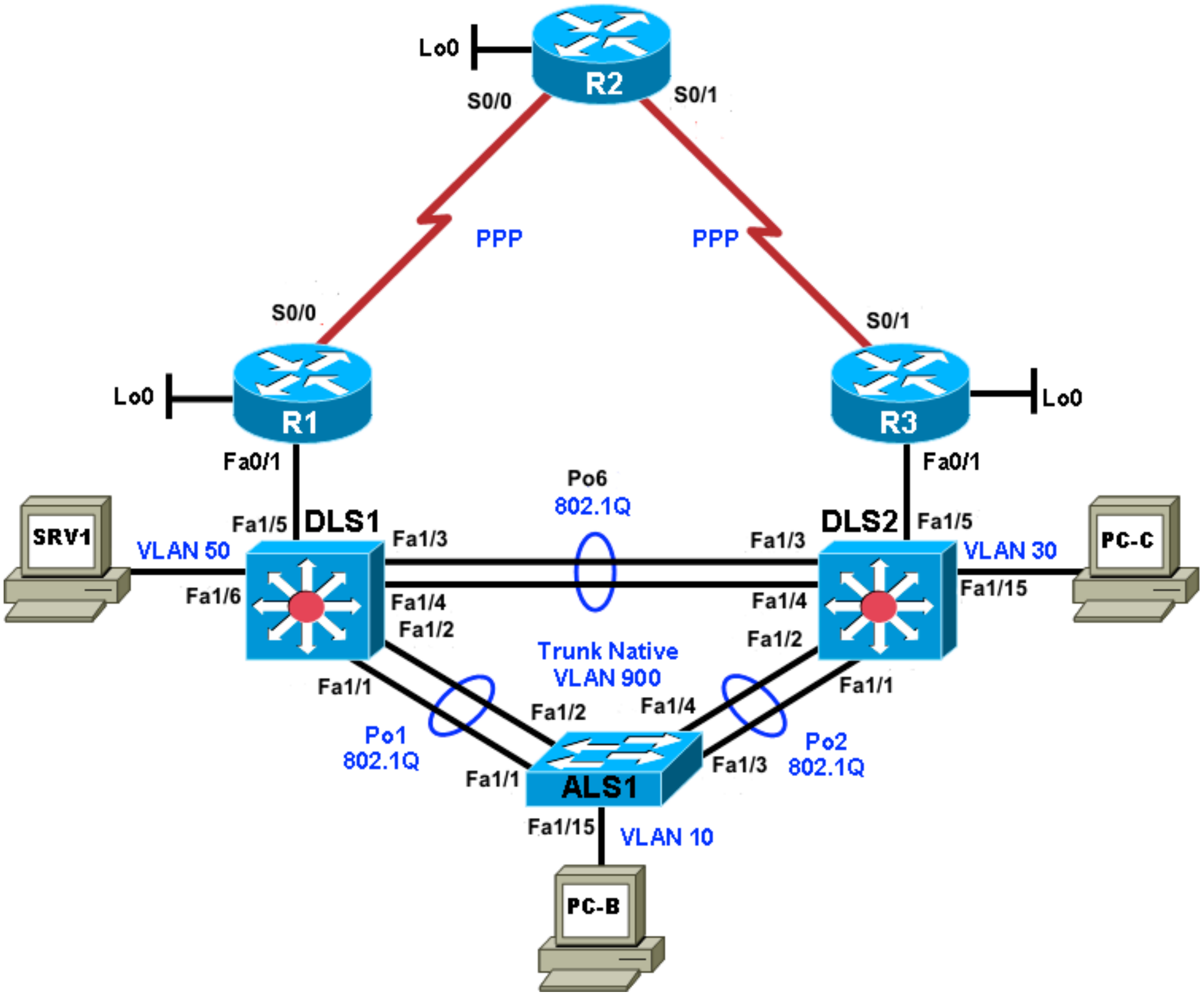
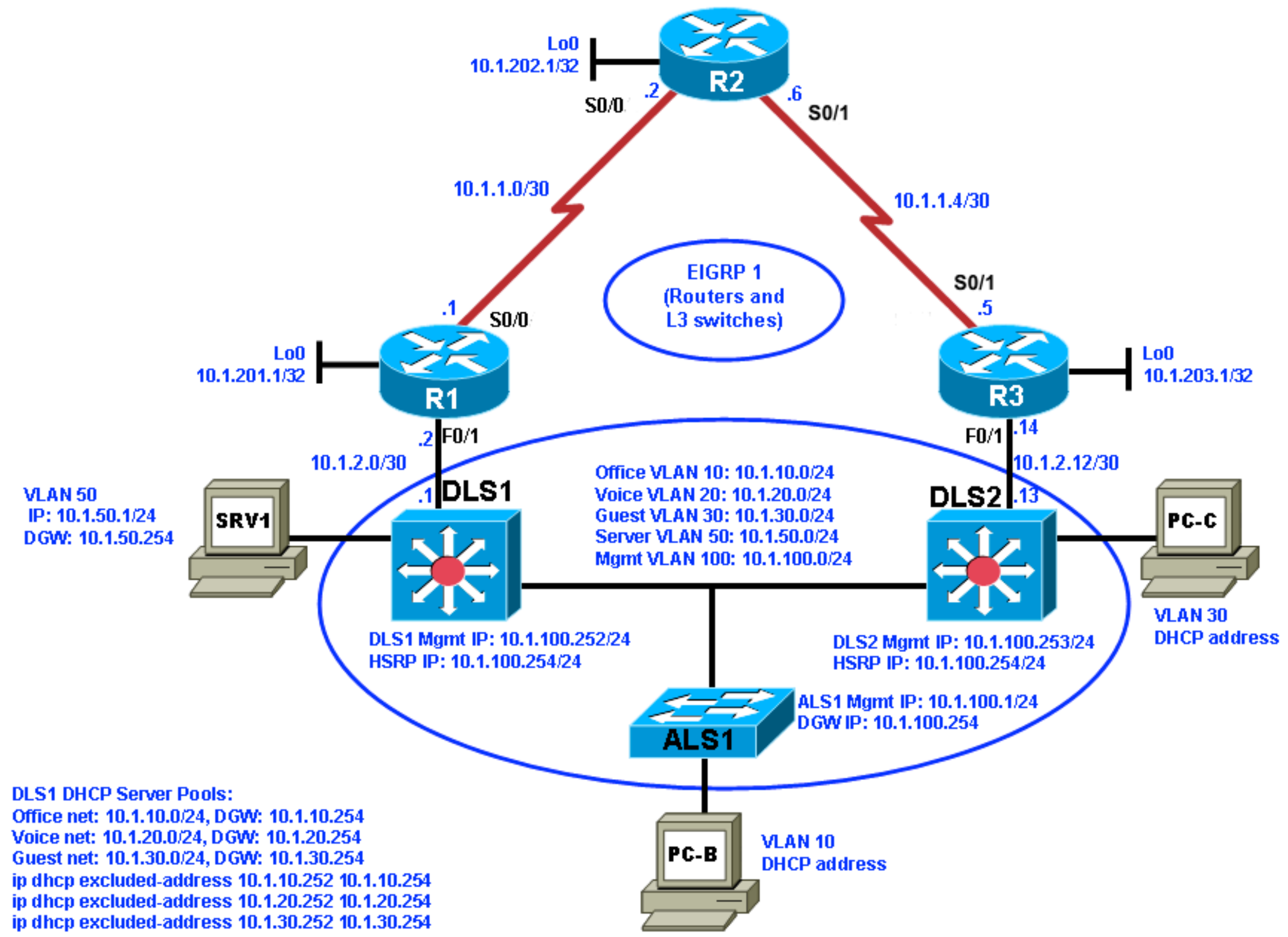
Lab 4-2, Layer 3 Switching and First-Hop Redundancy

