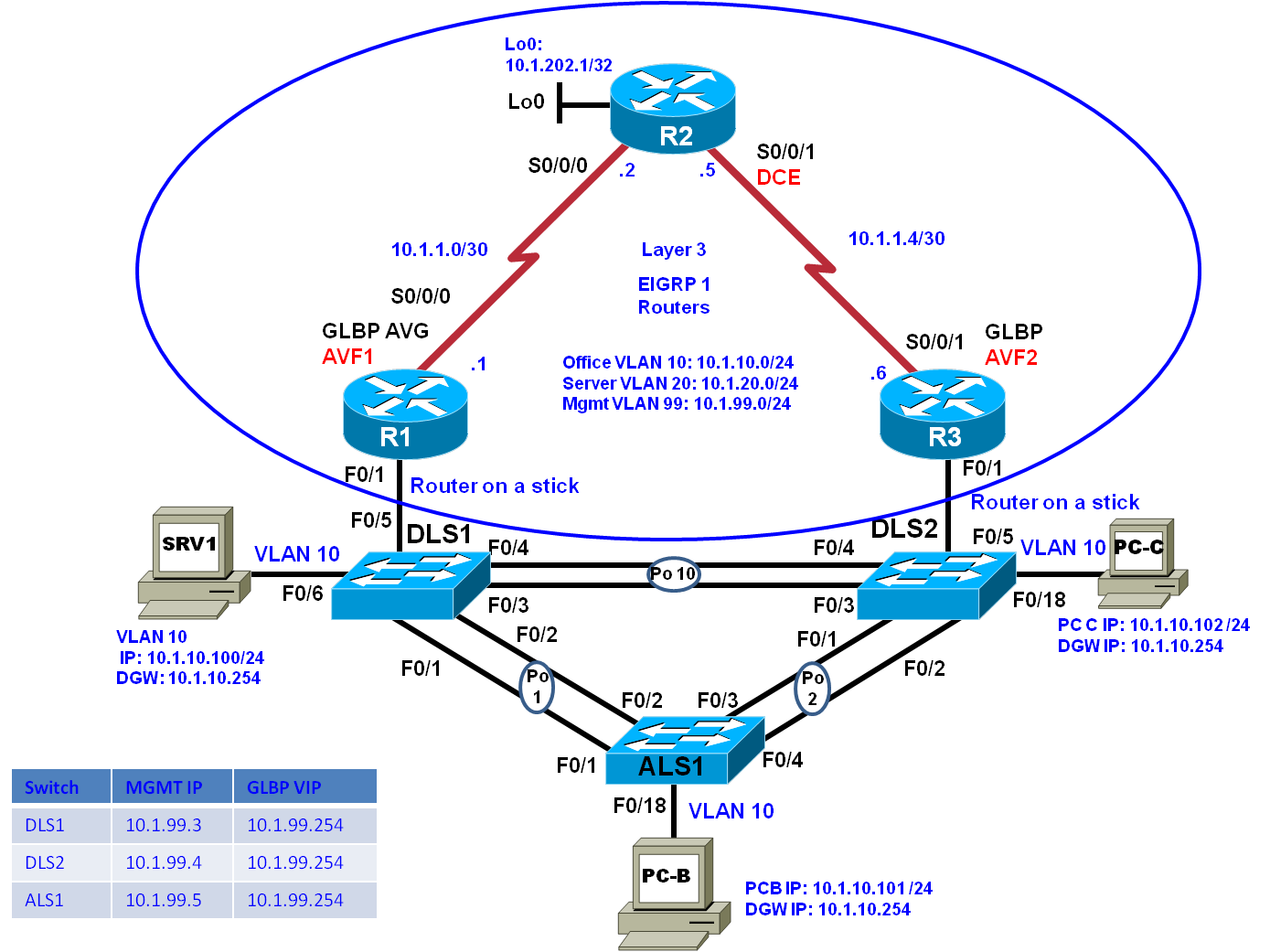
CCNPv7.1 SWITCH

Chapter 6 Lab 6-3, Gateway Load Balancing Protocol (GLBP)

Topology



Objectives

* Configure trunking, VTP, and inter-VLAN routing using router-on-a stick
* Configure GLBP
* Configure GLBP priorities
* Configure GLBP object tracking.

Background

Although HSRP and VRRP provide gateway resiliency for the standby members of the redundancy group, the upstream bandwidth is not used while the device is in standby mode. Only the active router for HSRP and the master for VRRP groups forward traffic for the virtual MAC. Resources associated with the standby router are not fully utilized. Some load balancing can be accomplished with these protocols through the creation of multiple groups and through the assignment of multiple default gateways, but this configuration creates an administrative burden. Previous labs provided you with experience configuring HSRP and VRRP to act as First Hop Redundancy Protocols. Gateway Load Balancing Protocol (GLBP) performs a similar function in redundancy, but offers the capability to load balance over multiple gateways.

GLBP is a Cisco-proprietary solution created to enable automatic selection and simultaneous use of multiple available gateways in addition to automatic failover between those gateways. Multiple routers share the load of frames that, from a client perspective, are sent to a single default gateway address.

Like HSRP and VRRP, an election occurs, but rather than a single active router winning the election, GLBP elects an Active Virtual Gateway (AVG). The AVG assigns virtual MAC addresses to each of the routers in the GLBP group (called Active Virtual Forwarders or AVFs). These virtual MAC addresses are then provided to hosts in an algorithmic manner in response to ARP requests from hosts for the default gateway.

