP address from the DHCP server or when a static IP source binding is configured by the user.

This process restricts the client IP traffic to those source IP addresses that are configured in the binding. Any IP traffic with a source IP address other than that in the IP source binding will be filtered out. This filtering limits the ability of a host to attack the network by claiming the IP address of a neighbor host.

For each untrusted port, there are two possible levels of IP traffic security filtering:

- **Source IP address filter** - IP traffic is filtered based on its source IP address and only IP traffic with a source IP address that matches the IP source binding entry is permitted. When a new IP source entry binding is created or deleted on the port, the PVACL automatically adjusts itself to reflect the IP source binding change.
- **Source IP and MAC address filter** - IP traffic is filtered based on its source IP address in addition to its MAC address. Only IP traffic with source IP and MAC addresses that match the IP source binding entry are permitted.

Refer to **Online Course** for Illustration

6.2.7.3 Configuring IP Source Guard

Examine the IP Source Guard reference topology in Figure 1.

As shown in Figure 2, IP Source Guard is enabled on untrusted ports using the **ip verify source** command. Remember that the feature can only be configured on a Layer 2 access or trunk port and that DHCP snooping is required to learn valid IP address and MAC address pairs.

Use the **show ip verify source** command to verify the IP Source Guard configuration, as shown in Figure 3. In the example, the FastEthernet F0/1 and F0/2 are configured with IP Source Guard. Each interface has one valid DHCP binding.

Use the Syntax Checker in Figure 4 to configure IP Source Guard.

Refer to **Online Course** for Illustration

6.2.8 Spanning Tree Protocol

6.2.8.1 Introduction to the Spanning Tree Protocol

Spanning Tree Protocol (STP) is another Layer 2 technology that is vulnerable in the Layer 2 infrastructure. For this reason, it is important to understand the role and operation of STP.

Redundancy increases the availability of the Layer 2 infrastructure by protecting the network from a single point of failure, such as a failed network cable or a failed switch. When physical redundancy is introduced into a design, loops and duplicate frames occur. Loops and duplicate frames have severe consequences for a switched network. STP was developed to address these issues.

STP ensures that redundant physical links are loop-free. It ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop. A port is considered blocked when user data is prevented from entering or leaving that port. Blocked ports still exchange BPDU frames which are used by STP to prevent loops by dynamically blocking redundant paths or unblocking them when there is a change in the network.

Blocking the redundant paths is critical to preventing loops on the network. The physical paths still exist to provide redundancy, but these paths are disabled to prevent the loops

from occurring. If the path is ever needed to compensate for a network cable or switch failure, STP recalculates the paths and unblocks the necessary ports to allow the redundant path to become active.

Click Play in the figure to view STP in action. In the example, all switches have STP enabled:

- PC1 sends a broadcast out onto the network.
- S2 is configured with STP and has set the port for Trunk2 to a blocking state. The blocking state prevents ports from being used to forward user data, thus preventing a loop from occurring. S2 forwards a broadcast frame out all switch ports, except the originating port from PC1 and the port for Trunk2.
- S1 receives the broadcast frame and forwards it out all of its switch ports, where it reaches PC4 and S3. S3 forwards the frame out the port for Trunk2 and S2 drops the frame. The Layer 2 loop is prevented.

Refer to Online Course for Illustration

6.2.8.2 Various Implementations of STP

Click Play in the figure to view STP recalculation when a failure occurs. In this example:

- PC1 sends a broadcast out onto the network.
- The broadcast is then forwarded around the network, just as in the previous animation.
- The trunk link between S2 and S1 fails, resulting in the previous path being disrupted.
- S2 unblocks the previously blocked port for Trunk2 and allows the broadcast traffic to traverse the alternate path around the network, permitting communication to continue. If this link comes back up, STP reconverges, and the port on S2 is again blocked.

There are various implementations of STP, such as Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). In order to communicate spanning tree concepts correctly, it is important to refer to the particular implementation or standard in context. The latest IEEE documentation on spanning tree, IEEE-802-1D-2004, says "STP has now been superseded by the RSTP". The IEEE uses "STP" to refer to the original implementation of spanning tree and "RSTP" to describe the version of spanning tree specified in IEEE-802.1D-2004. In this curriculum, when discussing the original STP, the phrase "original 802.1D spanning tree" is used to avoid confusion.