Physical Topology



Logical Topology


Lo0
10.1.202.1/32
R2
S0/0
.2
.6
S0/1
10.1.1.0/30
10.1.1.4/30
EIGRP 1
(Routers and
L3 switches)
.1
S0/0
S0/1
.5
Lo0
10.1.201.1/32
R1
R3
Lo0
10.1.203.1/32
.2
F0/1
F0/1
.14
10.1.2.0/30
10.1.2.12/30
.1
DLS1
DLS2
.13
Office VLAN 10: 10.1.10.0/24
Voice VLAN 20: 10.1.20.0/24
Guest VLAN 30: 10.1.30.0/24
Server VLAN 50: 10.1.50.0/24
Mgmt VLAN 100: 10.1.100.0/24
VLAN 50
IP: 10.1.50.1/24
DGW: 10.1.50.254
SRV1
PC-C
VLAN 30
DHCP address
DLS1 Mgmt IP: 10.1.100.252/24
HSRP IP: 10.1.100.254/24
DLS2 Mgmt IP: 10.1.100.253/24
HSRP IP: 10.1.100.254/24
ALS1
ALS1 Mgmt IP: 10.1.100.1/24
DGW IP: 10.1.100.254
PC-B
VLAN 10
DHCP address
DLS1 DHCP Server Pools:
Office net: 10.1.10.0/24, DGW: 10.1.10.254
Voice net: 10.1.20.0/24, DGW: 10.1.20.254
Guest net: 10.1.30.0/24, DGW: 10.1.30.254
ip dhcp excluded-address 10.1.10.252 10.1.10.254
ip dhcp excluded-address 10.1.20.252 10.1.20.254
ip dhcp excluded-address 10.1.30.252 10.1.30.254

Objectives

- Load the trouble ticket device configuration files for each trouble ticket.
- Diagnose and resolve problems related to switch virtual interfaces and multilayer switching.
- Diagnose and resolve problems related to First Hop Redundancy Protocols.
- Document troubleshooting progress, configuration changes, and problem resolution.

Background

Multilayer (Layer 3) switches have the capability to act as switches and routers when using switch virtual interfaces (SVIs), routed interfaces, and routing protocols. Layer 3 switches allow you to create SVIs or logical interfaces that represent a VLAN. They can also support routed physical interfaces. These versatile switches are frequently used as part of the LAN switch fabric and can be configured with a First Hop Redundancy Protocol (FHRP). Two or more Layer 3 switches (or routers) can provide redundant paths to the network edge for local hosts. A host is configured with a virtual default gateway address. If one of the gateways goes down, the other can take over for the client without the client's knowledge. Examples of FHRPs discussed in this course are Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP).

In this lab, you will troubleshoot problems related to Layer 3 switching and FHRPs, such as HSRP, including HSRP authentication. For each task or trouble ticket, the scenario and problem symptom is described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 42-A (1 Issue)

Step 1: Review trouble ticket Lab 42-A.

Upon arriving at the office this morning, you find the following ticket in the system:

Switch ALS1 has been showing CRC errors on a group of eight ports for several days. It was suspected that hardware was the cause. During yesterday evening's maintenance window, the switch was replaced with a similar switch from the lab. After this replacement, clients could connect, and no errors were shown on the ports. However, making a backup of the ALS1 configuration to server SRV1 did not work, and no syslog messages from ALS1 are being received by SRV1. The switch is not reachable via Telnet or SSH from server SRV1. There was no time for further research yesterday so, because there is no impact to users, it was decided to leave the switch and pick up this issue the next day.

Your task is to diagnose the issue and restore connectivity between switch ALS1 and server SRV1. After resolving the problem, make a backup of the configuration to server SRV1.

Step 2: Load the device trouble ticket configuration files for 42-A.

a. On each device issue the command **42-A**

b. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-42A**

c. Shut down GNS3, restart this new project. Restart all the devices..

Step 3: Clear mac address table on DSL1 and DSL2

a. `DLS1#`**`clear mac`**

b. `DLS2#`**`clear mac`**

Step 4: Check DHCP addresses on PC-B and PC-C.

Ensure that PC-B and PC-C are configured as DHCP clients and have the expected IP addresses.

Note: Problems introduced into the network by the trouble ticket might prevent one or both of these PCs from acquiring an IP address. Do not assign either PC a static address.

Step 5: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods and processes, and procedure and communication improvements.

____

____

____

Task 2: Trouble Ticket Lab 42-B (2 Issues)

Step 1: Review trouble ticket Lab 42-B.

During last Friday’s maintenance window, a series of failover tests at headquarters and the branch offices were executed. It was discovered during a reboot of switch DLS1 that connectivity between clients in OFFICE VLAN 10 and the Internet was lost. After router DLS1 came back online, the clients regained connectivity. This was not the expected behavior, because the network provides gateway first-hop redundancy for clients in the OFFICE VLAN to ensure correct failover during outages.

If one of the HSRP switches fails, the hosts on the OFFICE VLAN should still be able to access the Internet (by pinging R2 Lo0 10.1.202.1 during the outage).

Step 2: Load the device trouble ticket configuration files for 42-B.

a. On each device issue the command **42-B**

b. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-42B**

c. Shut down GNS3, restart this new project. Restart all the devices.

.

Step 3: Clear mac address table on DSL1 and DSL2

a. `DLS1#clear mac`

b. `DLS2#clear mac`

Step 4: Check DHCP addresses on PC-B and PC-C.

