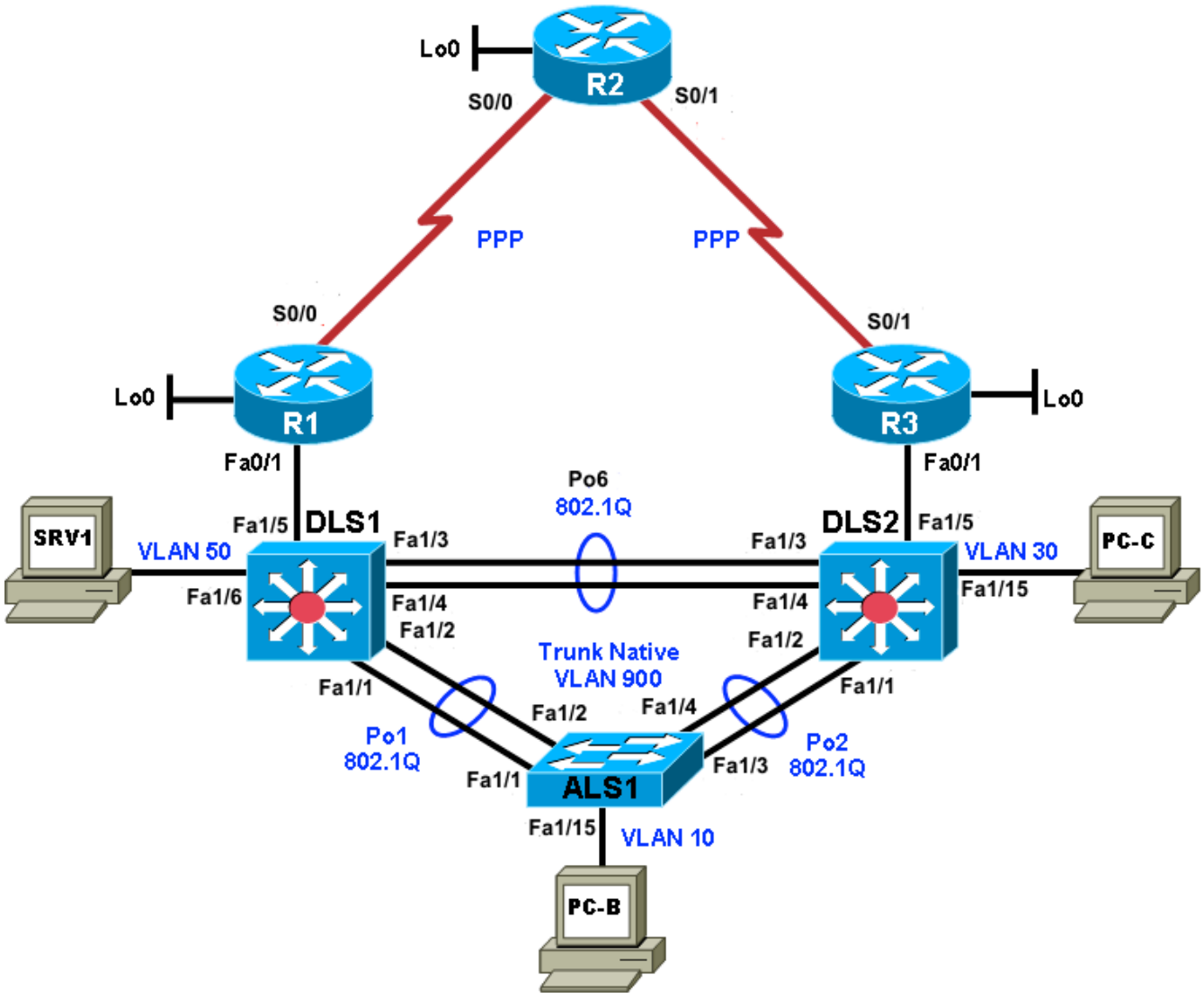
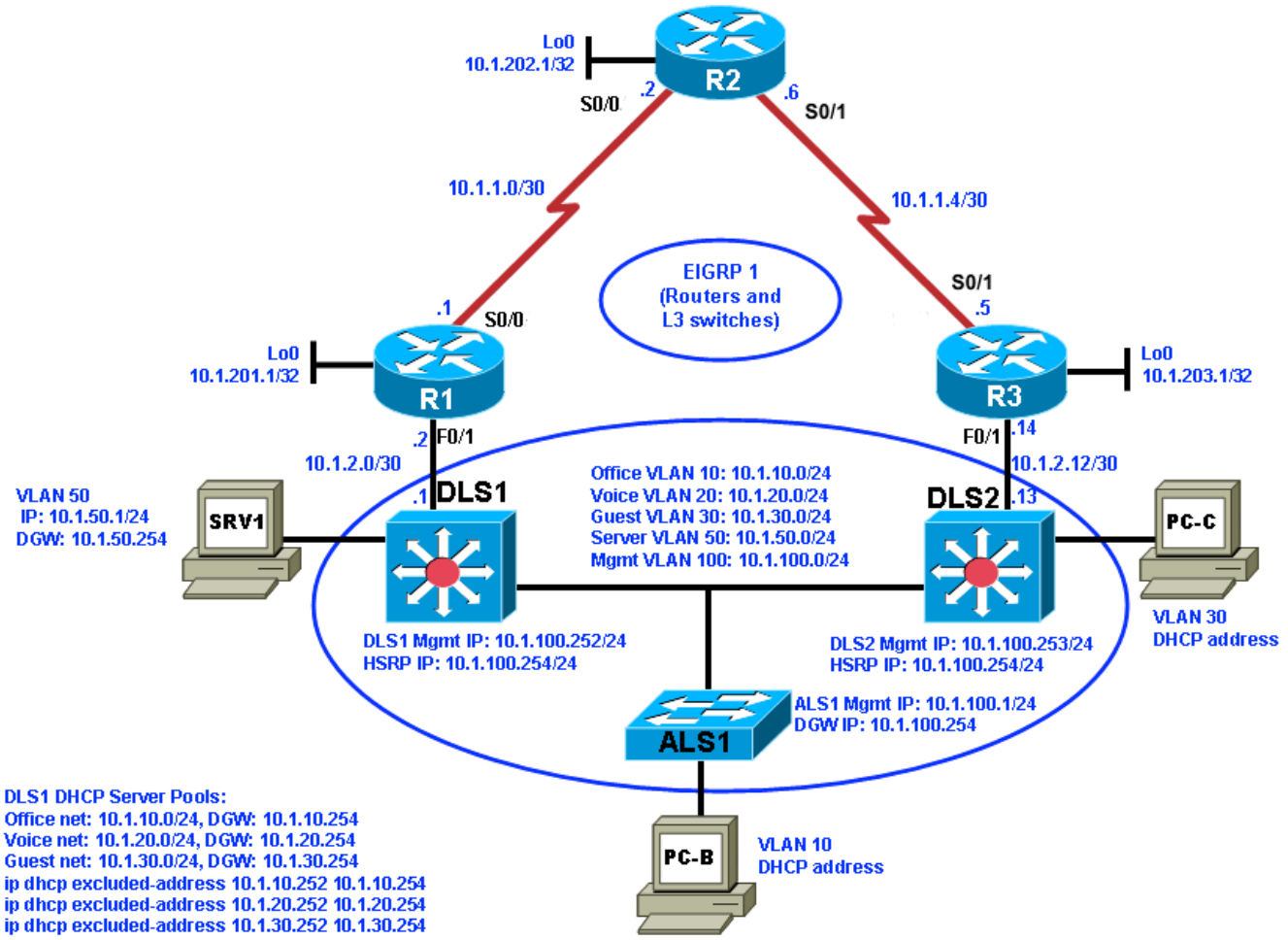
Lab 5-2, OSPF and Route Redistribution

Physical Topology (Baseline)



Logical Topology (Baseline)



Objectives

- Load the trouble ticket device configuration files for each trouble ticket.
- Diagnose and resolve problems related to the OSPF routing protocol.
- Diagnose and resolve problems related to route redistribution.
- Document troubleshooting progress, configuration changes, and problem resolution.

Background

In this lab, you troubleshoot various problems related to the Open Shortest Path First (OSPF) routing protocol and route redistribution between routing protocols. 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.

Migrating from EIGRP to OSPF

Your company has decided to migrate from using Enhanced Interior Gateway Protocol (EIGRP) to OSPF as the routing protocol. This migration will be executed in two phases.

The engineering team planned and designed the migration, but the support team must support the new network, so they are involved in migrating the branch during Phase 2.

Phase 1—The headquarters central site campus is migrated to OSPF as well as one of the branch offices (simulated by Lo0 on R3). EIGRP is still used on the WAN toward the R2 branch office. On router R1, redistribution is configured between OSPF and EIGRP to ensure connectivity between headquarters and the branch office connected to R2.