Note STP ensures a loop-free topology, providing important protection against accidental or malicious bridge loops. A bridge loop can easily and quickly disable the LAN, and therefore, STP should never be disabled except under specific conditions and when the risks are clearly understood.

Refer to Online Course for Illustration

6.2.8.3 STP Port Roles

The spanning tree algorithm designates a single switch as the root bridge and uses it as the reference point for all path calculations. In the figure, the root bridge (switch S1) is chosen through an election process. All switches that participate in STP exchange BPDU frames to determine which switch has the lowest bridge ID (BID) on the network. The switch with

the lowest BID automatically becomes the root bridge for the spanning tree algorithm calculations.

Note For simplicity, assume until otherwise indicated that all ports on all switches are assigned to VLAN 1. The switches are configured with the default PVST+. Each switch has a unique MAC address associated with VLAN 1.

A BPDU is a messaging frame exchanged by switches for STP. Each BPDU contains a BID that identifies the switch that sent the BPDU. The BID contains a priority value, the MAC address of the sending switch, and an optional extended system ID. The lowest BID value is determined by the combination of these three fields.

After the root bridge has been determined, the spanning tree algorithm calculates the shortest path to it. Each switch uses the spanning tree algorithm to determine which ports to block. While the spanning tree algorithm determines the best paths to the root bridge for all switch ports in the broadcast domain, traffic is prevented from being forwarded through the network. The spanning tree algorithm considers both path and port costs when determining which ports to block. The path costs are calculated using port cost values associated with port speeds for each switch port along a given path. The sum of the port cost values determines the overall path cost to the root bridge. If there is more than one path to choose from, spanning tree algorithm chooses the path with the lowest path cost.

When the spanning tree algorithm has determined which paths are most desirable relative to each switch, it assigns port roles to the participating switch ports. The port roles in the figure describe their relation in the network to the root bridge and whether they are allowed to forward traffic.

Note A port that is shut down is referred to as a disabled port.

Note In the figure, only one end of the trunk is blocked. This allows for faster transition to a forwarding state, when necessary.

Refer to **Online Course** for Illustration

6.2.8.4 STP Root Bridge

As shown in Figure 1, every spanning tree instance (switched LAN or broadcast domain) has a switch designated as the root bridge. The root bridge serves as a reference point for all spanning tree calculations to determine which redundant paths to block.

An election process determines which switch becomes the root bridge.

Figure 2 shows the BID fields. The BID is made up of a priority value, an extended system ID, and the MAC address of the switch.

All switches in the broadcast domain participate in the election process. After a switch boots, it begins to send out BPDU frames every two seconds. These BPDUs contain the switch BID and the root ID.

As the switches forward their BPDU frames, adjacent switches in the broadcast domain read the root ID information from the BPDU frames. If the root ID from a BPDU received is lower than the root ID on the receiving switch, then the receiving switch updates its root

ID, identifying the adjacent switch as the root bridge. Actually, it may not be an adjacent switch, but could be any other switch in the broadcast domain. The switch then forwards new BPDU frames with the lower root ID to the other adjacent switches. Eventually, the switch with the lowest BID ends up being identified as the root bridge for the spanning tree instance.

There is a root bridge elected for each spanning tree instance. It is possible to have multiple distinct root bridges. If all ports on all switches are members of VLAN 1, then there is only one spanning tree instance. The extended system ID plays a role in how spanning tree instances are determined.

Refer to Online Course for Illustration

6.2.8.5 STP Path Cost

When the root bridge has been elected for the spanning tree instance, the spanning tree algorithm starts the process of determining the best paths to the root bridge from all destinations in the broadcast domain. The path information is determined by summing up the individual port costs along the path from the destination to the root bridge. Each "destination" is actually a switch port.

The default port costs are defined by the speed at which the port operates. As shown in Figure 1, 10 Gb/s Ethernet ports have a port cost of 2, 1 Gb/s Ethernet ports have a port cost of 4, 100 Mb/s Fast Ethernet ports have a port cost of 19, and 10 Mb/s Ethernet ports have a port cost of 100.

