

CISCO CCNA Certifications

[Home](#)
[Entries \(RSS\)](#)
[Comments \(RSS\)](#)

Ads by AdBrite

Official Cisco Training
CCNA / CCNP / CCVP / CCIE Start from Any Date
www.koenig-solutions.com

IELTS Exam
Aim for a high IELTS Score. Online study course and practice tests.
www.scottsenglish.com

CCENT Class \$295
Self-Paced Training Class Led By CCIEs! Try It For Free Now
www.InternetNetworkExpert.com

Видео-уроки от Microsoft
Онлайн-доклады по Windows 7, Vista, XP, Office 2007
www.techdays.ru

Element Netwrx Cisco
Visit Element Save On Cisco 50% off Save \$Buy Used Cisco
Element Netwrx
www.elementnetwrx.com

CNC Router Hanter Tech
한터 테크놀러지-국산CNC조각기/라우터 CNC Router/Engraver
/Laser Cutter
www.hanter.kr

FastPulse / Lasermetrics
Pockels cells, Q-switches & Drivers E-O Laser Pulse Pickers & Choppers
fastpulse.com

Ethernet switch
RuggedCom Reliability & Performance For the Harshesht Environments
www.RuggedCom.com

Advertise on this site

Powered By AdBrite

Ads by AdBrite

Advertise on this site

Powered By AdBrite

05:36

CCNA 3:Module 7

POSTED BY ADMIN

Options With Highlight Colours are Correct Answer

1. Which two conditions have favored adoption of 802.11g over 802.11a? (Choose two.)

802.11a suffers from a shorter range than 802.11g.
The 2.4 GHz frequency band is not as crowded as the 5 GHz band.
802.11a is more susceptible to RF interference from common commercial items.
802.11a uses a more expensive modulation technique than 802.11g.
802.11g is backward compatible with 802.11b, but 802.11a is not.

2. Which two statements concerning network security are accurate? (Choose two.)

802.11i uses 3DES for encryption.
Open authentication uses no client or AP verification.
The 802.11i protocol is functionally identical to WPA.
802.11i incorporates a RADIUS server for enterprise authentication.
A wireless client first associates with an AP and then authenticates for network access.

3. Which installation method will allow connectivity for a new wireless network?

set up WEP on the access point only
set up open access on both the access point and each device connected to it
set up full encryption on the access point while leaving each device connected to the network open
set up full encryption on each device of the WLAN while leaving the access point settings open

4. Refer to the exhibit. When configuring the wireless access point, which setting does the network administrator use to configure the unique identifier that client devices use to distinguish this wireless network from others?

Network Mode
Network Name (SSID)
Radio Band
Wide Channel

Ads by AdBrite

Advertise on this site

Powered By AdBrite

Standard Channel

5. Which two statements are true regarding wireless security? (Choose two.)

MAC address filtering prevents the contents of wireless frames from being viewable.
 Providing a wireless client with the network key allows an available network to be visible.
 Disabling an access point from broadcasting the SSID prevents the access point from being discovered.

Default SSIDs on specific manufacturer APs are generally known and may permit hostile wireless connections.

Manually adding a network and setting the known SSID on a wireless client makes the network visible even if the SSID is not being broadcast.

6. Wireless users on a network complain about poor performance within a small area of a room. Moving away from this area in any direction improves performance dramatically. What is the first step in designing a solution to this problem?

This might be RF channel overlap, so the technician should verify the channels in use on each wireless access point and change to non-overlapping channels.

The RF power settings might be set too low on the wireless access points servicing the room. Increase the RF output power on all wireless access points.

Install a new wireless access point in this center area to provide coverage.

Verify that the wireless access points have sufficient in-line power and connectivity to the wired network.

7. Which three devices do many wireless routers incorporate? (Choose three.)

gateway for connecting to other network infrastructures
 built-in Ethernet switch

network management station

VTP server

wireless access point

VPN concentrator

8. Which access method does a wireless access point use to allow for multiple user connectivity and distributed access?

CSMA/CD

token passing

CSMA/CA

polling

9. Why is security so important in wireless networks?

Wireless networks are typically slower than wired networks.

Televisions and other devices can interfere with wireless signals.

Wireless networks broadcast data over a medium that allows easy access.

Environmental factors such as thunderstorms can affect wireless networks.

10. Which wireless technology standard provides the most compatibility with older wireless standards, but has greater performance?

802.11a

802.11b

802.11g

802.11n

11. Which two statements characterize wireless network security? (Choose two.)

A rogue access point represents a security risk for the local network.

Wireless networks offer the same security features as wired networks.

Using encryption prevents unauthorized clients from associating with an access point.

An attacker needs physical access to at least one network device to launch an attack.

With SSID broadcast disabled, an attacker must sniff the SSID before being able to connect.

12. Which network design process identifies where to place access points?

site survey

risk assessment

scalability design

network protocol analysis

13. What wireless security feature allows a network administrator to configure an access point with wireless NIC unique identifiers so that only these NICs can connect to the wireless network?

authentication

SSID broadcasting

MAC address filtering

EAP (Extensible Authentication Protocol)

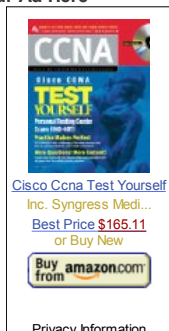
Radius (Remote Authentication Dial-In User Service)

14. What will a wireless client transmit to discover the available WLAN networks?

beacon

password

Your Ad Here



Cisco Ccna Test Yourself
 Inc. Syngress Medi...
 Best Price \$165.11
 or Buy New
 Buy amazon.com
 from

Privacy Information

Your Ad Here

Categories

CCNA 1 UPDATED (12)

CCNA 2 UPDATED (12)

CCNA 3 UPDATED (7)

CCNA tieng viet (1)

CCNA1 (16)

CCNA2 (20)

CCNA3 (10)

CCNA4 (8)

Cisco Exploration 4.0
(3)

ebook CCNA (2)

Ebook_tool_CCNA (7)

key_CCNA v4 (3)

key_CCNA4 (13)

Labpro (2)

probe request
association request

15. In a WLAN network, why should wireless access points be implemented with each access point using a different channel?

to keep users segregated on separate subnets
to control the amount of bandwidth that is utilized
to keep signals from interfering with each other
to keep traffic secure

16. What purpose does authentication serve in a WLAN?

converts clear text data before transmission
indicates which channel the data should flow on
determines that the correct host is utilizing the network
allows the host to choose which channel to use

17. What occurs when a rogue access point is added to a WLAN?

Authorized access points can transmit excess traffic to rogue access points to help alleviate congestion.
Unauthorized users can gain access to internal servers, thus causing a security hole.
All traffic that uses the same channel as the rogue access point will be encrypted.
All traffic that uses the same channel as the rogue access point will be required to authenticate.

