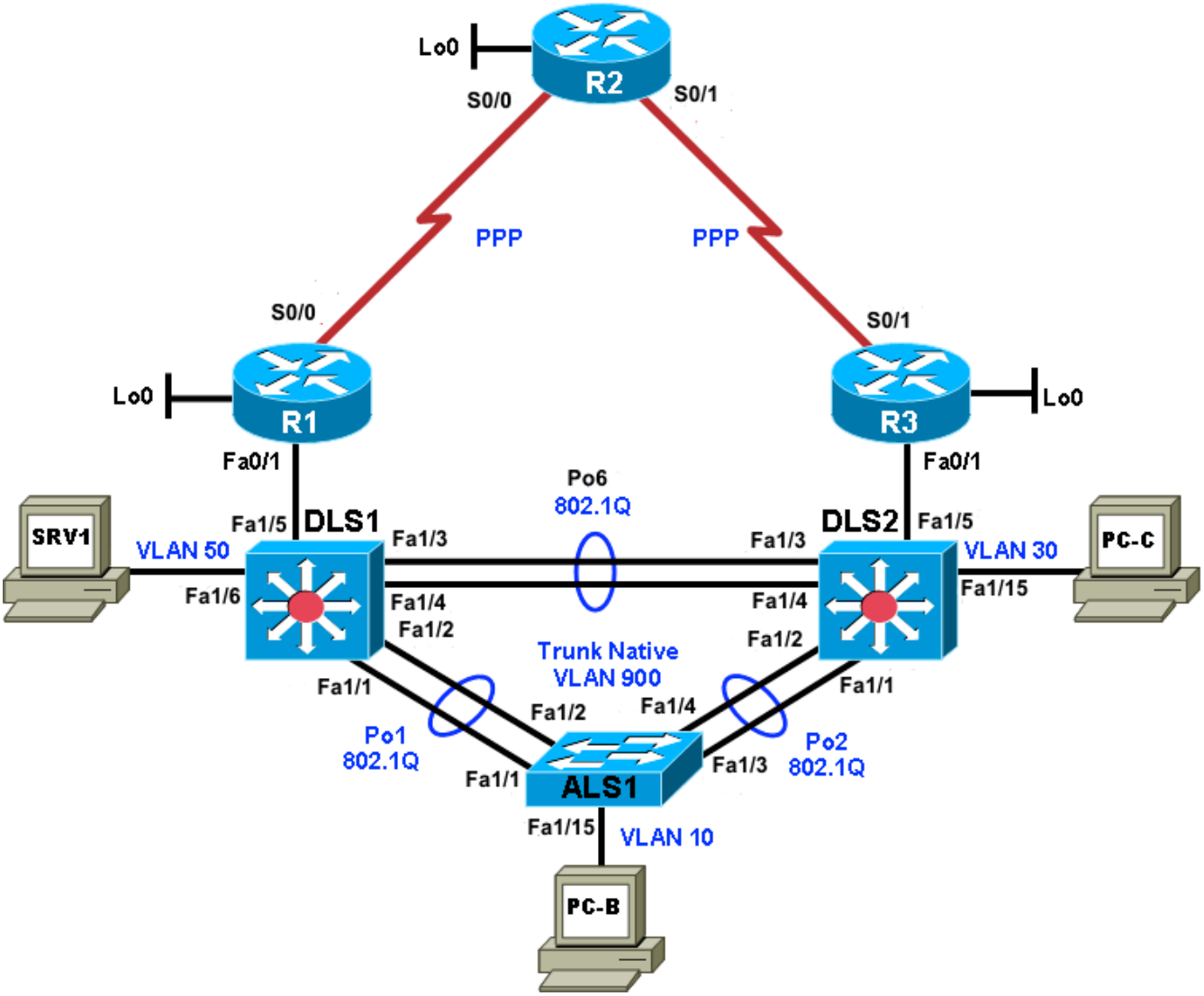
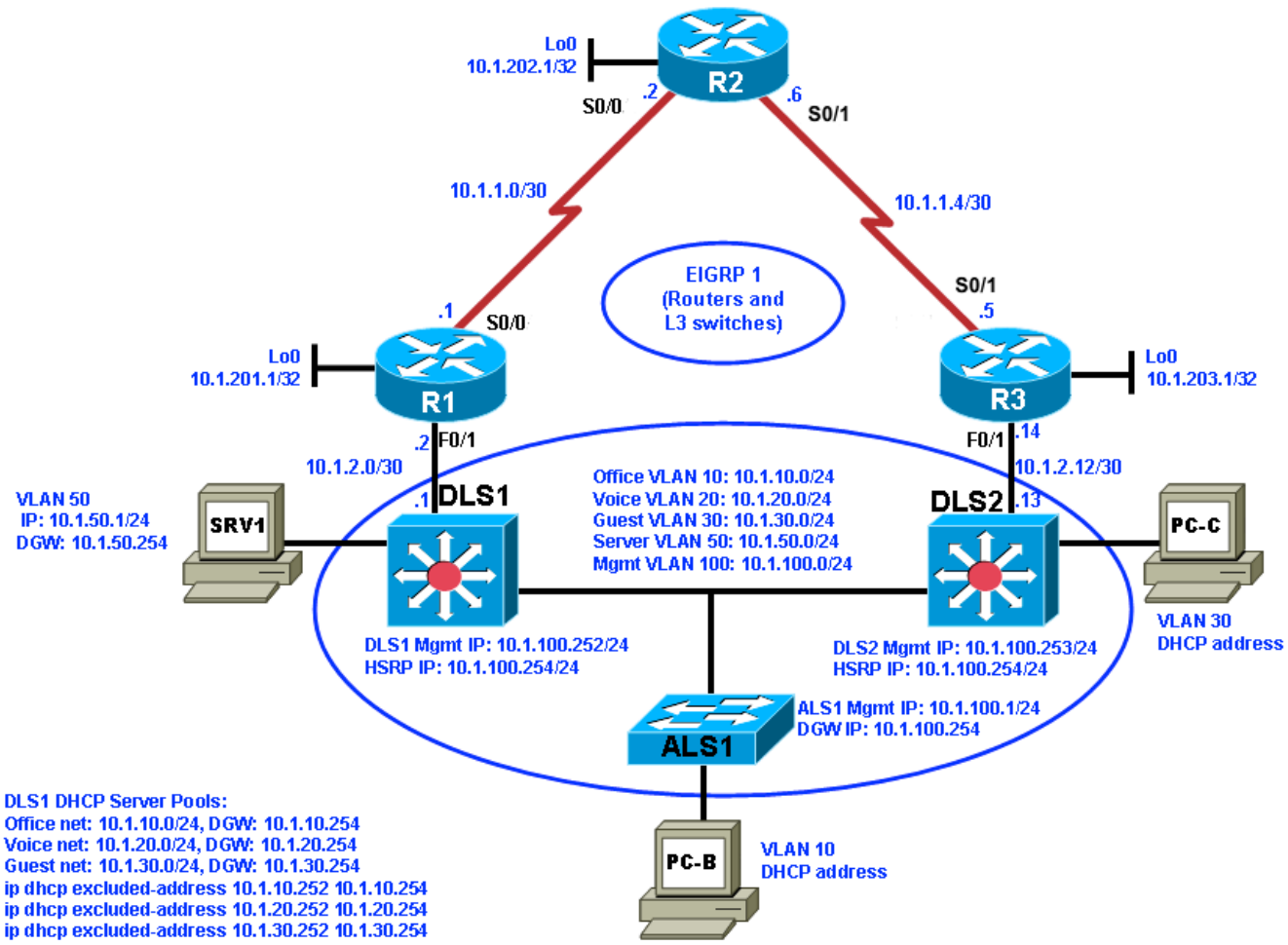
Lab 5-1, Layer 3 Connectivity and EIGRP