Ensure that PC-B and PC-C are configured as DHCP clients and have the expected IP addresses.

Note: Problems introduced into the network by the trouble ticket might prevent one or both of these PCs from acquiring an IP address. Do not assign either PC a static address.

Step 5: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

____

____

____

____

____

____

____

Section 2—Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course:

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Commands Summary

The table lists useful commands. The sample output is shown on the following pages.

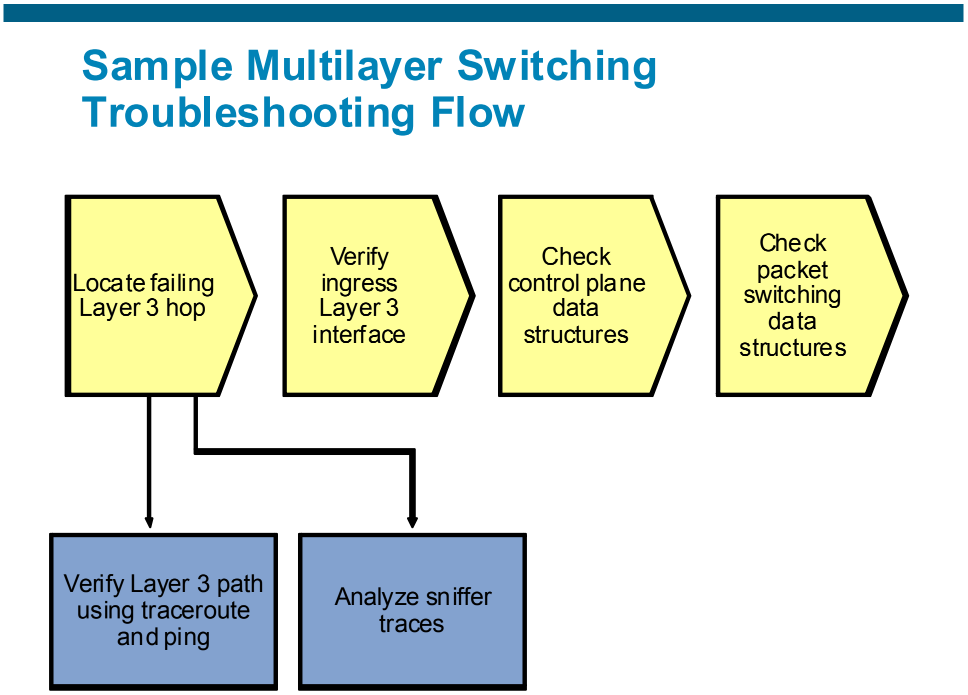
Command	Key Information Displayed
show spanning-tree vlan *vlan#*	Displays all essential parameters that affect the topology, such as the root port, designated ports, port state, and port type, as well as the spanning-tree mode being implemented.
show vlan brief	Displays a quick overview of all existing VLANs and the ports within them. Trunk ports are not listed.
show vlan id *vlan#*	Displays whether the VLAN exists and which ports are assigned to it. Includes the trunk ports on which the VLAN is allowed.
show interfaces vlan *vlan#*	Displays the SVI status, IP address, and statistics.
show ip route *ip-addr*	Displays the routing table information for a particular destination address.
show ip arp *ip-addr*	Displays the ARP table information for an IP address, including age, hardware address, and interface.
show interfaces *type/#* | **include bia**	Displays the MAC address of an interface on one output line.
show ip cef *ip-addr* **detail**	Displays the next hop and interface used for a particular destination address from the Cisco Express Forwarding table.
show adjacency *int-type/#* **detail**	Displays the information contained in the adjacency table for a next-hop IP address or interface.
show platform forward	Displays the hardware ternary content addressable memory (TCAM) information and exact forwarding behavior for a Layer 2 or Layer 3 switched frame.

	Note: Specific to the Catalyst 3560 and 3750 series of switches.
show standby vlan *vlan#* **brief**	Verify active and standby roles and IP addresses for a particular VLAN for HSRP routers.
debug standby packets	Displays real-time messages exchanged between HSRP routers.

Lab 4-2 Sample Troubleshooting Flows

Troubleshooting Multilayer Switching

The figure illustrates an example of a method that you could follow to diagnose and resolve problems related to multilayer switching.



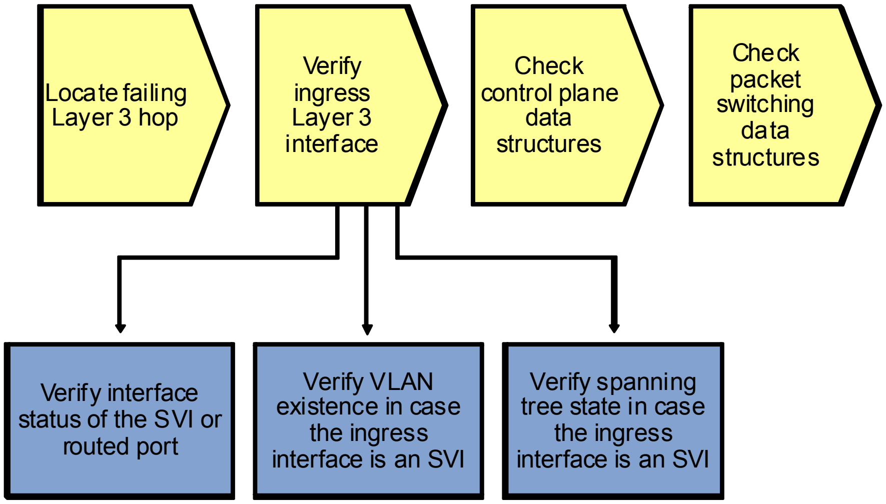
Sample Multilayer Switching Troubleshooting Flow

Locate failing Layer 3 hop
Verify ingress Layer 3 interface
Check control plane data structures
Check packet switching data structures
Verify Layer 3 path using traceroute and ping
Analyze sniffer traces

What is multilayer switching? In essence, a multilayer switch is a switch that is capable of switching Ethernet frames based on information in the Layer 2 and Layer 3 headers. Troubleshooting Layer 2 switching was covered in the previous lab exercise. This troubleshooting flow focuses on troubleshooting the process of switching Ethernet frames based on Layer 3 information.

Under which kind of circumstances do you start troubleshooting the multilayer switching process? Troubleshooting multilayer switching is just one of the steps in the bigger picture of troubleshooting network connectivity along a Layer 3 path. After you have determined—by using tools like traceroute or ping or through analysis of packet captures—that a particular hop in the Layer 3 path seems to be the point where packets start to get dropped and that hop is a multilayer switch, or when you are troubleshooting performance problems and you want to find the exact physical links on which packets travel, then start tracing and verifying the Layer 3 forwarding behavior of the multilayer switch that you suspect to be the cause of the problem.