18. What procedure can prevent man-in-the-middle attacks?

Force all devices on a WLAN to authenticate and monitor for any unknown devices.
Enable access points to send an SSID to each device wanting to use the network.
Configure MAC filtering on all authorized access points.
Disable SSID broadcasts.

19. Which function is provided by a wireless access point?

dynamically assigns an IP address to the host
provides local DHCP services
converts data from 802.11 to 802.3 frame encapsulation
provides a gateway for connecting to other networks

20. Which major problem does CSMA/CA overcome in wireless networks?

bandwidth saturation
privacy concerns
media contention
device interoperability

21. What does a wireless access point use to allow WLAN clients to learn which networks are available in a given area?

association response
beacon
key
probe request

comments (0)

TOP

05:35

CCNA 3:Module 6

POSTED BY ADMIN

Options With Highlight Colours are Correct Answer

1. Refer to the exhibit. Which three statements describe the network design shown in the exhibit? (Choose three.)

This design will not scale easily.
The router merges the VLANs into a single broadcast domain.
This design uses more switch and router ports than are necessary.
This design exceeds the maximum number of VLANs that can be attached to a switch.
This design requires the use of the ISL or 802.1q protocol on the links between the switch and the router.
If the physical interfaces between the switch and router are operational, the devices on the different VLANs can communicate through the router.

2. A router has two FastEthernet interfaces and needs to connect to four VLANs in the local network. How can this be accomplished using the fewest number of physical interfaces without unnecessarily decreasing network performance?

Implement a router-on-a-stick configuration.
Add a second router to handle the inter-VLAN traffic.
Use a hub to connect the four VLANs with a FastEthernet interface on the router.
Interconnect the VLANs via the two additional FastEthernet interfaces.

3. Refer to the exhibit. All devices are configured as shown in the exhibit. PC2 can successfully ping the F0/0 interface on R1. PC2 cannot ping PC1. What might be the reason for this failure?

R1 interface F0/1 has not been configured for subinterface operation.
S1 interface F0/6 needs to be configured for operation in VLAN10.
S1 interface F0/8 is in the wrong VLAN.
S1 port F0/6 is not in VLAN10.

4. Refer to the exhibit. The commands for a router to connect to a trunked uplink are shown in the exhibit. A packet is received from IP address 192.168.1.54. The packet destination address is 192.168.1.120. What will the router do with this packet?

The router will forward the packet out interface FastEthernet 0/1.1 tagged for VLAN 10.

The router will forward the packet out interface FastEthernet 0/1.2 tagged for VLAN 60.

The router will forward the packet out interface FastEthernet 0/1.3 tagged for VLAN 120.

The router will not process the packet since the source and destination are on the same subnet.

The router will drop the packet since no network that includes the source address is attached to the router.

5. What distinguishes traditional routing from router-on-a-stick?

Traditional routing is only able to use a single switch interface. Router-on-a-stick can use multiple switch interfaces.

Traditional routing requires a routing protocol. Router-on-a-stick only needs to route directly connected networks.

Traditional routing uses one port per logical network. Router-on-a-stick uses subinterfaces to connect multiple logical networks to a single router port.

Traditional routing uses multiple paths to the router and therefore requires STP.

Router-on-a-stick does not provide multiple connections and therefore eliminates the need for STP.

6. Which statement is true about ARP when inter-VLAN routing is being used on the network?

When router-on-a-stick inter-VLAN routing is in use, each subinterface has a separate MAC address to send in response to ARP requests.

When VLANs are in use, the switch responds to ARP requests with the MAC address of the port to which the PC is connected.

When router-on-a-stick inter-VLAN routing is in use, the router returns the MAC address of the physical interface in response to ARP requests.

When traditional inter-VLAN routing is in use, devices on all VLANs use the same physical router interface as their source of proxy ARP responses.

7. What two statements are true regarding the use of subinterfaces for inter-VLAN routing? (Choose two.)

subinterfaces have no contention for bandwidth

more switch ports required than in traditional inter-VLAN routing

fewer router ports required than in traditional inter-VLAN routing

simpler Layer 3 troubleshooting than with traditional inter-VLAN routing

less complex physical connection than in traditional inter-VLAN routing

8. Which three elements must be used when configuring a router interface for VLAN trunking? (Choose three.)

one subinterface per VLAN

one physical interface for each subinterface

one IP network or subnetwork for each subinterface

one trunked link per VLAN

a management domain for each subinterface

a compatible trunking protocol encapsulation for each subinterface

9. Refer to the exhibit. Which two statements are true about the operation of the subinterfaces? (Choose two.)

Incoming traffic that has a VLAN ID of 2 is processed by subinterface fa0/0.2.

Incoming traffic with VLAN ID 0 is processed by interface fa0/0.

Subinterfaces use unique MAC addresses by adding the 802.1Q VLAN ID to the hardware address.

Traffic inbound on this router is processed by different subinterfaces, depending on the VLAN from which the traffic originated.

Reliability of both subinterfaces is poor because ARP is timing out.

Both subinterfaces remain up with line protocol up, even if fa0/0 line protocol is down.

10. Refer to the exhibit. Port Fa0/0 on router R1 is connected to port Fa0/1 on switch S1. After the commands shown are entered on both devices, the network administrator determines that the devices on VLAN 2 are unable to ping the devices on VLAN 1. What is the likely problem?

R1 is configured for router-on-a-stick, but S1 is not configured for trunking.

R1 does not have the VLANs entered in the VLAN database.

Spanning Tree Protocol is blocking port Fa0/0 on R1.

The subinterfaces on R1 have not been brought up with the no shutdown command yet.

11. Refer to the exhibit. PC1 has attempted to ping PC2 but has been unsuccessful. What could account for this failure?

PC1 and R1 interface F0/0.1 are on different subnets.

The encapsulation is missing on the R1 interface F0/0.

