Exam Number/Code :   642-813

Exam Name: Implementing Cisco IP
Switched Networks

Version :   Demo

QUESTION 1
Which method of Layer 3 switching uses a forwarding information base (FIB)?

A. Topology-based switching
B. Demand-based switching
C. Route caching
D. Flow-based switching

Answer: A
Section: Layer 3, ip routing
Explanation/Reference:
The Layer 3 engine (essentially a router) maintains routing information, whether from static routes or dynamic routing protocols. Basically, the routing table is reformatted into an ordered list with the most specific route first, for each IP destination subnet in the table. The new format is called a Forwarding Information Base (FIB) and contains routing or forwarding information that the network prefix can reference. In other words, a route to 10.1.0.0/16 might be contained in the FIB, along with routes to 10.1.1.0/24 and 10.1.1.128/25, if those exist. Notice that these examples are increasingly more specific subnets. In the FIB, these would be ordered with the most specific, or longest match, first, followed by less specific subnets. When the switch receives a packet, it can easily examine the destination address and find the longest match entry in the FIB. The FIB also contains the next-hop address for each entry. When a longest match entry is found in the FIB, the Layer 3 next-hop address is found, too.

QUESTION 2
Refer to the exhibit. On the basis of the information provided in the exhibit, which two sets of procedures are best practices for Layer 2 and 3 failover alignment? (Choose two.)
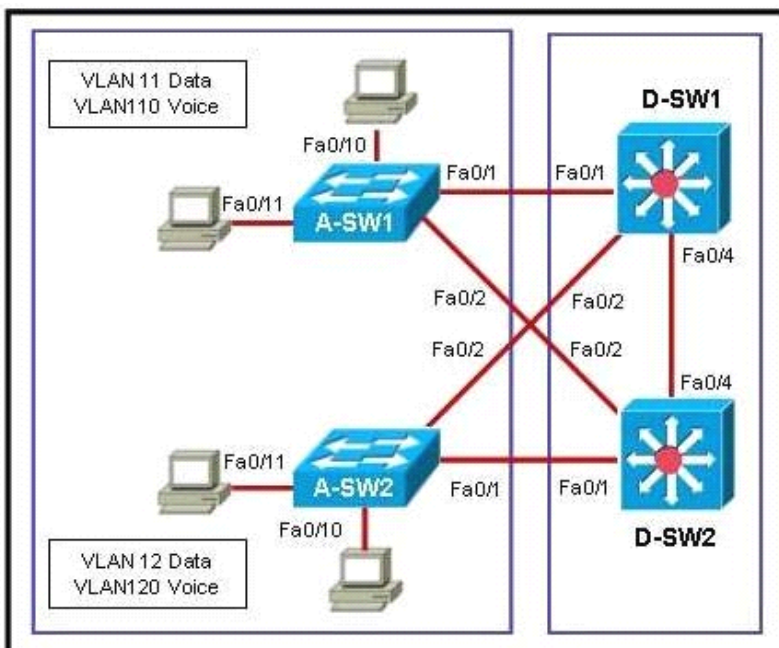
A. Configure the D-SW1 switch as the active HSRP router and the STP root for all VLANs. Configure the D-SW2 switch as the standby HSRP router and backup STP root for all VLANs.

B. Configure the D-SW1 switch as the standby HSRP router and the STP root for VLANs 11 and 110. Configure the D-SW2 switch as the standby HSRP router and the STP root for 111. VLANs 12 and 120.

C. Configure the D-SW1 switch as the active HSRP router and the STP root for VLANs 11 and 110. Configure the D-SW2 switch as the active HSRP router and the STP root for VLANs 12 and 120.

D. Configure the D-SW2 switch as the active HSRP router and the STP root for all VLANs. Configure the D-SW1 switch as the standby HSRP router and backup STP root for all VLANs.

E. Configure the D-SW1 switch as the active HSRP router and the backup STP root for VLANs 11 and 110. Configure the D-SW2 switch as the active HSRP router and the backup STP root for VLANs 12 and 120.

F. Configure the D-SW1 switch as the standby HSRP router and the backup STP root for VLANs 12 and 120. Configure the D-SW2 switch as the standby HSRP router and the backup STP root for VLANs 11 and 110.

