Chapter 1 - Configure, Verify, and Troubleshoot a Switch with VLANs and Interswitch Communications

Describe enhanced switching technologies (including: VTP, RSTP, VLAN, PVSTP, 802.1q).

Virtual LAN (VLANs) refers to a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on different LAN segments. As VLANs are based on logical connections, they are extremely flexible in terms of configuration and application.

Formally speaking, a VLAN is a switched network that is logically segmented on an organizational basis, typically by functions, project teams, or applications. It allows logical network topologies to overlay the physical switched infrastructure such that any arbitrary collection of LAN ports can be combined into an autonomous user group or community of interest. From a technical perspective, a VLAN can be thought of as a broadcast domain that exists within a defined set of switches. Such a broadcast domain can include a number of end systems that are connected by a single bridging domain supported on LAN switches that operate bridging protocols.

VLAN Trunk Protocol (VTP) can greatly reduce administration overhead in a switched network. When configuring a new VLAN on a VTP server, the VLAN is distributed through all switches in the domain. Therefore reducing the need to configure the same VLAN everywhere. VTP is Cisco-proprietary and is available on most of the Cisco Catalyst Family products.

The Inter-Switch Link (ISL) protocol is used to interconnect two VLAN-capable switches (and routers). As a packet-tagging protocol, ISL contains a standard Ethernet frame and the VLAN information associated with that frame. The packets on the ISL link contain a standard Ethernet, FDDI, or Token Ring frame and the VLAN information associated with that frame. At present, ISL is supported only over Fast Ethernet links, but a single ISL link can still carry different protocols from multiple VLANs.

NOTE: For the exam, you will be tested on your ability to understand the finer details of VLANs, VTP, trunking and Spanning Tree Protocol (STP). You will need to know how to solve problems within scenarios using any number of multiple technologies all at once. That being said, it’s imperative that you understand how all of the switching technologies interoperate. For example, understanding how a VLAN operates at Layer 2 of
the OSI model and how a Layer 3 interface (and IP address) allow intra-subnet routing. Understanding how mis-configuring your VTP parameters can propagate false VLAN information throughout your network is also important. For the exam you will need to understand how Spanning Tree Protocol (STP) works to keep your switched environment stable when you have redundant links. All of this and more will be tested on the exam, make sure you visit Cisco’s main website and their documentation and review all of the basic of switching before taking the exam.

As part of the IEEE 802.1 standard for media access control bridges, the Spanning Tree Protocol (STP) is a link management protocol that implements the spanning tree algorithm for providing path redundancy while preventing undesirable loops in a network that are created by multiple active paths between hosts. Rapid Spanning Tree Protocol (RSTP) can be thought of as an enhanced STP, which gives faster convergence after a topology change. Per-VLAN Spanning Tree (PVST), on the other hand, allows for the maintaining of a spanning tree instance for every individual VLAN configured on the network.

When working with STP (802.1d), you need to know how the Root and Designated ports are selected per segment. For each link between switches (if redundant or not), you need to figure out which end of the switched link will be the Designated port. The Designated port is the one with the lowest Root Path Cost configured. When deploying STP, the first action that will take place will be the ‘selection’ of the root bridge and this is selected by finding the switch on your network with the lowest-value bridge identifier. This can also be configured statically. This should be a switching device in the center/core of your infrastructure. Once the Root Bridge is selected, the root port on all other bridges is determined. A bridge's root port is the port through which the root bridge can be reached with the shortest root path (least aggregate) cost. Once this is determined, then the Designated bridges/switches and their designated ports are determined. The Designated Bridge is the switch on each network segment that provides the minimum root path cost. A networks designated bridge/switch is the only switch on that segment that will forward frames. The networks designated port is the port that will connect directly to the Designated Bridge.

Describe how VLANs create logically separate networks and the need for routing between them.