GLBP allows for simultaneous forwarding from routers participating in a GLBP group. GLBP can support up to 4 routers in a group. GLBP also offers authentication and object tracking.

In this lab, you will set the network up by configuring trunking, VTP, VLANs, router-on-a-stick and EIGRP routing. Once the network is set up, you will configure and verify GLBP.

**Note:** This lab uses Cisco ISR G2 routers running Cisco IOS 15.4(3) images with IP Base and Security packages enabled, and Cisco Catalyst 3560 and 2960 switches running Cisco IOS 15.0(2) IP Services and LAN Base images, respectively. The 3560 switches are being used only as layer 2 devices in this lab topology. The switches have Fast Ethernet interfaces, so the routing metrics for all Ethernet links in the labs are calculated based on 100 Mb/s, although the routers have Gigabit Ethernet interfaces. The 3560 and 2960 switches are configured with the SDM templates “dual-ipv4-and-ipv6 routing” and “lanbase-routing”, respectively. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab. Catalyst 3650 switches (running any Cisco IOS XE release) and Catalyst 2960-Plus switches (running any release).

**Note(2)**: The 3 switches in this topology are only being used to support layer-2 functions, so 3 Cisco 2960 switches are acceptable for this lab. All Inter-VLAN routing will be facilitated by implementing a router-on-a-stick on R1 and R3.

**Note(3):** This lab's topology is based on the NETLAB Multi-Purpose Academy Pod (MAP). If your classroom is using the standard Cuatro Switch Pod, the PC names may be different than displayed here. Consult with your instructor.

Required Resources

* 2 Cisco 3560 with the Cisco IOS Release 15.0(2)SE6 C3560-ipservicesK9-M image or comparable
* 1 Cisco 2960 with the Cisco IOS Release 15.0(2)SE6 C2960-LANBASEK9-M image or comparable
* Three routers (This lab uses Cisco ISR G2 routers running Cisco IOS 15.4(3) images with IP Base and Security packages enabled, or comparable)
* Ethernet and console cables
* 3 PC’s with Windows OS
  1. Prepare the switches for the lab

Use the **reset.tcl** script you created in Lab 1 “Preparing the Switch” to set your switches up for this lab. Then load the file BASE.CFG into the running-config with the command **copy flash:BASE.CFG running-config**. An example from DLS1:

DLS1# **tclsh reset.tcl**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Reloading the switch in 1 minute, type reload cancel to halt

Proceed with reload? [confirm]

\*Mar 7 18:41:40.403: %SYS-7-NV\_BLOCK\_INIT: Initialized the geometry of nvram

\*Mar 7 18:41:41.141: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload command.

*<switch reloads - output omitted>*

Would you like to enter the initial configuration dialog? [yes/no]: **n**

Switch> **en**

\*Mar 1 00:01:30.915: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down

Switch# **copy BASE.CFG running-config**

Destination filename [running-config]?

184 bytes copied in 0.310 secs (594 bytes/sec)

DLS1#

* 1. Configure basic switch parameters.

On each switch, configure an IP address on the management VLAN according to the diagram. VLAN 1 is the default management VLAN, but following best practice, we will use a different VLAN. In this lab, VLAN 99 will be used as the management VLAN.

DLS1 example:

DLS1# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

DLS1(config)# **interface vlan 99**

DLS1(config-if)# **ip address 10.1.99.3 255.255.255.0**

DLS1(config-if)# **no shutdown**

The interface VLAN 99 will not come up immediately, because the Layer 2 instance of the VLAN does not yet exist. This issue will be remedied in subsequent steps.

(Optional) On each switch, create an enable secret password and configure the VTY lines to allow remote access from other network devices.

DLS1 example:

DLS1(config)# **enable secret class**

DLS1(config)# **line vty 0 15**

DLS1(config-line)# **password cisco**

DLS1(config-line)# **login**

**Note**: The passwords configured here are required for NETLAB compatibility only and are NOT recommended for use in a live environment.

|  |
| --- |
| **Note(2)**: For purely lab environment purposes, it is possible to configure the VTY lines so that they accept any Telnet connection immediately, without asking for a password, and place the user into the privileged EXEC mode directly. The configuration would be similar to the following example for DLS1:  DLS1(config)# **enable secret class**  DLS1(config)# **line vty 0 15**  DLS1(config-line)# **no login**  DLS1(config-line)# **privilege level 15** |

* 1. Configure trunks and EtherChannels between switches.

EtherChannel is used for the trunks because it allows you to utilize both Fast Ethernet interfaces that are available between each device, thereby doubling the bandwidth.

Configure trunks and EtherChannels from DLS1, DLS2, and ALS1 according to the diagram. Use LACP as the negotiation protocol for EtherChannel configurations. Remember that BASE.CFG has all interfaces shut down, so don't forget to issue the **no shutdown** command.

Refer to diagram for port channel numbers.

**Note**: The **switchport trunk encapsulation dot1q** command is required on Cisco 3560 switches. It is not required on Cisco 2960 switches.

DLS1(config)# **interface range fastEthernet 0/1-2**

DLS1(config-if-range)# **switchport trunk encapsulation dot1q**

DLS1(config-if-range)# **switchport mode trunk**

DLS1(config-if-range)# **channel-group 1 mode active**

DLS1(config-if-range)# **no shut**

Creating a port-channel interface Port-channel 1

Verify trunking and EtherChannel configurations between all switches with the appropriate trunking and EtherChannel verification commands. Refer back to Chapter 3 labs as necessary.