Physical Topology



Logical Topology



Objectives

- Load the trouble ticket device configuration files for each trouble ticket.
- Diagnose and resolve problems related to network layer connectivity.
- Diagnose and resolve problems related to EIGRP.
- Document troubleshooting progress, configuration changes, and problem resolution.

Background

Because of the complexity of modern networks, Layer 3 routing issues are quite common and can also be difficult to troubleshoot. One of the most widely used enterprise routing protocols is Enhanced Interior Gateway Routing Protocol (EIGRP). It is a Cisco proprietary distance vector, classless routing protocol that was released in 1992 with Cisco IOS Release 9.21. EIGRP has features that are not commonly found in other distance vector routing protocols, such as the following:

- Reliable Transport Protocol (RTP)
- Bounded updates
- Diffusing Update Algorithm (DUAL)

- Establishing adjacencies
- Neighbor and topology tables

In this lab, you will troubleshoot problems related to Layer 3 connectivity and routing problems related to EIGRP.

For each task or trouble ticket, the trouble scenario and problem symptom are 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 51-A (3 Issues)

Step 1: Review trouble ticket Lab 51-A.

Your company is interested in implementing an IP-based closed circuit television (CCTV) solution. Currently, different solutions and vendors are being evaluated. One of the vendors has offered to implement a pilot to show the capabilities of their solution. To keep the traffic associated with the CCTV solution separate from the regular network traffic, it will be implemented using a new VLAN (VLAN 70 corresponding to subnet 10.1.70.0/24). There must be communication between the test server (PC-C) and the office users on the LAN. In addition, branch workers on the R2 LAN (simulated by Lo0) must be able to access the internal CCTV server.

The vendor will come in tomorrow to install the client and server software. The network team has been asked to make sure that the new VLAN has been implemented and that there is IP connectivity between the local test client (PC-B) and the CCTV test server (PC-C) in the CCTV VLAN. You must also verify that there is connectivity between the remote test client (Lo0 on R2) and the CCTV test server. The test server requires a static IP address. One of your colleagues implemented the static address yesterday afternoon, but did not have time to test the implementation.

You have the following tasks:

- Configure the CCTV test server (PC-C).
- Verify the CCTV VLAN device configurations for the pilot.
- Ensure that the local and remote test clients can communicate with the CCTV test server before the vendor arrives to implement the CCTV pilot.
- Verify Hot Standby Router Protocol (HSRP) redundancy for CCTV VLAN 70.

Step 2: Load the device trouble ticket configuration files for 51-A.

a. On each device issue the command **51-A**

b. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-51A**

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: Configure the CCTV server IP address.

Configure the test server PC-C with a static IP address in the CCTV test VLAN subnet 10.1.70.0/24. According to the test plan, the default gateway should be the last usable IP address in the subnet.

Note: After this TT is completed, restore PC-C to its status as a DHCP client in VLAN 30.

Step 6: 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 51-B (1 Issue)

Step 1: Review trouble ticket Lab 51-B.

You receive an emergency call and are told that a short circuit caused a small fire in the server room. Routers R1 and R3, which were mounted in the same rack, were damaged. Luckily, you had two comparable spare routers in storage. When you arrive at the office, two of your colleagues have already installed the replacement routers, cabled them, and tried to restore the routers by cutting and pasting the configurations from the console. However, the routers are not operational when you come in.

You receive a call from the network administrator at the branch office (LAN simulated by R2 Lo0) asking about the loss of the WAN. His users cannot access server SRV1 at the central site. He has started to troubleshoot. You tell him what happened and ask him not to do anything until you have resolved the problem at the central site.

Your task is to check the configuration of routers R1 and R3 and restore the configurations as necessary to regain connectivity between the branch office and the central site across the WAN.

Step 2: Load the device trouble ticket configuration files for 51-B.

a. On each device issue the command **51-B**

b. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-51B**

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 procedure, and procedure and communication improvements.

_____

_____

_____

Task 3: Trouble Ticket Lab 51-C (1 Issue)

Step 1: Review trouble ticket Lab 51-C.

A user on VLAN 10 (PC-B) called the help desk this morning because she does not have Internet access. When she tried to open a website (simulated by another Loopback Lo1 on R2 with address 209.165.200.225/30), she received an error message from her browser saying that it cannot display the web page. She can reach the internal server SRV1 without any problems.

One of your colleagues was working with the ISP to make some changes to the routing model used to access the ISP and the Internet. The ISP does not run EIGRP on its router. The colleague has called in sick today, but made some notes in the log about the ISP not running EIGRP on its router and not wanting R2 to attempt to establish an EIGRP neighbor relationship.

Your task is to diagnose and solve this problem and make sure that the user regains connectivity to the Internet.

Step 2: Load the device trouble ticket configuration files for 51-C.

c. On each device issue the command **51-C**

d. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-51C**

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

Step 3: Clear mac address table on DSL1 and DSL2

f. `DLS1#clear mac`

g. `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.

_____

_____

Task 4: Trouble Ticket Lab 51-D (1 Issue)

Step 1: Review trouble ticket Lab 51-D.

A contract worker called the help desk to report that he could not access the ISP email server (simulated by Lo0 on R2). He was working at a PC that is attached to a port in the GUEST VLAN (PC-C). You checked with the ISP and discovered that they had an unplanned outage, and the WAN link from R2 to R3 had gone down temporarily. Users in the OFFICE VLAN did not experience any loss of connectivity to the email server during the WAN link outage. Your expectation, if one of the WAN links went down, was that users in the GUEST VLAN would still be able to reach the server because of the redundancy in the network design.