Sample Multilayer Switching Troubleshooting Flow



Locate failing Layer 3 hop

Verify ingress Layer 3 interface

Check control plane data structures

Check packet switching data structures

Verify interface status of the SVI or routed port

Verify VLAN existence in case the ingress interface is an SVI

Verify spanning tree state in case the ingress interface is an SVI

Layer 3 packet switching generally consists of three major steps:

1. Receive the packet on a Layer 3 interface. This interface can either be a routed port or an SVI.
2. Perform a lookup in the hardware packet-switching data structures. Multilayer switches store packet-forwarding information in special TCAM data structures. The information contained in these data structures is compiled from the Cisco Express Forwarding data structures in the main memory of the route processor. These data structures are, in turn, derived from control plane tables, such as the routing table and the ARP cache.
3. Rewrite the frame and switch it to the outbound interface based on the information found in the TCAM.

Consequently, a straightforward approach to troubleshooting a Layer3 switching problem is to verify the components that are involved in this process. First, verify the ingress Layer 3 interface, then the control plane data structures and, subsequently, the packet-forwarding data structures. (Alternatively, you can perform these steps in the reverse order.)

If the ingress interface is a routed port, the first step in this process is simple because the Layer 3 and Layer 2 ports are identical. Verifying the physical interface status and the configured IP address and subnet mask for that interface is sufficient to determine the status of the Layer 3 ingress interface. However, if the ingress interface is an SVI, its status is not directly related to any particular physical interface.

Verify SVI Status (Missing VLAN)

```
DLS1#show vlan id 100
VLAN id 100 not found in current VLAN database


DLS1#show interfaces vlan 100
Vlan100 is down, line protocol is down
  Hardware is EtherSVI, address is 0017.5a5b.b441 (bia 0017.5a5b.b441)
  Internet address is 10.1.100.252/24

<Output Omitted>
```

A VLAN interface or SVI is up if there is at least one interface in the spanning-tree forwarding state for that VLAN. This implies that if an SVI is down, you should verify VLAN existence, VLAN port assignments, and the spanning-tree state for the SVI.

In the output above, you can see that a missing VLAN results in a VLAN interface that is in state “down, line protocol is down.”

Verify SVI Status (VLAN with No Port Assigned)

```
DLS1#show vlan id 100

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
100  MGMT                             active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
100  enet  100100     1500  -      -      -        -    -        0      0


DLS1#show interfaces vlan 100
Vlan100 is up, line protocol is down
  Hardware is EtherSVI, address is 0017.5a5b.b441 (bia 0017.5a5b.b441)
  Internet address is 10.1.100.252/24

<Output Omitted>
```

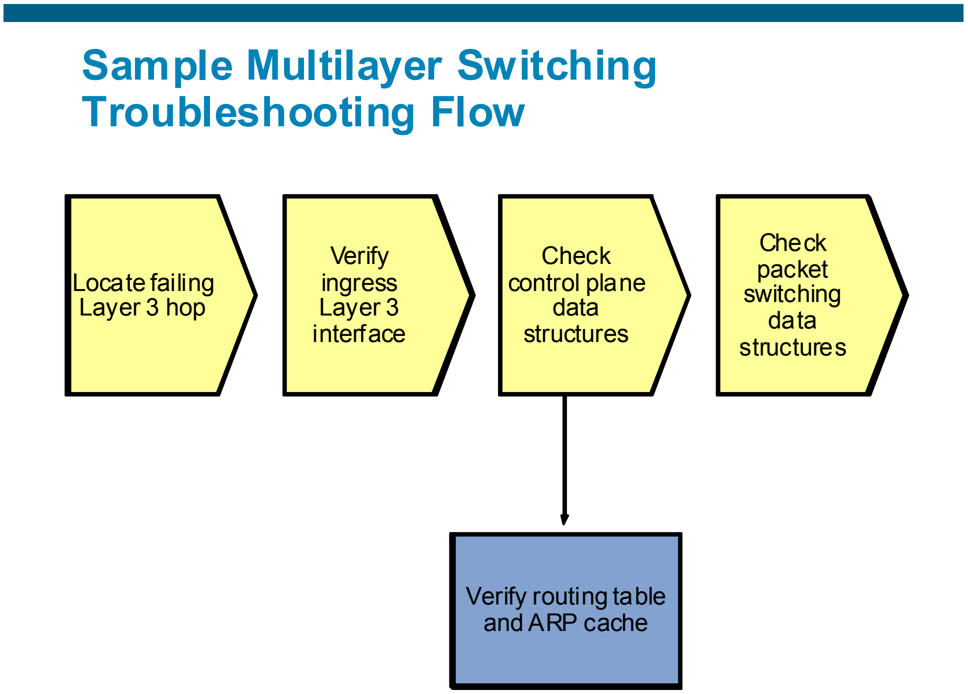
When the VLAN exists but no ports are assigned to that VLAN, the status of the SVI changes to “up, line protocol is down.”

Verify SVI Status (VLAN with No Port in Spanning-Tree Forwarding State)

```
DLS1#show spanning-tree vlan 100

<Output Omitted>

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Po1                 Desg LRN 12        128.56   P2p
Po10                Desg LRN 12        128.128  P2p

DLS1#show interfaces vlan 100
Vlan100 is up, line protocol is down
  Hardware is EtherSVI, address is 0017.5a5b.b441 (bia 0017.5a5b.b441)
  Internet address is 10.1.100.252/24

<Output Omitted>
```

Finally, if ports are assigned to the VLAN and at least one of these physical ports (trunk or access port) is up, one more condition needs to be met: The spanning-tree state for at least one of the ports needs to be forwarding. Under normal circumstances, if there is at least one interface assigned to a VLAN, an interface is in spanning-tree forwarding state. Either the switch is the root for the VLAN and all the ports assigned to the VLAN are designated ports and therefore forwarding, or the switch is not the root and it has a root port that is in forwarding state.

As a result, when you are troubleshooting a multilayer switching problem and you find that the ingress interface is an SVI and it is down, there is an underlying Layer 2 problem for that VLAN and you need to initiate a Layer 2 troubleshooting process.



Sample Multilayer Switching Troubleshooting Flow

Locate failing Layer 3 hop

Verify ingress Layer 3 interface

Check control plane data structures

Check packet switching data structures

Verify routing table and ARP cache

Verify the Routing Table and ARP Cache

The next step in this process is to verify that the control plane information that is necessary to forward the packets is present. The two control plane data structures that are relevant to multilayer switching are the routing table and the ARP cache.