* 1. Configure VTP Client mode on DLS2 and ALS1.

A sample configuration is provided for you.

DLS2(config)# **vtp mode client**

Setting device to VTP client mode for VLANS

**Note**: Switches default to vtp mode server. However, remember the base configuration modifies this setting to vtp mode transparent.

* 1. Configure VTP and VLANs on DLS1.

Create the VTP domain on VTP server DLS1 and create VLANs 10, 20, and 99 for the domain.

NOTE: Switches default to **vtp mode server**. Recall that the base configuration modifies this setting to **vtp mode transparent**.

DLS1(config)# **vtp domain GLBP**

DLS1(config)# **vtp version 2**

DLS1(config)# **vtp mode server**

Setting device to VTP Server mode for VLANS

DLS1(config)# **vlan 99**

DLS1(config-vlan)# **name Management**

DLS1(config-vlan)# **vlan 10**

DLS1(config-vlan)# **name Office**

DLS1(config-vlan)# **vlan 20**

DLS1(config-vlan)# **name Server**

DLS1(config-vlan)# **exit**

Verify that VLANs propagated to the other switches in the network.

* 1. Configure switch access ports.

As the diagram illustrates, there are PCs connected to DLS1 fa0/6, DLS2 fa0/18, and ALS1 fa0/18. All PCs connected to the lab topology will statically access VLAN 10. Additionally, configure spanning-tree portfast on these switchports. The simplest way to do all of this is to use the **switchport host** macro. Also, don't forget to issue the **no shutdown** command.

DLS1(config)# **interface FastEthernet 0/6**

DLS1(config-if)# **switchport access vlan 10**

DLS1(config-if)# **switchport host**

switchport mode will be set to access

spanning-tree portfast will be enabled

channel group will be disabled

DLS1(config-if)# **no shutdown**

Repeat this configuration for interface fa0/18 on DLS2 and ALS1, and then verify the switchports on DLS1, DLS2 and ALS1 are members of VLAN 10.

* 1. Configure DLS1 and DLS2 trunking to the R1 and R3 router.

Configure DLS1 and DLS2 interface fa0/5 for trunking with the R1 and R3 router Gigabit Ethernet interface, according to the topology diagram. An example from DLS1:

DLS1(config)# **interface FastEthernet 0/5**

DLS1(config)# **switchport trunk encap dot1q**

DLS1(config)# **switchport mode trunk**

DLS1(config)# **no shutdown**

**Note**: The **switchport trunk encapsulation dot1q** command is required on Cisco 3560 switches. It is not required on Cisco 2960 switches.

* 1. Configure basic settings on R1, R2, and R3.

Configure basic settings on all three routers. An example for R1 follows:

Router> **enable**

Router# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# **hostname R1**

R1(config)# **enable secret class**

R1(config)# **line con 0**

R1(config-line)# **logging synchronous**

R1(config-line)# **line vty 0 4**

R1(config-line)# **password cisco**

R1(config-line)# **login**

R1(config-line)# **exit**

R1(config)#

**Note**: The passwords configured here are required for NETLAB compatibility only and are NOT recommended for use in a live environment.

In addition to the basic settings on R2, configure interface Loopback 0 with the IP address 10.1.202.1/32

R2(config)# **interface loopback 0**

R2(config-if)# **ip address 10.1.202.1 255.255.255.255**

R2(config-if)# **no shut**

R2(config-if)# **exit**

* 1. Configure the R1 and R3 Gigabit Ethernet interfaces for VLAN trunking.

Create a sub-interface for each VLAN. Enable each sub-interface with the proper trunking protocol, and configure it for a particular VLAN with the encapsulation command. Assign an IP address to each sub-interface from the table below. Hosts on the VLAN will use this address as their default gateway.

|  |  |  |
| --- | --- | --- |
| VLAN | R1 | R3 |
| 99 | 10.1.99.1/24 | 10.1.99.2/24 |
| 10 | 10.1.10.1/24 | 10.1.10.2/24 |
| 20 | 10.1.20.1/24 | 10.1.20.2/24 |

The following is a sample configuration for the Gigabit Ethernet 0/1 interface:

R1(config)# **interface GigabitEthernet0/1**

R1(config-if)# **no shut**

R1(config)# **interface GigabitEthernet0/1.10**

R1(config-subif)# **description Office VLAN 10**

R1(config-subif)# **encapsulation dot1q 10**

R1(config-subif)# **ip address 10.1.10.1 255.255.255.0**

R1(config)# **interface GigabitEthernet0/1.20**

R1(config-subif)# **description Server VLAN 20**

R1(config-subif)# **encapsulation dot1q 20**

R1(config-subif)# **ip address 10.1.20.1 255.255.255.0**

R1(config)# **interface GigabitEthernet0/1.99**

R1(config-subif)# **description Management VLAN 99**

R1(config-subif)# **encapsulation dot1q 99**

R1(config-subif)# **ip address 10.1.99.1 255.255.255.0**

Now, move to the R3 router to repeat similar configurations**.** In order for the R3 router to provide load balancing and redundancy VLAN 10, 20 and 99 networks, R3 must be configured to logically participate in the network.Create a sub-interface for each VLAN. Enable each sub-interface with the respective trunking protocol, and configure it for a particular VLAN with the encapsulation command. Assign an IP address to each sub-interface from the table above. Hosts on the VLAN can use this address as their default gateway.