Note As newer, faster Ethernet technologies enter the marketplace, the path cost values may change to accommodate the different speeds available. The non-linear numbers in the table accommodate some improvements to the older Ethernet standard. The values have changed to accommodate the 10 Gb/s Ethernet standard. To illustrate the continued change associated with high-speed networking, Catalyst 4500 and 6500 switches support a longer path cost method; for example, 10 Gb/s has a 2000 path cost, 100 Gb/s has a 200 path cost, and 1 Tb/s has a 20 path cost.

Although switch ports have a default port cost associated with them, the port cost is configurable. The ability to configure individual port costs gives the administrator the flexibility to manually control the spanning tree paths to the root bridge.

To configure the port cost of an interface (Figure 2), enter the **spanning-tree cost value** command in interface configuration mode. The value can be between 1 and 200,000,000.

In the example, switch port F0/1 has been configured with a port cost of 25 using the **spanning-tree cost 25** interface configuration mode command on the F0/1 interface.

To restore the port cost back to the default value of 19, enter the **no spanning-tree cost** interface configuration mode command.

The path cost is equal to the sum of all the port costs along the path to the root bridge (Figure 3). Paths with the lowest cost become preferred, and all other redundant paths are blocked. In the example, the path cost from S2 to the root bridge S1, over path 1 is 19 (based on the IEEE-specified individual port cost), while the path cost over path 2 is 38. Because path 1 has a lower overall path cost to the root bridge, it is the preferred path. STP then configures the redundant path to be blocked, preventing a loop from occurring.

To verify the port and path cost to the root bridge, enter the **show spanning-tree** command (Figure 4). The Cost field is the total path cost to the root bridge. This value changes

depending on how many switch ports must be traversed to get to the root bridge. In the output, each interface is also identified with an individual port cost of 19.

Refer to **Online Course** for Illustration

6.2.8.6 802.1D BPDU Frame Format

The spanning tree algorithm depends on the exchange of BPDUs to determine a root bridge. A BPDU frame contains 12 distinct fields that convey path and priority information used to determine the root bridge and paths to the root bridge.

Click the BPDU fields in Figure 1 to see more detail.

- The first four fields identify the protocol, version, message type, and status flags.
- The next four fields are used to identify the root bridge and the cost of the path to the root bridge.
- The last four fields are all timer fields that determine how frequently BPDU messages are sent and how long the information received through the BPDU process is retained.

Figure 2 shows a BPDU frame that was captured using Wireshark. In the example, the BPDU frame contains more fields than previously described. The BPDU message is encapsulated in an Ethernet frame when it is transmitted across the network. The 802.3 header indicates the source and destination addresses of the BPDU frame. This frame has a destination MAC address of 01:80:C2:00:00:00, which is a multicast address for the spanning tree group. When a frame is addressed with this MAC address, each switch that is configured for spanning tree accepts and reads the information from the frame; all other devices on the network disregard the frame.

In the example, the root ID and the BID are the same in the captured BPDU frame. This indicates that the frame was captured from a root bridge. The timers are all set to the default values.

Refer to **Online Course** for Illustration

6.2.8.7 BPDU Propagation and Process

Each switch in the broadcast domain initially assumes that it is the root bridge for a spanning tree instance, so the BPDU frames that are sent contain the BID of the local switch as the root ID. By default, BPDU frames are sent every two seconds after a switch is booted. This means that the default value of the Hello timer specified in the BPDU frame is two seconds. Each switch maintains local information about its own BID, the root ID, and the path cost to the root.

When an adjacent switch receives a BPDU frame, it compares the root ID contained in the BPDU frame with its local root ID. If the BPDU root ID is lower than its local root ID, the switch updates the local root ID with the root ID contained in the BPDU. The switch will also include the new root in its BPDU messages to other switches. The distance to the root bridge is also indicated by the path cost update. For example, if the BPDU was received on a Fast Ethernet switch port, the path cost would increment by 19. If the local root ID is lower than the root ID received in the BPDU frame, the BPDU frame is discarded.