Network segmentation
One way to enhance the efficient of a network is to have it properly segmented. There are two benefits in restricting broadcast traffic to a small local segment. First, it becomes possible to avoid wasting bandwidth. Second, network scalability is improved for broadcast-intensive protocols and applications that work by flooding out packets everywhere. In fact, there are
MANY advantages of network segmentation. They include and possibly not limited to the following:

1. When the maximum physical limitations of a network has been reached, routers can be added to it in order to create new segments and allow additional hosts to join in.
2. Segmenting the network reduces the number of hosts per network and therefore reduces the frequency of collision.
3. Dividing a big network into multiple smaller segments reduces the overflow of problems from one segment to the next.
4. Utilizing segments ensures that the internal structure of the network will not become visible from the outside world, thus making the network more secure.

**LAN Segmentation Using Routers**
It is possible to have segments interconnected by routers to enable communication between LANs while blocking other types of traffic. Routers can also be used to allow for the interconnection of disparate LAN and WAN technologies while implementing security mechanisms such as broadcast filters and logical firewalls.

**LAN Segmentation Using Switches and VLANs**
Switches work at the data link layer to enable multiple physical LAN segments to be interconnected into a single larger network. Unlike routers, which make decisions based on the layer 3 IP addresses, switches forward and flood traffic based on the layer 2 MAC addresses. LAN switches can be used to segment networks into logically defined virtual workgroups known as VLANs to enjoy substantial benefits in LAN administration, security, and management of network broadcast across the entire network. And since that communication between VLANs is mostly accomplished through routing, most traditional security and filtering functions of the Cisco routers can be deployed.
Configure, verify, and troubleshoot VLANs.

Inter-Switch Link Protocol
Under ISL, an Ethernet frame is encapsulated with a header that transports VLAN IDs between switches and routers. A 26-byte header (which includes a 10-bit VLAN ID) is pre-pended to this Ethernet frame. Note that the VLAN ID is added to the frame only when the frame is destined for a non-local foreign network.

Do note that ISL support is hardware-dependent for the Catalyst switches. Therefore, when connecting an external router to a Catalyst switch, first use one of the following commands to determine the encapsulation support per module:

- In CatOS, use `show port capabilities`
- In IOS, use `show interfaces capabilities`

VLAN troubleshooting
A VLAN consists of several end systems, all of which are members of a single logical broadcast domain. It is supported on various pieces of network equipment that support VLAN trunking protocols (VTP) between them. Therefore, problematic VTP configuration can lead to problems in the VLAN.

Before a port has 802.1q trunking turned on, it belongs to a single VLAN. When trunking is on, the port can carry traffic for many VLANs, even though it will still remember the VLAN it was in before trunking was turned on (i.e. the native VLAN). If the native VLAN on each end of the link does not match, a port will go into a Disable state due to a mismatch error (certain Catalyst switches may shut down the port if software processes inside the switch detect an error).

Another possible cause of inactive ports is when the VLAN these ports belong to have disappeared. Each port in a switch belongs to a VLAN. If that VLAN is accidentally deleted, then the port will become inactive. Some switches show a steady orange light on each inactive port. To fix the problem, simply add the VLAN back into the VLAN table.

To configure a specific VLAN, use the `vlan` command in VLAN configuration mode. To delete a VLAN, use the no form of the same command. To enter VLAN configuration mode, use the `vlan database` command under privileged EXEC mode. The `show vlan` command can be used to tell what information has been configured for the VLAN.

VLAN Trunk Protocol (VTP) can greatly reduce administration overhead in a switched network. When configuring a new VLAN on a VTP server, the VLAN is distributed through all switches in the domain, thus reducing the need to configure the same VLAN everywhere. VTP is Cisco-proprietary and is available on most of the Cisco Catalyst Family products.
VLAN Frame Tagging
VLAN switching relies primarily on frame tagging, which is a mechanism that requires traffic originating and contained within a particular virtual topology carries a unique VLAN ID as it traverses a common backbone or trunk link. The VLAN ID enables VLAN switching devices to make intelligent forwarding decisions.

