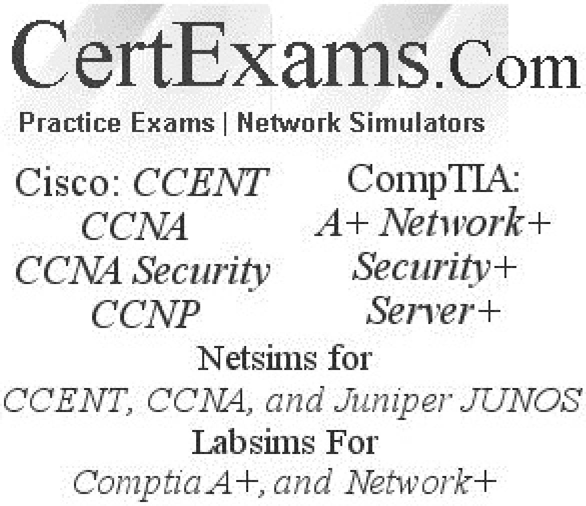
Cisco® CCNP Switch Exam Cram Notes : Configuring and verifying switch administration

examguides.com/CCNP-Switch/ccnp-switching-1.htm



1. Layer2 Technologies

1.1 Configure and verify switch administration

1.1.a SDM templates:

SDM stands for Switching Database Manager. SDM templates are used to manage the system resources on a switch to their appropriate location and usability on the network for specific features. You can configure a template to allocate more resources for ACL, Vlans, mac addresses tables, etc.

You can select SDM templates for IP Version 4 (IPv4) to optimize these features:

Routing: The routing template maximizes system resources for unicast routing, typically required for a router in the center of a network.

VLANs: The VLAN template disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 switch.

Default: The default template gives balance to all functions.

Access: The access template maximizes system resources for access control lists (ACLs) to accommodate a large number of ACLs.

Use the "no sdm" prefer command to reset the switch to the default desktop template. The default template balances the use of system resources.

To specify the SDM template to be used on the switch, use the following command in global config mode:

sdm prefer {access | default | dual-ipv4-and-ipv6 {default | routing | vlan} | routing | vlan}

The keywords have these meanings:

1. access - Maximize system resources for ACLs.

2. default - Give balance to all functions.

3. dual - ipv4 - and-ipv6 - Select a template that supports both IPv4 and IPv6 routing.

4. default - Balance IPv4 and IPv6 Layer 2 and Layer 3 functionality.

5. routing - Provide maximum usage for IPv4 and IPv6 routing, including IPv4 policy-based routing.

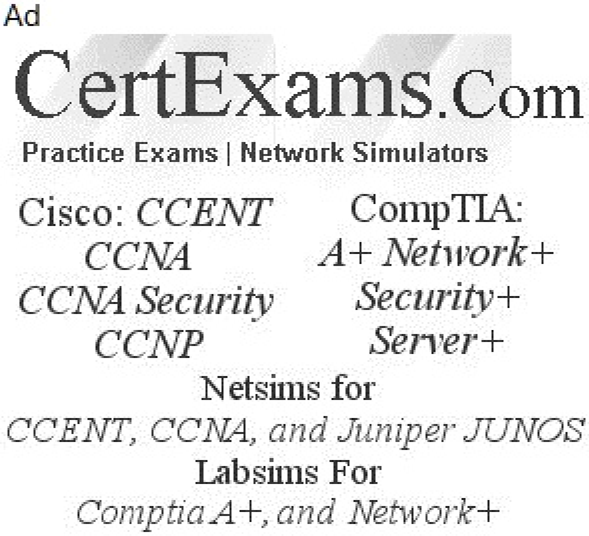
6. vlan - Provide maximum usage for IPv4 and IPv6 VLANs.

7. routing - Maximize routing on the switch.

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Managing Mac Address Table

examguides.com/CCNP-Switch/ccnp-switching-2.htm



1. Layer2 Technologies

1.1 Configure and verify switch administration

1.1.b Managing MAC address table:

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

Commands for Displaying the MAC Address Table

show mac address-table address - Displays MAC address table information for the specified MAC address.

show mac address-table aging-time - Displays the aging time in all VLANs or the specified VLAN.

show mac address-table count - Displays the number of addresses present in all VLANs or the specified VLAN.

show mac address-table dynamic - Displays only dynamic MAC address table entries.

show mac address-table interface - Displays the MAC address table information for the specified interface.

show mac address-table learning - Displays MAC address learning status of all VLANs or the specified VLAN.

show mac address-table static - Displays only static MAC address table entries.

show mac address-table vlan - Displays the MAC address table information for the specified VLAN.

Dynamic address: a source MAC address that the switch learns and then ages when it is not in use.

Static address: a manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).

Layer 2 switching is based on hardware based bridging, whereas Layer 3 switching is based on hardware based routing. Layer 2 switching is done based on physical (MAC) addresses, whereas Layer 3 switching is based on logical address.

The devices functioning at Access Layer are usually characterized with higher port density and lower cost. These devices also provide LAN segmentation.

Typically, the following are performed at the Access Layer (AL):

1. Enable MAC address filtering: Here, the switch is configured to allow/deny access to network resources depending on the host machine's MAC address (also called the physical address).

2. Create separate collision domains: A switch can be configured to use separate collision domain for each connected node to improve performance.

3. Support for various devices: The campus access layer supports multiple device types including phones, APs, video cameras, and laptops, with each requiring specific services and policies.

4. Handle switch bandwidth: You can move data from one network to another to perform load balancing.

5. Control of traffic: Ability to detect undesirable application traffic flows at the network access layer and allow for selected control (drop or police) of undesirable traffic.

Function of the core layer and distribution Layer

The primary function of a Core Layer is to switch traffic as fast as possible and providing connectivity between switch blocks, WAN blocks and/ or any other blocks that may be present. Provide back-bone High speed switching in a campus network enviornment

The Distribution Layer is responsible for routing traffic between VLANs, Broadcast domain definition, Inter-VLAN routing, and security.

The Access Layer is responsible for Layer 2 services, such as VLAN membership, traffic filtering based on broadcast or MAC addresses.

- Core layer: Designed for fast switching, high availability and redundancy.
- Distribution layer : The Distribution Layer is responsible for routing traffic between VLANs, Broadcast domain definition, Inter-VLAN routing, and security. Address summarization and media translation are applied in the distribution layer.
- Access layer : The access layer consists of the remote office sites using ISDN, Frame Relay etc. Local area networks segments are also part of the access layer.

Core layer is the high-speed switching backbone of any network. It is crucial for any corporate communication and any failure will be very costly. The core layer has the following characteristics:

1. High reliability

2. Adapt to changes quickly

3. Lower latency

4. Fast Switching

Distribution layer lies in between the Core layer and Access layer. It usually deals with the following:

1. Security

2. Access Control Lists

3. Route Summarization

4. Media translation

The distribution layer is already using 6500 series switches. Therefore, it is preferred to have same or better performance at Core level. Hence, the choice of Catalyst 6800 series switch is most appropriate among the given choices.

There are 3 primary ways to control access to distribution layer:

1. Access lists: Standard and extended access lists can be applied to filter unnecessary traffic from reaching Core Layer.

2. Route filters: The routes that are propagated to Core Layer can be controlled by using route filters by using the command distribution-list.

3. Network services control: Not all services need to be advertised to the Core Layer. Services such as DNS, DHCP, SAP updates can be filtered using commands such as ipx output-sap-filter.

Distribution layer is responsible for routing traffic between VLANs. This layer also provides LAN segmentation and terminates collision and broadcast domains.

When both the core and distribution layer functions are performed in the same device, it is said to be collapsed core design. A collapsed core design is suitable in small campus networks.

MAC addresses flooding: Here the attacking device floods frames with unique, invalid source MAC addresses to the switch and exhaust CAM table space of the attacked switch. The result is that new entries cannot be inserted because of the exhausted CAM table space, and traffic is subsequently flooded out all ports.

MAC address flooding may be prevented by using switch port security. By using "vlan access-map" switch ports may be configured to identify and block offending devices.

The "access-class in/out" command applies an access list to the virtual terminal line. Access list needs to be created before defining access-class command. Access lists applied with access-group command does not control traffic originating from that device (the device to which access-group is applied) itself. For this reason, you need to define access-class to control access to traffic, such as telnet that is originating in that device itself.

The following are true about a switch with TCAM:

1. Access list rules are compiles as TCAM entries

2. TCAM entries are evaluated in parallel

3. Access lists are processed with one TCAM table lookup.

4. Complex access lists take the same time as the simple access lists, using TCAM.

The command used to set the CAM table aging time is:

mac address-table aging-time <*seconds*>

Other important commands used with CAM table are:

1. **mac address-table static** <*mac-address*> **vlan** <*vlan-id*> **interface** <*type*> <*mode*>/<*num*>

The above command is used to configure a static CAM entry.

2. **clear mac address-table dynamic [address** <*mac-address*> |**interface** <*type*> <*mod*>/<*num*> | **vlan** <*vlan id*>**]**

The above command is used to clear a CAM table entry.

3. **show mac address-table dynamic [address** <*mac-address*> | **interface** <*type*> <*mod*>/<*num*> | **vlan** <*vlan-id*>**]**

The above command is used to view the contents of a CAM table.

4. **show tcam counts**

The above command is used to view TCAM information.

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Troubleshooting err-disable recovery

examguides.com/CCNP-Switch/ccnp-switching-3.htm

1. Layer2 Technologies

1.1 Configure and verify switch administration

1.1.c Troubleshoot Err-disable recovery:

Errdisable is a feature that automatically disables a port on a Cisco Catalyst switch. There are several reasons for which an administrator can configure ErrDisable on a switch port. These include the following:

1. Duplex Mismatch

2. Loopback Error

3. Link Flapping (up/down)

4. Port Security Violation

5. Unicast Flodding

6. UDLD Failure

7. Broadcast Storms

8. BPDU Guard

1. When a port is in error-disabled state, it is effectively shutdown and no traffic is sent or received on that port.

2. show interfaces command, the port status shows as Errdisabled.

3. To recover a port that is in an Errdisable state, manual intervention is required, and the administrator must access the switch and configure the specific port with 'shutdown' followed by the **'no shutdown'** command.

The error disabled feature is supported on most Catalyst switches running the Cisco IOS software. Including all the following models:

Catalyst 2940/2950/2960/2960S
Catalyst 3550/3560/3560-E/3750/3750-E
Catalyst 4000/4500/4507R
Catalyst 6000/6500

There are a number of reasons a port can enter the Errdisable state. One common reason is the Port Security error.

Of all the errors, Port Security is more a feature rather than an error. Port Security allows the restriction of MAC Addresses on an interface configured as a layer 2 port. This effectively prevents others connecting unwanted hubs or switches on the network. Port Security allows us to specify a single MAC Address to be connected to a specific port, thus restricting access to a specific computer. Some times, it is desirable to restart the switch port automatically after ErrDisabled. This is possible using ErrDisable recovery command as shown in the example below.

The following commands enable the autorecovery feature 30 seconds after a port security violation:

```
Switch(config)#errdisable recovery cause psecure-violation
Switch(config)#errdisable recovery interval 30
```

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : CDP And LLDP

examguides.com/CCNP-Switch/ccnp-switching-4.htm

1. Layer2 Technologies

1.2 Configure and verify Layer 2 protocols

1.2.a CDP and LLDP:

CDP : CDP, short for Cisco Discovery Protocol runs over Layer 2 (the data link layer) on all Cisco routers, bridges, access servers, and switches. CDP allows network management applications to discover Cisco devices that are neighbors of already known devices. CDP runs on all LAN and WAN media that support SubNetwork Access Protocol (SNAP). Cisco Discovery Protocol (CDP) is a protocol supported by Cisco devices and gives limited information about the devices and used for automatic discovery of Cisco networking components in a network.

The following are true about CDP:

1. CDP - Cisco Discovery Protocol is a Cisco proprietary Layer 2 protocol.

2. CDP uses a multicast packet to the common destination address 01-00-0c-cc-cc.

3. CDP packets are sent out with a non zero TTL after an interface is enabled and with a zero TTL value immediately before and interface is made idle. This enables the neighbouring devices to quickly discover the state of neighbours.

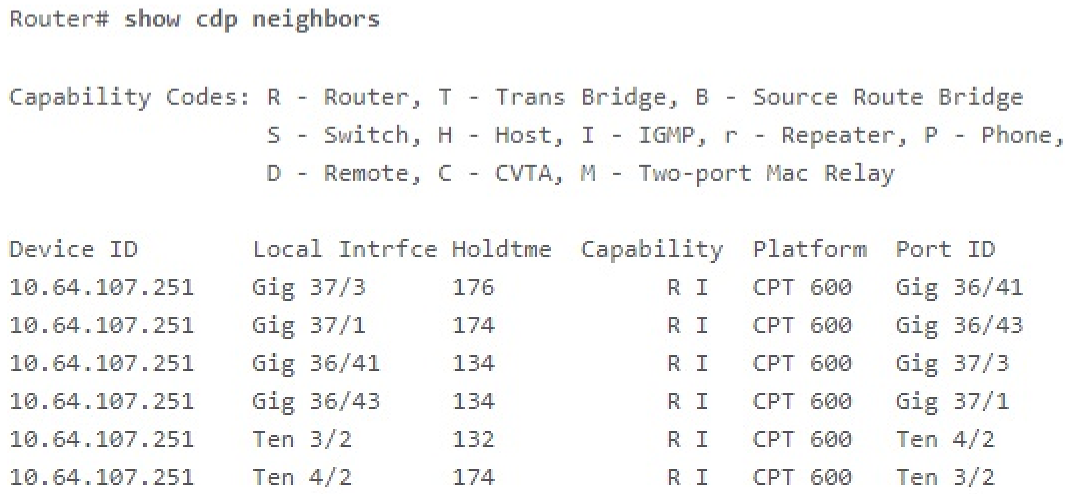
4. CDP packets will never be forwarded beyond the directly connected devices. To find CDP information on indirectly connected routers, administrators can "telnet" to the intended destination device and run CDP command.

The following command sets the cdp timer, holdtime

```
R1>enable
R1#configure terminal
R1(config)#cdp timer 30
R1(config)#cdp holdtime 90
```

The "**Show cdp interface**" command displays the status of all interfaces that are running cdp. For determining the neighbouring devices in a Cisco network, you can use the command "**show cdp neighbours**".

The following example is sample output from the show cdp neighbors command.



```
Router# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce Holdtme  Capability  Platform  Port ID
10.64.107.251    Gig 37/3      176            R I   CPT 600   Gig 36/41
10.64.107.251    Gig 37/1      174            R I   CPT 600   Gig 36/43
10.64.107.251    Gig 36/41     134            R I   CPT 600   Gig 37/3
10.64.107.251    Gig 36/43     134            R I   CPT 600   Gig 37/1
10.64.107.251    Ten 3/2       132            R I   CPT 600   Ten 4/2
10.64.107.251    Ten 4/2       174            R I   CPT 600   Ten 3/2
```

The Device ID column in the output indicates the remote node ID and the Port ID column indicates the remote port.

The command : **Switch#show cdp interface [<*type*> <*mod*>/<*num*>]**

Displays the CDP information pertaining to a specific interface.

The command : **Switch#show cdp neighbors [<*type*> <*mod*>/<*num*> | *vlan* <*vlan-id*>][*detail*]**

Displays the cdp information in detail, including the IP address for telnetting to the neighbor device.

LLDP : LLDP(Link Layer Discover Protocol) is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. LLDP like CDP, runs over the data-link layer of your network that includes a non Cisco devices or different network layer protocols.

LLDP supports a set of attributes that it uses to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors. Details such as configuration information, device capabilities, and device identity can be advertised using this protocol.

To globally disable LLDP the following command is used

Switch#configure terminal
Switch(config)#no lldp run

To globally enable lldp following command is used

Switch#configure terminal
Switch(config)#lldp run

clear lldp counters - Resets the traffic and error counters to zero.

clear lldp table - Deletes the LLDP table of information about neighbors.

show lldp - Displays global information, such as frequency of transmissions, the holdtime for packets being sent, and the delay time for LLDP to initialize on an interface.

show lldp entry entry-name - Displays information about a specific neighbor.

