

Packet Tracer Lab 20 Solution Guide

Multi-Site Connectivity Loss

Incident ID: INC-1020

Objective

This lab focuses on identifying and resolving a regional service reachability issue affecting all branch offices in an enterprise OSPF environment.

Branch users can reach local resources, other branch networks, and headquarters departmental networks, but they cannot access centralized DNS and file services hosted in the headquarters Server VLAN.

The objective is to isolate the affected destination network, identify the missing OSPF advertisement, restore route propagation, and validate service reachability from multiple regional sites.

Root Cause

The OSPF network statement for the headquarters Server VLAN was removed from SW-HQ-CORE during scheduled routing maintenance.

```
network 192.168.40.0 0.0.0.255 area 0
```

Because the Server VLAN was no longer included in OSPF, branch routers did not learn a route to 192.168.40.0/24. OSPF neighbor relationships remained fully established, and all other advertised networks continued functioning normally.

Symptoms Observed

- Branch users can reach their local default gateways.
- Local branch connectivity remains operational.
- Branch-to-branch communication remains operational.
- Headquarters Finance, HR, and IT networks remain reachable.
- The headquarters Server VLAN is unreachable from all branches.
- DNS server 192.168.40.10 is unreachable from branch networks.
- File server 192.168.40.20 is unreachable from branch networks.
- WAN interfaces remain up.
- OSPF neighbor relationships remain in the FULL state.
- Route 192.168.40.0/24 is missing from branch routing tables.

BridgeOpsOne

Troubleshooting Process

Step 1 — Verify Client IP Configuration

From an affected branch workstation, review its addressing information:

```
ipconfig
```

Verify that the workstation has a valid branch IP address, subnet mask, and default gateway. This rules out a local addressing issue.

Step 2 — Test the Local Default Gateway

From PC-A1, test Branch A's gateway:

```
ping 192.168.50.1
```

This should succeed, confirming that the workstation, access switch, and local router interface are operational.

Step 3 — Compare Reachable and Unreachable Destinations

Test a reachable headquarters departmental workstation:

```
ping 192.168.10.10
```

This should succeed.

Then test the headquarters file and DNS servers:

```
ping 192.168.40.20
```

```
ping 192.168.40.10
```

These tests should fail. The branch gateway may return "Destination host unreachable," indicating that the router does not have a route to the destination network.

Step 4 — Confirm Branch-to-Branch Connectivity

```
ping 192.168.60.10
```

```
ping 192.168.70.10
```

These should succeed. This demonstrates that the WAN and OSPF domain are not completely down.

BridgeOpsOne

Step 5 — Verify WAN Interface Status

On R-BRANCH-A and R-HQ, review interface status:

```
show ip interface brief
```

The serial WAN interfaces should be up/up. This rules out a physical or administrative interface failure.

Step 6 — Verify OSPF Neighbor Relationships

On R-HQ, run:

```
show ip ospf neighbor
```

The headquarters core and all three branch routers should remain in the FULL state. This confirms that OSPF adjacencies are healthy, but it does not confirm that every network is being advertised.

Step 7 — Review the Branch Routing Table

On R-BRANCH-A, run:

```
show ip route
```

The routing table should contain OSPF routes for the Finance, HR, and IT networks:

- 192.168.10.0/24
- 192.168.20.0/24
- 192.168.30.0/24

However, 192.168.40.0/24 will be absent. This is the primary evidence that the Server VLAN is not being advertised into OSPF.

Step 8 — Review OSPF Configuration on SW-HQ-CORE

Access SW-HQ-CORE and review the routing configuration:

```
show running-config | section router ospf
```

Packet Tracer versions that do not support the section filter can use:

```
show running-config
```

Compare the configured network statements with the headquarters VLAN plan. The statement for 192.168.40.0/24 will be missing.

BridgeOpsOne

Commands Used

```
ipconfig
ping
tracert
show ip interface brief
show ip ospf neighbor
show ip route
show ip protocols
show running-config
configure terminal
router ospf 1
network 192.168.40.0 0.0.0.255 area 0
copy running-config startup-config
```

Resolution

On SW-HQ-CORE, restore the missing Server VLAN OSPF advertisement:

```
enable
configure terminal
router ospf 1
network 192.168.40.0 0.0.0.255 area 0
end
copy running-config startup-config
```

Allow several seconds for OSPF to update the routing domain. The neighbor relationship does not need to be rebuilt because it remained established throughout the incident.

Validation

Successful resolution should include:

- 192.168.40.0/24 appears as an OSPF route on all branch routers.
- PC-A1 can ping 192.168.40.10 and 192.168.40.20.
- PC-B1 and PC-C1 can also reach both headquarters servers.
- Finance, HR, IT, and branch-to-branch connectivity remain operational.
- OSPF neighbors remain in the FULL state.
- No unrelated interface or routing changes were required.

Recommended validation commands:

```
show ip route
show ip ospf neighbor
ping 192.168.40.10
ping 192.168.40.20
```

BridgeOpsOne

Expected Post-Resolution Routing Entry

On a branch router, the restored network should appear as an OSPF-learned route similar to:

```
O 192.168.40.0/24 [110/66] via 10.255.0.1, Serial0/0/0
```

The exact OSPF metric and outgoing interface may vary by branch, but the destination network must be present.

Key Takeaways

- A FULL OSPF neighbor state does not guarantee that every required network is being advertised.
- Compare working and failing destinations to narrow the scope of an outage.
- A “Destination host unreachable” response from the local gateway often indicates missing routing information.
- Routing tables provide stronger evidence than assumptions based only on interface or neighbor status.
- Avoid modifying healthy WAN links when the evidence points to a missing destination route.
- Validate restoration from multiple affected sites after correcting an enterprise routing issue.
- Save configuration changes only after confirming the intended behavior.

Real-World Relevance

This type of issue is commonly encountered after routing maintenance, network migrations, VLAN additions, and configuration cleanup. A single omitted network advertisement can disrupt access to critical services across multiple sites while leaving routing adjacencies and unrelated business networks fully operational.

The lab reinforces operational troubleshooting skills used in NOC, enterprise networking, managed services, infrastructure support, and network engineering roles.