Chapter 9: Implementing Secure Network Designs

Study online at https://quizlet.com/_9j58rv

1.	**Consider the types of zones within a network's topology and locate the zone considered semi-trusted and requires hosts to authenticate to join.** **A.) Private network** **B.) Extranet** **C.) Internet** **D.) Anonymous**	B
2.	**This is a network of semi-trusted hosts, typically representing business partners, suppliers, or customers. Hosts must authenticate to join**	Extranet Zone
3.	**This is a network of trusted hosts owned and controlled by the organization. This type of trusted host network is under administrative control and subject to the security mechanisms set up to defend the network.**	Private Network (Intranet)
4.	**This or guest, zones permit anonymous access by untrusted hosts over the Internet. This can also be a mix of anonymous and authenticated access.**	Internet
5.	**Typical network security weaknesses include:**	-Single points of failure—a "pinch point" relying on a single hardware server or appliance or network channel. -Complex dependencies—services that require many different systems to be available. I -Availability over confidentiality and integrity—often it is tempting to take "shortcuts" to get a service up and

		running. -Lack of documentation and change control—network segments, appliances, and services might be added without proper change control procedures, leading to a lack of visibility into how the network is constituted. -Overdependence on perimeter security—if the network architecture is "flat" (that is, if any host can contact any other host), penetrating the network edge gives the attacker freedom of movement.
6.	**These forward frames between nodes in a cabled network. Switches work at layer 2 of the OSI model and make forwarding decisions based on the hardware or Media Access Control (MAC) address of attached nodes.**	Switches
7.	**These can establish network segments that either map directly to the underlying cabling or to logical segments, created in the switch configuration as virtual LANs (VLANs).**	Switches
8.	**These provide a bridge between a cabled network and wireless clients, or stations. APs work at layer 2 of the OSI model.**	Wireless access points
9.	**These forward packets around an internetwork, making forwarding decisions based on IP addresses. They work at layer 3 of the OSI model and can apply logical IP subnet addresses to segments within a network.**	Routers
10.		Firewalls

	These apply an access control list (ACL) to filter traffic passing in or out of a network segment. They can work at layer 3 of the OSI model or higher.	
11.	**This distribute traffic between network segments or servers to optimize performance. It can work at layer 4 of the OSI model or higher.**	Load Balancer
12.	**This host name records and perform name resolution to allow applications and users to address hosts and services using fully qualified domain names (FQDNs) rather than IP addresses. DNS works at layer 7 of the OSI model.**	Domain Name System (DNS) servers
13.	**This maps a network interface's hardware (MAC) address to an IP address. Normally a device that needs to send a packet to an IP address but does not know the receiving device's MAC address broadcasts an ARP Request packet, and the device with the matching IP responds with an ARP Reply.**	Address Resolution Protocol (ARP)
14.	**Where should an administrator place an internet-facing host on the network?** **A.) DMZ** **B.) Bastion host** **C.) Extranet** **D.) Private network**	A
15.	**This is a protected but untrusted area (zone) between the Internet and the private network. Traffic can not pass through this, but it enables external clients to access data on private systems, such as web servers, without compromising the security of the entire internal network.**	Demilitarized Zones

16.	**This reside in a DMZ and are not fully trusted by the internal network due to the possibility of Internet compromise.**	Bastion hosts
17.	**There are several types of security zones on a network. Analyze network activities to determine which of the following does NOT represent a security zone.** **A.) DMZ** **B.) Screened host** **C.) Wireless** **D.) Guest**	B
18.	**This is when a smaller network accesses the Internet using a dual-homed proxy/gateway servers. This uses two firewalls placed on either side of the DMZ. The edge firewall restricts traffic on the external/public interface and allows permitted traffic to the hosts in the DMZ.**	Screened host
19.	**This is a zone that allows untrusted or semi-trusted hosts on the local network. Examples include publicly accessible computers or visitors bringing their own portable computing devices to the premises.**	Guest Network
20.	**A DMZ can also be established using one router/firewall appliance with three network interfaces, referred to as this. One interface is the public one, another is the DMZ, and the third connects to the LAN. Routing and filtering rules determine what forwarding is allowed between these interfaces.**	Triple-Homed Firewall
21.	**Evaluate the typical weaknesses found in network architecture and determine which statement best aligns with a perimeter security weakness.**	D

A.) A company has a single network channel.
B.) A company has many different systems to operate one service.
C.) A company has a habit of implementing quick fixes.
D.) A company has a flat network architecture.

22. **Overdependence on perimeter security occurs when _____?** the network architecture is flat
If an attacker can penetrate the network edge, the attacker will then have freedom of movement throughout the entire network.

23. **Evaluate the following choices based on their potential to lead to a network breach. Select the choice that is NOT a network architecture weakness.** D

A.) The network architecture is flat.
B.) Services rely on the availability of several different systems.
C.) The network relies on a single hardware server.
D.) Not all hosts on the network can talk to one another.

24. **This is where all hosts can contact each other, exposing an overdependence on perimeter security. This is an architecture weakness.** flat architecture

25. **Identify the attack that can launch by running software such as Dsniff, Cain and Abel, or Ettercap from a computer attached to the same switch as the target.** A

A.) ARP poisoning attack
B.) MAC spoofing

C.) MAC flooding
D.) Man-in-the-Middle (MitM)

26.	**This attack broadcasts unsolicited ARP reply packets. A sophisticated ARP attack can launch by running software such as Dsniff, Cain and Abel, or Ettercap from a computer attached to the same switch as the target.**	ARP poisoning
27.	**This changes the MAC address configured on an adapted interface or asserts the use of an arbitrary MAC address. It is simple to override a MAC address in software via OS commands, alterations to the network driver configuration, or using packet crafting software.**	MAC spoofing or Mac Cloning
28.	**This is a variation of an ARP poisoning attack and usually directed against a switch. It overwhelms the table and causes the switch to stop trying to apply MAC-based forwarding and flood unicast traffic out of all ports, working as a hub.**	Mac Flooding
29.	**One way to launch this attack is to use a Trojan to replace some genuine software on the system. These attacks can also launch against antiquated protocols, such as ARP or DNS.**	Man-in-the-Middle (MitM)
30.	**Rather than obscure internal/external traffic flows with private to public address mapping, these should be configured to mirror the equivalent IPv4 architecture.**	IPv6 routing and filtering policies
31.	**. In data centers that support cloud and other Internet services, most traffic is actually between servers within the data center. This is referred to as _____?**	East-West Traffic

32.	**This also known as an on-path attack is where the threat actor gains a position between two hosts, and transparently captures, monitors, and relays all communication between the hosts.**	Man-in-the-Middle (MitM)
33.	**Given that layer 2 does not recognize Time to Live, evaluate the potential problems to determine which of the following options prevents this issue.** **A.) ICMP** **B.) L2TP** **C.) NTP** **D.) STP**	D
34.	**This is a switching protocol that prevents network loops by dynamically disabling links as needed. Since layer 2 protocol has no concept of Time To Live, layer 2 broadcast traffic could continue to loop through a network with multiple paths indefinitely.**	Spanning tree Protocol (STP)
35.	**This is an IP-level protocol for reporting errors and status information that supports the function of troubleshooting utilities such as ping.**	ICMP (Internet Control Message Protocol)
36.	**This is the standard VPN (Virtual Private Network) protocol for tunneling point-to-point sessions across a variety of network protocols.**	L2TP (Layer 2 Tunneling Protocol)
37.	**This is a Transmission Control Protocol/Internet Protocol (TCP/IP) application protocol allowing machines to synchronize to the same time clock that runs over UDP port 123.**	NTP (Network Time Protocol)
38.	**Analyze the techniques that are available to perform rogue machine detection and select**	C and D

	the accurate statements. (Select all that apply.) **A.) Visual inspection of ports and switches will prevent rogue devices from accessing the network.** **B.) Network mapping is an easy way to reveal the use of unauthorized protocols on the network or unusual traffic volume.** **C.) Intrusion detection and NAC are security suites and appliances that combine automated network scanning with defense and remediation suites to prevent rogue devices from accessing the network.** **D,) Wireless monitoring can reveal whether there are unauthorized access points.**	
39.	**These are security suites and appliances that can combine automated network scanning with defense and remediation suites to prevent rogue devices from accessing the network.**	Intrusion detection and NAC
40.	**This can identify hosts unless an OS is actively trying to remain unobserved by not operating when scans are running. Identifying a rogue host on a large network from a scan may still be difficult.**	Network Mapping
41.	**An attacker tricks a host within a subnet into routing through an attacker's machine, rather than the legitimate default gateway, allowing the attacker to eavesdrop on communications and perform a Man-in-the-Middle (MitM) attack. Compare the types of routing vulnerabilities and conclude what the attacker is exploiting in this scenario.** **A.) Route injection**	C

B.) Denial of service
C.) ARP poisoning
D.) Source routing

42.	**This occurs by tricking hosts on the subnet into routing through the attacker's machine rather than the legitimate default gateway. This allows the attacker to eavesdrop on communications and perform replay or MitM attacks.**	ARP poisoning
43.	**This occurs when routing protocols have weak or no authentication. This can mean traffic misdirected to a monitoring port, sent to a black hole, or continuously looped.**	Route injection
44.	**This uses an option in the IP header to pre-determine the route a packet will take through the network that it must pass through.**	Source Routing
45.	**Which statement regarding attacks on media access control (MAC) addresses accurately pairs the method of protection and what type of attack it guards against? (Select all that apply.)** **A.) MAC filtering guards against MAC snooping.** **B.) Dynamic Host Configuration Protocol (DHCP) snooping guards against MAC spoofing.** **C.) MAC filtering guards against MAC spoofing.** **D.) Dynamic address resolution protocol inspection (DAI) guards against MAC flooding.**	B and C
46.	**In this, a switch will record the specified number of MACs allowed to connect to a port, but then drop any traffic from other MAC addresses. It can also switch define which MAC**	Mac Filtering

	addresses are allowed to connect to a particular port, dropping other traffic to protect against MAC flooding attacks.	
47.	**This can be configured alongside DHCP snooping, prevents a host attached to an untrusted port from flooding the segment with gratuitous ARP replies.**	Dynamic ARP inspection (DAI)
48.	**Compare the characteristics of a rogue Access Point (AP) in wireless networks to determine which statements correctly summarize their attributes. (Select all that apply.)** **A.) An evil twin is a rogue AP masquerading as a legitimate AP, and an attacker may form this by using a Denial of Service (DoS) to overcome the legitimate AP.** **B.) Sometimes referred to as an evil twin, a rogue AP masquerading as a legitimate AP, may have a similar name to a legitimate AP.** **C.) An attacker can set up a rogue AP with something as simple as a smartphone with tethering capabilities.** **D.) A Denial of Service (DoS) will bypass authentication security (enabled on the AP), so it is important to regularly scan for rogue APs on the network.**	A, B and C
49.	**This is a rogue AP masquerading as a legitimate sometimes known as WiPhishing. A DoS attack can form this to overcome the legitimate AP.**	Evil Twin
50.	**This can also be formed by an attacker, giving the AP a similar name (SSID) to that of the legitimate AP. Users may select this AP by mistake, and enter their credentials, which the attacker will capture.**	Evil Twin

51.	**This can be setup with something as basic as a smartphone with tethering capabilities. It is vital to periodically survey the site to detect rogue APs.**	Rogue APs
52.	**A team is building a wireless network, and the company has requested the team to use a Wired Equivalent Privacy (WEP) encryption scheme. The team has developed a recommendation to utilize a different encryption scheme based on the problems with WEP. Analyze the features of WEP to determine what problems to highlight in the recommendation.** **A.) WEP only allows the use of a 128-bit encryption key and is not secure. The Initialization Vector (IV) is too large to provide adequate security.** **B.) WEP allows for a 256-bit key but is still not secure. The Initialization Vector (IV) is not sufficiently large, thus is not always generated using a sufficiently random algorithm.** **C.) WEP has the option to use either a 64-bit or a 128-bit key, which is not secure enough for the company. Packets use a checksum to verify integrity that is too difficult to compute.** **D.) WEP only allows the use of a 64-bit key, which is not secure enough for the company. The Initialization Vector (IV) is often not generated using a sufficiently random algorithm.**	B
53.	**Version 1 has both 64-bit and 128-bit keys, while version 2 has 128-bit and 256-bit keys but is still not secure. The main problem with it is the 24-bit Initialization Vector (IV). The IV changes the keystream each time, but this does not always occur due to problems. One**	WEP

of the problems is that the IV is not sufficiently large, meaning the system will reuse the IV within the same keystream under load.

54. **A company is reviewing the options for installing a new wireless network. They have requested recommendations for utilizing WEP, WPA, or WPA2. Differentiate between Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). Determine which of the following statements accurately distinguishes between the options. (Select all that apply.)**

A.) WEP uses RC4 with a Temporal Key Integrity Protocol (TKIP) and WPA, while WPA2 uses a 24-bit Initialization Vector (IV). WPA2 combines the 24-bit IV with an Advanced Encryption Standard (AES) to add security.
B.) WEP is the strongest encryption scheme, followed by WPA2, then WPA. WEP is difficult to crack when protected by a strong password, or if deploying enterprise authentication. WPA2 is more vulnerable to decryption due to replay attack possibilities.
C.) WPA and WEP use RC4, while WEP uses a 24-bit Initialization Vector (IV). WPA uses a Temporal Key Integrity Protocol (TKIP), and WPA2 uses an Advanced Encryption Standard (AES) for encryption.
D.) WPA2 is the strongest encryption scheme, followed by WPA, then WEP. WPA2 is difficult to crack if protected by a strong password, or if deploying enterprise authentication. WEP is more vulnerable to decryption due to replay attack possibilities.

C and D

55. **This uses an Advanced Encryption Standard (AES) for encryption, while WPA and WEP use RC4. It combines the RC4 with a Temporal**

WPA2

Key Integrity Protocol (TKIP), while WEP uses a 24-bit Initialization Vector (IV).