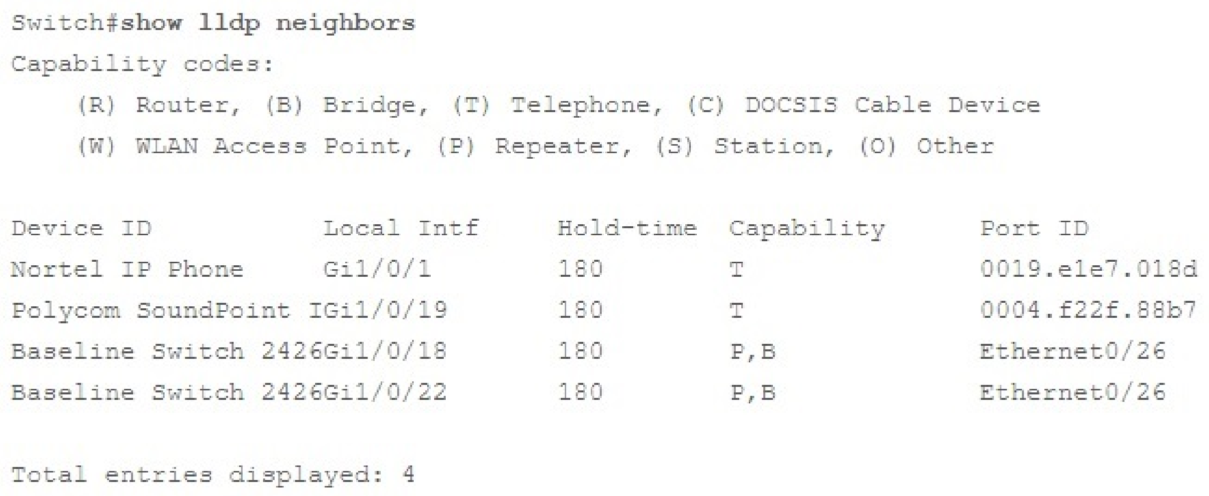
You can enter an asterisk (*) to display all neighbors, or you can enter the name of the neighbor about which you want information.

show lldp errors - Displays LLDP computational errors and overflows.

show lldp interface[interface-id] - Displays information about interfaces where LLDP is enabled. You can limit the display to the interface about which you want information.

show lldp neighbors - displays information about neighbors.

Typical output show lldp neighbors command output is shown below



```
Switch#show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
Nortel IP Phone     Gi1/0/1        180        T               0019.e1e7.018d
Polycom SoundPoint IGi1/0/19       180        T               0004.f22f.88b7
Baseline Switch 2426Gi1/0/18       180        P,B             Ethernet0/26
Baseline Switch 2426Gi1/0/22       180        P,B             Ethernet0/26

Total entries displayed: 4
```

show lldp neighbors[interface-id][detail] - Displays information about neighbors, including device type, interface type and number, holdtime settings, capabilities, and port ID.

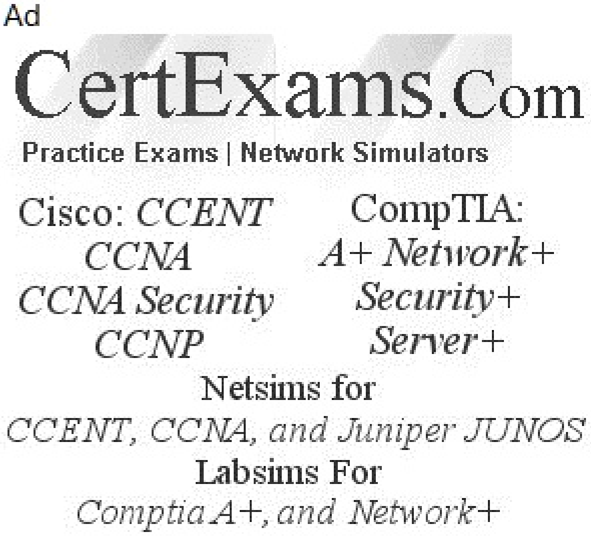
You can limit the display to neighbors of a specific interface or expand the display to provide more detailed information.

show lldp traffic - Displays LLDP counters, including the number of packets sent and received, number of packets discarded, and number of unrecognized TLVs.

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : UDLD

examguides.com/CCNP-Switch/ccnp-switching-5.htm



1. Layer2 Technologies

1.2 Configure and verify Layer 2 protocols

1.2.b UDLD:

UDLD(Unidirectional Link Detection): is a Cisco-proprietary layer two protocol devised to automatically detect the loss of bidirectional communication on a link monitors a port for bi-directional flow of data. This is done by sending Layer2 UDLD frames identifying the switch port at regular intervals.

The far-end port echos the frames with its own identification added. If UDLD does not receive the echos, the port is either flagged or disabled depending on the configuration. All connected devices must support UDLD in order for the protocol to successfully identify the unidirectional links.

Unidirectional Link Detection (UDLD): The UDLD protocol allows devices connected through media such as fiber-optic or twisted-pair Ethernet to monitor the physical configuration of the cables and detect when a unidirectional link exists. If a unidirectional link is detected, UDLD shuts down the affected port and send out an alert.

UDLD has two modes of operation.

1.Normal mode: Allows the port to operate even after detection of a uni-directional port. A syslog message is generated to alert the administrator.

2. Aggressive mode: Soon after a uni-directional port is detected, an attempt is made to verify the link. If the verification process fails, the link is immediately placed in errdisable state.

By default, UDLD is disabled on a switch. UDLD can be used either on interface basis or globally. To enable UDLD, use the following global configuration command:

Switch(config)# udld {aggressive | enable | message time *<seconds>***}**

Use "aggressive" keyword to enable "aggressive" mode.

Message time <seconds> can be set to any value between 7 seconds and 90 seconds. This is the time period that the switch port echos messages to the neighboring port to find whether the link is operation or not

Previous   Contents   Next

Cisco® CCNP Switch Exam Cram Notes : Configuring And Verifying VLANS

examguides.com/CCNP-Switch/ccnp-switching-6.htm

1. Layer2 Technologies

1.3 Configure and Verify VLANs

A VLAN is a group of devices on one or more logically segmented LANs. All devices working on a VLAN will have same broadcast domain. Like routers, switches (Layer 2) have the ability to provide domain broadcast segmentation called a VLAN. Using VLAN technology, you can group switch ports and their connected users into logically defined communities of interest. A VLAN operating on a Catalyst switch limits transmission of unicast, multicast, and broadcast traffic to only the other ports belonging to that VLAN, thereby controlling broadcasts.

To associate a switch with a management VLAN, you need to assign an IP address to the switch. The subnet portion of the switch IP address must match the subnet number of the management VLAN. Note that switches can maintain an IP stack, which enables us to manage the switches either locally, as well as remotely by Telnet.

Frame tagging is a technique used to uniquely identify a frame as it is forwarded through the switch fabric.

The benefits of VLANS include:

1. Easy Administration resulting in reduced administration costs,

2. Increased Security due to broadcast control, if you are using simple hub, you can observe traffic corresponding to any node by simply inserting a Network analyzer.

3. Grouping based on functional requirements irrespective of physical location of nodes, Simplify moves, adds, changes,

4. Distribution of traffic thereby using the network bandwidth more efficiently.

1. ISL: A Cisco proprietary trunking protocol, associated with Ethernet.. Supported by Catalyst switches and routers.

2. 802.1Q: This is an IEEE standard for the VLAN trunking protocols, associated with Ethernet. A VLAN identifier is inserted into the frame header, a technique called frame tagging.

3. 802.10: A Cisco proprietary method for transporting VLAN information inside the standard 802.10 FDDI frames.

4. LANE: LANE stands for LAN Emulation and is associated with ATM. This is an IEEE standard for transporting frames over ATM networks.

It is important to know the difference between a collision domain and a broadcast domain.

When you use Hubs, all the nodes connected to the hub will be in the same collision domain. However, when you use switches and implement VLANs, each VLAN will be in a separate broadcast domain. The packet forwarding between VLANs is achieved through the use of routing.

You use "**show vlan**" or "**show vlan vlan#**" command to see the configuration details of VLANs. The command "**sh vlan**" will display the configuration information for all VLANs, where as the command "**sh vlan vlan#**" shows only the configuration information pertaining to that vlan. For example, if you want to see the configuration information for vlan2, you give the command "**sh vlan 2**

Different types of VLAN

There are different types of VLANs, viz Native VLAN, Management VLAN, and Default VLAN which may be confusing. The terms are a little confusing. By default, all three are one and the same. VLAN 1 is the default and native VLAN that is used for management functions. However, you may change the native VLAN to some other number (from VLAN 1) for security reasons. Once the native VLAN is changed (to say, VLAN 2) the the management VLAN will be VLAN2. Note that native VLAN is not tagged. Different terms are as explained below:

1. Default VLAN: It is the the native VLAN that is used for management functions by default it is VLAN 1. However, you may change the native VLAN to any other number by using the following command:

```
(config-if)#switchport trunk native vlan 2
```

You may verify the native vlan using the show command:

```
(config-if)#do show interface f0/8 trunk
```

```
Port Mode Encapsulation Status Native vlan
Fa0/ on 802.1q other 2
```

The default VLAN is still VLAN 1.

2. Native VLAN: It is an untagged VLAN. Unttaged VLAN traffic does not have a .1q tag on trunk.

3. Management VLAN: it is the native vlan used for in-band management (SNMP trap source, syslog source interface, telnet, ssh access to a device). By default, VLAN 1 is management VLAN in Cisco switches.

4. Normal VLAN traffic: All normal VLAN traffic (other than native vlan) will have a VLAN tag (.1q tag) attached while traversing the trunk ports.

Note: Trunk ports send and receive tagged frames always. If an untagged frame is received they should ideally discard it, however .1q allows you to send untagged frames on a trunk link provided, your end devices (routers and switches) know which vlan they belong to.

Inter-Switch Link (ISL) is a Cisco proprietary VLAN trunking protocols, used for switched VLAN networks. ISL encapsulates the original Ethernet frame, and a VLAN-ID is inserted into the ISL header among several other fields.

The interface configuration command used to select the voice VLAN mode that will be used is given below:

switch(config-if)# switchport voice vlan {vlan-id | dot1p | untagged | none}

vlan-id: here the PC data is carried on native VLAN and the voice packets are carried on a separate voice vlan.

Dot1p: here the PC data is carried on native vlan and voice packets are carried on vlan 0.

Untagged: here both PC data and voice packets are carried on the native vlan. No separate voice vlan is required.

The default condition for every switch port is none, where a trunk is not used. All other modes, except "none" use special 802.1Q trunk.

Three parameters are required for defining an MST region. These are:

1. The region name

2. Configuration revision number

3. Instance to VLAN mappings

1. **Switch(config)# monitor session 1 source vlan 1 - 5 rx**

Sets up vlans 1 though 5 (receive traffic) for monitoring.

2. **Switch(config)# monitor session 1 destination interface gigabitethernet0/2**

Sets up destination interface to which the monitored traffic is mirrored.

3. **Switch(config)# monitor session 1 source vlan 10**

Vlan 10 is added to the monitored traffic.
Switch(config)#end

VLAN based SPAN allows VLAN be monitored instead of a simple physical port.

An SVI (Switched Virtual Interface) is used in multilayer switching. It has no physical significance. A vlan needs to be defined and assigned an ip address by using the commands:

```
Switch(config)# interface vlan <vlan-id>
Switch(config-if)# ip address <ip-address> <mask>
```

The first command defines a vlan given by the <vlan-id>. The second command assigns an IP address to the vlan. Here the SVI is represented physically by the specified vlan.

There are two common methods of VLAN Hopping

1. Switch Spoofing: A Switch Spoofing attack is used to exploit the network by configuring an end system (such as a work station) to mimic a switch. Here, the attacker emulates an ISL or 802.1q protocol, thus signaling with Dynamic Trunk Protocol signaling. If the attack is successful, the end system will have a membership across all VLANs. Thus the attacker may gain access to any network resource.

2. Double Tagging: Here, the attacker tags transmitted frames with double headers, both of which as 802.1q headers. This will allow the frames to be forwarded into the wrong VLAN. Double Tagging works because the first switch that the frames reach strips the first of the two 802.1q headers, and then forwards the frame with the second header destined for the victim VLAN.

Prevention: It can be avoided by disabling any unused switch ports and assigning them to a VLAN that is not being used. Explicitly disable DTP on all user ports to set them to non-trunking mode and/or force it to be an access port. To do this on a cisco switch, use the switchport nonegotiate and switchport mode access interface configuration commands.

End-to-end VLANs are typically implemented when the network traffic follows 80/20 rule. That is, 80% of the traffic is within the campus, and 20% is directed towards remote resources. The following are the important characteristics of end-to-end VLANs:

1. Users are grouped into a VLAN based on function, not location.

2. The user belongs to the same VLAN no matter where he plugs his PC into the network.

3. End-to-end VLANs are typically used for security reasons or resource requirements.

4. End-to-end VLANs are difficult to implement and troubleshoot. This is because the end-to-end VLAN spans across the enterprise, and identifying a problem node would be difficult.

The important characteristics of a Local VLANs compared to End-to-end VLAN are given below:

1. They are recommended where the traffic flow follows 20/80 rule, that is 80% of the user generated traffic is remote to the campus, and only 20% is local.

2. Local LANs are easy to maintain. Local LANs are typically confined to a floor or an area in a building and do not span several areas (or floors) in a building or campus.

3. Note that if a frame in a local VLAN needs to travel to another VLAN in the campus, a layer 3 device is required, which is resource intensive. Therefore, as the interVLAN traffic increases, you should consider End-to-end VLANs.

The following are the important characteristics of Dynamic VLANs and Static VLANs:

Static VLANs : which are also known as Port-based VLANs are created by manually assigning ports to a VLAN. When a device is connected to a port it automatically assumes the VLAN that the port is assigned to. If the user changes the port and still needs to access the same VLAN, the network administrator has to manually assign the access port on the switch to the VLAN. Static VLANs are generally used to reduce broadcast and to increase the security. Since static VLANs have a small administrative overhead and provide good security than traditional switches, they are widely used. Another strong point of static VLANs is the ability to control where the user moves within a large network. By assigning specific ports on the switches in the network, the network administrators can control access and limit the network resources that can be used by the users.

