CCNA Practice Assignment
Assignment # 1

By: Engr. Gul Raeez Gushan
**Course: CCNA Part I**

Lab 1: Configuring standard VLANs on Catalyst Switches

Lab Objective:
The objective of this lab exercise is for you to learn and understand how to configure standard VLANs 1-1001 on Cisco Catalyst IOS switches. In addition to this, you are also required to familiarize yourself with the commands available in Cisco IOS to validate and check your configurations.

Lab Topology:
Please use the following topology to complete this lab exercise:
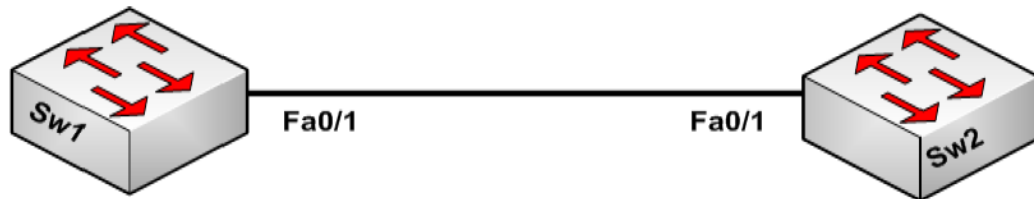
VLAN Number	VLAN Name	Port
10	SALES	FastEthernet0/5
20	MANAGERS	FastEthernet0/6
30	ENGINEERS	FastEthernet0/7
40	SUPPORT	FastEthernet0/8

Task 1:
In preparation for VLAN configuration, configure a hostname on Sw1 as well as the VLANs depicted in the topology.

Task 2:
Configure ports FastEthernet0/5 – FastEthernet0/8 as access ports and assign them to the VLANs specified.

Task 3:
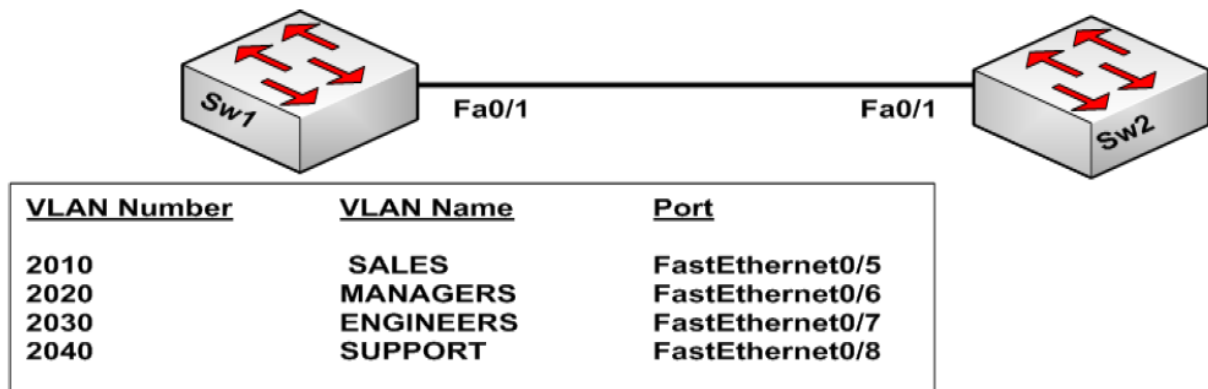Verify your VLAN configuration using relevant show commands in Cisco IOS.

Lab 2: Configuring extended VLANs on Catalyst Switches

Lab Objective:
The objective of this lab exercise is for you to learn and understand how to configure extended VLANs 1006-4096 on Cisco Catalyst IOS switches. In addition to this, you are also required to familiarize yourself with the commands available in Cisco IOS to validate and check your configurations.

Lab Topology:
Please use the following topology to complete this lab exercise:

VLAN Number	VLAN Name	Port
2010	SALES	FastEthernet0/5
2020	MANAGERS	FastEthernet0/6
2030	ENGINEERS	FastEthernet0/7
2040	SUPPORT	FastEthernet0/8

Task 1:
In preparation for VLAN configuration, configure a hostname on Sw1 as well as the VLANs depicted in the topology. Keep in mind that extended VLANs can only be configured on a switch in VTP Transparent mode.

Task 2:
Configure ports FastEthernet0/5 – FastEthernet0/8 as access ports and assign them to the VLANs specified.

Task 3:
Verify your VLAN configuration

Lab 3: Configuring VTP Clients and Servers on Catalyst Switches

Lab Objective:
The objective of this lab exercise is for you to learn and understand how to configure VTP Server and Client mode on Cisco Catalyst switches. By default, all Cisco switches are VTP Server devices.

Lab Purpose:
VTP Client and Server mode configuration is a fundamental skill. VLANs are configured on VTP Servers and VTP Clients receive VLAN information from the VTP Servers in the same VTP domain. VLAN sharing is possible by using a trunk between the switches.