After a root ID has been updated to identify a new root bridge, all subsequent BPDU frames sent from that switch contain the new root ID and updated path cost. That way, all other adjacent switches are able to see the lowest root ID identified at all times. As the BPDU frames pass between other adjacent switches, the path cost is continually updated to indicate the total path cost to the root bridge. Each switch in the spanning tree uses its path costs to identify the best possible path to the root bridge.

The following summarizes the BPDU process:

Note Priority is the initial deciding factor when electing a root bridge. If the priorities of all the switches are the same, the device with the lowest MAC address becomes the root bridge.

- Initially, each switch identifies itself as the root bridge. S2 forwards BPDU frames out all switch ports. (Figure 1)
- When S3 receives a BPDU from switch S2, S3 compares its root ID with the BPDU frame it received. The priorities are equal, so the switch is forced to examine the MAC address portion to determine which MAC address has a lower value. Because S2 has a lower MAC address value, S3 updates its root ID with the S2 root ID. At that point, S3 considers S2 as the root bridge. (Figure 2)
- When S1 compares its root ID with the one in the received BPDU frame, it identifies its local root ID as the lower value and discards the BPDU from S2. (Figure 3)
- When S3 sends out its BPDU frames, the root ID contained in the BPDU frame is that of S2. (Figure 4)
- When S2 receives the BPDU frame, it discards it after verifying that the root ID in the BPDU matched its local root ID. (Figure 5)
- Because S1 has a lower priority value in its root ID, it discards the BPDU frame received from S3. (Figure 6)
- S1 sends out its BPDU frames. (Figure 7)
- S3 identifies the root ID in the BPDU frame as having a lower value and, therefore, updates its root ID values to indicate that S1 is now the root bridge. (Figure 8)
- S2 identifies the root ID in the BPDU frame as having a lower value and, therefore, updates its root ID values to indicate that S1 is now the root bridge. (Figure 9).

Refer to **Online Course** for Illustration

6.2.8.8 Extended System ID

The bridge ID (BID) is used to determine the root bridge on a network. The BID field of a BPDU frame contains three separate fields. Each field is used during the root bridge election.

Bridge Priority

The bridge priority is a customizable value that can be used to influence which switch becomes the root bridge. The switch with the lowest priority, which implies the lowest BID, becomes the root bridge because a lower priority value takes precedence. For example, to ensure that a specific switch is always the root bridge, set the priority to a lower value than the rest of the switches on the network. The default priority value for all Cisco switches is 32768. The range is 0 to 61440 in increments of 4096. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected. A bridge priority of 0 takes precedence over all other bridge priorities.

Extended System ID

Early implementations of IEEE 802.1D were designed for networks that did not use VLANs. There was a single common spanning tree across all switches. For this reason, in older Cisco switches, the extended system ID could be omitted in BPDU frames. As VLANs became common for network infrastructure segmentation, 802.1D was enhanced to include support for VLANs, requiring the VLAN ID to be included in the BPDU frame. VLAN information is included in the BPDU frame through the use of the extended system ID. All newer switches include the use of the extended system ID by default.

As shown in Figure 1, the bridge priority field is 2 bytes or 16-bits in length; 4-bits used for the bridge priority and 12-bits for the extended system ID, which identifies the VLAN participating in this particular STP process. Using these 12 bits for the extended system ID reduces the bridge priority to 4 bits. This process reserves the rightmost 12 bits for the VLAN ID and the leftmost 4 bits for the bridge priority. This explains why the bridge priority value can only be configured in multiples of 4096, or 2^12. If the leftmost bits are 0001, then the bridge priority is 4096; if the leftmost bits are 1111, then the bridge priority is 61440 (= 15 x 4096). The Catalyst 2960 and 3560 Series switches do not allow the configuration of a bridge priority of 65536 (= 16 x 4096) because it assumes use of a 5th bit that is unavailable due to the use of the extended system ID.

The extended system ID value is added to the bridge priority value in the BID to identify the priority and VLAN of the BPDU frame.

When two switches are configured with the same priority and have the same extended system ID, the switch having the MAC address with the lowest hexadecimal value will have the lower BID. Initially, all switches are configured with the same default priority value. The MAC address is then the deciding factor on which switch is going to become the root bridge. To ensure that the root bridge decision best meets network requirements, it is recommended that the administrator configure the desired root bridge switch with a lower priority. This also ensures that the addition of new switches to the network does not trigger a new spanning tree election, which can disrupt network communication while a new root bridge is being selected.

