CCNP

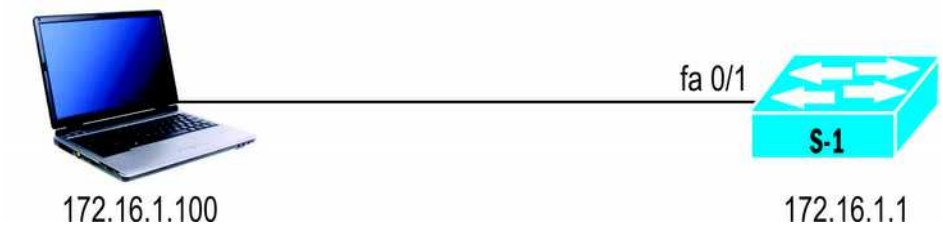
SWITCHING
LAB MANUAL

WWW.IPSOFTWARESOLUTIONS.COM

CONTENTS

SCENARIO - 1 BASIC CONFIGURATION

TOPOLOGY DIAGRAM



OBJECTIVES:

This Lab topology would make the student understand the following concepts.

1. Logging into a switch
2. Mode type and changes.
3. Switch Port Properties.
4. Assigning the switch IP address
5. Switching Password

LAB EXERCISES:

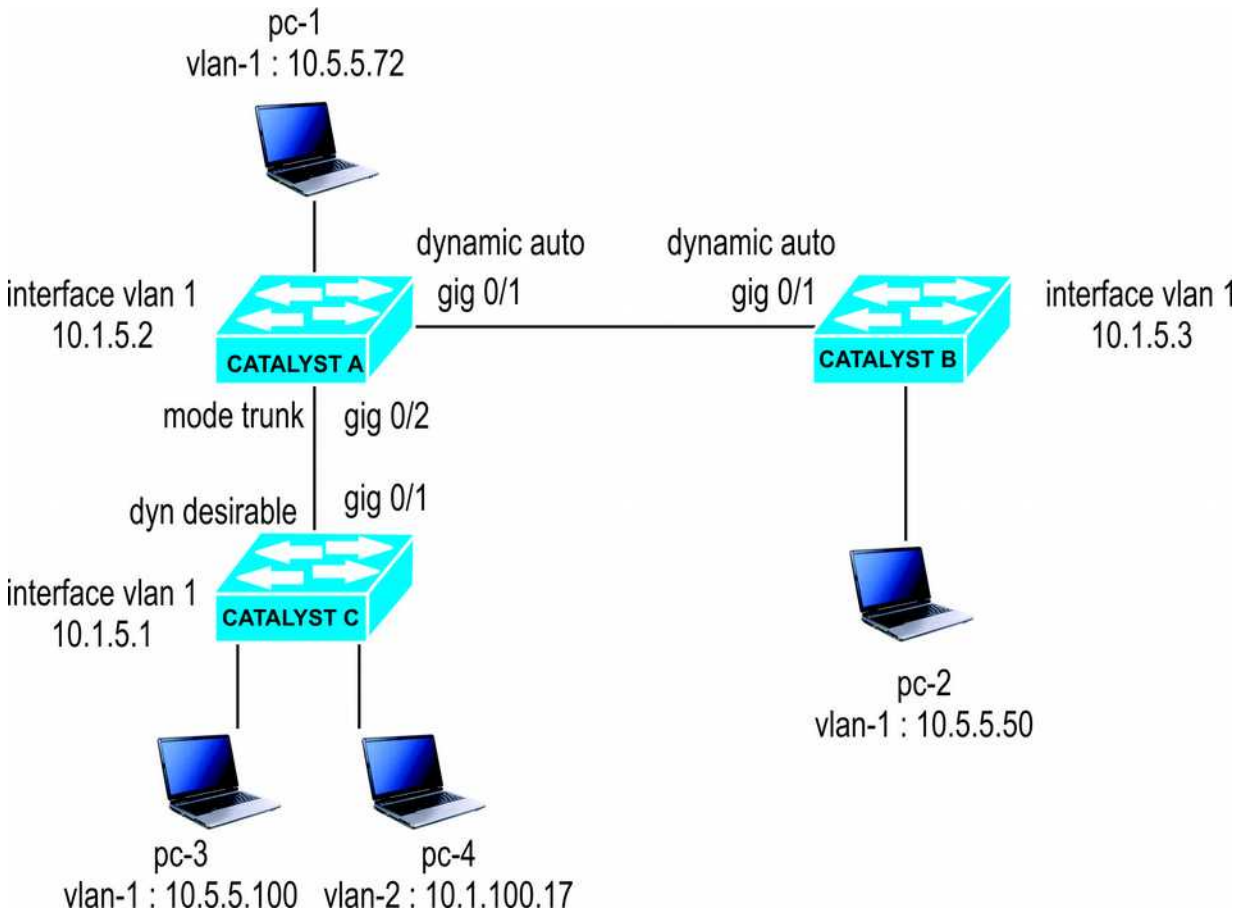
1. Changing the Switch Hostname.
2. Port characteristics
3. Assigning the switch Password
4. Setting Enable / Line / Console password
5. Setting Password and Local authorization.

COMMANDS:

# configure terminal	# Enable
# disable	# Hostname
# no hostname	# interface fast fastEthernet 0/1
# Interface fastEthernet 0/1	# shutdown
# No shutdown	# ip address
# Ip default-gateway A.B.C.D# show running-config	
# Show interface fastEthernet 0/1	# show interface fastEthernet 0/23
# Show ip interface brief	# show version
# end	# show flash
# show mac address-table	# show mac address-table count
# show mac address-tabel dynamic interface fastEthernet 0/0	
# show platform tcam utilization	# enable password
# login local	# password
# username u1 password p1	# line console 0 / vty 0 4

SCENARIO – 2 TRUNKING AND DTP

TOPOLOGY DIAGRAM



OBJECTIVE:

This scenario is built around a network of switches connected by trunking links. You need to think about how DTP operates and trunks are negotiated (or not) between switches. Consider the network shown in Figure and answer the questions that follow. Assume that all switches shown support DTP.

1. What is the mode of the link between Catalyst A and Catalyst B?
2. Suppose That the network administrator types these commands for interface Gigabit Ethernet 0/1 on Catalyst B:

   Switch (config) # interface gigabit ethernet 0/1
   Switch (config-if) # switchport trunk encapsulation dot1q
   Switch (config-if) # switchport mode trunk
   Switch (config-if) # switchport nonegotiate

   What will be link mode be now?
3. Catalyst B has been given the command no switchport nonnegotiate for interface fastethernet 0/1 What will the link mode be now?
4. What is the mode of the link between Catalyst A and Catalyst C?

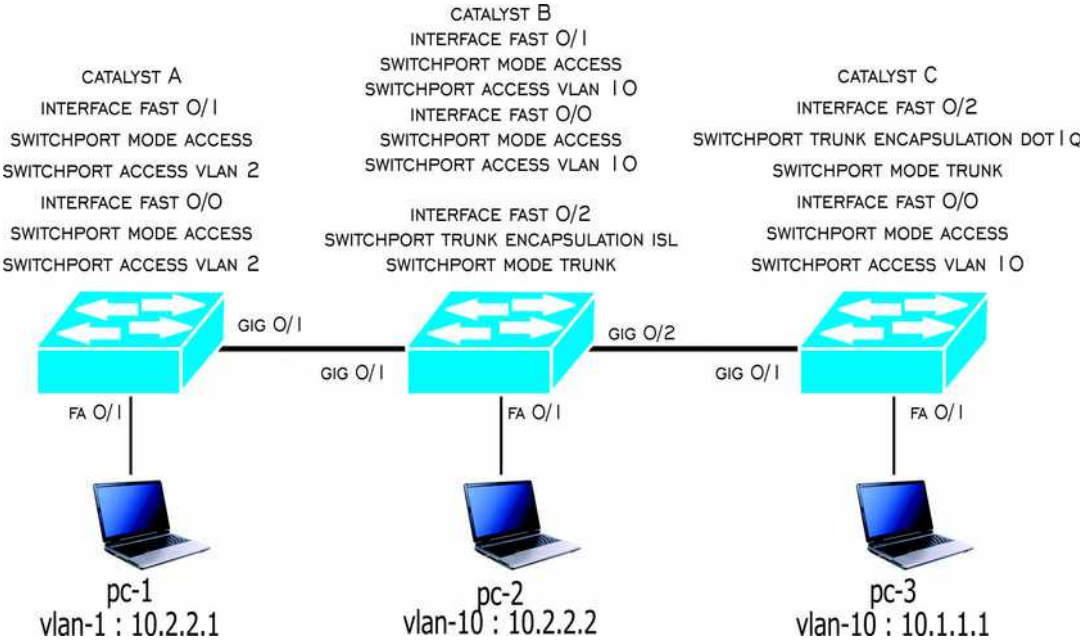
5. Assume that all links between Catalyst switches are in trunking mode, transporting VLANs 1 through 1005. Can PC-2 ping PC-4?
6. Suppose that PC-1 begins to generate a broadcast storm. Where would the effects of this storm be experienced in this network? Consider both devices and links. Will PC-4 receive the broadcast
7. VLAN Configuration
8. Verification of MAC Address
9. Understanding the concept of DTP and Trunk Ports.
10. DTP Modes and Types
11. DTP Negotiation.

COMMANDS:

Show mac-address-table
show cdp neighbor
show run interface fastethernet 0/1
interface fastethernet 0/1
description sales_department
vlan 10
switchport mode access
switchport access vlan 10
show vlan
switchport trunk encapsulation
switchport trunk allowed vlan
switchport mode [trunk | dynamic {desirable | auto}]
show interface fastethernet 0/1 switchport

SCENARIO – 3 VLANS, TRUNKING AND VTP

TOPOLOGY DIAGRAM



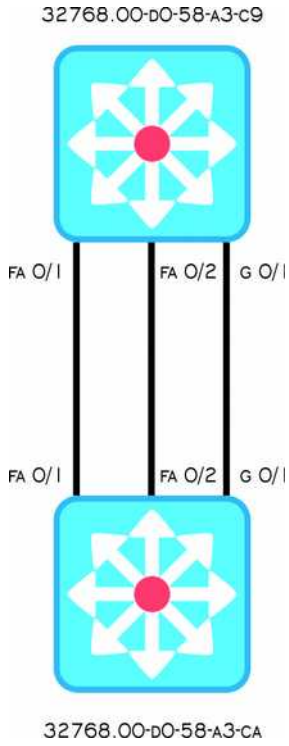
OBJECTIVE:

This scenario is designed to understand about VLAN and Trunking connectivity. See the diagram shown in figure and answer the questions that follow. The configurations of the three Catalyst switches are shown above them.