Answer: CF
Section: HSRP, VRRP, GLBP
Explanation/Reference:
Basically, each of the routers that provides redundancy for a given gateway address is assigned to a common HSRP group. One router is elected as the primary, or active, HSRP router, another is elected as the standby HSRP router, and all the others remain in the listen HSRP state. The routers exchange HSRP hello messages at regular intervals, so they can remain aware of each other's existence, as well as that of the active router.

HSRP election is based on a priority value (0 to 255) that is configured on each router in the group. By default, the priority is 100. The router with the highest priority value (255 is highest) becomes the active router for the group. If all router priorities are equal or set to the default value, the router with the highest IP address on the HSRP interface becomes the active router. To set the priority, use the following interface configuration command:
Switch(config-if)# standby group priority priority

When HSRP is configured on an interface, the router progresses through a series of states before becoming active. This forces a router to listen for others in a group and see where it fits into the pecking order. The HSRP state sequence is Disabled, Init, Listen, Speak, Standby, and, finally, Active.
You can configure a router to preempt or immediately take over the active role if its priority is the highest at any time. Use the following interface configuration command to allow preemption:
Switch(config-if)# standby group preempt [delay seconds]

QUESTION 3
If you needed to transport traffic coming from multiple VLANs (connected between switches), and your CTO was insistent on using an open standard, which protocol would you use?

A. 802.11B
B. spanning-tree
C. 802.1Q
D. ISL
E. VTP
F. Q.921

Answer: C
Section: Layer 2, VTP, VLAN design
Explanation/Reference:
The act involved in the above question is trunking. The two trunking protocols in the answer choices are: 802.1Q and ISL. ISL is Cisco proprietary and IEEE 802.1Q is based on an open standard. When non-Cisco switches are used along with Cisco switches and trunking is required, it is best to use the 802.1Q encapsulation.
Incorrect Answers:
A: This standard is used in wireless networking and has nothing to do with VLAN switching.
B: The Spanning Tree Protocol (STP) is used to prevent loops within a bridged network. Each VLAN runs a separate instance of the STP and this is enabled by default.
D: This is the alternative Cisco proprietary method of trunking.
E: VLAN Trunking Protocol (VTP) is a Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs on a network-wide basis. It is not used to actually transport VLAN traffic.
F: This is an ISDN signaling standard and is not related with VLAN switching.

QUESTION 4
Under what circumstances should an administrator prefer local VLANs over end-to-end VLANs?

A. Eighty percent of traffic on the network is destined for Internet sites.
B. There are common sets of traffic filtering requirements for workgroups located in multiple buildings.
C. Eighty percent of a workgroup's traffic is to the workgroup's own local server.
D. Users are grouped into VLANs independent of physical location.

Answer: A
Section: Layer 2, VTP, VLAN design

Explanation/Reference:

This geographic location can be as large as an entire building or as small as a single switch inside a wiring closet. In a geographic VLAN structure, it is typical to find 80 percent of the traffic remote to the user (server farms and so on) and 20 percent of the traffic local to the user (local server, printers, and so on). Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 93

QUESTION 5

What are some virtues of implementing end-to-end VLANs? (Choose two)

A. End-to-end VLANs are easy to manage.
B. Users are grouped into VLANs independent of a physical location.
C. Each VLAN has a common set of security and resource requirements for all members.
D. Resources are restricted to a single location.

Answer: BC
Section: Layer 2, VTP, VLAN design
Explanation/Reference:

In an end-to-end VLAN, users are grouped into VLANs independent of physical location and dependent on group or job function.
Each VLAN has a common set of security requirements for all members.
Incorrect Answers:
A: End to end VLANs are more difficult to manage than local VLANs, due to the physical distances that they can span.
D: In an end-to-end VLAN, network resources are generally distributed across the entire enterprise wide area network.

QUESTION 6

Which of the following statements is true about the 80/20 rule (Choose two)?