An IP address has not been assigned to the R1 physical interface.

The encapsulation command on the R1 F0/0.3 interface is incorrect.

12. Refer to the exhibit. R1 is routing between networks 192.168.10.0/28 and 192.168.30.0/28. PC1 can ping R1 interface F0/1, but cannot ping PC3. What is causing this failure?

PC1 and PC3 are not in the same VLAN.

The PC3 network address configuration is incorrect.
 The S1 interface F0/11 should be assigned to VLAN30.
 The F0/0 and F0/1 interfaces on R1 must be configured as trunks.

13. Devices on the network are connected to a 24-port Layer 2 switch that is configured with VLANs. Switch ports 0/2 to 0/4 are assigned to VLAN 10. Ports 0/5 to 0/8 are assigned to VLAN 20, and ports 0/9 to 0/12 are assigned to VLAN 30. All other ports are assigned to the default VLAN. Which solution allows all VLANs to communicate between each other while minimizing the number of ports necessary to connect the VLANs?

Configure ports 0/13 to 0/16 with the appropriate IP addresses to perform routing between VLANs.

Add a router to the topology and configure one FastEthernet interface on the router with multiple subinterfaces for VLANs 1, 10, 20, and 30.

Obtain a router with multiple LAN interfaces and configure each interface for a separate subnet, thereby allowing communication between VLANs.

Obtain a Layer 3 switch and configure a trunk link between the switch and router, and configure the router physical interface with an IP address on the native VLAN.

14. Which two statements are true about the interface fa0/0.10 command? (Choose two.)

The command applies VLAN 10 to router interface fa0/0.

The command is used in the configuration of router-on-a-stick inter-VLAN routing.

The command configures a subinterface.

The command configures interface fa0/0 as a trunk link.

Because the IP address is applied to the physical interface, the command does not include an IP address.

15. Refer to the exhibit. What two conclusions can be drawn from the output that is shown? (Choose two.)

The no shutdown command has not been issued on the FastEthernet 0/0 interface.
 Both of the directly connected routes that are shown will share the same physical interface of the router.

A routing protocol must be configured on the network in order for the inter-VLAN routing to be successful.

Inter-VLAN routing between hosts on the 172.17.10.0/24 and 172.17.30.0/24 networks is successful on this network.

Hosts in this network must be configured with the IP address that is assigned to the router physical interface as their default gateway.

16. What are the steps which must be completed in order to enable inter-VLAN routing using router-on-a-stick?

Configure the physical interfaces on the router and enable a routing protocol.

Create the VLANs on the router and define the port membership assignments on the switch.

Create the VLANs on the switch to include port membership assignment and enable a routing protocol on the router.

Create the VLANs on the switch to include port membership assignment and configure subinterfaces on the router matching the VLANs.

17. Refer to the exhibit. The network administrator correctly configures RTA to perform inter-VLAN routing. The administrator connects RTA to port 0/4 on SW2, but inter-VLAN routing does not work. What could be the possible cause of the problem with the SW2 configuration?

Port 0/4 is not active.

Port 0/4 is not a member of VLAN1.

Port 0/4 is configured in access mode.

Port 0/4 is using the wrong trunking protocol.

18. What is important to consider while configuring the subinterfaces of a router when implementing inter-VLAN routing?

The physical interface must have an IP address configured.

The subinterface numbers must match the VLAN ID number.

The no shutdown command must be given on each subinterface.

The IP address of each subinterface must be the default gateway address for each VLAN subnet.

19. In which situation could individual router physical interfaces be used for interVLAN routing, instead of a router-on-a-stick configuration?

a network with more than 100 subnetworks

a network with a limited number of VLANs

a network with experienced support personnel

a network using a router with one LAN interface

20. Refer to the exhibit. Switch1 is correctly configured for the VLANs that are displayed in the graphic. The configuration that is shown was applied to RTA to allow for interVLAN connectivity between hosts attached to Switch1. After testing the network, the administrator logged the following report:

Hosts within each VLAN can communicate with each other.

Hosts in VLAN5 and VLAN33 are able to communicate with each other.

Hosts connected to Fa0/1 through Fa0/5 do not have connectivity to host in other VLANs.

Why are hosts connected to Fa0/1 through Fa0/5 unable to communicate with hosts in different VLANs?

The router interface is shut down.

The VLAN IDs do not match the subinterface numbers.

All of the subinterface addresses on the router are in the same subnet.

The router was not configured to forward traffic for VLAN2.
The physical interface, FastEthernet0/0, was not configured with an IP address.

comments (1)

TOP

05:34

CCNA 3:Module 5

POSTED BY ADMIN

Options With Highlight Colours are Correct Answer

1. Which two statements are true about the default operation of STP in a Layer 2 switched environment that has redundant connections between switches? (Choose two.)

The root switch is the switch with the highest speed ports.

Decisions on which port to block when two ports have equal cost depend on the port priority and identity.

All trunking ports are designated and not blocked.

Root switches have all ports set as root ports.

Non-root switches each have only one root port.

2. Which two statements describe the BIDs used in a spanning tree topology? (Choose two.)

They are sent out by the root bridge only after the inferior BPDUs are sent.

They consist of a bridge priority and MAC address.

Only the root bridge will send out a BID.

They are used by the switches in a spanning tree topology to elect the root bridge.

The switch with the fastest processor will have the lowest BID.

3. In which two ways is the information that is contained in BPDUs used by switches? (Choose two.)

to negotiate a trunk between switches

to set the duplex mode of a redundant link

to identify the shortest path to the root bridge

to prevent loops by sharing bridging tables between connected switches

to determine which ports will forward frames as part of the spanning tree

4. Which two actions does an RSTP edge port take if it receives a BPDU? (Choose two.)

immediately loses its edge status

inhibits the generation of a TCN

goes immediately to a learning state

disables itself

becomes a normal spanning-tree port

5. Refer to the exhibit. All switches in the network have empty MAC tables. STP has been disabled on the switches in the network. How will a broadcast frame that is sent by host PC1 be handled on the network?

Switch SW1 will block the broadcast and drop the frame.

Switch SW1 will forward the broadcast out all switch ports, except the originating port. This will generate an endless loop in the network.

Switch SW1 will forward the broadcast out all switch ports, except the originating port. All hosts in the network will replay with a unicast frame sent to host PC1.