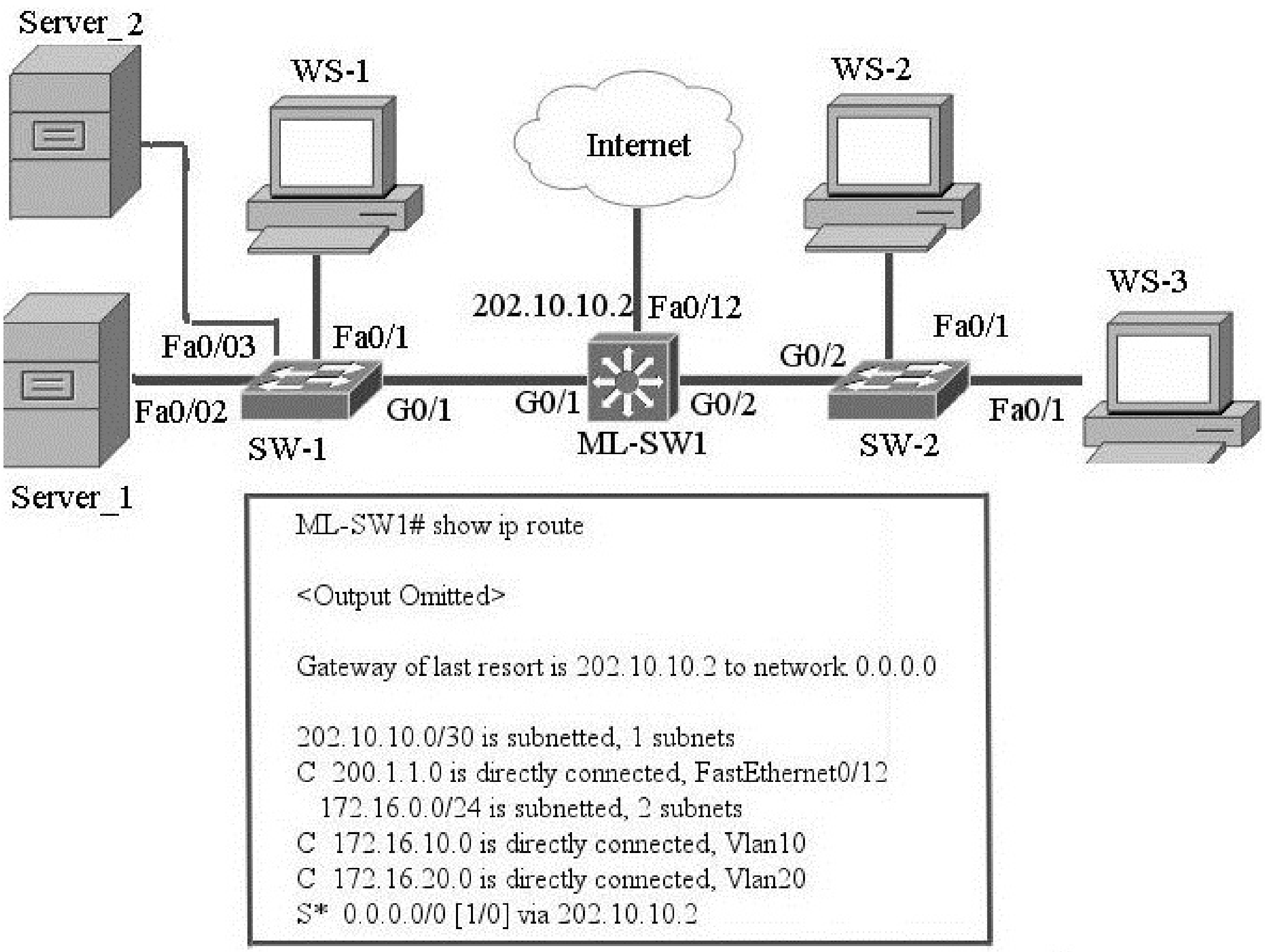
Dynamic VLANs : In dynamic VLANs the VLANs are assigned to switch ports using a centralized Policy Server. The policy server will have a mapping of Physical address (like MAC address) of a host to corresponding VLAN. The Policy Server will automatically assign the designated VLAN to the switch port after looking up into the VLAN-MAC address table. Therefore, even if a host is moved from one switch to another, the host will retain the same VLAN. However, dynamic VLANs are considered to be less secure than Static VLANs. For example, an attacker may spoof your Mac address over a wireless LAN and gain access to the company's network.

Static VLANs are also known as Port based VLANs. They are created by assigning ports on a switch to specific VLANs. Any host connected to a given port on a switch is automatically assigned the VLAN of the switch port. On the other hand, in dynamic VLANs, the VLANs are assigned to switch ports using a centralized Policy Server. The policy server will have a mapping of Physical address (like MAC address) of a host to corresponding VLAN. The Policy Server will automatically assign the designated VLAN to the switch port after looking up into the VLAN-MAC address table. Therefore, even if a host is moved from one switch to another, the host will retain the same VLAN. However, dynamic VLANs are considered to be less secure than Static VLANs. For example, an attacker may spoof your Mac address over a wireless LAN and gain access to the company's network.

When switch VLAN information is modified, the VTP configuration revision number and the configuration revision database number get modified.

For communicating between VLANs, you need a layer 3 device. Note that VLANs operate at Layer-2. When the access ports are configured with two distinct VLANs, the switch will not port the frames that belong to a different VLAN.

Example: Refer to the figure. VLAN10, VLAN20, and VLAN30 have been configured on the switch ML-SW1. Host computers are on VLAN 20 (172.16.20.0), servers are on VLAN 30 (172.16.30.0), and the management VLAN is on VLAN10 (172.16.10.0). Hosts are able to ping each other but are unable to communicate with the servers. What is the most likely problem?



```
ML-SW1# show ip route

<Output Omitted>

Gateway of last resort is 202.10.10.2 to network 0.0.0.0

202.10.10.0/30 is subnetted, 1 subnets
C  200.1.1.0 is directly connected, FastEthernet0/12
   172.16.0.0/24 is subnetted, 2 subnets
C  172.16.10.0 is directly connected, Vlan10
C  172.16.20.0 is directly connected, Vlan20
S*  0.0.0.0/0 [1/0] via 202.10.10.2
```

As per the exhibit, it appears that the VLAN IP address for VLAN 30 has not been configured. You need to configure the VLAN interfaces with the IP address as below:

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface Vlan30
Switch(config-if)#ip address 172.16.30.1 255.255.255.0
Switch(config-if)#no shutdown

Roaming between LAPs and autonomous APs is NOT supported. The reason is that, when connected to LWAPP APs, traffic is passed through an LWAPP tunnel. Since there is no mobility tunnel between the Wireless LAN Controller and the autonomous APs, the roam does not work.

When using light weight access point, all the traffic goes through Access Point, then through the Wireless Controller, and then back to Access Point, and then to the destination host. Wireless encryption can still be used to secure data over the air, as with traditional WLANs. However, the encrypted data does not pass through the LWAPP or CAPWAP tunnel at all. Packets are encrypted as they leave the wireless client and unencrypted when they arrive on the LAP. The same is true for packet authentication, if it is used.

One of the key principles behind the LWAPP and CAPWAP protocol architecture is that of a split 802.11 MAC (Media Access Control). Since the real processing power is implemented in controllers, most of the functions are performed in the controller instead of the access point. This concept is called "Split-MAC" by Cisco and most other controller-based vendors. The Lightweight Access Point is mainly limited to front-end activities. Even the rf power setting is usually done by the controller.

The Lightweight AP and Wireless Controller are linked by the LWAPP/CAPWAP protocol. The protocol uses a "control" channel (port 5246) for access point management, configuration, and control, and a "data" channel (port 5247) for forwarding of user traffic between the two entities. The control messages are sent securely over LWAPP control tunnel. The user data is not encoded or secured and sent via "data" channel.

The SSID needs to be consistent for a wireless client to roam between LWAPs that are managed by the same WLC. However, if the LAPs are managed by different WLCs, then the Mobility group must be same on the WLCs. A Mobility Group is a group of Wireless LAN Controllers (WLCs) in a network with the same Mobility Group name. These WLCs can dynamically share context and state of client devices, WLC loading information, and can also forward data traffic among them, which enables inter-controller wireless LAN roaming and controller redundancy. Note that the WLCs may be in the same or different IP subnet or VLAN. WLCs use what is known as Ether-IPtunnel to transfer User traffic from one WLC to another.

Assuming that a User (or Client) originally joined the WLAN on WLC1, WLC1 will always refer to itself as the User's anchor point. Any controller that is serving the User from a different subnet is known as a foreign agent. As the client continues to roam, the anchor WLC will follow its movement by shifting the Ether-IP tunnel to connect with the User's foreign WLC.

In order for a wireless client to seamlessly roam between mobility group members (WLCs), WLAN's SSID and security configuration must be configured identically across all WLCs comprising the mobility group

The following are true about LAP operation in sequential order:

1. LAP first learns it IP address from a DHCP server.

2. LAP obtains the IP address of WLC from a DHCP server, usually using Option 43 that provides a list of available WLCs. (Alternatively, you can assign WLC IP address statically on LAP using CLI.)

3. The LAP sends a join request to the first WLC from the list of IP addresses leaned from DHCP server. If that one fails to answer, the next WLC is tried. When a WLC accepts the LAP, it sends a join reply back to the LAP, resulting in a mutual binding between the two

devices.

4. The WLC compares the LAP's code image release with the one stored locally. If they differ, the LAP downloads the code image stored on the WLC and reboots itself.

5. The WLC and LAP build a secure LWAPP or CAPWAP tunnel for management traffic and wireless client data LAP client forms a LWAPP tunnel to the WLC. Therefore, the individual VLANs of the clients are not carried through the switch to the WLC. The proper configuration commands are:

1. **Switch(config-if)# switchport**
2. **Switch(config-if)# switchport access vlan 100**
3. **Switch(config-if)# switchport mode access**
4. **switch(config-if)# spanning-tree portfast**

ote that if Autonomous Access Point (instead of LAP), then it is required to configure the switch port as trunk port. This is because the VLANs are carried over the switch port to the distribution layer switch.

The switch interfaces feeding a WLC should be configured as trunk links. Some WLCs need a single interface, others have several interfaces that should be bundled into a single EtherChannel. The WLC shown in Figure has a four-interface Gigabit EtherChannel.

Note that we need to use the command "channel-group 1 mode on" because the WLC cannot negotiate an EtherChannel. Therefore, we cannot use other options like "desirable

This procedure for a LAP to register with a WLC is:

1. The LAP issues a DHCP request to a DHCP server in order to get an IP address, unless an assignment was made previously with a static IP address.

2. If Layer-2 LWAPP is supported on the LAP, the LAP broadcasts an LWAPP discovery message in a Layer-2 LWAPP frame. Any WLC that is connected to the network and that is configured for Layer-2 LWAPP mode responds with a Layer 2 discovery response. If the LAP does not support Layer 2 mode, or if the WLC or the LAP fails to receive an LWAPP discovery response to the Layer 2 LWAPP discovery message broadcast, the LAP proceeds to step 3.

3. If step 1 fails, or if the LAP or the WLC does not support Layer 2 LWAPP mode, the LAP attempts a Layer 3 LWAPP WLC discovery.

4. If step 3 fails, the LAP resets and returns to step 1

Here the client roams in the same subnet, known as layer-2 roaming. A layer-2 roam occurs when a WLAN client moves from one access point to another within the same subnet. If the client moves to a new access point on a different IP subnet, layer-3 roaming occurs. Roaming is always a client station decision and the client station is responsible for detecting, evaluating, and roaming to an alternative access point.

The following is the proper sequence of events that wireless client takes during the process of association with an accesspoint.

1. Client sends probe request

2. Access point sends probe response or beacon

3. Client initiates association process

4. Access point accepts association of the client

5. AP adds client's MAC address to association table

Unknown unicast flooding attack : To forward the incoming frames to the destination MAC address the switch looks up this address in the address table, hoping to find the switch port and VLAN where the destination address is attached. If it is found, the frame is forwarded out to the corresponding switch port. If the address is not found in the table, the switch must take more drastic action: The frame is flooded out to all switch ports assigned to the source VLAN. This is known as unknown unicast flooding , because the location of the unicast destination is unknown.

PoE Methods

Method	Name	Power Offered
Cisco Inline Power	ILP	7W
IEEE 802.3af	PoE	15.4W
IEEE 802.3at	PoE+	25.5W
Cisco Universal PoE	UPoE	60W

To telnet to a switch, the following are required:

1. Assignment of ip address and subnetmask to the management vlan,

2. Assignment of default gateway IP address.

The following are the typical steps in preparing a switch for telnet access:

```
Switch(config)# interface vlan <vlan-id>
Switch(config-if)# ip address <ip-address> <subnet-mask>
Switch(config-if)# ip default-gateway <ip-address>
Switch(config-if)# no shutdown
```

QoS: When frames (layer 2) carried from one switch boundary to another switch boundary, prioritization of traffic can be achieved by utilizing the Class of Service field (CoS) of the frame tag. For prioritization of traffic, both 802.1Q, and ISL provide a field to represent CoS of each frame. The value 0 of the CoS field indicates lowest priority, and the value 7 indicates the highest priority frame. CoS information is passed along ISL and 802.1Q trunks.

Traffic shaping is generally used for limiting the overall traffic. VOIP is a time sensitive traffic, and generic traffic shaping may not be suitable for VOIP traffic on a switch interface. Traffic policing is sensitive to the type of traffic (such as VOIP or any time critical traffic) and is suitable for use on a switch. GTS and AGTS are traffic shaping method used on Cisco routers.

Inline power is available on Catalyst 3550-24-PWR, Catalyst 4500, and Catalyst 6500 switches.

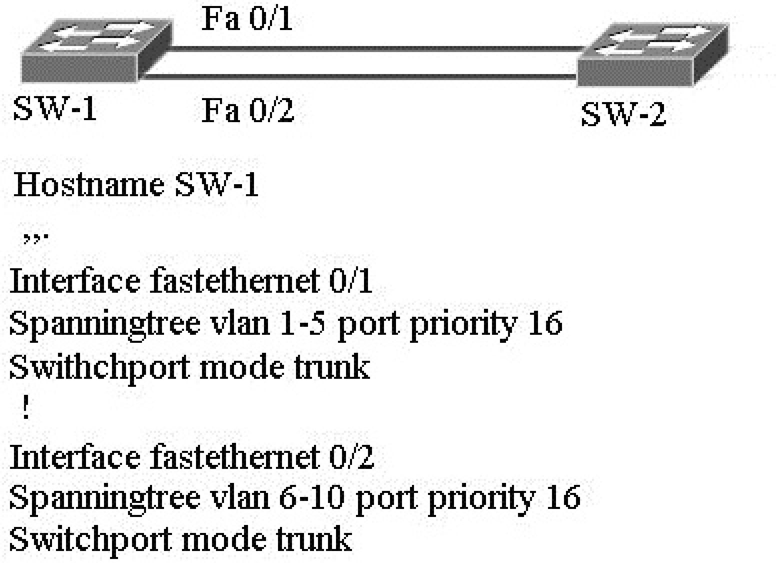
The trust boundary is an administrative boundary (normally used where external network interfaces). Here the CoS or DSCP values are either accepted or rejected based on the QoS restrictions of the switch interface.

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure such as Internet. Tunneling is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers.

Using the 802.1Q tunneling feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service-provider infrastructure even when they appear to be on the same VLAN. The 802.1Q tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy and tagging the tagged packets. A port configured to support 802.1Q tunneling is called a tunnel port. When you configure tunneling, you assign a tunnel port to a VLAN that is dedicated to tunneling.

Example: Given the partial configuration

As per the configuration, VLANs 1-5 are configured for port 0/1. Therefore, these VLANs will be transported on port 0/1. The other port will be in blocked state as far as these VLANs are concerned. On the otherhand, VLANs 6-10 are configured for port 0/2. Therefore, the traffic on these VLANs will be carried through port 0/2. The other port, port 0/10 will be in blocked state as far as VLANs 6-10 are concerned. In the event of a failure to the active port, the blocked port will become active and all the traffic will be carried on that port. Note that the default port priority is 128. By setting a value of 16, the port is given higher priority (lower value=higher port priority) for given VLANs, whereas other VLANs will still be set with default port priority (128).

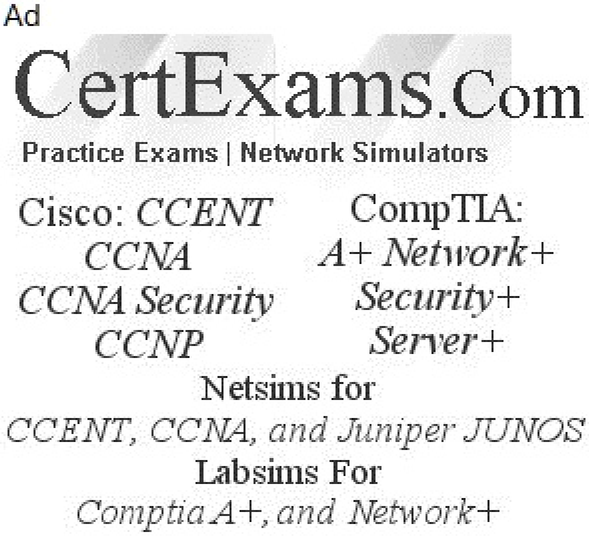


```
Hostname SW-1
 ,,.
Interface fastethernet 0/1
Spanningtree vlan 1-5 port priority 16
Swithchport mode trunk
 !
Interface fastethernet 0/2
Spanningtree vlan 6-10 port priority 16
Switchport mode trunk
```

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Configuring And Verifying Trunking

examguides.com/CCNP-Switch/ccnp-switching-7.htm



1. Layer2 Technologies

1.4 Configure and verify trunking

VLAN Trunk Protocol (VTP) is a layer 2 protocol that maintains VLAN configurations through a common administrative domain. Configurations are made to a VTP server, and are propagated across trunk lines to all switches in the VTP domain. VTP provides auto-intelligence for configuring switches across the network. VTP is a Layer 2 messaging protocol. It carries configuration information throughout a single domain.

VTP operates in one of three modes:

1. Server mode: VTP Servers can create, modify, or delete VLANs and other configuration parameters for the specified VLAN domain.

