2020

LAB 2 DOCUMENTATION

BAIS3410
GABRIEL KWAN, GBOLAHAN AIYETORO, ASIA WARAMMANUSAI & NAVDEEP SINGH

NAIT | BAIST

Table of Contents

Table of Figures

SECTION 1: SUMMARY QUESTIONS

BAIS3410 Assessment 2

True/False
Indicate whether the statement is true or false.

_T__ 1. DAD is used to determine if an IPv6 address is already in use on the network.

_F__ 2. An SVI is configured on a physical interface on an multilayer switch.

_T__ 3. If the Option flag is 1 and the Managed flag is 0 in the RA, this informs the host that it is to autogenerate its own IP Address and to check with a DHCP server for more information.

Multiple Choice
Identify the choice that best completes the statement or answers the question.

_D__ 4. A host resides in VLAN 10, with a default gateway configured as 10.1.1.1, and can ping VLAN 20's routed interface 10.2.1.1 successfully, but cannot successfully ping any other hosts that reside in VLAN 20, what could be a possible reason?

a. The routing protocol has not been configured correctly on the layer 3 switch
b. Hosts in VLAN 10 are not configured with the correct default gateway.
c. Trunking is not configured between the hosts.
d. Hosts in VLAN 20 are not configured with the correct default gateway.

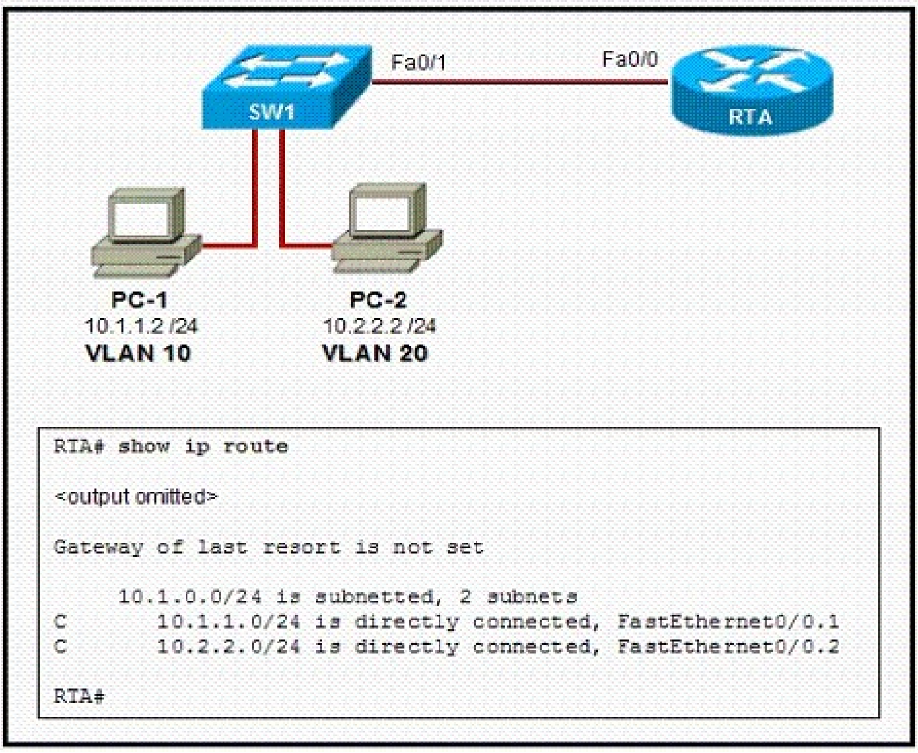
_B__ 5. When should the command "**ip routing**" be used when configuring a Multilayer switch?

a. Never - the command is configured by default and cannot be deactivated.
b. When communication between different layer 3 devices is required
c. When Spanning Tree is being configured to communicate with a layer 2 Etherchannel
d. When EIGRP is not used as a routing protocol.

__A__ 6. Which command is used to change an interface from a layer 3 interface to a layer 2 interface?

a. switchport
b. no switchport mode routed
c. ip routing
d. switchport mode access

_C__ 7.



Refer to the exhibit, and identify which answer is true from the information provided.

a. VLAN 20 is the native VLAN and does not require trunking, configuration.
b. Because the packets are being trunked, hosts on VLAN 10 do not need a default gateway.
c. The default gateway for hosts on VLAN 10 should point to the IP address of FA0/0.1
d. The default gateway for hosts on VLAN 20 should point to the IP address of FA0/0

__B_ 8. Which statement is true regarding about routed ports on a multilayer switch?

a. A routed port is a physical switch port with only layer 2 capability
b. Routed ports are configured with the "no switchport" command
c. Multilayer switches do not support routed ports
d. "Interface VLAN" global configuration command is used to create a routed port

__A_ 9. To enable Inter-vlan routing on a **multilayer switch**, what type of interface must be configured?

a. Switched virtual interface
b. Router subinterfaces
c. Switch based policy routing
d. A single routed port

_D__ 10. Which of the following is true about routed switch ports?

a. Allows multiple VLANs per port
b. Can be refered to as an SVI
c. Does not provide Layer 3 functionality
d. Does not support VLAN subinterfaces

_B__ 11. The generic name for the role which allows a router to forward broadcasts across the routed boundary is;

a. Broadcast Forwarder
b. Relay Agent
c. Helper process
d. Directed Traffic Engine (DTE)

_C__ 12. Which command is the IPv6 equivalent of "IP helper-address"

a. "ipv6 directed-broadcast"
b. "ipv6 dhcp pool"
c. "ipv6 dhcp relay destination"
d. "ipv6 nd other-config-flag"

_B__ 13. In order to use SLAAC how many bits must the host interface ID be?

a. 48
b. 64
c. 80
d. 96

__D_ 14. Neighbor Discovery Protocol relies upon which protocol for its operation?

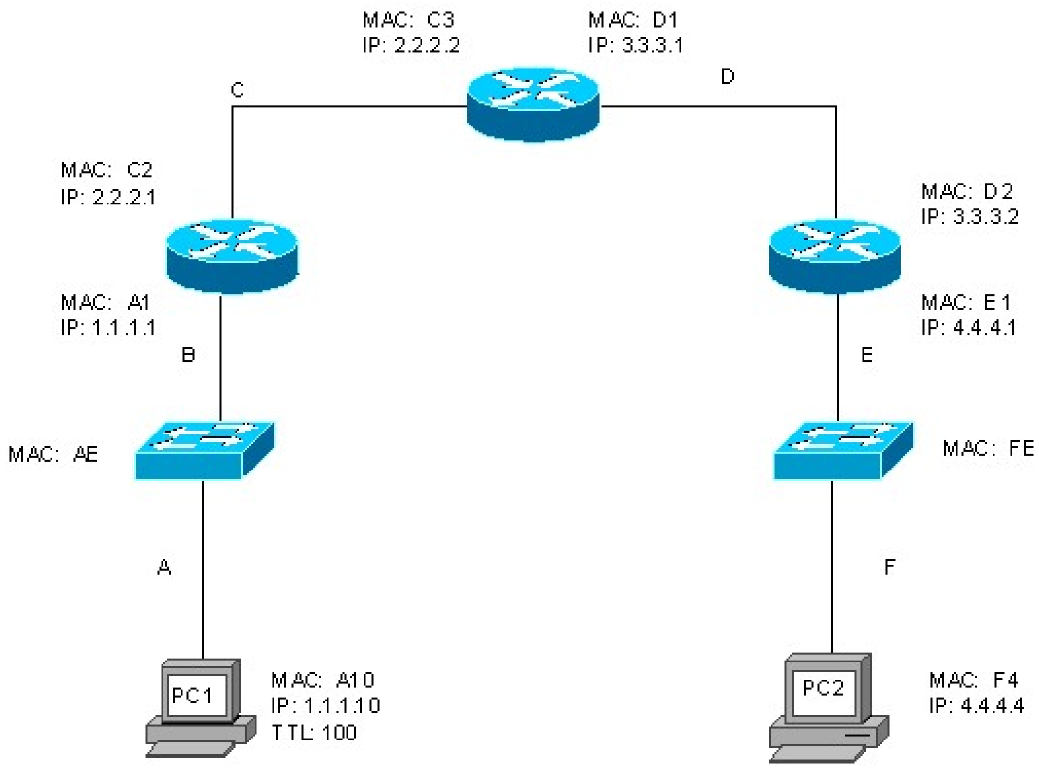
a. ARP
b. DHCP
c. DHCP Relay Protocol
d. ICMPv6

_A__ 15. Which message allows an IPv6 host to determine how it should get its IP address?

a. RA
b. RS
c. NS
d. NA

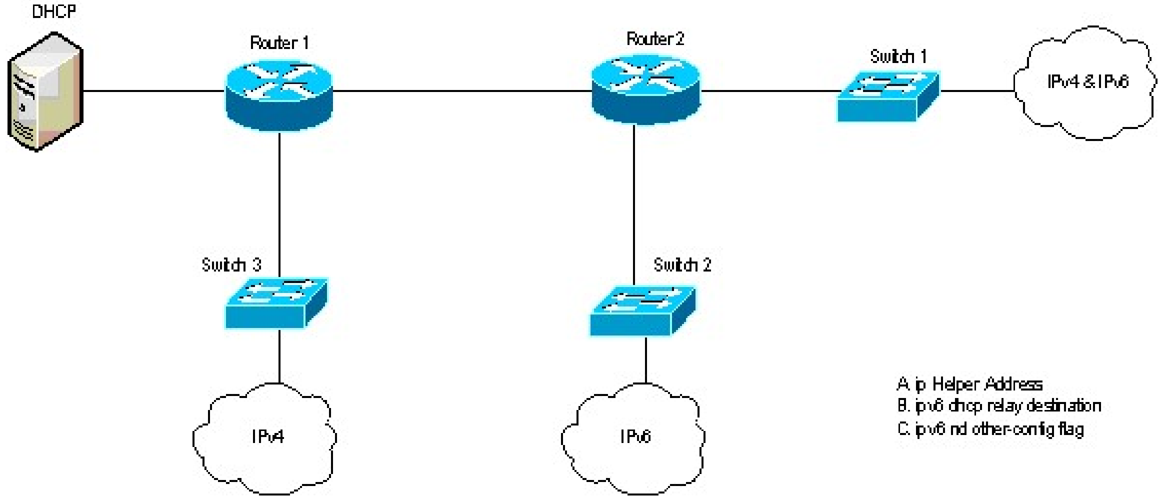
Problem

1. For a frame flowing from PC1 to PC2, fill in the following information at the indicated points on the network: (3 marks 1 mark for each correct column (A,C,E))



