==

Section 1. Layer 2 Technologies

==

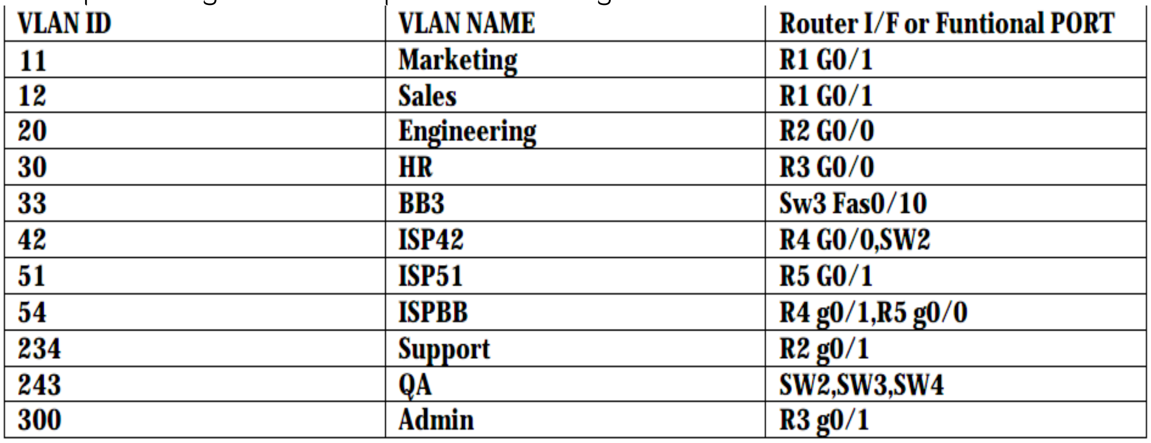
1.1 Troubleshoot Layer 2 Switching

Four faults have been injected into the pre-configuration just described, these issues may impede a working solution for certain portions of this labs exam and affect any labs exam section. You must verify that all of your configuration work as expected, if something is not working as expected then you must fix the underlying problem.

Point will be awarded for solving each problem. However, if you fail to solve a particular problem, and the injected fault prevents you from having a working solution of this lab, then you will lose points for the fault and the scenario that is not working.

1.2 Implement the Access-Switch Ports

VLAN port assignments are per the following table:



VLAN ID	VLAN NAME	Router I/F or Funtional PORT
11	Marketing	R1 G0/1
12	Sales	R1 G0/1
20	Engineering	R2 G0/0
30	HR	R3 G0/0
33	BB3	Sw3 Fas0/10
42	ISP42	R4 G0/0,SW2
51	ISP51	R5 G0/1
54	ISPBB	R4 g0/1,R5 g0/0
234	Support	R2 g0/1
243	QA	SW2,SW3,SW4
300	Admin	R3 g0/1

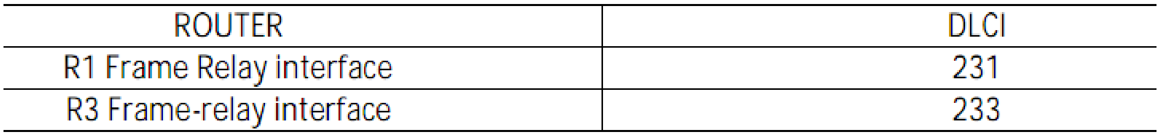
Configure all of the appropriate nontrunking access switch ports on SW1, SW2, SW3 and SW4, according to the following requirements:

- Use 802.1w on all of four switches.
- Backbone device can't be access and Don't consider the Backbone
- Ensure that the spanning tree enters the forwarding state immediately only for these access switch ports, by passing the listening and learning states. The interfaces connected to BB router are not the access switchport and do not use default command
- Avoiding transmitting BPDUs on any access switchport on any of these ports, the ports should be shutdown automatically if SW receives BPDU. You need to use only single command to do this task.
- Ensure that all four switches are able to read to unidirectional link failure for any switch to switchport the affected port should be disabled in the event failure.