2. Client mode: A VTP client can't create, change, or delete VLANs.

3. Transparent mode : A VTP transparent mode is used when a switch is not required to participate in VTP, but only pass the information to other switches. Transparent switches don't work either as Server or clients.

4. Configurations made to a single switch, called VTP server, are propagated across the switch fabric under a single domain control. Other switches, configured as VTP clients, learn the configuration information from the server. It is important to know that, Cisco switches such as Catalyst 1900, acting as VTP servers save the VLAN configuration information in their Non volatile memory (NVRAM), whereas client keep the information only in running configuration.

A VTP advertisement necessarily consists of "Configuration revision number". Every time a VTP server updates its VLAN information, it increments the configuration revision number by one count. VTP clients, use the revision number to enforce the VLAN configuration Update

There are two different VTP versions. VTP version 1 and VTP version 2. These versions are not interoperable. Version 1 is the default version. All switches in a given management domain should be configured in either version 1 or version 2.

Some of the advantages of VTP version 2 are as below:

1. Token Ring support: Supports Token Ring LAN switching and VLANs. If Token Ring is used, this is the version required.

2. Version number auto propagation: In case that all switches are capable of running Version 2, only one switch need to be Version 2 enabled, Version number is automatically propagated to others.

The command syntax for assigning a management domain for a switch is:

Switch# vtp domain *<domain-name>*

For example, if the domain name is newyork, the command is:

Switch# vtp domain *newyork*

You need to create a domain while configuring the first switch in a switch network. For subsequent switches, you only need to join the existing domain. The password is required if the domain need to be secured by a password. The command allows you to create a new domain (in case the first switch is being configured) or to join an existing domain (one or more switches have already been assigned a domain).

VTP pruning is a technique that enhances the available network bandwidth by reducing the broadcast, multicast, and flooded unicast messages. These frames are not forwarded to network devices that don't have ports associated with a given VLAN. When VTP pruning is enabled, a switch forwards the flooded traffic across a link to another switch, only if that switch has ports associated with that VLAN. For example, a switch, Switch A sends flooded messages (say belonging to VLAN 7) to Switch B, only if Switch B has ports associated with VLAN 7.

VTP pruning should only be enabled on VTP servers, all the clients in the VTP domain will automatically enable VTP pruning. By default, VLANs 2 - 1001 are pruning eligible, but VLAN 1 can't be pruned because it's an administrative VLAN. Both VTP versions 1 and 2 support pruning.

Domain name set on a switch can be known by viewing the VTP Configuration of the switch, so use "show vtp status" command to check the domain name.

The following points may be noted with respect to IP Phone and switch port:

1. The trunk between the IP phone and switch port is created dynamically.

2. The trunk between the IP phone and switch port can contain only two VLANs, a voice VLAN and the native VLAN.

3. A special trunk is negotiated through DTP and CDP between IP phone and the switch port.

4. By default, a switch port connected to an IP phone does not use a trunk. If you want to configure a trunk, use "switchport vlice vlan" command in the interface configuration mode.

5. The switch instructs an attached IP Phone through CDP messages as to how it should extend QoS trust to its PC data switch port

6. By default, a switch instructs an attached IP Phone not to trust the PC port. CoS values are overwritten to 0.

The following are important commands that can be used for troubleshooting IP Phone connectivity and configuration:

1. show cdp neighbors
2. show interface <type> <mod/<num> switchport
3. show mls qos interface <type> <mod>/<num>
4. show interface <type> <mod>/<num> capabilities
5. show mls qos interface queueing

A trunk link can be negotiated between two switches only if both switches belong to the same VLAN Trunking Protocol (VTP) management domain or, if one or both switches have not defined their VTP domain (that is, the NULL domain). If the two switches are in different VTP domains and trunking is desired between them, you must set the trunk links to ON mode or no-negotiate mode. This setting forces the trunk to be established.

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 for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN will be forwarding traffic for that VLAN. So, by ensuring that the port priorities are set differently for different VLANs, we can share the load on redundant links between two switches. The port priority is assigned using a 4-bit value. The priorities are now assigned in increments of 16 up to 256. Note that older standards used to have 8 bits for port priority, making it possible to have values ranging from 0 to 256. The new standard can take any value in multiples of 16, up to 256 and enables backward compatibility. The default port priority is 128, maximum possible value 256. Lower the value, higher the port priority. A port with a priority value of 16 is more preferred to one with a value of 32.

VTP advertisements may come from a VTP server or a VTP client. These are as given below

Summary Advertisements: These are sent by VTP domain servers every 5 minutes or every time the VLAN topology changes, It contains information about the management domain (VTP version, domain name, configuration revision number, timestamp, MD5 encryption hash code, and number of subset advertisements incoming). When there is a configuration change, summary advertisements are complimented by or more subset advertisements.

Subset advertisements: These are sent out by VTP domain servers after a configuration change. They list the specifics of the change (VLAN creation / deletion / suspension / activation / name change / MTU change) and the VLAN parameters (VLAN status, VLAN type, MTU, VLAN name, VLAN number, SAID value).

Advertisement Requests from Clients: VTP clients request specific VLAN information at times (say, Client switch is reset, or VTP domain name change) so they can be responded by summary and subset advertisements.

VTP Join message: It contains VTP domain name, and a VLAN bit string. If the bit is set, flood traffic for that VLAN should be received on that trunk. Each trunk port maintains a state variable per VLAN - Joined/Pruned.

By default, VLAN 1 is the native VLAN. Frames in the native VLAN are not tagged when sent over the Trunk port. Apart from native VLAN, all other VLAN frames sent over the Trunk port are tagged. You can change the native VLAN number from 1 to any other by manually configuring the same.

For Inter VLAN communication, you need a router or a Layer-3 switch.

Dynamic Trunking Protocol (DTP) is the Cisco-proprietary that actively attempts to negotiate a trunk link between two switches. Below is the switchport modes (or DTP modes) for easy reference:

1. Dynamic Auto: Creates the trunk based on the DTP request from the neighboring switch.

2. Dynamic Desirable: Communicates to the neighboring switch via DTP that the interface would like to become a trunk if the neighboring switch interface is able to become a trunk.

3. Trunk: Automatically enables trunking regardless of the state of the neighboring switch and regardless of any DTP requests sent from the neighboring switch.

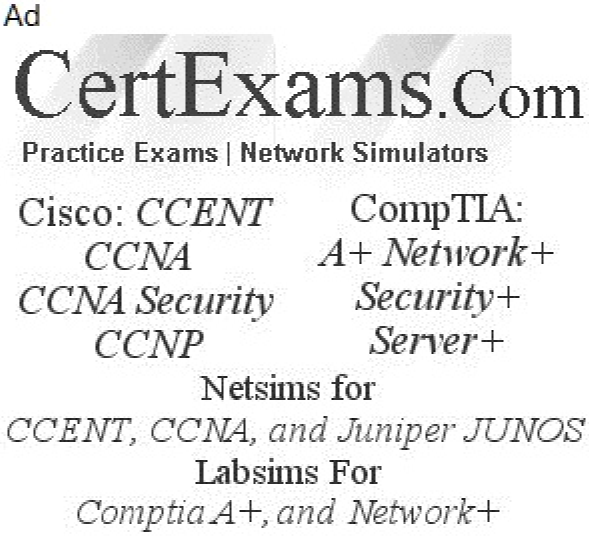
4. Access: Trunking is not allowed on this port regardless of the state of the neighboring switch interface and regardless of any DTP requests sent from the neighboring switch.

5. Nonegotiate: Prevents the interface from generating DTP frames. This command can be used only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Configuring And Verifying Etherchannels

examguides.com/CCNP-Switch/ccnp-switching-8.htm



1. Layer2 Technologies

1.5 Configure and Verify Etherchannels

Two protocols, namely PAgP or LACP may used for negotiating EtherChannel and Link Aggregation. We can configure Etherchannel in three ways in Cisco Switches.

1. Port Aggregation Protocol (PAgP) - Cisco Proprietary protocol

2. IEEE Link Aggregation Protocol (LACP) - Industry Standard

3. Manual Etherchannel Configuration - Without using any negotiation protocol listed above

PAgP : PAgP stands for Port Aggregation Protocol. PAgP helps in the automatic creation of Fast EtherChannel links. PagP is a Cisco proprietary link aggregation protocol used in Catalyst switches.

The following are features of Fast EtherChannel that is running PAgP (Port Aggregation Protocol):

1. PAgP helps in the automatic creation of Fast EtherChannel.

2. PAgP does not group ports configured for dynamic VLANs. PAgP requires that all ports in a channel must belong to the same VLAN or should be configured as trunk ports.

3. PAgP does not group ports that work at different speeds or port duplexes.

The following are available PAgP modes and the corresponding action:

1. ON mode does not send or receive PAgP packets. Therefore, both ends should be set to ON mode to form an EtherChannel.

2. Desirable mode tries to ask the other end in order to bring up the EtherChannel.

3. Auto mode participates in the EtherChannel only if the far end asks for participation. Two switches in auto mode will not form an EtherChannel.

If you are using Port Aggregation Protocol (PAgP) for EtherChannel negotiation, EtherChannel will be formed only if two ends are configured under following modes.

	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

EtherChannel can support from 2 to 8 links to be bundled into one logical link. Therefore, if Gigabit Ethernet links are bundled, 8 links represent 8 Gbps of one-way bandwidth, and 16 Gbps for full-duplex operation.

The load distribution algorithm in EtherChannel can use source IP, destination IP, a combination of source and destination IPs, Source MAC, destination MAC, or TCP.UDP port numbers for decision process. If there are only two links in the EtherChannel, only 1 bit in the IP are required. If there are 4 links in the EtherChannel, 2 bits are required. Similarly, for an 8 link EtherChannel, 3 bits are required.

LACP: Link Aggregation Control Protocol (LACP) is a standards based protocol and conforms to IEEE standard 802.3ad. Note that PAgP is Cisco proprietary protocol. If your network consists of both Cisco and non-Cisco devices, LACP is the desired option for configuring EtherChannel. If your network consists of all Cisco switches then PAgP would be recommended.

1. Active: The active end of the group sends out a LACP frame and initiates the negotiation to form the EtherChannel. Both ends could be active and the result would be the same.

2. Passive: Passive Mode does not initiate the negotiation. It just responds to LACP packets initiated by other end. So if both ends were passive, the EtherChannel would not be formed.

Passive Mode in Link Aggregation Control Protocol (LACP) does not start Link Aggregation Control Protocol (LACP) packet negotiation.

	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

EtherChannel can support from 2 to 8 links to be bundled into one logical link. Therefore, if Gigabit Ethernet links are bundled, 8 links represents 8 Gbps of one-way bandwidth, and 16 Gbps for full-duplex operation.

The load distribution algorithm in EtherChannel can use source IP, destination IP, a combination of source and destination IPs, Source MAC, destination MAC, or TCP,UDP port numbers for decision process. If there are only two links in the EtherChannel, only 1 bit in the IP are required. If there are 4 links in the EtherChannel, 2 bits are required. An XOR on 2 bits can have 4 possible outcomes. Similarly, for an 8 link EtherChannel, 3 bits are required. Conventionally, rightmost bits are always used for XOR operation.

The command : **switch# show etherchannel port**

can be used for verifying the channel negotiation mode of an EtherChannel.

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Configuring And Verifying Spanning Tree

examguides.com/CCNP-Switch/ccnp-switching-9.htm

1. Layer2 Technologies

1.6 Configure and Verify Spanning Tree

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on bridges and switches. The specification for STP is IEEE 802.1D. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network.

STP is necessary where you want redundant links, but not loops. Redundant links are as important as backups in the case of a failover in a network. A failure of your primary activates the backup links so that users can continue to use the network. Without STP on the bridges and switches, such a failure can result in a loop.

Note that there are different flavors of STP such as plain STP (802.1D), PVST+ (Cisco), RSTP (802.1w), Rapic PVST+ (Cisco) etc. Ensure that they are compatible and provide optimal performance when selecting a one or more flavors of STP.

During the process of Spanning-Tree Algorithm execution, some redundant ports need to be blocked. This is required to avoid bridging loops. To choose which port to use for forwarding frames, and which port to block.

The following three components are used by the Spanning-Tree Protocol:

1. Path Cost: The port with lowest path cost is placed in the forwarding mode. Other ports are placed in blocking mode.

2. Bridge ID: If the path costs are equal, then the bridge ID is used to determine which port should forward. The port with the lowest Bridge ID is elected to forward, and all other ports are blocked

3. Port ID: If the path cost and bridge ID are equal, the Port ID is used to elect the forwarding port. The lowest port ID is chosen to forward. This type of situation may arise when there are parallel links, used for redundancy.

A switch, participating in Spanning-Tree protocol, passes through the following states:

1. Blocked state: This is the initial state. All ports are put in a blocked state to prevent bridging loops.

2. Listen state: This is the second state of switch ports. Here all the ports are put in listen mode. The port can listen to frames but can't send. The period of time that a switch takes to listen is set by "fwd delay" .

3. Learn state: Learn state comes after Listen state. The only difference is that the port can add information that it has learned to its address table. The period of time that a switch takes to learn is set by "fwd delay".

4. Forward state: A port can send and receive data in this state. Before placing a port in forwarding state, Spanning-Tree Protocol ensures that there are no redundant paths or loops.

5. Disabled state: This is the state when the switch port is disabled. A switch port may be disabled due to administrative reasons or due to switch specific problems

The bridge ID consists of the following:

1. 2-byte priority: The default value on Cisco switches is 0X8000 (32,768), lower the priority, higher the chances of becoming a root bridge.

2. MAC address: The 6 byte MAC address of the bridge. Lower the MAC address, higher the chances of becoming a root bridge.

Note that, the bridge (or switch) with lowest value of 2-byte priority will become the root bridge. If the priority value is same, then the bridge with lowest value of 6-byte MAC address will become the root bridge.

The following methods are used for implementing Spanning-Tree in a VLAN environment:

1. PVST (Per VLAN Spanning Tree): This is a Cisco proprietary method. Requires Cisco ISL encapsulation. Separate instances of Spanning-Tree are for every VLAN.

2. CST (Common Spanning Tree): This is supported by IEEE802.1Q. Here, A single instance of Spanning Tree runs for all VLANs. BPDU information is exchanged on VLAN1

3. PVST+ (Per VLAN Spanning Tree Plus): This is also a Cisco proprietary method for implementing STP in VLAN environment.

PVST+ is available with Catalyst 4.1 release or above. Switches before release 4.1 are compatible with PVST implementation of Spanning-Tree. Note that PVST+ is backward compatible. PVST+ is also compatible with 802.1Q implementation of CST (Common Spanning Tree) protocol. PVST+ is in fact requires no configuration to make it compatible with PVST (Plug and play compatible).

To configure Rapid Spanning Tree Protocol (RSTP) on an edge port, use the command

Switch(config-if)#spanning-tree portfast.

To enable Multiple Spanning Tree (MST) on a switch, use the command

Switch(config)#spanning-tree mode mst

To enter MST configuration mode on a switch, use the command

Switch(config)#spanning-tree mst configuration

RSTP defines port states according to what the port does with the incoming frames. The allowed port states are as given below:

a. Discarding: The incoming frames are discarded. No MAC addresses are learned.

b. Learning: The incoming frames are dropped, but MAC addresses are learned.

c. Forwarding: The incoming frames are forwarded according to the learned MAC addresses.

The following are true about protected STP topology using Cisco switches:

1. When using **"root guard"** feature, a switch port blocks all superior BPDUs, or the ones with better bridge ID. No data can be sent or received through the port that is blocking any such BDPUs.

2. bpduguard is recommended to be enabled where PortFast is enabled. This is normally done on access layer switches, where the end user systems are connected.