Each VLAN on a network is differentiated by a "color", which is actually a VLAN identifier. The "frame coloring" of a VLAN is determined by the VLAN ID. Packets originating and contained within a particular VLAN carry the identifier that uniquely defines that VLAN.

The VLAN ID allows the VLAN switches (and routers) to selectively forward packets to ports with the same VLAN ID. The switch that receives the frame inserts the VLAN ID and the packet is switched onto the shared backbone network. When the frame exits the switched LAN, a switch strips the header and forwards the frame to the matching interfaces based on the VLAN color.

Inter-Switch Link Protocol
Under ISL, an Ethernet frame is encapsulated with a header that transports VLAN IDs between switches and routers. A 26-byte header (which includes a 10-bit VLAN ID) is pre-pended to this Ethernet frame. Note that the VLAN ID is added to the frame only when the frame is destined for a non-local foreign network.

Do note that ISL support is hardware-dependent for the Catalyst switches. Therefore, when connecting an external router to a Catalyst switch, first use one of the following commands to determine the encapsulation support per module:

- In CatOS, use `show port capabilities`
- In IOS, use `show interfaces capabilities`

VLAN troubleshooting
A VLAN consists of several end systems, all of which are members of a single logical broadcast domain. It is supported on various pieces of network equipment that support VLAN trunking.
protocols (VTP) between them. Therefore, problematic VTP configuration can lead to problems in the VLAN.

Before a port has 802.1q trunking turned on, it belongs to a single VLAN. When trunking is on, the port can carry traffic for many VLANs, even though it will still remember the VLAN it was in before trunking was turned on (i.e. the native VLAN). If the native VLAN on each end of the link does not match, a port will go into a Disable state due to a mismatch error (certain Catalyst switches may shut down the port if software processes inside the switch detect an error).

Another possible cause of inactive ports is when the VLAN these ports belong to have disappeared. Each port in a switch belongs to a VLAN. If that VLAN is accidentally deleted, then the port will become inactive. Some switches show a steady orange light on each inactive port. To fix the problem, add the VLAN back into the VLAN table.

Redundant topology eliminates single points of failure obviously, but caveats do exist. Redundant topology causes broadcast storms, multiple frame copies, and MAC address table instability problems as examples of what could happen if not configured correctly, or managed properly. In a redundant topology, multiple copies of the same frame can arrive at the intended host, potentially causing problems with the receiving protocol. Common issues resulting from a redundant topology are broadcast storms and instability in the switching tables/databases. A broadcast storm is when each switch on a redundant network floods broadcast frames with no end to the loop and an unending TTL. When you receive multiple copies of a frame arriving on different ports of a switch, you are experiencing a problem known as MAC table or MAC database instability.

**Configure, verify, and troubleshoot trunking on Cisco switches.**

With VLAN trunking, one single network adapter may behave as a number of virtual adapters (the theoretical limit is 4,096 but a limit of 1,000 is advised for practicality purposes).

**NOTE:** For VLAN Trunking to work the network switch, network adapter, and OS, drivers must support VLAN tagging.

IOS based Cisco gear that support trunking include:

- The 2900 Series
- The 2948 (Non L3)
- The 2950 Series
- The 3548
- The 3550 Series
- The 6500
Don’t worry about the CatOS counterparts. The exam does not really care too much about the CatOS based gears.

The two most important commands for setting trunking on IOS based switches are:

- **Switchport mode trunk** allows for the setting of the port to trunking mode.
- **Switchport trunk encapsulation dot1q** allows for the setting of the trunk type to 802.1q (if having to choose between ISL or 802.1q).

**Configure, verify, and troubleshoot interVLAN routing.**

When a host in one VLAN has to communicate with a host in another VLAN, the traffic needs to be routed. If routing it through the Catalyst switches, create Layer 3 interfaces (known as Switch virtual interfaces SVI) on them. On these switches the VLAN interfaces must be configured with valid IP address. When one switch receives a packet heading for another VLAN, this switch will look into the routing table to determine how to proceed with forwarding the packet. The packet is then passed accordingly.