1.3 Implement Frame Relay

Use the following requirement to configuration R1 and R3 for Frame Relay and R5 as the FRSW:

- Configure Frame-relay as in diagram.
- Use point-to-point sub interface for end-point
- Use the DLCI number to sub-interface number
- Use CISCO LMI on Frame Relay switch and auto-sensing on R1 and R3
- Use frame-relay encapsulation as “cisco”.
- Use the data-link connection identifier(DLCI) assignments from the table below



ROUTER	DLCI
R1 Frame Relay interface	231
R3 Frame-relay interface	233

1.4 Switching

- Use 802.1q on all four switches.
- Switches should not actively attempt to convert the links to trunk link by negotiating the trunk mode.
- Utilize Etherchannel between all switching interconnections using IEEE standard to actively negotiate channel.
- Etherchannel load balancing should be accomplished by destination ip address.
- Configure port R1 0/1 on SW2. Ensure that only Vlan SALES and MARKETING are allowed.
- Make sure SW1 must be root for all VLAN
- Make sure SW4 should not become root for any VLAN. Ensure that this occur without changing the switch priority
- Make sure SW1 should be aging-time out two times as fast as than other vlans of VLAN 20

1.5 Port Mirroring

Configure port monitoring on SW3 according to the following requirement.

- The Transmit and receive traffic on ports Fa0/1 through Fa0/8 and the Ether channel port-channel for Fa0/19 – 20 should monitored.
- A copy of the traffic should be forwarded to Fa0/11.

Section 2. Layer 3 Technologies

The loopback interface can be seen as /32 in the routing tables unless stated otherwise in a question.

2.1 Implement IPv4 OSPF

- Configure OSPF area 1 as in diagram.
- Other routers should be seen as an external route about the Backbone 2.
- Sw2 should inject default route.
- Configure OSPF area 0 and OSPF area 51 as in diagram
- SW1 should be seen as an external route about the Backbone 1
- SW1 should inject default route

2.2 Implement IPv4 EIGRP

- Configure EIGRP YY Between R4 & R5
- Configure EIGRP 100 as in the diagram
- EIGRP updates should be advertised only out to the interfaces indicated in the IGP topology.
- Configure SW3 Such that it will not receive any EIGRP queries. SW3 should also not send out information about BB3 routes to the EIGRP 100 neighbors. Do not configure any kind of outgoing filtering to do this.
- On SW3, Use route-maps to tag any CLASS A network address routes from External EIGRP with tag 200 and define ACL for CLASS A network.
- Redistribute loopback 0 of R4 & R5 should be seen as an external route.
- SW3 redistributed EIGRP 100 to OSPF summarize to the following routes into an aggregate YY.0.0.0/8:
  198.1.1.4/30
  198.2.1.0/24
  198.2.3.0/24
  198.2.5.0/24

2.3 Implement MPLS

- Name VRF as “vpnA”.
- Use rd 100:1 both R4 and R5
- Use OSPF as routing protocol between PE & CE.
- Use MPBGP AS 100 to exchange customer prefixes. Source all updates using loopback 0 address.
- Make sure that MPLS Backbone is preferred over the link between R1 & R2. Use the network YY.YY.100.X/24 to facilitate this.
- Address the need MPLS introduces of connecting portioned OSPF backbone and do not care about R3 backdoor

2.4 Implement IPv4 BGP

Referring the BGP Routing diagram. Configure BGP within these parameters

- SW1 connects to BB1 (150.1.YY.254) and from BB1 SW1 receives 197.68.Z.0 /24 networks with AS PATH: 254 253
- SW2 connects to BB2 (150.2.YY.254) and from BB2 SW2 receives 197.68.Z.0 /24 networks with AS PATH: 254
- SW2 should modify the AS PATH of its learned routes; adding AS253 by using single route-map.
- SW1, SW2, R2, R3 are IBGP peers, next-hop-self and route-reflector-client is not permitted.
- Use BGP command to cause R2 to prefer SW2 as the exit point for ASYY, and R3 to prefer SW1 and the exit point for ASYY to AS 254.
- Both R2 & R3 Should Still have routes to the other exit point in their BGP table.
- Use ONLY the loopback 0 IP address to propagate BGP routes information.
- No IGP router Should be advertised to AS254

2.5 Implement IPv6 RIPng

Configure IPV6 unique local unicast address as follows:

- R2
  - o fa0/0 :10YY:1010:10::1/64
  - o fa0/1 :10YY:1010:20::1/64
- SW3
  - o SVI 234 :10YY:1010:20::2/64
  - o SVI 33 :10YY:1010:30::2/64
- Configure RIPng between R2 and SW3
- Ensure that R2 can receive default route from SW3

Section 3. Multicast

3.1 IPv4 Multicast

Enable PIM Sparse mode (PIM-SM) between SW2, Sw3 and Sw4

- The QA and Support VLANs should handle multicast traffic.
- Configure Auto-RP, with SW3 loopback 0 serving as RP only for multicast group 239.10.5.0/24, and SW4 serving as mapping agent.
- Enable SW2 loopback0 to join group 239.10.5.1
- To verify you should be able to successfully generate multicast traffic for the group 239.10.5.1 using R2 as the source.