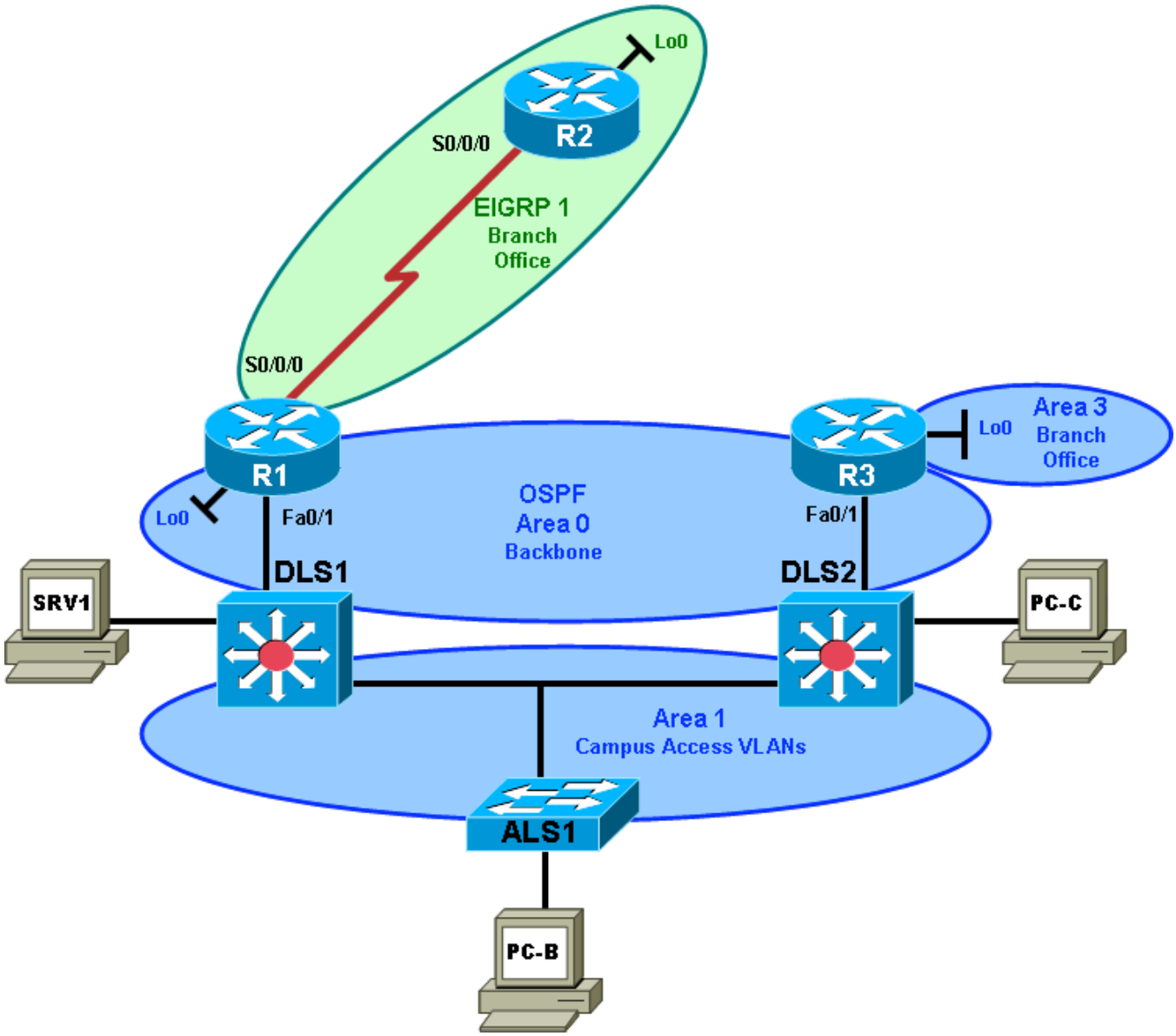
Phase 2—The R2 branch office (simulated by Lo0 on R2) is converted from EIGRP to OSPF, and all branch offices are migrated so that OSPF is used in the entire network. Each branch site is in a separate area that is configured as totally stubby.

Today is Saturday, and the engineering team has been busy implementing OSPF and removing EIGRP at the headquarters site. Although you have not taken part in the actual implementation, some of the senior engineers in the support team are on standby to assist during the verification and troubleshooting phase. Together with the engineering team, you will have to make the decision on Sunday to either accept the implementation or, if major issues are uncovered that would threaten the stability of the network, roll back to the original configurations.

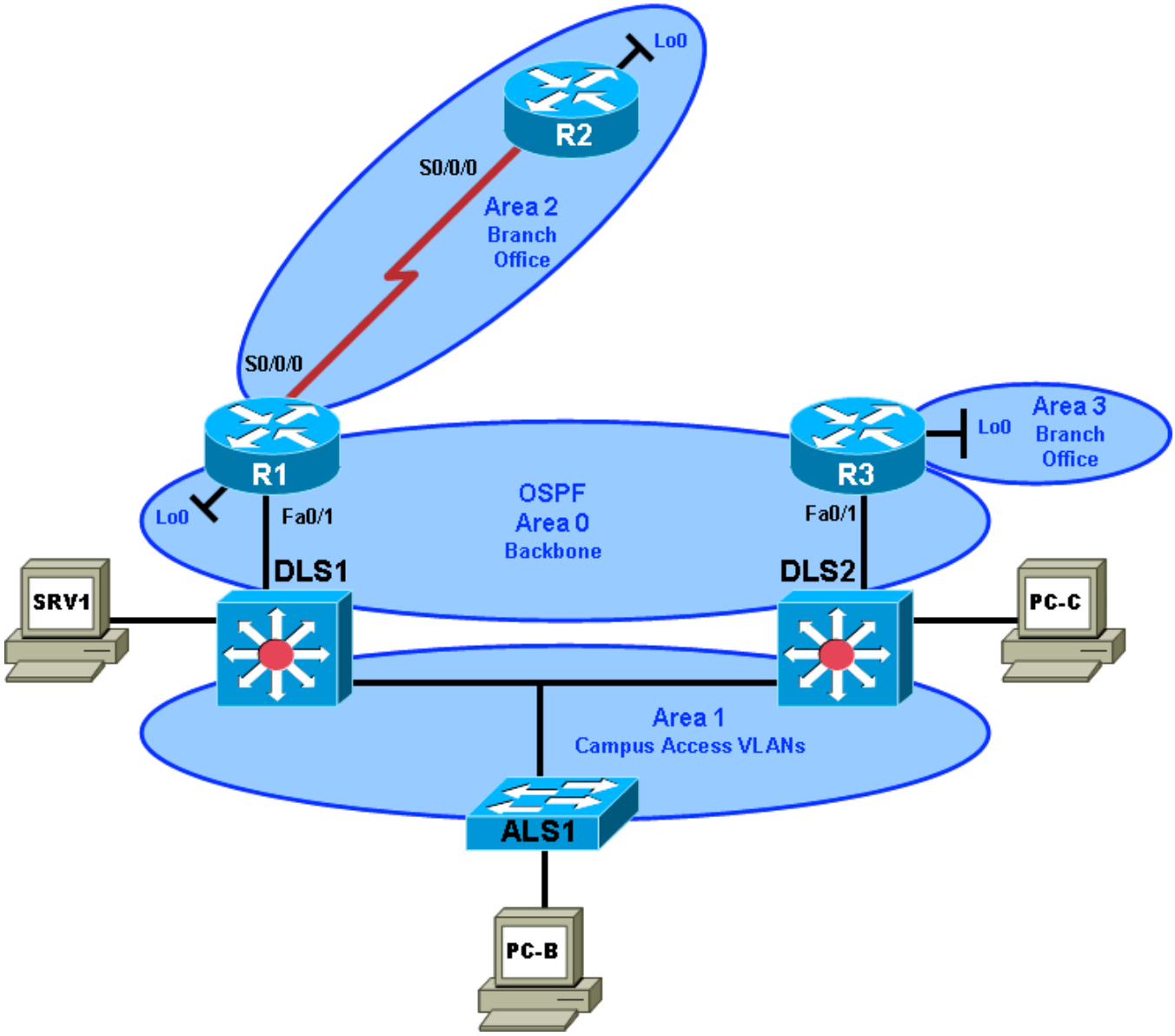
OSPF Network Design

Phases 1 and 2 of the OSPF design are depicted in the following figures. Backbone area 0 contains the FastEthernet interfaces on core Layer 3 switches DLS1 and DLS2 as well as those on routers R1 and R3. Area 0 also includes VLAN 200 and the corresponding SVI, which have been added to these two switches so that they can form an OSPF neighbor relationship and exchange routes. The headquarters campus access VLANs 10, 20, 30, and 50 and management VLAN 100 are in OSPF area 1. The R2 stub network is in area 2, and the R3 stub network is in area 3.

Phase 1 OSPF Network Design



Phase 2 OSPF Network Design



Test Plan

To test the branch connectivity using redistribution between EIGRP and OSPF and the eventual conversion to only OSPF, branch routers R2 and R3 have been specifically prepared for both of these scenarios. Router R2 functions as the default gateway for the R2 LAN, while router R3 is the default gateway for the R3 LAN. Router R2 runs EIGRP as usual. This allows testing the redistribution of EIGRP from the R2 branch office LAN (simulated by R2 Lo0) to OSPF area 0 and redistribution of OSPF into EIGRP using router R1 as an Autonomous System Border Router (ASBR). Router R3 is configured to run OSPF as an Area Border Router (ABR) between area 0 and area 3. The R3 branch office client is simulated by R3 Lo0).

At the end of Phase 1, when the network is fully converged, all OSPF routers should have EIGRP routes in their routing tables and EIGRP router R2 should have all OSPF routes in its routing table.

After the completion of Phase 2, all routers except R2 should have OSPF routes. Router R2 is totally stubby and should only have a default route to R1.

Note: Trouble ticket TT-A is related to the verification and acceptance of Phase 1 of the OSPF migration. Trouble tickets TT-B and C are related to the verification and acceptance of Phase 2 of the OSPF migration. Any interfaces that have been shut down on routers R2 and R3 should remain shut down for the duration of this lab exercise.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 52-A (2 Issues)

Step 1: Review trouble ticket Lab 52-A.