A. 20 percent of the traffic on a network segment should be local
B. no more than 20 percent of the network traffic should be able to move across a backbone.
C. no more than 80 percent of the network traffic should be able to move across a backbone.
D. 80 percent of the traffic on a network segment should be local

Answer: BD
Section: Layer 2, VTP, VLAN design
Explanation/Reference:

The 80/20 rule in network design originated from the idea that most of the traffic should remain local to the LAN, since bandwidth is plentiful compared to WAN links, and a great deal of broadcast traffic that is evident at the LAN is not passed over the backbone. Note:

With the availability of inexpensive bandwidth and centralized data centers, this rule appears to have become obsolete. In fact, most networks have taken on the 20/80 rules, as opposed to the legacy 80/20 rule.

QUESTION 7

The Company LAN is becoming saturated with broadcasts and multicast traffic. What could you do to help a network with many multicasts and broadcasts?

A. Creating smaller broadcast domains by implementing VLANs.
B. Separate nodes into different hubs.
C. Creating larger broadcast domains by implementing VLANs.
D. Separate nodes into different switches.
E. All of the above.

Answer: A
Section: Layer 2, VTP, VLAN design
Explanation/Reference:
Controlling broadcast propagation throughout the network is important to reduce the amount of overhead associated with these frames. Routers, which operate at Layer 3 of the OSI model, provide broadcast domain segmentation for each interface. Switches can also provide broadcast domain segmentation using virtual LANs (VLANs). A VLAN is a group of switch ports, within a single or multiple switches, that is defined by the switch hardware and/or software as a single broadcast domain. A VLANs goal is to group devices connected to a switch into logical broadcast domains to control the effect that broadcasts have on other connected devices. A VLAN can be characterized as a logical network.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 8

QUESTION 8

The Company LAN switches are being configured to support the use of Dynamic VLANs. Which of the following are true of dynamic VLAN membership? (Choose two)

A. VLAN membership of a user always remains the same even when he/she is moved to another location.
B. VLAN membership of a user always changes when he/she is moved to another location.
C. Membership can be static or dynamic.
D. Membership can be static only.

Answer: AC
Section: Layer 2, VTP, VLAN design
Explanation/Reference:
Dynamic VLAN memberships are based on the users MAC address connected to the port.

If you have VTP server, a VTP database file, a VTP client switch, and a dynamic port; regardless of where your physical location is, you can still remain in the same VLAN.
Incorrect Answers:
B: This was true before the use of Dynamic VLAN membership, as VLANs were assigned to ports, not users.
D: VLAN memberships can be either static or dynamic.

QUESTION 9
The Company LAN switches are being configured to support the use of Dynamic VLANs. What should be considered when implementing a dynamic VLAN solution? (Choose two)

A. Each switch port is assigned to a specific VLAN.
B. Dynamic VLANs require a VLAN Membership Policy Server.
C. Devices are in the same VLAN regardless of which port they attach to.
D. Dynamic VLAN assignments are made through the command line interface.

Answer: BC
Section: Layer 2, VTP, VLAN design
Explanation/Reference:
With VLAN Membership Policy Server (VMPS), you can assign switch ports to VLANs dynamically, based on the source Media Access Control (MAC) address of the device connected to the port. When you move a host from a port on one switch in the network to a port on another switch in the network, the switch assigns the new port to the proper VLAN for that host dynamically.
Note: There are two types of VLAN port configurations: static and dynamic.
Incorrect Answers
A: In a static VLAN, the administrator assigns switch ports to the VLAN, and the association does not change until the administrator changes the port assignment.
However, this is not the case of dynamic VLANs.
D: The Command Line Interface is not used for dynamic VLAN assignments. Reference: Cisco Online, Configuring Dynamic Port VLAN Membership with VMPS

QUESTION 10
In the three-layer hierarchical network design model; what's associated with the access layer? (Choose two)

A. optimized transport structure
B. high port density
C. boundary definition
D. data encryption
E. local VLANs

F. route summaries

Answer: BE
Section: Layer 2, VTP, VLAN design
Explanation/Reference:
The access layer is the outermost layer, and it is composed of the least sophisticated network equipment. The most important function of the access layer is high port density, since these devices connect the individual end users. The access layers are also where VLANs are implemented, since VLANs are assigned on a per-port basis.

QUESTION 11
You are assigning VLANs to the ports of switch R1. What VLAN number value is an assigned to the default VLAN?