3.2 IGMP Limit

Configure switches (SW2~SW4) so that hosts connected to VLAN QA can only join in multicast groups 239.10.5.1

Section 4. Advanced Services

4.1 LINK FRAGMENTATION

On R1 and R3

- Use end point identifier for multilink bundling
- Apply fragment delay pf 8ms to the MPPP bundle.
- Use bandwidth command on both virtual interface and multilink interface for interleaving to work (use ppp multilink interleave)

4.2 Link Efficiency

- Define CIR (and interface bandwidth) as 128K.
- Use a policy map to define a priority of 45 to all VoIP traffic whose proceeding as Critical. And using the access-list but don't use named extended and you should implement using the LLQ
- Use a Multilink group interface for all QoS and IP commands.
- The Committed burst size as 8Kbits and excess burst size is 1K bits

4.3 QoS for Video

Port fa0/6 on SW4, Will host a video server for streaming video to devices off the Marketing VLAN on R1.

- Configure MLS QoS in the network according to:
- The video server ip YY.YY.128.98
- Use Policy-map to assign video traffic a DSCP of 56
- Define policy for video traffic with rate of 3M and burst size of 1M. Additionally when these routes are exceeded, the DSCP value for video traffic should be mark down from 56 to 8.
- The distribution ports between all 4 switches should trust inbound DSCP value for classification.
- Additionally, for untagged packets the default CoS value should be defined as 1.
- Finally the expedite queue should be for all these ports.

4.4 RSVP

- Configure Reservable bandwidth 64K with largest reservable flow 64K.
- Configure R3 to simulate a host generating a RSVP PATH message to R1, Protocol should be a TCP.
- Configure R1 to simulate a host generating RSVP RECV message to R3.
- Use loopback address to R1 and R3 and the message protocol should be TCP with a source port 10000and a destination of telnet.
- The message should be for a single reservation with guaranteed average bit rate of 10k and max burst of 1K byte.

==

Section 5. IP Services & System management

==

5.1 Multiple-HSRP (MHSRP)

Configure MHSRP on SW3 and SW4 (sometimes it says for VLAN named Support):

- Do load balance and fault tolerance in SW3 and Sw4.
    - Group 1:
        - SW4 is the Master
        - HSRP IP: YY.YY.128.196
    - Group2:
        - SW3 is the Master.
        - HSRP IP: YY.YY.128.222
- The group 1 and group 2 on SW4 track to ip route 0.0.0.0 0.0.0.0

5.2 NTP

Between R5, SW1,SW2 and R3

- R5 should synchronize with a NTP source YY.YY.254.254
- In the event of R5 loses connection to NTP server it should act as NTP Server with a stratum 5 and its calendar as an authoritative time server.
- R3 and R5 should authenticate each other.
- SW1 and SW2 do not authenticate.
- Set clock on R5 8:00:00 AM 1 JAN 2010
- Ultimately, all clocks should be in Sync.

5.3 IP Service Level Agreements

- Configure IP SLA, intended to monitor the response across between MPLS network and Backdoor serials according to:
- SW2 will do all monitoring, SW1 act as IP SLAN responder, while R3 should have no Knowledge of IP SLAs.
- SW2 should use TCP to monitor SW1. The operation should repeat every 3 min. Starting immediately and repeat every day.
- TCP SLAs should use the well-known telnet port.
- SW2 should use ICMP to monitor R3. The operation should repeat every 3 min. Starting immediately and every day.
- Loopback address should be used for and by all devices.

5.4 SNMP

Configure SNMP on SW2 & R3 according to:

- All traps should be sent to the SNMP Server YY.YY.128.226 using the community string public.
- There should be 2 communities defined
  - [public] with read-only access
  - [ciscoADMIN] with read-write access.
- On SW2 enable SNMP traps for IP SLA in the event that round-trip time value violates the upper and lower threshold.
- On R3 enable SNMP traps for RSVP.

5.5 Logging, Management, Core Dumps

Configure the following system management feature on R2 according to:

- Enable local time-stamps with date and time in msec debug and logged messages.
- Configure the local logging buffer to be 10000 bytes, logging messages with set the severity level 4 (warning) and the higher.
- In the event that the local buffer is overwritten, enable the error counter. To facilitate troubleshooting, when there is unexpected system shutdown or reboot ensure that core dump is generated and saved to the host YY.YY.128.196 using passive FTP protocol.
- The file names should be RACKYYR2 and the file should be compressed. The username/password for the ftp transfer should be reload/cisco