What attacks occur against VLANs?	double-tagging switch-spoofing
How can you counteract double-tagging?	Don't use the native VLAN (VLAN 1) to transmit data example: config t int g0/1 switchport trunk native vlan 900
How can you counter switch spoofing attack?	1. turn off all trunk ports where you do not use them switchport mode access 2. configure any trunk ports to disable DTP switchport trunk encapsulation dot1q switchport mode trunk switchport trunk nonegotiate
what kinds of attacks can be made against VLANs and the mitigating controls.	VLAN hopping. The attacker wants to jump from the VLAN he has compromised to another higher - value VLAN. This chapter included discussions of double tagging and switch spoofi ng. The features to combat them include turning off DTP on trunk ports and confi guring the native VLAN to not carry user data.

Understand attacks against Spanning - Tree Protocol (STP) and the features you can configure to mitigate the threat.	An attack against STP involves introducing a rogue switch to the network. The mitigation for these types of attacks is to confi gure Root Guard and BPDU Guard.
how do you enable rootguard? how do you enable bpduguard?	config t int g0/1 spanning-tree guard root (on all non-root ports) spanning-tree portfast bootguard (on any access ports)
features that can be enabled to combat DHCP spoofing.	DHCP snooping dynamic arp inspection (DAI)
With --- - - - an attacker hopes to direct traffi c to a rogue - controlled host by setting either a rogue default gateway or a rogue DNS server.	DHCP Spoofing

How do you configure DHCP snooping to receive DHCP messages on g0/1 interface?	config t ip dhcp snooping int g0/1 ip dhcp snooping trust
How do you configure DHCP snooping to turn off a port if it receives a DHCP message?	config t ip dhcp snooping int g0/1 ip dhcp snooping untrust
how do you configure DHCP snooping for vlan 800?	config t ip dhcp snooping ip dhcp snooping vlan 50
how can you limit the number of DHCP messages that can be received per second to 3 on a port?	config t ip dhcp snooping int g0/1 ip dhcp snooping limit rate 3

If this type of port receives a DHCP message, it will shut down	untrusted port
this type of port is allowed to receive a DHCP message	trusted port
types of attacks that affect the CAM table, and how are they prevented?	CAM overload MAC spoofing prevent with: port security
What is a CAM or MAC overload attack?	The MAC table is filled up on a switch. When this occurs, and the switch can no longer learn MACs, it becomes a hub, broadcasting out all ports. Now, an attacker can monitor a port, and see all traffic coming through the switch.

What is MAC spoofing?	when an attacker sends out a false MAC address, thus gaining traffic that was intended for the original host, when the forwarding table in the switch gets updated.
how can port security mitigate CAM overload?	setting the max number of MACs that can come through a port, either through "secure", r maximum mac addresses, or just the default port-security, which limits to 1 mac
What are the three different secure MAC address configurations?	sticky secure static secure dynamic secure
How do you configure sticky secure?	config t int g0/1 switchport mode access switchport port-security mac-address sticky

how do you configure port to protect after a maximum of 5 MACs for a port?	config t int g0/1 switchport mode access switchport port-security switch port-security maximum 5 switchport port-security violation protect
how can you configure a switchport to use the MAC address aaaa.bbbb.cccc ?	config t int g0/1 swithcport port-security switchport port-security mac-addess aaaa.bbbb.cccc
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action (Count) (Count) (Count) --- Gi0/19 3 1 0 Protect --- Total Addresses in System (excluding one mac per port) :0 Max Addresses limit in System (excluding one mac per port) :6176	show port-security
Secure Mac Address Table Vlan Mac Address Type Ports Remaining Age (mins) --- 10 000c.0d3f.00ae SecureDynamic Gi0/18 13 --- Total Addresses in System (excluding one mac per port) :0 Max Addresses limit in System (excluding one mac per port) :6176	show port-security address

Port Security : Enabled Port Status : Secure-down Violation Mode : Protect Aging Time : 0 mins Aging Type : Absolute SecureStatic Address Aging : Disabled Maximum MAC Addresses : 3 Total MAC Addresses : 1 Configured MAC Addresses : 1 Sticky MAC Addresses : 0 Last Source Address:VLAN : 0000.0000.0000:0 Security Violation Count : 0	sh port-security interface
what is Switched Port Analyzer (SPAN) used for?	Switched Port Analyzer (SPAN) is used primarily for two things: capturing traffi c for analysis and sending traffi c to an intrusion detection system (IDS).
Configure SPAN, with source of G0/1, and destination of G0/15	monitor session 1 source int g0/1 monitor session 1 destination int g0/15
What does this command mean? monitor session 1 source ing g0/1 both	the keyword "both" means that you will monitor traffic that is both sent and received on the port.