After the completion of Phase 1—implementation of OSPF in the headquarters portion of the network and the redistribution between EIGRP and OSPF—the connectivity from the office LAN on the R2 branch router to server SRV1 at headquarters is tested. A ping from the R2 LAN client (sourced by Lo0 on R2) to server SRV1 fails.

Your task is to diagnose this problem and, if possible, resolve it. Connectivity from the R2 LAN to server SRV1 is mandatory to consider this phase of the migration successful.

Step 2: Load the device trouble ticket configuration files for 52-A.

a. On each device issue the command **52-A**

b. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-52A**

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.

_____

_____

_____

_____

_____

_____

Task 2: Trouble Ticket Lab 52-B (2 Issues)

Step 1: Review trouble ticket Lab 52-B.

Phase 2 has been completed and all routers have been converted to OSPF. The connectivity from a branch office client on the R2 LAN (simulated by R2 Lo0) to server SRV1 at the central site is tested. A ping from the client on the R2 LAN (using source interface Lo0) to server SRV1 fails. The connectivity problem is not limited to SRV1. An attempt to connect to other headquarters servers also fails. Your task is to diagnose this problem and, if possible, resolve it. Connectivity from the branch client to server SRV1 is mandatory for this phase of the migration to be considered successful.

Step 2: Load the device trouble ticket configuration files for 52-B.

a. On each device issue the command **52-B**

b. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-52B**

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.

_____

_____

_____

_____

Task 3: Trouble Ticket Lab 52-C (1 Issue)

Step 1: Review trouble ticket Lab 52-C.

After implementing OSPF, connectivity from the branch office on R3 (simulated by Lo0) to SRV1 is not working. A ping from PC-B to server SRV1 succeeds, but pings from R3 Lo0 to SRV1 fail.

Your task is to diagnose this problem and, if possible, resolve it. Connectivity from R3 branch office clients to server SRV1 is mandatory for this phase of the migration to be considered successful.

Step 2: Load the device trouble ticket configuration files for 41-A.

a. On each device issue the command **41-A**

b. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-41A**

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 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. Sample output is shown on the following pages.

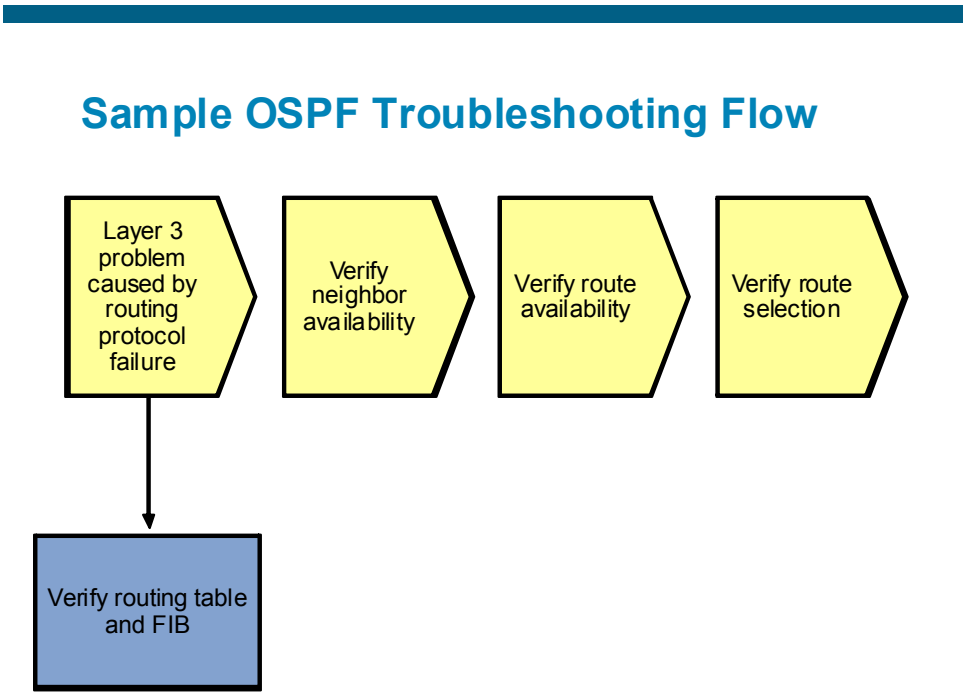
Command	Key Information Displayed
show ip route *ip-addr*	Displays the routing table information for a particular destination address.
show ip ospf interface *type/#* **show ip ospf interface brief**	Displays interfaces that are participating in the OSPF routing process. An interface does not need to be operational to be listed in the command output.
show ip ospf neighbor	Displays the OSPF neighbor table to verify that all expected neighbor relationships are operational.
show ip ospf database router *router-id*	Verifies whether the directly connected routers properly advertise the destination network. Use this command to display the router (type-1) for the connected routers.
show ip ospf database external *subnet*	Verifies the availability of a specific type-5 external link-state advertisement (LSA) in the OSPF database. The *subnet* option is the subnet IP address of the prefix in which you are interested.
show ip ospf database summary *subnet*	Verifies the availability of a specific target network in a different area. The *subnet* option is the subnet IP address of the prefix in which you are interested.
show ip ospf database asbr-summary *router-id*	Verifies if a type-4 summary autonomous system (AS) boundary LSA exists for the Autonomous System Boundary Router (ASBR) with the specified router ID.
show system mtu	Displays the switch or router Maximum Transmission

	Unit (MTU), normally 1500 bytes. Mismatches in MTU can cause neighbor relationships to fail.
debug ip ospf packet	Displays the headers of OSPF packets as they are received by the router. Transmitted packets are not displayed. Packets are only shown for interfaces that are enabled for OSPF.
debug ip ospf adj	Displays all the different stages of the OSPF adjacency building process. It also reveals mismatches in the basic parameters contained in the OSPF packet header, such as area ID mismatches, the source being on the wrong subnet, or authentication mismatches. It does not reveal other mismatches in hello parameters, such as hello timers, subnet masks, or flags.
debug ip ospf events	Displays the same information that is displayed by the **debug ip ospf adj** command. In addition, it displays the transmission and reception of hello packets and reports mismatches in the hello parameters.

Lab 5-2: Sample Troubleshooting Flows

Troubleshooting the OSPF Routing Protocol

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



The usual trigger to start investigating routing protocol operation is when you are troubleshooting IP connectivity to a particular destination and you find that 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:

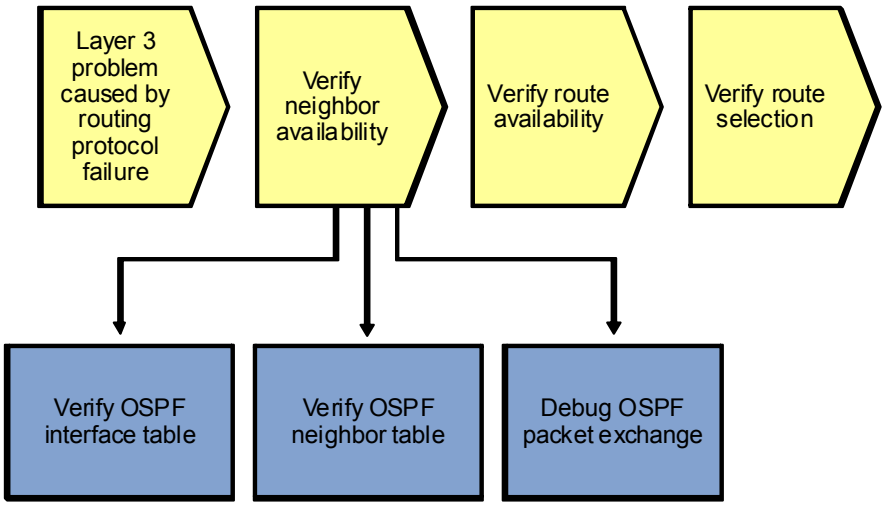
- Discovers neighbors and establishes a neighbor relationship.
- Exchanges routing information with neighbors and stores the received information in protocol-specific data structures.
- Selects the best route from the available routes and installs it in the routing table.

Errors during any of these stages can cause missing routing information or wrong routing information 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 of verification of the different process stages is not important as long as a structured approach is used.

Sample OSPF Troubleshooting Flow



OSPF establishes and maintains neighbor relationships by using hello packets. Neighbors from which a hello packet is received are entered in the neighbor table. Subsequently, OSPF goes through the process of establishing an adjacency by transitioning through several stages in which the link-state database of the router are synchronized with its neighbor. After the completion of the database synchronization, the neighbors are considered to be fully adjacent, and both link-state updates and user traffic can be passed between the neighbors. The neighbor remains registered in the neighbor table as long as hello packets are received regularly. A neighbor is removed from the neighbor table when its dead time expires or when the interface on which the neighbor is registered goes down. The default OSPF hello timer is 10 seconds for point-to-point interfaces, such as serial interfaces running PPP or High-Level Data Link Control (HDLC), point-to-point Frame Relay or ATM subinterfaces, and broadcast-type interfaces such as Ethernet. The default dead time for these interfaces is 40 seconds. Each router advertises its hello and hold times in its hello packets, and the values must match for two routers to become neighbors.