Your colleague will replicate this scenario during the maintenance window this evening. You have agreed to help her diagnose the problem and propose a plan that can account for an outage in one of the WAN links to R2 so that guest users do not lose connectivity to the ISP mail server.

Your plan is to simulate the R3-to-R2 WAN link going down. You do not have administrative control over ISP router R2. You will test connectivity, determine the cause of the problem, and recommend which configuration changes to the devices could correct the issue.

Step 2: Load the device trouble ticket configuration files for 51-D.

h. On each device issue the command **51-D**

i. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-51D**

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

Step 3: Clear mac address table on DSL1 and DSL2

k. `DLS1#clear mac`

l. `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.

Command Summary

The table lists useful commands for this lab. Sample output is shown on the following pages.

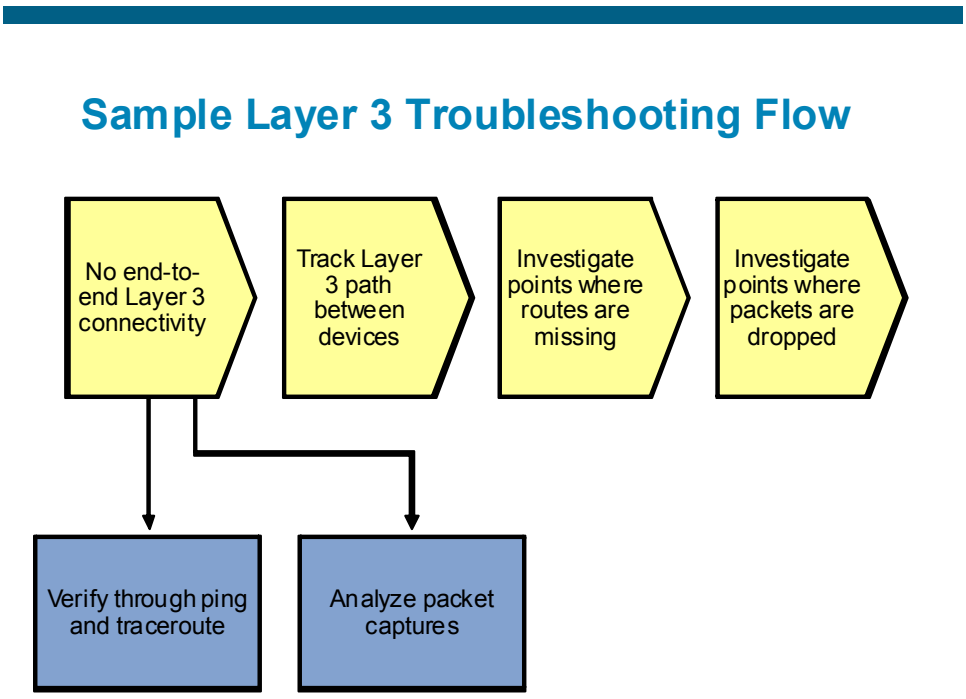
Command	Key Information Displayed
show spanning-tree vlan *vlan#*	Displays all essential parameters that affect the topology, such as the root port, designated ports, port state, and port type, as well as the spanning-tree mode being implemented.
show vlan brief	Displays a quick overview of all existing 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 ip interface vlan *vlan#*	Displays the SVI status, IP address, statistics, and IP Cisco Express Forwarding (CEF) information.
show ip route *ip-addr*	Displays the routing table information for a particular destination address.
show ip cef *ip-addr* **detail**	Displays the next hop and interface used for a particular destination address from the CEF table.
show ip cef exact-route src-*ip-addr dest-ip-addr*	Displays the next hop and interface used for a particular destination address from the CEF table.
show adjacency *int-type/#* **detail**	Displays information contained in the adjacency table for a next-hop IP address or interface.
show standby vlan *vlan#* **brief**	Verify active and standby roles and IP addresses for a particular VLAN for HSRP routers.

show standby brief	Verify active and standby roles and IP addresses for all VLANs on an HSRP router.
show ip eigrp interfaces	Displays interfaces that are participating in the EIGRP routing process. An interface does not need to be operational to be listed in the output.
show ip eigrp neighbors	Displays the EIGRP neighbor table to verify that all expected neighbor relationships are operational.
show ip eigrp topology *ip-addr net-mask*	Displays the EIGRP topology, which contains all routes that were received from all neighbors for a particular prefix.
debug eigrp packets	Displays real-time messages exchanged between EIGRP routers. **Caution:** Produces large amounts of output.
debug ip eigrp *as#* **neighbor** *ip-addr*	Displays real-time messages exchanged for a particular neighbor.
debug ip eigrp	Displays the processing of routing events by the router. **Caution:** Produces large amounts of output.

Lab 5-1 Sample Troubleshooting Flows

Troubleshooting IP Connectivity

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



Layer 3 is a common starting point for many troubleshooting procedures. An often applied method is the divide-and-conquer approach. When a user reports a problem concerning connectivity to a certain service or application running on a server, a good first step is to determine if there is end-to-end IP connectivity between the client and the server. If this is the case, you can focus on the higher layers of the Open Systems Interconnection (OSI) reference model.

End-to-end IP connectivity can be confirmed or denied by using the **ping** or **traceroute** commands. Almost every operating system supports these commands in some form, but the syntax might be slightly different for different operating systems.

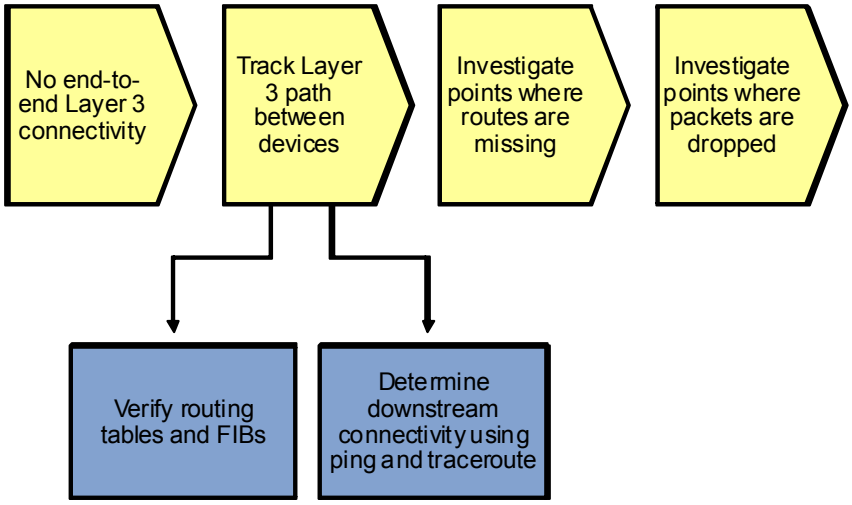
A prerequisite to using this method is that the appropriate Internet Control Message Protocol (ICMP) messages are allowed on the network and not blocked by any firewalls, including host-based firewalls on the destination host. If you cannot use ping and traceroute effectively, you might have to resort to analyzing traffic captures of the actual traffic flows to determine if packets can be sent at the network layer between the affected hosts.