In Figure 2, S1 has a lower priority than the other switches; therefore, it is preferred as the root bridge for that spanning tree instance.

When all switches are configured with the same priority, as is the case with all switches kept in the default configuration with a priority of 32768, the MAC address becomes the deciding factor for which switch becomes the root bridge (Figure 3).

Note In the example, the priority of all the switches is 32769. The value is based on the 32768 default priority and the VLAN 1 assignment associated with each switch (32768+1).

The MAC address with the lowest hexadecimal value is considered to be the preferred root bridge. In the example, S2 has the lowest value for its MAC address and is, therefore, designated as the root bridge for that spanning tree instance.

Refer to **Online Course** for Illustration

6.2.8.9 Select the Root Bridge

When an administrator wants a specific switch to become a root bridge, the bridge priority value must be adjusted to ensure it is lower than the bridge priority values of all the other switches on the network. There are two different methods to configure the bridge priority value on a Cisco Catalyst switch.

Method 1

To ensure that the switch has the lowest bridge priority value, use the **spanning-tree vlan** *vlan-id* **root primary** command in global configuration mode. The priority for the switch is set to the predefined value of 24,576 or to the highest multiple of 4,096, less than the lowest bridge priority detected on the network.

If an alternate root bridge is desired, use the **spanning-tree vlan** *vlan-id* **root secondary** global configuration mode command. This command sets the priority for the switch to the predefined value of 28,672. This ensures that the alternate switch becomes the root bridge if the primary root bridge fails. This assumes that the rest of the switches in the network have the default 32,768 priority value defined.

In Figure 1, S1 has been assigned as the primary root bridge using the **spanning-tree vlan 1 root primary** command, and S2 has been configured as the secondary root bridge using the **spanning-tree vlan 1 root secondary** command.

Method 2

Another method for configuring the bridge priority value is using the **spanning-tree vlan** vlan-id **priority** value global configuration mode command. This command gives more granular control over the bridge priority value. The priority value is configured in increments of 4,096 between 0 and 61,440.

In the example, S3 has been assigned a bridge priority value of 24,576 using the **spanning-tree vlan 1 priority 24576** command.

To verify the bridge priority of a switch, use the **show spanning-tree** command. In Figure 2, the priority of the switch has been set to 24,576. Also notice that the switch is designated as the root bridge for the spanning tree instance.

Use the Syntax Checker in Figure 3 to configure and verify the root bridge. Using Method 2 described above, configure S3 manually, setting the priority to 24,576 for VLAN 1. Using Method 1, configure S2 as the secondary root VLAN 1 and configure S1 as the primary root for VLAN 1. Verify the configuration with the **show spanning-tree** command on S1.

Refer to **Interactive Graphic** in online course

6.2.8.10 Activity – Identify the 802.1D RSTP Port Roles

Refer to **Interactive Graphic** in online course

6.2.8.11 Activity – Troubleshoot STP Configuration Issues

Refer to **Video** in online course

6.2.8.12 Video Demonstration - Observing Spanning Tree Protocol Operation

This video demonstrates Spanning Tree Protocol (STP) operation and includes the following:

- Characteristics of STP
- Fault tolerance
- Layer 2 Broadcast storm
- Debugging STP

Click here to read the transcript of this video.

Refer to Online Course for Illustration

6.2.9 Mitigating STP Attacks

6.2.9.1 STP Manipulation Attacks

Network attackers can manipulate 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 configuration and topology change BPDUs to force spanning-tree recalculations, as shown in Figure 1. The BPDUs sent by the attacking host announce a lower bridge priority in an attempt to be elected as the root bridge. If successful, as shown in Figure 2, the attacking host becomes the root bridge and sees a variety of frames that would otherwise not be accessible.

This attack can be used to defeat all three of the security objectives: confidentiality, integrity, and availability.

Refer to Online Course for Illustration

6.2.9.2 Mitigating STP Attacks

To mitigate STP manipulation attacks, use the Cisco STP stability mechanisms to enhance the overall performance of the switches and to reduce the time that is lost during topology changes.