Lab Topology:
Please use the following topology to complete this lab exercise:
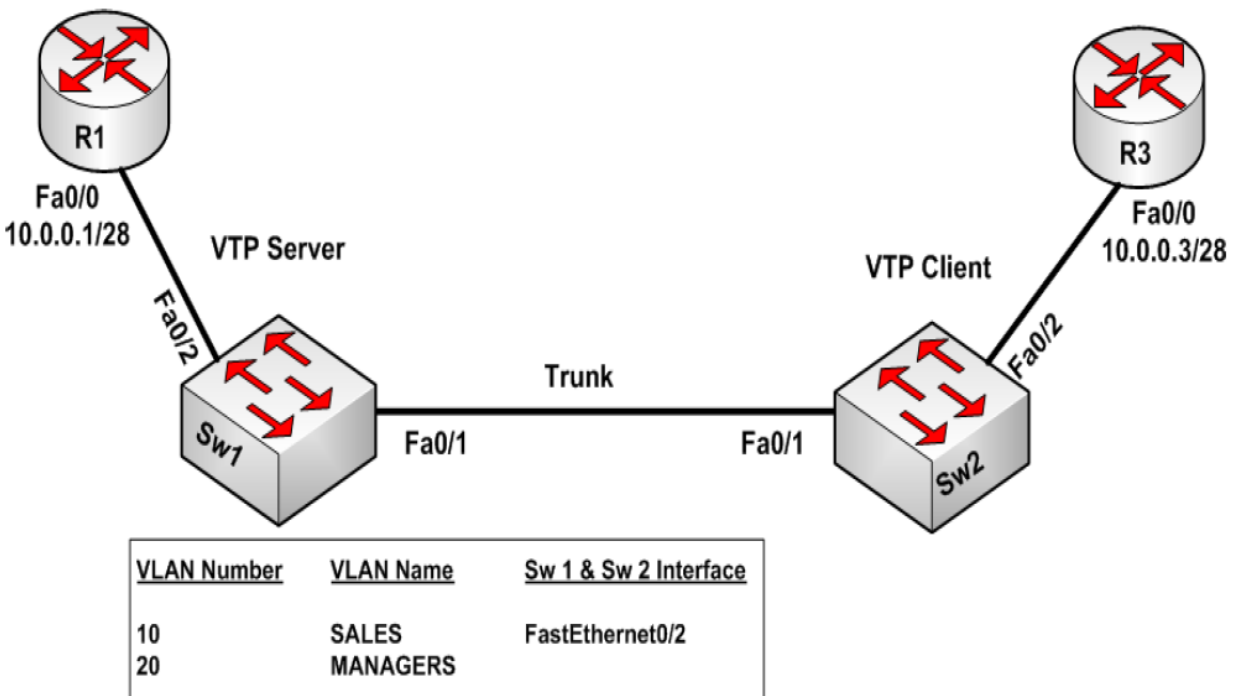
VLAN Number	VLAN Name	Sw 1 & Sw 2 Interface
10	SALES	FastEthernet0/2
20	MANAGERS	

Task 1:
In preparation for VLAN configuration, configure a hostname on Sw1 as well as the VLANs depicted in the topology. Keep in mind that the default mode of operation of Cisco Catalyst switches is VTP Server mode.

Task 2:
Configure and verify Sw1 as a VTP Server switch and configure Sw2 as a VTP Client switch. Both switches should be in the VTP domain named CISCO.

Task 3:
Configure and verify FastEthernet0/1 between Sw1 and Sw2 as an 802.1q trunk

Task 4:
Configure and verify VLANs 10 and 20 on Sw1 with the names provided above. Assign FastEthernet0/2 on both Sw1 and Sw2 to VLAN 10. This interface should be configured as an access port.

Task 5:
Configure R1 and R3 FastEthernet0/0 interfaces with the IP addresses 10.0.0.1/28 and 10.0.0.3/28 respectively. Test connectivity via your VLANs by pinging R1 from R3 and vice versa.

Lab 4: Configuring VTP Transparent Mode

Lab Objective:
The objective of this lab exercise is for you to learn and understand how to configure VTP Transparent mode on Cisco Catalyst switches. By default, all Cisco switches are VTP Server devices.

Lab Purpose:
VTP Transparent mode configuration is a fundamental skill. VLANs configured on a switch in VTP Transparent mode are not automatically propagated to other switches within the same VTP domain as would be done by a VTP Server. Switches configured in VTP Transparent mode use a trunk to forward traffic for configured VLANs to other switches.