Verify OSPF Interfaces

```
R1#show ip ospf interface brief
Interface    PID   area            IP Address/Mask    Cost  State Nbrs F/C
Lo0          1     0               10.1.201.1/32      1     P2P   0/0
Fa0/1        1     0               10.1.2.2/30        1     DR    1/1
Se0/0/0      1     2               10.1.1.1/30        64    P2P   1/1
```

Neighbors can only be discovered on an interface that has been enabled for OSPF and has not been configured as a passive interface. An interface can be enabled for OSPF in two ways. One way is if the IP address of the interface is covered by one of the **network** statements configured under the **router ospf** process, which assigns it to an area. Alternatively, an explicit **ip ospf** *process-id* **area** *area-id* command is configured on the interface, which assigns it to an area. To display a list of OSPF-enabled interfaces, use the **show ip ospf interface brief** command. This list includes interfaces that are down, which are marked as DOWN, and interfaces that have been configured as passive. However, passive interfaces are not easily recognizable in the output.

To verify whether an interface is passive, use the **show ip ospf interface** *interface-id* command. Instead of a short list, this command displays comprehensive details of the OSPF parameters and the operational state for the specified interface. This command is also useful to verify timer values, such as the hello and dead timers, which could prevent a neighbor relationship from being established.

```
R1#show ip ospf interface fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
  Internet Address 10.1.2.2/30, area 0
  Process ID 1, Router ID 10.1.201.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.201.1, Interface address 10.1.2.2
  No backup designated router on this network
  Timer intervals configured, hello 10, dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

What does this mean from a troubleshooting standpoint?

If you find that an interface is not listed in the output of the **show ip ospf interface brief** command as expected, verify the **network** commands under the **router ospf** configuration.

If you find that an interface is listed but no neighbors are registered on the interface, verify that the interface was not marked as passive by issuing the **show ip ospf interface** *interface-id* command for that interface.

Verify the OSPF Neighbor Table

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           dead Time   Address         Interface
10.1.211.1        1   FULL/DR         00:00:31    10.1.2.1        FastEthernet0/1
10.1.202.1        0   FULL/  -        00:00:38    10.1.1.2        Serial0/0/0

DLS1>show ip ospf neighbor

Neighbor ID     Pri   State           dead Time   Address         Interface
```



```
10.1.212.1        1   FULL/DR      00:00:35    10.1.200.253  Vlan200
10.1.201.1        1   FULL/BDR     00:00:39    10.1.2.2      FastEthernet0/5
```

To verify that all expected neighbor relationships are operational, you can display the OSPF neighbor table using the **show ip ospf neighbor** command.

While two routers establish an adjacency and synchronize their link-state databases, they go through the following phases: Attempt (optional), Init, 2-Way, Exstart, Exchange, Loading, and Full. The expected state for a neighbor relationship is Full. The other states are transitory states, and a neighbor should not be stuck in any of those states for an extended period of time.

The only exception to this rule is a broadcast or nonbroadcast network with more than three routers. On these types of networks, a designated router (DR) and backup designated router (BDR) are elected, and all routers establish a full adjacency with the DR and BDR. Any two routers that are both not a DR or BDR (marked "DROTHER" in the **show** commands) do not transition any further than the two-way state.

In the example output, the device has two neighbors: neighbor 10.1.212.1, which is the DR, and neighbor 10.1.201.1, which is the BDR.

Debug OSPF Packet Exchange

```
DLS1#debug ip ospf packet
OSPF packet debugging is on
DLS1#
Nov  5 15:54:32.574: OSPF: rcv. v:2 t:1 l:48 rid:10.1.212.1
      aid:0.0.0.0 chk:8B98 aut:0 auk: from Vlan200
Nov  5 15:54:38.917: OSPF: rcv. v:2 t:1 l:48 rid:10.1.201.1
      aid:0.0.0.0 chk:2394 aut:0 auk: from FastEthernet0/5

R1#debug ip ospf packet
Nov  5 15:57:21.503: OSPF: rcv. v:2 t:1 l:48 rid:10.1.211.1
      aid:0.0.0.0 chk:2394 aut:0 auk: from FastEthernet0/1
Nov  5 15:57:22.443: OSPF: rcv. v:2 t:1 l:48 rid:10.1.202.1
      aid:0.0.0.2 chk:4497 aut:0 auk: from Serial0/0/0

In this highlighted sample output for R1, router ID 10.1.202.1 is in area 2
(aid:0.0.0.2) and the hello was received on interface Serial 0/0/0.
```

When an OSPF neighbor relationship is not properly established, you can use several **debug** commands to display events related to the establishment of neighbor relationships. The most elementary command is **debug ip ospf packet**, which displays the headers of OSPF packets as they are received by the router.

This command lists only received packets. Transmitted packets are not displayed. In addition, because interfaces that are not enabled for OSPF do not listen to the OSPF multicast addresses, packets are only shown for interfaces that are enabled for OSPF.

The following fields are the most relevant in the header description of these packets:

- Type (t): Lists the type of packet. Possible packet types are:
  - Type 1: Hello packets
  - Type 2: Database description packets
  - Type 3: Link-state request packets
  - Type 4: Link-state update packets
  - Type 5: Link-state acknowledgement packets
- Router ID (rid): Lists the ID of the sending router. This is usually not the same as the source address of the packet.

- Area ID (aid): The 32-bit area ID of the sending router is represented in dotted-decimal IP address format.
- Authentication (aut): Lists the authentication type. Possible types are:
  - Type 0: No (null) authentication
  - Type 1: Cleartext authentication
  - Type 2: Message Digest 5 (MD5) authentication
- Interface (from): Lists the interface on which the packet was received.

Note: Only successfully received and accepted packets are listed in the output of the **debug ip ospf packet** command. If there is a mismatch between essential parameters in the header, such as the area ID, authentication type, or authentication data between this router and the neighbor, the packets from that neighbor are silently discarded and not listed in the output of the debug.

The usefulness of this command for troubleshooting is limited because it does not display sent packets, packets received on an interface that is not enabled for OSPF, or packets that carry mismatched header information. However, because of the relatively limited amount of generated output, it can be used to confirm the reception of correct hellos from a neighbor.