Use the **show ip interface brief** command to verify the interface configuration and status.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 unassigned YES unset up up

GigabitEthernet0/1.10 10.1.10.1 YES manual up up

GigabitEthernet0/1.20 10.1.20.1 YES manual up up

GigabitEthernet0/1.99 10.1.99.1 YES manual up up

Serial0/0/0 unassigned YES unset administratively down down

Serial0/0/1 unassigned YES unset administratively down down

Serial0/1/0 unassigned YES unset administratively down down

Serial0/1/1 unassigned YES unset administratively down down

Use the show vlans command on the R1 and R3 router to verify inter-vlan routing configurations. The following is a sample output from router R1. Verify configurations on router R3.

R1# **show vlans**

Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interface: GigabitEthernet0/1

This is configured as native Vlan for the following interface(s) :

GigabitEthernet0/1 Native-vlan Tx-type: Untagged

Protocols Configured: Address: Received: Transmitted:

GigabitEthernet0/1 (1)

Other 0 19

17 packets, 5572 bytes input

19 packets, 1856 bytes output

Virtual LAN ID: 10 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interface: GigabitEthernet0/1.10

Protocols Configured: Address: Received: Transmitted:

GigabitEthernet0/1.10 (10)

IP 10.1.10.1 0 0

Other 0 2

0 packets, 0 bytes input

2 packets, 92 bytes output

Virtual LAN ID: 20 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interface: GigabitEthernet0/1.20

Protocols Configured: Address: Received: Transmitted:

GigabitEthernet0/1.20 (20)

IP 10.1.20.1 0 0

Other 0 1

0 packets, 0 bytes input

1 packets, 46 bytes output

Virtual LAN ID: 99 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interface: GigabitEthernet0/1.99

Protocols Configured: Address: Received: Transmitted:

GigabitEthernet0/1.99 (99)

IP 10.1.99.1 0 0

Other 0 1

0 packets, 0 bytes input

1 packets, 46 bytes output

* 1. Configure EIGRP routing in AS 1 for use with GLBP interface tracking.

Configure R1 serial interface s0/0/0 as shown in the topology diagram. Also configure EIGRP AS 1 for the 10.0.0.0 network. Below is an example of the configuration:

R1(config)# **int s0/0/0**

R1(config-if)# **ip add 10.1.1.1 255.255.255.252**

R1(config-if)# **no shut**

R1(config)# **router eigrp 1**

R1(config-router)# **network 10.0.0.0**

Configure R2 serial interface s0/0/0 and s0/0/1 and R3 serial interface s0/0/1 using the addresses shown in the topology diagram, and configure EIGRP AS 1 for the 10.0.0.0 network.

Verify EIGRP neighbor adjacencies using the **show ip eigrp neighbor** command.

R1# **sh ip eigrp neighbors**

EIGRP-IPv4 Neighbors for AS(1)

H Address Interface Hold Uptime SRTT RTO Q Seq

(sec) (ms) Cnt Num

3 10.1.99.2 Gi0/1.99 14 00:00:21 2 100 0 10

2 10.1.20.2 Gi0/1.20 10 00:00:21 1 100 0 11

1 10.1.10.2 Gi0/1.10 14 00:00:21 1 100 0 12

0 10.1.1.2 Se0/0/0 14 00:00:27 1 100 0 7

R2# **sh ip eigrp neighbor**

EIGRP-IPv4 Neighbors for AS(1)

H Address Interface Hold Uptime SRTT RTO Q Seq

(sec) (ms) Cnt Num

1 10.1.1.6 Se0/0/1 11 00:01:59 4 100 0 9

0 10.1.1.1 Se0/0/0 10 00:02:10 1 100 0 14

R3# **sh ip eigrp neighbor**

EIGRP-IPv4 Neighbors for AS(1)

H Address Interface Hold Uptime SRTT RTO Q Seq

(sec) (ms) Cnt Num

3 10.1.1.5 Se0/0/1 13 00:02:26 2 100 0 8

2 10.1.99.1 Gi0/1.99 11 00:02:29 1596 5000 0 17

1 10.1.20.1 Gi0/1.20 12 00:02:29 1596 5000 0 16

0 10.1.10.1 Gi0/1.10 13 00:02:29 1596 5000 0 15

Verify the routing table and ensure that R1 and R3 can ping the loopback 0 (10.1.202.0) network connected to router R2. This network will be used to test the application of HSRP tracked interfaces.