A. VLAN 1003
B. VLAN 1
C. VLAN ON
D. VLAN A
E. VLAN 0

Answer: B
Section: Layer 2, VTP, VLAN design
Explanation/Reference:
The default VLAN is VLAN 1. Although this VLAN can be modified, it can not be deleted from the switch. The following VLANs are on by default for all Cisco Catalyst switches:
VLAN 1 - Default VLAN
VLAN 1002 - Default FDDI VLAN
VLAN 1003 - Default Token Ring VLAN
VLAN 1004 - Default FDDI Net VLAN
VLAN 1005 - Default Token Ring Net VLAN
Incorrect Answers:
A: This is the default Token Ring VLAN that is installed in the switch IOS. It is seldom used.
C: ON is a VTP configuration mode, but is not a normal VLAN name.
D: Although any VLAN can be named VLAN A, it is not created by default.
E: Although in Cisco IOS the number 0 has significance (i.e. ethernet 0, console port 0, serial 0) in VLANs 1 is the default. VLAN 0 is an invalid VLAN and can not be used.

QUESTION 12
The VLANs in switch R1 are being modified. Which of the following are updated in R1 every time a VLAN is modified? (Choose two)

A. Configuration revision number

B. Configuration revision flag field

C. Configuration revision reset switch

D. Configuration revision database

Answer: AD

**Section:** Layer 2, VTP, VLAN design

Explanation/Reference:

For accountability reasons, every time a VLAN is modified the revision number changes, as does the information in the configuration revision database (as that is where the VLAN information is stored).

Incorrect Answers:

B, C: The configuration revision flag field, and the configuration revision reset switch don't exist in this context.

QUESTION 13
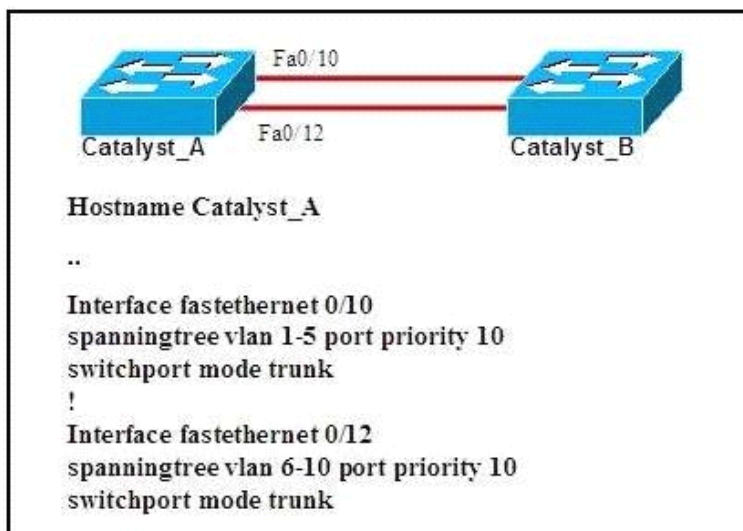
Given the above partial configuration, which two statements are true about VLAN traffic? (Choose two.)

A. VLANs 1-5 will use fa0/10 as a backup only.

B. VLANs 6-10 will use fa0/10 as a backup only.

C. VLANs 1-5 will be blocked if fa0/10 goes down.

D. VLANs 1-10 are configured to load share between fa0/10 and fa0/12.

E. VLANs 6-10 have a port priority of 128 on fa0/10.

Answer: BD

Section: Layer 2, VTP, VLAN design

Explanation/Reference:

Spanning-Tree Protocol (STP) is a Layer 2 protocol that utilizes a special-purpose

algorithm to discover physical loops in a network and effect a logical loop-free topology. STP creates a loop-free tree structure consisting of leaves and branches that span the entire Layer 2 network. The actual mechanics of how bridges communicate and how the STP algorithm works will be discussed at length in the following topics. Note that the terms bridge and switch are used interchangeably when discussing STP. In addition, unless otherwise indicated, connections between switches are assumed to be trunks.

Load sharing can be accomplished using a couple of methods. The most common method of load sharing is through root bridge placement on a per-VLAN basis. This will distribute traffic for separate VLANs across separate paths to different root bridges. A separate method divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, STP normally blocks all but one parallel link between switches. Using load sharing, traffic can be divided between the links according to which VLAN the traffic belongs.