Debug OSPF Adjacencies

In the following debug outputs, DLS1 interface Fa0/5 (link to R1) is shutdown and the OSPF adjacency terminates. When the DLS1 Fa0/5 interface is reactivated, an election occurs, DLS1 becomes the DR again and builds LSAs to send to R1. DLS1 and R1 establish a neighbor relationship and exchange OSPF database information.

```
DLS1#debug ip ospf adj
OSPF adjacency events debugging is on

DLS1(config)#interface fa0/5
DLS1(config-if)#shut

Nov  5 16:04:10.619: OSPF: Interface FastEthernet0/5 going Down
Nov  5 16:04:10.619: OSPF: 10.1.211.1 address 10.1.2.1 on FastEthernet0/5 is dea
d, state DOWN
Nov  5 16:04:10.619: OSPF: Neighbor change Event on interface FastEthernet0/5
Nov  5 16:04:10.619: OSPF: DR/BDR election on FastEthernet0/5
Nov  5 16:04:10.619: OSPF: Elect BDR 10.1.201.1
Nov  5 16:04:10.619: OSPF: Elect DR 10.1.201.1
Nov  5 16:04:10.619: OSPF: Elect BDR 10.1.201.1
Nov  5 16:04:10.619: OSPF: Elect DR 10.1.201.1
Nov  5 16:04:10.619
DLS1(config-if)#:         DR: 10.1.201.1 (Id)   BDR: 10.1.201.1 (Id)
Nov  5 16:04:10.619: OSPF: Flush network LSA immediately
Nov  5 16:04:10.619: OSPF: Remember old DR 10.1.211.1 (id)
Nov  5 16:04:10.619: OSPF: 10.1.201.1 address 10.1.2.2 on FastEthernet0/5 is dea
d, state DOWN
Nov  5 16:04:10.619: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.201.1 on FastEthernet0/
5 from FULL to DOWN, Neighbor Down: Interface down or detached
Nov  5 16:04:10.619: OSPF: Neighbor change Event on interface FastEthernet0/5
Nov  5 16:04:10.619: OSPF: DR/BDR election on FastEthernet0/5
Nov  5 16:04:10.619: OSPF: Elect BDR 0.0.0.0
Nov  5 16:04:10.619: OSPF: Elect DR 0.0.0.0
Nov  5 16:04:10.619:         DR: none    BDR: none
Nov  5 16:04:10.619: OSPF: Remember old DR 10.1.201.1 (id)
Nov  5 16:04:10.619: OSPF: [change notify] will poll [cnt 11] interface status f
or FastEthernet0/5
```



```
Nov  5 16:04:11.122: OSPF: We are not DR to build Net Lsa for interface FastEthe
rnet0/5
Nov  5 16:04:11.122: OSPF: Build network LSA for FastEthernet0/5, router ID 10.1
.211.1
Nov  5 16:04:11.122: OSPF: Build router LSA for area 0, router ID 10.1.211.1, se
q 0x80000012, process 1
Nov  5 16:04:12.599: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state t
o administratively down
Nov  5 16:04:13.606: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
t0/5, changed state to down
Nov  5 16:04:20.628: OSPF: will poll [count 10] interface status for FastEtherne
t0/5
Nov  5 16:04:30.636: OSPF: will poll [count 9] interface status for FastEthernet
0/5
Nov  5 16:04:40.821: OSPF: will poll [count 8] interface status for FastEthernet
0/5
Nov  5 16:04:50.830: OSPF: will poll [count 7] interface status for FastEthernet
0/5
Nov  5 16:05:00.838: OSPF: will poll [count 6] interface status for FastEthernet
0/5
Nov  5 16:05:10.839: OSPF: will poll [count 5] interface status for FastEthernet
0/5
Nov  5 16:05:20.847: OSPF: will poll [count 4] interface status for FastEthernet
0/5
Nov  5 16:05:30.856: OSPF: will poll [count 3] interface status for FastEthernet
0/5
Nov  5 16:05:40.865: OSPF: will poll [count 2] interface status for FastEthernet
0/5
Nov  5 16:05:50.865: OSPF: will poll [count 1] interface status for FastEthernet
0/5

DLS1(config)#interface fa0/5
DLS1(config-if)#no shut

Nov  5 16:05:59.800: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to
 up
Nov  5 16:05:59.800: OSPF: Interface FastEthernet0/5 going Up
Nov  5 16:05:59.800: OSPF: [change notify] will poll [cnt 11] interface status f
or FastEthernet0/5
Nov  5 16:06:00.303: OSPF: Build router LSA for area 0, router ID 10.1.211.1, se
q 0x80000013, process 1
Nov  5 16:06:00.807: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
t0/5, changed state to up
Nov  5 16:06:09.800: OSPF: will poll [count 10] interface status for FastEtherne
t0/5
Nov  5 16:06:09.800: OSPF: 2 Way Communication to 10.1.201.1 on FastEthernet0/5,
 state 2WAY
Nov  5 16:06:19.809: OSPF: will poll [count 9] interface status for FastEthernet
0/5
Nov  5 16:06:29.809: OSPF: will poll [count 8] interface status for FastEthernet
0/5
Nov  5 16:06:39.809: OSPF: end of Wait on interface FastEthernet0/5
Nov  5 16:06:39.809: OSPF: DR/BDR election on FastEthernet0/5
Nov  5 16:06:39.809: OSPF: Elect BDR 10.1.211.1
Nov  5 16:06:39.809: OSPF: Elect DR 10.1.211.1
Nov  5 16:06:39.809: OSPF: Elect BDR 10.1.201.1
Nov  5 16:06:39.809: OSPF: Elect DR 10.1.211.1
Nov  5 16:06:39.809:         DR: 10.1.211.1 (Id)   BDR: 10.1.201.1 (Id)
```

```
Nov  5 16:06:39.809: OSPF: Send DBD to 10.1.201.1 on FastEthernet0/5 seq 0x192E
opt 0x52 flag 0x7 len 32
Nov  5 16:06:39.818: OSPF: will poll [count 7] interface status for FastEthernet
0/5
Nov  5 16:06:40.313: OSPF: No full nbrs to build Net Lsa for interface FastEther
net0/5
Nov  5 16:06:42.209: OSPF: Rcv DBD from 10.1.201.1 on FastEthernet0/5 seq 0x8AC
opt 0x52 flag 0x7 len 32  mtu 1500 state EXSTART
Nov  5 16:06:42.209: OSPF: First DBD and we are not SLAVE
Nov  5 16:06:44.818: OSPF: Send DBD to 10.1.201.1 on FastEthernet0/5 seq 0x192E
opt 0x52 flag 0x7 len 32
Nov  5 16:06:44.818: OSPF: Retransmitting DBD to 10.1.201.1 on FastEthernet0/5 [
1]
Nov  5 16:06:44.818: OSPF: Rcv DBD from 10.1.201.1 on FastEthernet0/5 seq 0x192E
 opt 0x52 flag 0x2 len 432  mtu 1500 state EXSTART
Nov  5 16:06:44.818: OSPF: NBR Negotiation Done. We are the MASTER
Nov  5 16:06:44.818: OSPF: Send DBD to 10.1.201.1 on FastEthernet0/5 seq 0x192F
opt 0x52 flag 0x3 len 412
Nov  5 16:06:44.818: OSPF: Rcv DBD from 10.1.201.1 on FastEthernet0/5 seq 0x192F
 opt 0x52 flag 0x0 len 32  mtu 1500 state EXCHANGE
Nov  5 16:06:44.818: OSPF: Send DBD to 10.1.201.1 on FastEthernet0/5 seq 0x1930
opt 0x52 flag 0x1 len 32
Nov  5 16:06:44.818: OSPF: Send LS REQ to 10.1.201.1 length 24 LSA count 2
Nov  5 16:06:44.826: OSPF: Rcv LS REQ from 10.1.201.1 on FastEthernet0/5 length
36 LSA count 1
Nov  5 16:06:44.826: OSPF: Send UPD to 10.1.2.2 on FastEthernet0/5 length 64 LSA
 count 1
Nov  5 16:06:44.826: OSPF: Rcv DBD from 10.1.201.1 on FastEthernet0/5 seq 0x1930
 opt 0x52 flag 0x0 len 32  mtu 1500 state EXCHANGE
Nov  5 16:06:44.826: OSPF: Exchange Done with 10.1.201.1 on FastEthernet0/5
Nov  5 16:06:44.826: OSPF: Rcv LS UPD from 10.1.201.1 on FastEthernet0/5 length
108 LSA count 2
Nov  5 16:06:44.826: OSPF: No full nbrs to build Net Lsa for interface FastEther
net0/5
Nov  5 16:06:44.826: OSPF: Build network LSA for FastEthernet0/5, router ID 10.1
.211.1
Nov  5 16:06:44.826: OSPF: Synchronized with 10.1.201.1 on FastEthernet0/5, stat
e FULL
Nov  5 16:06:44.826: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.201.1 on FastEthernet0/
5 from LOADING to FULL, Loading Done
```

The **debug ip ospf adj** command is useful for troubleshooting OSPF neighbor-related events. It displays the different stages of the OSPF adjacency-building process as two neighbors transition from the init state to the full state. This command can be helpful in diagnosing problems in which a neighbor relationship is stuck in a particular stage of the adjacency-building process.

This command also reveals mismatches in the basic parameters contained in the OSPF packet header, such as area ID mismatches, the source being on the wrong subnet, or authentication mismatches. It does not, however, reveal other mismatches in hello parameters, such as hello timers, subnet masks, or flags.

Debug OSPF Events

```
DLS2#debug ip ospf events

*Nov  5 03:03:11.043: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet0/5 fr
om 10.1.2.13
DLS2#
*Nov  5 03:03:13.551: OSPF: Send hello to 224.0.0.5 area 0 on Vlan200 from 10.1.
200.253
```

```
*Nov  5 03:03:13.845: OSPF: Rcv hello from 10.1.211.1 area 0 from Vlan200 10.1.2
00.252
*Nov  5 03:03:13.845: OSPF: End of hello processing
DLS2#
*Nov  5 03:03:16.051: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet0/5 fr
om 10.1.2.13
*Nov  5 03:03:16.286: OSPF: Rcv hello from 10.1.203.1 area 0 from FastEthernet0/
5 10.1.2.14
*Nov  5 03:03:16.286: OSPF: Mismatched hello parameters from 10.1.2.14
*Nov  5 03:03:16.286: OSPF: dead R 40 C 15, hello R 10 C 5  Mask R 255.255.255.2
52 C 255.255.255.252
DLS2#

DLS2#undebug all
All possible debugging has been turned off
DLS2#
*Nov  5 03:03:28: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.203.1 on FastEthernet0/5 f
rom FULL to DOWN, Neighbor Down: dead timer expired
```

A third **debug** command that can be useful in troubleshooting the establishment of OSPF neighbor relationships is **debug ip ospf events**. This command displays the same information that is displayed by the **debug ip ospf adj** command, but it also displays the transmission and reception of hello packets and reports mismatches in the hello parameters.

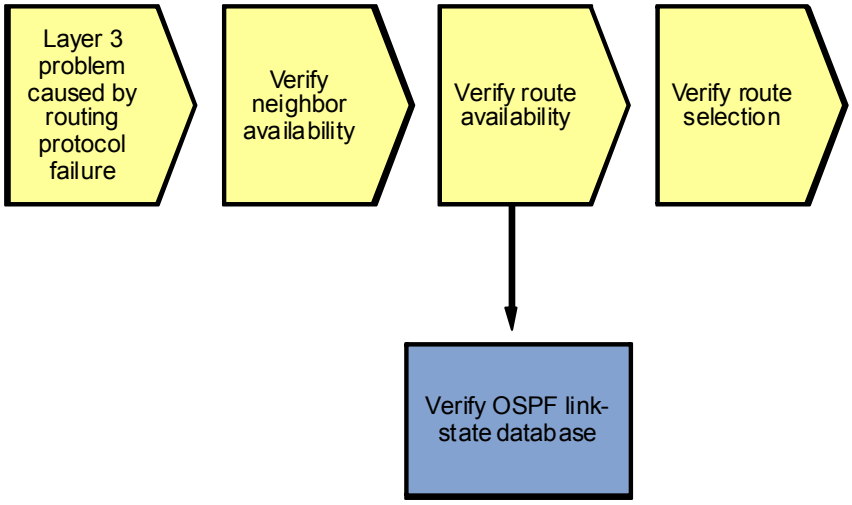
Confirming the transmission of hello packets by using this command can be useful because the **debug ip ospf packet** or **debug ip ospf adj** commands do not display the transmission of hello packets.

You can also use this command to display the reception of invalid hello packets. If there is a mismatch between the neighbors in the hello parameters that prevents the neighbor relationship from forming, this command displays the type of parameter mismatch and the value of the mismatched parameters. It displays mismatches for the following parameters:

- Hello and dead timers
- Area ID
- Subnet and subnet mask
- Authentication type and authentication data
- Flags that signify the area type, such as stub or not-so-stubby area (NSSA)

Because this command displays more events, it is often better to first enable the **debug ip ospf adj** command and only use the **debug ip ospf event** command if you did not get the information you need.

Sample OSPF Troubleshooting Flow



After you have verified that neighbor relationships have been established as expected, verify that the network topology information for the destination network that you are troubleshooting has been received correctly and entered into the OSPF link-state database.