In this sample troubleshooting flow, the multilayer switching data structures for an Internet Control Message Protocol (ICMP) echo request traveling from source IP address 10.1.50.1 to destination IP address 10.1.202.1 is verified by using various **show** commands.

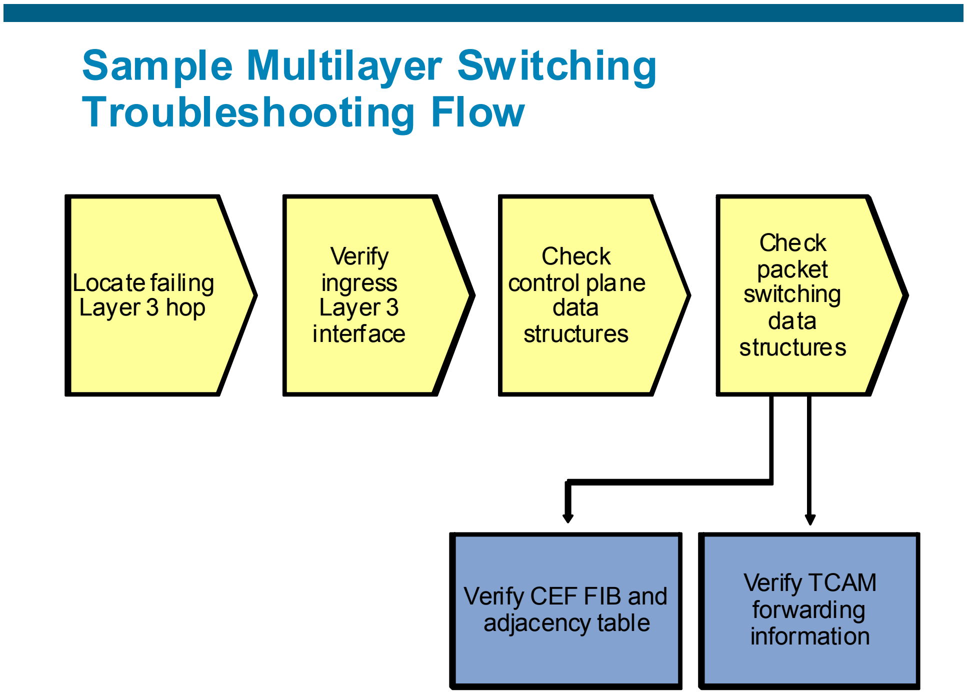
```
DLS1#show ip route 10.1.202.1
Routing entry for 10.1.202.1/32
  Known via "eigrp 1", distance 90, metric 2300416, type internal
  Redistributing via eigrp 1
  Last update from 10.1.2.2 on FastEthernet0/5, 02:41:16 ago
  Routing Descriptor Blocks:
  * 10.1.2.2, from 10.1.2.2, 02:41:16 ago, via FastEthernet0/5
      Route metric is 2300416, traffic share count is 1
      Total delay is 25100 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2

DLS1#show ip arp 10.1.2.2
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.2.2              162   001b.530d.60b1  ARPA   FastEthernet0/5
DLS1#show interfaces FastEthernet 0/5 | include bia
  Hardware is Fast Ethernet, address is 0017.5a5b.b442 (bia 0017.5a5b.b442)
```

In the output, you can see that a route is found in the routing table for the destination IP address 10.1.202.1, and the next hop and outbound interface for packets with that destination are listed.

If the routing table does not contain an entry (specific prefix or default route) for the destination, the problem is not a packet-switching problem but a routing problem, and you should initiate a process to troubleshoot the routing operation on the control plane.

The ARP cache provides the destination MAC address for the next hop. If an ARP entry for the destination is missing or listed as incomplete, either the next hop listed in the route is not valid, or there is a Layer 2 problem between the multilayer switch and the next hop. In both cases, the problem is not really a multilayer switching problem, and you should investigate the routing operation on the control plane and the Layer 2 connectivity to the next hop first.

The final element that the router needs to rewrite a frame and switch it out is the source MAC address of the frame, which corresponds to the MAC address of the outbound Layer 3 interface.



Sample Multilayer Switching Troubleshooting Flow

Locate failing Layer 3 hop
Verify ingress Layer 3 interface
Check control plane data structures
Check packet switching data structures
Verify CEF FIB and adjacency table
Verify TCAM forwarding information

When the control plane data structures have been verified, the next step in the multilayer switching troubleshooting process is to verify the data structures in software and hardware that are used to forward packets.

All recent Layer 3 switches use the Cisco Express Forwarding technology as the foundation for the multilayer switching process. The switches combine the information from the control plane data structure, such as the routing table and the ARP cache, into two different data structures: the Forwarding Information Base (FIB) and the adjacency table. These two data structures are stored in the main memory of the route processor. They are only used to forward packets that are not handled in hardware.

However, based on the information in the FIB and adjacency table, the hardware TCAM is populated, and the resulting TCAM information is what is eventually used to forward frames in hardware.

To verify the correct operation of the multilayer switching process, first verify that the control plane information is accurately reflected in the software FIB and adjacency table. Next, verify that the information from the FIB and adjacency table is correctly compiled into the TCAM.

Verify the FIB and Adjacency Table

```
DLS2#show ip cef 10.1.202.1
10.1.202.1/32
  nexthop 10.1.2.14 FastEthernet0/5

DLS2#show adjacency fastEthernet 0/5 detail
Protocol Interface                 Address
IP       FastEthernet0/5           10.1.2.14(19)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 0
                                   Encap length 14
                                   001B530D6029 00175A53A3C2 0800
                                   L2 destination address byte offset 0
                                   L2 destination address byte length 6
                                   Link-type after encap: ip
                                   ARP
```

The **show ip cef** command can be used in a similar way as the **show ip route** command. When you specify a destination IP address as an option to the command, it lists the entry in the Cisco Express Forwarding FIB that matches that IP address. It also shows the next-hop IP address and egress interface, which serve as a pointer to the adjacency table.

The **show adjacency** command can be used to display the information contained in the adjacency table. The next-hop IP address or interface can be specified to select specific adjacencies. Adding the **detail** keyword to the command shows the frame rewrite information for packets that are switched through that adjacency. The frame rewrite information lists the complete Ethernet header. For the example in the output, this consists of the destination MAC address 001B.530D.6029 (which is the same MAC address that was listed as the MAC address of next hop 10.1.2.14 in the ARP cache), followed by the source MAC address 0017.5A53.A3C2 (which equals the MAC address of the egress interface F0/5), and finally, the Ethertype 0x0800 (which indicates that the protocol contained in the Ethernet frame is IP version 4).