Switch SW1 will forward the traffic out all switch ports except the originating port as a unicast frame. All hosts in the network will replay with a unicast frame sent to switch SW1.

6. Which two items are true regarding the spanning-tree portfast command? (Choose two.)

PortFast is Cisco proprietary.

PortFast can negatively effect DHCP services.

PortFast is used to more quickly prevent and eliminate bridging loops.

Enabling PortFast on trunks that connect to other switches improves convergence.

If an access port is configured with PortFast, it immediately transitions from a blocking to a forwarding state.

7. Refer to the exhibit. Server sends an ARP request for the MAC address of its default gateway. If STP is not enabled, what will be the result of this ARP request?

Router_1 will drop the broadcast and reply with the MAC address of the next hop router.

Switch_A will reply with the MAC address of the Router_1 E0 interface.

Switch_A and Switch_B will continuously flood the message onto the network.

The message will cycle around the network until its TTL is exceeded.

8. What is the first step in the process of convergence in a spanning tree topology?

election of the root bridge

blocking of the non-designated ports

selection of the designated trunk port

determination of the designated port for each segment

9. How can a network administrator influence which STP switch becomes the root bridge?

Configure all the interfaces on the switch as the static root ports.

Change the BPDU to a lower value than that of the other switches in the network.
Assign a lower IP address to the switch than that of the other switches in the network.

Set the switch priority to a smaller value than that of the other switches in the network.

10. Refer to the exhibit. The spanning-tree port priority of each interface is at the default setting. The network administrator enters the spanning-tree vlan 1 root primary command on S4. What is the effect of the command?

Spanning tree blocks Gi0/1 on S3.

Gi0/2 on S3 transitions to a root port.

Port priority makes Gi0/2 on S1 a root port.

S4 is already the root bridge, so there are no port changes.

11. What two features of the Spanning-Tree Protocol contribute to the time it takes for a switched network to converge after a topology change occurs? (Choose two.)

the max-age timer

the spanning-tree hold down timer

the forward delay

the spanning-tree path cost

the blocking delay

12. In which STP state does a port record MAC addresses but not forward user data?

blocking

Learning

disabling

listening

forwarding

13. Which three statements are accurate regarding RSTP and STP? (Choose three.)

RSTP uses a faster algorithm to determine root ports.

RSTP introduced the extended system ID to allow for more than 4096 VLANs.

Both RSTP and STP use the portfast command to allow ports to immediately transition to forwarding state.

Like STP PortFast, an RSTP edge port that receives a BPDU loses its edge port status immediately and becomes a normal spanning-tree port.

Configuration commands to establish primary and secondary root bridges are identical for STP and RSTP.

Because of the format of the BPDU packet, RSTP is backward compatible with STP.

14. What two elements will exist in a converged network with one spanning tree? (Choose two.)

one root bridge per network

all non-designated ports forwarding

one root port per non-root bridge

multiple designated ports per segment

one designated port per network

15. Which statement or set of paired statements correctly compares STP with RSTP?

STP and RSTP use the same BPDU format.

STP specifies backup ports. RSTP has only root ports, alternate ports, and designated ports.

STP port states are independent of port roles. RSTP ties together the port state and port role.

STP waits for the network to converge before placing ports into forwarding state.

RSTP places alternate ports into forwarding state immediately.

16. Refer to the exhibit. What can be determined from the output shown?

Two hosts communicating between ports Fa0/2 and Fa0/4 have a cost of 38.

The priority was statically configured to identify the root.

STP is disabled on this switch.

The timers have been altered to reduce convergence time.

17. Which two criteria does a switch use to select the root bridge? (Choose two.)

bridge priority

switching speed

number of ports

base MAC address

switch location

memory size

18. What three link types have been defined for Rapid Spanning-Tree Protocol? (Choose three.)

Shared

end-to-end

edge-type

boundary-type

point-to-many

point-to-point

19. What Rapid Spanning Tree Protocol (RSTP) role is assigned to the forwarding port elected for every switched Ethernet LAN segment?

alternate
backup
Designated
root

20. When PVST+ was developed, the Bridge ID was modified to include which information?

bridge priority
MAC address
protocol
VLAN ID

comments (0)

TOP

05:32

CCNA 3:Module 4

POSTED BY ADMIN

Options With Highlight Colours are Correct Answer

1. Refer to the exhibit. The switches in the exhibit are connected with trunks within the same VTP management domain. Each switch is labeled with its VTP mode. A new VLAN is added to Switch3. This VLAN does not show up on the other switches. What is the reason for this?

VLANs cannot be created on transparent mode switches.

Transparent mode switches do not forward VTP advertisements.

VLANs created on transparent mode switches are not included in VTP advertisements.

Server mode switches neither listen to nor forward VTP messages from transparent mode switches.

2. Which two statements are true about the implementation of VTP? (Choose two.)

Switches must be connected via trunks.

The VTP domain name is case sensitive.

Transparent mode switches cannot be configured with new VLANs.

The VTP password is mandatory and case sensitive.

Switches that use VTP must have the same switch name.

3. Which two statements describe VTP transparent mode operation? (Choose two.)

Transparent mode switches can create VLAN management information.

Transparent mode switches can add VLANs of local significance only.

Transparent mode switches pass any VLAN management information that they receive to other switches.

Transparent mode switches can adopt VLAN management changes that are received from other switches.

Transparent mode switches originate updates about the status of their VLANs and inform other switches about that status.

4. Which three VTP parameters must be identical on all switches to participate in the same VTP domain? (Choose three.)

revision number

domain name

pruning

mode

domain password

version number

5. What causes a VTP configured switch to issue a summary advertisement?

A five-minute update timer has elapsed.

A port on the switch has been shutdown.

The switch is changed to the transparent mode.

A new host has been attached to a switch in the management domain.

6. Refer to the exhibit. Switches SW1 and SW2 are interconnected via a trunk link but failed to exchange VLAN information. The network administrator issued the show vtp status command to troubleshoot the problem. On the basis of the provided command output, what could be done to correct the problem?

Switch SW2 must be configured as a VTP client.

The switches must be interconnected via an access link.

The switches must be configured with the same VTP domain name.

Both switches must be configured with the same VTP revision number.

7. Refer to the exhibit. Which two facts can be confirmed by this output? (Choose two.)

If this switch is added to an established network, the other VTP-enabled switches in the same VTP domain will consider their own VLAN information to be more recent than the VLAN information advertised by this switch.