56. **This is the strongest encryption scheme due to the use of AES. WPA is stronger than WEP because of the TKIP. WEP uses the 24-bit IV, which has known vulnerabilities and is the weakest encryption system of the three.** — WPA

57. **This is the most vulnerable due to the possibility of replay attacks.** — WEP

58. **A hotel guest opens their computer and logs into the Wi-Fi without prompting the guest for a username and password. Upon opening an internet browser, a splash page appears that requests the guest's room number and last name for authentication. Which type of authentication is the hotel utilizing?**

    A.) Protected
    B.) Extensive
    C.) Group
    D.) Open — D

59. **This requires all of the wireless devices to be WPS capable and use a PIN. This type of authentication is common for residential consumers.** — Wi-Fi Protected Setup (WPS)

60. **This supports different types of authentication within the same overall topology of devices. It can include smart cards, one-time passwords, and biometric scanning for authentication.** — Extensive Authentication Protocol (EAP)

61. **This uses a pre-shared key that employs a passphrase to generate the key that encrypts communication. The group uses the same secret key.** — Group Authentication

62.	**A network is under a Distributed Denial of Service (DDoS) attack. The Internet Service Provider (ISP) decides to use a blackhole as a remedy. How does the ISP justify their decision?** **A.) A blackhole drops packets for the affected IP address(es) and is in a separate area of the network that does not reach any other part of the network.** **B.) A blackhole makes the attack less damaging to the ISP's other customers and continues to send legitimate traffic to the correct destination.** **C.) A blackhole routes traffic destined to the affected IP address to a different network. Here, the ISP can analyze and identify the source of the attack, to devise rules to filter it.** **D.) A blackhole is preferred, as it evaluates each packet in a multi-gigabit stream against an Access Control List (ACL) without overwhelming the processing resources.**	A
63.	**This drops packets for the affected IP addresses(es). It is an area of the network that cannot reach any other part of the network which protects the unaffected portion.**	Blackhole
64.	**This does make the attack less damaging to the other ISP customers but does not send legitimate traffic to the correct destination. It does not look at packets and simply drops all packets into the black hole.**	Blackhole
65.	**This routes traffic to a particular IP address, to a different network, so the ISP can analyze and identify the source of the attack.**	Sinkhole Routing

66.	**During the planning/scoping phase of the kill chain, an attacker decides that a Distributed Denial of Service (DDoS) attack would be the best way to disrupt the target website and remain anonymous. Evaluate the following explanations to determine the reason the attacker chose a DDoS attack.** **A.)A DDoS attack can launch via covert channels** **B.) DDoS attacks utilize botnets** **C.) A DDoS attack creates a backdoor to a website** **D.) DDoS attacks use impersonation**	B
67.	**This uses a botnet to launch the attack. It means the attack launches from multiple, compromised computers and devices, which is a botnet. Since the attack will come from multiple IP addresses, it will mask the identity of the attacker.**	Distributed Denial of Services (DDoS) attack
68.	**This is a means of secretly communicating with a compromised machine. The purpose of a DDoS is to overload the target so it's unavailable to legitimate users, not to communicate with it.**	Covert Channel
69.	**This is a mechanism for gaining access to a computer that bypasses the normal method of authentication. DDoS aims to deny service, not gain access.**	Backdoor
70.	**Given knowledge of load balancing and clustering techniques, which configuration provides both fault tolerance and consistent performance for applications like streaming audio and video services?** **A.) Active/Passive clustering**	A

B.) Active/Active clustering
C.) First in, First out (FIFO) clustering
D.) Fault tolerant clustering

71.	**In this clustering, if the active node suffers a fault, the connection can failover to the passive node, without performance degradation.**	active/passive
72.	**In this cluster, both nodes process connections concurrently, using the maximum hardware capacity. During failover, the failed node's workload shifts to the remaining node, the workload on the remaining nodes increases, and performance degrades.**	active/active
73.	**This framework prioritizes traffic based on its characteristics, like bandwidth requirements for video and voice applications., to better support voice and video applications susceptible to latency and jitter.**	Quality of Service (QoS)
74.	**This ensures that a redundant component, device, or application can quickly and efficiently take over the functionality of an asset that has failed.**	Failover
75.	**Which statement best describes the difference between session affinity and session persistence?** **A.) With persistence, once a client device establishes a connection, it remains with the node that first accepted its request, while an application-layer load balancer uses session affinity to keep a client connected by setting up a cookie.** **B.) Session affinity makes node scheduling decisions based on health checks and processes incoming requests based on each node's load. Session persistence makes**	C

scheduling decisions on a first in, first out (FIFO) basis.
C.) With session affinity, when a client establishes a session, it remains with the node that first accepted its request, while an application-layer load balancer uses persistence to keep a client connected by setting up a cookie.
D.) Session persistence makes scheduling decisions based on traffic priority and bandwidth considerations, while session affinity makes scheduling decisions based on which node is available next.

76.	**This is a layer 4 approach to handling user sessions. When a client establishes a session, it stays with the node that first accepted the request.**	Session affinity
77.	**Most network appliances process packets on a best effort and _____ basis. Layer 4 load balancers only make basic connectivity tests, while layer 7 appliances can test the application's state.**	First In First Out (FIFO)
78.	**An application-layer load balancer uses _____ to keep a client connected to a session. It typically works by setting a cookie, which can be more reliable than session affinity.**	Persistence
79.	**This products can extend the scope of authentication to allow administrators to devise policies or profiles describing a minimum security configuration that devices must meet to be granted network acces**	Network access control (NAC)

1. **We have seen that using VLANs to segment a switched network provides improved performance, manageability, and security. Trunks are used to carry information from multiple VLANs between devices. However, because these VLANs have segmented the network, a Layer 3 process is required to allow traffic to move from one network segment to another.**

   This Layer 3 routing process can either be implemented using a router or a Layer 3 switch interface. The use of a Layer 3 device provides a method for controlling the flow of traffic between network segments, including network segments created by VLANs.

   This chapter focuses on the methods used for the implementation of inter-VLAN routing. It includes configurations for both the use of a router and a Layer 3 switch. It also describes issues encountered when implementing inter-VLAN routing and standard troubleshooting techniques.

   Switching to Local-Network Channels

   You work for a small- to medium-size business. As the network administrator, you are responsible for ensuring that your network operates efficiently and securely.

   Several years ago, you created VLANs on your only switch for two of your departments, Accounting and Sales. As the business has grown, it has become apparent that sometimes these two departments must share company files and network resources.

   You discuss this scenario with network administrators in a few branches of your company. They tell you to consider using inter-VLAN routing.

   Research the concept of inter-VLAN routing.

   Design a simple presentation to show your manager how you would use inter-VLAN routing to allow the Accounting and Sales departments to remain separate, but share company files and network resources.

2. **What is Inter-VLAN Routing?**
   VLANs are used to segment switched networks. Layer 2 switches, such as the Catalyst 2960 Series, can be configured by a network professional with over 4,000 VLANs. However, Layer 2 switches have very

   Historically, the first solution for inter-VLAN routing relied on routers with multiple physical interfaces. Each interface had to be connected to a separate network and configured with a distinct subnet.

limited IPv4 and IPv6 functionality and cannot perform the routing function of routers. While Layer 2 switches are gaining more IP functionality, such as the ability to perform static routing, these switches do not support dynamic routing. With the large number of VLANs possible on these switches, static routing is insufficient.

A VLAN is a broadcast domain, so computers on separate VLANs are unable to communicate without the intervention of a routing device. Any device that supports Layer 3 routing, such as a router or a multilayer switch, can be used to perform the necessary routing functionality. Regardless of the device used, the process of forwarding network traffic from one VLAN to another VLAN using routing is known as inter-VLAN routing.

In this legacy approach, inter-VLAN routing is performed by connecting different physical router interfaces to different physical switch ports. The switch ports connected to the router are placed in access mode and each physical interface is assigned to a different VLAN. Each router interface can then accept traffic from the VLAN associated with the switch interface that it is connected to, and traffic can be routed to the other VLANs connected to the other interfaces.

Click the Play button in the figure to view an animation of legacy inter-VLAN routing.

As seen in the animation:

1. PC1 on VLAN 10 is communicating with PC3 on VLAN 30 through router R1.

2. PC1 and PC3 are on different VLANs and have IP addresses on different subnets.

3. Router R1 has a separate interface configured for each of the VLANs.

4. PC1 sends unicast traffic destined for PC3 to switch S2 on VLAN 10, where it is then forwarded out the trunk interface to switch S1.

5. Switch S1 then forwards the unicast traffic through its interface F0/3 to interface G0/0 on router R1.

		6. The router routes the unicast traffic through its interface G0/1, which is connected to VLAN 30. 7. The router forwards the unicast traffic to switch S1 on VLAN 30. 8. Switch S1 then forwards the unicast traffic to switch S2 through the active trunk link, after which switch S2 can then forward the unicast traffic to PC3 on VLAN 30. In this example, the router was configured with two separate physical interfaces to interact with the different VLANs and perform the routing. Note: This method of inter-VLAN routing is not efficient and is generally no longer implemented in switched networks. It is shown in this course for explanation purposes only.
3.	**While legacy inter-VLAN routing requires multiple physical interfaces on both the router and the switch, a more common, present-day implementation of inter-VLAN routing does not. Instead, some router software permits configuring a router interface as a trunk link, meaning only one physical interface is required on the router and the switch to route packets between multiple VLANs.** **'Router-on-a-stick' is a type of router configuration in which a single**	The router-on-a-stick implementation of inter-VLAN routing requires only one physical interface on a router and one interface on a switch, simplifying the cabling of the router. However, in other implementations of inter-VLAN routing, a dedicated router is not required. Multilayer switches can perform Layer 2 and Layer 3 functions, replacing the need for dedicated routers to perform basic routing on a network. Multilayer switches support dynamic routing

physical interface routes traffic between multiple VLANs on a network. As seen in the figure, the router is connected to switch S1 using a single, physical network connection (a trunk).

The router interface is configured to operate as a trunk link and is connected to a switch port that is configured in trunk mode. The router performs inter-VLAN routing by accepting VLAN-tagged traffic on the trunk interface coming from the adjacent switch, and then internally routing between the VLANs using subinterfaces. The router then forwards the routed traffic, VLAN-tagged for the destination VLAN, out the same physical interface as it used to receive the traffic.

Subinterfaces are software-based virtual interfaces, associated with a single physical interface. Subinterfaces are configured in software on a router and each subinterface is independently configured with an IP address and VLAN assignment. Subinterfaces are configured for different subnets corresponding to their VLAN assignment to facilitate logical routing. After a routing decision is made based on the destination VLAN, the data frames are VLAN-tagged and sent back out the physical interface.

Click the Play button in the fig-

and inter-VLAN routing.

Click the Play button in the figure to see an animation of how switch-based inter-VLAN routing occurs.

As seen in the animation:

1. PC1 on VLAN 10 is communicating with PC3 on VLAN 30 through switch S1 using VLAN interfaces configured for each VLAN.

2. PC1 sends its unicast traffic to switch S2.

3. Switch S2 tags the unicast traffic as originating on VLAN 10 as it forwards the unicast traffic out its trunk link to switch S1.

4. Switch S1 removes the VLAN tag and forwards the unicast traffic to the VLAN 10 interface.

5. Switch S1 routes the unicast traffic to its VLAN 30 interface.

6. Switch S1 then retags the unicast traffic with VLAN 30 and forwards it out the trunk link back to switch S2.

7. Switch S2 removes the VLAN tag of the unicast frame and forwards the frame out to PC3 on port F0/23.

To enable a multilayer switch to perform routing functions, the multilayer

ure to view an animation of how a router-on-a-stick performs its routing function.

As seen in the animation:

1. PC1 on VLAN 10 is communicating with PC3 on VLAN 30 through router R1 using a single, physical router interface.

2. PC1 sends its unicast traffic to switch S2.

3. Switch S2 then tags the unicast traffic as originating on VLAN 10 and forwards the unicast traffic out its trunk link to switch S1.

4. Switch S1 forwards the tagged traffic out the other trunk interface on port F0/3 to the interface on router R1.

5. Router R1 accepts the tagged unicast traffic on VLAN 10 and routes it to VLAN 30 using its configured subinterfaces.

6. The unicast traffic is tagged with VLAN 30 as it is sent out the router interface to switch S1.

7. Switch S1 forwards the tagged unicast traffic out the other trunk link to switch S2.

8. Switch S2 removes the VLAN tag of the unicast frame and forwards switch must have IP routing enabled.

Multilayer switching is more scalable than any other inter-VLAN routing implementation. This is because routers have a limited number of available ports to connect to networks. Additionally, for interfaces that are configured as a trunk line, limited amounts of traffic can be accommodated on that line at one time.

With a multilayer switch, traffic is routed internal to the switch device, which means packets are not filtered down a single trunk line to obtain new VLAN-tagging information. A multilayer switch does not, however, completely replace the functionality of a router. Routers support a significant number of additional features, such as the ability to implement greater security controls. Rather, a multilayer switch can be thought of as a Layer 2 device that is upgraded to have some routing capabilities.

Note: In this course, configuring inter-VLAN routing on a switch is restricted to configuring static routes on a 2960 switch, which is the only routing functionality supported on the 2960 switches. The 2960 switch supports up to 16 static routes (including user-configured routes and the default route) and any directly connected routes and default routes for the management interface; the 2960 switch can have an IP address as-

the frame out to PC3 on port F0/23.

Note: The router-on-a-stick method of inter-VLAN routing does not scale beyond 50 VLANs.

signed to each switch virtual interface (SVI). To enable the routing functionality on the 2960 switch, the sdm prefer lanbase-routing global configuration command must be entered and the router must be reloaded. For a full-featured, relatively inexpensive multilayer switch, the Cisco Catalyst 3560 Series switches support the EIGRP, OSPF, and BGP routing protocols.

4. **Legacy inter-VLAN routing requires routers to have multiple physical interfaces. The router accomplishes the routing by having each of its physical interfaces connected to a unique VLAN. Each interface is also configured with an IP address for the subnet associated with the particular VLAN to which it is connected. By configuring the IP addresses on the physical interfaces, network devices connected to each of the VLANs can communicate with the router using the physical interface connected to the same VLAN. In this configuration, network devices can use the router as a gateway to access the devices connected to the other VLANs.**

The routing process requires the source device to determine if the destination device is local or remote to the local subnet. The source device accomplishes this by comparing the source and destination IP addresses against the subnet mask. When the destination IP address has

Configure Legacy Inter-VLAN Routing: Switch Configuration
To configure legacy inter-VLAN routing, start by configuring the switch.