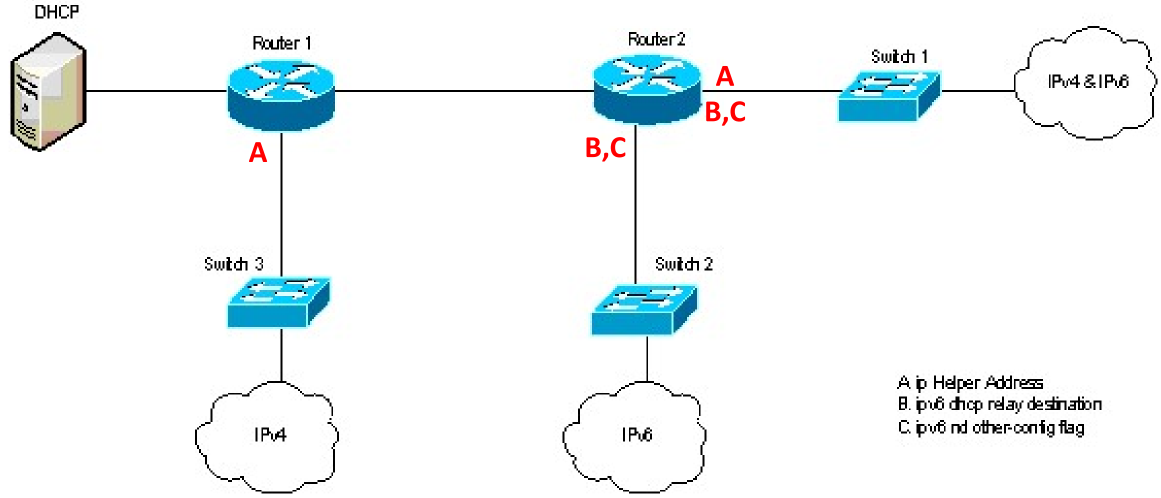
	A	C	E
Source MAC	A10	C2	E1
Destination MAC	A1	C3	F4
Source IP	1.1.1.10	1.1.1.10	1.1.1.10
Destination IP	4.4.4.4	4.4.4.4	4.4.4.4
TTL	100	99	97

2.

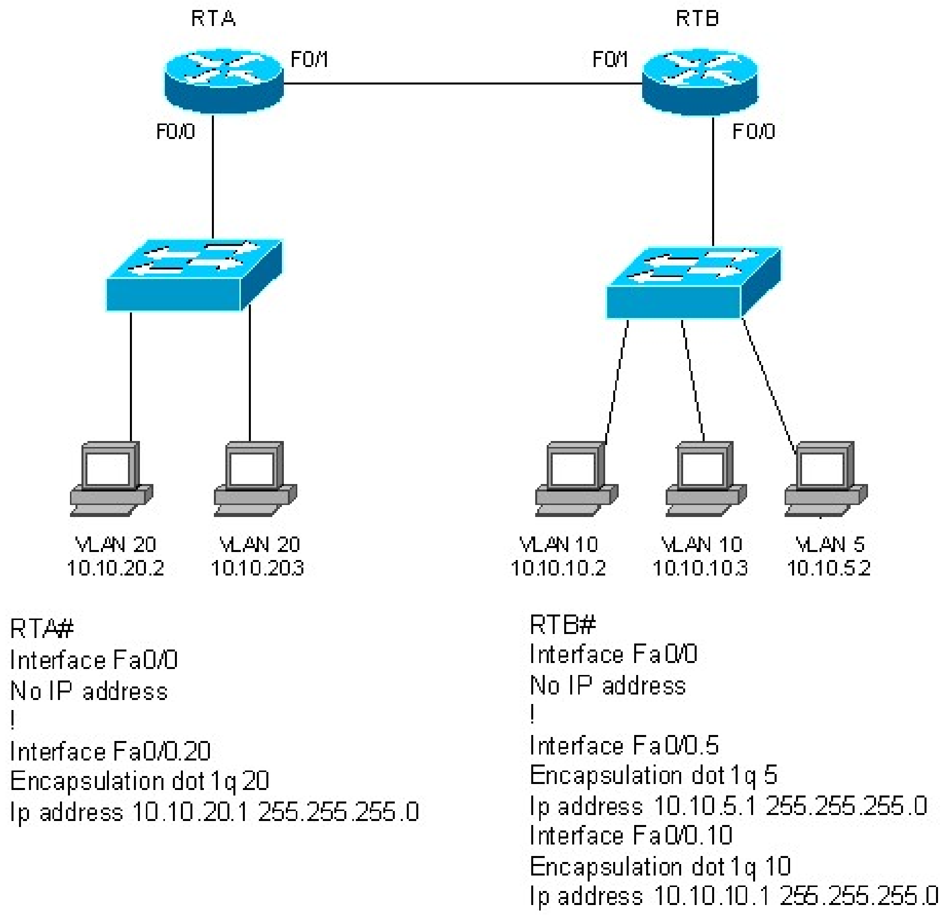


To allow IPv4 DHCP and stateless DHCP to operate correctly, indicate on the diagram, where the commands (ABC) should be configured on the appropriate device.
(You may use the reference letter (A,B,C)to refer to a command)
Incorrect, unnecessary or missing commands will result in a mark deduction.

3 marks



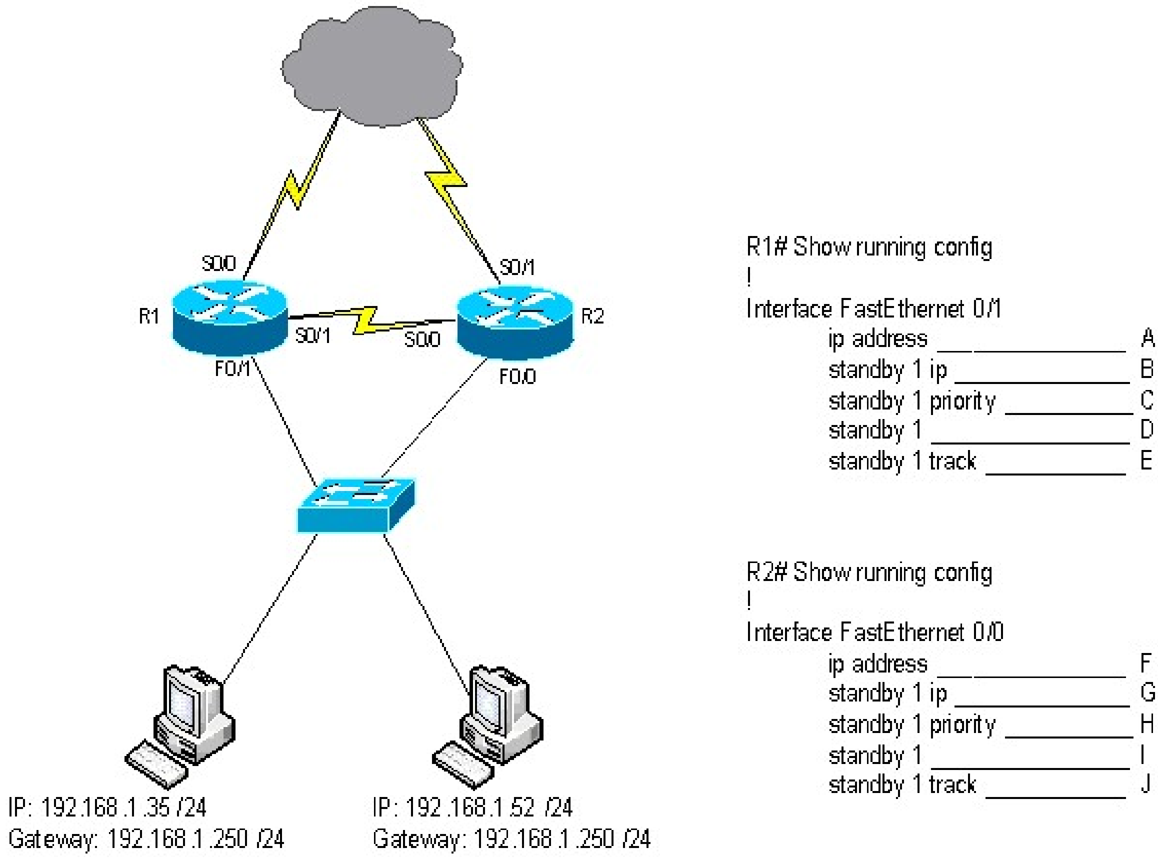
3. All hosts can successfully ping their default gateway, PCs on VLAN 5 and 10 can communicate with each other, but cannot communicate with any hosts on VLAN 20. The two routers can only ping their neighbors F0/1 interface and devices connected on their own F0/0 interface. Identify two potential reasons as to what might be the cause of the problem.



The first reason could be that there is no routing happening between the two routers. As such, the VLANs 20 does not know how to reach VLANs 5 and 10.

Another potential issue is that the hosts on VLAN 20 do not have a default gateway configured. As such, even though they can communicate with RTA at layer 2, they cannot reach any subnet beyond their own.

4.



Given the diagram above, fill in the lines (indicated by A-J) with the correct option (address, or keyword) to configure HSRP. R2 - F0/0 is to have the highest available address, R1 - F0/1 the next highest. R1 is to be primary active router, R2 is to have the ability to take over from R1 if R1 fails or has an interface fail, and R1 must be able to retake the active role once restored. 1 Mark will be deducted for each misconfigured line

A____192.168.1.253 255.255.255.0____

B_____192.168.1.250 255.255.255.0___

C_______110________

D_______preempt _____________

E______1___ decrement 20__________

F____192.168.1.254 255.255.255.0_________

G___192.168.1.250 255.255.255.0_____

H_______100__________

I_______preempt ____________

J_______1__ decrement 20 _________

SECTION 2: TECHNICAL BRIEF ON CISCO VSS

1.0 Introduction

The need for reliability at different levels of the three hierarchies (access, distribution and core layers) in modern enterprise networks has become increasingly a necessity. Hence, the use of redundant network elements and links in enterprise network architectures. However, this causes additional level of complexity to the design, implementation and operation of the network. The redundant hierarchical network design leads to challenges that relates with the management of per Virtual Local Area network (VLAN) Spanning Tree Protocol (STP), extensive routing topology, layer 2 and 3 reconvergences and additional overheads. Therefore, there is need for a technology that will provide expected level of redundancy without excessive overheads and complexities. It is on this premise that a Virtual Switching System (VSS) has been introduced.

VSS is a network system virtualization technology. VSS actualized this by simplifying the network through reduction in the number of network elements to be deployed, therefore, concealing the complexity involved in the management of redundant switches and links. It combines two switches (Cisco Catalyst 6500 series Switches) into one virtual switch. VSS helps in increasing operational efficiency by boosting nonstop communications. One of the virtual switch members act as an active virtual switch, while the other member is in standby state. Though, one virtual switch member is in a standby mode, both members still act in an active mode and forward the traffic. If it happens that one of the virtual switch members fails, there is no disruption occurs to the traffic flowing through the VSS and there is no convergence of protocols in the network.