This switch shows no configuration revision errors.

This switch has established two-way communication with the neighboring devices.

This switch is configured to advertise its VLAN configuration to other VTP-enabled switches in the same VTP domain.

This switch is configured to allow the network manager to maximize bandwidth by restricting traffic to specific network devices.

8. Refer to the exhibit. Switch S1 is in VTP server mode. Switches S2 and S3 are in client mode. An administrator accidentally disconnects the cable from F0/1 on S2. What will the effect be on S2?

S2 will automatically transition to VTP transparent mode.

S2 will remove all VLANs from the VLAN database until the cable is reconnected.
S2 will retain the VLANs as of the latest known revision, but will lose the VLANs if it is reloaded.

S2 will automatically send a VTP request advertisement to 172.17.99.11 when the cable is reconnected.

9. Refer to the exhibit. What information can be learned from the output provided?

It verifies the configured VTP password.

It verifies the VTP domain is configured to use VTP version 2.

It verifies VTP advertisements are being exchanged.

It verifies the VTP domain name is V1.

10. How are VTP messages sent between switches in a domain?

Layer 2 broadcast

Layer 2 multicast

Layer 2 unicast

Layer 3 broadcast

Layer 3 multicast

Layer 3 unicast

11. What statement describes the default propagation of VLANs on a trunked link?

only VLAN 1

all VLANs

no VLANs

the native VLAN

12. Which two statements are true about VTP pruning? (Choose two.)

Pruning is enabled by default.

Pruning can only be configured on VTP servers.

Pruning must be configured on all VTP servers in the domain.

VLANs on VTP client-mode switches will not be pruned.

Pruning will prevent unnecessary flooding of broadcasts across trunks.

13. What does a client mode switch in a VTP management domain do when it receives a summary advertisement with a revision number higher than its current revision number?

It suspends forwarding until a subset advertisement update arrives.

It issues an advertisement request for new VLAN information.

It increments the revision number and forwards it to other switches.

It deletes the VLANs not included in the summary advertisement.

It issues summary advertisements to advise other switches of status changes.

14. Refer to the exhibit. All switches in the network participate in the same VTP domain. What happens when the new switch SW2 with a default configuration and revision number of 0 is inserted in the existing VTP domain Lab_Network?

The switch operates as a VTP client.

The switch operates in VTP transparent mode.

The switch operates as a VTP server and deletes the existing VLAN configuration in the domain.

The switch operates as a VTP server, but does not impact the existing VLAN configuration in the domain.

The switch operates as a VTP server in the default VTP domain and does not affect the configuration in the existing VTP domain.

15. What are two features of VTP client mode operation? (Choose two.)

unable to add VLANs

can add VLANs of local significance

forward broadcasts out all ports with no respect to VLAN information

can only pass VLAN management information without adopting changes

can forward VLAN information to other switches in the same VTP domain

16. Refer to the exhibit. S2 was previously used in a lab environment and has been added to the production network in server mode. The lab and production networks use the same VTP domain name, so the network administrator made no configuration changes to S2 before adding it to the production network. The lab domain has a higher revision number. After S2 was added to the production network, many computers lost network connectivity. What will solve the problem?

Reset the revision number on S2 with either the delete VTP command or by changing the domain name and then changing it back.

Re-enter all appropriate VLANs, except VLAN 1, manually on Switch1 so that they propagate throughout the network.*

Change S1 to transparent VTP mode to reclaim all VLANs in vlan.dat and change back to server mode.

Change S2 to client mode so the VLANs will automatically propagate.

17. A network administrator is replacing a failed switch with a switch that was previously on the network. What precautionary step should the administrator take on the replacement switch to avoid incorrect VLAN information from propagating through the network?

Enable VTP pruning.

Change the VTP domain name.

Change the VTP mode to client.

Change all the interfaces on the switch to access ports.

18. Refer to the exhibit. Switch1 is not participating in the VTP management process with the other switches that are shown in the exhibit. What are two possible explanations for this? (Choose two.)

Switch1 is in client mode.

Switch2 is in server mode.

Switch2 is in transparent mode.

Switch1 is in a different management domain.

Switch1 has end devices that are connected to the ports.

Switch1 is using VTP version 1, and Switch2 is using VTP version 2.

19. Refer to the exhibit. All switches in the VTP domain are new. Switch SW1 is configured as a VTP server, switches SW2 and SW4 are configured as VTP clients, and switch SW3 is configured in VTP transparent mode. Which switch or switches receive VTP updates and synchronize their VLAN configuration based on those updates?

All switches receive updates and synchronize VLAN information.

Only switch SW2 receives updates and synchronizes VLAN information.

Only switches SW3 and SW4 receive updates and synchronize VLAN information.

SW3 and SW4 receive updates, but only switch SW4 synchronizes VLAN information.

20. Which statement is true when VTP is configured on a switched network that incorporates VLANs?

VTP is only compatible with the 802.1Q standard.

VTP adds to the complexity of managing a switched network.

VTP allows a switch to be configured to belong to more than one VTP domain.

VTP dynamically communicates VLAN changes to all switches in the same VTP domain.

comments (0)

TOP

05:31

CCNA 3:Module 3

POSTED BY ADMIN

Options With Highlight Colours are Correct Answer

1. What statement about the 802.1q trunking protocol is true?

802.1q is Cisco proprietary.

802.1q frames are mapped to VLANs by MAC address.

802.1q does NOT require the FCS of the original frame to be recalculated.

802.1q will not perform operations on frames that are forwarded out access ports.

2. Which two statements describe the benefits of VLANs? (Choose two.)

VLANs improve network performance by regulating flow control and window size.

VLANs enable switches to route packets to remote networks via VLAN ID filtering.

VLANs reduce network cost by reducing the number of physical ports required on switches.

VLANs improve network security by isolating users that have access to sensitive data and applications.

VLANs divide a network into smaller logical networks, resulting in lower susceptibility to broadcast storms.

3. What are two characteristics of VLAN1 in a default switch configuration? (Choose two.)

VLAN1 should be renamed.

VLAN 1 is the management VLAN.

All switch ports are members of VLAN1.

Only switch port 0/1 is assigned to VLAN1.

Links between switches must be members of VLAN1.