As shown in the figure, router R1 is connected to switch ports F0/4 and F0/5, which have been configured for VLANs 10 and 30, respectively.

Use the vlan vlan_id global configuration mode command to create VLANs. In this example, VLANs 10 and 30 were created on switch S1.

After the VLANs have been created, the switch ports are assigned to the appropriate VLANs. The switchport access vlan vlan_id command is executed from interface configuration mode on the switch for each interface to which the router connects.

In this example, interfaces F0/4 and F0/11 have been assigned to VLAN 10 using the switchport access vlan 10 command. The same process is

been determined to be on a remote network, the source device must identify where it needs to forward the packet to reach the destination device. The source device examines the local routing table to determine where it needs to send the data. Devices use their default gateway as the Layer 2 destination for all traffic that must leave the local subnet. The default gateway is the route that the device uses when it has no other explicitly defined route to the destination network. The IP address of the router interface on the local subnet acts as the default gateway for the sending device.

When the source device has determined that the packet must travel through the local router interface on the connected VLAN, the source device sends out an ARP request to determine the MAC address of the local router interface. When the router sends its ARP reply back to the source device, the source device can use the MAC address to finish framing the packet before it sends it out on the network as unicast traffic.

Because the Ethernet frame has the destination MAC address of the router interface, the switch knows exactly which switch port to forward the unicast traffic out of to reach the router interface for that VLAN. When the frame arrives at the router, the router removes the source and des-

used to assign interface F0/5 and F0/6 on switch S1 to VLAN 30.

Finally, to protect the configuration so that it is not lost after a reload of the switch, the copy running-config startup-config command is executed to back up the running configuration to the startup configuration.

tination MAC address information to examine the destination IP address of the packet. The router compares the destination address to entries in its routing table to determine where it needs to forward the data to reach its final destination. If the router determines that the destination network is a locally connected network, as is the case with inter-VLAN routing, the router sends an ARP request out the interface physically connected to the destination VLAN. The destination device responds back to the router with its MAC address, which the router then uses to frame the packet. The router then sends the unicast traffic to the switch, which forwards it out the port where the destination device is connected.

Click the Play button in the figure to view how legacy inter-VLAN routing is accomplished.

Even though there are many steps in the process of inter-VLAN routing, when two devices on different VLANs communicate through a router, the entire process happens in a fraction of a second

5. **Configure Legacy Inter-VLAN Routing: Router Interface Configuration**
Next, the router can be configured to perform inter-VLAN routing.

Router interfaces are configured in a manner similar to configuring VLAN

Configure Router-on-a-Stick: Preparation
Legacy inter-VLAN routing using physical interfaces has a significant limitation. Routers have a limited number of physical interfaces to connect to different VLANs. As the num-

interfaces on switches. To configure a specific interface, change to interface configuration mode from global configuration mode.

As shown in Figure 1, each interface is configured with an IP address using the ip address ip_address subnet_mask command in interface configuration mode.

In the example, interface G0/0 is configured with IP address 172.17.10.1 and subnet mask 255.255.255.0 using the ip address 172.17.10.1 255.255.255.0 command.

Router interfaces are disabled by default and must be enabled using the no shutdown command before they are used. After the no shutdown interface configuration mode command has been issued, a notification displays, indicating that the interface state has changed to up. This indicates that the interface is now enabled.

The process is repeated for all router interfaces. Each router interface must be assigned to a unique subnet for routing to occur. In this example, the other router interface, G0/1, has been configured to use IP address 172.17.30.1, which is on a different subnet than interface G0/0.

After the IP addresses are assigned to the physical interfaces and the

ber of VLANs increases on a network, having one physical router interface per VLAN quickly exhausts the physical interface capacity of a router. An alternative in larger networks is to use VLAN trunking and subinterfaces. VLAN trunking allows a single physical router interface to route traffic for multiple VLANs. This technique is termed router-on-a-stick and uses virtual subinterfaces on the router to overcome the hardware limitations based on physical router interfaces.

Subinterfaces are software-based virtual interfaces that are assigned to physical interfaces. Each subinterface is configured independently with its own IP address and subnet mask. This allows a single physical interface to simultaneously be part of multiple logical networks.

When configuring inter-VLAN routing using the router-on-a-stick model, the physical interface of the router must be connected to a trunk link on the adjacent switch. On the router, subinterfaces are created for each unique VLAN on the network. Each subinterface is assigned an IP address specific to its subnet/VLAN and is also configured to tag frames for that VLAN. This way, the router can keep the traffic from each subinterface separated as it traverses the trunk link back to the switch.

	interfaces are enabled, the router is capable of performing inter-VLAN routing. **Examine the routing table using the show ip route command.**	Functionally, the router-on-a-stick model is the same as using the legacy inter-VLAN routing model, but instead of using the physical interfaces to perform the routing, subinterfaces of a single physical interface are used.
	In Figure 2, there are two routes visible in the routing table. One route is to the 172.17.10.0 subnet, which is attached to the local interface G0/0. The other route is to the 172.17.30.0 subnet, which is attached to the local interface G0/1. The router uses this routing table to determine where to send the traffic it receives. For example, if the router receives a packet on interface G0/0 destined for the 172.17.30.0 subnet, the router would identify that it should send the packet out interface G0/1 to reach hosts on the 172.17.30.0 subnet. **Notice the letter C to the left of each of the route entries for the VLANs. This letter indicates that the route is local for a connected interface, which is also identified in the route entry. Using the output in this example, if traffic was destined for the 172.17.30.0 subnet, the router would forward the traffic out interface G0/1.**	In the figure, PC1 wants to communicate with PC3. PC1 is on VLAN 10 and PC3 is on VLAN 30. For PC1 to communicate with PC3, PC1 must have its data routed through router R1 via subinterfaces. Click the Play button in the figure to see how subinterfaces are used to route between VLANs. When the animation pauses, read the text to the left of the topology. Click Play again to continue the animation. Using trunk links and subinterfaces decreases the number of router and switch ports used. Not only can this save money, it can also reduce configuration complexity. Consequently, the router subinterface approach can scale to a much larger number of VLANs than a configuration with one physical interface per VLAN design.
6.	**To enable inter-VLAN routing using router-on-a stick, start by enabling trunking on the switch port that is connected to the router.**	Configure Router-on-a-Stick: Router Subinterface Configuration The configuration of the router is different when a router-on-a-stick configuration is used compared to legacy

In the figure, router R1 is connected to switch S1 on trunk port F0/5. VLANs 10 and 30 are added to switch S1.

Because switch port F0/5 is configured as a trunk port, the port does not need to be assigned to any VLAN. To configure switch port F0/5 as a trunk port, execute the switchport mode trunk command in interface configuration mode for port F0/5.

Note: The router does not support the Dynamic Trunking Protocol (DTP), which is used by switches, so the following commands cannot be used: switchport mode dynamic auto or switchport mode dynamic desirable.

The router can now be configured to perform inter-VLAN routing.

inter-VLAN routing. The figure shows that multiple subinterfaces are configured.

Each subinterface is created using the interface interface_id subinterface_id global configuration mode command. The syntax for the subinterface is the physical interface, in this case g0/0, followed by a period and a subinterface number. The subinterface number is configurable, but it typically reflects the VLAN number. In this example, the subinterfaces use 10 and 30 as subinterface numbers to make it easier to remember the VLANs with which they are associated. Subinterface GigabitEthernet0/0.10 is created using the interface g0/0.10 global configuration mode command.

Before assigning an IP address to a subinterface, the subinterface must be configured to operate on a specific VLAN using the encapsulation dot1q vlan_id command. In this example, subinterface G0/0.10 is assigned to VLAN 10.

Note: There is a native keyword option that can be appended to this command to set the IEEE 802.1Q native VLAN. In this example the native keyword option was excluded to leave the native VLAN default to VLAN 1.

Next, assign the IP address for the subinterface using the ip address

ip_address subnet_mask subinterface configuration mode command. In this example, subinterface G0/0.10 is assigned the IP address 172.17.10.1 using the ip address 172.17.10.1 255.255.255.0 command.

This process is repeated for all router subinterfaces required to route between the VLANs configured on the network. Each router subinterface must be assigned an IP address on a unique subnet for routing to occur. For example, the other router subinterface, G0/0.30, is configured to use IP address 172.17.30.1, which is on a different subnet from subinterface G0/0.10.

Once a physical interface is enabled, subinterfaces will automatically be enabled upon configuration. Subinterfaces do not need to be enabled with the no shutdown command at the subinterface configuration mode level of the Cisco IOS software.

If the physical interface is disabled, all subinterfaces are disabled. In this example, the command no shutdown is entered in interface configuration mode for interface G0/0, which in turn, enables all of the configured subinterfaces.

Individual subinterfaces can be administratively shut down with the shutdown command. Also, individual subinterfaces can be enabled inde-

pendently with the no shutdown command in the subinterface configuration mode.

7. **Configure Router-on-a-Stick: Verifying Subinterfaces**
By default, Cisco routers are configured to route traffic between local subinterfaces. As a result, routing does not specifically need to be enabled.

In Figure 1, the show vlan command displays information about the Cisco IOS VLAN subinterfaces. The output shows the two VLAN subinterfaces, GigabitEthernet0/0.10 and GigabitEthernet0/0.30.

Next, examine the routing table using the show ip route command (Figure 2). In the example, the routes defined in the routing table indicate that they are associated with specific subinterfaces, rather than separate physical interfaces. There are two routes in the routing table. One route is to the 172.17.10.0 subnet, which is attached to the local subinterface G0/0.10. The other route is to the 172.17.30.0 subnet, which is attached to the local subinterface G0/0.30. The router uses this routing table to determine where to send the traffic it receives. For example, if the router received a packet on subinterface G0/0.10 destined for the 172.17.30.0 subnet, the router would identify that it should send

After the router and switch have been configured to perform inter-VLAN routing, the next step is to verify host-to-host connectivity. Access to devices on remote VLANs can be tested using the ping command.

For the example shown in the figure, a ping and a tracert is initiated from PC1 to the destination address of PC3.

Ping Test

The ping command sends an ICMP echo request to the destination address. When a host receives an ICMP echo request, it responds with an ICMP echo reply to confirm that it received the ICMP echo request. The ping command calculates the elapsed time using the difference between the time the echo request was sent and the time the echo reply was received. This elapsed time is used to determine the latency of the connection. Successfully receiving a reply confirms that there is a path between the sending device and the receiving device.

Tracert Test

Tracert is a useful utility for confirming the routed path taken between two

the packet out subinterface G0/0.30 to reach hosts on the 172.17.30.0 subnet.

In Figure 3, use the Syntax Checker to configure and verify router-on-a-stick on R1.

devices. On UNIX systems, the utility is specified by traceroute. Tracert also uses ICMP to determine the path taken, but it uses ICMP echo requests with specific time-to-live values defined on the frame.

The time-to-live value determines exactly how many router hops away the ICMP echo is allowed to reach. The first ICMP echo request is sent with a time-to-live value set to expire at the first router on route to the destination device.

When the ICMP echo request times out on the first route, an ICMP message is sent back from the router to the originating device. The device records the response from the router and proceeds to send out another ICMP echo request, but this time with a greater time-to-live value. This allows the ICMP echo request to traverse the first router and reach the second device on route to the final destination. The process repeats recursively until finally the ICMP echo request is sent all the way to the final destination device. After the tracert utility finishes running, it displays a list of ingress router interfaces that the ICMP echo request reached on its way to the destination.

In the example, the ping utility was able to send an ICMP echo request to the IP address of PC3. Also, the tracert utility confirms that the path

to PC3 is through the 172.17.10.1 subinterface IP address of router R1.

8. **There are several common switch misconfigurations that can arise when configuring routing between multiple VLANs.**

   When using the legacy routing model for inter-VLAN routing, ensure that the switch ports that connect to the router interfaces are configured with the correct VLANs. If a switch port is not configured for the correct VLAN, devices configured on that VLAN cannot connect to the router interface; therefore, those devices are unable to send data to the other VLANs.

   As shown in the Figure 1 topology, PC1 and router R1 interface G0/0 are configured to be on the same logical subnet, as indicated by their IP address assignment. However, the switch port F0/4 that connects to router R1 interface G0/0 has not been configured and remains in the default VLAN. Because router R1 is on a different VLAN than PC1, they are unable to communicate.

   To correct this problem, execute the switchport access vlan 10 interface configuration mode command on switch port F0/4 on switch S1. When the switch port is configured for the correct VLAN, PC1 can communicate with router R1 interface G0/0,

   When a problem is suspected with a switch configuration, use the various verification commands to examine the configuration and identify the problem.

   The screen output in Figure 1 shows the results of the show interfaces interface-id switchport command. Assume that you have issued these commands because you suspect that VLAN 10 has not been assigned to port F0/4 on switch S1. The top highlighted area shows that port F0/4 on switch S1 is in access mode, but it does not show that it has been directly assigned to VLAN 10. The bottom highlighted area confirms that port F0/4 is still set to the default VLAN. The show running-config and the show interfaces interface-id switchport commands are useful for identifying VLAN assignment and port configuration issues.

   Figure 2 shows that after a device configuration has changed, communication between router R1 and switch S1 has stopped. The link between the router and the switch is supposed to be a trunk link. The screen output shows the results of the show interfaces interface_id switchport and the show running-config commands. The top highlighted area confirms that port F0/4 on switch S1 is in access

which allows it to access the other VLANs connected to router R1.

The Figure 2 topology shows the router-on-a-stick routing model. However, interface F0/5 on switch S1 is not configured as a trunk and is left in the default VLAN for the port. As a result, the router is unable to route between VLANs because each of its configured subinterfaces is unable to send or receive VLAN-tagged traffic.

To correct this problem, issue the switchport mode trunk interface configuration mode command on switch port F0/5 on S1. This converts the interface to a trunk port, allowing a trunk to be established between R1 and S1. When the trunk is successfully established, devices connected to each of the VLANs are able to communicate with the subinterface assigned to their VLAN, thus enabling inter-VLAN routing.