2.0 Key concepts

2.1 Virtual Switching System

VSS is a system that combines two switches into a single switch. Any connection to the VSS will be via one logical port channel not two despite the VSS containing two switches. Furthermore, it can manage redundancy and load balancing using just this one logical port channel connection. It uses this concept to ensure a loop-free layer 2 network topology and reduction in layer 3 network topology by reducing the number of layer 3 network element it is connected to.

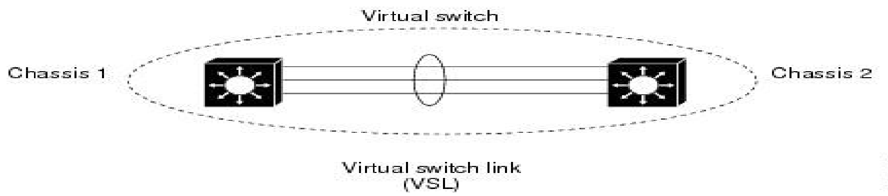


Figure 2-1 Overview of Virtual Switch System

2.2 Virtual Switch Link

The Virtual Switch Link (VSL) is the unique link that is responsible for transporting both the data and control traffic between the two switches (chassis). The VSL is developed using EtherChannel and can accommodate up to eight links. The control traffic is given priority over data traffic when transporting traffic over the VSL.

2.3 VSS Active and VSS Standby Chassis

The VSS consist of two switches (chassis) and once the VSS is created or rebooted, the roles of the two switches are negotiated. One switch (chassis) becomes the active and the other becomes the standby. The VSS active chassis does not only manage the VSS but also runs both layer 2 and layer 3 control protocols that are used to switch modules on both chassis.

While both switches (chassis) forwards traffic, the standby chassis forwards all control traffic to the active switch.

2.4 Dual Active Detection

If the VSL link fails completely, there won't be direct communication between the two switches, hence both switches will be in active mode because the standby switch will assume the active switch is down. This scenario is referred to as dual active scenario. The VSS uses Enhanced Port Aggregation Protocol (PAgP) and Dual Active Detection over IP Bidirectional Forwarding Detection (IP-BFD) to detect this scenario. Once detected, the VSS then goes through the dual active recovery process to ensure that standby switch return to its mode. This is actualized by shutting down all its interfaces of the standby chassis and renegotiating its role upon detection of the dual active scenario.

3.0 VSS Functionalities

The VSS has several functionalities, some of the main functionalities are as follows:

3.1 Redundancy and High Availability

This is the major function of the VSS. The supervisor engine redundancy uses the principle of Stateful SwitchOver (SSO) and NonStop Forwarding (NSF) to operate between the VSS active and standby chassis. The configuration and state information are constantly exchanged between the two chassis via the VSL. The VSS supervisor engine operates in standby mode and the standby chassis constantly monitors the active chassis via the VSL. If it detects that the active chassis fails, it initiates a switchover and takes on the active chassis role and if the failed chassis comes back online, it switches back to standby mode.

3.2 System management

The VSS uses the active supervisor engine to handle issues relating with control and management of the system. The active supervisor engine uses its command console to control both chassis. The active supervisor engine also handles the online insertion and removal of switching modules on both chassis. Though, the active chassis handles most of the management functionalities, the standby chassis still handles a subset of these, this includes power management.

3.3 Packet Handling

Asides of redundancy, high availability and system management, the VSS also handles packets by ensuring proper forwarding to appropriate destination. Both the active and standby chassis are actively responsible forwarding data traffic and as a result, the VSS active chassis constantly sends updates to the VSS standby chassis via the VSL. The active supervisor engine also uses the VSL the communicate the system information and protocol to the standby chassis.

4.0 Strengths and Weakness

The VSS design solution has provided a room to achieve high level of redundancy without adding a significant level of complexities as compared to traditional hierarchical redundant network. Furthermore, it offers the following strengths:

- Reduction of managed network elements by 50% and network latency
- Actualization of a loop-free network topology
- Provisioning of non-stop communications
- Relatively high throughput and faster convergence
- Maximization of bandwidth utilization, system and network usage
- Simplification of operational management

The major weakness is the fact that this technology is vendor specific, it can only be used with cisco switches and not compatible with other vendors. Also, additional virtual switching supervisor engines are required depending on the scale of implementation.

5.0 Deployment options

There are multiple scenarios in which VSS can be deployed. The VSS can be deployed in an enterprise or campus environment as well as in a data center environment. The technology can be deployed at distribution layer, core layer or both layers in an enterprise or campus network environment. In a data center environment, beyond the distribution and core layers, the VSS can be deployed even at the access layer for direct connections to servers.

When implementing VSS, for example when VSS 1440 is deployed at core, distribution and access layers. There would be only need for one switch instead of two at each layer. There would be unique benefits at each layer. For example, if VSS is only deployed at distribution layer, it will ensure loop-free topology and full bandwidth utilization with multi-chassis EtherChannel. It won't need STP and FHRP, less routing peers will be required and there will be single point of management. In case of failover, it will be stateful, so won't disrupt any applications or traffic through the distribution layer. If VSS is deployed at core and distribution layer, the benefits would be simplified network design and deterministic core failover. If VSS is deployed at core, distribution and access layers in a data center, this will help if the one of the links or switches fail, the second active link will be used to let the traffic flow and provides single point of management at access layer level. It will also provide a much-simplified network design and layer 2 topology scalability with no need of STP.

6.0 Notable References

1. Philip Nedev "Introducing Virtual Switch System (VSS)" available at https://www.cisco.com/c/dam/global/bg_bg/assets/expo/presentations/pnedev_VSS.pdf
2. Cisco "Catalyst 6500 Release 12.2SX Software Configuration Guide" available at https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vss.html#wp1062785
3. Cisco "Virtual Switching System (VSS) Best Practices" available at https://www.cisco.com/c/dam/global/da_dk/assets/docs/presentations/VSS_0109.pdf
4. Cisco "Catalyst 6500 Virtual Switching 1440" available at https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-virtual-switching-system-1440/product_solution_overview0900aecd806fa5d0.html

SECTION 3: GLBP ANALYSIS

1.0 Introduction

Upon electing an Active Virtual Gateway (AVG), the AVG assigns vMAC addresses associated with an Active Virtual Forwarders (AVFs). The AVG and the AVFs, communicate with each other using Hello, requests and response type messages in UDP packets using the multicast address of 224.0.0.102 on port 3222. In our case, because we have given L3-SW2 higher priority, it is the AVG. As such L3-SW2 will be handing out AVFs.

```
L3-SW2(config-if)#do sh glbp
Vlan25 - Group 25
  State is Active
    1 state change, last state change 14:13:35
  Virtual IP address is 172.16.25.254
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.080 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 172.16.25.2, priority 100 (expires in 8.672 sec)
  Priority 120 (configured)
  Weighting 200 (configured 200), thresholds: lower 100, upper 150
    Track object 15 state Up decrement 100
  Load balancing: round-robin
  Group members:
    0078.88cd.b1f1 (172.16.25.3) local
    54a2.7443.6971 (172.16.25.2)
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      5 state changes, last state change 13:15:30
    MAC address is 0007.b400.1901 (default)
    Owner ID is 0078.88cd.b1f1
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 200
    Client selection count: 26
  Forwarder 2
    State is Listen
    MAC address is 0007.b400.1902 (learnt)
    Owner ID is 54a2.7443.6971
    Redirection enabled, 598.688 sec remaining (maximum 600 sec)
    Time to live: 14398.688 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 172.16.25.2 (primary), weighting 100 (expires in 9.408 sec)
    Client selection count: 23
L3-SW2(config-if)#
```

Figure 3-2 L3-SW2 as AVG

Basic GLBP Configuration is like HSRP and VRRP. We will be using the same topology as our lab and converting VLAN 25 into GLBP for IPv4.

The configuration is as shown here:

```
!!!!! L3-SW1
Int vlan 25
      glbp 25 ip 172.16.25.254
      glbp 25 preempt

!!!! L3-SW2
Int vlan 25
      glbp 25 ip 172.16.25.254
      glbp 25 priority 120
      glbp 25 preempt
```

```
L3-SW2(config)#do sh glbp bri
Interface   Grp  Fwd Pri State    Address          Active router   Standby router
Vl25        25   -   120 Active   172.16.25.254    local           172.16.25.2
Vl25        25   1   -   Active   0007.b400.1901   local           -
Vl25        25   2   -   Listen   0007.b400.1902   172.16.25.2     -
L3-SW2(config)#
```

Figure 3-3 AVG and AVF result as of configuration

As seen in the output of "show glbp brief" and "show glbp", L3-SW2 is the active AVG, and is also the AVG for the vMAC address of 0007.b400.1901. As such, we know that if a client receives 0007.b400.1901 from the ARP reply for 172.16.25.254, then it is L3-SW2 as forwarder 1 is forwarding their traffic. Conversely, if 0007.b400.1902 responds to the ARP request, then L3-SW1 as forwarder 2 is forwarding for them.

Based on the MAC address, we can also tell what the GLPB group number is. The standard GLBP MAC address is 0007.b400.XXYY where XX is the group number and YY is the forwarder number. In our case, GLBP group number 25, the hex value of which is 19.

2.0 GBLP Hello and AVG Elections

GLBP Hello messages are typically related to AVG configuration and election. The states of AVG elections go from listen, speak and active/standby. As seen in the figure below, L3-SW1 (172.16.25.2) starts listening first, going to speaking and then to active first. It sends 3 listening packets messages before moving to Speak and then active within a short period of time. This is because L3-SW2's interface is still shutdown. After a short period of time, L3-SW2 (172.16.25.3) VLAN interface comes up as seen in packet 25. This results in an election as shown in packets 35 on as L3-SW1 goes from Active to speak to standby.

glbp

No.	Time	Source	Protocol	HW SRC	VG state?
7	5.812355	172.16.25.2	GLBP	Cisco_43:69:71	Listen
10	8.601079	172.16.25.2	GLBP	Cisco_43:69:71	Listen
13	11.482210	172.16.25.2	GLBP	Cisco_43:69:71	Listen
15	12.859245	172.16.25.2	GLBP	Cisco_43:69:71	Speak
16	13.051066	172.16.25.2	GLBP	Cisco_43:69:71	Active
19	14.235532	172.16.25.2	GLBP	Cisco_00:19:01	
20	14.556569	172.16.25.2	GLBP	Cisco_00:19:02	
24	15.999724	172.16.25.2	GLBP	Cisco_00:19:01	Active
25	16.001206	172.16.25.3	GLBP	Cisco_cd:b1:f1	Speak
32	18.627698	172.16.25.3	GLBP	Cisco_cd:b1:f1	Speak
33	18.728198	172.16.25.2	GLBP	Cisco_00:19:02	Active
34	18.730005	172.16.25.3	GLBP	Cisco_cd:b1:f1	Active
35	18.731895	172.16.25.2	GLBP	Cisco_00:19:01	Speak
39	21.479628	172.16.25.3	GLBP	Cisco_cd:b1:f1	Active
40	21.609204	172.16.25.2	GLBP	Cisco_00:19:02	Speak
43	24.200685	172.16.25.2	GLBP	Cisco_00:19:01	Speak
44	24.457273	172.16.25.3	GLBP	Cisco_cd:b1:f1	Active
49	26.957247	172.16.25.2	GLBP	Cisco_00:19:02	Speak
50	27.145485	172.16.25.3	GLBP	Cisco_cd:b1:f1	Active
52	28.717299	172.16.25.2	GLBP	Cisco_00:19:01	Standby
53	29.677027	172.16.25.3	GLBP	Cisco_cd:b1:f1	Active
57	31.566714	172.16.25.2	GLBP	Cisco_00:19:02	Standby

Figure 3-4 AVG election completed with L3-SW2 becoming AVG

Upon examining the hello packets, we can verify that the result in the election is due to the priority value. As seen in the figures below, L3-SW2 has a priority of 120 and L3-SW1 has a priority of 100. In the case that L3-SW2 goes down or if the priority drops below L3-SW1, then the L3-SW1 will take over as AVG for group 25 due to the preempt command.