4. Refer to the exhibit. SW1 and SW2 are new switches being installed in the topology shown in the exhibit. Interface Fa0/1 on switch SW1 has been configured with trunk mode "on". Which statement is true about forming a trunk link between the switches SW1 and SW2?

Interface Fa0/2 on switch SW2 will negotiate to become a trunk link if it supports DTP.

Interface Fa0/2 on switch SW2 can only become a trunk link if statically configured as a trunk.

Interface Fa0/1 converts the neighboring link on the adjacent switch into a trunk link if the neighboring interface is configured in nonegotiate mode.

Interface Fa0/1 converts the neighboring link on the adjacent switch into a trunk link automatically with no consideration of the configuration on the neighboring interface.

5. Refer to the exhibit. Computer 1 sends a frame to computer 4. On which links along the path between computer 1 and computer 4 will a VLAN ID tag be included with the frame?

A

A, B

A, B, D, G

A, D, F

C, E

C, E, F

6. The network administrator wants to separate hosts in Building A into two VLANs numbered 20 and 30. Which two statements are true concerning VLAN configuration? (Choose two.)

The VLANs may be named.

VLAN information is saved in the startup configuration.

Non-default VLANs created manually must use the extended range VLAN numbers.

The network administrator may create the VLANs in either global configuration mode or VLAN database mode.

Both VLANs may be named BUILDING_A to distinguish them from other VLANs in

different geographical locations.

7. Refer to the exhibit. Which two conclusions can be drawn regarding the switch that produced the output shown? (Choose two.)

The network administrator configured VLANs 1002-1005.

The VLANs are in the active state and are in the process of negotiating configuration parameters.

A FDDI trunk has been configured on this switch.

The command `switchport access vlan 20` was entered in interface configuration mode for Fast Ethernet interface 0/1.

Devices attached to ports fa0/5 through fa0/8 cannot communicate with devices attached to ports fa0/9 through fa0/12 without the use of a Layer 3 device.

8. What happens to the member ports of a VLAN when the VLAN is deleted?

The ports cannot communicate with other ports.

The ports default back to the management VLAN.

The ports automatically become a part of VLAN 1.

The ports remain a part of that VLAN until the switch is rebooted. They then become members of the management VLAN.

9. A network administrator is removing several VLANs from a switch. When the administrator enters the `no vlan 1` command, an error is received. Why did this command generate an error?

VLAN 1 can never be deleted.

VLAN 1 can only be deleted by deleting the `vlan.dat` file.

VLAN 1 can not be deleted until all ports have been removed from it.

VLAN 1 can not be deleted until another VLAN has been assigned its responsibilities.

10. What is the effect of the `switchport mode dynamic desirable` command?

DTP cannot negotiate the trunk since the native VLAN is not the default VLAN.

The remote connected interface cannot negotiate a trunk unless it is also configured as dynamic desirable.

The connected devices dynamically determine when data for multiple VLANs must be transmitted across the link and bring the trunk up as needed.

A trunk link is formed if the remote connected device is configured with the `switchport mode dynamic auto` or `switchport mode trunk` commands.

11. Refer to the exhibit. The exhibited configurations do not allow the switches to form a trunk. What is the most likely cause of this problem?

Cisco switches only support the ISL trunking protocol.

The trunk cannot be negotiated with both ends set to `auto`.

By default, Switch1 will only allow VLAN 5 across the link.

A common native VLAN should have been configured on the switches.

12. Switch port fa0/1 was manually configured as a trunk, but now it will be used to connect a host to the network. How should the network administrator reconfigure switch port Fa0/1?

Disable DTP.

Delete any VLANs currently being trunked through port Fa0/1.

Administratively shut down and re-enable the interface to return it to default.

Enter the `switchport mode access` command in interface configuration mode.

13. Refer to the exhibit. Computer B is unable to communicate with computer D. What is the most likely cause of this problem?

The link between the switches is up but not trunked.

VLAN 3 is not an allowed VLAN to enter the trunk between the switches.

The router is not properly configured to route traffic between the VLANs.

Computer D does not have a proper address for the VLAN 3 address space.

14. Refer to the exhibit. The network administrator has just added VLAN 50 to Switch1 and Switch2 and assigned hosts on the IP addresses of the VLAN in the 10.1.50.0/24 subnet range. Computer A can communicate with computer B, but not with computer C or computer D. What is the most likely cause of this problem?

There is a native VLAN mismatch.

The link between Switch1 and Switch2 is up but not trunked.

The router is not properly configured for inter-VLAN routing.

VLAN 50 is not allowed to enter the trunk between Switch1 and Switch2.

15. Refer to the exhibit. Which statement is true concerning interface Fa0/5?

The default native VLAN is being used.

The trunking mode is set to `auto`.

Trunking can occur with non-Cisco switches.

VLAN information about the interface encapsulates the Ethernet frames.

16. What statements describe how hosts on VLANs communicate?

Hosts on different VLANs use VTP to negotiate a trunk.

Hosts on different VLANs communicate through routers.

Hosts on different VLANs should be in the same IP network.

Hosts on different VLANs examine VLAN ID in the frame tagging to determine if the frame is for their network.

17. Refer to the exhibit. How far is a broadcast frame that is sent by computer A propagated in the LAN domain?

none of the computers will receive the broadcast frame

computer A, computer B, computer C

computer A, computer D, computer G

computer B, computer C

computer D, computer G

computer A, computer B, computer C, computer D, computer E, computer F, computer G, computer H, computer I

18. What is a valid consideration for planning VLAN traffic across multiple switches?

Configuring interswitch connections as trunks will cause all hosts on any VLAN to receive broadcasts from the other VLANs.

A trunk connection is affected by broadcast storms on any particular VLAN that is carried by that trunk.

Restricting trunk connections between switches to a single VLAN will improve efficiency of port usage.

Carrying all required VLANs on a single access port will ensure proper traffic separation.

19. Which two statements about the 802.1q trunking protocol are true? (Choose two.)

802.1q is Cisco proprietary.

802.1q frames are mapped to VLANs by MAC address.

If 802.1q is used on a frame, the FCS must be recalculated.

802.1q will not perform operations on frames that are forwarded out access ports.

802.1q allows the encapsulation of the original frame to identify the VLAN from which a frame originated.