The Figure 3 topology shows the trunk link between S1 and S2 is down. Because there is no redundant connection or path between the devices, all devices connected to S2 are unable to reach router R1. As a result, all devices connected to S2 are unable to route to other VLANs through R1.

To reduce the risk of a failed inter-switch link disrupting in-

mode, not trunk mode. The bottom highlighted area also confirms that port F0/4 has been configured for access mode.

ter-VLAN routing, redundant links and alternate paths should be accounted for within the network design.

9. **When enabling inter-VLAN routing on a router, one of the most common configuration errors is to connect the physical router interface to the wrong switch port. This places the router interface in the incorrect VLAN and prevents it from reaching the other devices within the same subnet.**

   As shown in the figure, router R1 interface G0/0 is connected to switch S1 port F0/9. Switch port F0/9 is configured for the default VLAN, not VLAN 10. This prevents PC1 from being able to communicate with the router interface. Therefore, it is unable to route to VLAN 30.

   To correct this problem, physically connect the router R1 interface G0/0 to switch S1 port F0/4. This puts the router interface in the correct VLAN and allows inter-VLAN routing. Alternately, change the VLAN assignment of switch port F0/9 to VLAN 10. This also allows PC1 to communicate with router R1 interface G0/0.

Verify Router Configuration
With router-on-a-stick configurations, a common problem is assigning the wrong VLAN ID to the subinterface.

As shown in Figure 1, router R1 has been configured with the wrong VLAN on subinterface G0/0.10, preventing devices configured on VLAN 10 from communicating with subinterface G0/0.10. This subsequently prevents those devices from being able to send data to other VLANs on the network.

Using the show interfaces and the show running-config commands can be useful in troubleshooting this type of issue, as shown in the figure.

The show interfaces command produces a lot of output, making it sometimes difficult to see the problem, as shown in Figure 2. However, the top highlighted section shows that the subinterface G0/0.10 on router R1 uses VLAN 100.

The show running-config command confirms that subinterface G0/0.10 on router R1 has been configured to allow access to VLAN 100 traffic and not VLAN 10.

To correct this problem, configure subinterface G0/0.10 to be on the correct VLAN using the encapsulation dot1q 10 subinterface configuration mode command. When the subinterface has been assigned to the correct VLAN, it is accessible by devices on that VLAN and the router can perform inter-VLAN routing.

With proper verification, router configuration problems are quickly addressed, allowing inter-VLAN routing to function properly.

10. **VLANs correspond to unique subnets on the network. For inter-VLAN routing to operate, a router must be connected to all VLANs, either by separate physical interfaces or by subinterfaces. Each interface, or subinterface, must be assigned an IP address that corresponds to the subnet to which it is connected. This permits devices on the VLAN to communicate with the router interface and enables the routing of traffic to other VLANs connected to the router.**

    The following are some common IP addressing errors:

    As shown in Figure 1, router R1 has been configured with an incorrect IP address on interface G0/0. This prevents PC1 from being able to communicate with router R1 on VLAN 10. To correct this problem,

Each interface, or subinterface, must be assigned an IP address corresponding to the subnet to which it is connected. A common error is to incorrectly configure an IP address for a subinterface. Figure 1 displays the output of the show running-config command. The highlighted area shows that subinterface G0/0.10 on router R1 has an IP address of 172.17.20.1. The VLAN for this subinterface should support VLAN 10 traffic. The IP address has been configured incorrectly. The show ip interface command is useful in this setting. The second highlight shows the incorrect IP address.

Sometimes it is the end-user device, such as a personal computer, that is improperly configured. Figure 2 shows the displayed IP configuration for PC1. The IP address is 172.17.20.21, with a subnet mask of

assign the correct IP address to router R1 interface G0/0 using the ip address 172.17.10.1 255.255.255.0 command. After the router interface has been assigned the correct IP address, PC1 can use the router interface as a default gateway for accessing other VLANs.
In Figure 2, PC1 has been configured with an incorrect IP address for the subnet associated with VLAN 10. This prevents PC1 from being able to communicate with router R1 on VLAN 10.To correct this problem, assign the correct IP address to PC1. Depending on the type of PC being used, the configuration details may be different.
In Figure 3, PC1 has been configured with the incorrect subnet mask. According to the subnet mask configured for PC1, PC1 is on the 172.17.0.0 network.The result is that PC1 calculates that PC3, with the IP address 172.17.30.23, is on the same subnet as PC1. PC1 does not forward traffic destined for PC3 to router R1 interface G0/0; therefore, the traffic never reaches PC3.To correct this problem, change the subnet mask on PC1 to 255.255.255.0. Depending on the type of PC being used, the configuration details can be different.

255.255.255.0. But in this scenario, PC1 should be in VLAN 10, with an address of 172.17.10.21 and a subnet mask of 255.255.255.0.

Note: Although configuring subinterface IDs to match the VLAN number makes it easier to manage inter-VLAN configuration, it is not a requirement. When troubleshooting addressing issues, ensure that the subinterface is configured with the correct address for that VLAN.

11. **Router-on-a-stick is simple to implement because routers are usually available in every network. As shown in the figure, most enterprise**

In the early days of switched networks, switching was fast (often at hardware speed, meaning the speed was equivalent to the time it took to

networks use multilayer switches to achieve high-packet processing rates using hardware-based switching. Layer 3 switches usually have packet-switching throughputs in the millions of packets per second (pps), whereas traditional routers provide packet switching in the range of 100,000 pps to more than 1 million pps.

All Catalyst multilayer switches support the following types of Layer 3 interfaces:

Routed port - A pure Layer 3 interface similar to a physical interface on a Cisco IOS router.
Switch virtual interface (SVI) - A virtual VLAN interface for inter-VLAN routing. In other words, SVIs are the virtual-routed VLAN interfaces.
High-performance switches, such as the Catalyst 6500 and Catalyst 4500, perform almost every function involving OSI Layer 3 and higher using hardware-based switching that is based on Cisco Express Forwarding.

All Layer 3 Cisco Catalyst switches support routing protocols, but several models of Catalyst switches require enhanced software for specific routing protocol features. Catalyst 2960 Series switches running IOS Release 12.2(55) or later, support static routing.

physically receive and forward frames onto other ports) and routing was slow (routing had to be processed in software). This prompted network designers to extend the switched portion of the network as much as possible. Access, distribution, and core layers were often configured to communicate at Layer 2. This topology created loop issues. To solve these issues, spanning-tree technologies were used to prevent loops while still enabling flexibility and redundancy in inter-switch connections.

However, as network technologies have evolved, routing has become faster and cheaper. Today, routing can be performed at wire speed. One consequence of this evolution is that routing can be transferred to the core and the distribution layers without impacting network performance.

Many users are in separate VLANs, and each VLAN is usually a separate subnet. Therefore, it is logical to configure the distribution switches as Layer 3 gateways for the users of each access switch VLAN. This implies that each distribution switch must have IP addresses matching each access switch VLAN.

Layer 3 (routed) ports are normally implemented between the distribution and the core layer.

The network architecture depicted is

Catalyst switches use different default settings for interfaces. All members of the Catalyst 3560 and 4500 families of switches use Layer 2 interfaces by default. Members of the Catalyst 6500 family of switches running Cisco IOS use Layer 3 interfaces by default. Depending on which Catalyst family of switches is used, the switchport or no switchport interface configuration mode commands might be present in the running config or startup configuration files.

not dependent on spanning tree because there are no physical loops in the Layer 2 portion of the topology.

12. **An SVI is a virtual interface that is configured within a multilayer switch, as shown in the figure. An SVI can be created for any VLAN that exists on the switch. An SVI is considered to be virtual because there is no physical port dedicated to the interface. It can perform the same functions for the VLAN as a router interface would, and can be configured in much the same way as a router interface (i.e., IP address, inbound/outbound ACLs, etc.). The SVI for the VLAN provides Layer 3 processing for packets to or from all switch ports associated with that VLAN.**

    By default, an SVI is created for the default VLAN (VLAN 1) to permit remote switch administration. Additional SVIs must be explicitly created. SVIs are created the first time the VLAN interface configura-

A routed port is a physical port that acts similarly to an interface on a router. Unlike an access port, a routed port is not associated with a particular VLAN. A routed port behaves like a regular router interface. Also, because Layer 2 functionality has been removed, Layer 2 protocols, such as STP, do not function on a routed interface. However, some protocols, such as LACP and EtherChannel, do function at Layer 3.

Unlike Cisco IOS routers, routed ports on a Cisco IOS switch do not support subinterfaces.

Routed ports are used for point-to-point links. Connecting WAN routers and security devices are examples of the use of routed ports. In a switched network, routed ports are mostly configured between switches in the core and distribution layer. The

tion mode is entered for a particular VLAN SVI, such as when the interface vlan 10 command is entered. The VLAN number used corresponds to the VLAN tag associated with data frames on an 802.1Q encapsulated trunk or to the VLAN ID (VID) configured for an access port. When creating an SVI as a gateway for VLAN 10, name the SVI interface VLAN 10. Configure and assign an IP address to each VLAN SVI.

Whenever the SVI is created, ensure that particular VLAN is present in the VLAN database. In the figure, the switch should have VLAN 10 and VLAN 20 present in the VLAN database; otherwise, the SVI interface stays down.

The following are some of the reasons to configure SVI:

To provide a gateway for a VLAN so that traffic can be routed into or out of that VLAN
To provide Layer 3 IP connectivity to the switch
To support routing protocol and bridging configurations
The following are some of the advantages of SVIs (the only disadvantage is that multilayer switches are more expensive):

It is much faster than router-on-a-stick, because everything is hardware switched and rout-

figure illustrates an example of routed ports in a campus switched network.

To configure routed ports, use the no switchport interface configuration mode command on the appropriate ports. For example, the default configuration of the interfaces on Catalyst 3560 switches are Layer 2 interfaces, so they must be manually configured as routed ports. In addition, assign an IP address and other Layer 3 parameters as necessary. After assigning the IP address, verify that IP routing is globally enabled and that applicable routing protocols are configured.

Note: Routed ports are not supported on Catalyst 2960 Series switches.

ed.
No need for external links from the switch to the router for routing.
Not limited to one link. Layer 2 EtherChannels can be used between the switches to get more bandwidth.
Latency is much lower, because it does not need to leave the switch.

13. **A Catalyst 2960 switch can function as a Layer 3 device and route between VLANs and a limited number of static routes.**

    The Cisco Switch Database Manager (SDM) provides multiple templates for the 2960 switch. The templates can be enabled to support specific roles depending on how the switch is used in the network. For example, the SDM lanbase-routing template can be enabled to allow the switch to route between VLANs and to support static routing.

    In Figure 1, the show sdm prefer command is entered on switch S1 and the default template is applied. The default template is the factory default setting for a Catalyst 2960 switch. The default template does not support static routing. If IPv6 addressing has been enabled, the template will be dual-ipv4-and-ipv6 default.

    The SDM template can be changed in global configuration mode with the sdm prefer command.

    The issues common to legacy inter-VLAN routing and router-on-a-stick inter-VLAN routing are also manifested in the context of Layer 3 switching. To troubleshoot Layer 3 switching issues, the following items should be checked for accuracy:

    VLANs - VLANs must be defined across all the switches. VLANs must be enabled on the trunk ports. Ports must be in the right VLANs.
    SVIs - SVI must have the correct IP address or subnet mask. SVI must be up. SVI must match with the VLAN number.
    Routing - Routing must be enabled. Each interface or network should be added to the routing protocol.
    Hosts - Hosts must have the correct IP address or subnet mask. Hosts must have a default gateway associated with an SVI or routed port.
    To troubleshoot the Layer 3 switching problems, be familiar with the implementation and design layout of the topology.

Note: In Figures 2, 4, 6, and 7, the do command is used to execute user EXEC or privileged EXEC commands from other router configuration modes.

In Figure 2, the SDM template options are displayed with the sdm prefer ? command. The SDM template is changed to lanbase-routing. The switch must be reloaded for the new template to take effect.

In Figure 3, the lanbase-routing template is active on S1. With this template, static routing is supported for up to 750 static routes.

In Figure 4, interface F0/6 on S1 is assigned to VLAN 2. The SVIs for VLANs 1 and 2 are also configured with IP addresses 192.168.1.1/24 and 192.168.2.1/24, respectively. IP routing is enabled with the ip routing global configuration mode command.

Note: The ip routing command is automatically enabled on Cisco routers; however, the corresponding command for IPv6, ipv6 unicast-routing, is disabled, by default, on Cisco routers and switches.

In Figure 5, router R1 has two IPv4 networks configured: interface G0/1 has IP address 192.168.1.10/24 and loopback interface Lo0 has IP ad-

dress 209.165.200.225/27. The show ip route command output is displayed.

A default route is configured on S1 in Figure 6. The show ip route command output is displayed.

A static route to the remote network 192.168.2.0/24 (VLAN 2) is configured on R1 in Figure 7. The show ip route command output is displayed.

In Figure 8, PC-A is configured with IP address 192.168.2.2/24 in VLAN 2 and PC-B is configured with IP address 192.168.1.2/24 in VLAN 1. PC-B is able to ping both PC-B and the loopback interface on R1.

In Figure 9, use the Syntax Checker to configure static routing on S1.

14. **Company XYZ is adding a new floor, floor 5, to the network. Based on this, the current requirements are to make sure the users on floor 5 can communicate with users on other floors. Currently, users on floor 5 cannot communicate with users on other floors. The following is an implementation plan to install a new VLAN for users on floor 5 and to ensure the VLAN is routing to other VLANs.**

    There are four steps to implementing a new VLAN:

    Your company has just purchased a three-level building. You are the network administrator and must design the company inter-VLAN routing network scheme to serve a few employees on each floor.

    Floor 1 is occupied by the HR Department, Floor 2 is occupied by the IT Department, and Floor 3 is occupied by the Sales Department. All Departments must be able to communicate with each other, but at the same time have their own separate working networks.

Step 1. Create a new VLAN 500 on the fifth floor switch and on the distribution switches. Name this VLAN.

Step 2. Identify the ports needed for the users and switches. Set the switchport access vlan command to 500 and ensure that the trunk between the distribution switches is properly configured and that VLAN 500 is allowed on the trunk.