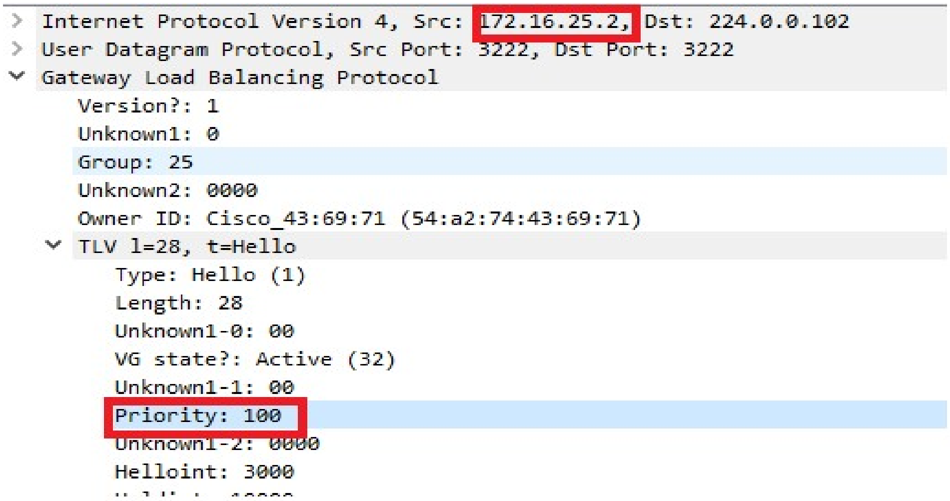


Figure 3-5 Priority of L3-SW1

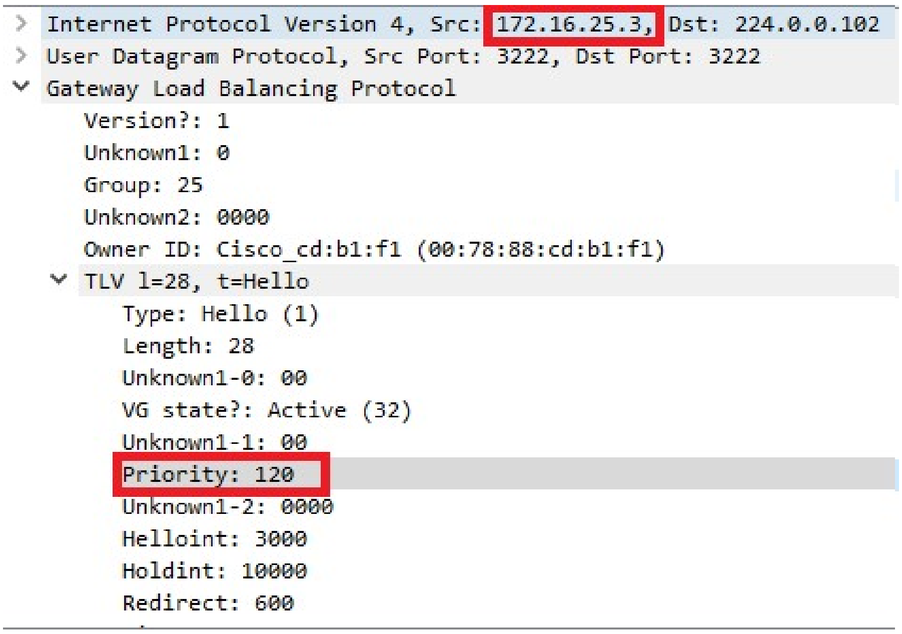


Figure 3-6 Priority of L3-SW2

3.0 Forwarder Requests/Responses

As previously mentioned, once the AVG election has been completed. The AVGs will distribute and respond to requests of vMAC address assignment through Request/Response messages as shown in the figure below.

Source	Protocol	HW SRC	Forwarder?	VF state?	Virtualmac	Pri
172.16.25.3	GLBP	Cisco_cd:b1:f1	1	Listen	00:07:b4:00:19:01	
172.16.25.2	GLBP	Cisco_00:19:01	1,2	Active,Active	00:07:b4:00:19:01,00:07:b4:00:19:02	
172.16.25.3	GLBP	Cisco_cd:b1:f1	1	Listen	00:07:b4:00:19:01	
172.16.25.2	GLBP	Cisco_00:19:02	1,2	Active,Active	00:07:b4:00:19:01,00:07:b4:00:19:02	
172.16.25.3	GLBP	Cisco_cd:b1:f1	1	Listen	00:07:b4:00:19:01	
172.16.25.3	GLBP	Cisco_cd:b1:f1	1	Listen	00:07:b4:00:19:01	
172.16.25.2	GLBP	Cisco_00:19:01	1,2	Active,Active	00:07:b4:00:19:01,00:07:b4:00:19:02	
172.16.25.2	GLBP	Cisco_00:19:02	1,2	Active,Active	00:07:b4:00:19:01,00:07:b4:00:19:02	
172.16.25.3	GLBP	Cisco_cd:b1:f1	1	Listen	00:07:b4:00:19:01	
172.16.25.2	GLBP	Cisco_00:19:01	1,2	Active,Active	00:07:b4:00:19:01,00:07:b4:00:19:02	
172.16.25.3	GLBP	Cisco_cd:b1:f1	1	Listen	00:07:b4:00:19:01	
172.16.25.2	GLBP	Cisco_00:19:02	1,2	Active,Active	00:07:b4:00:19:01,00:07:b4:00:19:02	
172.16.25.3	GLBP	Cisco_00:19:01	1	Active	00:07:b4:00:19:01	
172.16.25.3	GLBP	Cisco_00:19:01	1	Active	00:07:b4:00:19:01	
172.16.25.2	GLBP	Cisco_00:19:02	2	Active	00:07:b4:00:19:02	
172.16.25.3	GLBP	Cisco_00:19:01	1	Active	00:07:b4:00:19:01	
172.16.25.2	GLBP	Cisco_00:19:02	2	Active	00:07:b4:00:19:02	
172.16.25.3	GLBP	Cisco_00:19:01	1	Active	00:07:b4:00:19:01	
172.16.25.2	GLBP	Cisco_00:19:02	2	Active	00:07:b4:00:19:02	
172.16.25.3	GLBP	Cisco_00:19:01	1	Active	00:07:b4:00:19:01	
172.16.25.3	GLBP	Cisco_00:19:01	1	Active	00:07:b4:00:19:01	
172.16.25.2	GLBP	Cisco_00:19:02	2	Active	00:07:b4:00:19:02	

Figure 3-7 After AVG election is been completed, AFV will be assigned vMACs

AVFs will normally be distributed between the AVFs as shown in the last couple of packets. Note that per the 1024 maximum groups, only 4 AVFs are possible per group. L3-SW2 eventually becomes forward 1 as shown in the forwarder column and its vMAC will be naturally become 0007:b400:1901. Conversely, L3-SW1 that had both forwarding roles initially now takes only forwarding for vMAC address 0007:b400:1902 as forwarder 2.

4.0 Load Balancing Methods

There are 3 load balancing types available to GLBP. Those are round robin, weight based, and Host-dependent. The following subsections will briefly demonstrate those in action.

4.1 Round Robin Load Balancing

Once the vMACs have been assigned, the default method of load balancing is round robin. This means that each active forwarder will respond to an ARP request for them in sequence. Once AVF 1 has responded once, AVF 2 respond to the second request. The following request will then be answered by AVF 1 before going back to AVF 2. We can demonstrate this behavior repeating the process of ICMP echo request from a windows client, clearing the ARP cache, reinitiating an ICMP echo request, and verifying the ARP cache as shown below. Some information in the following figure have been removed for brevity.

```
C:\Windows\system32>ping 172.16.25.254 -n 1

Pinging 172.16.25.254 with 32 bytes of data:
Reply from 172.16.25.254: bytes=32 time=1ms TTL=254

Ping statistics for 172.16.25.254:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Windows\system32>arp -a

Interface: 172.16.25.55 --- 0xf
  Internet Address      Physical Address      Type
  172.16.25.254         00-07-b4-00-19-01     dynamic
  224.0.0.10            01-00-5e-00-00-0a     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.102           01-00-5e-00-00-66     static

C:\Windows\system32>arp -d

C:\Windows\system32>ping 172.16.25.254 -n 1

Pinging 172.16.25.254 with 32 bytes of data:
Reply from 172.16.25.254: bytes=32 time=3ms TTL=254
C:\Windows\system32>arp -a

Interface: 172.16.25.55 --- 0xf
  Internet Address      Physical Address      Type
  172.16.25.254         00-07-b4-00-19-02     dynamic
  224.0.0.10            01-00-5e-00-00-0a     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.102           01-00-5e-00-00-66     static

C:\Windows\system32>arp -d

C:\Windows\system32>ping 172.16.25.254 -n 1

Pinging 172.16.25.254 with 32 bytes of data:
Reply from 172.16.25.254: bytes=32 time=3ms TTL=254
```