R1# **show ip route | begin Gateway**

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

D 10.1.1.4/30

[90/2172416] via 10.1.99.2, 00:04:15, GigabitEthernet0/1.99

[90/2172416] via 10.1.20.2, 00:04:15, GigabitEthernet0/1.20

[90/2172416] via 10.1.10.2, 00:04:15, GigabitEthernet0/1.10

C 10.1.10.0/24 is directly connected, GigabitEthernet0/1.10

L 10.1.10.1/32 is directly connected, GigabitEthernet0/1.10

C 10.1.20.0/24 is directly connected, GigabitEthernet0/1.20

L 10.1.20.1/32 is directly connected, GigabitEthernet0/1.20

C 10.1.99.0/24 is directly connected, GigabitEthernet0/1.99

L 10.1.99.1/32 is directly connected, GigabitEthernet0/1.99

D 10.1.202.1/32 [90/2297856] via 10.1.1.2, 00:04:15, Serial0/0/0

R3# **show ip route | begin Gateway**

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks

D 10.1.1.0/30

[90/2172416] via 10.1.99.1, 00:05:09, GigabitEthernet0/1.99

[90/2172416] via 10.1.20.1, 00:05:09, GigabitEthernet0/1.20

[90/2172416] via 10.1.10.1, 00:05:09, GigabitEthernet0/1.10

C 10.1.1.4/30 is directly connected, Serial0/0/1

L 10.1.1.6/32 is directly connected, Serial0/0/1

C 10.1.10.0/24 is directly connected, GigabitEthernet0/1.10

L 10.1.10.2/32 is directly connected, GigabitEthernet0/1.10

C 10.1.20.0/24 is directly connected, GigabitEthernet0/1.20

L 10.1.20.2/32 is directly connected, GigabitEthernet0/1.20

C 10.1.99.0/24 is directly connected, GigabitEthernet0/1.99

L 10.1.99.2/32 is directly connected, GigabitEthernet0/1.99

D 10.1.202.1/32 [90/2297856] via 10.1.1.5, 00:05:09, Serial0/0/1

From R1 and R3, ensure that you can ping the 10.1.202.1 destination address.

R1# **ping 10.1.202.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.202.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R3# **ping 10.1.202.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.202.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

* 1. Configure the routers for GLBP operation.

In this step you will configure a single GLBP group consisting of two members (R1 and R3). A GLBP group can have as many as four members. A single member will be elected as the AVG, and then routers will be designated as AVFs and their virtual MAC address will be distributed to hosts by the AVG in response to ARP requests.

AVG election is based on highest GLBP priority. In case of a tie, the highest assigned IP address is used. The **glbp <grp #> priority** interface configuration command can be used to modify the priority from the default of 100 in order to influence the election of the AVG. Should the AVG lose its role, the backup router with highest priority will assume the role. If you desire for the original AVG router to reassume its role once it comes back up, the **glbp <grp #> preempt** command must be configured.

The AVF is responsible for forwarding packets that are sent to the virtual MAC address assigned to that gateway by the AVG. Forward preemption is used with the AVFs and allows another AVF to assume responsibility for forwarding packets for an AVF that has lost its role or been disconnected. While AVG preemption must be manually configured, AVF preemption is enabled by default.

However, the AVFs use a weighting value rather than a priority value. Weighting thresholds are defined in conjunction with interface tracking. This functionality will be demonstrated later in the lab.

In this lab R1 will act as AVG and AVF1 and R3 will acts the AVF2. R1's GLBP priority will be modified to ensure its election as AVG.

The standby address for each VLAN will be the host address 254; VLAN 10 will use 10.1.10.254, VLAN 20 will use 10.1.20.254.

The following is a sample GLBP configuration on R1.

R1(config)# **interface GigabitEthernet0/1.10**

R1(config-subif)# **glbp 10 ip 10.1.10.254**

R1(config-subif)# **glbp 10 priority 150**

R1(config-subif)# **glbp 10 preempt**

R1(config-subif)# **exit**

R1(config)# **interface GigabitEthernet0/1.20**

R1(config-subif)# **glbp 20 ip 10.1.20.254**

R1(config-subif)# **glbp 20 priority 150**

R1(config-subif)# **glbp 20 preempt**

R1(config-subif)# **exit**

R1(config)# **interface GigabitEthernet0/1.99**

R1(config-subif)# **glbp 99 ip 10.1.99.254**

R1(config-subif)# **glbp 99 priority 150**

R1(config-subif)# **glbp 99 preempt**

Except for the priority command, the same commands are used on the sub-interfaces on R3.

As a result of our configuration, we should see R1 router with the AVG role. Issue the **show glbp** command for GLBP configuration analysis. Before examining the output, it might be useful to take note of the MAC address of R1 and R3’s G0/1 interfaces.

R1# **sho int g0/1 | i bia**

Hardware is CN Gigabit Ethernet, address is **acf2.c523.7a09** (bia acf2.c523.7a09)

R1#

R3# **show int g0/1 | i bia**

Hardware is CN Gigabit Ethernet, address is **acf2.c518.0651** (bia acf2.c518.0651)

R3#

R1# **show glbp**

GigabitEthernet0/1.10 - Group 10

State is Active

1 state change, last state change 00:01:28

Virtual IP address is 10.1.10.254

Hello time 3 sec, hold time 10 sec

Next hello sent in 2.272 secs

Redirect time 600 sec, forwarder timeout 14400 sec

Preemption enabled, min delay 0 sec

Active is local

Standby is 10.1.10.2, priority 100 (expires in 7.840 sec)

Priority 150 (configured)

Weighting 100 (default 100), thresholds: lower 1, upper 100

Load balancing: round-robin

Group members:

acf2.c518.0651 (10.1.10.2)

acf2.c523.7a09 (10.1.10.1) local

There are 2 forwarders (1 active)

Forwarder 1

State is Active

1 state change, last state change 00:00:46

MAC address is 0007.b400.0a01 (default)

Owner ID is acf2.c523.7a09

Redirection enabled

Preemption enabled, min delay 30 sec

Active is local, weighting 100

Forwarder 2

State is Listen

MAC address is 0007.b400.0a02 (learnt)

Owner ID is acf2.c518.0651

Redirection enabled, 597.856 sec remaining (maximum 600 sec)

Time to live: 14397.856 sec (maximum 14400 sec)

Preemption enabled, min delay 30 sec

Active is 10.1.10.2 (primary), weighting 100 (expires in 8.384 sec)

<output omitted>

The **show glbp brief** command can also be used to view a brief synopsis of GLBP operation.