Remote Switched Port Analyzer (RSPAN).	Remote SPAN, or RSPAN, is used when you want to send traffi c from multiple switches to a single remote port.

configure RSPAN, on switch3, we want both send/receive traffic from g0/5 on switch1 we want traffic sent to port g0/4, and on switch5, we want to monitor that traffic in port g0/10, in vlan 100	switch3(config)#monitor session 1 source interface g0/5 both switch3(config)#monitor session 1 destination remote vlan 100 switch1(config)#monitor session 1 source interface g0/4 switch1(config)#monitor session 1 destination remote vlan 100 switch5(config)#monitor session 1 source remote vlan 100 switch5(config)#monitor session 1 destination g0/10

What is a LAN storm?	LAN storms can result from misconfi gurations, denial of service attacks, broadcast storms, or users plugging in equipment where they shouldn ' t — the list goes on and on. The symptoms of a LAN storm are anything from a minor delay in processing to a complete shutdown of the network, stopping traffi c fl ow. It can be a crippling event in which drastic action needs to be taken to restore normal operations.

What are the three types of packets on which you can configure storm control?	unicast multicast broadcast

There are three types of packets on which you can confi gure storm control: ---------. Each can be confi gured with a -------- threshold. You can specify the threshold in terms of a ---------- of traffi c, ----- per second, or ------- per second. Responses to reaching the threshold are to----------.	unicast, multicast, and broadcast suppression rate percentage bits packets shut down the port and to send an SNMP trap
What are the two types of VLAN hopping attacks?	Double - tagging and switch spoofi ng
BPDU Guard protects what type of ports?	access ports
Switch spoofing involves what type of attack?	VLAN hopping

Which type of attack requires the use of native VLAN to send data?	Double tagging
What does DTP do?	Dynamic Trunk Protocol allows a trunk port to confi gure itself automatically. This is discouraged because it allows an attacker access if he can connect a rogue switch
What is the difference in SPAN and RSPAN?	RSPAN works on multiple switches, whereas SPAN is used on a single switch.
DHCP spoofing is countered with which features?	DHCP snooping and DAI

What is a tool that can be used to do MAC - level attacks?	Dsniff
What is the name of the command that is used when configuring a SPAN port?	monitor
What are the three types of suppression rate thresholds that can be configured for storm control?	Percentage of traffi c, bits per second, and packets per second
configure root guard on int g0/48 configure bpduguard on int g0/12	config t int g0/48 spanning-tree guard root int g0/12 spanning-tree portfast bpduguard

configure SPAN to monitor the traffic that g0/12 is receiving. your laptop running packet sniffer software is connected to g0/1	config t monitor session 1 source int g0/12 monitor session 1 destination int g0/1
You will be confi guring one port to have a maximum limit of three MAC addresses. You will confi gure the same port to be in protect mode. Additionally, you will confi gure the port to be sticky secure.	config t int g0/1 swtichport mode access switchport port-security switchport port-security maximum 3 switchport port-security mac-address sticky
that there is a highly sensitive server connected to the port, so you will confi gure the port to shut down in the event of a violation. Further, you will confi gure a static MAC address and specify that this MAC address is the only one allowed.	config t int g0/15 switchport mode access swtichport port-security switch port-security mac-address aaaa.bbbb.cccc
What three modes can you configure a port can do when you're configuring port security?	shutdown - turn the port off restrict - send SNMP trap protect - limit how many MACs can be configured to the port, no notifications are sent

What feature would you configure if you had to do some troubleshooting with a network analyzer such as Wireshark?	SPAN, or RSPAN
Which two methods are primarily used when an attacker attempts a VLAN hopping attack? (Choose two.)	double tagging switch spoofing
Which type of port security method can be described by learning a MAC address and not adding it to the running config?	dynamic secure
If a non - root port on a switch receives a BPDU that is superior and Root Guard is enabled, what happens?	The port goes into root - inconsistent mode.