Load sharing can be configured on trunk ports by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch. For load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches.
Load Sharing Using STP Port Priorities
When two ports on the same switch form a loop, the STP port priority setting determines which port is enabled and which port is in a blocking state. The priorities on a parallel trunk port can be set so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a Blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.

QUESTION 14
What is a characteristic of a static VLAN membership assignment?

A. VMPS server lookup is required
B. Easy to configure
C. Ease of adds, moves, and changes
D. Based on MAC address of the connected device

Answer: B
Section: Layer 2, VTP, VLAN design
Explanation/Reference:
Static port VLAN membership on the switch is assigned manually by the administrator on a port-by-port basis.
Characteristics of static VLAN configurations include the following:
1. Secure
2. Easy to configure
3. Straight forward to monitor

4. Works well in networks where moves, adds, and changes are rare.

Incorrect Answers:

A: VMPS server lookups are a function of dynamic VLANs and are not used with statically assigned VLANs.

C: Moves, adds, and changes, would require a network administrator to change the configuration of the switch every time a change is required.

D: This would describe a function of dynamic VLAN configurations, where the MAC address of the end user determines the VLAN that it belongs in, instead of the physical port.

QUESTION 15

Static VLANs are being used on the Company network. What is true about static VLANs?

A. Devices use DHCP to request their VLAN.

B. Attached devices are unaware of any VLANs.

C. Devices are assigned to VLANs based on their MAC addresses.

D. Devices are in the same VLAN regardless of which port they attach to.

Answer: B

Section: Layer 2, VTP, VLAN design

Explanation/Reference:

LAN port VLAN membership can be assigned manually on a port-by-port basis. When you assign LAN ports to VLANs using this method, it is known as port-based, or static, VLAN membership.

Attached devices will be unaware of any VLANs.

Incorrect Answers:

A: The DHCP service is not involved in VLAN assignment.

C: Devices are not assigned to VLAN based on their MAC addresses. This is a function of dynamic VLANs.

D: Static VLANs are configured on a port by port basis.

Reference: Configuring VLANs

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/121_8aex/swconfig/vlans.htm

QUESTION 16

Two Company switches are connected via a trunk using VTP. Which VTP information does a Catalyst switch advertise on its trunk ports when using VTP? (Choose two)

A. STP root status

B. VTP mode

C. Negotiation status

D. Management domain

E. Configuration revision number

Answer: DE

Section: Layer 2, VTP, VLAN design

Explanation/Reference:

The role of the VLAN Trunking Protocol (VTP) is to maintain VLAN configuration consistency across the entire network. VTP is a messaging protocol that uses Layer 2 trunk frames to manage the addition, deletion, and renaming of VLANs on a network-wide basis from a centralized switch that is in the VTP server mode. VTP is responsible for synchronizing VLAN information within a VTP domain. This reduces the need to configure the same VLAN information on each switch. Using VTP, each Catalyst Family Switch advertises the following on its trunk ports:

1. Management domain

2. Configuration revision number

3. Known VLANs and their specific parameters

QUESTION 17

The lack of which two prevents VTP information from propagating between switches? (Choose two.)

A. A root VTP server

B. A trunk port

C. VTP priority

D. VLAN 1

Answer: BD

Section: Layer 2, VTP, VLAN design

Explanation/Reference:

In Switch tow types of links are available, access and trunk. The interface is in access mode can carry the information of only one VLAN and trunk can carry the information of more than one VLAN. VTP carry the information of more than one vlan so Switch port should be in trunk mode. VLAN1 is the default VLAN on Cisco Switch, by default all interface belongs to VLAN 1.

QUESTION 18

What is the default VTP advertisement for subset advertisements in Catalyst switches that are in server or client mode?