R1# **show glbp brief**

Interface Grp Fwd Pri State Address Active router Standby router

Line 1 ->

Line 2 ->

Line 3 ->

Gi0/1.10 10 - 150 Active 10.1.10.254 local 10.1.10.2

Gi0/1.10 10 1 - Active 0007.b400.0a01 local -

Gi0/1.10 10 2 - Listen 0007.b400.0a02 10.1.10.2 -

Gi0/1.20 20 - 150 Active 10.1.20.254 local 10.1.20.2

Gi0/1.20 20 1 - Active 0007.b400.1401 local -

Gi0/1.20 20 2 - Listen 0007.b400.1402 10.1.20.2 -

Gi0/1.99 99 - 150 Active 10.1.99.254 local 10.1.99.2

Gi0/1.99 99 1 - Active 0007.b400.6301 local -

Gi0/1.99 99 2 - Listen 0007.b400.6302 10.1.99.2 -

The first line in the GLBP output shows the role of the AVG for group 10. The priority has been set to 150 for this group and the state shows R1 as the active AVG. The virtual IP address is 10.1.10.254. The standby AVG is 10.1.10.2 which is the R3 router.

Notice the next two lines also pertain to GLBP group 10. These lines detail information about the AVF. There are two forwarders in this group. The virtual MAC addresses are **0007.b400.0a01** and **0007.b400.0a02**.

The last hextet is **0a01**. The first two hex characters, **0a** equal 10 in decimal, which corresponds to the group number. The last two digits (**01**) correspond to one of the four MAC addresses (01-04) that can be used in GLBP operation.

The second line in the GLBP output displays information about the AVF. Line 2 shows that R1 is forwarding packets for the MAC address ending in 01. Line 3 of the output shows that R1 is listening or in standby AVF mode for the MAC address ending in 02.

Continue the analysis on the remaining lines of output for GLBP.

Which router is the active forwarder MAC Address 0007.b400.6302 for GLBP group 99?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What MAC address is the active forwarder for GLBP group 99 listening? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Verify PCs can reach R2 L0 using the GLBP gateway

Configure the PCs with the IP Addresses shown in the topology diagram. The PCs used in this lab scenario were given access earlier to VLAN 10. The gateway address is set to the GLBP virtual address 10.1.10.254.

This is the IPCONFIG output from SRV1 connected to DLS1 F0/6.

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::a940:91fe:38dd:da0c%10

IPv4 Address. . . . . . . . . . . : 10.1.10.100

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 10.1.10.254

This is the IPCONFIG output from PC-B connected to ALS1 F0/18.

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::ee:d834:9d99:45e8%11

IPv4 Address. . . . . . . . . . . : 10.1.10.101

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 10.1.10.254

This is the IPCONFIG output from PC-C connected to DLS2 F0/18.

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::a4d3:c82d:93c4:f2e6%11

IPv4 Address. . . . . . . . . . . : 10.1.10.102

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 10.1.10.254

Verify that SRV1, PC-B, and PC-C can ping their default gateway. Upon successful ping of the gateway, view the **arp** cache on each PC using the **arp –a**.

Output from SRV1

C:\Users\student>ping -n 3 10.1.10.254

Pinging 10.1.10.254 with 32 bytes of data:

Reply from 10.1.10.254: bytes=32 time=1ms TTL=255

Reply from 10.1.10.254: bytes=32 time=1ms TTL=255

Reply from 10.1.10.254: bytes=32 time=1ms TTL=255

Ping statistics for 10.1.10.254:

Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\student>arp -a

Interface: 10.1.10.100 --- 0xa

Internet Address Physical Address Type

10.1.10.101 00-0c-29-80-cb-b6 dynamic

10.1.10.102 00-0c-29-6a-07-e6 dynamic

10.1.10.254 00-07-b4-00-0a-02 dynamic

10.1.10.255 ff-ff-ff-ff-ff-ff static

169.254.69.232 00-0c-29-80-cb-b6 dynamic

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

The output of the arp cache reveals the 10.1.10.254 associated with GLBP virtual MAC address 00-07-b4-00-0a-02. The first address to be issued to the first client request was the 00-07-b4-00-0a-02 MAC address.

**NOTE: The MAC addresses and other output you receive will vary. The important thing to note is that each router is listening for one MAC address either ending in 01 or 02 and that the AVG alternated these MAC addresses in the ARP replies as part of the *default* round robin algorithm.**

Now, move to PC-B and ping the default gateway address 10.1.10.254. View the **arp** cache using the **arp –a** command.

What MAC Address has been issued to the PC-B client?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

OUTPUT from PC-B

C:\Users\student>ping -n 3 10.1.10.254

Pinging 10.1.10.254 with 32 bytes of data:

Reply from 10.1.10.254: bytes=32 time=2ms TTL=255

Reply from 10.1.10.254: bytes=32 time=1ms TTL=255

Reply from 10.1.10.254: bytes=32 time=1ms TTL=255

Ping statistics for 10.1.10.254:

Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\student>arp -a

Interface: 10.1.10.101 --- 0xb

Internet Address Physical Address Type

10.1.10.100 00-0c-29-15-ab-9d dynamic

10.1.10.102 00-0c-29-6a-07-e6 dynamic

10.1.10.254 00-07-b4-00-0a-01 dynamic

10.1.10.255 ff-ff-ff-ff-ff-ff static

11.0.0.5 00-0c-29-6a-07-e6 dynamic

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

Repeat these steps PC-C.