3. True, a port configured with BPDU guard is put into errdisable state when a BPDU is received.

4. BPDU guard is recommended on switch ports with PortFast already enabled.

If you have enabled STP protection features, the following command lists the ports that have been labeled as having inconsistent state:

show spanning-tree inconsistentports

The following command enables you to look at reasons for inconsistencies:

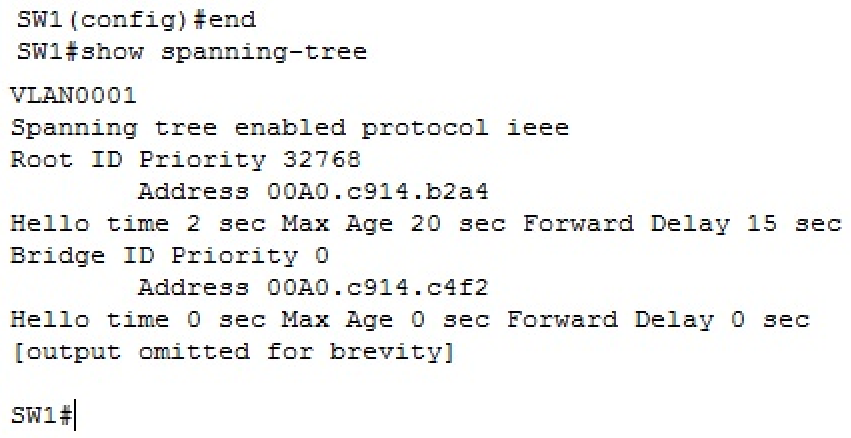
show spanning-tree interface *<type> <mod>/<num>* **[detail]**

During the process of Spanning-Tree Protocol execution, Root switch (say, switch A) is elected first. Next, the switch closest to the root switch is selected. This switch is known as Designated switch or Parent switch (say switch B). The frames are forwarded to the root switch(A) through the designated switch(B). Now the lowest cost port on the switch(say switch C) is selected. This is known as the Root port. Here, switch B is the designated switch for switch C and switch A is known as the root switch for switch C. Note that switch C is connected to the root switch (A) through its designated switch (B).

The command **"show spanningtree"** includes information about the following:

1. VALN number
2. Root bridge priority, MAC address
3. Bridge timers (Max Age, Hello Time, Forward Delay)

The following is the sample output of the "show spanning-tree" command



```
SW1(config)#end
SW1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32768
        Address 00A0.c914.b2a4
Hello time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 0
        Address 00A0.c914.c4f2
Hello time 0 sec Max Age 0 sec Forward Delay 0 sec
[output omitted for brevity]

SW1#
```

PVST (Per VLAN Spanning Tree) implementation has one instance of STP running for each VLAN. Therefore, when there are 32 VLANs in the bridge network, there will be 32 instances of STP running. Also, each VLAN has a unique root, path cost etc. corresponding to that VLAN.

PVST+ implementation of Spanning-Tree interoperates with 802.1Q compliant switches, that are using Common Spanning Tree (CST) protocol.

The three different types of SPAN are:

1. Local SPAN: The SPAN source and destination are located on the local switch.

2. Remote SPAN: The SPAN source and destination are located on different switches.

3. VLAN based SPAN: Here the source is a VLAN instead of a port.

Rapid Spanning Tree Protocol (RSTP) is based on the IEEE standard 802.1w. The standard has evolved from its predecessor 802.1D. 802.1w has the advantage of faster convergence over 802.1D.

1. 802.1D: This is a Spanning Tree Protocol (STP) that provides loop free switched or bridged network. Topology changes are made dynamically.

2. 802.1Q: The IEEE 802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information.

3. 802.1w: This standard is developed subsequent to 802.1D and offers faster convergence. 802.1w is known as Rapid Spanning Tree Protocol (RSTP).

4. 802.1s: IEEE 802.1s standard represents Multiple Spanning Tree protocol.

The following statements are true:

- Cisco's implementation of Multiple Spanning Tree (MST) supports 16 instances of STP.
- MST is interoperable with PVST+
- The use of MST does not eliminate the need for CST.
- Rapid Spanning Tree Protocol (RSTP) goes through what is known as synchronization during convergence

Two switch features available with Cisco switches for preventing un-intentional BPDUs are:

a. root guard: When configured at the interface level, BPDU Guard shuts the port down as soon as the port receives a superior BPDU. By default, it is disabled on all switch ports. To enable root guard, use the command:

switch(config-if)#spanning-tree guard root

If the superior BPDUs are no more received, the port is restarts the normal STP states to return to normal use.

b. bpdu guard: Here if any BPDU (superior or not) is received on a port configured with BPDU guard, the port is immediately put into errdisable state. The port is effectively shutdown and it must either be enabled manually or by use of a timeout function. By default, it is disabled on all ports. To enable BPDU guard use the command at interface configuration mode:

switch(config-if)#spanning-tree bpduguard enable

A port that is shutdown will continue to be in errdisable state even if the BPDUs are no longer received. It is recommended to use bpdu guard on all ports that have portfast enabled. The protection is useful for access layer nodes where the end user computers are expected to be connected.

The following STP features are useful in preventing mis-behaviour of STP due to sudden loss of BPDUs:

a. BPDU skew detection: It measures the amount of time that elapses from the expected time of arrival of a BDPU to the actual time of arrival of the BDPU. The arrival skew time condition is reported via syslog messages.

b. Loop guard: The loop guard is intended to provide additional protection against L2 forwarding loops (STP loops). For example, an STP loop is created when a blocking port in a redundant topology erroneously transitions to forwarding state. The loop guard needs to be enabled on the non-designated ports to effectively prevent STP loops. Non-designated ports are the root port, alternate root ports, and ports that are normally blocking. The command used to enable loop guard is:

Switch(config-if)# spanning-tree guard loop

The command is used at port level, loop guard is disabled by default on all switch ports.

Unidirectional Link Detection (UDLD) - The UDLD protocol allows devices connected through media such as fiber-optic or twisted-pair Ethernet to monitor the physical configuration of the cables and detect when a unidirectional link exists. If a unidirectional link is detected, UDLD shuts down the affected port and send out an alert.

UDLD has two modes of operation.

1. Normal mode: Allows the port to operate even after detection of a uni-directional port. A syslog message is generated to alert the administrator.

2. Aggressive mode: Soon after a uni-directional port is detected, an attempt is made to verify the link. If the verification process fails, the link is immediately placed in errdisable state.

By default, UDLD is disabled on a switch. UDLD can be used either on interface basis or globally. To enable UDLD, use the following global configuration command:

Switch(config)#udld *{aggressive | enable | message time <seconds>}*

Use "aggressive" keyword to enable "aggressive" mode.

Message time <seconds> can be set to any value between 7 seconds and 90 seconds. This is the time period that the switch port echos messages to the neighboring port to find whether the link is operation or not

There are two different ways of protecting against bad or unexpected BPDUs:

1. Root Guard, and

2. BPDU Guard

There are three ways of protecting against sudden loss of BPDUs:

1. BPDU Skew Detection

2. Loop Guard

3. UDLD

1. Root Guard -When configured at the interface level, BPDU Guard shuts the port down as soon as the port receives a superior BPDU.

2. BPDU Guard: Here if any BPDU (superior or not) is received on a port configured with BPDU guard, the port is immediately put into errdisable state. The port is effectively shutdown.

3. BPDU Skew Detection -It measures the amount of time that elapses from the expected time of arrival of a BDPU to the actual time of arrival of the BDPU. The arrival skew time condition is reported via syslog messages.

4. Loop Guard - The loop guard is intended to provide additional protection against L2 forwarding loops (STP loops). For example, an STP loop is created when a blocking port in a redundant topology erroneously transitions to forwarding state. The loop guard needs to be enabled on the non-designated ports to effectively prevent STP loops. Non-designated ports are the root port, alternate root ports, and ports that are normally blocking.

5. Unidirectional Link Detection (UDLD) - The UDLD protocol allows devices connected through media such as fiber-optic or twisted-pair Ethernet to monitor the physical configuration of the cables and detect when a unidirectional link exists. If a unidirectional link is detected, UDLD shuts down the affected port and send out an alert.

The STP ensures that timers are set on a switch, so that the bridging loops are avoided and the network is stable. Default timer values are as below:

Hello time: 2 seconds
Maximum time (max age): 20 seconds
Forward delay (fwd delay): 15 seconds.

These default values are assigned based on the assumption that the switch diameter is 7. The diameter can have values from 2 to 7. Diameter is measured from the root bridge (including root bridge) to the destination bridge. Each bridge increments the diameter by one count.

STP is enabled on every port on Cisco switches, by default. It is preferred to leave it enabled, so that bridging loops don't occur.

STP can be disabled selectively on any specific port by issuing the command:

Switch (enable) set spantree disable *<mod-number>/<port-number>*

Ex: **Switch (enable) set spantree disable** *2/4*

The above command disables STP on port 4 of module 2.

The advantages of Common Spanning Tree (CST) approach to VLAN implementation are fewer BPDUs and less processing overhead. Remember that in PVST, each VLAN has a separate instance of STP running.

The disadvantages of CST implementation are sub-optimal root bridge (since there will be only one root bridge for all VLANs, which may not be place optimally for some VLANs), and possibly, longer convergence times.

STP UplinkFast is most suitable for use with access layer switches. This feature is not supported in Core layer switches like 8500 series switches.

The following are true about Rapid Spanning Tree Protocol:

1. RSTP uses 802.1D BDPU format to provide backward compatibility. However, the BDPU version is set to 2 to distinguish RSTP BDPU from 802.1D BDPUs.

2. A switch running RSTP can detect a neighbor failure in three Hello intervals or 6 seconds. This is much shorter than the normal 20 seconds max age used for 802.1D.

3. RSTP uses "Root Bridge" in the same manner as that of 802.1D STP.

4. If a switch running RSTP receives and 802.1D BDPU, the switch begins to use 802.1D rules on that port.

To configure Rapid Spanning Tree Protocol (RSTP) on an edge port, use the command

Switch(config-if)#spanning-tree portfast

To enable Multiple Spanning Tree (MST) on a switch, use the command

Switch(config)#spanning-tree mode mst

To enter MST configuration mode on a switch, use the command

Switch(config)#spanning-tree mst configuration

- The instance 0 of MST corresponds to Internal Spanning Tree (IST).
- By default all VLANs within an MST region belong to IST
- MST and PVST+ are interoperable.
- IST of MST corresponds to CST of 802.1Q

The following are important commands that you need to know:

To display the UDLD status on one or all ports :

Show udld *[type <mod>/<num>]*

To re-enable port that UDLD aggressive mode has errdisabled

udld reset

PVST+ is based on IEEE802.1D standard and includes Cisco proprietary extensions such as BackboneFast, UplinkFast, and PortFast.

Cisco's Rapid-PVST+ is based on IEEE 802.1w (RSTP) standard and has a faster convergence than 802.1D.

Cisco's STP Implementations: PVST, PVST+
Cisco's RSTP Implementation: RPVST+
Rapid-PVST+ is backward compatible with PVST+.

RSTP is able to interoperate with legacy STP protocols. However, it is important to note that the inherent fast convergence benefits of 802.1w are lost when it interacts with legacy bridges.

The primary advantage of MST over RSTP (or Cisco's PVSTP+) is that it requires less number of Spanning Tree instances running on a switch network. Several VLANs can be grouped and assigned to an MST instance. Cisco supports a maximum of 16 MSTIs in each region. IST always exists as MSTI number 0, leaving MSTI 1 through 15 available for use. MST must be manually configured on the all switches using CLI or SNMP.

IEEE 802.1s MST: MST extends the IEEE 802.1w Rapid Spanning Tree (RST) algorithm to multiple spanning trees. The advantages of using MST are: 1. Reduced processor load, improved convergence. MST is backward compatible with 802.1D STP, 802.1w (rapid spanning tree protocol [RSTP).

- All switches in the same MST regison must have the same VLAN-to-instance mapping to exchange VLAN information.

- You need to configure region name, revision number, and VLAN-to-instance mapping on each switch running MST. On enablingMST, all VLANs are mapped to instance 0 by default, MST (802.1s) uses a modified version of RSTP (802.1w). This modified version is incorporated inside of MST and provides a fast convergence time in case of a failure in the network. Note that RSTP that gets enabled with MST is different from Cisco's PVSTP+. The UplinkFast, BackboneFast, and cross-stack UplinkFast features are not supported with the RSTP and MSTP.

There are three different types of Switch Port Analyzers:

1. Local SPAN: Mirrors traffic from one or more interface on the switch to one or more interfaces on the same switch

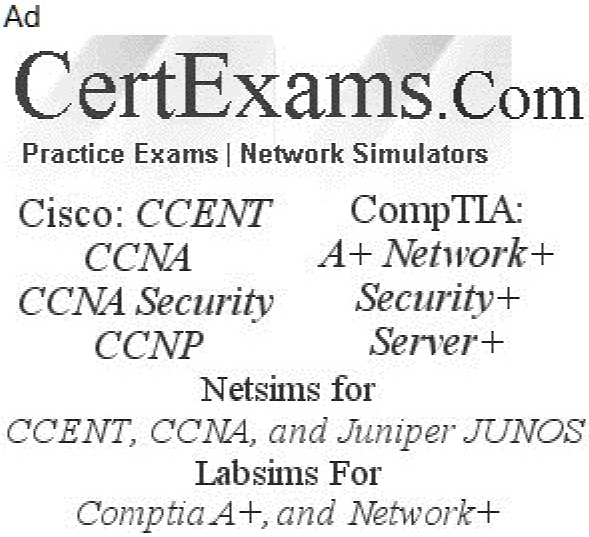
2. Remote SPAN (or RSPAN): RSPAN allows you to monitor traffic from source ports distributed over multiple switches, which means that you can centralize your network capture devices. RSPAN works by mirroring the traffic from the source ports of an RSPAN session onto a VLAN that is dedicated for the RSPAN session. This VLAN is then trunked to other switches, allowing the RSPAN session traffic to be transported across multiple switches. The destination session collects all RSPAN VLAN traffic and sends it out the RSPAN destination port.

3. Encapsulated remote SPAN (ERSPAN): encapsulated Remote SPAN (ERSPAN), as the name says, brings generic routing encapsulation (GRE) for all captured traffic and allows it to be extended across Layer 3 domains. ERSPAN is a Cisco proprietary feature

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Describing Chassis Virtualization And Aggregation Technologies

examguides.com/CCNP-Switch/ccnp-switching-10.htm



1. Layer2 Technologies

1.7 Describe chassis virtualization and aggregation technologies

1.7.a Stackwise:

In Cisco StackWise technology, individual switches intelligently join to create a single switching unit. Configuration and routing information is shared by every switch in the stack, creating a single logical switching unit.

Switches can be added to and deleted from a working stack without affecting performance. All stack members have full access to the stack interconnect bandwidth.

The stack is managed as a single unit by a master switch, which is elected from one of the stack member switches.

The following are the important features of Cisco StackWise technology:

1. Each switch in the stack has the capability to behave as a master or subordinate (member) in the hierarchy.

2. When the StackWise switches are properly connected and operational, they form a bi-directional ring where data flow is bidirectional.

3. Each stack of Switches has a single IP address and is managed as a single object.

4. Each stack has only one configuration file, which is distributed to each member in the stack.

5. A working stack can accept new members or delete old ones without service interruption.

6. Each switch in the stack can serve as a master, creating a 1:N availability scheme for network control

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : DHCP snooping,IP Source Guard,Dynamic ARP inspection

examguides.com/CCNP-Switch/ccnp-switching-11.htm

2. Infrastructure Security

2.1 Configure and verify switch security features

2.1.a DHCP snooping

DHCP snooping is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. Rogue DHCP servers are often used in man in the middle or denial of service attacks for malicious purposes. When DHCP snooping is enabled, switch ports are categorized as either trusted or un-trusted. Only trusted ports are allowed to send DHCP replies. Therefore, you should identify and configure only those ports that are trusted and connected to DHCP server(s).

You can do this with the following interface configuration command:

Switch(config-if)#ip dhcp snooping trust

IP Source Guard prevents IP spoofing by forwarding only packets that have a source address consistent with the DHCP Snooping table.

2.1.b IP Source Guard:

IPSG helps to prevent IP spoofing, which is when an attacker claims the IP address of a server or device on your network. By pretending to be that device, the attacker could potentially direct sensitive data towards a port he's connected to. IPSG is configured at the access layer and uses the DHCP Snooping database, or static IP binding entries, to dynamically create ACLs on a per-port basis (these can't be viewed in the running-configuration). Any traffic which doesn't match the binding entries is dropped in hardware. However, the port won't go into the errdisable state, it won't even display a violation message at the console.IPSG is supported on layer two ports and cannot be used on layer 3 ports or SVIs.