A. 30 seconds

B. 5 minutes

C. 1 minute

D. 10 seconds

E. 5 seconds

Answer: B

**Section:** Layer 2, VTP, VLAN design

Explanation/Reference:

Periodic (default is 5 minutes) VTP advertisements are sent out each trunk port with the multicast destination MAC address 01-00-0C-CC-CC-CC. VTP advertisements contain the following configuration information:

1. VLAN IDs (ISL and 802.1Q)

2. Emulated LAN names (ATM LANE)

3. 802.10 SAID values (FDDI)

4. VTP domain name

5. VTP configuration revision number

6. VLAN configuration, including the maximum transmission unit (MTU) size for each VLAN

7. Frame format

QUESTION 19

Refer to the exhibit. VTP has been enabled on the trunk links between all switches within the TEST domain. An administrator has recently enabled VTP pruning. Port 1 on Switch 1 and port 2 on Switch 4 are assigned to VLAN 2. A broadcast is sent from the host connected to Switch 1. Where will the broadcast propagate?
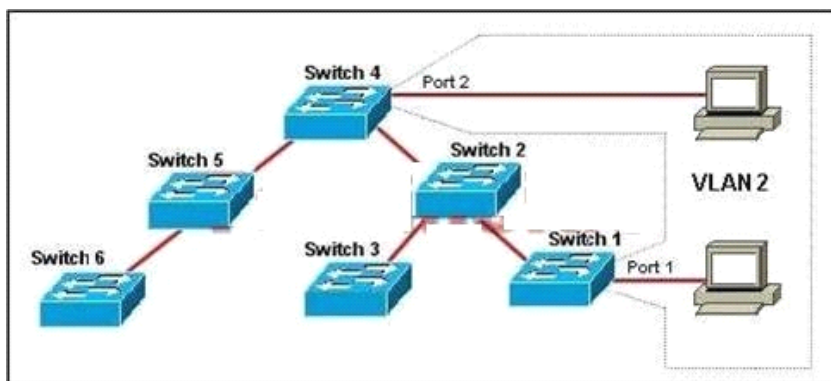
A. Every switch in the network receives the broadcast and will forward it out all ports.

B. Every switch in the network receives the broadcast, but only Switch 4 will forward it out port 2.

C. Switches 1, 2, and 4 will receive the broadcast, but only Switch 4 will forward it out port 2.

D. Only Switch 4 will receive the broadcast and will forward it out port 2.

Answer: C

Section: Layer 2, VTP, VLAN design

Explanation/Reference:

The default behavior of a switch is to propagate broadcast and unknown packets across the network. This behavior results in a large amount of unnecessary traffic crossing the network.

VTP pruning increases bandwidth efficiency by reducing unnecessary flooding of traffic, such as broadcast, multicast, unknown, and flooded unicast packets. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices. By default, VTP pruning is disabled.

Enabling VTP pruning on a VTP server enables pruning for the entire management domain. VTP pruning takes effect several seconds after it is enabled. By default, VLANs 2 through 1000 or 2 through 1001 are pruning eligible, depending upon the platform. VTP pruning does not prune traffic from VLANs that are pruning ineligible. VLAN 1 is always pruning ineligible and VLAN 1 cannot be removed from a trunk. However, the "VLAN 1 disable on trunk" feature available on Catalyst 4000, 5000, and 6000 family switches enables the pruning of user traffic, but not protocol traffic such as CDP and VTP, for VLAN 1 from a trunk. Use the vtp pruning command to make VLANs pruning eligible on a Cisco IOS-based switch.

Switch(vlan)#vtp pruning

Once pruning is enabled, use the switchport trunk pruning command to make a specific VLAN pruning ineligible.

Switch(config)#interface fastethernet 0/3

Switch(config-if)#switchport trunk pruning vlan remove vlan 5

QUESTION 20

What must be configured on a Cisco switch in order to advertise VLAN information?

A. VTP mode

B. VTP password

C. VTP revision number

D. VTP pruning

E. VTP domain name

Answer: E

Section: Layer 2, VTP, VLAN design

Explanation/Reference:

If the switch being installed is the first switch in the network, the management domain will need to be created. However, if the network has other switches running VTP, then the new switch will join an existing management domain. Verify the name of the management domain. If the management domain has been secured, verify and configure the password

for the domain.

To create a management domain or to add a switch to a management domain, use the vtp domain command in the global configuration mode or VLAN configuration mode.

Switch(config)#vtp domain name

Switch(vlan)#vtp domain