Figure 3-8 Round Robin in action Part 1, switches from 01 forwarder to 02 forwarder after cache clear

```
C:\Windows\system32>arp -a

Interface: 172.16.25.55 --- 0xf
  Internet Address      Physical Address      Type
  172.16.25.254         00-07-b4-00-19-01     dynamic
  224.0.0.10            01-00-5e-00-00-0a     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.102           01-00-5e-00-00-66     static

C:\Windows\system32>arp -d

C:\Windows\system32>arp -a

Interface: 172.16.25.55 --- 0xf
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.102           01-00-5e-00-00-66     static

C:\Windows\system32>ping 172.16.25.254 -n 1

Pinging 172.16.25.254 with 32 bytes of data:
Reply from 172.16.25.254: bytes=32 time=3ms TTL=254

C:\Windows\system32>arp -a

Interface: 172.16.25.55 --- 0xf
  Internet Address      Physical Address      Type
  172.16.25.254         00-07-b4-00-19-02     dynamic
  224.0.0.10            01-00-5e-00-00-0a     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.102           01-00-5e-00-00-66     static

C:\Windows\system32>
```

Figure 3-9 Round Robin in action part 2, after cache clear and ping the f01 has responded to the ARP request

As you can see from the ARP cache, each forwarder responds in succession once the other has responded. We can further verify with Wireshark as shown below:

No.	Time	Source	Destination	Protocol	Length	HW SRC	HW DST	Info
8	2.992449	172.16.25.55	172.16.25.254	ICMP	74	VMware_d2:c0:57	Cisco_00:19:01	Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (reply in 9)
9	2.994212	172.16.25.254	172.16.25.55	ICMP	74	Cisco_cd:b1:f1	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=30/7680, ttl=254 (request in 8)
23	9.527282	VMware_d2:c0:57	Broadcast	ARP	42	VMware_d2:c0:57	Broadcast	Who has 172.16.25.254? Tell 172.16.25.55
24	9.529057	Cisco_cd:b1:f1	VMware_d2:c0:57	ARP	60	Cisco_cd:b1:f1	VMware_d2:c0:57	172.16.25.254 is at 00:07:b4:00:19:02
25	9.529100	172.16.25.55	172.16.25.254	ICMP	74	VMware_d2:c0:57	Cisco_00:19:02	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (reply in 26)
26	9.530713	172.16.25.254	172.16.25.55	ICMP	74	Cisco_43:69:71	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=31/7936, ttl=254 (request in 25)
44	18.949882	VMware_d2:c0:57	Broadcast	ARP	42	VMware_d2:c0:57	Broadcast	Who has 172.16.25.254? Tell 172.16.25.55
45	18.951597	Cisco_cd:b1:f1	VMware_d2:c0:57	ARP	60	Cisco_cd:b1:f1	VMware_d2:c0:57	172.16.25.254 is at 00:07:b4:00:19:01
46	18.951624	172.16.25.55	172.16.25.254	ICMP	74	VMware_d2:c0:57	Cisco_00:19:01	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (reply in 47)
47	18.952908	172.16.25.254	172.16.25.55	ICMP	74	Cisco_cd:b1:f1	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=32/8192, ttl=254 (request in 46)
117	37.495834	VMware_d2:c0:57	Broadcast	ARP	42	VMware_d2:c0:57	Broadcast	Who has 172.16.25.254? Tell 172.16.25.55
118	37.497733	Cisco_cd:b1:f1	VMware_d2:c0:57	ARP	60	Cisco_cd:b1:f1	VMware_d2:c0:57	172.16.25.254 is at 00:07:b4:00:19:02
119	37.497769	172.16.25.55	172.16.25.254	ICMP	74	VMware_d2:c0:57	Cisco_00:19:02	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 120)
120	37.499160	172.16.25.254	172.16.25.55	ICMP	74	Cisco_43:69:71	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=33/8448, ttl=254 (request in 119)

Figure 3-10 GLBP Round Robin demonstrated in Wireshark

Demonstratable, despite using the same L3 address for the ICMP echo requests, the hardware address has a consistent pattern every time the ARP cache has been cleared and new ARP requests are made. That pattern being that it rotates amongst all available forwarders.

4.2 Weight-based Load Balancing

Weight can be assigned to GLBP ASFs. Rather than responding in round robin, the number of responses given by any ASF will be the ratio derived from the ASFs weight divided by the sum of all ASF weights. Take the following configuration for example:

```
!! L3-SW2
interface vlan 25
      glbp 25 ip 172.16.25.254
      glbp 25 priority 120
      glbp 25 preempt
      glbp 25 weighting 200
      glbp 25 load-balancing weighted
!! L3-SW1
 interface vlan 25
      glbp 25 ip 172.16.25.254
      glbp 25 preempt
      glbp 25 weighting 100
      glbp 25 load-balancing weighted
```

We can verify that this weight information is being shared amongst the GLBP devices as show in the following two figures:

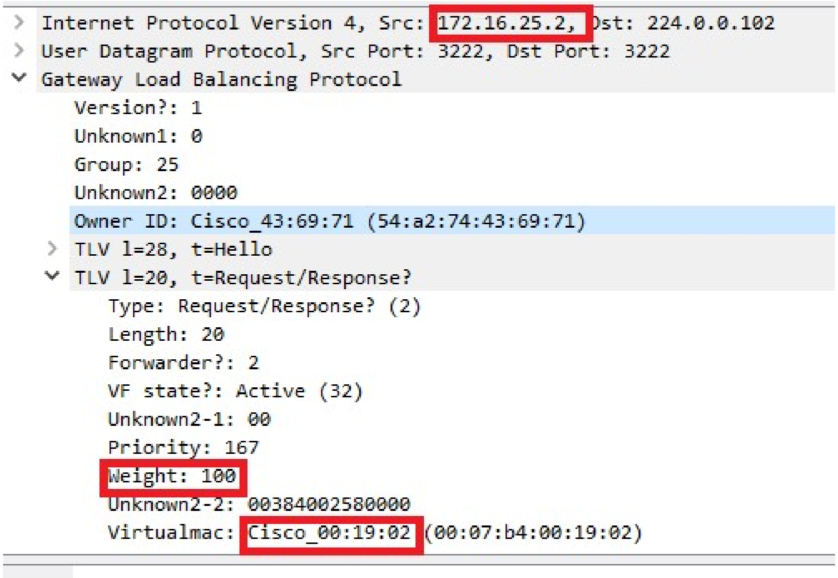


Figure 3-11 Weight as specified in configuration for L3-SW1 in Wireshark

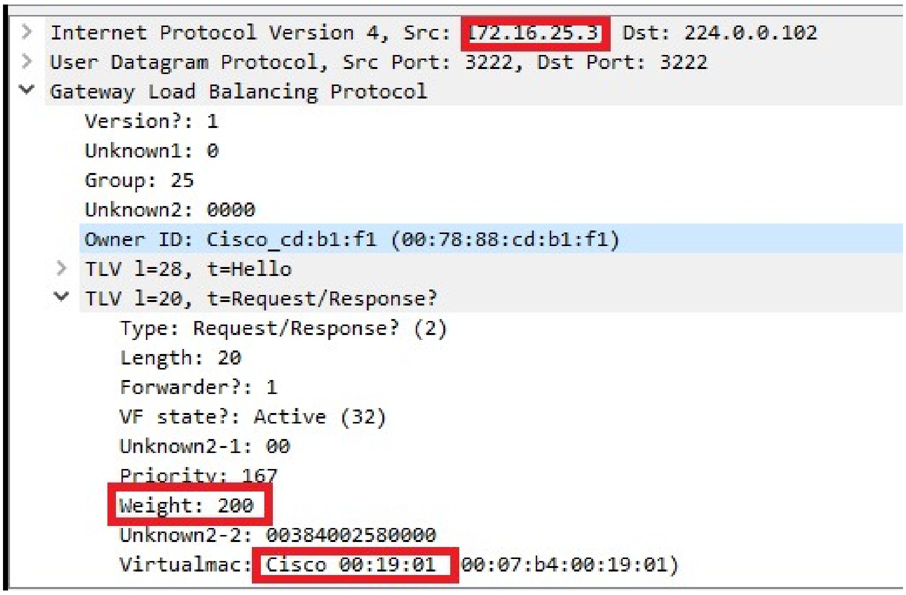
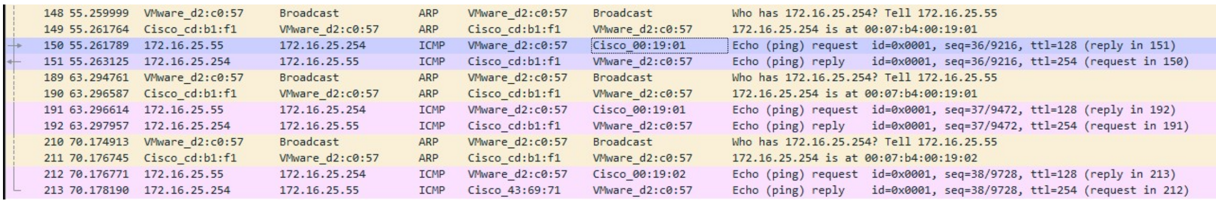


Figure 3-12 Weight as specified in configuration for L3-SW2 in Wireshark

As per the weighting, L3-SW2 should respond to the ARP requests $2/3^{rd}$ s of the time (200/300) and L3 -SW1 should respond to $1/3^{rd}$ s of the time (100/300). To demonstrate, 3 echo requests will be sent with the ARP cache being cleared in between each echo request.

```
C:\Windows\system32>arp -a

Interface: 172.16.25.55 --- 0xf
  Internet Address      Physical Address      Type
  172.16.25.254         00-07-b4-00-19-01     dynamic
  224.0.0.10            01-00-5e-00-00-0a     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.102           01-00-5e-00-00-66     static

C:\Windows\system32>arp -d

C:\Windows\system32>ping 172.16.25.254 -n 1

Pinging 172.16.25.254 with 32 bytes of data:
Reply from 172.16.25.254: bytes=32 time=3ms TTL=254

Ping statistics for 172.16.25.254:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\Windows\system32>arp -a

Interface: 172.16.25.55 --- 0xf
  Internet Address      Physical Address      Type
  172.16.25.254         00-07-b4-00-19-01     dynamic
  224.0.0.10            01-00-5e-00-00-0a     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.102           01-00-5e-00-00-66     static

C:\Windows\system32>arp -d

C:\Windows\system32>ping 172.16.25.254 -n 1

Pinging 172.16.25.254 with 32 bytes of data:
Reply from 172.16.25.254: bytes=32 time=3ms TTL=254

Ping statistics for 172.16.25.254:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\Windows\system32>arp -a

Interface: 172.16.25.55 --- 0xf
  Internet Address      Physical Address      Type
  172.16.25.254         00-07-b4-00-19-02     dynamic
  224.0.0.10            01-00-5e-00-00-0a     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.102           01-00-5e-00-00-66     static

C:\Windows\system32>                    Microsoft Edge
```

Figure 3 13 Load Balance; of the 3 echo requests and cache clears, two were from forwarder 1 and one was from forwarder 2