The presence or absence of specific topology information in the OSPF link-state database can help isolate the source of the problem.

Verify the OSPF Link-State Database for Intra-Area Routes

```
DLS2#show ip ospf database router 10.1.212.1

            OSPF Router with ID (10.1.212.1) (Process ID 1)

                Router Link States (area 0)

  LS age: 60
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 10.1.212.1
  Advertising Router: 10.1.212.1
  LS Seq Number: 80000012
  Checksum: 0x592C
  Length: 60
  area Border Router
  Number of Links: 3

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 10.1.212.1
     (Link Data) Network Mask: 255.255.255.255
      Number of TOS metrics: 0
       TOS 0 Metrics: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 10.1.2.13
     (Link Data) Router Interface address: 10.1.2.13
```

```
      Number of TOS metrics: 0
       TOS 0 Metrics: 1
```

To decide which information to look for in the link-state database, you first need to discern in which type of route you are interested. If the destination network that you are troubleshooting is in the same area as the router from which you are troubleshooting, you know that the path to this destination network was derived from the type-1 and type-2 LSAs in the database of that area. To begin with, you can verify whether the directly connected routers properly advertise the destination network. To do this, display the router (type-1) for the connected routers by issuing the **show ip ospf database router** *router-id* command for these routers. To troubleshoot OSPF effectively, it is necessary to know the router IDs of all routers in your network, because these are used to identify a router in many of the OSPF **show** commands.

As part of the type-1 router LSA for a specific router, all subnets corresponding to a point-to-point link, loopback interface, or nontransit broadcast network (Ethernet) are listed as stub networks. If the target network is missing in this list, this indicates that the interface on the advertising router has not been enabled for OSPF.

In the example above subnet 10.1.212.1 is advertised by router 10.1.212.1 in area 0.

For transit networks, such as an Ethernet LAN with multiple routers attached, a link to the DR for the segment is listed. This points to the type-2 network LSA that contains the full topology information for the segment.

In the example above, this router is connected to a transit network with router 10.1.2.13 as the DR. Note that this IP address is the interface IP address of the DR, not the router ID.

```
DLS1#show ip ospf database network 10.1.2.13

            OSPF Router with ID (10.1.211.1) (Process ID 1)

                Net Link States (area 0)

  Routing Bit Set on this LSA
  LS age: 695
  Options: (No TOS-capability, DC)
  LS Type: Network Links
  Link State ID: 10.1.2.13 (address of Designated Router)
  Advertising Router: 10.1.212.1
  LS Seq Number: 80000004
  Checksum: 0xDBAA
  Length: 32
  Network Mask: /30
        Attached Router: 10.1.212.1
        Attached Router: 10.1.203.1
```

To display full information about a transit LAN, issue the **show ip ospf database network** *designated-router* command, using the IP address of the DR that was listed in the type-1 router LSA for one of the routers connected to the transit LAN. In the type-2 LSA, the DR advertises the subnet mask and connected routers for the segment. The connected routers are listed by their router ID values.

In the example above, a subnet mask of /30 is advertised for the transit LAN, and two connected routers are listed.

Verify the OSPF Link-State Database for Inter-Area Routes

```
DLS1>show ip ospf database summary 10.1.203.1

            OSPF Router with ID (10.1.211.1) (Process ID 1)

                Summary Net Link States (area 0)

  LS age: 577
  Options: (No TOS-capability, DC, Upward)
```

```
  LS Type: Summary Links(Network)
  Link State ID: 10.1.203.1 (summary Network Number)
  Advertising Router: 10.1.203.1
  LS Seq Number: 8000000B
  Checksum: 0x2A58
  Length: 28
  Network Mask: /32
        TOS: 0  Metric: 1
```

If the destination network that you are troubleshooting is in a different area than the area of the router from which you are troubleshooting, the router will not learn about this network through type-1 and type-2 LSAs because these are only used for intra-area routes. OSPF inter-area routes are calculated based on type-3 LSAs that are generated by the Area Border Routers (ABRs) for the area.

To verify the availability of a specific target network in a different area, you can use the **show ip ospf database summary** *subnet* command, where *subnet* is the subnet IP address of the prefix in which you are interested.

The type-3 summary LSA contains the subnet, mask, and cost of the targeted subnet and also lists the router ID of the ABR. If multiple ABRs are advertising the same network, all entries are listed.

In the example above, subnet 10.1.203.1/32 is advertised with a cost of 1 by ABR 10.1.203.1. The cost advertised by the ABR is the cost from the advertising ABR to the target network. When executing the Shortest Path First (SPF) algorithm, the router calculates its own cost to reach the ABR within the area and adds that to the cost advertised by the ABR.

If you do not find an entry for the target network, the next step is to connect to the ABR that you expected to be advertising the route and verify if the route is available there.

Verify the OSPF Link-State Database for External Routes

```
DLS1#show ip ospf database external 10.1.1.0

            OSPF Router with ID (10.1.211.1) (Process ID 1)

                Type-5 AS External Link States

  Routing Bit Set on this LSA
  LS age: 1196
  Options: (No TOS-capability, DC)
  LS Type: AS External Link
  Link State ID: 10.1.1.0 (External Network Number )
  Advertising Router: 10.1.201.1
  LS Seq Number: 80000006
  Checksum: 0x6804
  Length: 36
  Network Mask: /30
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 100
        Forward Address: 0.0.0.0
        External Route Tag: 0
```

If the destination network that you are troubleshooting did not originate in the OSPF network but was redistributed from a different source, the OSPF router learns about this network through type-5 external routes that are injected into the OSPF database by an Autonomous System Boundary Router (ASBR).

To verify the availability of a specific type-5 external LSA in the OSPF database, issue the **show ip ospf database external** *subnet* command, where *subnet* is the subnet IP address of the prefix in which you are interested.

The type-5 summary LSA contains the subnet, mask, metric type, and cost of the targeted subnet. In addition, it lists the router ID of the advertising ASBR. If multiple ASBRs are advertising the same network, all entries are listed.

In the example above, subnet 10.1.1.0/30 is advertised with a cost of 100 as a metric-type 2 external route by ASBR 10.1.201.1.

If you do not find an entry for the target network, the next step is to connect to the ASBR that you expected to be advertising the route and verify if the route is available. If the route is available but not advertised by the ASBR, troubleshoot the route redistribution process on that router.

```
DLS1#show ip ospf database router 10.1.201.1

            OSPF Router with ID (10.1.211.1) (Process ID 1)

                Router Link States (area 0)

  Routing Bit Set on this LSA
  LS age: 391
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 10.1.201.1
  Advertising Router: 10.1.201.1
  LS Seq Number: 8000000E
  Checksum: 0x1163
  Length: 48
  AS Boundary Router
  Number of Links: 2

<Output omitted>
```

Instead of connecting to the ASBR, the OSPF database can also be used to verify if any form of redistribution has been configured on the router that is supposed to be an ASBR. If that router is in the same area as the router from which you are troubleshooting, you can inspect the type-1 router LSA for the ASBR and verify that it advertises itself as an ASBR.

In the example above, the router 10.1.201.1 announces its ASBR status in its type-1 LSA. If the router does not advertise its ASBR status in its type-1 LSA, this indicates that redistribution has not been configured correctly on that router.

```
DLS1#show ip ospf database asbr-summary 10.1.201.1

            OSPF Router with ID (10.1.211.1) (Process ID 1)

                Summary ASB Link States (area 1)

  LS age: 723
  Options: (No TOS-capability, DC, Upward)
  LS Type: Summary Links(AS Boundary Router)
  Link State ID: 10.1.201.1 (AS Boundary Router address)
  Advertising Router: 10.1.211.1
  LS Seq Number: 8000000D
  Checksum: 0xF583
  Length: 28
  Network Mask: /0
        TOS: 0  Metric: 1
```

If the ASBR is not in the same area as the router from which you are troubleshooting, you do not have its type-1 LSA in the database of the router. As a result, you cannot verify its ASBR status by displaying the type-1 LSA. However, if an ASBR is available in a different area, the ABRs for the area generate a type-4 summary AS

Boundary (ASB) entry to announce the availability of the ASBR. The presence or absence of a type-4 entry can also yield a clue about the operation of the redistribution.

You can use the **show ip ospf database asbr-summary** *router-id* command to verify if a type-4 summary ASB LSA exists for the ASBR with the specified router ID.

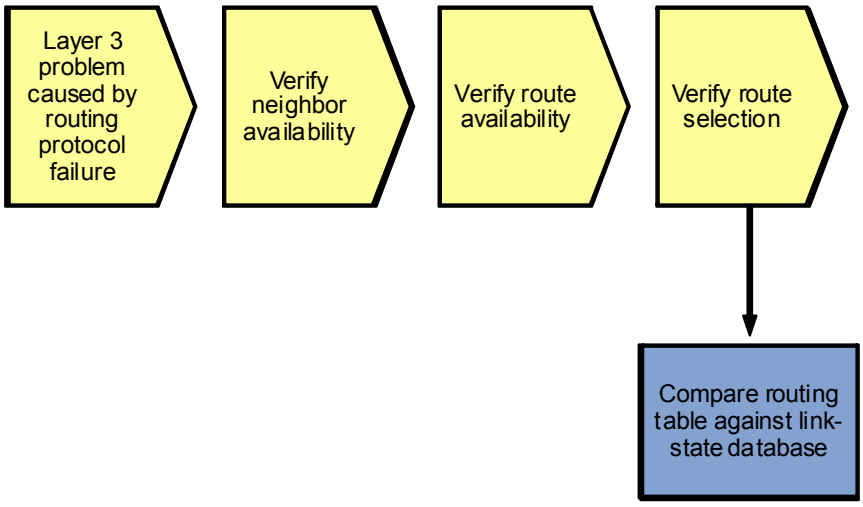
In the example above, ABR 10.1.211.1 announces the availability of ASBR 10.1.201.1.

```
DLS1#show ip ospf border-routers

OSPF Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 10.1.212.1 [1] via 10.1.200.253, Vlan200, ABR, area 0, SPF 5
i 10.1.201.1 [1] via 10.1.2.2, FastEthernet0/5, ASBR, area 0, SPF 5
i 10.1.203.1 [2] via 10.1.200.253, Vlan200, ABR, area 0, SPF 5
```

During the execution of the SPF algorithm, a router combines the information from the various LSAs that contain information about ABR and ASBR status and calculates the shortest paths to each ABR and ASBR. You can view the result of this calculation with the **show ip ospf border-routers** command.