The information displayed in these **show** commands should accurately reflect the information in the routing table and ARP cache.

Verify the Hardware TCAM Information

```
DLS2#show platform forward fa0/3 vlan 50 0017.5a5b.b405 0017.5a53.a385 ip 10.1.50.1
10.1.202.1 icmp 8 0
Ingress:
Global Port Number: 129, lpn: 4 Asic Number: 0
Source Vlan Id: Real 50, Mapped 5. L2EncapType 0, L3EncapType 0

<Output Omitted>

Egress: Asic 0, switch 1
        CPU queues: 7 14.
Source Vlan Id: Real 50, Mapped 5. L2EncapType 0, L3EncapType 0
portMap 0x1000, non-SPAN portMap 0x1000

<Output Omitted>

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Fa0/5      1006 0017.5a53.a385  0017.5a53.a3c2
```

Note: The **show platform forward** command shown in the above output is specific to the Catalyst 3560 and 3750 series of switches. Consult the documentation for the platform that you are working with to find similar commands to examine the content of the hardware forwarding data structures for the platform.

The **show platform forward** command consults the hardware TCAM information and displays the exact forwarding behavior for a Layer 2 or Layer 3 switched frame.

This command displays the exact forwarding behavior for a packet, taking into account all features that affect packet forwarding, including Cisco Express Forwarding load balancing, EtherChannel load balancing, and packet filtering using access control lists. Therefore, you must specify the exact content of all the relevant fields in the header of the packet.

In the example command output above, the following fields are specified:

- **Ingress interface:** In the example interface, FastEthernet 0/3 is specified as the ingress interface for the packet.
- **Ingress VLAN:** It is not necessary to specify this parameter if the port is an access port. For trunk ports, you must specify the VLAN that the frame is tagged with when it enters the ingress interface. VLAN 50 is specified as the ingress VLAN.
- **Source MAC address:** The source MAC address of the frame when it enters the switch needs to be specified. In the example, the address is 0017.5A5B.B405. This is the MAC address of the egress interface of the previous hop (DLS1 Fa0/3 MAC).
- **Destination MAC address:** The destination MAC address of the frame when it enters the switch needs to be specified. In the example, the address is 0017.5A53.A385 (DLS2 Fa0/3 MAC). For a Layer 3 switched packet, this address is the MAC address of the ingress Layer 3 interface (routed port or SVI).
- **Protocol:** This is not necessary for Layer 2 switched frames. For Layer 3 switching, the Layer 3 protocol that is used and the major fields in that protocol's header must be specified. In the example, IP is listed as the protocol.
- **Source IP address:** When IP is specified as the Layer 3 protocol, the source IP address of the packet must be specified. In the example, it is 10.1.50.1.
- **Destination IP address:** When IP is specified as the Layer 3 protocol, the destination IP address of the packet must be specified. In the example, it is 10.1.202.1.
- **IP protocol:** When IP is specified as the Layer 3 protocol, the protocol in the IP header, for example, TCP, UDP, or ICMP, must be specified. In the example, ICMP is specified because the example represents an ICMP echo request packet.
- **ICMP type and code:** When ICMP is specified as the protocol, the ICMP type and code values must be specified. When TCP or UDP is specified as the protocol, additional header fields that are appropriate for those protocols, such as source and destination port numbers, must be specified. In the example, ICMP type 8 and code 0 are specified to represent an echo request packet.

This command is very powerful because it shows you exactly how frames will be forwarded based on all features that affect forwarding behavior, such as load balancing, EtherChannel, and access control lists. Also, if a frame is dropped instead of forwarded, the command lists the reason why the frame is dropped.

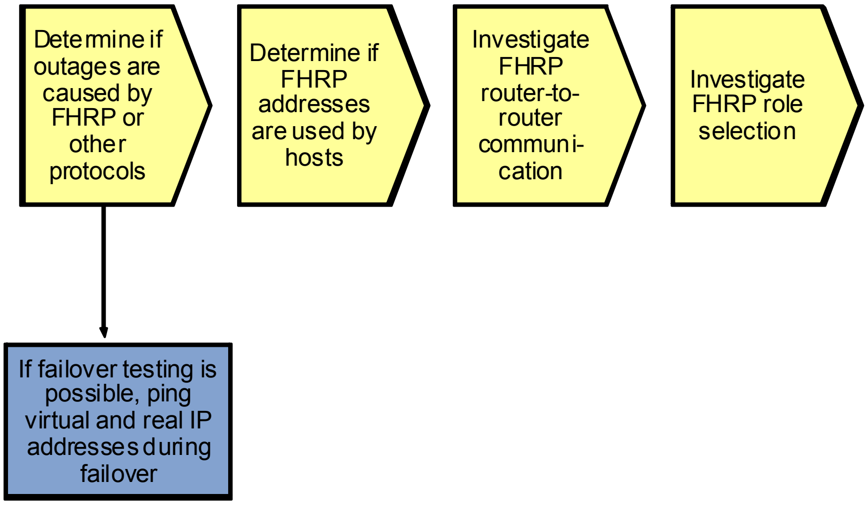
What should you do if somewhere in this chain of verifying the control plane, you find an inconsistency between the software and hardware packet-forwarding data structures?

The process of building the FIB and adjacency table from the routing table and ARP cache, and subsequently populating the TCAM based on the FIB and adjacency table, is internal to the Cisco IOS software and not configurable. Whenever you find an instance where the information in these data structures is not consistent, open a case with the Cisco Technical Assistance Center (provided that you have a valid support contract for your device) to investigate and resolve the issue. As a workaround, you can try to clear the control plane data structures, such as the routing table and the ARP cache, for the particular entries that you are troubleshooting. This triggers both the control plane and the packet-forwarding data structures to be repopulated for those entries and, in certain cases, this might resolve the inconsistencies. However, this is only a workaround, not a real solution, because it only addresses the symptoms of the problem and not the underlying cause.

Troubleshooting First Hop Redundancy Protocols

The figure illustrates an example of a method that you could follow to diagnose and resolve problems related to FHRPs, such as HSRP, VRRP, and GLBP.

Sample First Hop Redundancy Troubleshooting Flow



Determine if outages are caused by FHRP or other protocols

Determine if FHRP addresses are used by hosts

Investigate FHRP router-to-router communication

Investigate FHRP role selection

If failover testing is possible, ping virtual and real IP addresses during failover

The most common reason to start troubleshooting FHRP behavior is because during an outage or a test, network connectivity is lost for longer than expected when a redundant device or link is temporarily disabled. In redundantly configured IP networks, a number of different protocols usually need to reconverge to recover from a failure. The FHRP that is used is just one of the protocols that could be the cause of the loss of connectivity. Other protocols that need to converge as well—and could be the cause of the problem—are routing protocols and Spanning Tree Protocol (STP).