1. PC-1 and PC-2 both are configured with IP addresses on the same subnet. Notice that each PC connects to a different VLAN number. Given the switch configurations shown, can PC-1 ping PC-2?
2. PC-2 and PC-3 are assigned to the same IP subnet (using subnet mask 255.0.0.0) and the same VLAN. Can PC-2 and PC -3 ping each other?
3. Will the trunk link between Catalyst C come up successfully?
4. Suppose that the trunk between Catalyst B and Catalyst C is configured properly. Where will VLAN 1 be pruned? Why?
5. Suppose that Catalyst A is a VTP server, Catalyst C is a VTP client, and Catalyst B is configured for VTP transparent mode. All switches are in the Bermuda management domain. If VLAN 14 is created on Catalyst A, Which switches also will create VLAN 14 using VTP?
6. If VLAN 15 is created on Catalyst B, What other switches also will create VLAN 15 through VTP?
7. If VLAN 16 is created on Catalyst C what will happen?

SCENARIO - 4 TRADITIONAL STP

TOPOLOGY DIAGRAM



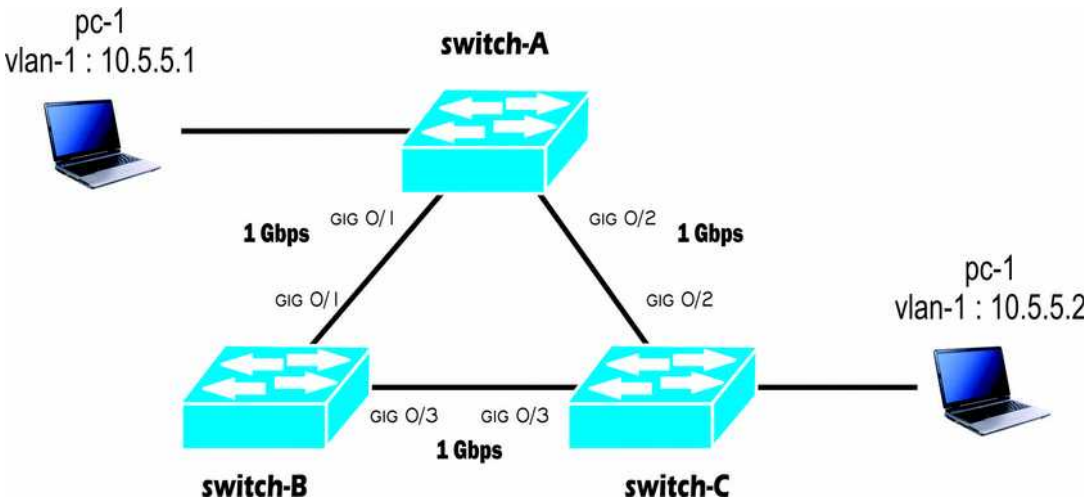
OBJECTIVE:

This scenario exercises the Spanning Tree Protocol operation. This keeps the STP complexity to a minimum while forcing you to think through the STP convergence process on a live network. Given the network diagram shown in Figure complete the following exercises.

1. Manually compute the spanning –tree topology. Note which the root bridge is, which ports are root ports and designated ports, and which ports are in the Blocking state.
2. If the 100-Mbps link (port Fast Ethernet 1/2) is disconnected, what happens with the STP?
3. If the 1000-Mbps link (port Gigabit Ethernet 2/1) is disconnected, how much time will elapse before the two switches can communicate again? (Assume that both switches use the default STP timer values and no additional features for faster convergence.)
4. Assume that the physical 1000-Mbps link (port Gigabit Ethernet 0/1) stays up and active, but BPDUs are not allowed to pass (that is, an access list filter is blocking BPDUS) what happens and when?

SCENARIO – 5 STP CONVERGENCES

TOPOLOGY DIAGRAM



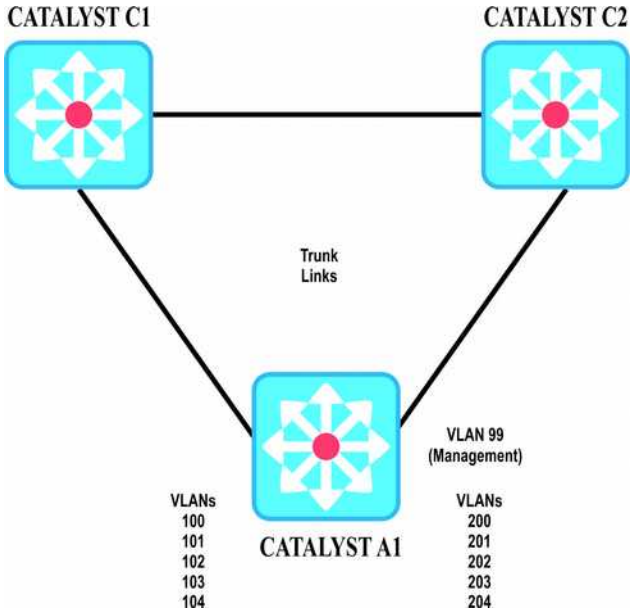
OBJECTIVE:

This scenario exercises the Spanning Tree Protocol operation. This keeps the STP complexity to a minimum while forcing you to think through the STP convergence process on a live network.

1. Turning the Root Path Cost
2. Tuning the Port ID
3. Tuning the STP Convergence
   Modifying the STP Timers
4. Redundant Link convergence
   PortFast
   UplinkFast
   BackboneFast

SCENARIO - 6 ADVANCED STP

TOPOLOGY DIAGRAM



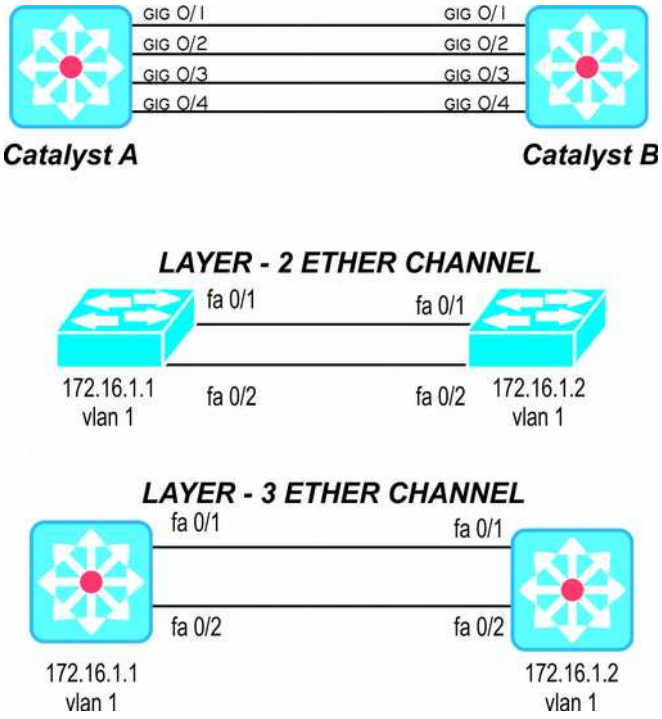
OBJECTIVE:

A small network consists of two core switches, Catalyst C1 and C2, and access switch, A1, as shown in figure. Advanced Spanning Tree Protocol features will improve the convergence times and reduce the number of STP instances. Answer these questions.

1. To prevent the possibility of a unidirectional link occurring on switch A1 uplinks, what switch feature can be used? What commands are necessary to enable this feature? Assume that the links should be disabled if a unidirectional condition is found. Which switches need to be configured this way?
2. On Catalyst A1, what feature and command should be used to prevent unexpected STP BPDUs from being received on the ports connected to end users?
3. For the links between switch A1 and the user PCs, what command is needed to configure these as RSTP edge ports?
4. By default, the traditional PVST+ mode is enabled on a switch. What command can be used to enable RSTP to use with PVST+?
5. Suppose that MST is to be configured to reduce the number of STP instances because 12 unique VLANs are being used across the network. How many MST instances are needed for the three switches shown in Figure, assuming that traffic should be load-balanced across the two uplinks of switch A1?
6. What commands are needed to configure switch C1 for MST?
7. Now make sure that C1 is configured as the root bridge for one MST instance. What commands are needed?

SCENARIO - 7 ETHERCHANNELS

TOPOLOGY DIAGRAM



OBJECTIVE:

This scenario focuses on EtherChannel links between switches. See the diagram shown in Figure and answer the questions that follow.

1. Four Gigabit Ethernet interfaces on Catalyst A are to be bundled in to a Gigabit Ether Channel with Catalyst B. if each of these interfaces also is configured as the trunk, what next be similar about these switches?
2. Catalyst A should actively initiate an Ether Channel with catalyst B. PAgP negotiation should be used. What commands should be used on each of Catalyst A, ports to configure negotiation of Ether Channel 1?
3. What is the default load distribution algorithm, assuming that the switches are Catalyst 6500s?
4. Suppose that the Ether Channel is a Layer 3 interface on both switches so that each switch uses one MAC and one IP address. Should you choose the **src- dst mac** or **src- dst- ip** algorithm to maximize the load distribution across all the links?

LAB EXERCISES:

1. Aggregating Switch Links.
2. Switch port aggregation with EtherChannel
3. Configuration of EtherChannel.
4. EtherChannel Negotiation Protocol.
5. Troubleshooting an EtherChannel.
6. Configuration of Layer-2 and Layer-3 EtherChannel.
7. Configuration of EtherChannel Load Balancing.
8. Configuration of EtherChannel Group.
9. Verification of EtherChannel.