What virtual MAC address is being used by PC-C? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Move to R1 router and issue the **show glbp brief** command. Notice how the MAC addresses correlate to the MAC address issued to the VLAN 10 clients.

R1>sh glbp brief

Interface Grp Fwd Pri State Address Active router Standby router

Gi0/1.10 10 - 150 Active 10.1.10.254 local 10.1.10.2

Gi0/1.10 10 1 - Active 0007.b400.0a01 local -

Gi0/1.10 10 2 - Listen 0007.b400.0a02 10.1.10.2 -

Gi0/1.20 20 - 150 Active 10.1.20.254 local 10.1.20.2

Gi0/1.20 20 1 - Active 0007.b400.1401 local -

Gi0/1.20 20 2 - Listen 0007.b400.1402 10.1.20.2 -

Gi0/1.99 99 - 150 Active 10.1.99.254 local 10.1.99.2

Gi0/1.99 99 1 - Active 0007.b400.6301 local -

Gi0/1.99 99 2 - Listen 0007.b400.6302 10.1.99.2 -

R1>

The highlighted line above in the **show glbp brief** output shows that R1 is the active forwarder for the MAC address 0007.b400.0a01 and the standby for the MAC address 0007.b400.0a02.

Move to the R3 router and issue the **show glbp brief** command. Notice how the MAC addresses correlate to the MAC address issued to the VLAN 10 clients.

R3>show glbp brief

Interface Grp Fwd Pri State Address Active router Standby router

Gi0/1.10 10 - 100 Standby 10.1.10.254 10.1.10.1 local

Gi0/1.10 10 1 - Listen 0007.b400.0a01 10.1.10.1 -

Gi0/1.10 10 2 - Active 0007.b400.0a02 local -

Gi0/1.20 20 - 100 Standby 10.1.20.254 10.1.20.1 local

Gi0/1.20 20 1 - Listen 0007.b400.1401 10.1.20.1 -

Gi0/1.20 20 2 - Active 0007.b400.1402 local -

Gi0/1.99 99 - 100 Standby 10.1.99.254 10.1.99.1 local

Gi0/1.99 99 1 - Listen 0007.b400.6301 10.1.99.1 -

Gi0/1.99 99 2 - Active 0007.b400.6302 local -

R3>

The highlighted line above in the **show glbp brief** output shows that R3 is the active forwarder for the MAC address 0007.b400.0a02 and the standby for the MAC address 0007.b400.0a01. With PC-C being issued the MAC address 0007.b400.0a02, this demonstrates GLBPs ability to offer simultaneous forwarding and load balancing from the R1 and R3 routing devices participating in GLBP.

The GLBP behavior demonstrated is based on the GLBP default load-balancing algorithm of round-robin. As clients send ARP requests to resolve the MAC address of the default gateway, the AVG reply to each client contain the MAC address of the next possible router in a round-robin fashion.

Load balancing options with GLBP are weighted, host dependent and round robin (default). The load balancing algorithm can be changed using the interface configuration command **glbp***group* **load-balancing**[**host-dependent**| **round-robin**| **weighted**]

* 1. Configure GLBP interface tracking.

If R1’s interface s0/0/0 goes down, clients using R1 as an AVF will not be able to reach the destinations located off of the R2 router. Similarly, if R3’s serial interface s0/0/1 goes down, clients using R3 as an AVF will not be able to reach the destinations located off of the R2 router.

GLBP interface tracking uses a weighting mechanism which is different than HSRP or VRRP. With GLBP, two thresholds are defined: one lower threshold that applies when the router loses weight and one upper threshold that applies when the router regains weight. The weighting mechanism offers more flexibility with upper and lower thresholds defined over its counterparts HSRP and VRRP which only allow a single threshold to be defined. If the router priority (or weight) falls below the threshold, the router loses its active state. As soon as the router weight (or priority) exceeds the upper threshold, the router regains its active state.

Because R1's s0/0/0 interface and R3's s0/0/1 interface affect GLBP forwarding operations, we will need to configure tracking on these interfaces. Tracking with GLBP uses objects. The first step is to track the line protocol status of R1’s serial interface s0/0/0. On R1, issue the following command:

R1(config)# **track 15 interface s0/0/0 line-protocol**

On R1, enter in sub-interface configuration mode for VLAN 10 and configure the weighting mechanism and associate it with the track object number 15.

Consider the example configuration below.

In the first command, R1's g0/1.10 is configured with a **glbp weight** of 110 and lower threshold of 85 and an upper threshold of 105. When the weight falls below the specified lower threshold, the R1 AFV is forced to relinquish its role for the ACTIVE MAC address assigned to it.

In the second command, GLBP weighting is associated with the line protocol status of s0/0/0. If the line protocol state changes, the weight configured for 110 will be decreased by 30 resulting in a weight of 80. R1 would then lose its AVF role until the weight exceeds the upper defined threshold of 105.

R1(config)# **interface gi0/1.10**

R1(config-subif)# **glbp 10 weighting 110 lower 85 upper 105**

R1(config-subif)# **glbp 10 weighting track 15 decrement 30**

For testing purposes, on a PC that is using R1 as an AVF, start a continuous ping to the destination address 10.1.202.1. This will be useful to demonstrate the automatic failover of one AVF to the other when the tracked object decrements the GLBP weight.