Step 3. Create an SVI interface on the distribution switches and ensure that IP addresses are assigned.

Step 4. Verify connectivity.

The troubleshooting plan checks for the following:

Step 1. Verify that all VLANs have been created:

Was the VLAN created on all the switches?
Verify with the show vlan command.
Step 2. Ensure that ports are in the right VLAN and trunking is working as expected:

Did all access ports have the switchport access VLAN 500 command added?
Were there any other ports that should have been added? If so, make those changes.
Were these ports previously used? If so, ensure that there are no extra

You brought three Cisco 2960 switches and a Cisco 1941 series router from the old office location to serve network connectivity in the new building. New equipment is non-negotiable.

Refer to the PDF for this activity for further instructions.

commands enabled on these ports that can cause conflicts. If not, is the port enabled?
Are any user ports set to trunks? If so, issue the switchport mode access command.
Are the trunk ports set to trunk mode?
Is manual pruning of VLANs configured? If so, ensure that the trunks necessary to carry VLAN 500 traffic have the VLAN in the allowed statements.
Step 3. Verify SVI configurations (if necessary):

Is the SVI already created with the correct IP address and subnet mask?
Is it enabled?
Is routing enabled?
Is this SVI added in the routing protocol?
Step 4. Verify connectivity:

Are all the links between switches in trunk mode?
Is VLAN 500 allowed on all trunks?
Is spanning-tree blocking any of the participating links?
Are the ports enabled?
Do the hosts have the right default gateways assigned?
Ensure that the default route or some routing protocol is enabled if necessary.

15. Inter-VLAN routing is the process of routing traffic between different

VLANs, using either a dedicated router or a multilayer switch. Inter-VLAN routing facilitates communication between devices isolated by VLAN boundaries.

Legacy inter-VLAN routing depended on a physical router port being available for each configured VLAN. This has been replaced by the router-on-a-stick topology that relies on an external router with subinterfaces trunked to a Layer 2 switch. With the router-on-a-stick option, appropriate IP addressing and VLAN information must be configured on each logical subinterface and a trunk encapsulation must be configured to match that of the trunking interface of the switch.

Another option is multilayer inter-vlan option using Layer 3 switching. Layer 3 switching involves SVIs and routed ports. Layer 3 switching is normally configured at the distribution and core layers of the hierarchical design model. Layer 3 switching with SVIs is a form of inter-VLAN routing. A routed port is a physical port that acts similarly to an interface on a router. Unlike an access port, a routed port is not associated with a particular VLAN.

Catalyst 2960 switches can be used in multilayer inter-vlan routing. These switches support static routing, but dynamic routing protocols

are not supported. SDM templates are required for enabling IP routing on 2960 switches.

Troubleshooting inter-VLAN routing with a router or a Layer 3 switch are similar. Common errors involve VLAN, trunk, Layer 3 interface, and IP address configurations.

Chapter 9 - Implementing Secure Network Designs

Study online at https://quizlet.com/_bv10l8

1.	**Single Point of Failure**	a "pinch point" relying on a single hardware server or appliance or network channel
2.	**Complex Dependencies**	services that require many different systems to be available
3.	**Switch**	forward frames between nodes in a cabled network that work at layer 2 of the OSI model and make forwarding decisions based on the hardware or MAC address of the attached nodes
4.	**Virtual LANs (VLANs)**	a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group
5.	**Wireless Access Point**	a layer 2 device that provides a bridge between a cabled network and wireless clients (stations)
6.	**Routers**	a layer 3 device that forwards packets around an internetwork, making forwarding decisions based on IP addresses
7.	**Firewalls**	apply an access control list to filter traffic passing in or out of a network segment (layer 3+)
8.	**Load Balancer**	this layer 4 device distributes traffic between network segments or servers to optimize performance
9.	**Domain Name System (DNS) Server**	this layer 7 device hosts name records and performs name resolution to allow applications and users to address hosts and servers using fully qualified domain names (FQDNs) rather than IP addresses
10.	**Layer 2 Forwarding**	this type of forwarding occurs between nodes on the same local network segment that are all in the same broadcast domain and identified by MAC address
11.	**Layer 3 Forwarding**	this type of forwarding, also known as routing, occurs between both logically and physically defined networks and is identified by IP address

12.	**Address Resolution Protocol (ARP)**	maps a network interface's hardware (MAC) address to an IP address
13.	**Internet Protocol (IP)**	provides the addressing mechanism for logical networks and subnets
14.	**Border Gateway Protocol (BGP)**	a gateway protocol that enables the internet to exchange routing information between autonomous systems (AS)
15.	**Open Shortest Path First (OSPF)**	a link-state routing protocol that was developed for IP networks and is based on the Shortest Path First (SPF) algorithm
16.	**Enhanced Interior Gateway Routing Protocol (EIGRP)**	a network protocol that enables routers to exchange information more efficiently than earlier network protocols
17.	**Routing Information Protocol (RIP)**	a distance vector protocol that defines how routers should share information when moving traffic among an interconnected group of local area networks
18.	**Network Segment**	a portion of a computer network where all hosts attached to the segment can use local (layer 2) forwarding to communicate freely with one another
19.	**Segregation**	means that the hosts in one segment are restricted in the way they communicate with hosts in other segments
20.	**Network Topology**	a description of how a computer network is physically or logically organized
21.	**Zone**	an area of the network where the security configuration is the same for all hosts within it
22.	**Intranet (Private Network)**	this is a network of trusted hosts owned and controlled by the organization
23.	**Extranet**	

		this is a network of semi-trusted hosts, typically representing business partners, suppliers, or customers. Hosts must authenticate to join the extranet
24.	**Internet/guest**	this is a zone permitting anonymous access (or perhaps a mix of anonymous and authenticated access) by untrusted hosts over the Internet
25.	**Demilitarized Zones (DMZs)**	a perimeter or edge network that enables external clients to access data on private systems without compromising the security of the internal network as a whole
26.	**Bastion Host**	is a specialized computer that is deliberately exposed on a public network
27.	**Screened Subnet**	a network architecture where a single firewall is used with three network interfaces
28.	**Triple-Homed Firewall**	one router/firewall appliance with three network interfaces
29.	**Screened Host**	a firewall that is implemented using a firewall router and a proxy server, with the router acting as a front end to the server
30.	**North-South Traffic**	traffic that goes to and from a data center
31.	**East-West Traffic**	traffic that goes from a server to a data center and vice versa
32.	**Zero-Trust**	uses systems such as continuous authentication and conditional access to mitigate privilege escalation and account compromise by threat actors
33.	**Network Mapping**	a method of discovering and visualizing physical and virtual network connectivity through interconnected tasks that include flow charts, network diagrams, topology identification, and device inventories

34.	**Eavesdropping**	when a hacker intercepts, deletes, or modifies data that is transmitted between two devices
35.	**Man-in-the-Middle (MitM) Attack**	where the threat actor gains a position between two hosts, and transparently captures, monitors, and relays all communication between the hosts
36.	**MAC Cloning**	this type of attack changes the hardware address configured on an adapter interface or asserts the use of an arbitrary MAC address
37.	**ARP Poisoning**	uses a packet crafter to broadcast unsolicited ARP reply packets and update their MAC:IP address cache table with the spoofed address
38.	**MAC Flooding**	in this attack, the intention of the attacker is to exhaust the memory used to store the switch's MAC address table
39.	**Spanning Tree Protocol (STP)**	a means for the bridges to organize themselves into a hierarchy and prevent loops from forming
40.	**Broadcast Storm**	an abnormally high number of broadcast packets within a short period of time
41.	**Bridge Protocol Data Unit (BPDU)**	data units used to communicate information about the topology and are not expected on access ports
42.	**MAC Filtering**	this is configured on a switch to define which MAC Addresses are allowed to connect to a particular port
43.	**Dynamic Host Configuration Protocol (DHCP) Snooping**	determines whether traffic sources are trusted or untrusted and filters messages and rate-limits traffic from untrusted sources
44.	**Dynamic ARP Inspection**	prevents a host attached to an untrusted port from flooding the segment with gratuitous ARP replies
45.		means that the switch uses an AAA server to authenticate the attached device before activating the port

	Port-Based Network Access Control (PNAC)	
46.	**Network Access Control (NAC)**	these products extend the scope of authentication to allow administrators to devise policies or profiles describing a minimum security configuration that devices must meet to be granted network access (health policy)
47.	**Posture Assessment**	is the process by which host health checks are performed against a client device to verify compliance with the health policy
48.	**Persistent Agent**	agent is installed as a software application on the client
49.	**Non-Persistent Agent (Dissolvable)**	agent is loaded into memory during posture assessment but not installed on the device
50.	**Source Routing**	This uses an option in the IP header to pre-determine the route a packet will take through the network (strict) or "waypoints" that it must pass through (loose)
51.	**Service Set Identifier (SSID)**	a sequence of characters that uniquely names a wireless local area network (WLAN)
52.	**Basic Service Set Identifier (BSSID)**	used in infrastructure mode to identify the media access control (MAC) address of the access point
53.	**Co-Channel Interference (CCI)**	when two WAPs in close proximity use the same channel and compete for bandwidth within that channel as signals collide and have to be re-transmitted
54.	**Adjacent Channel Interference (ACI)**	when the channels selected for WAPs are not cleanly spaced, the interference pattern creates significant numbers of errors and loss of bandwidth
55.	**Site Survey**	used to measure signal strength and channel usage throughout the area to cover

56.	**Heat Map**	shows the real-time coverage (if a signal is strong (red) or weak (green/blue)) and quality of a wireless infrastructure overlaid on a map, typically a floor plan
57.	**Wireless Controller**	can be a hardware appliance or a software application and manages wireless network access points that allow wireless devices to connect to the network
58.	**Fat WAP**	an access point whose firmware contains enough processing logic to be able to function autonomously and handle clients without the use of a wireless controller
59.	**Thin WAP**	an access point whose firmware does not contain enough processing logic to be able to function autonomously and handle clients without the use of a wireless controller
60.	**Temporal Key Integrity Protocol (TKIP)**	a security protocol used in the IEEE 802.11 wireless networking standard as a solution to replace WEP without requiring the replacement of legacy hardware
61.	**Simultaneous Authentication of Equals (SAE)**	replaces WPA's 4-way handshake authentication and association mechanism with a protocol based on Diffie-Hellman key agreement
62.	**Enhanced Open**	enhances encryption for the open authentication method
63.	**AES Galois Counter Mode Protocol (GCMP)**	a block cipher mode of operation that uses universal hashing over a binary Galois field to provide authenticated encryption
64.	**Management Protection Frames**	mandates the use of these to protect against key-recovery attacks
65.	**Pre-Shared Key Authentication (PSK)**	uses a passphrase to generate the key that is used to encrypt communications in WPA2
66.	**Password Authenticated**	

	Key Exchange (PAKE)	in WPA3, uses a passphrase to authenticate stations in personal mode but changes the method by which this secret is used to agree on session keys
67.	**Simultaneous Authentication of Equals (SAE) protocol**	in WPA3, this uses the Dragonfly handshake, which is basically Diffie-Helllman over elliptic curves key agreement, combined with a hash value derived from the password and device MAC address to authenticate the nodes
68.	**Wi-Fi Protected Setup (WPS)**	is a network security standard to create a secure wireless home network
69.	**Captive Portal**	a web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi or wired network before they are granted broader access to network resources
70.	**Extensible Authentication Protocol (EAP)**	is an authentication framework for providing the transport and usage of material and parameters generated by EAP methods
71.	**Protected Extensible Authentication Protocol (PEAP)**	an encrypted tunnel is established between the supplicant and authentication server and only requires a server-side public key certificate
72.	**EAP-Tunneled TLS (EAP-TTLS)**	uses a server-side certificate to establish a protected tunnel through which the user's authentication credentials can be transmitted to the authentication server using any inner authentication protocol
73.	**EAP with Flexible Authentication via Secure Tunneling (EAP-FAST)**	uses a Protected Access Credential (PAC) generated for each user from the authentication server's master key to set up the tunnel
74.	**RADIUS federation**	multiple organizations allow access to one another's users by joining their RADIUS servers into a RADIUS hierarchy or mesh

75.	**Rogue Access Point**	one that has been installed on the network without authorization, whether with malicious intent or not
76.	**Evil Twin**	rogue WAP masquerading as a legitimate one
77.	**Deauthentication Attack**	sends a stream of spoofed frames to cause a client to deauthenticate from a WAP by spoofing the MAC address of the target station
78.	**Initialization Vector (IV) Attack**	an attack on a wireless network that modifies the IV of an encrypted wireless packet during transmission
79.	**Jamming Attack**	the transmission of radio signals that disrupt communications by decreasing the Signal-to-Inference-plus-Noise ratio (SINR)
80.	**Spectrum Analyzer**	displays a spectrum of signal amplitudes on different frequencies
81.	**Distributed DoS Attack (DDoS)**	a DoS attack that is launched from multiple devices simultaneously
82.	**SYN Flood Attack**	this type of attack aims to bombard a target system with SYN requests in an attempt to overwhelm connection queues and force a system to become unresponsive to legitimate requests
83.	**Distributed Reflection DoS (DRDoS)**	when the threat actor spoofs the victim's IP address and attempts to open connections with multiple servers
84.	**Application Attack**	this type of attack targets vulnerabilities in the headers and payloads of specific application protocols
85.	**Operational Technology**	systems that monitor and control physical electromechanical components such as valves, motors, electrical switches, gauges, and sensors
86.	**Blackhole**	an area of the network that cannot reach any other area of the network

87.	**Remotely Triggered Blackhole (RTBH)**	a technique that provides the ability to drop undesirable traffic before it enters a protected network
88.	**Sinkhole Routing**	this defense works by intercepting DNS requests attempting to connect to known malicious or unwanted domains and returning a false, or rather controlled IP address
89.	**Layer 4 Load Balancer**	basic load balancers make forwarding decisions on IP address and TCP/UDP port values, working at the transport layer of the OSI model
90.	**Layer 7 Load Balancer**	(content switch) this exists because of the need to be able to make forwarding decisions based on application-level data
91.	**Session Affinity**	a layer 4 approach to handling user sessions, when a client establishes a session, it becomes stuck to the node that first accepted the request
92.	**Clustering**	allows multiple redundant processing nodes that share data with one another to accept connections
93.	**Virtual IP**	the public IP used to access the service is shared between the two instances in the cluster
94.	**Quality of Service (QoS)**	a framework for prioritizing traffic based on its characteristics
95.	**Latency**	the time it takes for a transmission to reach the recipient, measured in milliseconds (ms)
96.	**Jitter**	defined as being a variation in the delay, or an inconsistent rate of packet delivery