20. What switch port modes will allow a switch to successfully form a trunking link if the neighboring switch port is in "dynamic desirable" mode?

dynamic desirable mode

on or dynamic desirable mode

on, auto, or dynamic desirable mode

on, auto, dynamic desirable, or nonegotiate mode

21. Refer to the exhibit. Company HR is adding PC4, a specialized application workstation, to a new company office. The company will add a switch, S3, connected via a trunk link to S2, another switch. For security reasons the new PC will reside in the HR VLAN, VLAN 10. The new office will use the 172.17.11.0/24 subnet. After installation, the existing PCs are unable to access shares on PC4. What is the likely cause?

The switch to switch connection must be configured as an access port to permit access to VLAN 10 on S3.

The new PC is on a different subnet so Fa0/2 on S3 must be configured as a trunk port.

PC4 must use the same subnet as the other HR VLAN PCs.

A single VLAN cannot span multiple switches.

22. What must the network administrator do to remove Fast Ethernet port fa0/1 from VLAN 2 and assign it to VLAN 3?

Enter the no vlan 2 and the vlan 3 commands in global configuration mode.

Enter the switchport access vlan 3 command in interface configuration mode.

Enter the switchport trunk native vlan 3 command in interface configuration mode.

Enter the no shutdown in interface configuration mode to return it to the default configuration and then configure the port for VLAN 3.

comments (1)

TOP

05:29

CCNA 3:Module 2

POSTED BY ADMIN

Options With Highlight Colours are Correct Answer

1. When a switch receives a frame and the source MAC address is not found in the switching table, what action will be taken by the switch to process the incoming frame?

The switch will request that the sending node resend the frame.

The switch will issue an ARP request to confirm that the source exists.

The switch will map the source MAC address to the port on which it was received.

The switch ends an acknowledgement frame to the source MAC of this incoming frame.

2. Refer to the exhibit. How many collision domains are depicted in the network?

1

2

4

6

7

8

3. Refer to the exhibit. What action does SW1 take on a frame sent from PC_A to PC_C if the MAC address table of SW1 is empty?

SW1 drops the frame.

SW1 floods the frame on all ports on SW1, except port Fa0/1.

SW1 floods the frame on all ports on the switch, except Fa0/23 and Fa0/1.

SW1 uses the CDP protocol to synchronize the MAC tables on both switches and then forwards the frame to all ports on SW2.

4. If a network administrator enters these commands in global configuration mode on a switch, what will be the result?

Switch1(config-line)# line console 0

Switch1(config-line)# password cisco

Switch1(config-line)# login

to secure the console port with the password "cisco"

to deny access to the console port by specifying 0 lines are available

to gain access to line configuration mode by supplying the required password
to configure the privilege exec password that will be used for remote access

5. A network administrator uses the CLI to enter a command that requires several parameters. The switch responds with "% Incomplete command". The administrator cannot remember the missing parameters. What can the administrator do to get the parameter information?

append ? to the last parameter

append a space and then ? to the last parameter

use Ctrl-P to show a parameter list

use the Tab key to show which options are available

6. Refer to the exhibit. The switch and the hub have default configurations, and the switch has built its CAM table. Which of the hosts will capture a copy of the frame when workstation A sends a unicast packet to workstation C?

workstation C

workstations B and C

workstations A, B, C, and the interfaces of the router

workstations B, C, D, E, F, and interfaces of the router

7. Which two statements are true regarding switch port security? (Choose two.)

The three configurable violation modes all log violations via SNMP.

Dynamically learned secure MAC addresses are lost when the switch reboots.

The three configurable violation modes all require user intervention to re-enable ports.

After entering the sticky parameter, only MAC addresses subsequently learned are converted to secure MAC addresses.

If fewer than the maximum number of MAC addresses for a port are configured statically, dynamically learned addresses are added to CAM until the maximum number is reached.

8. Refer to the exhibit. The exhibit shows partial output of the show running-config command. The enable password on this switch is "cisco." What can be determined from the output shown?

The enable password is encrypted by default.

An MD5 hashing algorithm was used on all encrypted passwords.

Any configured line mode passwords will be encrypted in this configuration.

This line represents most secure privileged EXEC mode password possible.

9. What are two ways to make a switch less vulnerable to attacks like MAC address flooding, CDP attacks, and Telnet attacks? (Choose two.)

Enable CDP on the switch.

Change passwords regularly.

Turn off unnecessary services.

Enable the HTTP server on the switch.

Use the enable password rather than the enable secret password.

10. Refer to the exhibit. The switch and workstation are administratively configured for full-duplex operation. Which statement accurately reflects the operation of this link?

No collisions will occur on this link.

Only one of the devices can transmit at a time.

The switch will have priority for transmitting data.

The devices will default back to half duplex if excessive collisions occur.

11. Where is the startup configuration stored?

DRAM

NVRAM

ROM

startup-config.text

12. Refer to the exhibit. What happens when Host 1 attempts to send data?

Frames from Host 1 cause the interface to shut down.

Frames from Host 1 are dropped and no log message is sent.

Frames from Host 1 create a MAC address entry in the running-config.

Frames from Host 1 will remove all MAC address entries in the address table.

13. Which statement is true about the command banner login "Authorized personnel Only" issued on a switch?

The command is entered in privileged EXEC mode.

The command will cause the message Authorized personnel Only to display before a user logs in.

The command will generate the error message % Ambiguous command: "banner motd" " to be displayed.

The command will cause the message End with the character "%" to be displayed after the command is entered into the switch.

14. Refer to the exhibit. The network administrator's attempts to connect to Switch1 via Secure Shell are failing. What is most likely the problem?

incorrect vty lines configured

incompatible Secure Shell version

incorrect default gateway address

vtty lines that are configured to allow only Telnet

15. What happens when the transport input ssh command is entered on the switch vty lines?

The SSH client on the switch is enabled.

Communication between the switch and remote users is encrypted.

A username/password combination is no longer needed to establish a secure remote connection to the switch.

The switch requires remote connections via proprietary client software.

16. Which two statements about Layer 2 Ethernet switches are true? (Choose two.)

Layer 2 switches prevent broadcasts.

Layer 2 switches have multiple collision domains.

Layer 2 switches route traffic between different networks.

Layer 2 switches decrease the number of broadcast domains.

Layer 2 switches can send traffic based on the destination MAC address.