148	55.259999	VMware_d2:c0:57	Broadcast	ARP	VMware_d2:c0:57	Broadcast	Who has 172.16.25.254? Tell 172.16.25.55
149	55.261764	Cisco_cd:b1:f1	VMware_d2:c0:57	ARP	Cisco_cd:b1:f1	VMware_d2:c0:57	172.16.25.254 is at 00:07:b4:00:19:01
150	55.261789	172.16.25.55	172.16.25.254	ICMP	VMware_d2:c0:57	Cisco_00:19:01	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 151)
151	55.263125	172.16.25.254	172.16.25.55	ICMP	Cisco_cd:b1:f1	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=36/9216, ttl=254 (request in 150)
189	63.294761	VMware_d2:c0:57	Broadcast	ARP	VMware_d2:c0:57	Broadcast	Who has 172.16.25.254? Tell 172.16.25.55
190	63.296587	Cisco_cd:b1:f1	VMware_d2:c0:57	ARP	Cisco_cd:b1:f1	VMware_d2:c0:57	172.16.25.254 is at 00:07:b4:00:19:01
191	63.296614	172.16.25.55	172.16.25.254	ICMP	VMware_d2:c0:57	Cisco_00:19:01	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply in 192)
192	63.297957	172.16.25.254	172.16.25.55	ICMP	Cisco_cd:b1:f1	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=37/9472, ttl=254 (request in 191)
210	70.174913	VMware_d2:c0:57	Broadcast	ARP	VMware_d2:c0:57	Broadcast	Who has 172.16.25.254? Tell 172.16.25.55
211	70.176745	Cisco_cd:b1:f1	VMware_d2:c0:57	ARP	Cisco_cd:b1:f1	VMware_d2:c0:57	172.16.25.254 is at 00:07:b4:00:19:02
212	70.176771	172.16.25.55	172.16.25.254	ICMP	VMware_d2:c0:57	Cisco_00:19:02	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply in 213)
213	70.178190	172.16.25.254	172.16.25.55	ICMP	Cisco_43:69:71	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=38/9728, ttl=254 (request in 212)

Figure 3-14 In Wireshark, L3-SW2 responds two times out of 3 as per the weight.

As shown above, the L3 address remains the same. However, two of the three ARP responses for 172.16.25.254 come from vMAC 00007:b400:1902 associated with L3-SW1 AVF 2.

4.3 Host Based load balancing

With host-based load balancing, GLBP will track hosts request and respond only with the initial vMAC offered. The following configuration will demonstrate this:

```
interface vlan 25
      glbp 25 ip 172.16.25.254
      glbp 25 priority 120
      glbp 25 preempt
      glbp 25 load-balancing host-dependent

!! L3-SW1
 interface vlan 25
      glbp 25 ip 172.16.25.254
      glbp 25 preempt
      glbp 25 load-balancing host-dependent
```

Administrator: Command Prompt

```
C:\Windows\system32>arp -a

Interface: 172.16.25.55 --- 0xf
  Internet Address      Physical Address      Type
  172.16.25.254         00-07-b4-00-19-02     dynamic
  224.0.0.10            01-00-5e-00-00-0a     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.102           01-00-5e-00-00-66     static

C:\Windows\system32>arp -d

C:\Windows\system32>ping 172.16.25.254 -n 1

Pinging 172.16.25.254 with 32 bytes of data:
Reply from 172.16.25.254: bytes=32 time=4ms TTL=254

Ping statistics for 172.16.25.254:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\Windows\system32>arp -a

Interface: 172.16.25.55 --- 0xf
  Internet Address      Physical Address      Type
  172.16.25.254         00-07-b4-00-19-02     dynamic
  224.0.0.10            01-00-5e-00-00-0a     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.102           01-00-5e-00-00-66     static

C:\Windows\system32>arp -d

C:\Windows\system32>ping 172.16.25.254 -n 1

Pinging 172.16.25.254 with 32 bytes of data:
Reply from 172.16.25.254: bytes=32 time=3ms TTL=254

Ping statistics for 172.16.25.254:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\Windows\system32>arp -a

Interface: 172.16.25.55 --- 0xf
  Internet Address      Physical Address      Type
  172.16.25.254         00-07-b4-00-19-02     dynamic
  224.0.0.10            01-00-5e-00-00-0a     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.102           01-00-5e-00-00-66     static

C:\Windows\system32>_
```

Figure 3-15 Host-dependent GLBP results in the host receiving the same vMAC every time it makes the request.

23	9.254043	VMware_d2:c0:57	Broadcast	ARP	VMware_d2:c0:57	Broadcast	Who has 172.16.25.254? Tell 172.16.25.55
24	9.256482	Cisco_cd:b1:f1	VMware_d2:c0:57	ARP	Cisco_cd:b1:f1	VMware_d2:c0:57	172.16.25.254 is at 00:07:b4:00:19:02
25	9.256517	172.16.25.55	172.16.25.254	ICMP	VMware_d2:c0:57	Cisco_00:19:02	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (reply in 26)
26	9.259466	172.16.25.254	172.16.25.55	ICMP	Cisco_43:69:71	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=39/9984, ttl=254 (request in 25)
39	14.997767	172.16.25.55	172.16.25.254	ICMP	VMware_d2:c0:57	Cisco_00:19:02	Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (reply in 40)
40	14.999922	172.16.25.254	172.16.25.55	ICMP	Cisco_43:69:71	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=40/10240, ttl=254 (request in 39)
52	21.461415	172.16.25.55	172.16.25.254	ICMP	VMware_d2:c0:57	Cisco_00:19:02	Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (reply in 53)
53	21.463038	172.16.25.254	172.16.25.55	ICMP	Cisco_43:69:71	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=41/10496, ttl=254 (request in 52)
63	27.523337	VMware_d2:c0:57	Broadcast	ARP	VMware_d2:c0:57	Broadcast	Who has 172.16.25.254? Tell 172.16.25.55
64	27.525515	Cisco_cd:b1:f1	VMware_d2:c0:57	ARP	Cisco_cd:b1:f1	VMware_d2:c0:57	172.16.25.254 is at 00:07:b4:00:19:02
65	27.525541	172.16.25.55	172.16.25.254	ICMP	VMware_d2:c0:57	Cisco_00:19:02	Echo (ping) request id=0x0001, seq=42/10752, ttl=128 (reply in 66)
66	27.527321	172.16.25.254	172.16.25.55	ICMP	Cisco_43:69:71	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=42/10752, ttl=254 (request in 65)
80	34.090868	VMware_d2:c0:57	Broadcast	ARP	VMware_d2:c0:57	Broadcast	Who has 172.16.25.254? Tell 172.16.25.55
81	34.092569	Cisco_cd:b1:f1	VMware_d2:c0:57	ARP	Cisco_cd:b1:f1	VMware_d2:c0:57	172.16.25.254 is at 00:07:b4:00:19:02
82	34.092618	172.16.25.55	172.16.25.254	ICMP	VMware_d2:c0:57	Cisco_00:19:02	Echo (ping) request id=0x0001, seq=43/11008, ttl=128 (reply in 83)
83	34.094011	172.16.25.254	172.16.25.55	ICMP	Cisco_43:69:71	VMware_d2:c0:57	Echo (ping) reply id=0x0001, seq=43/11008, ttl=254 (request in 82)

Figure 3-16 Host-Dependent GLBP Results in Wireshark

As shown in the above two figures, each time the cache has been cleared, the same vMAC address from forwarder 2 has been received from the ARP request.

5.0 References

1. Andy "GLBP Weights, Load Balancing, and Redirection" available at https://cisconinja.wordpress.com/2009/02/11/glbp-weights-load-balancing-and-redirection/, February 2009

SECTION 4: DEVICE CONFIGURATIONS

This section will include a list of relevant commands we used, and why these configurations meet the requirements of the lab.

1.0 VLAN

Commands:

```
vlan 5
      name Server
vlan 10
      name IT
vlan 15
      name Finance
vlan 20
      name Sales
vlan 25
      name Management
vlan 666
      name parkinglot
      Interface vlan 666
      shutdown
```

Implemented these commands on all four switches. The reason being, in our lab setup, we did not plan on using VTP server & client model to distribute VLANs from one switch to the rests. Regarding the exit command, you need to type that down every time you have finished creating a VLAN, otherwise that VLAN will not register to the VLAN database. We have made a VLAN 666 for parking all unused ports and shut the VLAN interface down, because it's a best practice to store away all unused ports into segregated VLAN.

```
L2-SW1(config)#do sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
5    Server                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
10   IT                               active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
15   Finance                          active
20   Sales                            active
25   management                       active
666  parkinglot                       act/lshut Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
L2-SW1(config)#
L2-SW2(config-if-range)#do sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
5    Server                           active
10   IT                               active
15   Finance                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
20   sales                            active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
25   Management                       active
666  parkinglot                       act/lshut Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figure 4-1 VLAN details

2.0 DHCP

Commands:

```
ip dhcp excluded-address 172.16.5.252 172.16.5.254

ip dhcp excluded-address 172.16.20.252 172.16.20.254

ip dhcp excluded-address 172.16.10.252 172.16.10.254

ip dhcp excluded-address 172.16.15.252 172.16.15.254
```

Implemented on R1, the DHCP server, because you do not want your DHCP client to potentially take an in used statically configured IP on network devices, which would create duplicate IP address.

```
R1(config)#do sh ip dhcp pool

Pool 5 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 2
 Excluded addresses             : 3
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 172.16.5.12          172.16.5.1       - 172.16.5.254      2     / 3     / 254

Pool 10 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 2
 Excluded addresses             : 3
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 172.16.10.21         172.16.10.1      - 172.16.10.254     2     / 3     / 254

Pool 15 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 4
 Excluded addresses             : 3
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 172.16.15.13         172.16.15.1      - 172.16.15.254     4     / 3     / 254