COMMANDS:

interface range fastethernet

channel-protocol pagp

channel-group 1 mode desirable

show ip interface brief

show etherchannel 1 port

show etherchannel 1 detail

int port-channel 1

ip address 10.1.1.1 255.255.255.0

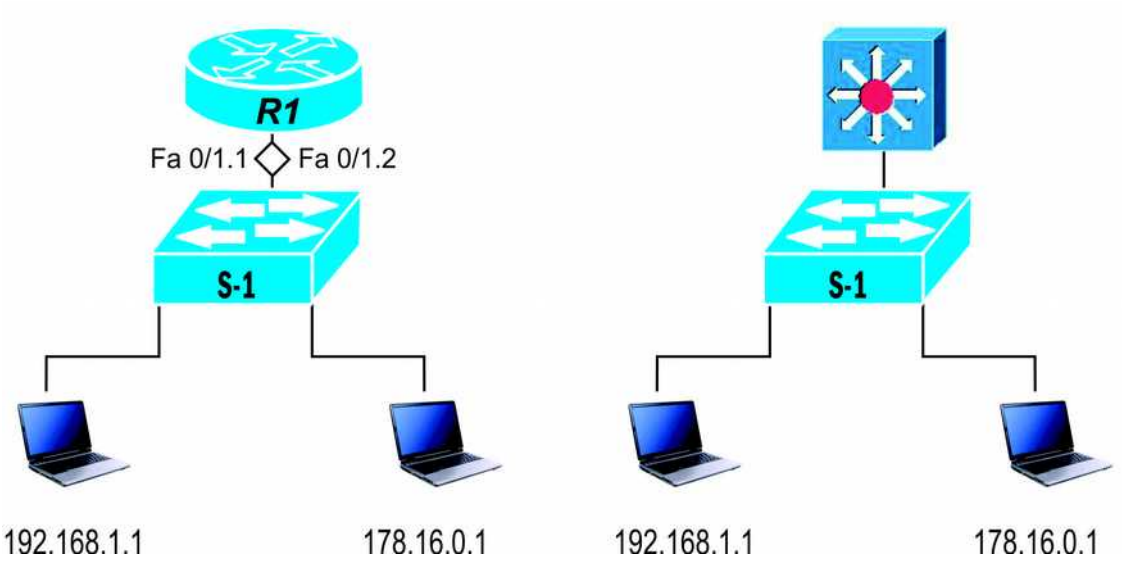
interface range fastethernet

channel-group 1 mode desirable

no switchport

SCENARIO – 8 INTER VLAN ROUTING

TOPOLOGY DIAGRAM



OBJECTIVES:

This Lab topology would make the student understand the following concepts.

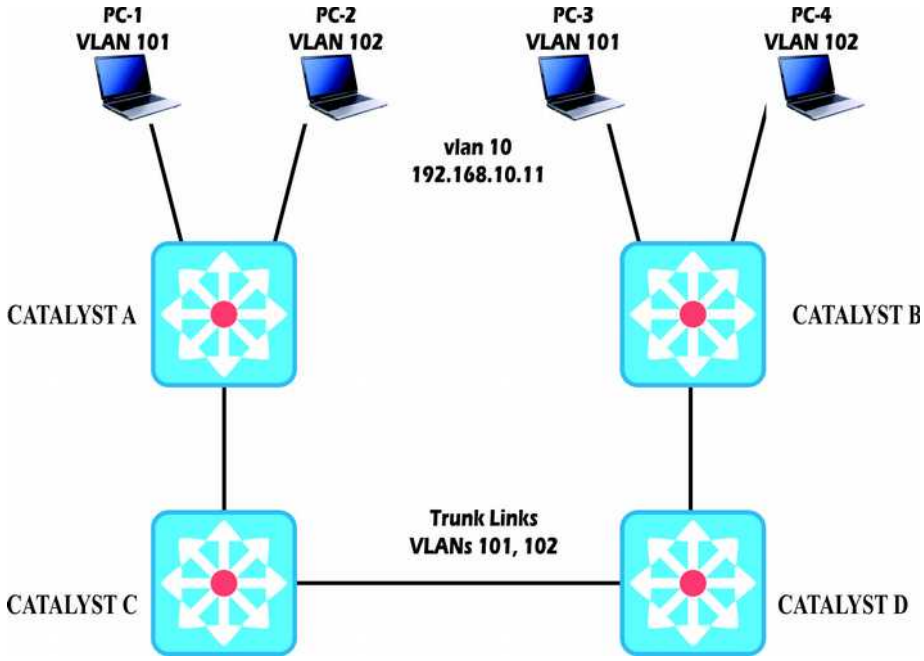
1. Inter VLAN Routing
2. SVI-Switched Virtual Interface
3. Configure Inter-VLAN Routing
4. Layer 2 Port Configuration
5. Layer 3 Port Configuration
6. IPv6 Configuration

COMMANDS:

Show mac-address table
Vlan <number> name <name of the Vlan>
Show interface fastethernet 0/20 switchport
No switchport
interface vlan 10
ip add 10.0.0.1 255.0.0.0
no shutdown
interface vlan 20
ip add 20.0.0.1 255.0.0.0
no shutdown
ip routing
show ip route
Show interface fastethernet 0/20 switchport

SCENARIO - 9 MULTICAST

TOPOLOGY DIAGRAM



OBJECTIVE:

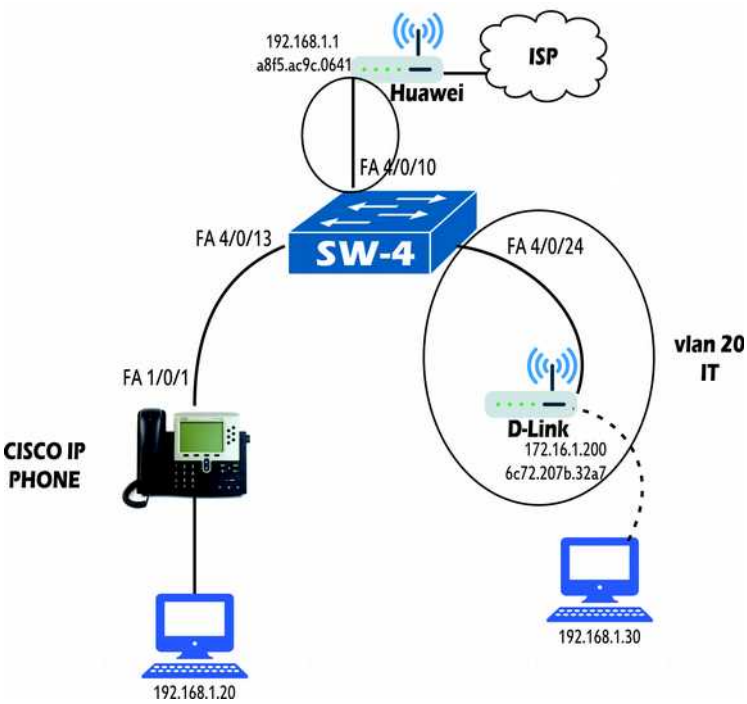
This scenario tests your knowledge of various multicast switching feature. Think about how multicast traffic traverses a network and how switches can be configure to participate in building multicast topologies. Then consider how you can switches to limit the forwarding of unnecessary multicast traffic.

1. Under what conditions is IGMP snooping more suitable then CGMP for handling multicast traffic?
2. Figure shows a network diagram. Assume that all switches use the default multicast configurations. Where in the network will multicast traffic originating from PC-1 on Catalyst A (VLAN 101) be seen?
3. What configuration is needed on Catalysts C and D to limit multicast traffic to only those ports that explicitly join multicast groups, using CGMP with PIM dense mode? Assume that this is needed on both VLANs 101 and 102. What configuration is needed on Catalysts A and B, which are not capable of IGMP snooping?

SCENARIO - 10

IP TELEPHONY IN A SWITCHED NETWORK

TOPOLOGY DIAGRAM



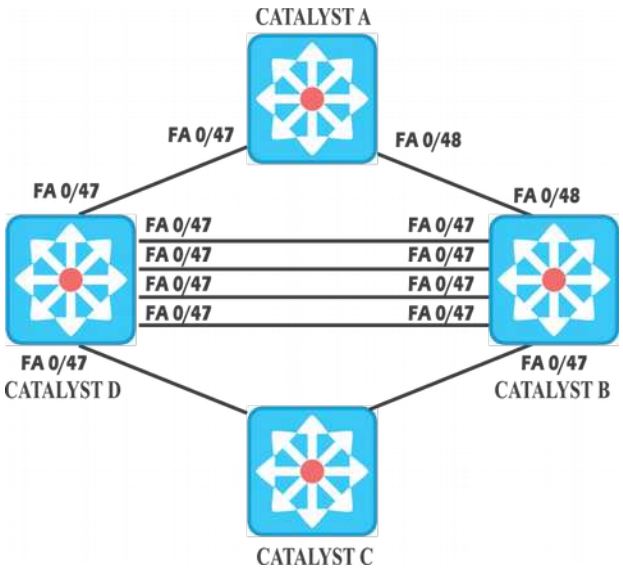
OBJECTIVE:

This scenario uses a simple two- switch network to reinforce the concepts needed to properly implement IP telephony. Think about supplying power to the Cisco IP phone, as well as how to implement Qos trust within this network. Use Figure as a reference for the following questions.

1. Assume that Catalyst supports Power over Ethernet. If interface Fa1/0/1 has its default configuration, will power be supplied to the IP Phone? Now suppose that someone has entered the power inline never command for that interface. What command could you use to begin supplying power to the phone dynamically?
2. Where a QoS trust boundary should be implemented? In other worlds, which switches should trust incoming QoS information and which ones should not?
3. One catalyst , configure interface fast Ethernet 3/1 to inform the IP phone to use VLAN 17 for voice traffic. Also add a configuration command to ensure that on QoS trust is extended to the IP Phone‘s PC date port.
4. What configuration commands would be necessary to enable QoS trust on Catalyst B’s Gig 1/0/1 uplink and to disable trust on port Fa 1/0/2 where the user PC is connected?