Implement Secure Switching and Routing

Study online at https://quizlet.com/_alzdbe

1.	**network mapping**	Software that can scan a network and identify hosts, addresses, protocols, network interconnections, and so on
2.	**eavesdropping**	listening in to communications sent over the media
3.	**MAC Cloning**	An attack in which an attacker falsifies the factory-assigned MAC address of a device's network interface
4.	**packet crafting**	A method of manually generating packets (instead of modifying existing network traffic) to test the behavior of network devices, enabling a hacker to enumerate firewall or intrusion detection rules that are in place
5.	**ARP Poisoning Attack**	A network-based attack where an attacker with access to the target local network segment redirects an IP address to the MAC address of a computer that is not the intended recipient. This can be used to perform a variety of attacks, including DoS, spoofing, and Man-in-the-Middle
6.	**MAC flooding**	A variation of an ARP poisoning attack where a switch's cache table is inundated with frames from random source MAC addresses
7.	**MAC address table**	The table on a switch keeping track of MAC addresses associated with each port. As the switch uses a type of memory called Content Addressable Memory (CAM), this is sometimes called the CAM table
8.	**Spanning Tree Protocol (STP)**	A protocol that enables switches to detect and repair bridge loops automatically.
9.	**broadcast storm**	Traffic that is recirculated and amplified by loops in a switching topology, causing network slowdowns and crashing switches
10.	**port security**	Preventing a device attached to a switch port from communicating on the network unless it matches a given MAC address or other protection profile
11.	**MAC filtering**	

		Applying an access control list to a switch or access point so that only clients with approved MAC addresses can connect to it
12.	**Dynamic Host Configuration Protocol (DHCP) snooping**	A configuration option that enables a switch to inspect DHCP traffic to prevent MAC spoofing.
13.	**port-based network access control (PNAC)**	A switch (or router) that performs some sort of authentication of the attached device before activating the port
14.	**Network Access Control (NAC)**	A general term for the collected protocols, policies, and hardware that authenticate and authorize access to a network at the device level
15.	**posture assessment**	The process for verifying compliance with a health policy by using host health checks.

Topic 9B
Implement Secure Switching and Routing

Study online at https://quizlet.com/_9mts91

1.	**Network Mapping**	The process of discovering and identifying the devices on a network.
2.	**Eavesdropping**	Some transmission media are susceptible to eavesdropping (listening in to communications sent over the media). To secure transmissions, they must be encrypted
3.	**Man-in-the-Middle/On-Path Attacks**	MitM or on-path attack is where the threat actor gains a position between two hosts, and transparently captures, monitors, and relays all communication between the hosts
4.	**MAC Cloning**	MAC address spoofing, changes the hardware address configured on an adapter interface or asserts the use of an arbitrary MAC address.
5.	**Address Resolution Protocol (ARP)**	The broadcast mechanism by which individual hardware MAC addresses are matched to an IP address on a local network segment.
6.	**ARP Poisoning Attack**	Uses a packet crafter, such as Ettercap, to broadcast unsolicited ARP reply packets. Because ARP has no security mechanism, the receiving devices trust this communication and update their MAC:IP address cache table with the spoofed address
7.	**MAC Flooding Attacks**	A variation of an ARP poisoning attack where a switch's cache table is inundated with frames from random source MAC addresses.
8.	**Spanning Tree Protocol (STP).**	A switching protocol that prevents network loops by dynamically disabling links as needed. Designed to prevent Broadcast Storms
9.	**Broadcast Storm**	Traffic that is recirculated and amplified by loops in a switching topology, causing network slowdowns and crashing switches.
10.		Switch port security feature that disables the port if it receives BPDU notifications related to spanning tree. This

	Bridge Protocol Data Unit (BPDU) Guard	is configured on access ports where there any BPDU frames are likely to be malicious.
11.	**Port Security**	Preventing a device attached to a switch port from communicating on the network unless it matches a given MAC address or other protection profile.
12.	**MAC filtering**	Applying an access control list to a switch or access point so that only clients with approved MAC addresses can connect to it. On a switch means defining which MAC addresses are allowed to connect to a particular port.
13.	**DHCP Snooping**	A configuration option that enables a switch to inspect DHCP traffic to prevent MAC spoofing.
14.	**DHCP**	protocol that allows a server to assign IP address information to a client when it connects to the network
15.	**port-based network access control (PNAC)**	
16.	**Endpoint security**	Set of security procedures and technologies designed to restrict network access at a device level.
17.	**Network access control (NAC)**	A general term for the collected protocols, policies, and hardware that authenticate and authorize access to a network at the device level.
18.	**Posture assessment**	The process by which host health checks are performed against a client device to verify compliance with the health policy.

CCNA Routing and Switching Essentials Chapter 9

Study online at https://quizlet.com/_1byepf

1. **B. 172.16.2.0 to 172.16.3.255**

Which IPv4 address range covers all IP addresses that match the ACL filter specified by 172.16.2.0 with wildcard mask 0.0.1.255?
A. 172.16.2.1 to 172.16.255.255
B. 172.16.2.0 to 172.16.3.255
C. 172.16.2.1 to 172.16.3.254
D. 172.16.2.0 to 172.16.2.255

2. **D. R1(config)# interface gi0/0**
R1(config-if)# no ip access-group 105 out
R1(config)# no access-list 105
R1(config)# access-list 105 permit udp host 10.0.70.23 host 10.0.54.5 range 1024 5000
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
R1(config)# access-list 105 deny ip any any
R1(config)# interface gi0/0
R1(config-if)# ip access-group 105 out

Consider the following access list that allows IP phone configuration file transfers from a particular host to a TFTP server:
R1(config)# access-list 105 permit udp host 10.0.70.23 host 10.0.54.5 range 1024 5000
R1(config)# access-list 105 deny ip any any
R1(config)# interface gi0/0
R1(config-if)# ip access-group 105 out
Which method would allow the network administrator to modify the ACL and include FTP transfers from any source IP address?
A. R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
B. R1(config)# access-list 105 permit udp host 10.0.70.23 host 10.0.54.5 range 1024 5000
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
R1(config)# access-list 105 deny ip any any
C. R1(config)# interface gi0/0
R1(config-if)# no ip access-group 105 out
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
R1(config)# interface gi0/0
R1(config-if)# ip access-group 105 out
D. R1(config)# interface gi0/0

R1(config-if)# no ip access-group 105 out
R1(config)# no access-list 105
R1(config)# access-list 105 permit udp host 10.0.70.23 host 10.0.54.5 range 1024 5000
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 20
R1(config)# access-list 105 permit tcp any host 10.0.54.5 eq 21
R1(config)# access-list 105 deny ip any any
R1(config)# interface gi0/0
R1(config-if)# ip access-group 105 out

3. **A. permit tcp any host 2001:DB8:10:10::100 eq 25**

Which IPv6 ACL command entry will permit traffic from any host to an SMTP server on network 2001:DB8:10:10::/64?
A. permit tcp any host 2001:DB8:10:10::100 eq 25
B. permit tcp host 2001:DB8:10:10::100 any eq 23
C. permit tcp host 2001:DB8:10:10::100 any eq 25
D. permit tcp any host 2001:DB8:10:10::100 eq 23

4. **B. named extended**

What is the only type of ACL available for IPv6?
A. named standard
B. named extended
C. numbered standard
D. numbered extended

5. **A. Filter unwanted traffic before it travels onto a low-bandwidth link.**
B. Place standard ACLs close to the destination IP address of the traffic.
C. Place extended ACLs close to the source IP ad-

Which three statements are generally considered to be best practices in the placement of ACLs? (Choose three.)
A. Filter unwanted traffic before it travels onto a low-bandwidth link.
B. Place standard ACLs close to the destination IP address of the traffic.
C. Place extended ACLs close to the source IP address of the traffic.
D. For every inbound ACL placed on an interface, there should be a matching outbound ACL.
E. Place extended ACLs close to the destination IP address of the traffic.

	dress of the traffic.	F. Place standard ACLs close to the source IP address of the traffic.
6.	**E. 8**	If a router has two interfaces and is routing both IPv4 and IPv6 traffic, how many ACLs could be created and applied to it? A. 4 B. 16 C. 6 D. 12 E. 8
7.	**C. Each statement is checked only until a match is detected or until the end of the ACE list.** **D. An implicit deny any rejects any packet that does not match any ACE.** **E. A packet can either be rejected or forwarded as directed by the ACE that is matched.**	Which three statements describe ACL processing of packets? (Choose three.) A. A packet that has been denied by one ACE can be permitted by a subsequent ACE. B. A packet that does not match the conditions of any ACE will be forwarded by default. C. Each statement is checked only until a match is detected or until the end of the ACE list. D. An implicit deny any rejects any packet that does not match any ACE. E. A packet can either be rejected or forwarded as directed by the ACE that is matched. F. Each packet is compared to the conditions of every ACE in the ACL before a forwarding decision is made.
8.	**B. limiting debug outputs** **D. controlling virtual terminal access to routers**	What are two possible uses of access control lists in an enterprise network? (Choose two.) A. allowing Layer 2 traffic to be filtered by a router B. limiting debug outputs C. reducing the processing load on routers D. controlling virtual terminal access to routers E. controlling the physical status of router interfaces
9.		

D. an implicit permit of neighbor discovery packets

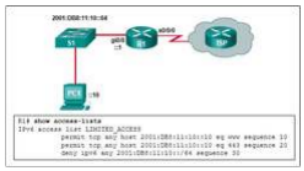
Which feature is unique to IPv6 ACLs when compared to those of IPv4 ACLs?
A. the use of named ACL entries
B. an implicit deny any any ACE
C. the use of wildcard masks
D. an implicit permit of neighbor discovery packets

10. **D. They filter traffic based on source IP addresses only.**

Which statement describes a characteristic of standard IPv4 ACLs?
A. They are configured in the interface configuration mode.
B. They can be configured to filter traffic based on both source IP addresses and source ports.
C. They can be created with a number but not with a name.
D. They filter traffic based on source IP addresses only.

11. **D. ICMPv6 packets that are destined to PC1**

Refer to the exhibit. The IPv6 access list LIMITED_ACCESS is applied on the S0/0/0 interface of R1 in the inbound direction. Which IPv6 packets from the ISP will be dropped by the ACL on R1?
A. HTTPS packets to PC1
B. neighbor advertisements that are received from the ISP router
C. packets that are destined to PC1 on port 80
D. ICMPv6 packets that are destined to PC1



12. **A. The ACL is applied to the wrong interface.**

Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.
Why is the ACL not working?
A. The ACL is applied to the wrong interface.
B. No ACL is needed for this scenario.
C. The ACL is missing a deny ip any any ACE.
D. The ACL is applied in the wrong direction.
E. The access-list 105 command or commands are incorrect.

13.

D. Both can be created by using either a descriptive name or number.
E. Both include an implicit deny as a final ACE.

Which two characteristics are shared by both standard and extended ACLs? (Choose two.)
A. Both can permit or deny specific services by port number.
B. Both filter packets for a specific destination host IP address.
C. Both kinds of ACLs can filter based on protocol type.
D. Both can be created by using either a descriptive name or number.
E. Both include an implicit deny as a final ACE.

14. **C. Router1(config)# access-list 10 permit host 192.168.15.23**
D. Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.0

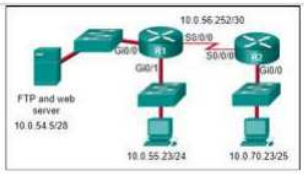
A network administrator needs to configure a standard ACL so that only the workstation of the administrator with the IP address 192.168.15.23 can access the virtual terminal of the main router. Which two configuration commands can achieve the task? (Choose two.)
A. Router1(config)# access-list 10 permit 192.168.15.23 255.255.255.255
B. Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.255
C. Router1(config)# access-list 10 permit host 192.168.15.23
D. Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.0
E. Router1(config)# access-list 10 permit 192.168.15.23 255.255.255.0

15. **the first valid host address in a subnet**
subnetwork address of a subnet with 14 valid host addresses
all IP address bits must match exactly
hosts in a subnet with the

subnet mask 255.255.252.0 addresses with a subnet mask of 255.255.255.248 -NOT SCORED-

16. **B. R1(config)# interface gi0/0 R1(config-if)# ip access-group 105 out E. access-list 105 permit tcp host 10.0.70.23 host 10.0.54.5 eq 20 access-list 105 permit tcp host 10.0.70.23 host 10.0.54.5 eq 21 access-list 105 permit tcp 10.0.0.0 0.255.255.255 host 10.0.54.5 eq www access-list 105 deny ip any host 10.0.54.5 access-list 105 permit ip any any**

Refer to the exhibit. The network administrator that has the IP address of 10.0.70.23/25 needs to have access to the corporate FTP server (10.0.54.5/28). The FTP server is also a web server that is accessible to all internal employees on networks within the 10.x.x.x address. No other traffic should be allowed to this server. Which extended ACL would be used to filter this traffic, and how would this ACL be applied? (Choose two.)
A. access-list 105 permit ip host 10.0.70.23 host 10.0.54.5
access-list 105 permit tcp any host 10.0.54.5 eq www
access-list 105 permit ip any any
B. R1(config)# interface gi0/0
R1(config-if)# ip access-group 105 out
C. access-list 105 permit tcp host 10.0.54.5 any eq www
access-list 105 permit tcp host 10.0.70.23 host 10.0.54.5 eq 20
access-list 105 permit tcp host 10.0.70.23 host 10.0.54.5 eq 21
D. R2(config)# interface gi0/0
R2(config-if)# ip access-group 105 in
E. access-list 105 permit tcp host 10.0.70.23 host 10.0.54.5 eq 20
access-list 105 permit tcp host 10.0.70.23 host 10.0.54.5 eq 21
access-list 105 permit tcp 10.0.0.0 0.255.255.255 host 10.0.54.5 eq www
access-list 105 deny ip any host 10.0.54.5
access-list 105 permit ip any any
F. R1(config)# interface s0/0/0
R1(config-if)# ip access-group 105 out



17. **A. ACLs can control which areas a host can access on a network.**
B. ACLs provide a basic level of security for network access.