So how do you determine if the FHRP is the problem?

If you have the opportunity to execute failover tests (for instance, during a scheduled maintenance window), a good way to determine if the problem is caused by the FHRP or by another protocol is by sending multiple continuous pings from a client that is using the virtual router as its default gateway. Ping to the virtual and real IP addresses of the routers that participate in the FHRP, and ping to an IP address of a host that is one or more router hops removed from the client. Observe and compare the behavior of the pings while you force a failover by disabling a device or a link.

Based on the observed differences between the ping responses, you can draw conclusions about the likelihood that the problem is related to the FHRP or to any other protocols that are involved in the convergence. Here are a few examples:

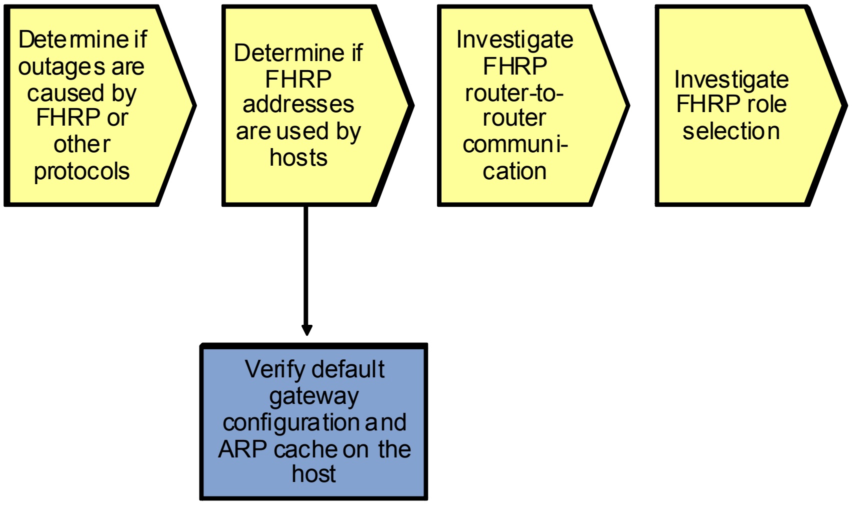
- If you observe that the pings to the real IP address of the redundant router and the virtual IP address of the FHRP both fail at the same time and resume at the same time when you disable the primary router, assume that the problem is not related to the FHRP (because the FHRP does not affect the pings to the real IP address). The most likely cause in this scenario is the Layer 2 convergence for the VLAN, so you should start a Layer 2 troubleshooting procedure.
- If you observe that the pings to the real IP address of the redundant router do not suffer any packet loss, but pings to the virtual IP address fail, this strongly suggests that there is a problem with the FHRP.

- If you observe that the pings to the real IP address of the redundant router and to the virtual IP address do not suffer packet loss, but the ping to the host further out in the network fails, this might indicate an issue with the routing protocol. Alternatively, it could indicate that the client is using the primary router address as its default gateway rather than the virtual IP address.

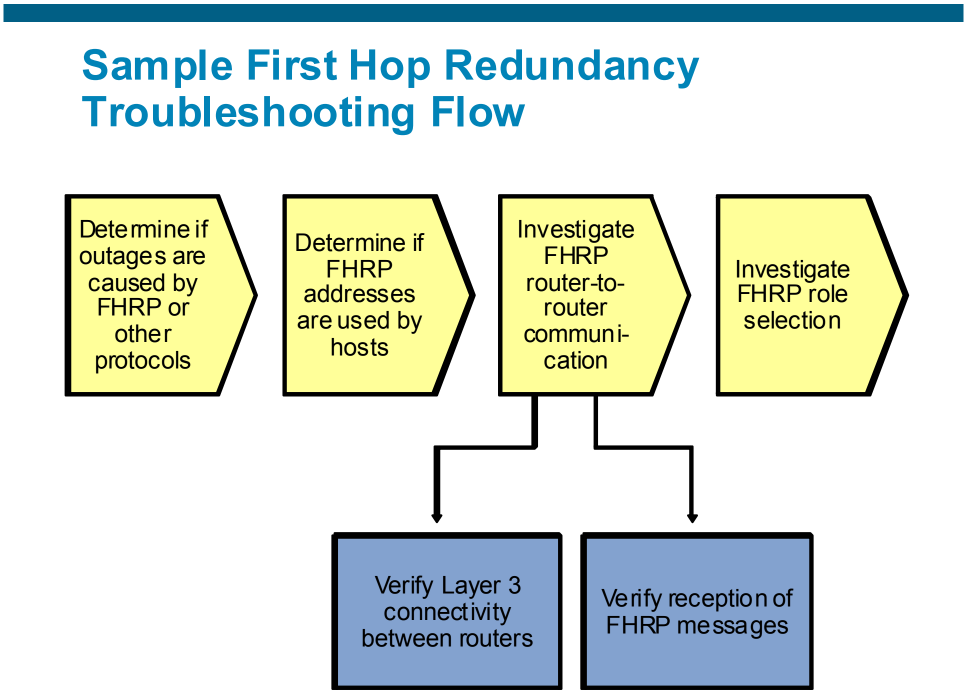
There are too many possible scenarios, combinations of ping results, and conclusions to list, but important clues can be gained in any scenario by comparing the differences between several pings during a failover.

If you have to troubleshoot without the opportunity to force failover for testing purposes, you might need to assume that the FHRP is the cause of the problem and carefully verify its implementation and operation, even if you cannot determine beforehand if this might be the cause of the problem.

Sample First Hop Redundancy Troubleshooting Flow


Determine if outages are caused by FHRP or other protocols
Determine if FHRP addresses are used by hosts
Investigate FHRP router-to-router communi-cation
Investigate FHRP role selection
Verify default gateway configuration and ARP cache on the host

Before starting to troubleshoot the FHRP itself, verify if the client is correctly using the virtual IP address and MAC address of the FHRP as its default gateway. This involves verifying the default gateway configuration (whether statically configured or learned via DHCP) and the ARP cache on the client to verify that both the virtual IP address and the virtual MAC address on the client match the expected values for the FHRP that is in use.