In the example above, area 0 has two ABRs: 10.1.212.1 and 10.1.203.1. The cost to reach ABR 10.1.212.1 is 1, as can be seen from the number in the square brackets. The cost to reach ABR 10.1.203.1 is 2. The cost to reach ASBR 10.1.201.1 is 1. This cost is important to know because it is added to the cost advertised by these routers in their type-3 LSAs to obtain the total cost to the destination network.

Sample OSPF Troubleshooting Flow



If all appropriate entries are available in the OSPF link-state database, these should result in correct routes in the IP routing table after calculation of the SPF algorithm. Unfortunately, the results of the SPF algorithm for each individual route cannot be directly verified.

Keep in mind that OSPF competes with other routing sources to install routes in the routing table. Therefore, an OSPF route might not be installed in the routing table because a route with a better administrative distance from a different source is available.

Verify the MTU between OSPF Neighbors

Maximum Transmission Unit (MTU) mismatch between two OSPF neighbors is common when connecting together two multilayer switches of a different type (for example 3550 and 3560) or when interconnecting a multilayer switch with a router. Multilayer switches often have the system MTU set to 1504 bytes while routers typically use an MTU of 1500 bytes. An MTU mismatch usually causes two OSPF neighbors to remain stuck in EXSTART/EXCHANGE state, failing to create full adjacency.

Changes to the system MTU are made using the **system mtu** *mtu-size* command. The routing MTU can be changed using the **system mtu routing** *mtu-size* command. System MTU on a Cisco Catalyst 3560 switch can range from 1500-1998 bytes.

Note: Changes to MTU size will not take effect until the next reload is done.

MTU settings can be verified using the **show interfaces** or the **show system mtu** commands:

```
DLS2#show interfaces fastEthernet 0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0017.5a53.a3c2 (bia 0017.5a53.a3c2)
  Description: FE to R3
  Internet address is 10.1.2.13/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255

DLS2#show system mtu

System MTU size is 1500 bytes
System Jumbo MTU size is 1500 bytes
Routing MTU size is 1500 bytes
```

OSPF Neighbor status can be verified using the **show ip ospf neighbor** command. In the example shown below, the system and system routing MTU for Layer 3 switch DLS2 has been changed to 1504 bytes. The MTU of the neighbors, DLS1 (10.1.211.1) and R3 (10.1.203.1) is set to the default of 1500 bytes.

```
DLS2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.211.1        1   EXSTART/BDR     00:00:38    10.1.200.252    Vlan200
10.1.203.1        1   EXSTART/BDR     00:00:37    10.1.2.14       FastEthernet0/5
```

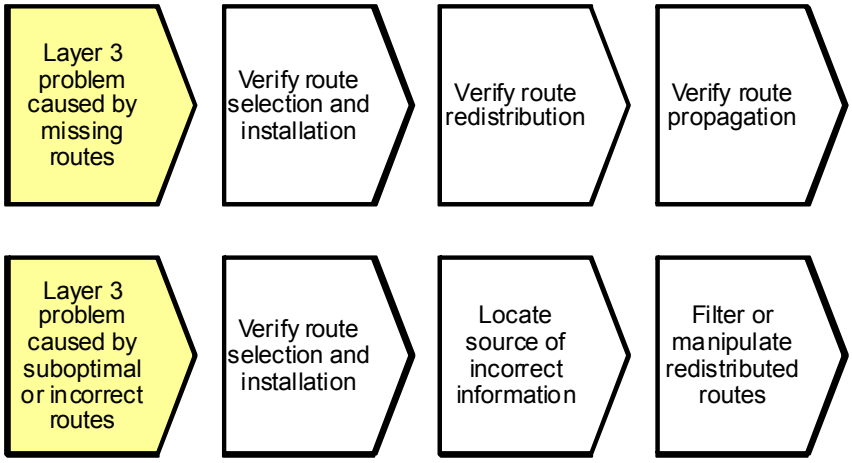
Console messages:

```
DLS2#
%OSPF-5-ADJCHG: Process 1, Nbr 10.1.203.1 on FastEthernet0/5 from DOWN to
DOWN, Neighbor Down: Ignore timer expired
DLS2#
%OSPF-5-ADJCHG: Process 1, Nbr 10.1.211.1 on Vlan200 from EXSTART to DOWN,
Neighbor Down: Too many retransmissions
```

Troubleshooting Route Redistribution

The figure illustrates an example of a method that you can use to diagnose and resolve problems related to route redistribution.

Sample Route Redistribution Troubleshooting Flow



When do you start troubleshooting route redistribution?

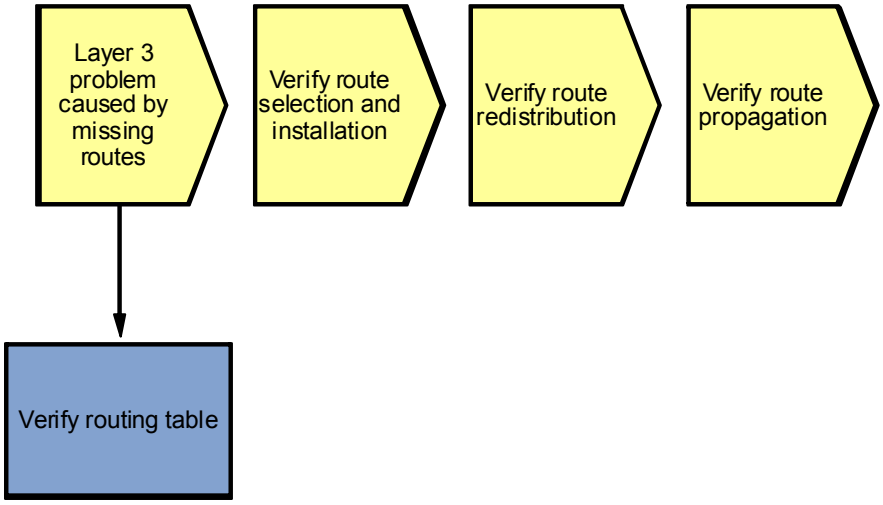
There are two major reasons to start troubleshooting the route redistribution. The first reason is when you are experiencing IP connectivity problems in an environment in which information from a specific routing domain is redistributed into a different routing domain and the connectivity problem is caused by a route from the source routing domain that is not available on one or more of the routers participating in the destination routing domain. In this scenario, the cause of the problem is that the exchange of routing information between the source routing domain and the destination routing domain is not working correctly.

Note: In this section, the terms *source* and *destination* are used to indicate the source and destination of the routing information, not the source and destination of a traffic flow.

The second reason to start troubleshooting route redistribution is if you are experiencing IP connectivity problems caused by the use of incorrect routing information by some of the routers in a network that use route redistribution. This behavior could be caused by routing information feedback or improper route selection.

Sample troubleshooting flows for each of these scenarios are provided in this section.

Sample Route Redistribution Troubleshooting Flow



The first scenario in which you start troubleshooting route redistribution is when redistribution is configured and you are troubleshooting connectivity problems to a network in the source routing domain from a router in the destination routing domain. This type of problem is usually encountered during a generic IP connectivity troubleshooting process when a route is discovered missing from the routing table on one of the routers in the destination routing domain while the route is present in the routing tables of the routers in the source routing domain.

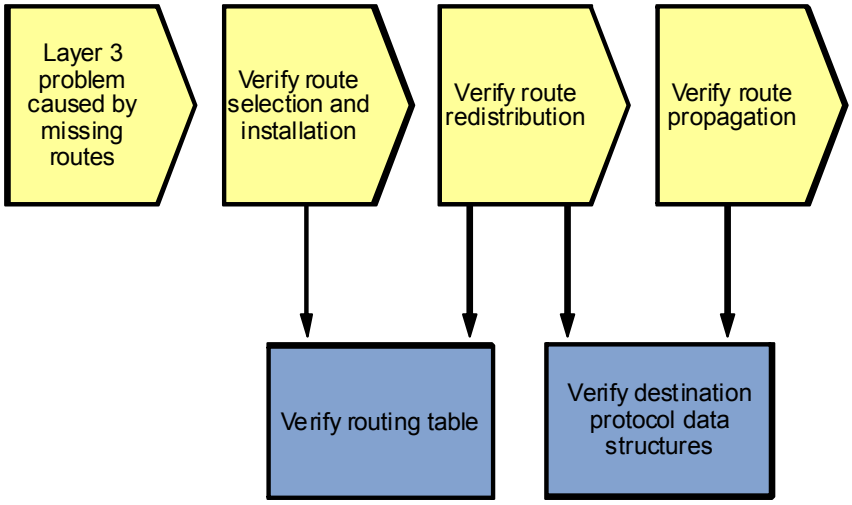
Troubleshooting redistribution consists of troubleshooting four generic areas:

- Source routing protocol
- Route selection and installation
- Redistribution
- Destination protocol

In this scenario, the reason to start troubleshooting the redistribution is when the route is available in the source routing domain but not in the destination routing domain. Therefore, the first step has already been taken at this point. If the route is not available everywhere in the source routing domain to begin with, there is no reason to start troubleshooting redistribution, but you should initiate a troubleshooting process for the source routing protocol first.