2.1.c Dynamic ARP inspection (DAI):

Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. Further, ARP attacks are Layer-2 attacks. Therefore, each switch needs to be configured with DAI for effectively preventing ARP spoofing attacks. Because ARP attacks are limited to a single Layer 2 broadcast domain, separate the VLAN with DAI checks from the one with no checking. This action secures the ARP caches of hosts in the VLAN enabled for DAI. DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. DAI is supported on access ports, trunk ports, EtherChannel ports, and private VLAN ports.

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Port Security

examguides.com/CCNP-Switch/ccnp-switching-12.htm

2. When you enable port security on a switch, by default only one MAC address can be learned. To allow more than one MAC address on a switch port simultaneously, use the command:

3. **port-security maximum** <*max-number*>.

4. You can either define the allowed MAC addresses statically or allow the port to learn the MAC addresses. If you define only part of maximum allowed MAC addresses statically, the remaining MAC addresses are learned dynamically. This may lead to security breach if misused.

The following are true about inline power switch port:

1. By default, the inline power is disabled when a switch port is down.

2. When a device is connected to an inline power switch port, it first ensures that the device connected requires inline power by sending tone signals at 340kHz. Inline power is enabled only after ensuring that the connected device requires inline DC power. Otherwise, the DC power may damage connected devices if provided indiscriminately.

3. Use debug ilpower controller and debug cdp packets commands to view inline power adjustments.

4. Inline power is supplied at 48V DC, and pins 1,2 and 3,6 of the RJ-45 connector are used.

You can instruct the switch as to what to do if there is any port security violation. The command to configure port security violation is

Switch(config-if)#switchport port-security violation *{shutdown | restrict | protect}*

Shutdown: The port is effectively shuts down on any port violation.

Restrict: The port stays up, but drops all packets violating MAC addresses. Use SNMP to trigger a violation.

Protect: The packets from violating addresses are dropped, but no record of violation is kept.

The syntax for configuring a switch port to use 802.1x is:

Switch(config-if)#dot1x port-control [force-authorized | force-un-autorized | auto]

Ports can be in one of three authorization modes. The first mode, force-authorized, and default mode. In first mode, a port is always authorized. Force-authorized mode is used when you do not want to run 802.1X on a particular port. This is typically the case when connecting to another switch, or a client PC that do not support 802.1X. The next mode, auto, is the normal 802.1X mode. A port in auto mode will not become authorized unless it receives a positive response from the authentication server. The final mode, force-unauthorized, prevents a port from becoming authorized even if the user has the appropriate credentials. This mode essentially disables the port from use by any user or device.

The command "**switchport port security maximum** *10*" is not properly configured.

Note that the switch will take the mac addresses dynamically for the balance . In this case, after assigning an IP phone mac, and one for the PC, the switch is still left with 8 dynamically configurable mac addresses. You need to choose only the required number of macs. In this case, it is 2 mac addresses, one for the IP phone and the other for the user PC.

The command

Switch#show power inline *[type <mod>/<num>]*

Can be used to verify the inline power status for a switch port.

The command used for displaying the size of the CAM table is :

show mac address-table count

The interface configuration command :

Switch(config-if)#power inline *{auto|never}*

is used for configuring inline power supply on a switch port. By default, every switch port attempts to discover an inline-powered device

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Private Vlan,Strom Control

examguides.com/CCNP-Switch/ccnp-switching-13.htm

2. Infrastructure Security

2.1 Configure and verify switch security features

2.1.e Private VLAN

Also known as port isolation, is a technique in computer networking where a VLAN contains switch ports that are restricted such that they can only communicate with a given "uplink". The restricted ports are called "private ports".

A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing you to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs. All VLANs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. The secondary VLANs may either be isolated VLANs or community VLANs. A host on an isolated VLAN can only communicate with the associated promiscuous port in its primary VLAN. Hosts on community VLANs can communicate among themselves and with their associated promiscuous port but not with ports in other community VLANs.

The following are true about PVLANs:

- 1. There are three types of private VLAN ports
  - Promiscuous port: A promiscuous port communicates with all other PVLAN ports, and is the port typically used to communicate with external routers, servers, administrative workstations, etc.
  - Isolated port: An isolated port has complete L2 separation, including broadcasts, from other ports within the same PVLAN, with the exception of the promiscuous port. Traffic received from an isolated port is forwarded to all promiscuous ports only. None of the other isolated ports receive traffic from another isolated port.
  - Community port: Community ports can communicate among themselves and with their promiscuous ports. Community ports are isolated at L2 from all other ports in other communities, or isolated ports within their private VLAN. Broadcasts are forwarded only between associated community ports and the promiscuous port.
- Switches that use PVLANs must be configured for transparent VTP mode.
- Isolated ports can only forward traffic to promiscuous ports.

- In a PVLAN, promiscuous ports are called the primary VLAN, while community and isolated ports are called secondary VLANs.
- A PVLAN will only have one primary VLAN, but may have several secondary VLANS.

The syntax for associating a switch port with a Private VLAN is given by:

```
Switch(config-if)#switchport mode private-vlan {host | promiscuous}
```

If the port is connected to a router etc, then you need to select the keyword "promiscuous". If the port is connected to a host such as a server or a workstation then you normally choose "host" keyword. By choosing the keyword "host", you are setting the port as community or isolated port on the secondary VLAN.

The command sequence to map the promiscuous ports to primary and secondary VLANs are as given below:

```
switch(config)#interface fastethernet 3/9
switch(config-if)#switchport mode private-vlan promiscuous
switch(confgi-if)#switchport private-vlan mapping 100, 10,20
```

The steps involved in implementing VLAN access lists:

1. Define VLAN Access Map. To define a VLAN access-map use the command:

```
Switch(config)#vlan access-map <map-name> [sequence-number]
```

Access map statements are performed according to the sequence number.

2. Define matching conditions to identify traffic to be filtered. Use the access-map configuration command:

```
Switch(config-access-map)# match {ip address {acl-address {<acl-number> | <acl name>}} | {ipx address {<acl-number> | <acl name>}} | {mac address <acl-name>}
```

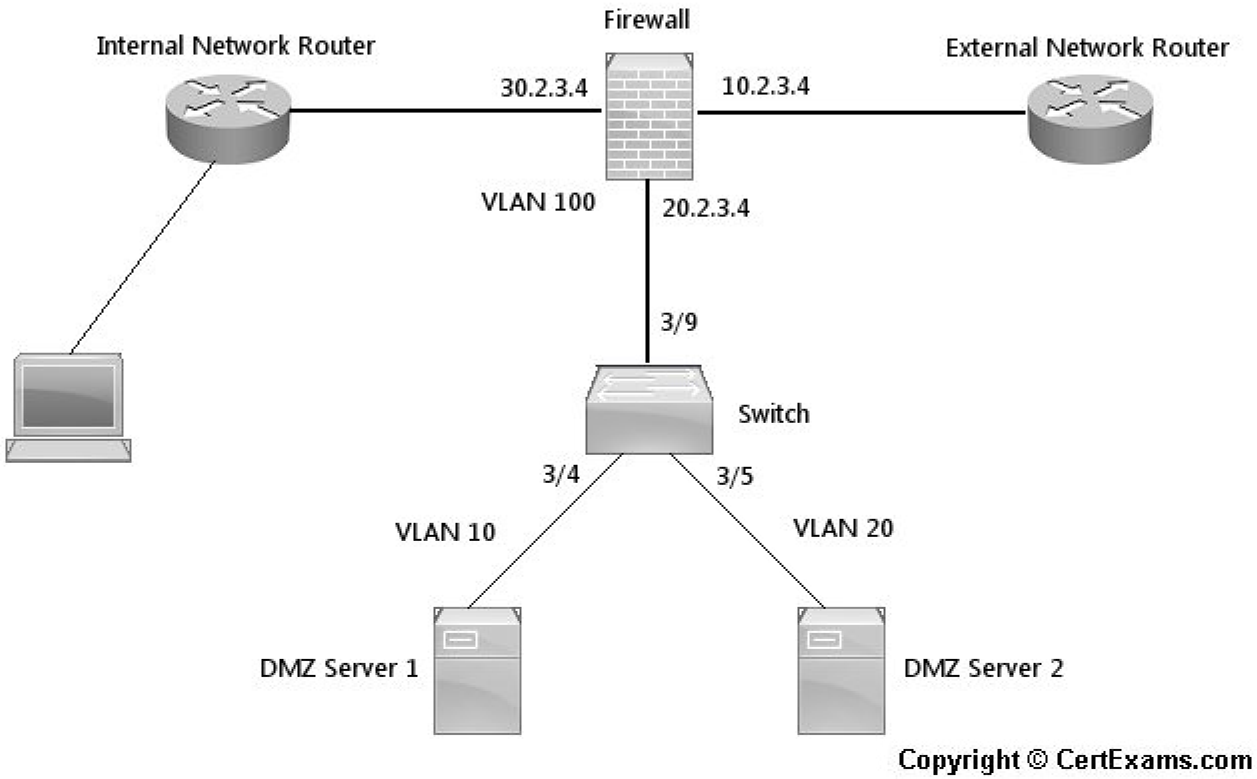
3. Define the action to be performed on the filtered traffic. Use the command:

```
Switch(config-access-map)# action {drop | forward [capture] | redirect <interface type> <mod>/<num>}
```

4. Apply the VACL to a VLAN interface. Use the global configuration command:

```
Switch(config)# vlan filter <map-name> vlan-list <list-of-vlans-here>
```

Example: Please look at the figure. You have DMZ that has two servers as shown in the figure. You want to secure the DMZ using Private VLAN. How the switch ports 3/4 and 3/5 be configured so that the servers are secure and do not talk to each other?



In the DMZ shown, the servers Server1 and Server2 do not have to talk to each other. Therefore a private vlan be defined with ports 3/4 and 3/5 as isolated ports. An isolated port has complete L2 separation, including broadcasts, from other ports within the same PVLAN, with the exception of the promiscuous port. Traffic received from an isolated port is forwarded to all promiscuous ports only. None of the other isolated ports receive traffic from another isolated port.On the otherhand port 3/9 has to be configured as promiscuous it needs to talk to the isolated ports 3/4 and 3/5 and with the other switches, routers, or other network components.

2.1.f Storm control:

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. You can use the traffic storm control feature to prevent disruptions on Layer 2 ports by a broadcast, multicast, or unicast traffic storm on physical interfaces. Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming broadcast, multicast, and unicast traffic over a 1-second interval. During this interval, the traffic level is compared with the traffic storm control threshold that you had configured. If the ingress traffic reaches the traffic storm control threshold that is configured on the port, traffic storm control drops the traffic until the interval ends. You will be able to make the traffic storm control to monitor only the broadcast traffic, or broadcast and multicast and/or all broadcast, multicast, and unicast traffic and trigger traffic control on a variety of criteria.

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Device Security Using Cisco Ios Aaa With Tacacs+ And Radius

examguides.com/CCNP-Switch/ccnp-switching-14.htm

2. Infrastructure Security

2.2 Describe device security using Cisco IOS AAA with TACACS+ and RADIUS

2.1.a AAA with TACACS+ and RADIUS

Cisco switches can use the following two protocols to communicate with AAA servers:

TACACS+: A Cisco proprietary protocol that separates each of the AAA functions, communication is secure and encrypted over TCP port 49. Only TACACS+ server authorizes users with permission to use specific commands. Other methods given in the question could not provide the granular access to switch commands

RADIUS: A standards-based protocol that combines authentication and authorization into a single resource; communication uses UDP ports 1812 and 1813 (accounting), but is not completely encrypted. The authentication server (RADIUS) authenticates each workstation (supplicant) that is connected to a switch port before making available any services requested by the user. If the authentication succeeds, normal traffic can pass through the port. The RADIUS security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server for use with 802.1x port based security protocol.

The global configuration command used for enabling authentication, authorization, and accounting on a switch is.

```
aaa new-model
```

By default, AAA is disabled on a switch. For providing an access to a switch, you configure Authentication. To provide access to various resources, you use Authorization. To record various switch events you use Accounting.

There are broadly four steps in configuring authentication on a Catalyst switch:

Enable AAA on the switch using the command :

```
switch(config)# aaa new-model
```

Define source of authentication using one or more of these commands:

locally configured username and password (stored in local switch database):

```
switch(config)# username <user name> password <pass word>
```

To use external authentication server, for example RADIUS:

```
Switch(config)# radius-server host {host-name | ip-address} [key string]
```

Where [key string] is the password known to switch and the radius server.

Define authentication methods by using the command:

```
switch(config)# aaa authentication login {default | list-name} method1 method2...
```

ex: **switch(config)#aaa authentication login default radius**

will enable radius authentication as default.

Also note that the local authentication is tried last after other authentication methods have failed to authenticate.

Finally, trigger the authentication defined at step 3 to the switch by entering line command prompt by using the command

```
switch(line)# login authentication {default | listname}
```

You use the command

```
login authentication {default | listname}
```

to trigger user authentication on that line to use an AAA method list.

The command syntax for applying an authorization method list to a specific line on a switch is given below:

```
Switch(config-line)# authorization {commands <level> | exec | reverse-access} {default | <list-name>}
```

To define a method for authorization on a Catalyst switch, use the command:

```
Switch(config)#aaa authorization {commands | config-commands | configuration | exec | network | reverse-access |} {default | list-name} [method1 [method2...]
```

Syntax Description

network: Runs authorization for all network-related service requests, including SLIP, and PPP

exec: Runs authorization to determine if the user is allowed to run an EXEC shell. commands: Runs authorization for all commands at the specified privilege level.

configuration: The server returns permission to enter the switch configuration mode

config-commands: The server returns permission to use any switch configuration command.

level: Specific command level that should be authorized. Valid entries are 0 through 15.

reverse-access: Runs authorization for reverse access connections, such as reverse Telnet.

default: Uses the listed authorization methods that follow this argument as the default list of methods for authorization.

For recording any switch events, you need to configure and enable Accounting module of the AAA.

Previous   Contents   Next

Cisco® CCNP Switch Exam Cram Notes : Device Security Using local Privilege Authorization Fallback

examguides.com/CCNP-Switch/ccnp-switching-15.htm

2. Infrastructure Security

2.2 Describe device security using Cisco IOS AAA with TACACS+ and RADIUS

2.1.b Local privilege authorization fallback

Three normally used methods to verify user credentials at a switch port are:

- By using locally configured username and password
- By using RADIUS authentication
- By using TACACS+ authentication.

1. To configure username and password locally, use the command at global configuration mode of the switch:

Username *<username>* **password** *<password>*

2. To define authentication using RADIUS, use the command

Radius-server host {<hostname | *<ip-address>***} [key string]**

3. To define the server along with its secret shared password.

Define a group name that will contain a list of servers using the command:

```
Switch(config)# aaa group server {radius | tacacs+) <group-name>
```

4. Now, define each server of the group by using the command:

```
Switch(config)#server <ip-address>
```

5. If you have more than one RADIUS or TACACS servers, repeat the above command for each server.

Locally configured username and password are enabled by default on a switch. If there is any other authentication scheme defined, it is tried first before using local authentication. You can disable local authentication when other authentication methods are in use. You configure username and password for local authentication on a switch by using the command:

```
Switch(config)# username <user name> password <password>
```

You define a radius server for user authentication by using the command

```
Switch(config)#radius-server host {host-name | ip-address} [key string]
```

[key string] is the password that is shared between the switch and the radius server.

The command :

```
Switch(config)# aaa group server radius <group-name>
```

is used to define the group name that will contain a list of servers.

The command :

```
Switch(config)# aaa authentication login default radius
```

specifies that the default login method is RADIUS.

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : HSRP

examguides.com/CCNP-Switch/ccnp-switching-16.htm

3. Infrastructure Services

3.1 HSRP

HSRP stands for Hot Standby Routing Protocol. HSRP is a Cisco proprietary protocol that offers router redundancy. Here one router is elected as active router, and another router is elected as standby router. All other routers are put in listen HSRP state. HSRP messages are exchanges using multicast destination address 244.0.0.2 to keep a router aware of all others in the group.

Members of HSRP group

1. Virtual router: virtual router is what is seen by the end user device. The virtual router has its own IP and MAC addresses.

2. Active router: Forwards packets sent to the virtual router. An active router assumes the IP and MAC addresses of the virtual router.

3. Standby router: Standby router monitors the state of HSRP by using Hello massages. It assumes the role of Active router, should the current Active router fail.

When an Active router fails in HSRP environment, Standby router assumes the Active router role. This new Active router will remain as Active router even if the failed Active router comeback to service, irrespective of the priority levels.