Pool 20 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 3
 Excluded addresses             : 3
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 172.16.20.18         172.16.20.1      - 172.16.20.254     3     / 3     / 254
```

Figure 4-17 DHCP pool details highlighting excluded addresses

Command: "`default-router 172.16.5.254`" on R1, under ip dhcp pool configuration.

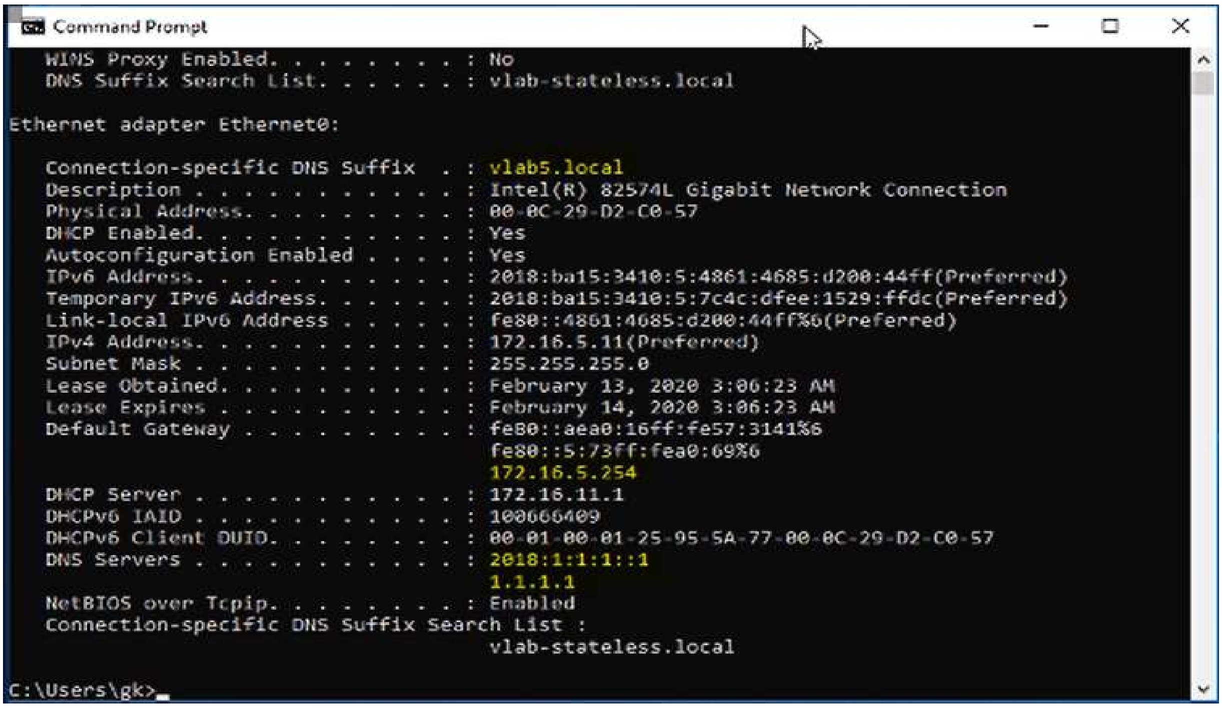
This command is a way to tell IPv4 DHCP clients which address to use for their default gateway.

Command: "`domain-name vlab(vlan number).local" on R1,` under ip/ipv6 dhcp pool.

This command displays DNS domain suffix name. Beside VLAN identification on addresses' octets, we could use a DNS suffix to define which VLAN is the client on.

Command: "`dns-server 1.1.1.1`" on R1, under ip/ipv6 dhcp pool configuration.

This command specifies DNS server that client should use for resolving names into IPs.

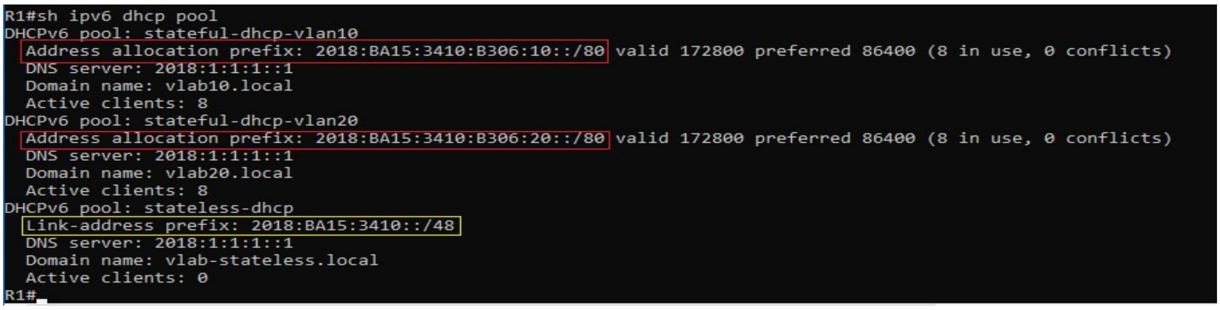


```
Command Prompt
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : vlab-stateless.local

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : vlab5.local
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-D2-C0-57
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2018:ba15:3410:5:4861:4685:d200:44ff(Preferred)
   Temporary IPv6 Address. . . . . . : 2018:ba15:3410:5:7c4c:dfee:1529:ffdc(Preferred)
   Link-local IPv6 Address . . . . . : fe80::4861:4685:d200:44ff%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.5.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : February 13, 2020 3:06:23 AM
   Lease Expires . . . . . . . . . . : February 14, 2020 3:06:23 AM
   Default Gateway . . . . . . . . . : fe80::aea0:16ff:fe57:3141%6
                                       fe80::5:73ff:fea0:69%6
                                       172.16.5.254
   DHCP Server . . . . . . . . . . . : 172.16.11.1
   DHCPv6 IAID . . . . . . . . . . . : 100666409
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-95-5A-77-00-0C-29-D2-C0-57
   DNS Servers . . . . . . . . . . . : 2018:1:1:1::1
                                       1.1.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       vlab-stateless.local

C:\Users\gk>
```

Figure 4-18 Configured DHCP pool options by a DHCP client

Command: "`address prefix 2018:BA15:3410:B306:(10/20)::/80`" for stateful DHCPv6 config, and "`link-address 2018:BA15:3410::/48`" for stateless DHCPv6 config on R1. These two commands define the type of DHCPv6 pool, whether it would be a stateless or stateful DHCPv6 pool.

Command: "`ipv6 nd other-config-flag`" on L3 Switch 1 and 2 under VLAN 5 and 15 for stateless DHCP address assigning, and; command: "`ipv6 nd managed-config-flag`" on L3 Switch 1 and 2 under VLAN 10 and 20 for stateful DHCP address assigning

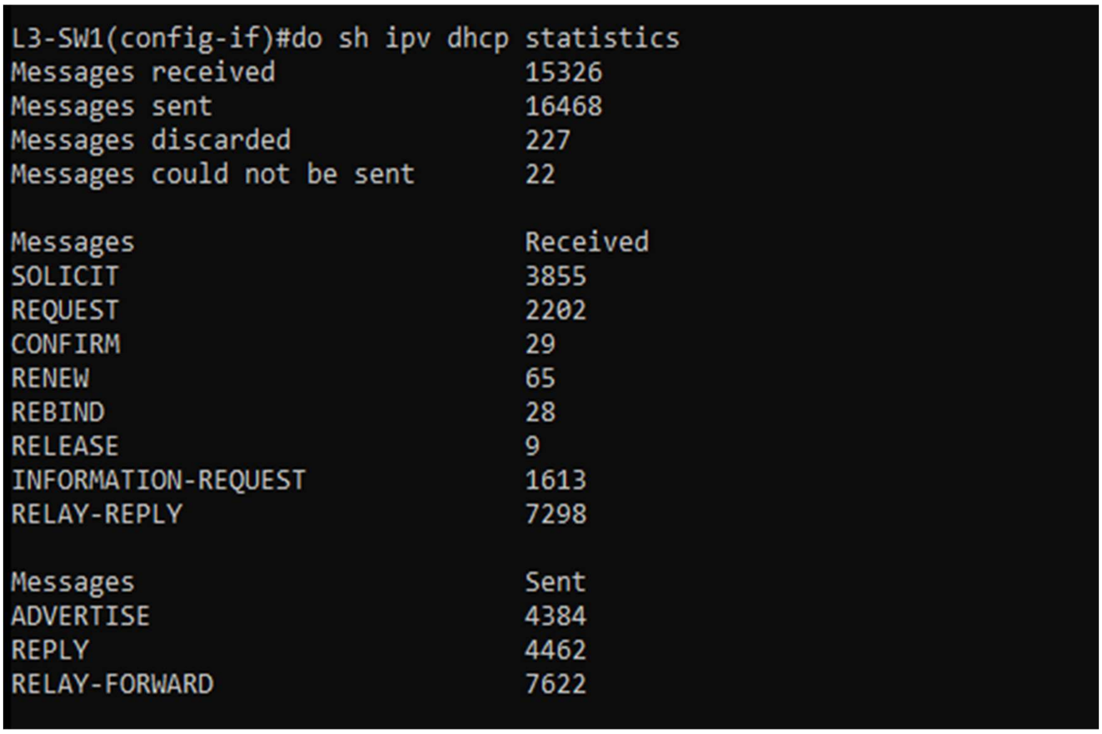


```
R1#sh ipv6 dhcp pool
DHCPv6 pool: stateful-dhcp-vlan10
  Address allocation prefix: 2018:BA15:3410:B306:10::/80 valid 172800 preferred 86400 (8 in use, 0 conflicts)
  DNS server: 2018:1:1:1::1
  Domain name: vlab10.local
  Active clients: 8
DHCPv6 pool: stateful-dhcp-vlan20
  Address allocation prefix: 2018:BA15:3410:B306:20::/80 valid 172800 preferred 86400 (8 in use, 0 conflicts)
  DNS server: 2018:1:1:1::1
  Domain name: vlab20.local
  Active clients: 8
DHCPv6 pool: stateless-dhcp
  Link-address prefix: 2018:BA15:3410::/48
  DNS server: 2018:1:1:1::1
  Domain name: vlab-stateless.local
  Active clients: 0
R1#
```

Figure 4-4 DHCP pool for IPv6 with prefix highlighted

Command: "`ipv6 dhcp server automatic rapid-commit allow-hint`" on R1. Rapid-commit makes dhcpv6 negotiation faster, allow hint allows dhcpv6 server to use the segment it received the request from to figure out which pool to use. P.S. no show command that supports this command.

Command: “`ip helper-address 1.1.1.1`” for IPv4 and “`ipv6 dhcp relay destination <2018:BA15:3410:11::1 | 2018:BA15:3410:12::1> GigabitEthernet1/0/17`” for IPv6 on L3 switch 1 and L3 switch 2 under vlan5, 10, 15, 20. These 2 commands would relay DHCP traffic to addresses specified on the command, in IPv6 case you also specify exit interface.



```
L3-SW1(config-if)#do sh ipv dhcp statistics
Messages received                15326
Messages sent                    16468
Messages discarded               227
Messages could not be sent       22

Messages                         Received
SOLICIT                          3855
REQUEST                          2202
CONFIRM                          29
RENEW                            65
REBIND                           28
RELEASE                          9
INFORMATION-REQUEST              1613
RELAY-REPLY                      7298

Messages                         Sent
ADVERTISE                        4384
REPLY                            4462
RELAY-FORWARD                    7622
```

Figure 4-19 DHCP statistics showing DHCP negotiations

3.0 HSRP

Commands:

```
track 5 interface GigabitEthernet1/0/17 line-protocol

track 10 interface GigabitEthernet1/0/17 line-protocol

Interface vlan 5

      standby 5 track 5 decrement 20

      standby 5 priority 110
```

```
      standby 105 track 5 decrement 20
      standby 105 priority 110
interface vlan 10
      standby 10 track 10 decrement 20
      standby 10 priority 110
      standby 110 track 10 decrement 20
      standby 110 priority 110
```

Implemented on L3 Switch 1.

Commands:

```
track 15 interface GigabitEthernet1/0/17 line-protocol
track 20 interface GigabitEthernet1/0/17 line-protocol
interface vlan 15
      standby 15 track 15 decrement 20
      standby 15 priority 110
      standby 115 track 15 decrement 20
      standby 115 priority 110
interface vlan 20
      Standby 20 track 20 decrement 20
      standby 20 priority 110
      standby 120 track 20 decrement 20
      standby 120 priority 110
```

Implemented on L3 Switch 2.

This set of command tracks credibility of an interface in HSRP operation. If an interface goes down the priority will be decremented by 20 each time.