These are recommended practices for using STP stability mechanisms:

- **PortFast** - PortFast immediately brings an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states. Apply to all end-user ports. PortFast should only be configured when there is a host attached to the port, and not another switch.
- **BPDU Guard** - BPDU guard immediately error disables a port that receives a BPDU. Typically used on PortFast enabled ports. Apply to all end-user ports.
- **Root Guard** - Root guard prevents an inappropriate switch from becoming the root bridge. Root guard limits the switch ports out of which the root bridge may be negotiated. Apply to all ports which should not become root ports.
- **Loop Guard** - Loop guard prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. Apply to all ports that are or can become non-designated.

These features enforce the placement of the root bridge in the network and enforce the STP domain borders.

The figure highlights on which ports these features should be implemented.

Refer to Online Course for Illustration

6.2.9.3 Configuring PortFast

The spanning-tree PortFast feature causes an interface configured as a Layer 2 access port to transition from the blocking to the forwarding state immediately, bypassing the listening and learning states. PortFast can be used on Layer 2 access ports that connect to a single workstation or server, as shown in the figure. This allows those devices to connect to the network immediately, instead of waiting for STP to converge.

Because the purpose of PortFast is to minimize the time that access ports must wait for STP to converge, it should be used only on access ports. If PortFast is enabled on a port connecting to another switch, there is a risk of creating a spanning-tree loop.

Portfast can be configured globally on all non-trunking ports using the **spanning-tree portfast default** global configuration command. Alternatively, PortFast can be enabled on an interface using the **spanning-tree portfast interface** configuration command.

To verify if PortFast has been enabled, use the **show running-config interface** *type slot/port* command.

Refer to Online Course for Illustration

6.2.9.4 Configuring BPDU Guard

Even though PortFast is enabled, the interface will listen for BPDUs. The receipt of unexpected BPDUs might be accidental, or part of an unauthorized attempt to add a switch to the network.

BPDU Guard protects the integrity of ports that are PortFast-enabled. BPDU also protects against additional switches added to the topology, which may violate the number of end-to-end switches allowed in the STP topology. If any BPDU is received on a BPDU Guard enabled port, that port is put into error-disabled state. This means the port is shut down and must be manually re-enabled or automatically recovered through the error-disabled timeout function.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on all PortFast-enabled ports. If PortFast is not configured, then BPDU Guard is not activated. Alternatively, BPDU Guard can be enabled on a PortFast-enabled port using the **spanning-tree bpduguard enable** interface configuration command.

Note Always enable BPDU Guard on all PortFast-enabled ports.

As shown in Figure 1, the BPDU guard is best deployed towards user-facing ports to prevent rogue switch network extensions by an attacking host. In this example, an attacker is attempting to send a BPDU on a switch with PortFast and BPDU guard enabled globally. Notice the CLI notification message that was generated stating that the FastEthernet 0/1 port is shut down.

To display information about the state of spanning tree, use the **show spanning-tree summary** command. In the example in Figure 2, BPDU guard is enabled.

Another useful command to verify BPDU guard configuration is the **show spanning-tree summary totals** command shown in Figure 3. The command displays a summary of port states or the total lines of the spanning-tree state section.

Refer to Online Course for Illustration

6.2.9.5 Configuring Root Guard

On a network, there are some switches that should never, under any circumstances, become the STP root bridge. Root Guard provides a way to enforce the placement of root bridges on the network by limiting which switch can become the root bridge.

Root guard is best deployed toward ports that connect to switches that should not be the root bridge. If a root-guard-enabled port receives BPDUs that are superior to those that the current root bridge is sending, that port is moved to a root-inconsistent state. This is effectively equal to an STP listening state, and no data traffic is forwarded across that port. Recovery occurs as soon as the offending device ceases to send superior BPDUs.

Use the **spanning-tree guard root** interface configuration command to configure root guard on an interface.

In the figure, D1 is the root bridge. If D1 fails, only D2 switch should become the root bridge. To ensure that S1 never becomes a root bridge, the F0/1 interfaces of D1 and D2 should be enabled for Root guard.