SCENARIO - 11 DHCP

TOPOLOGY DIAGRAM



OBJECTIVES:

This Lab topology would make the student understand the following concepts.

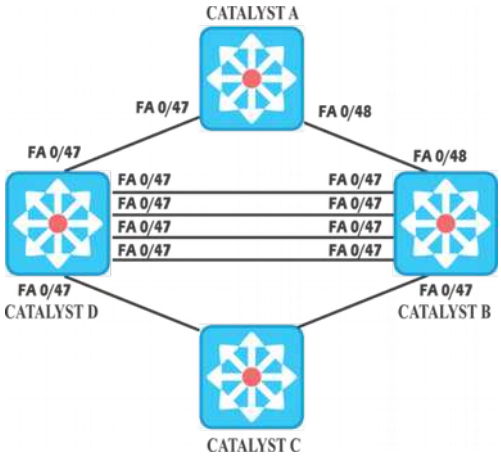
1. Overview of the DHCP Server
2. DHCP Attribute Inheritance
3. Excluding IP Addresses
4. Configuring DHCP Address Pools
5. Troubleshooting Tips

COMMANDS:

Switch - 1 # interface vlan 10 # ip address 10.0.0.1 255.0.0.0 # no shutdown # ip dhcp exclude-address 10.0.0.2 10.0.0.5 # ip dhcp pool tendauser # network 10.0.0.0 255.0.0.0 Switch-1 Client Identifier # host 10.0.0.6 255.0.0.0 # client – identifier 000.000.001 Verification and Troubleshoot # debug ip dhcp server # Show ip dhcp binding # Clear ip dhcp binding	Switch - 4 # ipv6 dhcp pool beetel # address prefix 2001::1/64 # dns-server 2001::10 # domain-name cisco.com #exit # interface vlan 20 # ipv6 address 2001::1/64 # ipv6 dhcp server beetel # no shutdown Verification and Troubleshoot # debug ipv6 dhcp server # Show ipv6 dhcp binding # Clear ipv6 dhcp binding

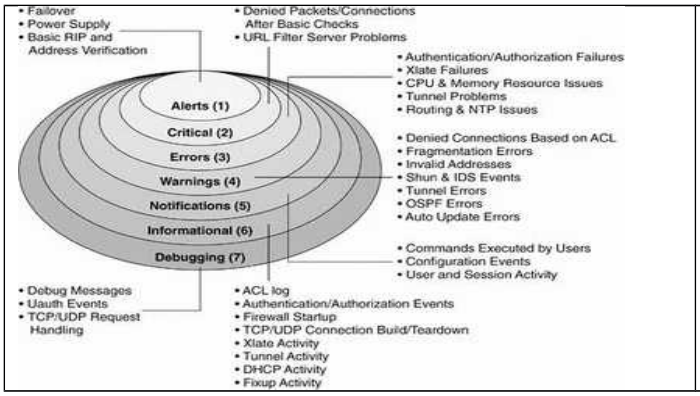
SCENARIO - 12 SYSLOG

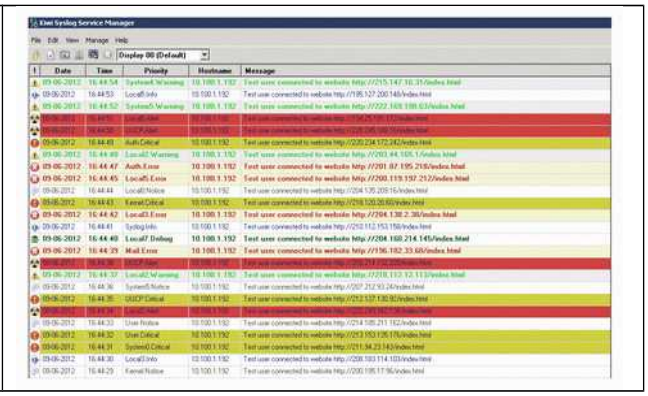
TOPOLOGY DIAGRAM



OBJECTIVES:

This Scenario describes how to enable **Logging Switch Activity**



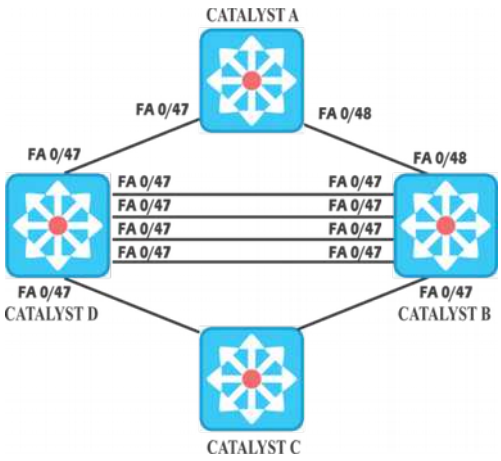


LAB EXERCISES:

Syslog Messages
Security Level 0 to 7
Logging to the switch console
logging console *severity*
terminal monitor
Logging to the internal buffer
logging buffered severity
(4096 bytes or 50 Lines)
logging buffered *size*
show logging

SCENARIO - 13 NTP

TOPOLOGY DIAGRAM



OBJECTIVES:

Using NTP to Synchronize with an External Time Source

LAB EXERCISES:

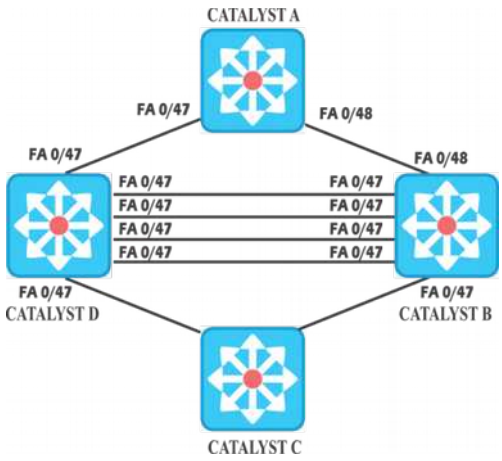
1. Enable the Internal system clock
2. Configure the External Time Source.
3. NTP Mode types
4. Securing the NTP

COMMANDS:

interface range fastethernet 0/0
ip name-server 8.8.8.8
ntp server 216.239.35.4 / 8 / 12
show ntp associations
show ntp status
ntp authentication – key
ntp authenticate
ntp trusted-key

SCENARIO - 14 IP SLA

TOPOLOGY DIAGRAM



OBJECTIVES:

This Scenario describes how to use Cisco IOS IP Service Level Agreements (SLAs) on the switch

LAB EXERCISES:

1. Enable the IP SLAs responder
2. Configure the required IP SLAs operation type.
3. Configure any options available for the specified operation type.
4. Configure threshold conditions
5. Schedule the operation to run, and then let the operation run for a period of time to gather statistics.
6. Display and interpret the results of the operation using the Cisco IOS CLI or a network management system.

STEP -1

Define Source

STEP -2

Type of test operation

STEP -3

Set the frequency of the operation

STEP -4

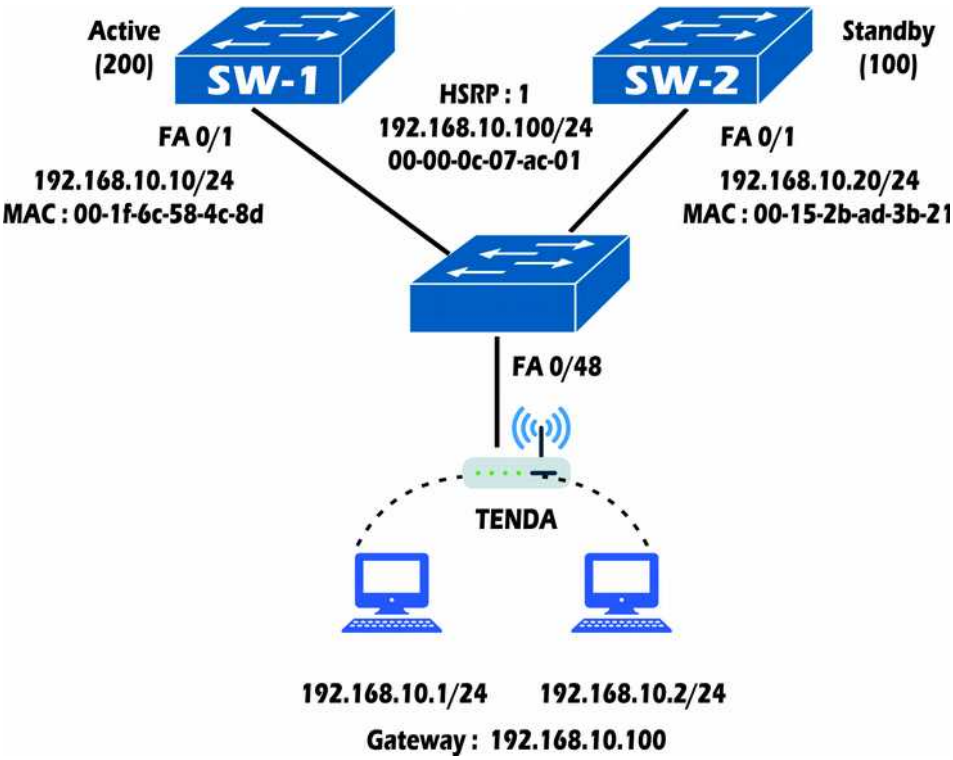
Schedule the test operations

COMMANDS:

ip sla 10
icmp-echo 172.16.1.2
frequency 5
ip sla schedule 100 life forever start-time now
show ip sla configuration
Show ip sla statistics 10
Show ip sla statistics aggregated 10

SCENARIO – 15 [REDUNDANCY - HSRP]

TOPOLOGY DIAGRAM



OBJECTIVES:

1. HSRP Router Election
2. HSRP Authentication
3. HSRP Gateway Addressing

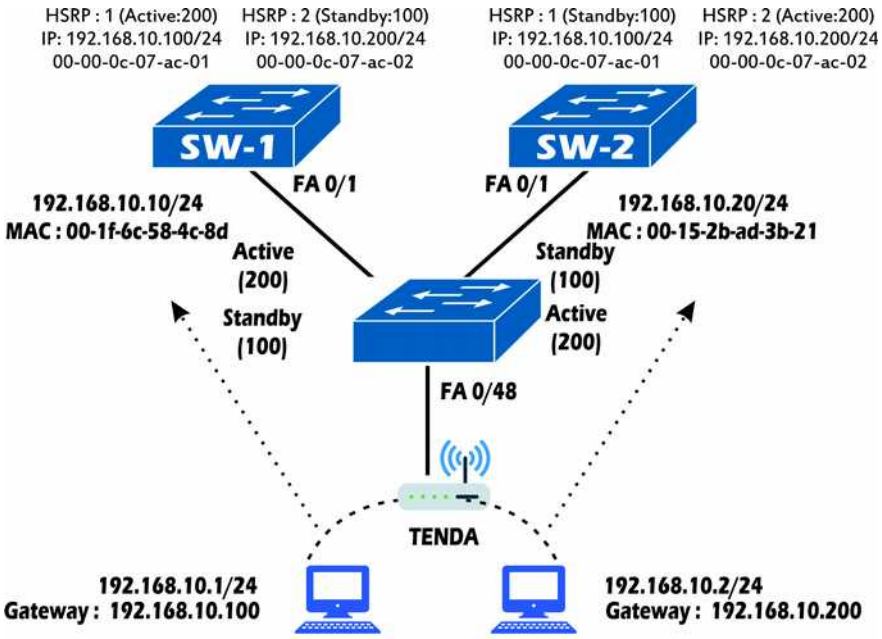
COMMANDS:

Switch - 1 ip add 192.168.10.10/24 standby 1 priority 200 standby 1 ip 192.168.10.100 standby 1 preempt standby 1 authentication cisco Switch – 2 ip add 192.168.10.20 / 24 standby 1 priority 100 standby 1 ip 192.168.10.100 standby 1 preempt standby 1 authentication cisco	Switch – 1 ip add 192.168.10.10/24 standby 1 priority 200 standby 1 ip 192.168.10.100 standby 1 preempt standby 1 authentication md5 key-string cisco Switch – 2 ip add 192.168.10.20 standby 1 priority 100 standby 1 ip 192.168.10.100 standby 1 preempt standby 1 authentication md5 key-string cisco

SCENARIO - 16 [REDUNDANCY - HSRP]

[LOAD BALANCING]

TOPOLOGY DIAGRAM



OBJECTIVES:

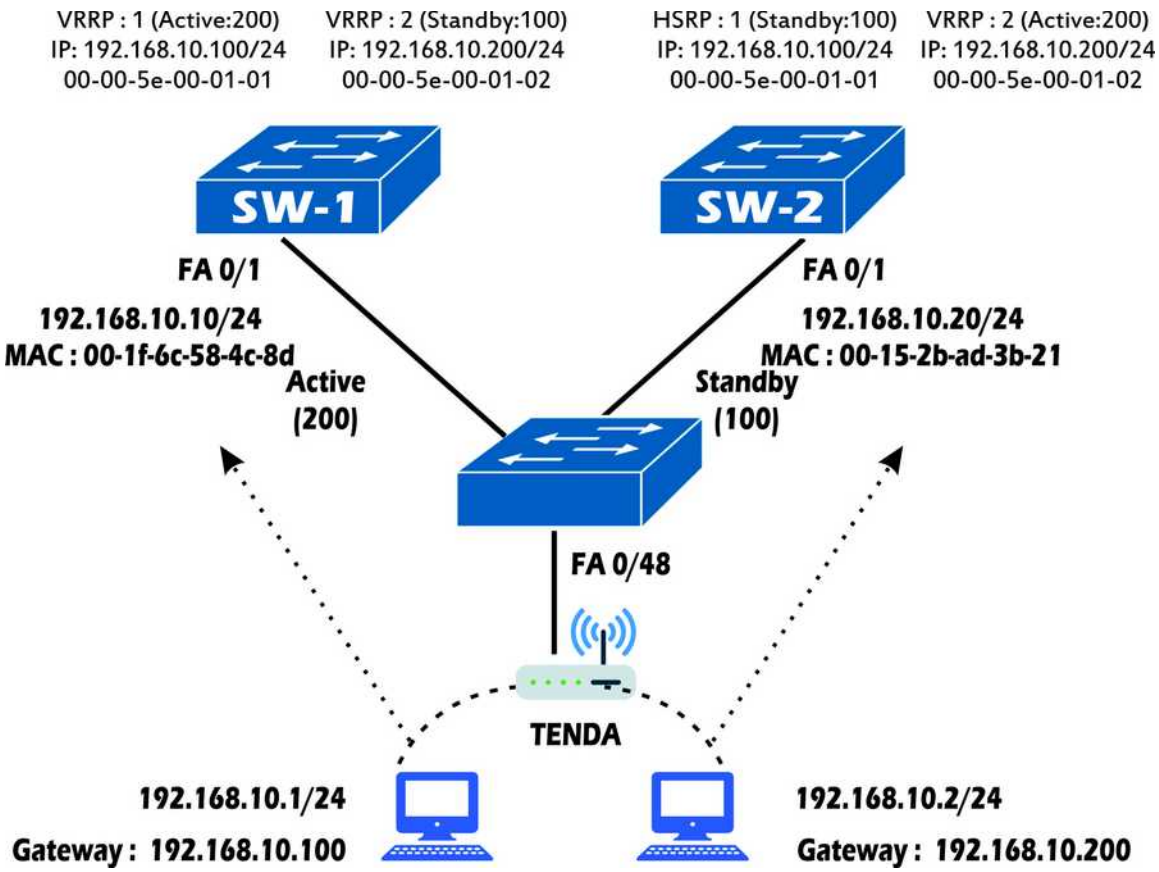
1. HSRP Router Election
2. HSRP Load Balancing
3. HSRP Verification

COMMANDS:

Switch - 1	Switch - 2
interface vlan 10 ip add 172.16.10.82 255.255.255.0 standby 1 priority 200 standby 1 ip 172.16.10.1 standby 1 preempt standby 2 priority 100 standby 2 ip 172.16.10.2 standby 2 preempt	interface vlan 10 ip add 172.16.10.169 255.255.255.0 standby 1 priority 100 standby 1 ip 172.16.10.1 standby 1 preempt standby 2 priority 200 standby 2 ip 172.16.10.2 standby 2 preempt

SCENARIO - 17 [REDUNDANCY – VRRP]

TOPOLOGY DIAGRAM



OBJECTIVES:

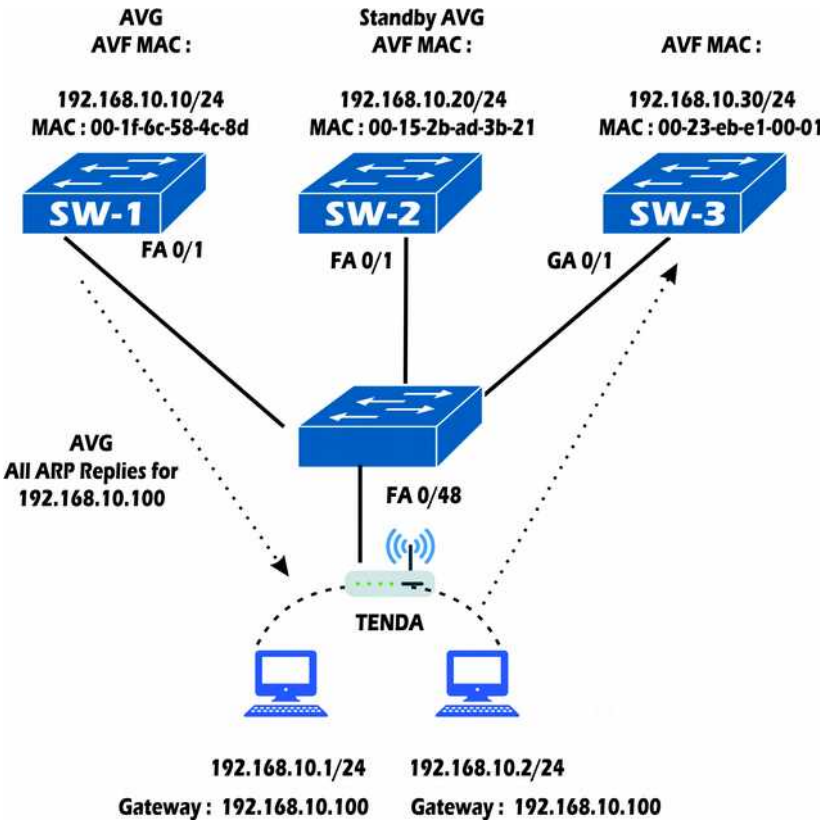
1. VRRP Router Election
2. VRRP Load Balancing
3. VRRP Verification

COMMANDS:

interface fa 0/1 ip address 10.0.0.1 255.255.255.0 vrrp 1 ip 10.0.0.1 vrrp 1 priority 255 vrrp 2 ip 10.0.0.2 vrrp 2 priority 110	interface fa 0/1 ip address 10.0.0.2 255.255.255.0 vrrp 2 ip 10.0.0.2 vrrp 2 priority 255 vrrp 1 ip 10.0.0.1 vrrp 1 priority 110

SCENARIO - 18 [REDUNDANCY - GLBP]

TOPOLOGY DIAGRAM



OBJECTIVES:

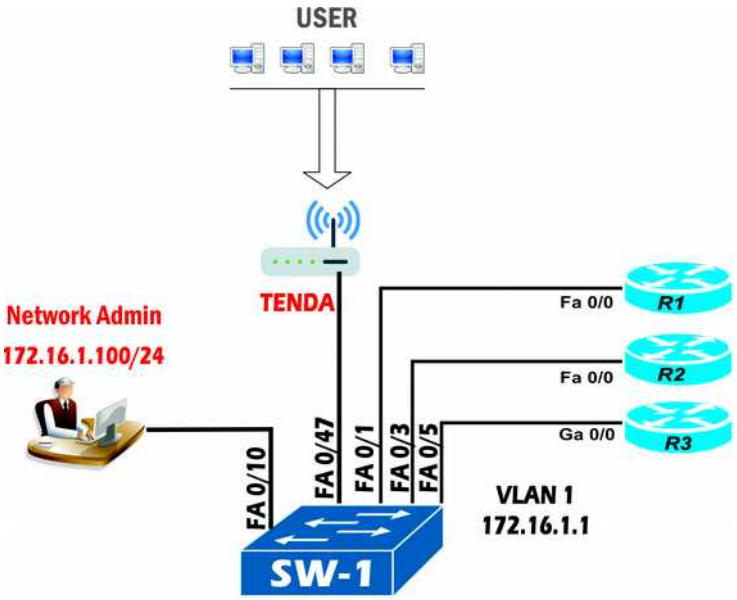
1. Active Virtual Gateway
2. Active Virtual Forwarder
3. GLBP Load Balancing
   a. Round Robin
   b. Weighted
   c. Host dependent

COMMANDS:

interface vlan 10
glbp 1 priority 200
glbp 1 preempt
glbp 1 ip 172.32.10
glbp group laad-balancing [round-robin]
Show glbp brief
show glbp

SCENARIO - 19 [PORT SECURITY]

TOPOLOGY DIAGRAM



OBJECTIVE

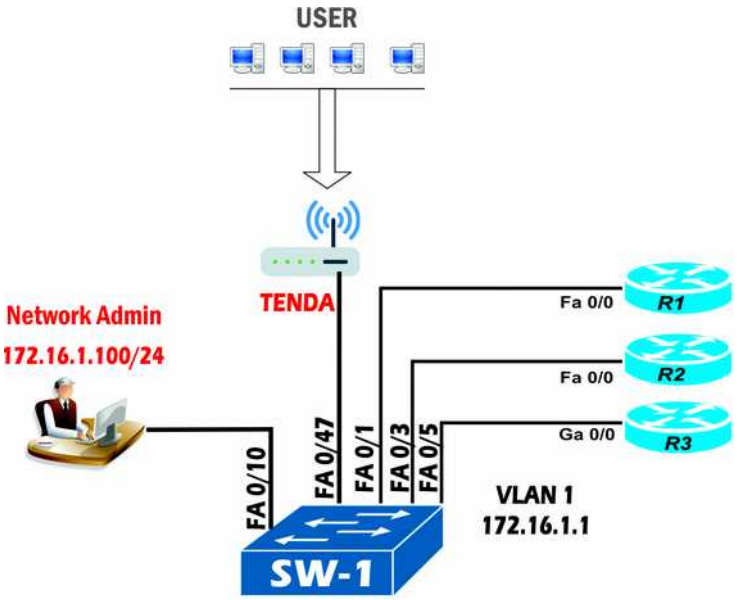
- Control port access based on MAC address
- Switch virtual interface
- Access MAP Statement
- Port access violation and Actions
  - Shutdown
  - Restrict
  - Protect

COMMANDS

Switchport port-security
switchport port-security maximum 2 (Maximum 1 to 1024)
switchport port-security mac-address sticky
switchport port-securiy mac-address *mac-addr*
switchport port-security violation *{shutdown | restrict | protect}*
clear port-security *{all | configured | dynamic | sticky}*
show port-security interface
Show interface status err-disable
Show port-security
show port-security address

SCENARIO - 20 [STORM CONTROL]

TOPOLOGY DIAGRAM



OBJECTIVE

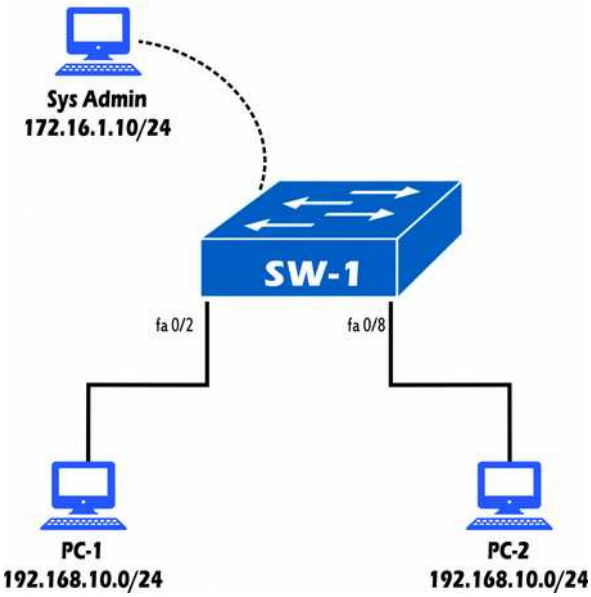
- Limit on flooded traffic before it can cause problem in network.
  - Broadcast Frames
  - Multicast Frames
  - Unknown Unicast Frames

COMMANDS

Storm control broadcast level 50
Storm control multicast level 50
Storm control unicast level 20 10
Show storm-control
show storm-control fastethernet 0/10
show storm-control broadcast
show storm-control fastEthernet 0/10 broadcast / unicast / broadcast

SCENARIO - 21 [SECURE PASSWORD & SWITCH ACCESS]

TOPOLOGY DIAGRAM



OBJECTIVE

- Secure Password
- System Banner
- Secure the Web interface
- Secure the switch Console
- Secure the Virtual Terminal access
- Secure Shell (SSH)
- Secure unused switch ports
- Secure STP Operation
- Secure use of CDP and LLDP

COMMANDS

Password Policy

security password min-length 10
enable secret cisco12345
service password-encryption

Secure the switch console

line console 0 / vty 0 4
password cisco12345 / vty 0 4
exec-timeout 1 0
logging synchronous
service password-encryption

Hidden Password

service password-encryption
line vty 0 4
password 7 20843028423

Use system banners

banner motd $
==========

"This system is for the use of authorized users only.
Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials."

==========

Copyright IPSOFTWARE SOLUTION (WWW.IPSOFTWARESOLUTION.COM)
========== $

Secure the web interface

no ip http server
ip http server
access-list 1 permit host 172.16.1.10
ip http access-class 1
no ip http server
ip domain-name ipss.com

Secure virtual terminal access and Local Database

username user1 privilege 15 secret cisco12345
line vty 0 4
privilege level 15
login local

Protect VTY

access-list 1 permit 172.16.1.10 0.0.0.0
line vty 0 4
ACCESS-CLASS 1 IN

SSH

ip domain-name ipss.com
crypto key zeroize rsa
crypto key generate rsa gneral-keys modulus 1024
line vty 0 4
transport input ssh
show ip ssh
ip ssh time-out 90
ip ssh authentication-retries 2

Secure unused switch ports

interface fastethernet 0/10
Switchport host
show interface fastethernet 0/12 switchport

Secure STP operations

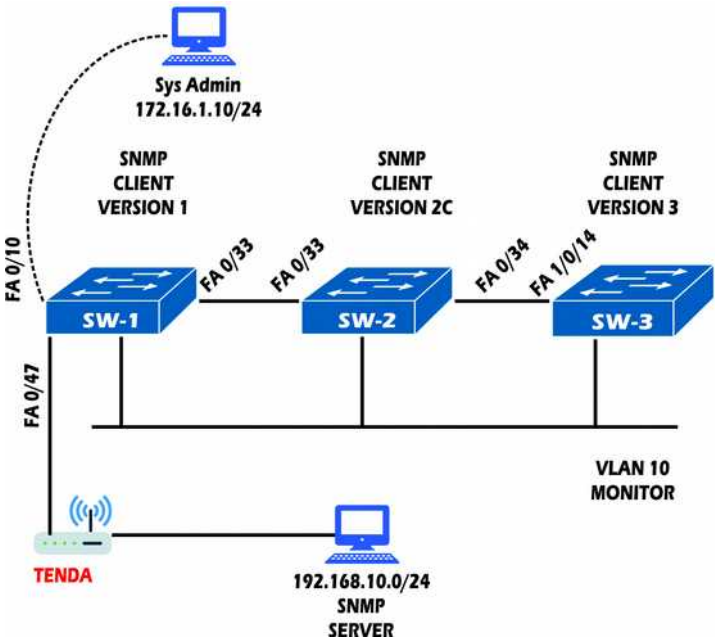
spanning-tree portfast bpduguard default
spanning-tree bpduguard enable
show spanning-tree interface fastethernet 0/48

Secure the use of CDP and LLDP

no CDP enable
no LLDP run

SCENARIO - 22 [SNMP]

TOPOLOGY DIAGRAM



OBJECTIVE

- SNMP Manager and SNMP Client
- Configuration of SNMP
- SNMP Versions
- SNMP Authentication
- Verification of SNMP

COMMANDS

VERSION 1

access-list 1 permit 192.168.10.1
snmp-server community **ipss1** ro 1
snmp-server host 192.168.10.1**ipss1**

VERSION 2c

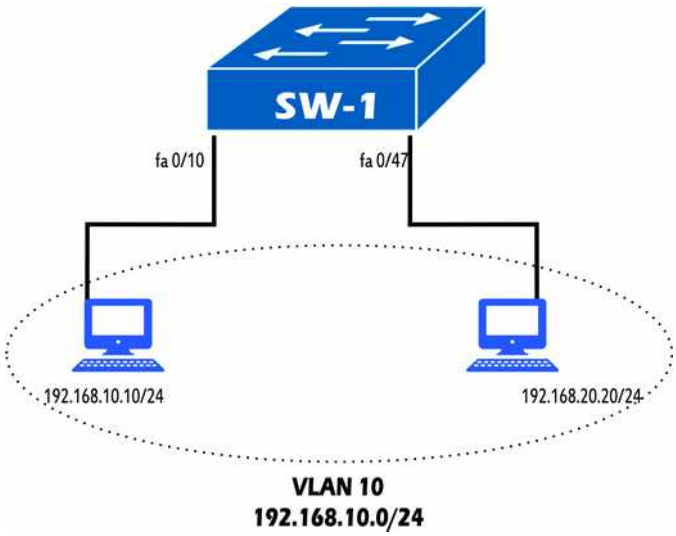
access-list 2 permit 192.168.10.1
snmp-server community ipss2 rw 2
snmp-server host 192.168.10.1inform version 2C ipss2