Sample First Hop Redundancy Troubleshooting Flow

Determine if outages are caused by FHRP or other protocols
Determine if FHRP addresses are used by hosts
Investigate FHRP router-to-router communi-cation
Investigate FHRP role selection
Verify Layer 3 connectivity between routers
Verify reception of FHRP messages

Many problems with FHRPs are caused by underlying problems in the Layer 3 connectivity between the routers. Therefore, a good next-step in the troubleshooting process is to verify that there is Layer 3 connectivity between all routers that are participating in the FHRP. Ping from each of the participating routers to the IP addresses of the other participating routers. If one of these pings fail, start a troubleshooting process to diagnose and resolve the Layer 3 connectivity issues between the routers before further investigating the FHRP.

When you have confirmed that there is Layer 3 connectivity between the participating routers in general, you must verify the proper transmission and reception of FHRP packets. To limit potential disruption, always use **`show`** commands to gather information before using **`debug`** commands.

Verify Reception of FHRP Messages

```
DLS1#show standby vlan 100 brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl100       100  110 P Active  local           10.1.100.253    10.1.100.254


DLS2#show standby vlan 100 brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl100       100  100 P Standby 10.1.100.252    local           10.1.100.254
```

This example shows how to confirm proper transmission and reception of HSRP messages. For GLBP or VRRP, the procedure is similar, although the command output is slightly different.

To confirm the proper reception of HSRP messages on all routers in the group, verify that all routers list an active and a standby router and that these roles are listed in a consistent way across all the routers. The **`show standby brief`** command is concise and still shows the most relevant information. As you can see in the example, switch DLS2 lists the IP address of switch DLS1 as the active router. As the standby router, it lists “local” to indicate that it considers itself to be the standby router. On switch DLS1, the situation is the opposite: The address of switch DLS2 is listed as the standby address, while the active router is listed as local. While you are verifying these roles, this is also a good opportunity to confirm that both the standby group number and the virtual IP address are configured in a consistent manner. Misconfiguration of these parameters is a common cause of HSRP problems.

```
DLS1#debug standby packets

DLS1#show logging | include Grp 100
Oct 26 15:29:00.049: HSRP: Vl100 Grp 100 Hello  in  10.1.100.253 Standby pri 100
vIP 10.1.100.254
Oct 26 15:29:01.659: HSRP: Vl100 Grp 100 Hello  out 10.1.100.252 Active  pri 110
vIP 10.1.100.254
```

Note: If you used Telnet, you cannot see the debug messages without using the **terminal monitor** command.

If you find inconsistencies in the output of the **show standby brief** commands, such as a missing standby router on one of the routers or multiple routers claiming the active or standby role for a group, this strongly suggests that there is a problem with the reception or interpretation of the HSRP messages on the routers. A **debug** command can now be used to investigate the transmission and reception of HSRP messages to gather more clues about the failure.

Before enabling a debug, first verify that the CPU of the device is not running at such high levels that adding the load of a debug would risk overloading the CPU. Secondly, it is always good to have a fallback plan to stop the debug when it unexpectedly starts to affect the performance of the device. For instance, you could open a second connection to the device and before you enable the debug in your primary session, type the **undebug all** command in the secondary session, but do not confirm it by pressing the Enter key yet. Another fallback scenario is to schedule a timed reload within a short time by using the **reload in** command. If you lose your connection to the device as a result of your debug, you can be assured that it will reload shortly and you will be able to reconnect to it. And finally, you should always refer to your organization's policies before executing any commands on a device that put the operation of the network at risk.

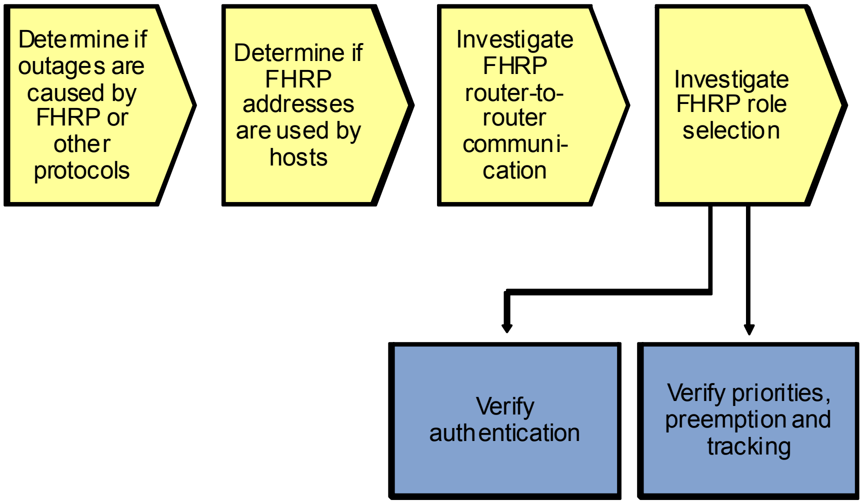
The **debug standby packets** command displays all HSRP packets sent or received by the device. This can quickly generate a lot of output, especially if you have configured many different HSRP groups or if you have tuned the hello timer to be shorter than the default value of three seconds. To make it easier to select the packets that you are interested in, you could use the technique shown in the example above. Instead of logging the debug output to the console or virtual terminal session, you can capture the output in a buffer in the device's RAM and then display the buffer's content by using the **show logging** command. The output of the command can then be filtered by using a regular expression to select the HSRP group that you are interested in.

In the example above, the output reveals that hellos are sent by this router and received from the other router. Just like the **show** commands in the previous output examples, execute the **debug** command on both routers to spot possible differences in behavior between the devices.

Do not forget to disable the debug by using the **no debug** command after you have gathered the information that you were interested in.

If these debugs reveal that HSRP protocol packets are not properly received on any router, check if access lists are blocking the packets. Given that you have already verified the Layer 3 connectivity between the devices, this problem should be on a higher layer.

Sample First Hop Redundancy Troubleshooting Flow



Determine if outages are caused by FHRP or other protocols

Determine if FHRP addresses are used by hosts

Investigate FHRP router-to-router communi-cation

Investigate FHRP role selection

Verify authentication

Verify priorities, preemption and tracking

After you have established that FHRP messages are sent and received properly on all routers and still the FHRP does not perform as expected, the problem must be related to the role selection and transferring roles between routers during failover. You might need to verify two potential problem areas.

If the FHRP is using authentication and there is a mismatch between the authentication parameters, the devices will not accept each other's messages as valid when they are received. A typical symptom is that more than one router considers itself to be the active router for a group.

For all FHRPs, role selection is influenced by two parameters: priority and preemption. Tracking objects such as interfaces and routes can further alter these priorities. If an unexpected router is selected for the primary role at any point in the process, carefully analyze the priorities configured on the different devices and how they are affected by potential tracking options. However, to properly determine how properties behave during a failover, you must be able to force a failover, which means that you might need to postpone this type of testing until a regularly scheduled maintenance interval.