To view Root Guard ports that have received superior BPDUs and are in a root-inconsistent state, use the **show spanning-tree inconsistent ports** command.

Note Root guard may seem unnecessary because an administrator can manually set the bridge priority of a switch to zero. However, this does not guarantee that this switch will be elected as the root bridge. Another switch may still become the root if it also has a priority of zero and a lower MAC address.

Refer to **Online Course** for Illustration

6.2.9.6 Configuring Loop Guard

Traffic on bidirectional links flows in both directions. If for some reason one direction traffic flow fails, this creates a unidirectional link which can result in a Layer 2 loop. STP relies on continuous reception or transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs. A Layer 2 loop is usually created when an STP port in a redundant topology stops receiving BPDUs and erroneously transitions to the forwarding state.

The STP Loop Guard feature provides additional protection against Layer 2 loops. If BPDUs are not received on a non-designated Loop Guard-enabled port, the port transitions to a loop-inconsistent blocking state, instead of the listening / learning / forwarding state. Without the Loop Guard feature, the port would assume a designated port role and create a loop.

As shown in Figure 1, Loop Guard is enabled on all non-Root guard ports using the **spanning-tree guard loop** interface configuration command.

Note Loop Guard can also be enabled globally using the **spanning-tree loopguard default** global configuration command. This enables Loop guard on all point-to-point links.

Use the Syntax Checker in Figure 2 to configure PortFast and BPDU Guard.

Refer to **Online Course** for Illustration

6.3 Summary

6.3.1 Conclusion

Refer to **Lab Activity** for this chapter

6.3.1.1 Lab – Securing Layer 2 Switches

In this lab, you will complete the following objectives to configure security on Layer 2 switches:

- Configure basic settings.
- Configure SSH.

- Configure secure trunks and access ports by enabling features including port security, root guard, BPDU guard, loop guard and PVLAN Edge.
- Configure DHCP Snooping.

Refer to **Packet Tracer Activity** for this chapter

6.3.1.2 Packet Tracer – Layer 2 Security

In this Packet Tracer, you will complete the following objectives:

- Assign the Central switch as the root bridge.
- Secure spanning-tree parameters to prevent STP manipulation attacks.
- Enable port security to prevent CAM table overflow attacks.

Refer to **Packet Tracer Activity** for this chapter

6.3.1.3 Packet Tracer – Layer 2 VLAN Security

In this Packet Tracer, you will complete the following objectives:

- Connect a new redundant link between SW-1 and SW-2.
- Enable trunking and configure security on the new trunk link between SW-1 and SW-2.
- Create a new management VLAN (VLAN 20) and attach a management PC to that VLAN.
- Implement an ACL to prevent outside users from accessing the management VLAN.

Refer to **Online Course** for Illustration

6.3.1.4 Securing the Local Area Network

Endpoint security includes securing the network infrastructure devices in the LAN and end systems, such as workstations, servers, IP phones, access points, and storage area networking (SAN) devices.

There are several endpoint security applications and devices available to accomplish endpoint security. These include Advanced Malware Protection (AMP), Cisco Email Security Appliance (ESA) and Web Security Appliance (WSA), security to provide antispam, antivirus, antispyware security, and Cisco NAC, which only allows authorized and compliant systems to access the network and enforce a network security policy.

At Layer 2, a number of vulnerabilities exist that require specialized mitigation techniques:

- CAM table overflow attacks are addressed with port security.
- VLAN attacks are controlled by disabling DTP and following basic guidelines for configuring trunk ports.
- DHCP attacks are addressed with DHCP snooping.
- ARP spoofing and ARP poisoning attacks are mitigated using Dynamic ARP Inspection (DAI).
- MAC and IP address spoofing attacks are mitigated using IP Source Guard.
- STP manipulation attacks are handled by PortFast, BPDU guard, root guard, and loop guard.

Go to the online course to take the quiz and exam.

Chapter 6 Quiz

This quiz is designed to provide an additional opportunity to practice the skills and knowledge presented in the chapter and to prepare for the chapter exam. You will be allowed multiple attempts and the grade does not appear in the gradebook.

Chapter 6 Exam

The chapter exam assesses your knowledge of the chapter content.

Your Chapter Notes