What two functions describe uses of an access control list? (Choose two.)
A. ACLs can control which areas a host can access on a network.
B. ACLs provide a basic level of security for network access.
C. ACLs can permit or deny traffic based upon the MAC address originating on the router.
D. ACLs assist the router in determining the best path to a destination.
E. Standard ACLs can restrict access to specific applications and ports.

18. **D. Inbound ACLs are processed before the packets are routed while outbound ACLs are processed after the routing is completed.**

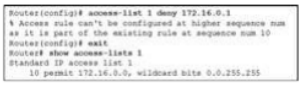
Which statement describes a difference between the operation of inbound and outbound ACLs?
A. In contrast to outbound ALCs, inbound ACLs can be used to filter packets with multiple criteria.
B. On a network interface, more than one inbound ACL can be configured but only one outbound ACL can be configured.
C. Inbound ACLs can be used in both routers and switches but outbound ACLs can be used only on routers.
D. Inbound ACLs are processed before the packets are routed while outbound ACLs are processed after the routing is completed.

19. **B. deny ip any any**
E. deny icmp any any
F. permit icmp any any nd-ns

Which three implicit access control entries are automatically added to the end of an IPv6 ACL? (Choose three.)
A. deny ipv6 any any
B. deny ip any any
C. permit ipv6 any any
D. permit icmp any any nd-na
E. deny icmp any any
F. permit icmp any any nd-ns

20. **B. Manually add the new deny ACE with a sequence number of 5.**

Refer to the exhibit. A router has an existing ACL that permits all traffic from the 172.16.0.0 network. The administrator attempts to add a new ACE to the ACL that denies packets from host 172.16.0.1 and receives the error message that is shown in the exhibit. What action can the administrator take to block packets from host 172.16.0.1 while still permitting all other traffic from the 172.16.0.0 network?
A. Manually add the new deny ACE with a sequence number of 15.
B. Manually add the new deny ACE with a sequence number of 5.
C. Create a second access list denying the host and apply it to the same interface.
D. Add a deny any any ACE to access-list 1.



21. **C. R1(config-line)# access-class 1 in**

An administrator has configured an access list on R1 to allow SSH administrative access from host 172.16.1.100. Which command correctly applies the ACL?
A. R1(config-if)# ip access-group 1 out
B. R1(config-line)# access-class 1 out
C. R1(config-line)# access-class 1 in
D. R1(config-if)# ip access-group 1 in

Topic 9C: Implement Secure Wireless Infrastructure

Study online at https://quizlet.com/_bqne3c

1.	**Co-channel interference (CCI)**	when two WAPs in close proximity use the same channel, they compete for bandwidth within that channel, as signals collide and have to be re-transmitted.
2.	**Adjacent channel interference (ACI)**	channels have only ~5 MHz spacing, but Wi-Fi requires 20 MHz of channel space. When the channels selected for WAPs are not cleanly spaced, the interference pattern creates significant numbers of errors and loss of bandwidth.
3.	**site survey**	A collection of information about a location for the purposes of building an ideal infrastructure; it often contains optimum locations for wireless antenna and access point placement to provide the required coverage for clients and identifying sources of interference. used to measure signal strength and channel usage throughout the area to cover
4.	**heat map**	In a Wi-Fi site survey, a diagram showing signal strength at different locations. shows where a signal is strong (red) or weak (green/blue), and which channel is being used and how they overlap
5.	**wireless controller**	A device that provides wireless LAN management for multiple APs.

Topic 9C
Implement Secure Wireless Infrastructure

Study online at https://quizlet.com/_9mtvtj

1.	**Access Point**	A device that provides a connection between wireless devices and can connect to wired networks.
2.	**Wireless Access Point**	enables devices to connect to a wireless network to communicate with each other
3.	**Service Set Identifier (SSID)**	Each WAP is identified by its MAC address, also referred to as its basic service set identifier (BSSID)
4.	**Co-channel interference (CCI)**	When two WAPs in close proximity use the same channel, they compete for bandwidth within that channel, as signals collide and have to be re-transmitted.
5.	**Adjacent channel interference (ACI)**	Channels have only ~5 MHz spacing, but Wi-Fi requires 20 MHz of channel space. When the channels selected for WAPs are not cleanly spaced, the interference pattern creates significant numbers of errors and loss of bandwidth.
6.	**Wireless controllers**	A device that provides wireless LAN management for multiple APs.
7.	**Wi-Fi Protected Access (WPA)**	Standards for authenticating and encrypting access to Wi-Fi networks.
8.	**Wired Equivalent Privacy (WEP)**	A legacy mechanism for encrypting data sent over a wireless connection.
9.	**Temporal Key Integrity Protocol (TKIP)**	A mechanism used in the first version of WPA to improve the security of wireless encryption mechanisms, compared to the flawed WEP standard.
10.	**WPA2**	Uses the Advanced Encryption Standard (AES) cipher with 128-bit keys, deployed within the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP).
11.	**WPA3**	
12.		

	Simultaneous Authentication of Equals (SAE)	Personal authentication mechanism for Wi-Fi networks introduced with WPA3 to address vulnerabilities in the WPA-PSK method.
13.	**AES Galois Counter Mode Protocol (GCMP)**	WPA3 Mode of operation for AES that ensures authenticated encryption.
14.	**WPA2 Pre-Shared Key Authentication**	WIFI Password-Passphrase-based mechanism to allow group authentication to a wireless network. The passphrase is used to derive an encryption key.
15.	**WPA3 Personal Authentication**	Password- Uses Password Authenticated Key Exchange (PAKE)
16.	**Wi-Fi Protected Setup (WPS)**	A feature of WPA and WPA2 that allows enrollment in a wireless network based on an 8-digit PIN.
17.	**Captive Portal**	A web page or website to which a client is redirected before being granted full network access.
18.	**Open authentication**	means that the client is not required to authenticate
19.	**Extensible Authentication Protocol (EAP)**	A framework for transporting authentication protocols that defines the format of the messages.
20.	**EAP-TLS**	"EAP-Transport Layer Security--Uses PKI, requiring both server-side and client-side certificates."
21.	**Protected Extensible Authentication Protocol (PEAP)**	as with EAP-TLS, an encrypted tunnel is established between the supplicant and authentication server, but PEAP only requires a server-side public key certificate.
22.	**EAP-Tunneled TLS (EAP-TTLS)**	similar to PEAP. It uses a server-side certificate to establish a protected tunnel through which the user's authentication credentials can be transmitted to the authentication server. The main distinction from PEAP is that EAP-TTLS

		can use any inner authentication protocol (PAP or CHAP, for instance), while PEAP must use EAP-MSCHAP or EAP-GTC.
23.	**EAP with Flexible Authentication via Secure Tunneling (EAP-FAST)**	is similar to PEAP, but instead of using a certificate to set up the tunnel, it uses a Protected Access Credential (PAC), which is generated for each user from the authentication server's master key
24.	**RADIUS Federation**	means that multiple organizations allow access to one another's users by joining their RADIUS servers into a RADIUS hierarchy or mesh
25.	**rogue access point**	AP that has been installed on the network without authorization, whether with malicious intent or not
26.	**Evil Twin**	A wireless access point that deceives users into believing that it is a legitimate network access point.
27.	**Disassociation**	A disassociation frame is sent in order to terminate the association from either side in an access point.
28.	**Deauthentication**	Spoofing frames to disconnect a wireless station to try to obtain authentication data to crack.
29.	**IV attacks**	A wireless attack where the attacker is able to predict or control the IV of an encryption process, thus giving the attacker access to view the encrypted data that is supposed to be hidden from everyone else except the user or network.
30.	**Jamming**	An attack in which radio waves disrupt 802.11 wireless signals.

9C and 9D: Implement Secure Wireless Infrastructure, Implement Load Balancers

Study online at https://quizlet.com/_c0zd01

1.	**Wireless Network Installation Considerations**	- Ensure good availability of authorized Wi-Fi access points. - Wireless Access Point (WAP) Placement, channel overlaps - Site surveys, WiFi Analyzers and heat maps - Controller and Access Point Security
2.	**Wireless Access Point (WAP) Placement**	- WAP identified by its MAC address (basic service set identifier (BSSID). 1. Wireless network is identified by its name, or service set identifier (SSID) and can operate in 2.4GHz or 5GHz radio band 2. Each radio band has number of channels. WAP configured on each channel. 3. Should be widely spaced out to reduce interferences. Types of interferences: CCI and ACI
3.	**CCI (Co-channel interference) and ACI (Adjacent channel interference)**	- CCI: When 2 WAPs in close proximity use the same channel, they compete for bandwidth -> § signals collide and have to be re-transmitted. - ACI: channels have only ~5 MHz spacing, but Wi-Fi requires 20 MHz. When the channels selected for WAPs are not spaced properly, can create numbers of errors and loss of bandwidth.
4.	**Site surveys, Wi-Fi Analyzer, Heat Maps**	- Site survey: used to measure signal strength and channel usage in area covered. Makes areas that cause interferences i.e. microwave, solid walls, reflective surfaces - Use a Wi-Fi analyser: records where signal is at regularly spaced points as surveyor moves around - Create a heat map from the readings: red = strong, green/blue = weak. Shows which channels are used and how they overlap
5.	**Controller and Access Point Security**	- Configuring authentication and encryption ensures confidentiality and integrity of the network - Enterprise wireless solutions implement wireless con-

trollers for centralized management and monitoring
- An access point whose firmware contains enough processing logic to be able to function autonomously and handle clients without the use of a wireless controller is known as a fat WAP, while one that requires a wireless controller in order to function is known as a thin WAP.

6. **WEP (Wired Equivalent Privacy)**
- Uses RC4 stream cipher
- Uses 24-bit IV
- Allows for a 256-bit key but not secure

7. **WPA (v1)**
- Designed to fix vulnerabilities in WEP
- Uses the RC4 stream cipher with Temporal Key Integrity Protocol (TKIP)

8. **WPA2 (Wi-Fi Protected Access 2)**
- Uses the Advanced Encryption Standard (AES) cipher with 128-bit keys
-- AES replaces RC4
- Keys deployed with the Counter Mode with Cipher Block Chaining Message Authentication Code (CBC-MAC) Protocol (CCMP)
-- CCMP replaces TKIP
- CCMP provides authenticated encryption -> makes replay attacks harder
- Difficult to crack if protected by a strong password, or if deploying enterprise authentication

9. **WPA3 (Wi-Fi Protected Access 3)**
- Personal Mode: Uses Simultaneous Authentication of Equals (SAE). For securing small servers
-- Replaces WPA'S 4-way handshake authentication and association mechanism with a protocol based on Diffie-Hellman key agreement.
- Enhanced Open - enables encryption for the open authentication method
- AES Galois Counter Mode Protocol (GCMP) mode of operation replaces AES CCMP
- Enterprise authentication methods must use 192-bit AES, personal authentication use either 128-bit or 192-bit

	- Management protection frames - mandates use of these to protect against key recovery attacks.
10. **WPA2 pre-shared key authentication (WPA2-PSK)**	- Passphrase used to generate a pairwise master key (PMK) that is used to encrypt communications - Referred to as group authentication because a group of users share the same secret. - PMK is used as part of WPA2's 4-way handshake to derive session keys
11. **WPA3 personal authentication**	- Uses Password Authenticated Key Exchange (PAKE) - Simultaneous Authentication of Equals (SAE) protocol replaces the 4-way handshake - SAE uses Dragonfly handshake, which is Diffie-Helllman over elliptic curves key agreement, combined with a hash value derived from the password and device MAC address to authenticate the nodes - Dragonfly also implements ephemeral session keys, providing forward secrecy
12. **Wi-Fi Protected Setup (WPS)**	- Pushbutton or passcode autoconfiguration of access points and clients. The system generates a random SSID and PSK. - Brute-force vulnerability in passcode algorithm. o Prevent this by increase lockout period but this can still be vulnerable to DoS attack. - Make sure access point firmware is up-to-date - EasyConnect/ Device Provisioning Protocol (DPP) method with WPA3 replaces WPS; it is a better way to configure client devices with the information required to access a Wi-Fi network. o Each participating device must be configured with a public/private key pair o It uses quick response (QR) codes or near-field communication (NFC) tags to communicate each device's public key. Scans code/tag in the configurator app. o It is a straightforward means of configuring headless Internet of Things (IoT) devices with Wi-Fi connectivity.