What does RSPAN require that SPAN doesn't?	use of VLAN to send the monitored traffic to
What are the methods of basic layer 2 security?	SNMPv3 logging SSH secure port and VLAN configurations
If you were an attacker and you wanted to capture packets on a switch but you were armed with a PC with access to only a single port on the switch, which attack might you attempt?	CAM table attack VLAN attack DHCP snooping MAC spoofing
What layer 2 feature of a Cisco Catalyst switch would allow two hosts in the same VLAN to be unable to communicate with each other?	private VLAN

A double - tagging attack uses which feature of the Catalyst switch to facilitate the attack?	native VLAN
secure port configuration options?	sticky secure static secure dynamic secure
When dynamic ARP inspection is used, which of the following correctly identifies the response to an ARP reply entering an untrusted port if it does not match an entry in the DHCP binding table?	Reply is dropped Port is disabled
What happens when an attacker is able to send enough MAC addresses to max out the CAM table?	Frames are flooded to all ports.

What can be configured for storm control?	unicast broadcast multicast
commands needed to enable DHCP snooping on a switch port?	config t ip dhcp snooping int g0/1 ip dhcp snooping trust
basic approach to maintaining layer 2 security?	SSH, SNMPv3, Logging secure port and VLAN configurations: turn off unused ports, assign unused ports to a nonruted VLAN, set trunks to off instead of auto, don't use native VLAN to transmit user data, use private VLANs to further secure sensitive data within a VLAN
What are the options when configuring RSPAN?	VLAN RX only TX only both

how do you enable root guard on a switch port?	config t int g0/1 spanning-tree guard root
What command shows you the status of port security on an interface?	show port-security interface Note: show port-security shows you the port security for the whole switch)
Depending on which type of switch you are on, there are two different terms for dynamically learned MAC addresses on a switch that mean the same thing. Which two are they?	CAM (content addressable memory) MAC address table
What are the basic approaches to maintaining layer 2 security?	To maintain layer 2 security, you can use SSH instead of Telnet, use SNMP version 3, enable logging, and confi gure port and VLAN security features as follows: Turn off ports that are not used. Set trunk ports to be off instead of auto. Avoid using native VLANs to transmit user data. Use private VLANs to further secure sensitive data with a VLAN.

how can you configure dynamic arp inspection for vlan 11?	config t ip arp inspection vlan 11
how can you configure dynamic arp to trust a port g0/15? it is in vlan 100	config t ip arp inspection vlan 100 int g0/15 ip arp inspection trust
will do just what it says and shut down a port when it perceives a security violation. It will also send an SNMP trap and a Syslog message. No traffi c will fl ow over the port after a port security violation.	shutdown
operates with a method of notifi cation. Each time there is a violation, a Syslog message and an SNMP trap are generated, and a violation counter is incremented	restrict

allows you to use a single MAC address (the default) and allow no others, or you can specify the number of MAC addresses you want to allow. When you get a violation of the confi gured number of MAC addresses, any previously allowed MAC addresses will continue to pass traffi c, but any beyond that will be dropped and no notifi cation will be sent.	Protect
MAC address is confi gured from the command line and is saved in the running confi guration and the CAM table.	static secure
you don ' t have to manually confi gure the MAC address. The switch learns the MAC address dynamically and then stores it in the running confi guration and the CAM table.	sticky secure
the MAC address is learned; however, the difference is that it is only stored in the CAM table, not in the running confi guration. It will be lost if the switch is rebooted.	dynamic secure

Configure storm control on int g0/1 unicast - 56,000 bits per second, with a falling suppression level of 28,000 bits per second multicast - 75 percent broadcast - 200,000 packets per second	config t int g0/1 storm-control unicast level bps 56k 28k storm-control multicast level 75 storm-control broadcast level pps 200k storm-control action shutdown
What actions can be configured wtih storm control?	shutdown and send an SNMP trap
What does this command mean? storm-control unicast level bps 64k 38k	storm-control will block traffic once the bits per second rate exceeds 64,000 bits per second. the interface will not begin to forward traffic again until this rate falls below 38,000 bits per second