

Packet Tracer Lab 20

Regional Communications Outage

Incident ID: INC-1020

Difficulty

Advanced

Estimated Time

30–50 Minutes

Skills Covered

- Enterprise WAN Troubleshooting
- OSPF Route Advertisement Analysis
- Routing Table Verification
- Multi-Site Connectivity Testing
- Ping and Traceroute Analysis
- Layer 3 Fault Isolation
- Structured Troubleshooting Methodology
- Operational Incident Communication

Scenario

Following scheduled routing maintenance, users at multiple regional branch offices report that centralized corporate services hosted at headquarters are unavailable.

Branch users remain able to communicate with local devices, reach their local default gateways, and access systems located at other branch offices. Headquarters users report that local departmental systems remain operational.

The disruption appears isolated to services hosted within the headquarters server network, including internal DNS and file services. You have been assigned to investigate the regional access issue, identify the root cause, restore connectivity, and validate that normal operations have resumed.

BridgeOpsOne

Customer Report

Reported By: Regional Operations

Users Affected: Branch A, Branch B, and Branch C users

Business Impact: Regional users cannot access centralized DNS and file services hosted at headquarters. Local branch operations remain available.

Issue Started: Shortly after scheduled routing maintenance.

Priority: High

Goal

- Identify the cause of the multi-site service reachability issue.
- Restore branch access to centralized headquarters services.
- Confirm that local branch and inter-branch connectivity remain operational.
- Validate routing behavior after corrective action.
- Document the troubleshooting process and final resolution.

Environment

- Headquarters router and multilayer core switch
- Three regional branch routers and access switches
- OSPF Area 0 enterprise routing domain
- Headquarters Finance, HR, IT, and Server VLANs
- Branch A, Branch B, and Branch C user networks
- Internal DNS server
- Internal file server
- Simulated ISP router

BridgeOpsOne

Known Variables

- Branch users can communicate with their local default gateways.
- Local connectivity remains operational within each branch office.
- Branch-to-branch communication remains available.
- Headquarters departmental networks remain operational.
- WAN interfaces remain operational.
- OSPF neighbor relationships remain established.
- The issue affects access to centralized services hosted in the headquarters server network.
- The headquarters server network is 192.168.40.0/24.
- The DNS server is assigned 192.168.40.10.
- The file server is assigned 192.168.40.20.
- Branch default gateways are:
 - Branch A: 192.168.50.1
 - Branch B: 192.168.60.1
 - Branch C: 192.168.70.1
- Scheduled routing maintenance was completed before the incident began.
- Follow a structured troubleshooting methodology before making configuration changes.

Troubleshooting Mindset

During troubleshooting, think through the following questions:

- Do affected workstations have valid IP addressing and default gateway information?
- Can branch users reach local resources and other branch networks?
- Can branch users reach headquarters departmental networks?
- Which specific destination network is unavailable?
- Are WAN interfaces and OSPF adjacencies healthy?
- Do branch routing tables contain a route to the headquarters server network?
- Are all required headquarters networks being advertised into OSPF?
- Did recent routing maintenance remove or alter a required advertisement?

Focus on identifying the exact boundary where connectivity stops. A healthy interface or OSPF neighbor relationship does not automatically confirm that every required network is being advertised.

BridgeOpsOne

BridgeOpsOne

Expected Outcome

By the end of this lab, users should restore regional access to the headquarters server network while preserving connectivity across all other enterprise networks.

Users should also be able to explain how routing adjacencies can remain healthy even when a required destination network is missing from the routing domain.

Optional BridgeOpsOne Workflow

This section is optional but recommended for users who want a more realistic operations-center experience.

1. Create an Initial Update

Create a customer-safe incident update describing:

- Multiple regional sites unable to access centralized corporate services
- Local branch connectivity remains operational
- Network investigation is underway

2. Save Timeline Updates

Provide 2–3 operational updates describing:

- Initial connectivity tests
- WAN and OSPF validation
- Routing-table findings
- Progress toward service restoration

Add these updates to the incident timeline within the Command Center. Keep updates professional, concise, and customer safe.

3. Create a Final Resolution Statement

Summarize the identified cause, corrective action, restored service status, and validation completed across affected sites.

BridgeOpsOne

Real-World Relevance

This issue simulates realistic troubleshooting commonly encountered in:

- Network Operations Centers (NOC)
- Enterprise Network Operations
- Managed Service Providers
- Regional Infrastructure Support
- Network Engineering
- Major Incident Support

The lab reinforces the difference between OSPF adjacency health and route advertisement completeness. In production environments, routing neighbors may remain fully established while a specific business network becomes unreachable because it is no longer advertised.

Deliverables

At the conclusion of this lab, users should be able to:

- Explain the reported business impact.
- Identify the unavailable destination network.
- Demonstrate a structured troubleshooting process.
- Analyze OSPF neighbors and routing tables.
- Restore the missing route advertisement.
- Validate access to centralized services from multiple branches.
- Communicate findings and resolution clearly.

Hints

- Verify local and branch-to-branch connectivity before assuming a complete WAN outage.
- Compare a reachable headquarters destination with an unreachable headquarters destination.
- Use ipconfig, ping, and tracert from an affected workstation.
- Use show ip interface brief to verify interface state.
- Use show ip ospf neighbor to confirm adjacency health.
- Use show ip route to identify missing destination networks.
- Review the OSPF configuration on the device responsible for advertising headquarters VLANs.
- Avoid changing working WAN interfaces or OSPF neighbors without evidence.