13.	**Open Authentication and Captive Portals**	- Selecting open authentication means client is not required to authenticate, it uses hotspot (public WAP) with no encryption. - WAP2 - Secondary authentication may be used -> client connects to open hotspot, it launches the browser -> client redirected to a captive portal or splash page -> Allows the client to authenticate to the hotspot provider's network - The portal may enforce terms and conditions and/or take payment to access the Wi-Fi service. - Everything sent over link can be snooped - Use secure protocols for confidential data (HTTPS, Secure IMAP, FTPS) - Use a Virtual Private Network (VPN) to create a secure tunnel so no one can eavesdrops on the open Wi-Fi network - WAP3 - Uses Wi-Fi Enhanced Open
14.	**Enterprise Authentication**	- Implements: IEEE 802.1X to use EAP over EAPoW(an Extensible Authentication Protocol (EAP) over Wireless (EAPoW)) -> - allow an access point to forward authentication data without allowing any other type of network access. - Configured by selecting WPA2-Enterprise or WPA3-Enterprise on the access point. - User credential is used to generate session encryption key o Credentials of the supplicant is validated through AAA server (RADIUS or TACACS+) o Once validated, RADIUS or TACACS+ transmits a master key (MK) to supplicant o The supplicant and authentication server then derive the same pairwise master key (PMK) from the MK o The AAA server transmits the PMK to the access point o The wireless station and access point use the PMK to derive session keys, using either the WPA2 4-way handshake or WPA3 SAE methods.
15.		- Used in smart cards, one-time passwords, biometric identifiers, or simpler username and password combina-

	EAP - Extensible Authentication Protocol	tions - Uses a RADIUS server to validate the authentication credentials for each user (supplicant).
16.	**EAP-TLS**	- Strongest authentication, highest level of security - Uses public key certificates on the authentication server and supplicant - Provides mutual authentication - User provides certificate using a smart card or a certificate could be installed on the client device, in TPM
17.	**EAP-TTLS: EAP with Tunneled TLS**	- Server-side certificate only to get secure tunnel - User don't require certificate - Uses server-side certificate to create a secure tunnel to transmit user authentication credentials to authentication server - Uses any inner authentication protocol (PAP or CHAP)
18.	**PEAP - Protected Extensible Authentication Protocol**	- Server-side certificate only to get secure tunnel - User don't require certificate - Uses server-side certificate to create a secure tunnel to transmit user authentication credentials to authentication server - The user authentication method uses either MS-CHAPv2 or EAP-GTC - The Generic Token Card (GTC) method transfers a token for authentication against a network directory or using a one-time password mechanism.
19.	**EAP-FAST: EAP with Flexible Authentication via Secure Tunneling**	- Alternative to PEAP - Uses Protected Access Credential (PAC) to set up the tunnel o This is generated for each user from the authentication server's master key - Drawback: Access point to the user is not authenticated as PAC is distributed either via o an out-of-band method o a server with a digital certificate o anonymous Diffie-Hellman key exchange

		Hence a rogue access point can obtain the user credentials to perform an ASLEAP password cracking attack
20.	**RADIUS Federation**	- Members of one organization can authenticate to the network of another organization. Use their normal credentials. - Use 802.1x as the authentication method and RADIUS on the backend. - Example eduroam network - Uni students can use their normal authentication when visiting a different campus.
21.	**Rogue Access Points**	- Installed on the network without authorisation - Can be malicious or accident - Example: can be set up from mobile hotspot -> so check this regularly - Can create a backdoor to capture user logon attempts, private info, allow MiTM attacks - Identified through o Intrusion detection and NAC (security suites that combine automated network scanning with defense) o Wireless monitoring - Wi-Fi analyzers and monitoring systems o Examples: insider, Kismet, Cambium Networks (formerly Xirrus) Wi-Fi Inspector o Physical inspection (but will not show a sophisticated attack)
22.	**Disassociation and Replay Attacks**	- Deauthentication attack o Attacker sends spoofed frames to cause a client to deauthenticate (disconnect) from a WAP o The deauth frames spoof the MAC address of the target station (when users reconnect, they are connected to evil twin AP & attacker gets info about authentication) o This helps attacker to perform a replay attack, DoS attack - Disassociation attack o Similar but just causes the target to disassociate instead of fully deauthenticating the station o Helps perform DoS attack

		- Configure Management Frame Protection (MFP/802.11w) to mitigate the attacks - Initialization vector (IV) attack o Done by generating packets to strip IV - KRACK Attack o Uses a replay mechanism that targets the 4-way hand-shake o Effective on personal and enterprise authentication mechanism - Prevent attacks by full patching on clients and access points
23.	**Jamming Attacks**	- Can be environmental or malicious interference from other radio sources - Done to disrupt services on the wireless network or to place an evil twin on the network - Performed by setting up a WAP with a stronger signal and by at physical proximity to the wireless network - Prevent this by o Disabling the radio source o Boost the signal from the legitimate equipment. - Use spectrum analyzer to find the source o This uses a special radio receiver
24.	**DDoS (Distrib-uted Denial of Service) Attacks**	- Attack is launched from multiple hosts simultaneously - Forms a command and control (C&C) network from botnets - Consumes network bandwidth with number of bots - Exhausts the hosts processing requests, consuming CPU cycles and memory - Delays processing legitimate traffic and crashes the host system - Use spoofed source addresses or launched by bots, making them hard to find the source of the attack - SYN flood attack o Withholds the client's ACK packet during TCP's three-way handshake o Spoofs the clients IP address (invalid/random IP is en-tered so the servers SYN/ACK packet is misdirected)

		- A server, router or firewall can record a queue of pending connections in its state table. When it does not receive an ACK packet from the client, it sends the SYN/ACK packet a set num of times before timing out. However, server can only hold a limited num of pending connections, which DoS attacks quickly fills up so server is unable to respond to genuine traffic
25.	**Distributed Reflection DoS (DRDoS) or Amplified SYN flood Attack**	- Threat actor spoof victim's IP address and attempt to open connections with multiple servers - Those servers direct their SYN/ACK responses to the victim - This rapidly consumes the victim's available handwidth
26.	**Application attacks**	- Targets vulnerabilities in the headers and payloads of specific application protocols - e.g. amplification attack targets DNS services with bogus queries o Advantage: The request is small but the response to a DNS query can be made to include a lot of information o Very effective way to overwhelm the bandwidth of the victim network using limited resources on the attacker's botnet - e.g Network Time Protocol (NTP) o NTP helps servers on a network and on the Internet to keep the correct time. o Servers and clients must be synchronised. o One NTP query can be used to generate a response that contains the last 600 machines the NTP server has contacted. o This allows a short request to direct a long response at the victim network - Both are attacked in a similar way
27.	**Operational technology (OT) Attack**	- An OT network is established between embedded systems devices and their controllers - DDoS attacks against the controllers - Older DDoS techniques like Smurf or Ping of Death can be effective against embedded systems if the controllers

		have limited processing ability o They can rapidly overwhelm available memory or CPU time. - DoS against embedded systems
28.	**DDoS/flooding Attack Mitigation**	- Check traffic spikes that have no legitimate explanation - Provide high availability services like load balancing and cluster services - Use stateful firewall to detect a DDoS attack and block it. - Use ACL to drop packets for the affected IP address(es) - Use a blackhole to drop packets for the affected IP address(es) -- Blackhole is a separate area of the network that cannot reach any other part of the network. -- Use remotely triggered blackhole (RTBH). This is the border gateway protocol (BGP) routing - Use sinkhole routing o This routes the traffic flooding a particular IP address to another network o This helps you identify the source of the attack and devise rules to filter it. o The target can then use low TTL DNS records to change the IP address advertised for the service and try to allow legitimate traffic past the flood.
29.	**Load Balancing**	- Distributes client requests across available server nodes in a farm or pool - Used to provision light to heavy loads on services - Provide mitigations against DDoS attacks - Provides fault tolerance o If there are multiple servers available in a farm, all addressed by a single name/IP address via a load balancer, then if a single server fails, client requests can be routed to another server in the farm - Examples load balancing is used in: o Web servers, front-end email servers, and web conferencing, A/V conferencing, or streaming media servers - Two main types of load balancers o Layer 4 load balancer (Transport Layer of OSI model)

§ Forwards relevant IP address and TCP/UDP port values
§ Makes basic connectivity tests
o Layer 7 load balancer (content switch)
§ Forwards decisions based on application-level data, such as a request for a particular URL or data types like video or audio streaming.
§ Requires more complex logic, but the processing power of modern appliances is sufficient to deal with this.
§ Tests the application state

30. **Scheduling**

o The scheduling algorithm is the code and metrics that determine which node is selected for processing each incoming request
o Round robin - picking the next node
o Picking the node with the fewest existing connections or best response time
o Weighting - using administrator set preferences or dynamic load information or both.
o Heartbeat or health checks - to verify whether each node is available and under load or not

31. **Load Balancing pt2**

- When a client device has established a session with a particular node in the server farm, it may be necessary to continue to use that connection for the duration of the session.
o Session affinity (Layer 4)
§ Handles user sessions
§ When a client establishes a session, it becomes stuck to the node that first accepted the request.
o Session persistence
§ Works by setting a cookie, either on the node or injected by the load balancer. This is more reliable than session affinity.
§ Requires the browser to accept the cookie but more reliable that session affinity

32. **Clustering**

- Provides redundancy
If one of the processing nodes in the cluster stops working, connections can failover to a working node

33.	**Virtual IP**	- Using public IP to access the service that is shared between the twice instances in the cluster (use two load balancers so that if one fails, the other can still handle client connections) - The instances are configured with a private connection that runs on a redundancy protocol like Common Address Redundancy Protocol (CARP) o CARP enabled the active node to own the virtual IP and respond to connections. o CARP implements a heartbeat mechanism to allow failover to the passive node if the active one should suffer a fault.
34.	**Active/Passive clustering**	- When one node is active and the other is passive - Advantage: Performance is not adversely affected during failover - Drawback: The hardware and operating system costs are higher because of the unused capacity
35.	**Active/Active (A/A) Clustering**	- Both nodes are processing connections parallel - Admin can use the max capacity from the available hardware while all nodes are functional - If there is a failover, the failed node workload is shifted onto the remaining node - Drawback: the workload on the remaining nodes are higher and performance is degraded
36.	**Application clustering**	o Cluster is used to provision fault tolerant application services. § If an application server suffers a fault in the middle of a session, the session state data will be lost. o Application clustering allows servers in the cluster to communicate session information to one another § E.g. if a user logs in on one instance, the next session can start on another instance, and the new server can access the cookies or other information used to establish the login.

37. **Quality of Service (QoS)**

- A framework to prioritize traffic with certain characteristics
- Used to support voice and video applications that require a minimum level of bandwidth and are sensitive to latency and jitter
o Latency - The milliseconds (ms) time it takes for a transmission to reach the recipient
o Jitter - a variation in the delay, or an inconsistent rate of packet delivery
- Involves identifying trust boundaries to establish a legitimate authority for marking traffic.
- QoS implementation:
1. Organization performs application discovery to identify bandwidth, latency, and jitter thresholds of the protocols in use and determine their relative priority.
The applications are then mapped to standard class of service (CoS) codes at layer 2 & 3
These codes are configured across the range of hosts and intermediate systems that handle QoS traffic.
2. A QoS-compatible endpoint device or application uses the DiffServ field in the IP header (layer 3) and adds an 802.1p field to the Ethernet header (layer 2) to indicate that the packet should be treated as priority (traffic marking). It transmits the frame to the switch.
3. If the switch supports QoS, 802.1p header is used to prioritize the frame (by holding a queue of outgoing traffic and delaying nonpriority frames). If the queue is full, a traffic policing policy must state if non-priority frames should be dropped, or if the queue should be cleared at the expense of reducing QoS.
4. A similar process occurs at routers and load balancers on the network edge, though they can inspect the DiffServ IP packet header, rather than having to rely on the more limited 802.1p header. Prioritization always takes place on the outbound interface, with low priority traffic being held in a queue.
- QoS marking introduces the potential for DoS attacks
o Network can be overwhelmed if a threat actor crafts packets to be treated as high priority and send them at a

high rate
- Ensure that there is always sufficient bandwidth for security-critical monitoring data and network management/ configuration traffic.

Topic 9D
Implement Load Balancers

Study online at https://quizlet.com/_9mtyla

1.	**Denial of Service (DoS)**	Any type of physical, application, or network attack that affects the availability of a managed resource.
2.	**distributed DoS (DDoS)**	An attack that uses multiple compromised hosts (a botnet) to overwhelm a service with request or response traffic. Most denial of service (DoS) attacks against websites and gateways are distributed DoS (DDoS
3.	**SYN flood attack**	A DoS attack where the attacker sends numerous SYN requests to a target server, hoping to consume enough resources to prevent the transfer of legitimate traffic.
4.	**Application Attacks**	A network-based attack where the attacker dramatically increases the bandwidth sent to a victim during a DDoS attack by implementing an amplification factor.
5.	**Network Time Protocol (NTP)**	TCP/IP application protocol allowing machines to synchronize to the same time clock that runs over UDP port 123.
6.	**DNS amplification attack**	An attack that uses publicly accessible and open DNS servers to flood a system with DNS response traffic.
7.	**operational technology (OT)**	A communications network designed to implement an industrial control system rather than data networking.
8.	**Operational Technology (OT) Attacks**	DDoS attack established between embedded systems devices and their controllers such as valves, motors, electrical switches, gauges, and sensors.
9.	**DDoS attacks can be diagnosed**	traffic spikes that have no legitimate explanation
10.	**DDoS attacks can be counteracted by**	providing high availability services, such as load balancing and cluster services.
11.		

	emotely triggered blackhole (RTBH)	Using a trigger device to send a BGP route update that instructs routers to drop traffic that is suspected of attempting DDoS.
12.	**Border Gateway Protocol (BGP)**	A core routing protocol that bases routing decisions on the network path and rules. TCP 179
13.	**sinkhole**	A DoS attack mitigation strategy that directs the traffic that is flooding a target IP address to a different network for analysis.
14.	**Load Balancer**	A type of switch or router that distributes client requests between different resources, such as communications links or similarly-configured servers. This provides fault tolerance and improves throughput
15.	**Two Types of Load Balancers**	Layer 4 (TransPort Layer) and Layer 7(Application Layer) load balancer
16.	**Layer 4 load balancer**	basic load balancers make forwarding decisions on IP address and TCP/UDP port values, working at the transport layer of the OSI model.
17.	**Layer 7 load balancer (content switch)**	as web applications have become more complex, modern load balancers need to be able to make forwarding decisions based on application-level data, such as a request for a particular URL or data types like video or audio streamin
18.	**Scheduling**	the code and metrics that determine which node is selected for processing each incoming request
19.	**Round Robin Scheduling**	picking the next node
20.	**Session affinity**	A scheduling approach used by load balancers to route traffic to devices that have already established connections with the client in question.
21.	**persistence**	

	In load balancing, the configuration option that enables a client to maintain a connection with a load-balanced server over the duration of the session. Also referred to as sticky sessions.
22. **Clustering**	A load balancing technique where a group of servers are configured as a unit and work together to provide network services.
23. **Virtual IP**	A single IP address shared by multiple systems
24. **Active-active cluster**	that both nodes are processing connections concurrently.
25. **active/passive clustering**	One server is actively responding to requests while the other acts as a live standby
26. **Quality of Service (QoS)**	Systems that differentiate data passing over the network that can reserve bandwidth for particular applications. A system that cannot guarantee a level of available bandwidth is often described as Class of Service (CoS).
27. **Latency**	the time it takes for a transmission to reach the recipient, measured in milliseconds (ms)
28. **Jitter**	defined as being a variation in the delay, or an inconsistent rate of packet delivery.