Using the Correct Source Address

```
R2#ping 10.1.50.1 source Lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.50.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.202.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/20/32 ms

R2#traceroute 10.1.50.1 source Lo0

Type escape sequence to abort.
Tracing the route to 10.1.50.1

  1 10.1.1.1 16 msec 16 msec 8 msec
  2 10.1.2.1 8 msec 16 msec 12 msec
  3 10.1.50.1 12 msec 12 msec 8 msec
```

Be aware that a successful ping or traceroute response is dependent on two things: the availability of a route to the destination and a route back to the source. Especially when running tests from the first-hop router in the path, make sure to specify the source address of the ping or traceroute. If you do not specify the source address, the router uses the IP address of the egress interface as the source for the packets. Using an address from a different source subnet than the client might lead you to reach wrong conclusions if the problem concerns the return path for the packets.

Sample Layer 3 Troubleshooting Flow



If you have determined that there is a problem with the end-to-end IP connectivity between the affected hosts, you want to reduce the scope of the problem and isolate the points in the path between the hosts where the connectivity is lost.

A commonly used method is to track the path of the packets. You can use the following method to diagnose end-to-end IP connectivity problems:

- Determine the Layer 3 path. Based on documentation, baselines, and knowledge of your network in general, the first step is to determine the path that you would expect packets to follow between the affected hosts. Determining the expected traffic path beforehand helps in two ways. It provides a starting point for gathering information about what is happening on the network, and it makes it easier to spot abnormal behavior. The second step in determining the Layer 3 path is to follow the expected path and verify that the links on the path are up and forwarding traffic. If the actual traffic path is different from your expected path, this step might provide clues about which links or protocols are failing and the cause of these failures.
- To track the path of the packets between the hosts, first track the path that is being used according to the control plane information. Start at the client and verify the IP address, subnet mask, and default gateway. Then go to the router that is listed as the default gateway and check which route is used for the destination IP address. Determine the next-hop router based on the information in the routing table. Connect to the next-hop router and repeat this procedure until you arrive at the router that is directly connected to the destination host. Then repeat the process for the route back from the destination to the source.
- If the router has no route in the table for the destination network, you must diagnose the process that is the source of the routing information on this router, such as the routing protocol or static routes.
- If you have verified that the routing information is present on the complete path from the source to the destination and from the destination back to the source but connectivity is failing, you must track the path again, but now determine at which point packets are being dropped. The likely causes for dropped packets are Layer 1 problems, Layer 2 problems, or Layer 3 to Layer 2 mapping problems. When you have determined the point where the packets are dropped, use the specific troubleshooting methods appropriate for the Layer 2 technology that is used on the egress interface.

These steps do not necessarily have to be taken in the order presented here. Often different aspects of this generic procedure are combined, and shortcuts can be taken based on the result. For instance, determining proper packet forwarding is often done in parallel with determining the routes by using ping to verify the

reachability of the next-hop derived from the route or using ping and traceroute to the final destination from intermediate routers in the path.

If you find that a ping is successful from a particular point in the path, you know that routes to the destination must be available on all the downstream routers. You can then use traceroute to determine the path to the destination, instead of connecting to each router in the path. However, this method has a hidden assumption: Packets traveling to the same destination use the same path, regardless of their source. This is not necessarily the case in a redundant network with equal-cost paths to a certain destination. The source address is typically used as part of the load-balancing algorithm that determines the path used when equal-cost paths are available. It is important to determine the exact path for the actual source and destination IP address pair that is affected, especially in cases where control plane information is available in both directions but packets are dropped.

Verify the Routing Table

```
R2#show ip route 10.1.10.1
Routing entry for 10.1.10.0/24
  Known via "eigrp 1", distance 90, metric 2172672, type internal
  Redistributing via eigrp 1
  Last update from 10.1.1.5 on Serial0/0/1, 02:05:21 ago
  Routing Descriptor Blocks:
    10.1.1.5, from 10.1.1.5, 02:05:21 ago, via Serial0/0/1
      Route metric is 2172672, traffic share count is 1
      Total delay is 20110 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
  * 10.1.1.1, from 10.1.1.1, 02:05:21 ago, via Serial0/0/0
      Route metric is 2172672, traffic share count is 1
      Total delay is 20110 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

When you are troubleshooting IP connectivity to a specific destination IP address, you can use the **show ip route *ip-address*** command to determine the best prefix match for the IP address, the egress interface, and, for multipoint interfaces, the next-hop IP address. If multiple equal-cost paths are present, as can be seen in the example above, each entry is listed.

The routing source is also listed, such as directly connected, static, or the routing protocol. Additional control plane parameters that are associated with the route source, such as the administrative distance, routing protocol metrics, source router, and route age, are also displayed. To interpret these parameters, more detailed knowledge of the specific routing protocol is required. More detailed information can often be gathered from that specific protocol's data structures.

This command never displays the default route 0.0.0.0/0 as a match, even if it is the longest prefix match for a packet. Therefore, if this command displays the message "% Network not in table," you cannot conclude that packets will be dropped, so you need to verify if a default route is present by using the **show ip route 0.0.0.0 0.0.0.0** command.

Verify the Cisco Express Forwarding Information Base

```
R2#show ip cef 10.1.10.1
10.1.10.0/24
  nexthop 10.1.1.1 Serial0/0/0
  nexthop 10.1.1.5 Serial0/0/1
```

To see the best match for a specific IP address in the Forwarding Information Base (FIB), use the **show ip cef *ip-address*** command. This command lists the same forwarding information as the **show ip route** command but without the associated control plane information, such as routing protocol metrics, administrative distance, and so on. This command displays the default route 0.0.0.0/0 if it is the best match for the destination IP address. If the routing table for a route contains multiple entries, these same entries will also be present in the FIB.