In this lab scenario, SRV1 uses R1 as its default gateway.

Output from SRV1

ping 10.1.202.1 -t

On R1, shut down the interface s0/0/0.

R1(config)# **int s0/0/0**

R1(config-if)# **shutdown**

Notice the console messages listed below.

\*Jul 29 12:53:45.263: %TRACK-6-STATE: 15 interface Se0/0/0 line-protocol Up -> Down

\*Jul 29 12:53:45.263: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.2 (Serial0/0/0) is down: interface down

\*Jul 29 12:53:47.263: %LINK-5-CHANGED: Interface Serial0/0/0, changed state to administratively down

\*Jul 29 12:53:48.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

\*Jul 29 12:54:19.835: %GLBP-6-FWDSTATECHANGE: GigabitEthernet0/1.10 Grp 10 Fwd 1 state Active -> Listen

We see state change of the tracked interface and then the GLBP state of AFV 2 go from an active state to listen.

After the GLBP state change occurs, notice the ping output from the PC. The ping should continue without fail. GLBP failed over automatically to the R3 device and the client experienced no disruption in service.

View the output of the **show glbp** command. Output has been omitted here to only show the output for group 10 since this was the only group in which we applied interface tracking.

R1# **show glbp**

GigabitEthernet0/1.10 - Group 10

State is Active

1 state change, last state change 18:04:27

Virtual IP address is 10.1.10.254

Hello time 3 sec, hold time 10 sec

Next hello sent in 0.288 secs

Redirect time 600 sec, forwarder timeout 14400 sec

Preemption enabled, min delay 0 sec

Active is local

Standby is 10.1.10.2, priority 100 (expires in 9.376 sec)

Priority 150 (configured)

Weighting 80, low (configured 110), thresholds: lower 85, upper 105

Track object 15 state Down decrement 30

Load balancing: round-robin

Group members:

acf2.c518.0651 (10.1.10.2)

acf2.c523.7a09 (10.1.10.1) local

There are 2 forwarders (0 active)

Forwarder 1

State is Listen

2 state changes, last state change 00:05:52

MAC address is 0007.b400.0a01 (default)

Owner ID is acf2.c523.7a09

Redirection enabled

Preemption enabled, min delay 30 sec

Active is 10.1.10.2 (secondary), weighting 100 (expires in 10.592 sec)

Client selection count: 13

Forwarder 2

State is Listen

MAC address is 0007.b400.0a02 (learnt)

Owner ID is acf2.c518.0651

Redirection enabled, 599.392 sec remaining (maximum 600 sec)

Time to live: 14399.392 sec (maximum 14400 sec)

Preemption enabled, min delay 30 sec

Active is 10.1.10.2 (primary), weighting 100 (expires in 10.368 sec)

Client selection count: 13

<output omitted>

The first part of the GLBP output deals with R1’s role as an AVG. The AVG role has not been affected by the configuration we applied above. The highlighted portion shows the impact of the interface tracking and weighting mechanism configurations. The weighting mechanism only affects the forwarder role in GLBP. Notice that R1 is no longer the forwarder for the MAC address 0007.b400.0a01. R1 shows the forwarder roles for both MAC addresses in the listen state.

It is important to note that similar configurations should be applied on R1 for GLBP groups 20 and 99 for consistency of operations. R3 would need to be configured to track the serial interface s0/0/1 and have the weighting mechanism applied as appropriate. To limit the length and time required to perform this lab, these steps have been omitted.

Activate R1 serial interface s0/0/0 using the no shutdown command.

On R1, shutdown the interface s0/0/0.

R1(config)# **int s0/0/0**

R1(config-if)# **no shut**

Use the **show glbp** command to ensure R1 resumed its AVF role.

* 1. Configure GLBP authentication.

GLBP authentication is important to ensure that no rogue device is allowed join your GLBP group and adversely affect GLBP operations by initiating attacks such as Man-in-the-Middle, etc. GLBP supports two options for authentication: plain text authentication and MD5 authentication. MD5 authentication offers greater security. Using MD5 authentication, a coordinated secret key is used to generate a keyed MD5 hash, which is then included in GLBP packets sent back and forth. A keyed hash of an incoming packet is generated and if the hash within the incoming packet does not match the generated hash the packet is ignored.

Configure the R1 and R3 routers sub-interfaces to support MD5 authentication using the following command: **glbp <0-1023> Group Number authentication MD5 key-string cisco123**

R1(config)# **interface GigabitEthernet0/1.10**

R1(config-subif)# **glbp 10 authentication md5 key-string cisco123**

R1(config)# **interface GigabitEthernet0/1.20**

R1(config-subif)# **glbp 20 authentication md5 key-string cisco123**

R1(config)# **interface GigabitEthernet0/1.99**

R1(config-subif)# **glbp 99 authentication md5 key-string cisco123**

NOTE: The cisco123 is used as the shared key password in this lab scenario.

When you added the commands for GLBP authentication to the R1 router, a GLBP state change occurred because only one router was configured with authentication. Now move to R3 router and add glbp authentication to each sub-interface **using the same command with the respective glbp group number and the same key-string shown above.**

Verify the GLBP operation. Ensure that the R1 is still the AVG and both routers are participating as AVFs for each configured GLBP group. If there is a problem, check the GLBP authentication configuration for errors.

Step 13: End of Lab

Do not save your configurations. The equipment will be reset for the next lab.