To enable the previous Active router to resume its activity as Active router by taking over the role from a lower priority Active router, use the command

Rtr(config-if)#standby *<group-number>* **preempt**

The hosts served by HSRP router use the IP address of virtual router as the default IP address.

Each router in a standby group can be assigned a priority value. The range of priority values is between 0 and 255 (including 0 and 255). The default priority assigned to a router in a standby group is 100. The router with numerically higher priority value will become Active router in the HSRP standby group.

The command used to set the router's priority in standby group is:

R(config-if)#standby *<group-number>* **priority** *<priority-value>*

HSRP Features:

1. Within the standby group of routers, the router with the highest standby priority in the group becomes the active router. For example, a router with a priority of 100 will become active router over a router with a priority of 50. The active router forwards packets sent to the virtual router. It maintains its active state by using Hello messages.

2. The default HSRP standby priority is100. If the standby priorities of routers participating in HSRP are same, the router with the highest IP address becomes the Active router.

3. HSRP authentication is carried out in clear text.

4. An HSRP router status can be displayed by using the command :

RouterA# show standby

The above command displays the router priority, state (active/standby), group number among other things.

5. To enable HSRP debugging, use the command :

RouterA#debug standby

6. To disable debugging, use the command :

RouterA# no debug standby

In HSRP, the MAC address used by virtual router is made up of the following three components:

- Vendor ID: The first three bytes of the MAC address correspond to the vendor ID.
- HSRP ID: The next two bytes of the MAC address correspond to HSRP code. It is always 07.ac. Therefore, the virtual router MAC address will have 07.ac in the fourth and fifth bytes.
- Group ID: The last byte of the MAC address is the group's identification number.

In the choices given, only 00.00.07.0c.ac.1e has 4th and 5th bytes 07.0c and hence a valid HSRP MAC address.

All routers in an HSRP standby group can send and/or receive HSRP message. Also, HSRP protocol packets are addressed to all-router address (224.0.0.2) with a TTL of 1. Note that the HSRP messages are encapsulated in the data portion of UDP packets.

The correct command syntax for configuring a router as a member of an HSRP standby group is:

R(config-if)#standby *<group-number>* **ip** *<virtual-ip-address>*

For group number 45 and virtual IP address of 192.32.16.5, the command is:

R(config-if)#standby *45* **ip** *192.32.16.5*

The command : "**standby <group-number> preempt**" is used to force an interface to resume Active router state. Note that the priority of the router should be higher than the current Active router.

HSRP uses multicast address 224.0.0.3 UDP port 1985 for sending its hello messages.

In HSRP, each of the routers of the participating routers is assigned to a common HSRP group. One router is elected as the primary, or active HSRP router. One router 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 that they can remain aware of each other's existence and that of the active router. HSRP sends its hello messages to the multicast destination 224.0.0.2 (all routers) using UDP port 1985.

The following statements are true about HSRP routers:

1. The priority value of a HSRP group router can have values between 0 and 255

2. The router with highest priority value will be elected as the primary. The highest value possible is 255. Higher priority value corresponds to higher priority in HSRP. You need to be careful in interpreting the priority value with priority. Both are different.

3. There can be only one router in active state and one in the standby state at any given time.

4. HSRP uses unicast messages to exchange Hello packets

5. 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.

6. By default, hellos are sent every 3 seconds, and only the standby router. If hellos are missed for the duration of the holdtime timer (default 10 seconds, or three times the hello timer), the active router is presumed to be down.

In HSRP, one router with highest priority is elected as the active router, and one with next highest priority will become the standby router. All other routers in the HSRP group will be put in Listen state.

You can configure a router to immediately take over (assuming that the router had been previously taken out of the group due to some reason) 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 [minimum <seconds>] [reload <seconds>]]**

By default, the local router immediately can preempt another router that has the active role. To delay the preemption, use the delay keyword followed by one or both of the following parameters:

- Add the minimum keyword to force the router to wait for seconds (0 to 3600 seconds) before attempting to overthrow an active router with a lower priority
- The optional "reload <seconds>" will force the router to wait for seconds (0 to 3600 seconds) after it has been reloaded or restarted. This enables routing protocols that need time to converge after a hard reset.

The key chain has been named as hsrp10. However, on the interface, the association is wrong. Key-chain name has wrongly been associated with hsrp1 instead of hsrp10.

HSRP will track the availability of interface serial 0/0. If serial 0/0 goes down, the priority of the router in group 1 will be decremented by 25. The default value of the track argument is 10.

Consider the following HSRP configurations

catalystA(config)#interface vlan *100*
catalystA(config-if)#ip address *192.168.1.16 255.255.255.0*
catalystA(config-if)#standby *1* **priority** *175*
catalystA(config-if)#standby *1* **preempt**
catalystA(config-if)#standby *1* **ip** *192.168.1.1*

In the example given, 192.168.1.1 is the gateway address that is used to reach the gateway in the HSRP group of routers. It is a virtual IP address, and tied to a virtual MAC address. All the routers in the HSRP group use the same virtual IP address and MAC address pair. This way, even if active HSRP router goes down, the new active router will still have the same IP address and MAC address for the gateway, and the client computers need not worry about changing the default gateway.

In HSRP, higher the priority value (range is 0 to 255), higher the priority of the router. The router with highest priority value will become the Active HSRP router. Default priority of a HSRP router is 100. Further, an HSRP group can be assigned an arbitrary group number, from 0 to 255

For the virtual router address, HSRP defines a special MAC address of the form 0000.0c07.acxx, where xx represents the HSRP group number as a two-digit hex value.

For example, HSRP Group 1 appears as 0000.0c07.ac01, HSRP Group 16 appears as 0000.0c07.ac10, and so on.

Examples for loadbalancing in HSRP

Load balancing traffic across two uplinks to two HSRP routers with a single HSRP group is not possible. However, we can load balance between two HSRP routers using VLANs and creating two HSRP groups.

For example, you can make HSRP RourterA as Active for one VLAN (say VLAN1) in HSRP group1 and RouterB as Active for the second VLAN (say VLAN2) in HSRP group2. RouterB will be the Standby for VLAN1 (HSRP group 1) and RouterA will be the Standby for VLAN2 (HSRP group 2). This can be done by adjusting the HSRP router priorities for respective VLANs as below:

```
RouterA(config)# interface vlan 100
RouterA (config-if)# ip address 192.168.1.15 255.255.255.0
RouterA (config-if)# standby 1 priority 200
RouterA (config-if)# standby 1 preempt
RouterA (config-if)# standby 1 ip 192.168.1.1
RouterA (config-if)# standby 1 authentication MyKey
RouterA (config-if)# standby 2 priority 100
RouterA (config-if)# standby 2 ip 192.168.1.2
RouterA (config-if)# standby 2 authentication MyKey
```

```
RouterB(config)# interface vlan 50
RouterB(config-if)#ip address 192.168.1.16 255.255.255.0
RouterB(config-if)#standby 1 priority 100
RouterB(config-if)#standby 1 ip 192.168.1.1
RouterB(config-if)#standby 1 authentication MyKey
RouterB(config-if)#standby 1 priority 200
RouterB(config-if)#standby 2 preempt
Router(config-if)#standby 2 ip 192.168.1.2
RoutertB(config-if)#standby 2 authentication MyKey
```

Note that in the above example, RouterA will be the active router in HSRP group 1 as the priority has been set higher (200). On the otherhand, RouterB will be the Active router in HSRP group 2 as the priority has been set higher (200).

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : VRRP

examguides.com/CCNP-Switch/ccnp-switching-17.htm

3. Infrastructure Services

3.2 VRRP

Virtual Router Redundancy Protocol (VRRP): VRRP is very similar to HSRP. VRRP is a standards based protocol and defined in RFC 2338. VRRP sends advertisements to multicast destination address 244.0.0.18 using IP protocol.

Given below are the important characteristics of Virtual Router Redundancy Protocol (VRRP):

1. VRRP advertisements are sent at 1-second intervals.

2. VRRP has no mechanism for tracking interfaces to allow more capable routers to take over the master role.

3. Router priorities range from 1 to 254.

4. The default VRRP router priority is 100

5. The Virtual Router Redundancy Protocol (VRRP) is a standards-based protocol

6. The router with highest priority is called Master router

7. The multicast address 224.0.0.18 is used by VRRP to send advertisements. It uses IP protocol 112.

The following are true about Virtual Router Redundancy protocol (VRRP):

1. VRRP will have one master router, and all other routers are in the backup state.

2. VRRP router priorities range from 1 to 254. By default, the priority is set to 100. 254 is the highest priority.

3. The MAC address of the virtual router is of the form 0000.5e00.01xx, where xx is the VRRP group number in the range 0 to 255 or 0 to ff hex.

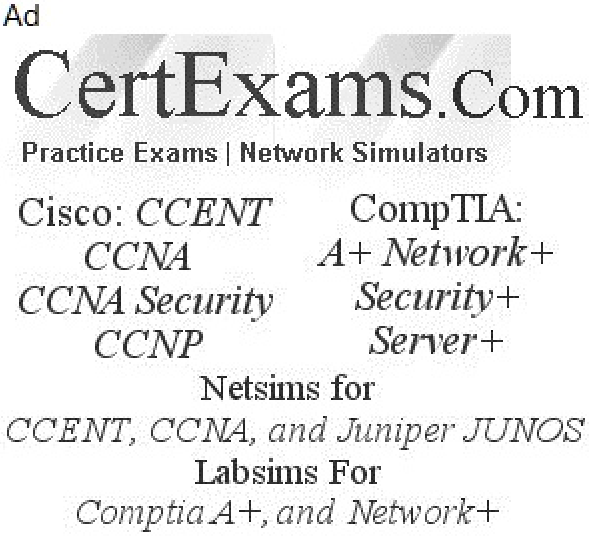
4. The interval for VRRP advertisements is 1 second by default.

5. All VRRP routers are configured to preempt the current master router by default. The router priority should be highest for the preemption to occur.

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : GLBP

examguides.com/CCNP-Switch/ccnp-switching-18.htm



3. Infrastructure Services

3.3 GLBP

Gateway Load Balancing Protocol (GLBP): GLBP overcomes some of the limitations of HSRP/VRRP. Here, instead of just one active router, all routers in the group can participate and offer load balancing.

Features of GLBP

1. Gateway Load Balancing Protocol (GLBP) is Cisco proprietary protocol. Like many other protocols, the protocol is yet to be adopted by the standards organization.

2. GLBP uses only one virtual IP address for gateway. However, the master router can assign up to 4 virtual MAC addresses for the routers participating in the GLBP protocol. This will ensure that the clients need to be configured with only one gateway IP address, and at the same time the traffic sent to different GLBP routers.

3. The router priority can be 1 to 255 with default being 100

4. The router with the highest priority value, or the highest IP address in the group, if there is no highest priority, is elected as the Active Virtual Gateway (AVG)

5. GLBP group numbers range from 0 to 1023.

The following load-balancing methods can be used in a GLBP group:

1. Round robin: Each new ARP request for the virtual router address receives the next available virtual MAC address in reply. This is the default method used by GLBP. One drawback with this method is that if a server sends disproportionate traffic, the gateway forwarding the packets from the server will get overloaded.

2. Weighted: The GLBP group interface's weighting value determines the proportion of traffic that should be sent to that AVF. A higher weighting results in more frequent ARP replies containing the virtual MAC address of that router.

3. Host dependent: Each client that generates an ARP request for the virtual router address always receives the same virtual MAC address in reply. This method is useful if a client such as a file server needs a consistent MAC address for load balancing.

Server Load Balancing (SLB): SLB provides a virtual server IP address to which client machines can connect. The virtual server, in turn, is a group of real physical servers arranged in a server farm.

Server Load Balancing (SLB) uses the following methods for load balancing traffic:

1.Weighted round-robin: Each physical server is assigned a weight. For a weight n, a server is assigned n new connections before SLB moves on to the next server.

2. Weighted least connections: Here the SLB assigns new connections to the physical server that has the least number of weighted active connections. If the weight of a physical server is m, then its capacity for active connections is m divided by the sum of all server weights. New connections are assigned to the server with least load.

The command : **Switch(config)# port-channel load-balance** *src-ip* will configure load balancing on EtherChannel switch links using source IP address.

Note that the load balancing can be done based on source IP, destination IP, both source and destination IP (XOR), source and destination MAC addresses or TCP/UDP port numbers.

The following are the basic commands used for configuring a server farm when using SLB:

1. To name the server farm, use the command:

switch(config)# ip slb serverfarm *<serverfarm-name>*

<serverfarm-name> can be up to 15 characters.

2. Choose load-balancing method by using the command:

```
switch(config-slb-sfarm)# predictor {roundrobin | leastconns}
```

weighted round-robin is the default.

3. Identify the real servers using the command:

```
switch(config-slb-sfarm)# real <ip-address>
```

where <ip-address> is the servers actual IP address.

4. Assign a weight for the server. The weight represents the capacity of the server to accept new connections.

```
Switch(config-slb-real)# weight <value>
```

The <value> ranges from 1 to 255, with a default value of 8.

5. Switch the server into service by using the command:

```
switch(config-slb-real)# inservice
```

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Switch Ios

examguides.com/CCNP-Switch/ccnp-switching-19.htm

4. Appendix

4.1 Cisco Switch IOS

Files in Catalysts switches

The following are the important file systems available in Catalyst switches and their usage:

1. IOS image files: The switch binary software resides in the IOS image files. The IOS image files are internally stored in Flash memory of the switch.

2. Configuration files: These are the text files containing the configuration commands for operation of the switch.

3. Flash memory: IOS files are stored in the Flash memory. When the switch boots, the IOS files are read from the Flash memory.

4. Network servers: External locations can hold IOS image file or configuration files. This is useful for upgrade or backup purpose. You can load files from external file systems such as network servers using TFTP, and FTP.

5. NVRAM: NVRAM contains the switch configuration files. These files are used during boot-up for proper configuration of the switch.

6. RAM: The switch configuration is stored in RAM during run-time. Any configuration commands entered are first reflected in RAM. You need to use save config startup-config running-config to save them to NVRAM.

6807-XL and 4500X provide dual chassis and virtual switching system (VSS). VSS pools multiple Cisco Catalyst Switches into one virtual switch, increasing operational efficiency, boosting nonstop communications, and scaling system bandwidth capacity. The VSS manages the redundant links, which externally act as a single port channel.

The VSS simplifies network configuration and operation by reducing the number of Layer 3 routing neighbors and by providing a loop-free Layer 2 topology.

Frequently used show commands on a switch:

show version: The command displays

a. The current version of IOS running in a switch
b. Available hardware, RAM, Flash memory,
c. Switch uptime
d. Configuration register's content
e. Reason for the last reload etc.

show running-config [interface <type> <mod>/<num> | vlan <vlan-id> | module <mod>]:

The command displays the contents of the configuration file.

show tech-support: The command is primarily used to send switch information to Cisco TAC support personnel.

verify flash:<*filename*>: This command is used to verify whether the Flash contents are intact, and not corrupted. The checksum of the flash file specified is verified for correctness.

The command "**show module**" provides the Module types, Serial numbers, status, and MAC addresses among other things. "**Show module**" command without any specific module number displays information on all modules installed in the box.

To enable a switch port for layer 2 functionality use the following commands:

1. **switch(config)# interface** <*type*> <*mod*>/<*num*>

2. **switch(config-if)# switchport**

The first command enters interface configuration mode for the switch interface <mod>/<num>, and the second command enables layer 2 functionality on the port.

Use the "no" form of the switchport command to enable layer3 functionality.

When CEF (Cisco Express Forwarding) is enabled on a switch, an FIB (Forwarding Information Base) is build that enables forwarding of arriving packets at wire speed. However, there are packets that may still need intervention by Layer 3 Engine. If an arriving packet is required to be forwarded to Layer 3 Engine, then the packet is marked as "CEF punt" and sent to Layer 3 engine for further processing.