```
DLS1#show ip cef exact-route 10.1.10.1 10.1.202.1
10.1.10.1 -> 10.1.202.1 => IP adj out of FastEthernet0/5, addr 10.1.2.2

R2#show ip cef exact-route 10.1.202.1 10.1.50.1
10.1.202.1 -> 10.1.50.1 => IP adj out of Serial0/0/0
```

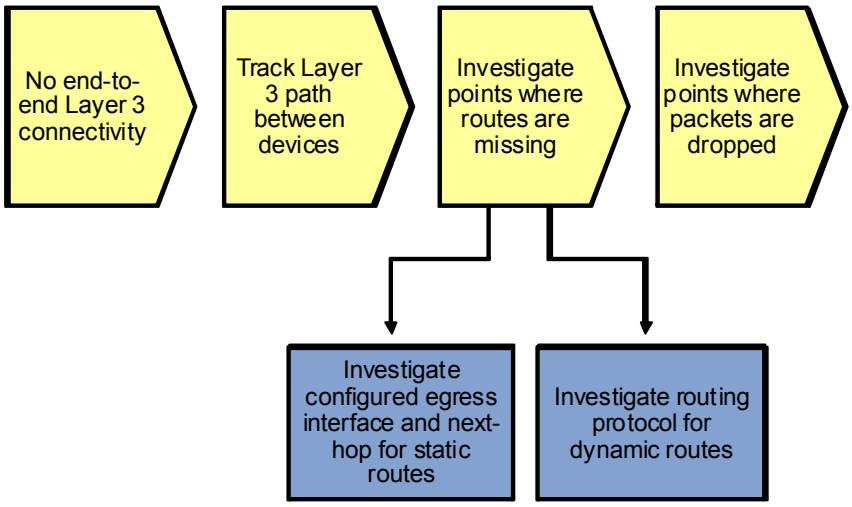
When you are tracing the packet flow between two specific hosts and the routing table and the FIB lists multiple entries (because there are multiple equal-cost paths), you must determine which entry is used to forward the packets associated with the specific source and destination IP address pair that you are troubleshooting. You can use the **show ip cef exact-route** command in these situations to determine the specific egress interface and next-hop IP address for the specific IP address pair.

On multilayer switches, instead of consulting the FIB that is stored in the main memory of the switch, you must consult the forwarding information stored in the hardware ternary content addressable memory (TCAM), because packet forwarding is handled by the TCAM, not the Cisco Express Forwarding FIB.

Although the FIB is used to compile the information that is loaded into the TCAM, the load-balancing algorithms that are used are different and do not necessarily yield the same result.

To learn more about the commands that can be used to verify the Layer 3 forwarding information contained in the TCAM, see the multilayer switching sections of the TSHOOT Student Guide and this Lab Guide.

Sample Layer 3 Troubleshooting Flow



After you have found a point in the network where no route is present in the routing table for the destination IP address (or when analyzing the return path for the source IP address) of the session, you need to investigate what caused that route not to be installed in the routing table.

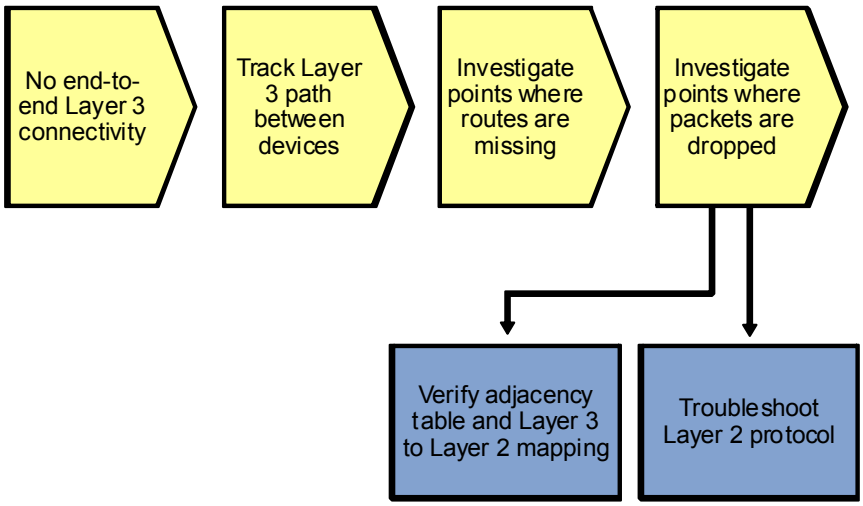
To correctly diagnose why a particular route is missing from the routing table, you first need to consult your documentation and baselines to find out what is the expected routing source. Is static routing or a routing protocol used on this router?

If a static route has been configured but it is not listed in the routing table, verify the status of the associated egress interface. If the egress interface for a static route is down, the route will not be installed in the routing table. If the route is not configured with an egress interface but with a next-hop IP address, the same rule applies. The router executes a recursive routing table lookup on the next hop for the static route. If no matching route and

associated egress interface can be found for the configured next-hop IP address of the static route, the route is not installed in the routing table. If a match is found for the next-hop IP address, the static route is installed.

For dynamic routing protocols, you must initiate a troubleshooting process that is appropriate for that specific protocol and try to determine why the route was not learned on this router or, if it was learned, why it is not used.

Sample Layer 3 Troubleshooting Flow



If you have verified the presence of correct routing information along the paths in both directions but you find that packets are dropped at a certain hop in the path, you must diagnose the packet-forwarding process.

If a route is present in the routing table (and the FIB if Cisco Express Forwarding is used) but packets are not forwarded correctly, verify if a correct mapping between the IP next hop and the Layer 2 protocol is used on the egress interface. If the router cannot find all the necessary Layer 2 information to construct a frame to encapsulate a packet, it is dropped, even if the routing information is present in the routing table.

The exact command to verify the Layer 3-to-Layer 2 protocol mapping is dependent on the Layer 2 technology used on the egress interface. Examples are the **show ip arp** command for Ethernet networks and the **show frame-relay map** command for Frame Relay.

For more information about the exact command syntax, research the Layer 2 technology used in the configuration guides and command references on http://www.cisco.com.

If you find incorrect mappings, or if you find the mappings to be correct but frames are not forwarded correctly, initiate a Layer 2 troubleshooting procedure for the Layer 2 technology that is being used.

Verify the Adjacency Table

```
DLS1#show adjacency fa0/5 detail
Protocol  Interface                 Address
IP        FastEthernet0/5           10.1.2.2(15)
                                    0 packets, 0 bytes
                                    epoch 0
                                    sourced in sev-epoch 0
                                    Encap length 14
                                    001B530D60B100175A5BB4420800
                                    L2 destination address byte offset 0
```