17. Refer to the exhibit. Which hosts will receive a broadcast frame sent from Host A?

hosts A and B

hosts B and C

hosts D and E

hosts A, B, and C

hosts B, C, D, and E

hosts A, B, C, D, E, and F

18. Which command line interface (CLI) mode allows users to configure switch parameters, such as the hostname and password?

user EXEC mode

privileged EXEC mode

global configuration mode

interface configuration mode

19. Which two statements are true about EXEC mode passwords? (Choose two.)

The enable secret password command stores the configured password in plain text.

The enable secret password command provides better security than the enable password.

The enable password and enable secret password protect access to privileged EXEC mode.

The service password-encryption command is required to encrypt the enable secret password.

Best practices require both the enable password and enable secret password to be configured and used simultaneously.

20. When a collision occurs in a network using CSMA/CD, how do hosts with data to transmit respond after the backoff period has expired?

The hosts return to a listen-before-transmit mode.

The hosts creating the collision have priority to send data.

The hosts creating the collision retransmit the last 16 frames.

The hosts extend their delay period to allow for rapid transmission.

[comments \(1\)](#)

[TOP](#)

05:27

CCNA 3:Module 1

POSTED BY ADMIN

Options With Highlight Colours are Correct Answer

1. A network technician is asked to examine an existing switched network. Following this examination, the technician makes recommendations for adding new switches where needed and replacing existing equipment that hampers performance. The technician is given a budget and asked to proceed. Which two pieces of information would be helpful in determining necessary port density for new switches? (Choose two.)

forwarding rate

traffic flow analysis

expected future growth

number of required core connections

number of hubs that are needed in the access layer to increase performance

2. Configuring communication between devices on different VLANs requires the use of which layer of the OSI model?

Layer 1

Layer 3

Layer 4

Layer 5

3. What is the likely impact of moving a conventional company architecture to a completely converged network?

Local analog phone service can be completely outsourced to cost-effective providers.

The Ethernet VLAN structure is less complex.

A shared infrastructure is created resulting in a single network to manage.

QoS issues are greatly reduced.

There is less bandwidth competition between voice and video streams

4. Which hierarchical design model layer controls the flow of network traffic using policies and delineates broadcast domains by performing routing functions between virtual LANs (VLANs)?

application

access

distribution

network

core

5. A network administrator is selecting a switch that will operate at the

network core. Which three features should the switch support for optimum network performance and reliability? (Choose three.)

- port security
- security policies
- 10 Gigabit Ethernet
- quality of service (QoS)
- hot-swappable hardware
- Power over Ethernet (PoE)

6. Which three features are commonly supported at the distribution layer of the Cisco hierarchical network model? (Choose three.)

- security policies
- Power over Ethernet
- switch port security
- quality of service
- Layer 3 functionality
- end user access to network

7. Which two features are supported at all three levels of the Cisco three-layer hierarchical model? (Choose two.)

- Power over Ethernet
- load balancing across redundant trunk links
- redundant components
- Quality of Service
- link aggregation

8. Which two characteristics are associated with enterprise level switches? (Choose two.)

- low port density
- high forwarding rate
- high latency level
- support link aggregation
- predefined number of ports

9. Link aggregation should be implemented at which layer of the hierarchical network?

- core only
- distribution and core
- access and distribution
- access, distribution, and core

10. For organizations that are implementing a voice over IP solution, what functionality should be enabled at all three layers of the hierarchical network?

- Power over Ethernet
- quality of service
- switch port security
- inter-VLAN routing

11. Which layer of the hierarchical design model provides a means of connecting devices to the network and controlling which devices are allowed to communicate on the network?

- application
- access
- distribution
- network
- core

12. At which hierarchical layer are switches normally not required to process all ports at wire speed?

- core layer
- distribution layer
- access layer
- entry layer

13. Which layer of the OSI model does an access layer LAN switch use to make a forwarding decision?

- Layer 1
- Layer 2
- Layer 3
- Layer 4

14. Refer to the exhibit. What characteristic of hierarchical network designs is exhibited by having SW3 connected to both SW1 and Sw2?

- scalability
- security
- redundancy
- maintainability

15. Which layer of the hierarchical network design model is referred to as the high-speed backbone of the internetwork, where high availability and redundancy are critical?

- access layer
- core layer
- data-link layer
- distribution layer
- network layer
- physical layer

16. What statement best describes a modular switch?

- a slim-line chassis
- allows interconnection of switches on redundant backplane

defined physical characteristics
[flexible characteristics](#)

17. A technician is attempting to explain Cisco StackWise technology to a client that is setting up three stackable switches. Which explanation accurately describes StackWise technology?

StackWise technology allows up to eight ports to be bound together to increase available bandwidth.
 StackWise technology allows the switch to deliver power to end devices by using existing Ethernet cabling.
 StackWise technology allows the switch capabilities and ports to be expanded by the addition of line cards.
[StackWise technology allows up to nine switches to be interconnected via the use of a fully redundant backplane.](#)

18. Which hierarchical design characteristic would be recommended at both the core and distribution layers to protect the network in the case of a route failure?

PoE
[redundancy](#)
 aggregation
 access lists

19. Which feature supports higher throughput in switched networks by combining multiple switch ports?

convergence
 redundant links
[link aggregation](#)
 network diameter

20. Refer to the exhibit. Beginning with HR servers and workstations, a network engineer is designing a new security structure for the network. Which set of policies adheres to the hierarchical network model design principles?

Implement Layer 3 switching on S1 to reduce the packet processing load on D1 and D2. Install all security processing on S1 to reduce network traffic load.
[Configure port security options on S1. Use Layer 3 access control features on D1 and D2 to limit access to the HR servers to just the HR subnet.](#)
 Move all HR assets out of the data center and connect them to S1. Use Layer 3 security functions on S1 to deny all traffic into and out of S1.
 Perform all port access and Layer 3 security functions on C1.

[comments \(0\)](#)

[TOP](#)

[Newer Posts](#) [Older Posts](#) | [Home](#)
 Subscribe to: [Posts \(Atom\)](#)

ВНИМАНИЕ!
ВПЕРВЫЕ!
 Определение местонахождения
 мобильного телефона с точностью
 до 500 метров!
[Регистрация](#) [Подробнее...](#)
 Пример: +79130000001
 +7
[Показать на карте](#)

mobile-spy.ru

Обратная связь - Реклама от Google

Advertise Here

Advertise Here

7203671944

Место информации на этом сайте