Therefore, we will start at the second step: troubleshooting route selection and installation.

Sample Route Redistribution Troubleshooting Flow



There are not many tools that are specifically targeted at troubleshooting the redistribution process. The redistribution process takes routes from the routing table after they have been installed by the source routing protocol and then injects them into the destination protocol's data structures. Therefore, the main tools that are available to track this flow of information are the commands that allow you to examine the routing table and the destination protocol data structures.

After you have verified that the routes are injected into the destination protocol's data structures, you have finished troubleshooting the actual redistribution process. If the routes are not properly propagated by the destination protocol, initiate a troubleshooting process for the destination protocol.

The **show ip route 10.1.202.1 255.255.255.255** command on R1 indicates that the route is known via EIGRP 1 and is redistributing via OSPF, but it is not being advertised by OSPF.

```
R1#show ip route 10.1.202.1 255.255.255.255
Routing entry for 10.1.202.1/32
  Known via "eigrp 1", distance 90, metric 2297856, type internal
  Redistributing via eigrp 1, ospf 1
  Last update from 10.1.1.2 on Serial0/0/0, 07:02:16 ago
  Routing Descriptor Blocks:
  * 10.1.1.2, from 10.1.1.2, 07:02:16 ago, via Serial0/0/0
      Route metric is 2297856, traffic share count is 1
      Total delay is 25000 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

The **show ip route 10.1.203.1 255.255.255.255** command on R1 indicates that the route is known via EIGRP 1 and is redistributing via EIGRP. It is also being advertised by EIGRP 1.

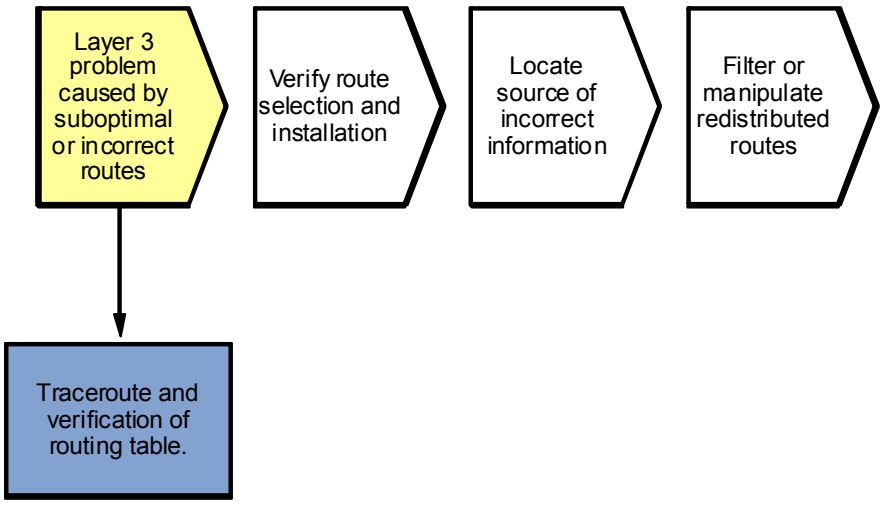
```
R1#show ip route 10.1.203.1 255.255.255.255
Routing entry for 10.1.203.1/32
  Known via "ospf 1", distance 110, metric 4, type inter area
  Redistributing via eigrp 1
  Advertised by eigrp 1 metric 1544 2000 255 1 1500
  Last update from 10.1.2.1 on FastEthernet0/1, 07:13:32 ago
  Routing Descriptor Blocks:
```

```
* 10.1.2.1, from 10.1.203.1, 07:13:32 ago, via FastEthernet0/1
    Route metric is 4, traffic share count is 1
```

The best tool available in troubleshooting redistribution problems is the **show ip route** *network mask* command. Routes that are being redistributed and advertised to other routers by the destination protocol are marked with a line starting with “Advertised by” and then lists the destination protocol and any parameters configured on the redistribution statement, such as configured metrics and metric type.

What makes this command useful is that it takes into account any route maps or distribute lists that are applied to the redistribution.

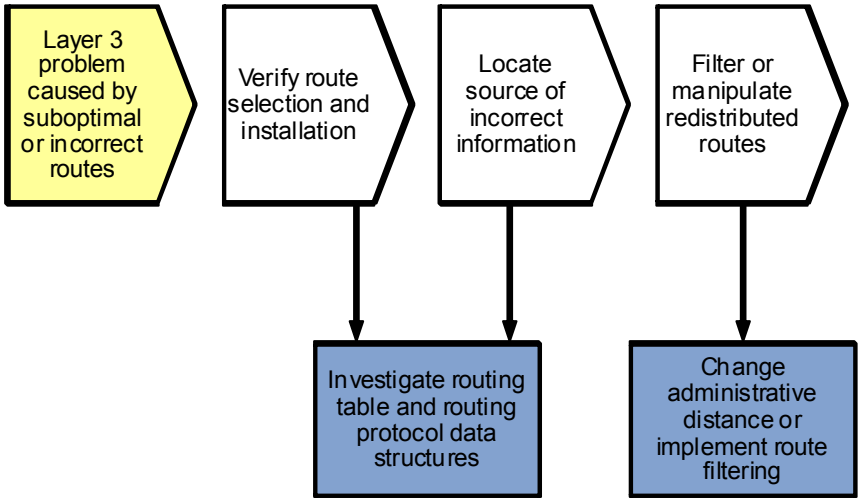
Sample Route Redistribution Troubleshooting Flow



The second common scenario that might lead you to start troubleshooting route redistribution is when you discover that traffic is using unexpected suboptimal routes to reach certain destinations or that traffic enters a routing loop. This is often discovered while troubleshooting IP connectivity to a certain destination and using the **show ip route** and **traceroute** commands to track the flow of traffic. When you are redistributing routing information between routing protocols, you have to be aware that improper route selection or routing feedback can cause suboptimal paths to be used or traffic to enter a routing loop. Whenever you spot unexpected routing behavior in a network that uses redistribution, consider routing feedback or improper route selection as a possible cause.

A typical symptom of a redistribution problem is when the expected route is available on the router that you are troubleshooting, but it is not selected as the best route in the routing table. A route from a different protocol or a route of the same protocol but originated from a different source is selected as the best route and installed in the routing table.

Sample Route Redistribution Troubleshooting Flow



The first question to ask at this point is if the route is only improperly selected. In other words, you expected this route to be present but did not want it to be selected as the best route. If this is the case, you can manipulate the route selection process by changing the administrative distance. This can be done for all routes learned via a particular routing protocol or selectively using an access list.

If the route was not only improperly selected but should not have been present at all in the routing protocol data structures in this router, you must track the source of the route and use route-filtering techniques at the source to stop it from being advertised.

Verify the Routing Table

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 15 subnets, 3 masks
O IA    10.1.10.0/24 [110/2] via 10.1.2.1, 07:43:07, FastEthernet0/1
O       10.1.2.12/30 [110/3] via 10.1.2.1, 07:42:57, FastEthernet0/1
C       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.1.2.0/30 is directly connected, FastEthernet0/1
C       10.1.1.0/30 is directly connected, Serial0/0/0
O IA    10.1.30.0/24 [110/2] via 10.1.2.1, 07:43:07, FastEthernet0/1
O IA    10.1.20.0/24 [110/2] via 10.1.2.1, 07:43:07, FastEthernet0/1
O IA    10.1.50.0/24 [110/2] via 10.1.2.1, 07:43:07, FastEthernet0/1
O IA    10.1.100.0/24 [110/2] via 10.1.2.1, 07:43:07, FastEthernet0/1
D       10.1.202.1/32 [90/2297856] via 10.1.1.2, 07:43:48, Serial0/0/0
O IA    10.1.203.1/32 [110/4] via 10.1.2.1, 07:42:57, FastEthernet0/1
C       10.1.201.1/32 is directly connected, Loopback0
```

```
O       10.1.200.0/24 [110/2] via 10.1.2.1, 07:43:00, FastEthernet0/1
O       10.1.211.1/32 [110/2] via 10.1.2.1, 07:43:10, FastEthernet0/1
O       10.1.212.1/32 [110/3] via 10.1.2.1, 07:43:00, FastEthernet0/1

R1#show ip route 10.1.50.0 255.255.255.0
Routing entry for 10.1.50.0/24
  Known via "ospf 1", distance 110, metric 2, type inter area
  Redistributing via eigrp 1
  Advertised by eigrp 1 metric 1544 2000 255 1 1500
  Last update from 10.1.2.1 on FastEthernet0/1, 07:42:07 ago
  Routing Descriptor Blocks:
  * 10.1.2.1, from 10.1.211.1, 07:42:07 ago, via FastEthernet0/1
      Route metric is 2, traffic share count is 1
```

The source of a route in the routing table is marked by the “from” field that follows the next-hop IP address. For distance vector protocols, the source and next-hop addresses are typically the same. For a link-state protocol, such as OSPF, this is the router that originated the LSA on which the route is based. By tracking the routing source from router to router, you can determine the point where the incorrect routing information is injected into the routing protocol’s data structures, and you can apply filtering to stop it from being propagated.