```
L2 destination address byte length 6
Link-type after encap: ip
ARP
```

Regardless of the Layer 2 technology, if Cisco Express Forwarding is used as the Layer 3 forwarding method, you can verify the availability of Layer 2 forwarding information using the **show adjacency** *int-type/#* **detail** command.

As can be seen in the example above, this command lists the Layer 2 frame header that is used to encapsulate packets transmitted via the listed adjacency. In this example, the frame header is 001B530D60B100175A5BB4420800, which is dissected as follows:

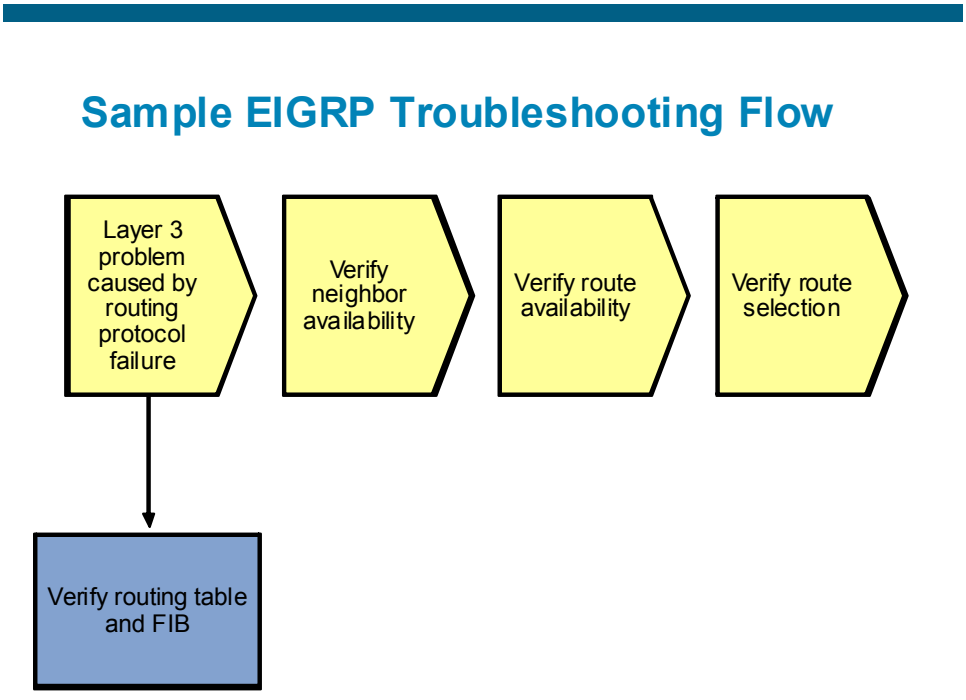
- **001B530D60B1** – This is the destination MAC address of the frame, which corresponds to the MAC address of the next hop 10.1.2.2.
- **00175A5BB442** – This is the source MAC address of the frame, which corresponds to the MAC address of interface FastEthernet 0/5.
- **0800** – This is the Ethernet type field, which indicates that the frame contains an IP packet, because Ethernet type value 0x800 is registered as the value for IP.

If you are troubleshooting a Layer 3 forwarding problem and the IP next hop and interface listed in the routing table are not present in the adjacency table, there is a problem with the Layer 3-to-Layer 2 mapping mechanisms.

If a Layer 2 frame header is listed in the adjacency table but the frames are not forwarded correctly across the Layer 2 medium, you must troubleshoot the underlying Layer 2 technology. The information contained in the header can be useful information when you start the Layer 2 troubleshooting process.

Troubleshooting EIGRP

The figure illustrates a method for diagnosing and resolving problems related to EIGRP.



The usual trigger to start investigating routing protocol operation is when you are troubleshooting IP connectivity to a particular destination and you find that the route to the destination network is missing from the routing table of one of the routers or that a different route than expected was selected to forward the packets to that destination.

To install a route into the routing table, each router that uses a routing protocol goes through several stages:

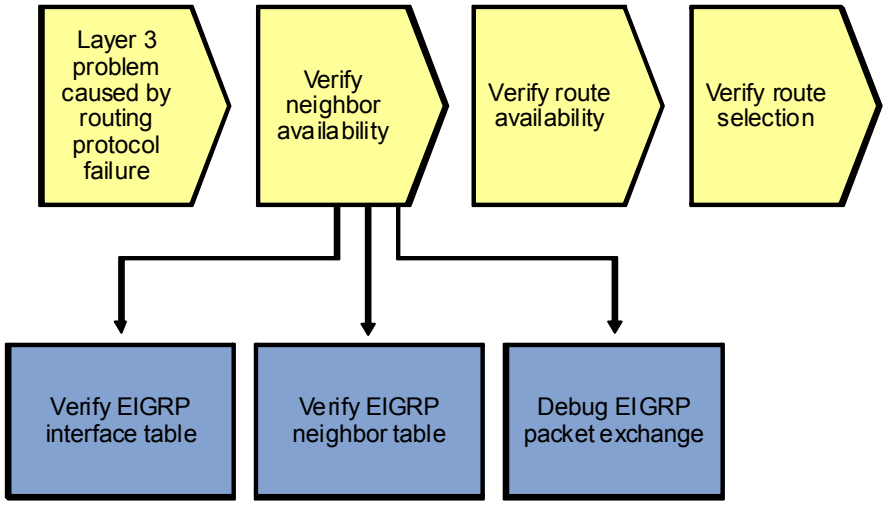
- Discover neighbors and establish a neighbor relationship.
- Exchange routing information with neighbors and store the received information in protocol specific data structures.
- Select the best route from the available routes and install it in the routing table.

Errors during any of these stages can cause routing information to be missing or incorrect routing information to be installed in the routing table.

The exact processes that take place, the data structures that are used, and the commands to gather information about these processes and data structures are protocol-specific, but the generic troubleshooting principles are similar for all routing protocols.

The order to perform the different stages is not important as long as a structured approach is used.

Sample EIGRP Troubleshooting Flow



EIGRP discovers and maintains neighbor relationships by using hello packets. Neighbors that are discovered are registered in the EIGRP neighbor table and remain in the neighbor table as long as hello packets are received. A neighbor is removed from the table when its hold time expires or when the interface on which the neighbor is registered goes down. The default EIGRP hello timer is 5 seconds for these interfaces:

- High-speed multipoint interfaces, such as Ethernet interfaces
- Point-to-point interfaces, such as the following:
  - Serial interfaces running PPP or High-Level Data Link Control (HDLC)
  - Point-to-point Frame Relay subinterfaces
  - Point-to-point ATM subinterfaces

The default hold time for these interfaces is 15 seconds. Each router advertises hello and hold timers that it uses in its hellos. Although it is recommended that the timers are changed in a consistent manner on all routers if they need to be tuned, they do not need to match between two routers to allow them to become neighbors.

Verify the EIGRP Interfaces