```
L3-SW1(config-if)#do sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl5         5    110 P Active  local           172.16.5.253    172.16.5.254
Vl5         105  110 P Active  local           FE80::3         FE80::5:73FF:FEA0:69
Vl10        10   110 P Active  local           172.16.10.253   172.16.10.254
Vl10        110  110 P Active  local           FE80::3         FE80::5:73FF:FEA0:6E
Vl15        15   100 P Standby 172.16.15.253   local           172.16.15.254
Vl15        115  100 P Standby FE80::3         local           FE80::5:73FF:FEA0:73
Vl20        20   100 P Standby 172.16.20.253   local           172.16.20.254
Vl20        120  100 P Standby FE80::3         local           FE80::5:73FF:FEA0:78
Vl25        25   110 P Active  local           172.16.25.3     172.16.25.254
L3-SW1(config-if)#
```

Figure 4-20 HSRP brief

Commands:

```
interface vlan 5
      standby 5 preempt
      standby 105 preempt
interface vlan 10
      standby 10 preempt
      standby 110 preempt
interface vlan 15
      standby 15 preempt
      standby 115 preempt
interface vlan 20
      standby 20 preempt
      standby 120 preempt
```

Implemented on L3 switch 1 and 2. These commands allow switch interface with higher priority than the current active HSRP interface to become an active HSRP interface, instead of waiting until the active HSRP interface priority goes down to 0, to change an HSRP active interface.

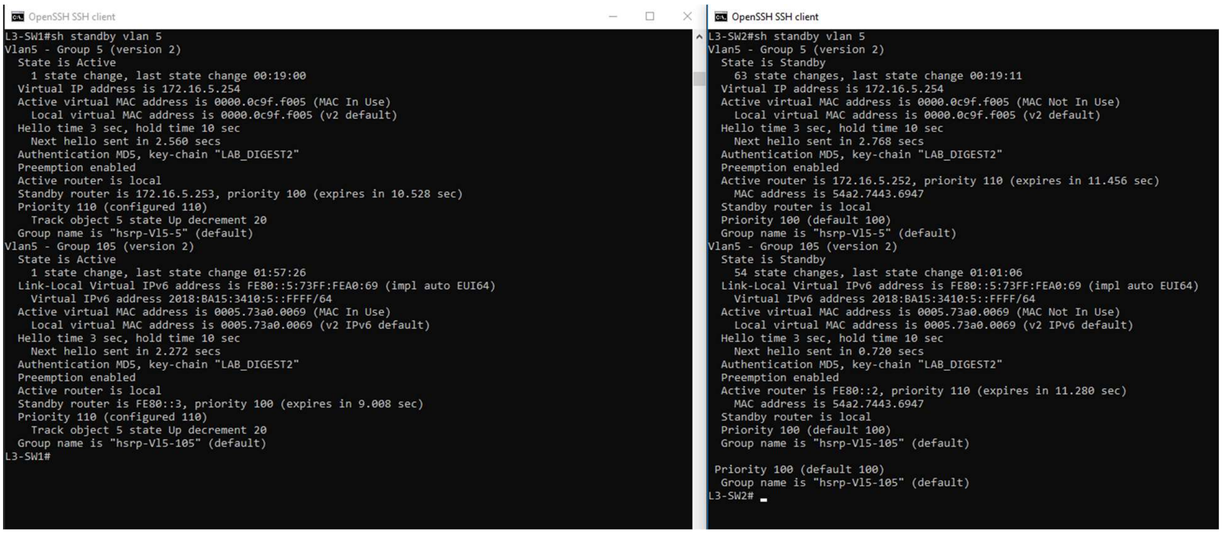


Figure 4-21 HSRP Details for VLAN 5

Note: L3-SW1 has standby priority of 110, and right side L3-SW2 has standby priority of 100.

Commands:

```
interface vlan 5
        standby 5 ip 172.16.5.254
        standby 105 ipv6 2018:BA15:3410:B306:5::FFFF/80
interface vlan 10
        standby 10 ip 172.16.10.254
        standby 110 ipv6 2018:BA15:3410:B306:10::FFFF/80
interface vlan 15
        standby 15 ip 172.16.15.254
        standby 115 ipv6 2018:BA15:3410:B306:15::FFFF/80
interface vlan 20
        standby 20 ip 172.16.20.254
        standby 120 ipv6 2018:BA15:3410:B306:20::FFFF/80
```

Implement on L3 switch 1 and 2. This set of commands are used to make a virtual IP address for HSRPv4 and HSRPv6 instances. That's how HSRP communicate with HSRP on another device, and those virtual IPv4 and IPv6 must match on different devices as well as the group ID.

```
L3-SW1(config-if)#do sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl5         5    110 P Active  local           172.16.5.253    172.16.5.254
Vl5         105  110 P Active  local           FE80::3         FE80::5:73FF:FEA0:69
Vl10        10   110 P Active  local           172.16.10.253   172.16.10.254
Vl10        110  110 P Active  local           FE80::3         FE80::5:73FF:FEA0:6E
Vl15        15   100 P Standby 172.16.15.253   local           172.16.15.254
Vl15        115  100 P Standby FE80::3         local           FE80::5:73FF:FEA0:73
Vl20        20   100 P Standby 172.16.20.253   local           172.16.20.254
Vl20        120  100 P Standby FE80::3         local           FE80::5:73FF:FEA0:78
Vl25        25   110 P Active  local           172.16.25.3     172.16.25.254
L3-SW1(config-if)#
```

Figure 4-22 HSRP Virtual IP addresses

Commands:

```
key chain LAB_DIGEST2
 key 100
  key-string 7 110A1016141D
Interface vlan 5
      standby 5 authentication md5 key-chain LAB_DIGEST2
      standby 105 authentication md5 key-chain LAB_DIGEST2
Interface vlan 10
      standby 10 authentication md5 key-chain LAB_DIGEST2
      standby 110 authentication md5 key-chain LAB_DIGEST2
Interface vlan 15
      standby 15 authentication md5 key-chain LAB_DIGEST2
      standby 115 authentication md5 key-chain LAB_DIGEST2
Interface vlan 20
      standby 20 authentication md5 key-chain LAB_DIGEST2
      standby 120 authentication md5 key-chain LAB_DIGEST2
```

Implemented on L3 switch 1 and 2. This set of commands secure the HSRP link between L3 switch 1 and 2 by using md5 authentication, line after "key-chain" must match on both devices. Because service password encryption has been enabled, the keys in the key chain have been encrypted in the config file.

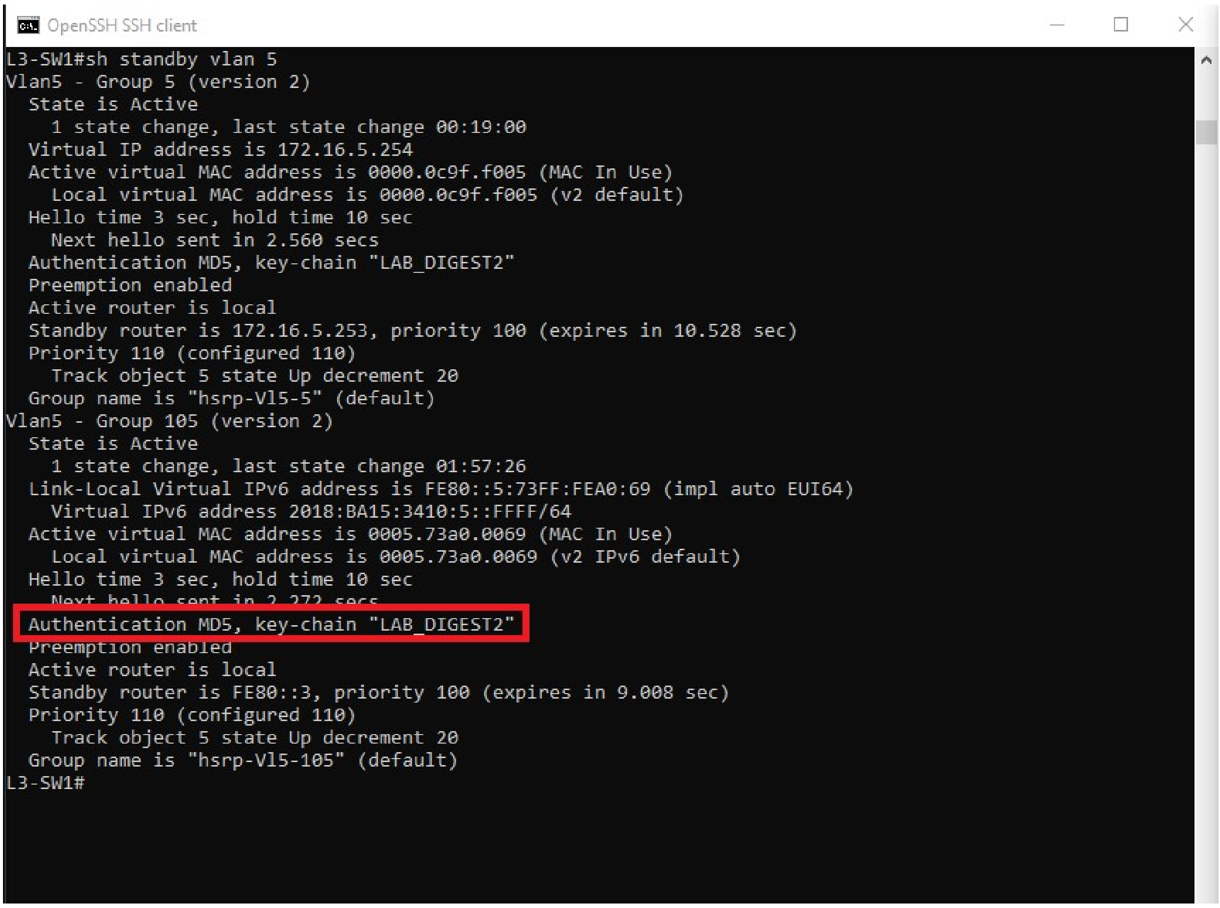


Figure 4-23 MD5 Authentication for HSRP