VERSION 3

access-list 1 permit 192.168.10.1
snmp-server group ipss3 v3 priv
snmp-server user ccnp ipss3 v3 auth sha cisco priv aes 128 cisco access 1
snmp-server host 192.168.10.1informs version 3 priv ccnp

SCENARIO - 23 [VLAN ACCESS-LISTS]

TOPOLOGY DIAGRAM



OBJECTIVE

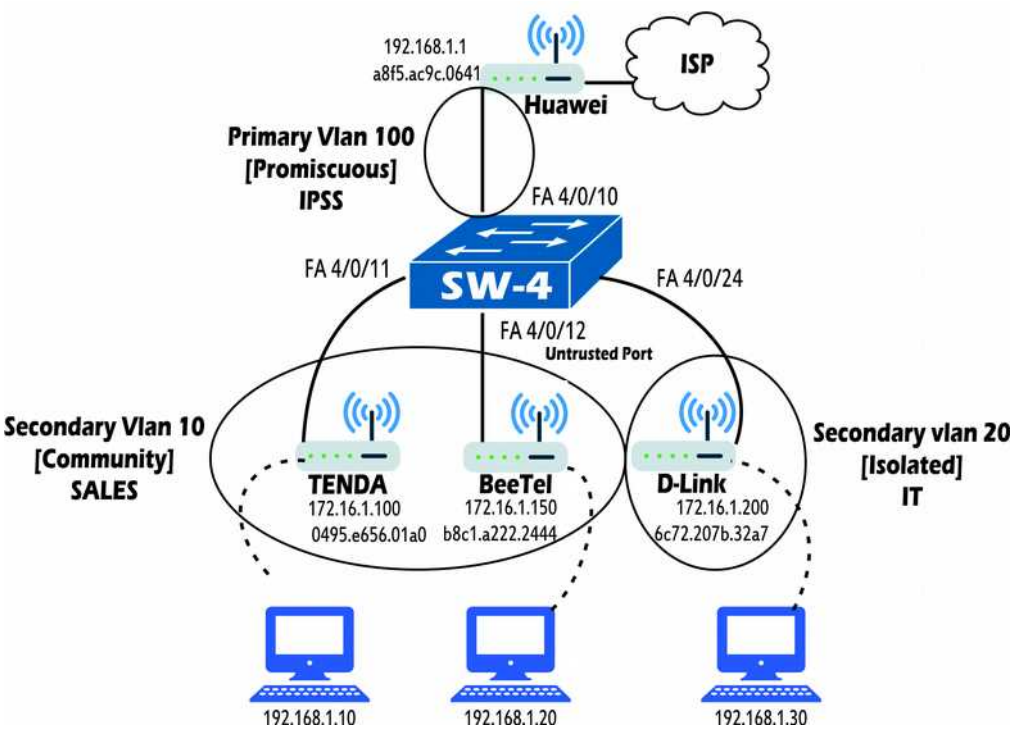
- Filter traffic through the use of TCAM
- Router Access Lists (RACL)
- Route-Map
- Vlan Filter

COMMANDS

```
# ip access-list  extended ipss
# permit ip host 192.168.10.10 192.168.10.0 0.0.0.255
# vlan access-map red 10
# match ip address ipss
# action drop
# vlan access-map red 20
# action forward
# vlan filter red vlan-list 10
```

SCENARIO - 24 [Private VLAN]

TOPOLOGY DIAGRAM



OBJECTIVE

- Client communicate to Service provider gateway and protect client do not need to interact with each other.
- Primary VLAN and Secondary VLAN
- Isolated and Community
- Promiscuous port.

COMMANDS

#vlan 10

private-vlan community

vlan 20

private-vlan isolated

vlan 100

private-vlan primary

private-vlan association 10,20

interface fastethernet 4/0/11 – 12

switchport mode private-vlan host

switchport private-vlan host-association 100 10

interface fastethernet 4/0/24

switchport mode private-vlan host

switchport private-vlan host-association 100 20

interface fastethernet 4/0/10

switchport mode private-vlan promiscuous

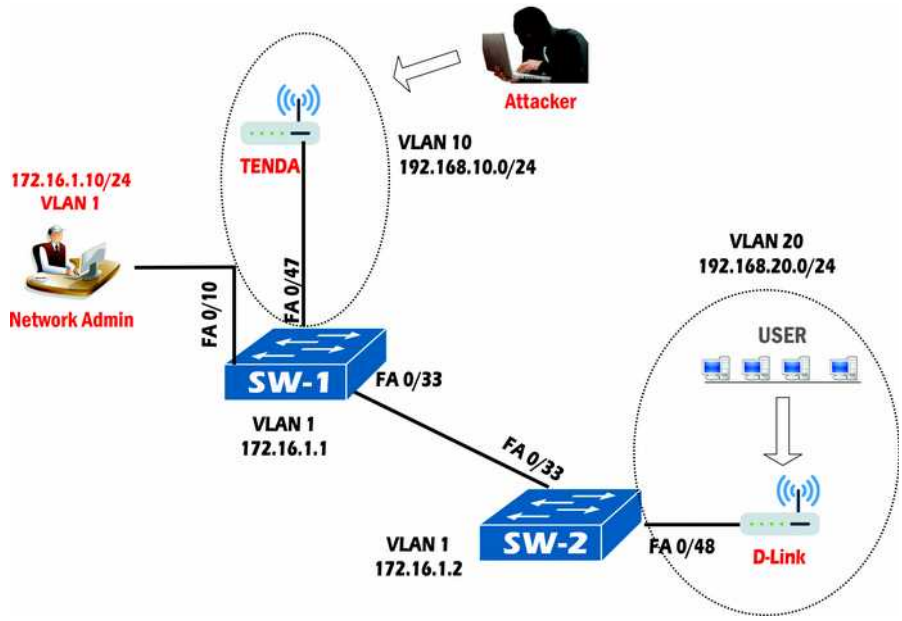
switchport private-vlan mapping 100 10,20

Show vlan private-vlan

Show vlan private-vlan type

SCENARIO - 25 [SWITCH SPOOFING - VLAN HOPPING]

TOPOLOGY DIAGRAM



OBJECTIVE

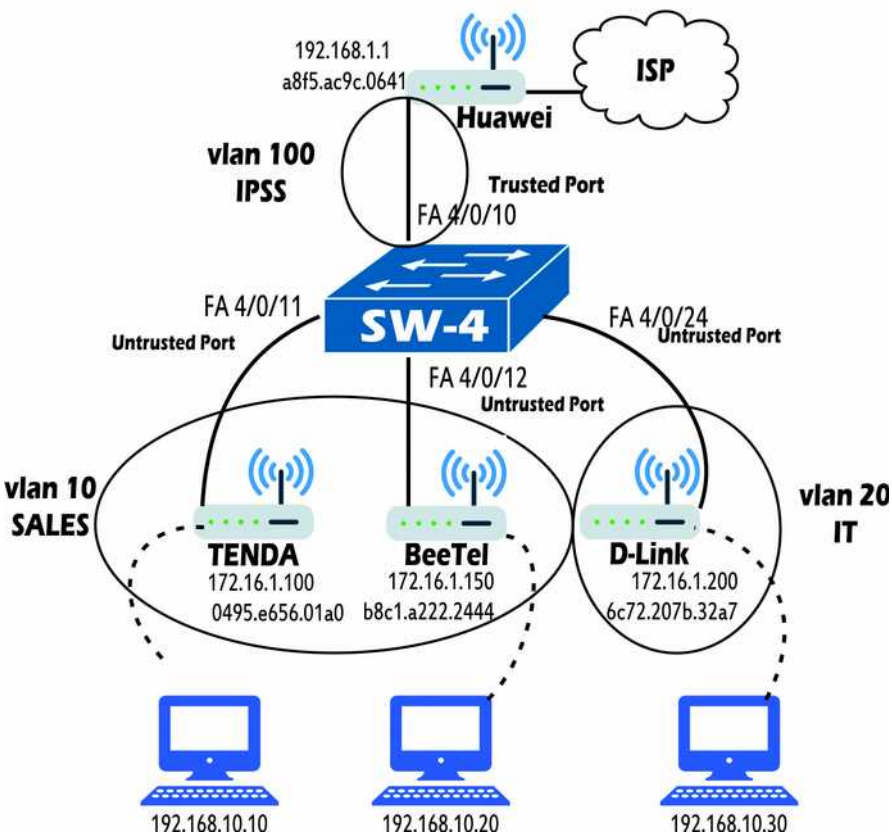
- VLANs and Trunk Link
- Dynamic Trunking Protocol (DTP)
- Exploit DTP
- VLAN Hopping

COMMANDS

interface fastethernet 0/10
switchport access vlan 10
switchport mode access
vlan 800
#name bogus_native
interface fastethernet 0/33
switchport trunk native vlan 800
switchport trunk allowver vlan 10 20
#switchport trunk allowed vlan remove 800
switchport mode trunk

SCENARIO - 26 [DHCP SNOOPING]