```
R1#show ip eigrp interfaces
IP-EIGRP interfaces for process 1

                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se0/0/0            1        0/0        19       0/15          99           0
Fa0/1              1        0/0         8       0/1           50           0
```

Neighbors can only be discovered on an interface that is operational and has been activated for EIGRP processing. An interface is activated for EIGRP packet processing if the IP address of the interface is covered by one of the network statements in the **router eigrp** configuration and the interface is not configured as a passive interface. Use the **show ip eigrp interfaces** command to display the EIGRP interfaces. An interface does not need to be operational to be listed in the output. The operational status of the interface must be verified separately using the **show interfaces**, **show interface status,** or **show ip interfaces brief** command.

If an interface is not listed in the output of the **show ip eigrp interfaces** command as expected, verify the **network** and **passive-interface** commands under the **router eigrp** configuration.

Verify the EIGRP Neighbor Table

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   10.1.2.1                Fa0/1             13 04:50:36    8   200  0  12
1   10.1.1.2                Se0/0/0           10 04:07:52   19   200  0  36
```

To verify that all expected neighbor relationships are operational, display the EIGRP neighbor table using the **show ip eigrp neighbors** command.

For troubleshooting purposes, the two most relevant columns in this output are Hold, which lists the number of seconds before a neighbor expires from the table, and Uptime, which lists how long this neighbor has been operational since it was last discovered. These two items can give you a good indication of the stability of the neighbor relationship. The uptime tells you for how long the neighbor relationship has been successfully maintained, while displaying the hold time several times in a row can tell you if hellos are being received in a timely fashion. Based on the default 5 second hello and 15 second hold time, the value in this column should be between 15 and 10 seconds, because it counts down and is reset to the hold time whenever a hello is received from the neighbor.

If the uptime of a neighbor is shorter than expected, verify the console or syslog logs for interface-related events or EIGRP neighbor-related events, such as the following (these are default message – not the result of debug):

```
Nov 2 06:25:01 EST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
Nov 2 06:25:02 EST: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to
down
Nov 2 06:25:02 EST: %DUAL-5-NBRCHANGE: EIGRP-IPv4:(1) 1: Neighbor 10.1.2.1
(FastEthernet0/1) is down: interface down
Nov 2 06:25:14 EST: %DUAL-5-NBRCHANGE: EIGRP-IPv4:(1) 1: Neighbor 10.1.2.1
(FastEthernet0/1) is up: new adjacency
Nov 2 06:25:16 EST: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Nov 2 06:25:17 EST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
```


Specifically, the %DUAL-5-NBRCHANGE messages are very useful in troubleshooting because they indicate why the neighbor was lost. In this case, it was caused by the interface going down.

Debug EIGRP Packet Exchange

If an expected neighbor is not listed in the neighbor table on a specific interface, and you have confirmed that the interface is operational and is listed in the interface table, use the **debug eigrp packets** command to display the transmission and reception of EIGRP packets in real time. This command can potentially generate a large amount of output, so be cautious about using it.

You can limit the output by specifying the packet type (update, request, query, reply, hello, ipxsap, probe, ack, stub, siaquery, or siareply). You can also add other conditions using the **debug ip eigrp *as-number*** command, such as limiting the output to a specific neighbor or network.

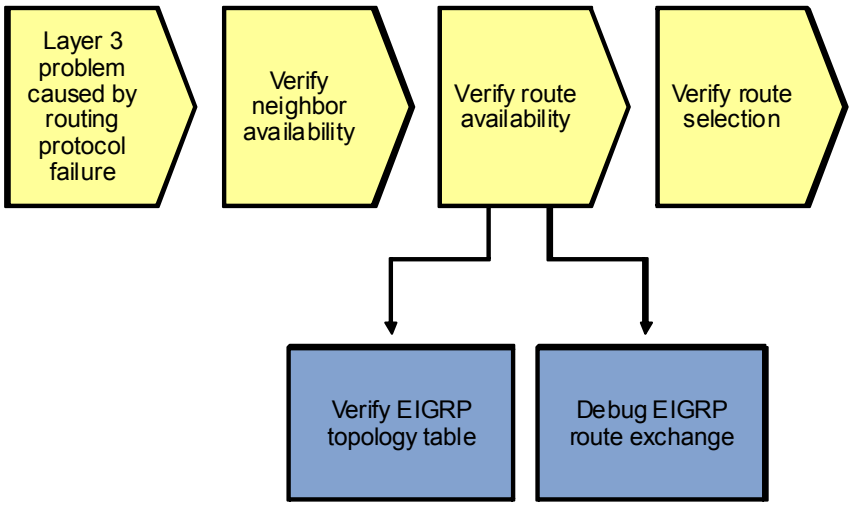
To further reduce the impact of the command, disable logging to the console and log to buffers in the router instead. You can then display the contents of the log buffer using the **show logging** command. The following example shows you how to use this technique:

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no logging console
R1(config)#logging buffered 16384
R1(config)#^Z

R1#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
SIAREPLY)

R1#debug ip eigrp 1 neighbor 10.1.2.1
IP Neighbor target enabled on AS 1 for 10.1.2.1
IP-EIGRP Neighbor Target Events debugging is on

R1#clear logging
Clear logging buffer [confirm]

R1#show logging
Syslog logging: enabled (1 messages dropped, 108 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 13924 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled

No active filter modules.

    Trap logging: level informational, 242 message lines logged
        Logging to 10.1.50.1(global) (udp port 514, audit disabled,  link up), 242
message lines logged, xml disabled,
               filtering disabled

Log Buffer (16384 bytes):

Nov 2 07:40:38.177 PDT: EIGRP: Received HELLO on FastEthernet0/1 nbr 10.1.2.1
```



```
Nov 2 07:40:38.177 PDT:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
un/rely 0/0
Nov 2 07:40:42.517 PDT: EIGRP: Received HELLO on FastEthernet0/1 nbr 10.1.2.1
Nov 2 07:40:42.517 PDT:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
un/rely 0/0
Nov 2 07:40:47.237 PDT: EIGRP: Received HELLO on FastEthernet0/1 nbr 10.1.2.1
Nov 2 07:40:47.237 PDT:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
un/rely 0/0
```

Sample EIGRP Troubleshooting Flow



After you have verified that neighbor relationships have been established as expected, verify that the route for the destination network that you are troubleshooting has been received correctly from all appropriate neighbors. EIGRP stores all routes that it receives from its neighbors in its topology table and then selects the best route from these routes to be installed in the routing table.

By investigating the available routes to the destination network in the topology table, you can see if all options that you expected were learned and if they have the correct associated metrics.

If routes are missing from the topology table, you might need to debug the EIGRP route exchange process to see if they were not received or if they were not entered into the topology table.

Verify the EIGRP Topology Table