The following are the occasions when the packet is marked as CEP punt and forwarded to Layer 3 engine:

1. An entry can not be found in the FIB

2. The FIB is full

3. The IP TTL has expired

4. The MTU is exceeded, and the packet needs to be fragmented.

5. The encapsulation type is not supported

6. Compression or encryption operation is needed etc.

CEF can be performed on a single hardware platform or distributed over several line cards, depending on the switch type. There are two techniques for distributed processing:

1. Accelerated CEF (aCEF): Here the CEF is distributed over multiple Layer 3 forwarding engines. However, the FIB is not distributed completely, only a portion of FIB is downloaded to them at a given time. This is more like the concept of Cache memory. If an entry is not found, a request is made to the Layer 3 engine for more FIB information.

2. Distributed CEF (dCEF): Here the CEF is completely distributed among multiple Layer 3 forwarding engines. The FIB is used for complete Layer 3 forwarding. A central Layer 3 engine maintains the routing table and generates the FIB. This central FIB is used for dynamic update of each of the distributed CEFs.

The command:

Switch#show ip cef

displays the entire FIB contents of a switch running CEF (Cisco Express Forwarding).

A switch configured for CEF, uses adjacency tables to prepend Layer 2 addressing information. Nodes in the network are said to be adjacent if they are within a single hop from each other. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries. The adjacency table information is build from the ARP table.

The command

```
Switch# show ip cef <type> <mod>/<num> [detail]
```

provides complete FIB and adjacency table information for a given interface.

Switches like Catalyst 3750 and 4500 run CEF by default. However, you can disable CEF on a per-interface basis by using interface configuration commands "no ip route-cache cef" and "no ip cef" on the Catalyst 3750 and 4500, respectively.

The EtherChannel also provides link redundancy. If one of the bundled links fail, the traffic through the failed link is distributed to other working links in the channel. The failover is transparent to the end user. Similarly traffic again flows through the restored link, as and when a link is restored.

The command

```
switch#show etherchannel summary
```

shows each port in the channel along with the status flag

Multi-layer switching is based on Route once, switch many. It incorporates Layer 2 switching and Layer 3 routing functionality.

EtherChannel can support from two to 8 links to be bundled into one logical link. Therefore, if fast Ethernet links are bundles, 8 links represents 800 Mbps of oneway bandwidth, and 1600 Mbps for full-duplex operation.

The following are true about bundling ports using EtherChannel:

1. The bundled ports must have identical Spanning Tree settings
2. The bundled ports must have the same speed, duplex, and Ethernet media.
3. The bundled ports must belong to the same VLAN if not used as VLAN trunk.
4. If the bundled ports represent a VLAN trunk, then they must have same native VLAN, and each port should have same set of VLANs in the trunk.

The command

```
switch#show etherchannel port
```

can be used for verifying the channel negotiation mode of an EtherChannel.

The syntax for setting port speed on an IOS switch is

```
speed { 10 | 100 | auto }
```

For setting the speed to 10mbps on module 1 port 5, the command is

```
speed 10
```

Similarly, to set the duplex mode on a switch:

```
duplex { auto | full | half}
```

For setting the duplex to half, use the command:

```
duplex half
```

A switch floods a frame through all the ports except the port on which the frame is received, if the destination MAC address is not found in the CAM table.

The Catalyst IOS software is very similar to a router IOS. IOS image files are stored in the Flash memory on a switch.

Some of the copy commands:

1. copy running-config startup-config: allows the running configuration file to be saved onto the startup configuration file on the switch. Make sure that you use this command whenever you have made any configuration changes to the switch. Otherwise, your configuration command are not permanently saved in the switch memory, and lost soon after power cycling the switch.

2. copy startup-config running-config: allows startup configuration file to be copied into the current running configuration file.

3. copy running-config tftp: copies the running configuration of a switch to a TFTP server. You will be prompted for the server address and destination filename.

4. copy tftp: startup-config: this command is useful to restore the startup-config file incase the original is lost or corrupt. The command loads the startup-config file from a remote tftp server.

Each Telnet port is known as a virtual terminal. There are a maximum of five virtual terminal (VTY) ports, allowing five concurrent Telnet sessions. Please note that the communication server provides more VTY ports. The virtual terminal ports are numbered from 0 through 4.

The console and auxiliary ports on Cisco IOS routers and switches are asynchronous serial ports and use asynchronous protocols such as PPP, SLIP, and ARA.

Runts are packets that are smaller than the medium's minimum packet size. For example, Ethernet has a minimum allowed packet size of 64 bytes. Any packet that is less than 64 bytes in size is considered a runt in Ethernet.

Giants are packets that bigger than the medium's maximum packet size. Fro example, Ethernet has a maximum allowed packet size of 1,518 bytes. Any packet that is bigger than 1,518 bytes is considered a Giant in Ethernet.

CRC error occurs when the check sum calculated at the receiving end of the frame does not match with the check sum calculated at the source end.

The most probable reasons for runts, giants, and CRC errors is frame collisions while traveling from source to destination. It is also possible that a network card or device is bad and generating runts and giants.

Inline power is defined by the IEEE 802.3af standard.

The interface configuration command :

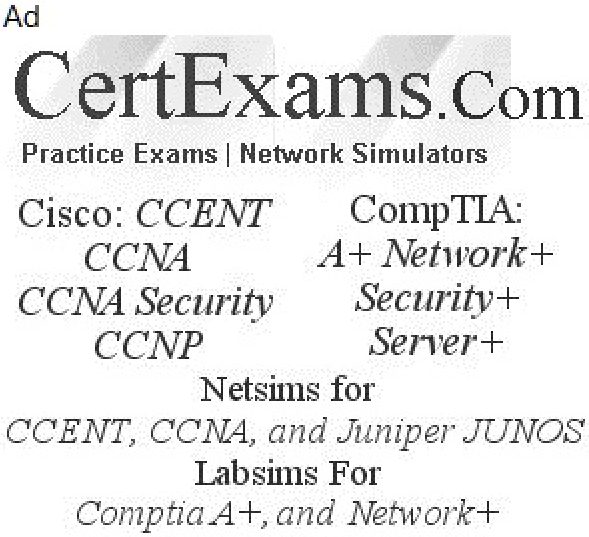
```
Switch(config-if)#power inline {auto|never}
```

is used for configuring inline power supply on a switch port. By default, every switch port attempts to discover an inline-powered device

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : 6800 Series Switches

examguides.com/CCNP-Switch/ccnp-switching-20.htm



4. Appendix

4.2 6800 series switches

Cisco Catalyst 6880-X Switch

4 module slots, 5 RU
80 x 10/1 G SFP or 20 x 40 G SFP/SFP+
Slot capacity 80 - 240 Gb/s
Switching capacity up to 4 Tb/s (VSS)
Cisco Catalyst Instant Access

Cisco Catalyst 6840-X Switch

4 slots, 2 RU
16, 32 x 10 SFP/SFP+ (Small Form-Factor Pluggable)
24, 40 x 10 G SFP/SFP+ and 2x40G QSFP
Slot capacity 80 - 240 Gb/s
Switching capacity up to 1.92 Tb/s (VSS)

Cisco Catalyst 6807-XL Switch

5 module slots, 2 SUP slots 10 RU
Slot capacity of up to 880 Gb per slot
Switching capacity up to 11.4 Tb/s
Supports ASA, NAM-3 (Network Analysis Module - 3), and WiSM2 (Wireless Services Module 2)

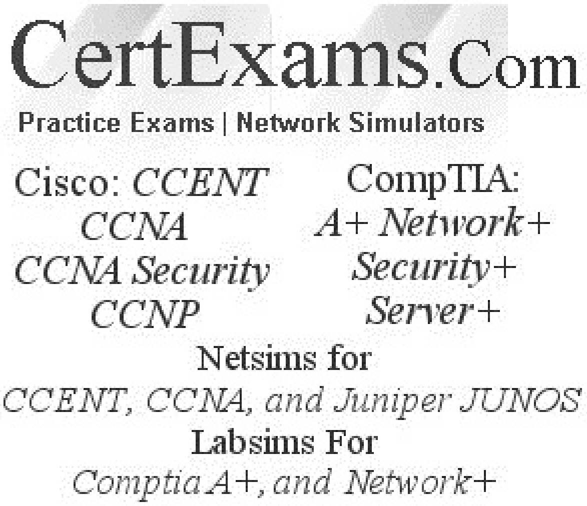
Cisco Catalyst 6800ia Switch

1 Slot, 1 RU
48 10/100/1000 E ports
PoE/PoE+
Stackable (3x)

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Cisco Access-Layer Switches

examguides.com/CCNP-Switch/ccnp-switching-21.htm



4. Appendix

4.3 Cisco Access-Layer switches

The following are the Cisco recommended Access Layer switches:

Catalyst 2950: For less than 50 users 10/100BaseT; 100BaseFX or 1000Base-X uplinks

Catalyst 3550: For less than 50 users 10/100BaseT; 1000Base-X uplinks;Advanced QOS, Inline power

Catalyst 4000/4500: For 250+ users 10/100/1000Base-T; 1000Base-X uplinks; Advanced QOS, Inline power.

Note that Catalyst 4000/4500 Supervisor III and IV support Cisco IOS.

Given below are some Access Layer switches available from Cisco :

1. Model: 2960-X

Max Port Density:384 (Up to 8 48-port switches in a stack)
Uplinks: 2 10GE or 4 1 Gigabit Ethernet per switch
Max Backplane Speed: 80 Gbps
Power over Ethernet: PoE+

2. Model: 3650

Max Port Density: 432 (Up to 9 48-port switches in a stack)
Uplinks: 2 Gigabit Ethernet or 4 10GE
Max Backplance Speed: 160 Gbps
Others: Full-featured routing available, integrated wireless controller, PoE+

3. Model: 3850

Max Port Density: 432 (Up to 9 48-port switches in a stack)
Uplinks: 4 Gigabit Ethernet, 4 10GE
Max Backplane Speed: 480 Gbps
Others: Full-featured routing available, integrated wireless controller,
Power Over Ethernet: PoE+, UpoE

4. Model: 4500E

Port Density: 384 (Up to 8 48-port modules per chassis)
Uplinks: Up to 12-port 10GE per module
Max Backplance Speed: 928 Gbps
Other Features: Dual supervisors, full-featured routing available, integrated wireless controller
Power Over Ethernet: PoE+, UpoE

For the given requirement, 2960-X is the appropriate answer. It will also have RIP and OSPF available for routed access. 4500-X, 6807-XL are recommended for Distribution/Core Layers. 3850 model is also an Access Layer switch, but with higher performance parameters.

Recommended Distribution and Core Layer in a campus wide network:

Model: 4500-X

Max Port Density: 80 10GE
Max Backplane: 1.6 Tbps
Others: Dual-chassis Virtual Switching System (VSS), redundancy

Model: 4500E

Max Port Density: 96 10GE or 384 Gigabit Ethernet
Max Backplane: 928 Gbps
Others: Dual supervisors

Model: 6807-XL

Max Port Density: 40 40Gbps, 160 Gigabit Ethernet, 480 Gigabit Ethernet
Max Backplane: 22.8 Tbps
Others: Dual supervisor, dual-chassis VSS, redundancy

2960-X and 3650 are access layer switches and high port density of 384 ports and 432 ports respectively.

The following Line Mode configuration options are available on a 1900/2800 or 2900XL series switches:

1. **Auto:** The port is put into auto negotiation mode. This is the default for 100baseTX ports. Available only on 100baseTX ports.

2. **Full:** Puts the port into full duplex mode. Available both on 10BaseTX and 100BaseTX

3. **Full-flow-control:** Puts the 100BaseTX port into full duplex mode with flow control. Available only on 100BaseTX ports.

4. **Half:** Puts the port into half-duplex mode. Available both on 10BaseTX and 100BaseTX.

The following are the Cisco recommended security measures for controlling access to a campus network:

1. **Access Layer:** This is the layer at which users log into the network and access network resources. The recommended security measures at Access Layer are:

- Controlling physical access to network devices (This applies to all layers),
- Port security, also known as 'MAC address lockdown' is Cisco feature that enables the switch to prevent input from a port when the MAC address of a station trying to access the port is different from the configured MAC address for that port.
- Passwords: A properly managed network should have login and password for each network device. There are several ways of accessing Cisco devices such as Console, vty, TFTP servers etc. Each of these should have properly defined passwords to control access to the network.

2. **Distribution Layer:** The security at distribution layer is implemented by using Access Policies. These in turn make use of Access Control Lists. There are two types of IP access lists:

- Standard
- Extended

In addition to security, Distribution layer is responsible for sending only the data that need to reach the Core Layer. This not only achieves security, but also makes sure that Core Layer is not burdened with unnecessary traffic. This is achieved by applying Access Control Lists.

Core Layer Security: Core layer is responsible for transmitting data efficiently. For this reason, Cisco recommends that there is little or no policy at Core layer.

Cisco recommends that management VLAN (VLAN 1) be moved to another VLAN. Another way to handle the problem is to disable the ports that are not being used, and secure physical access to the networking devices

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : Gigabit Ethernet Standards

examguides.com/CCNP-Switch/ccnp-switching-22.htm

4. Appendix

4.4 Gigabit Ethernet Standards

Commonly used Gigabit ethernet standards:

Given below are some of the important gigabit ethernet standards that are widely used.

Gigabit Eth Type	Cable Type	Distance
000BASE-CX	Shielded twisted pair (STP)	25 m
000BASE-T	TIA Category 5 UTP	100 m
1000BASE-SX	Multimode fiber (MMF) 62.5-micron	275m
50 micro	550 m	
1000BASE-LX/LH	MMF with 62.5-micron core	550 m
9 micro core	10 km	
1000BASE-ZX	SMF with 9-micron core; 1550-nm laser	70km

SMF with 8-micron core; 1550-nm laser	100km

By moving the routing functionality to the switches, the routing efficiency is significantly improved. Traditionally, routing is performed in software, resulting in poor performance. By moving the routing functionality to Layer 3 switching, the efficiency with which the routes are resolved improved significantly. Multilayer switching is based on the concept: Route Once and Switch Many. The initial routing is performed by router, and subsequent flow in the same route is handled by Layer 3 switches.

10-Gigabit Ethernet switch ports support a variety of rectangular X2 and SFP+ media modules as given below:

1. 10GBASE-CX4: Provides Copper connectivity up to 15 m

2. 10GBASE-SR: Provides short-reach connectivity using 62.5 or 50 micron MMF for distances up to 33 m or 300 m, respectively

3. 10GBASE-LRM: Provides long-reach multimode connectivity using 62.5 or 50 micron MMF for distances up to 220 m

4. 10GBASE-LX4: Provides connectivity using 62.5 or 50 micron MMF for distances up to 300 m

5. 10GBASE-LR: Long-reach connectivity using SMF for distances up to 10 km

6. 10GBASE-ER: Extended-reach connectivity using SMF for distances up to 40 km

The IEEE standard 802.3ae describes 10Gigabit Ethernet.

Previous Contents Next

Cisco® CCNP Switch Exam Cram Notes : IEEE 802.1x

examguides.com/CCNP-Switch/ccnp-switching-23.htm

4. Appendix

4.5 IEEE 802.1x

802.1x authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WAN. The authenticator is a network device, such as an Ethernet switch or wireless access point. The authentication server is typically a host running software supporting the RADIUS and EAP protocols.

Before authentication takes place, the only traffic allowed is EAP-over-LAN(EAPOL), CDP, and STP packets (BDPUs). After the client device has been authenticated, the port is opened, and access to other LAN resources are granted

The IEEE 802.1x standard defines a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN switch or an Access Point through publicly accessible switch ports.

802.1X consists of three components for port control, which are as follows:

An 802.1X authenticator: This is the port on the switch that has services to offer to an end device, provided the device supplies the proper credentials.

An 802.1X supplicant: This is the end device; for example, a PC that connects to a switch that is requesting to use the services (port) of the device. The 802.1X supplicant must be able to respond to communicate.

An 802.1X authentication server: This is a RADIUS server that examines the credentials provided to the authenticator from the supplicant and provides the authentication service. The authentication server is responsible for letting the authenticator know if services should be granted.

The authentication server (RADIUS) authenticates each workstation (supplicant) that is connected to a switch port before making available any services requested by the user. If the authentication succeeds, normal traffic can pass through the port. The RADIUS security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server for use with 802.1x port based security protocol.

IEEE 802.3af Power Classes

Power Class	Maximum Power Offered at 48V DC	Notes
0	15.4 W	Default class
1	4.0 W	Optional class
2	7.0 W	Optional class
3	5.4 W	Optional class
4	Up to 50 W	Optional class (802.3at)

Previous Contents