TOPOLOGY DIAGRAM



OBJECTIVE

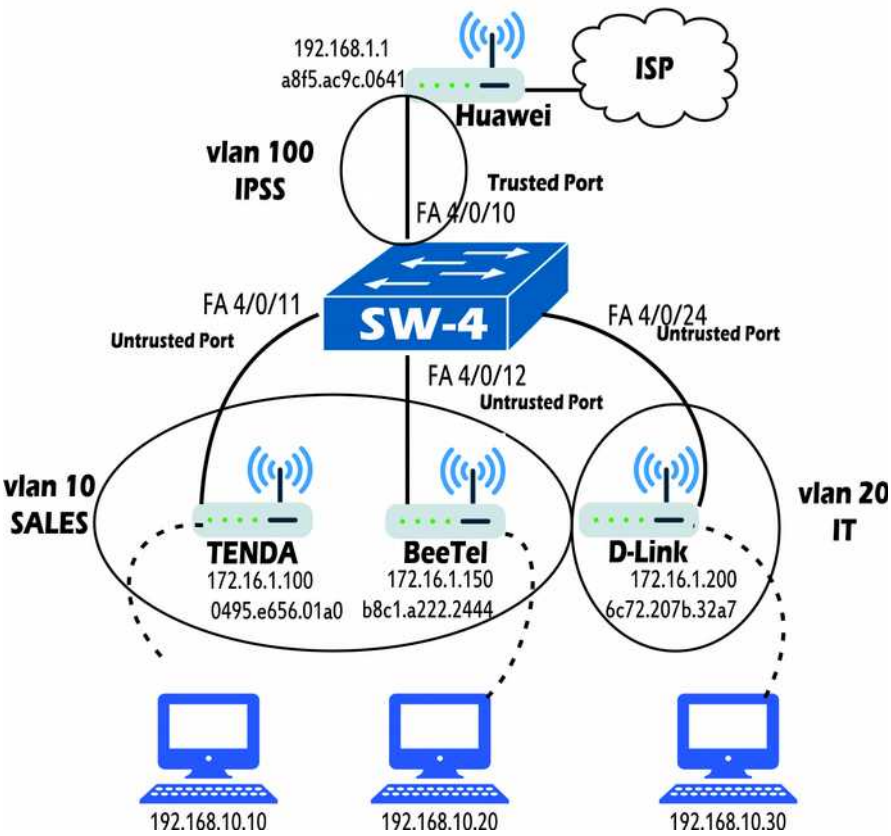
1. Prevent the Man in Middle attack
2. Rogue DHCP Server
3. Trusted and Untrusted Ports
4. Legitimate DHCP Servers and trusted Ports
5. Rate Limit on untrusted ports [1 to 2048 packets per second]

COMMANDS

```
# ip dhcp snooping
# ip dhcp snooping vlan
# interface fastethernet 0/10
# ip dhcp snooping trust
# interface fastehternet 0/12
# ip dhcp snooping limit rate 3
# ip dhcp snooping trust
# show ip dhcp snooping
```

SCENARIO - 27 [IP SOURCE GUARD]

TOPOLOGY DIAGRAM



OBJECTIVE

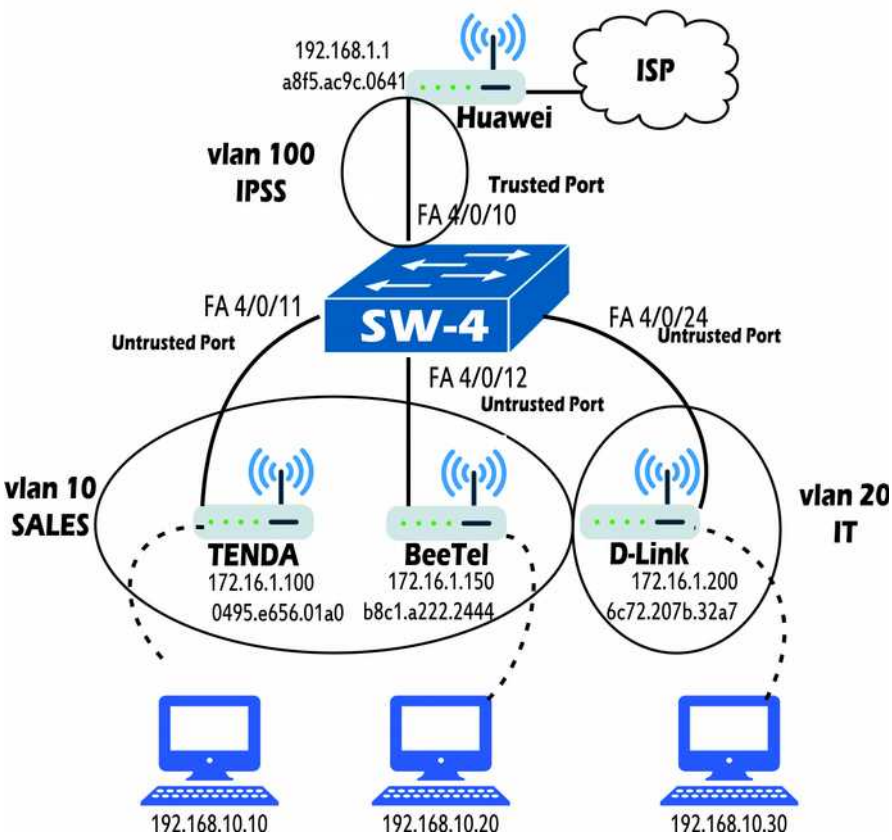
1. Denial of Service attacks
2. IP Source Guard detects suppressed address
3. MAC and IP Binding address
4. DHCP Snooping.
5. Static IP source binding.

COMMANDS

ip source binding MAC-ADDRESS vlan VLAN-ID IP-ADDRESS interface MEMBER
ip verify source port-security
show ip verify source interface MEMBER.
Show ip source binding

SCENARIO – 28 [DYNAMIC ARP INSPECTION]

TOPOLOGY DIAGRAM



OBJECTIVE

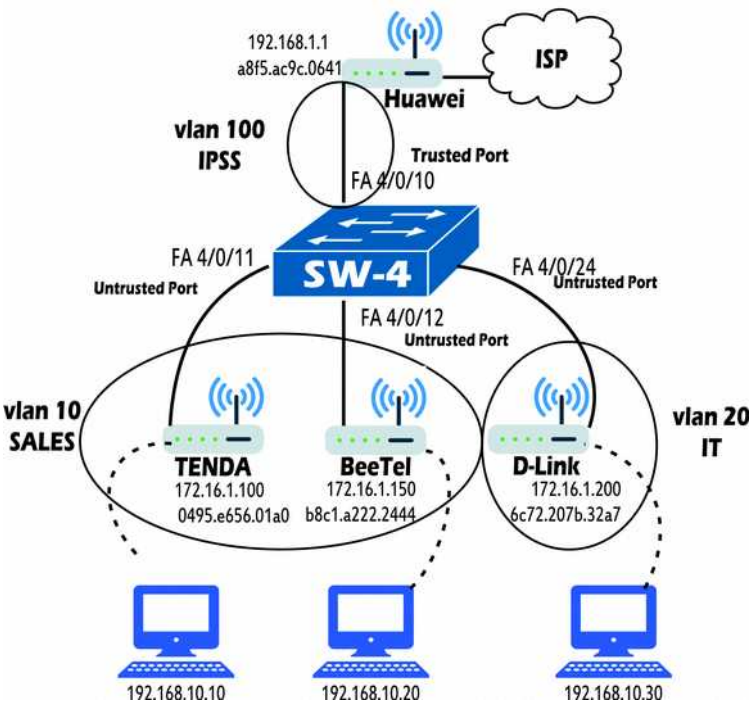
1. Address Resolution Protocol functionality.
2. ARP Poisoning or ARP Spoofing
3. Dynamic ARP inspection (DAI)
4. DHCP Snooping Trusted and Untrusted.
5. Static IP source binding.

COMMANDS

```
# ip arp inspection vlan 10
# arp access-list ipss
# permit ip host 192.168.20.10 mac host 0000.0000.0001
# ip arp inspection filter ipss vlan 10
# ip arp inspection trust
```

SCENARIO – 29 [PORT MONITOR TRAFFIC]

TOPOLOGY DIAGRAM



OBJECTIVE

1. Local SPAN
2. Remote SPAN
3. Local SPAN Configuration
4. Remote SPAN Configuration
5. Managing SPAN Session

COMMANDS

vlan 100
name MONITOR
vlan 10
name SALES
monitor session 1 source interface fastethernet 0/47 both
monitor session 1 destination interface fastethernet 0/10
vlan 100
remote-span
#vlan 100
monitor session 1 source remote vlan 100
monitor session 1 destination interface fastethernet 1/0/23

SCENARIO - 30

MANAGING TRAFFIC IN A SWITCHED NETWORK

OBJECTIVE:

This scenario is designed to stir your thinking about how to control access to switched networks, how to control traffic within a VLAN, and how to monitor traffic.

1. Network administrators want to have tight control over hosts moving around within their network. A Catalyst 3750 needs to have port - level security enabled on all 48 of its Fast Ethernet access-layer port. Only one host should be connected per port, so the default behavior of shutting down the port is acceptable. What Commands are necessary to do this?
2. Port – level security is desired on a Catalyst 3750 interface Fast Ethernet 1/0/18, where 24 users are connected through an Ethernet hub. Rather than have the switch port shut down upon a security violation, network administrators want only the hosts in violation to be rejected. What command can accomplish this?
3. Configure a VLAN access control list that can perform packet filtering within a VLAN. User in the 192.168.191.0 255.255.255.0 network should be allowed to use only HTTP (www) traffic to the web server 192.168.191.199/24,on VLAN 180. How can you configure the VACL to accomplish this?
4. An access- layer switch has ports Fast Ethernet 1/0/1 through 1/0/48 connected to end –user PCs. Is it possible for a user to make one of these ports come up in trunlink mode? If so, what commands should you enter to prevent unexpected trunk negotiation?
5. Suppose that a switch has a drunk link Gigabit Ethernet 1/0/1 configured with the following commands:

   # interface gigabitethernet 1/0/1
   # switcport
   # switcport trunk encapsulation dot1q
   # switcport trunk native vlan 100
   # switcport trunk allowed vlan 100-300
   # switcport mode trunk

   VLANs 100, 200, and 300 all are used for user traffic. What, if anything, Should be done to the trunk configuration to prevent a VLAN hopping attack from occurring?
6. A Catalyst switch has users connected to ports Fast Ethernet 1/0/1 through 1/0/30. These users are associated with VLAN 50. Two production DHCP servers are connected to ports Fast Ethernet 1/0/40

and 1/0/41.What commands should be entered to enable DHCP snooping so that DHCP spoofing attacks can be detected and prevented?

7. Assume that a server is connected to interface Gigabit Ethernet 3/3 on a Catalyst 6500. What command can be used to monitor traffic transmitted and received on the server port with a network analyzer connected to interface Gigabit Ethernet 5/8 on the same switch?
8. Suppose that the only network analyzer available has a 10/100 Ethernet NIC. It is connected to Catalyst 6500 interface Fast Ethernet 2/1, to monitor the server on Gigabit Ethernet 3/3. Explain any problems you might encounter with this setup.