```
R2#show ip eigrp topology 10.1.50.0 255.255.255.0
IP-EIGRP (AS 1): Topology entry for 10.1.50.0/24
  State is Passive, Query origin flag is 1, 2 Successor(s), FD is 2172672
  Routing Descriptor Blocks:
  10.1.1.1 (Serial0/0/0), from 10.1.1.1, Send flag is 0x0
      Composite metric is (2172672/28416), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 20110 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
```

```
      Hop count is 2
10.1.1.5 (Serial0/0/1), from 10.1.1.5, Send flag is 0x0
    Composite metric is (2172672/28416), Route is Internal
    Vector metric:
      Minimum bandwidth is 1544 Kbit
      Total delay is 20110 microseconds
      Reliability is 255/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 2
```

The EIGRP topology table contains all routes that were received from all neighbors.

For each particular prefix, there might be the following three types of entries:

- **Successors** – These are the entries selected from the topology table as the best routes and installed in the routing table. For a router to be a successor, it must provide the lowest total metric (its advertised distance plus the metric of the link towards it) among all the routes in the topology table for that prefix. Also, the advertised distance to the prefix by that router must be strictly lower than the feasible distance (FD). Secondly, it will only be marked as a successor if it was actually installed in the routing table. If a competing route for that prefix, such as a static route, was installed in the routing table instead because it had a better administrative distance, the EIGRP route will not be marked as a successor.
- **Feasible successors** – These routers have a metric that is higher than the current lowest total metric for the prefix but still meet the feasibility condition. The feasibility condition is met if the advertised distance of the route is lower than the FD. This means that the route is considered a backup route and can be used immediately if the best route is lost, without needing to confirm its feasibility as a backup route through a query and reply process.
- **Possible successors** – These routers do not meet the feasibility condition. They are potential backup routes, but if the best route is lost, a query and reply process is necessary to confirm that they are valid and loop-free.

As an example, the content of the EIGRP topology table for network 10.1.50.0/24 is listed below and comments are interspersed with the output to help interpret the entries.

```
R2#show ip eigrp topology 10.1.50.0 255.255.255.0
IP-EIGRP (AS 1): Topology entry for 10.1.50.0/24
  State is Passive, Query origin flag is 1, 2 Successor(s), FD is 2172672
```

There are two successors for this prefix, and the FD is 2172672. This entry is the first successor, because its distance of 2172672 (the first number between the parentheses) towards the 10.1.50.0/24 network through 10.1.1.5 is also equal to the FD of 2172672.

```
Routing Descriptor Blocks:
  10.1.1.1 (Serial0/0/0), from 10.1.1.1, Send flag is 0x0
      Composite metric is (2172672/28416), Route is Internal
      Vector metric:
              Minimum bandwidth is 1544 Kbit
              Total delay is 20110 microseconds
              Reliability is 255/255
              Load is 1/255
              Minimum MTU is 1500
              Hop count is 2
```

This entry is the second successor, because its distance of 28416 is also equal to the FD of 28416.

```
10.1.1.5 (Serial0/0/0), from 10.1.1.5, Send flag is 0x0
      Composite metric is (2172672/28416), Route is Internal
      Vector metric:
            Minimum bandwidth is 1544 Kbit
```



```
Total delay is 20110 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 2
```

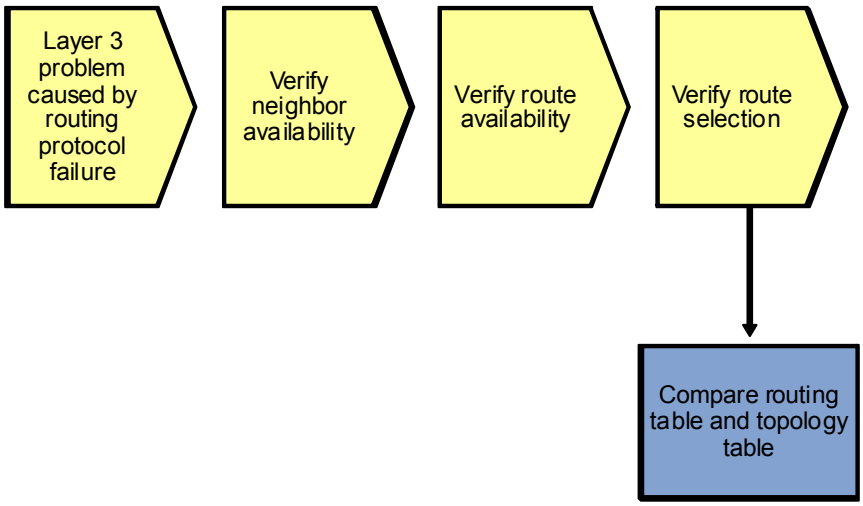
Verify the EIGRP Topology Table

```
R2#debug ip eigrp
IP-EIGRP Route Events debugging is on

R2#debug ip eigrp 1 neighbor 10.1.1.1
IP Neighbor target enabled on AS 1 for 10.1.1.1
IP-EIGRP Neighbor Target Events debugging is on

R2#clear ip eigrp neighbors 10.1.1.1
R2#
Nov  2 17:18:50.945: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.2 (Serial
0/0/0) is down: Interface Goodbye received
Nov  2 17:18:55.085: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.2 (Serial
0/0/0) is up: new adjacency
```

If you find expected route entries to be missing from the topology table, consider using the **debug ip eigrp** command to display the processing of routing events by the router. However, this command can produce a large number of messages and, as a result, has a high risk of disrupting the router's operation. Do not use this command unless guided by the Cisco TAC or in a nonoperational network, such as a lab network that you have built to reproduce a problem.

Like the **debug eigrp packets** command, you can limit the impact of this command by logging to buffers instead of the console and by limiting the output to specific neighbors or routes. Even then, extreme care should be taken.

Sample EIGRP Troubleshooting Flow



If you find that an EIGRP route for a specific destination network is available in the topology table, but a different route is present in the routing table, compare the value of the administrative distance of the route in the routing table to the value of the EIGRP route (which is 90 for internal routes and 170 for external routes, by default). If the distance of the EIGRP route is higher than the distance of the competing route, it will not be installed in the routing table.