To troubleshoot, first verify that there is Layer 2 connectivity. Initiate a ping from a host to the switch's corresponding VLAN interface. Next, initiate a ping to the VLAN interface on another VLAN. This is to verify that the switch does properly route between VL ANs. Then, initiate a ping from one VLAN to the destination in another VLAN.

If connectivity problem arises, verify that the default route on the switch does point to the correct "default gateway". Also remember to verify that the corresponding IP address and subnet mask on the switch have been correctly configured.
Configure, verify, and troubleshoot VTP.
A VTP domain is made up of one or more interconnected switches that share the same VTP domain name. Possible VTP modes include Server, Client, and Transparent.

A switch in the VTP domain sends periodic advertisements out each trunk port. These advertisements are received by neighboring switches for updating the VTP and VLAN configurations. VTP pruning may reduce network bandwidth use by cutting down unnecessary flooded traffic, including broadcast, multicast, unknown, and flooded unicast packets.

There are 2 possible methods that can be used to configure VTP. Configuration through the global configuration mode method is not available in earlier Catalyst switches running IOS, so a better option may be to do it through the database mode. First, enter VLAN configuration mode via the command `vlan database`. Then, set the VTP domain name via `vtp mode {client | server | transparent}`.

Note that all switches involved should have the same the VTP domain name, and that all switches in the concerned VTP domain must run the same VTP version, via matching VTP password. Also note that VTP version 2 is disabled by default on version 2-capable switches.

NOTE: You should always take certain precautions when working on a production network. Any changes you make could impact the current network and halt production. When redeploying an older switch to a new VTP domain in your network you should always take steps to verify that the VTP revision number is lower than the existing domain otherwise the current VTP domain information may be overwritten with that of the older switch. If they do not match, then you will impact the VTP service on the current switched infrastructure.

In order to display the relevant VLAN configuration information such as VLAN ID, name, and so forth, use the `show vlan` command. VTP information, such as mode, domain, and so forth, can be displayed via the `show vtp status` command. Do not panic if the VLAN information and the VTP information are not displayed through `show running-config` when the switch is in VTP server/client mode, as this is a normal behavior. Also ensure that either no password is set between the server and client, or that the password is identically set on both sides.

NOTE: VTP version 2 includes supports for Token Ring LAN switching and VLANs, Unrecognized Type-Length-Value (TLV), Version-Dependent Transparent Mode and Consistency Checks.
Configure, verify, and troubleshoot RSTP operation.
RSTP will assign a port role to the individual ports. A root port provides the best path when the involved switch is forwarding packets to the root switch. A designated port refers to the port through which a designated switch is attached to the network. An alternate port provides an alternate path toward the root switch, while a backup port serves as a backup for the path offered by the designated port. A disabled port has no role at all within the entire operation.

For purpose of the exam, understand the following key points:

- RSTP allows for rapid convergence of the spanning tree. MSTP (Multiple STP) makes use of RSTP for providing rapid convergence, thus enabling multiple VLANs to be grouped into one spanning tree instance.
- Per-VLAN RSTP is not supported.
- For multiple switches to be maintained in the same MST region, they must be equipped with the same VLAN-to-instance mapping. Use spanning-tree mst configuration to enter into the MST configuration mode. Use spanning-tree mode mst to enable MST, which would also automatically enable RSTP.

NOTE: When working with Rapid Spanning Tree Protocol (RSTP), or also known as IEEE 802.1w, you need to know the differences between standard STP and RSTP. With STP (802.1d), there may be lag time to get the topology converged because of the main port roles in which a port may go through – such as blocking, listening, learning and so on. With RSTP, the process has been shortened and made quicker in order to bring a port back up in less than a minute, where with 802.1d, the port could have remained inactive (or unusable) for a period of a minute or more. With RSTP, the two port roles included in the active topology are ‘root’ and ‘designated’.

Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network.

Troubleshooting in general
Use the show commands to monitor switch behavior during initial installation; to monitor normal network operation; to isolate problem interfaces, nodes, media, or applications; to determine when a network is congested; and to determine the status of servers, clients, or other neighbors.

The debug commands can be used to provide a wealth of information about the traffic on an interface, error messages generated by nodes on the network, protocol-specific diagnostic packets and cells, and other useful troubleshooting data.
NOTE: Many debug commands are processor intensive and can cause serious network problems if they are running on an already heavily loaded switch.

Keep in mind, when troubleshooting a network environment, the recommended approach is to first define the specific symptoms, then identify all potential problems that could be causing the symptoms, and systematically eliminate each potential problem until the symptoms disappear.

The show interfaces command can be used to display statistics for all interfaces configured. The resulting output varies depending on the network for which an interface has been configured.

Below is a portion of the sample output from the show interfaces command:

```
Router# show interfaces

Ethernet 0 is up, line protocol is up
Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
Internet address is 131.108.28.8, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 4:00:00
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters 0:00:00
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 2000 bits/sec, 4 packets/sec
  1127576 packets input, 447251251 bytes, 0 no buffer
  Received 354125 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  5332142 packets output, 496316039 bytes, 0 underruns
  0 output errors, 432 collisions, 0 interface resets, 0 restarts
---More---
```

Use SHOW IP PROTOCOLS to display the parameters and current state of the active routing protocol process. The information displayed can be very useful in debugging routing operations. In particular, information in the Routing Information Sources field of the output can help identify a router suspected of delivering bad routing information.

Use SHOW IP ROUTE to display the current state of the routing table. If you specify that you want information about a specific network displayed (by specifying an address after the command, such as show ip route 10.0.0.1), more detailed statistics can be obtained.

It is also possible to use the debug commands only during non-peak hours. The debug commands are highly processor intensive. They can slow things down almost to a halt.
**Implement basic switch security (including: port security, unassigned ports, trunk access, etc.)**

Security is increasingly gaining attention, especially when modern networks are known to have much vulnerability. A penetration test may come to the rescue. It involves the use of various methods for evaluating the security of a computer or a network by simulating an actual attack. The process involves a thorough analysis of weaknesses or vulnerabilities as carried out from the perspective of a serious attacker. Any security issues that are found will then be addressed for considering mitigation or technical solution. This type of assessment is necessary, especially on computer about to be deployed in a hostile environment.

When dealing with switch security, attention is actually focused on layer 2. Why is it necessary to care about layer 2 security? Generally speaking, layer 3 has the primary responsibility of sending data packets from the source network to the destination network using a pre-specified routing method. Because threats from the internet are IP based, filtering at layer 3 is what has to be done to safeguard against these threats. However, once entered into the private network, traffics are processed through switches at layer 2. And in fact there could be threats from inside the private network (internal threat that is). Therefore, layer 2 security is a topic that deserves serious attention.

Port security could be the best tool against spoofing attacks. The port security feature of the Catalyst switch can restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. When secure MAC addresses are assigned to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. On the other hand, if assigning a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.

On a port that is configured as a secure port, when the maximum number of secure MAC addresses is reached and when the MAC address of a workstation attempting to access that port is different from the identified secure MAC addresses, a security violation occurs. It is possible to configure the interface to take actions against any of these violations. The available options are primarily Restrict and Shutdown.

Broadcast suppression may also be of great use against attacks that aim at flooding the network. This feature refers to the use of filtering techniques to measures broadcast activity in a subnet over a one-second interval and compares the measurement with a predefined threshold. If the threshold is reached, further broadcast activity is suppressed for the duration of the interval.

**NOTE:** When you want to configure port security, you need to use the `switchport port-security` command. If you want to restrict the amount of users (or connections) to a specific port, you need to add more to the command. In order to restrict a port to a maximum of 10 connections, you need to use the `switchport port-security maximum 10` command.