Lab Topology:
Please use the following topology to complete this lab exercise:
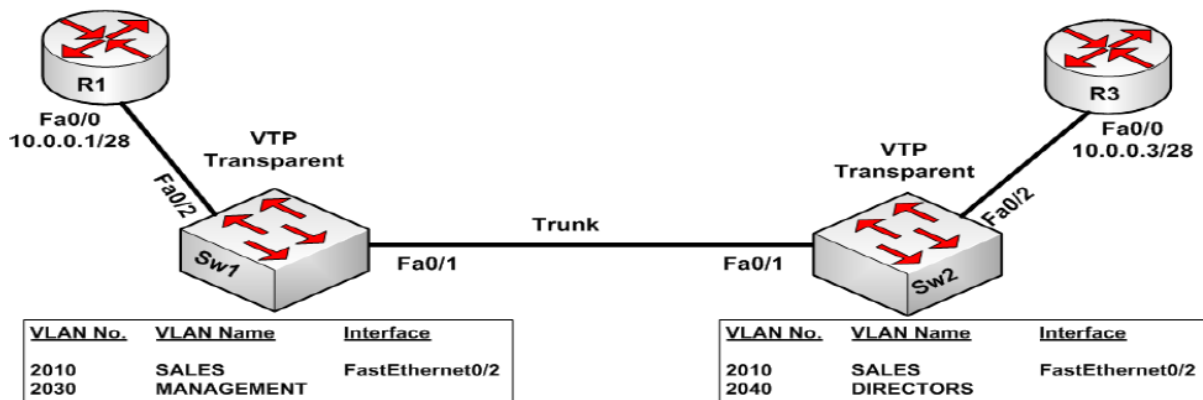
Task 1:
In preparation for VLAN configuration, configure a hostname on switches 1 and 2 and routers 1 and 3 as illustrated in the topology.

Task 2:
Configure and verify Sw1 and Sw2 in VTP Transparent mode. Both switches should be in the VTP domain named CISCO. Remember that switches must be in the same VTP domain to share VLAN information via a trunk.

Task 3:
Configure and verify FastEthernet0/1 between Sw1 and Sw2 as an 802.1q trunk.

Task 4:
Configure and verify VLANs 2010 and 2030 on Sw1 with the names provided above. Assign FastEthernet0/2 on Sw1 to VLAN 2010 as an access port. Configure and verify VLANs 2010 and 2040 on Sw2 with the names provided above. Assign FastEthernet0/2 on Sw2 to VLAN 2010 as an access port.

Task 5:
Configure R1 and R3 FastEthernet interfaces with the IP addresses 10.0.0.1/28 and 10.0.0.3/28 respectively. Test VLAN connectivity by pinging between R1 and R3.
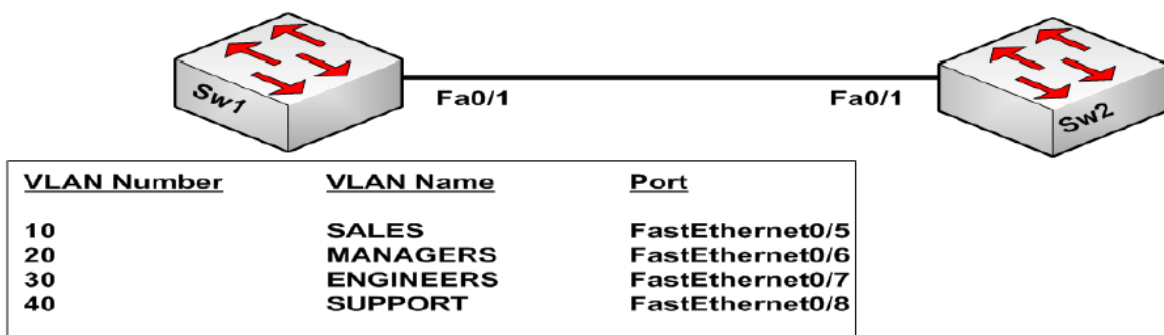
Lab 5: Securing VTP Domains

Lab Objective:
The objective of this lab exercise is for you to learn and understand how to secure VTP domains using Cisco Catalyst switches. By default, VTP domains are not password-protected.

Lab Purpose:
Securing the VTP domain is a fundamental skill. When VTP domains are not configured with a password, rogue switches can be added to the network and disrupt service.

Lab Topology:
Please use the following topology to complete this lab exercise:

VLAN Number	VLAN Name	Port
10	SALES	FastEthernet0/5
20	MANAGERS	FastEthernet0/6
30	ENGINEERS	FastEthernet0/7
40	SUPPORT	FastEthernet0/8

Task 1:
In preparation for VLAN configuration, configure a hostname on Sw1 and as depicted in the topology.

Task 2:
Configure and verify Sw1 as a VTP Server switch and configure Sw2 as a VTP Client switch. Both switches should be in the VTP domain named CISCO. Secure VTP messages with the VTP password CISCO.

Task 3:
Configure and verify FastEthernet0/1 between Sw1 and Sw2 as an 802.1q trunk.

Task 4:
Configure and verify VLANs 10 and 20 on Sw1 with the names provided above. Validate that these VLANs are still propagated to Sw2 after VTP has been secured.