

Packet Tracer Lab 18

Severe Network Performance Degradation Investigation

Incident ID: INC-1018

Difficulty

Advanced

Estimated Time

30-45 Minutes

Skills Covered

- Routing Loop Identification
- Static and Dynamic Route Analysis
- OSPF Verification
- Administrative Distance Concepts
- Ping and Traceroute Analysis
- WAN Troubleshooting
- Structured Troubleshooting Methodology
- Operational Validation

Scenario

Following scheduled overnight WAN maintenance, users at headquarters began reporting that branch-hosted applications and services were unavailable.

The maintenance window included temporary routing changes used to validate traffic flow across the enterprise WAN. The work was reported as complete before the start of business operations.

Headquarters resources remain available, and users at the branch office can still communicate with devices on their local network. However, traffic originating from headquarters cannot successfully reach the branch network.

You have been assigned to investigate the incident, identify where traffic is failing, restore connectivity, and validate normal operations.

BridgeOpsOne

Customer Report

Reported By: Network Operations Center

Users Affected: Headquarters users accessing branch-hosted resources

Business Impact: Branch applications, shared files, and remote services are unavailable to headquarters users.

Issue Started: Following scheduled overnight WAN maintenance.

Priority: High

Goal

- Identify the cause of the branch connectivity failure.
- Determine where traffic stops or repeats along the path.
- Restore communication between headquarters and the branch office.
- Validate that OSPF and end-to-end routing operate normally.
- Document the investigation and corrective action.

Environment

- Headquarters HR, Finance, Engineering, and Server VLANs
- SW-D1 access switch
- SW-CORE core switch
- R-EDGE headquarters edge router
- R-WAN-HQ WAN transit router
- R-BRANCH branch router
- SW-BRANCH access switch
- Branch office workstations
- OSPF Area 0 dynamic routing
- Serial WAN connection between headquarters and branch

BridgeOpsOne

Known Variables

- HR-PC1: 192.168.10.10 /24, default gateway 192.168.10.1
- SERVER01: 192.168.50.10 /24, default gateway 192.168.50.1
- BRANCH-PC1: 192.168.60.10 /24, default gateway 192.168.60.1
- BRANCH-PC2: 192.168.60.11 /24, default gateway 192.168.60.1
- The R-EDGE to R-WAN-HQ transit network is 10.10.2.0/30.
- The R-WAN-HQ to R-BRANCH WAN network is 10.10.3.0/30.
- Headquarters users can access SERVER01.
- Branch users can communicate with other devices on the branch LAN.
- Router interfaces appear operational.
- The issue began after routing changes performed during the maintenance window.

Use these values to test specific portions of the network and compare local connectivity with remote connectivity. Do not assume that an operational interface or routing protocol neighbor guarantees that the selected forwarding path is correct.

Troubleshooting Mindset

During troubleshooting, think through the following questions:

- Can affected systems reach their default gateway?
- Are headquarters-local resources still reachable?
- Is the failure unidirectional or bidirectional?
- Where does traceroute show traffic traveling?
- Do any router addresses repeat in the packet path?
- Are all routing protocol neighbors established?
- Which route is selected for the branch network?
- Was a recent configuration change given preference over a dynamically learned route?

Follow the evidence from the endpoint toward the destination. Avoid changing OSPF, interfaces, or cabling until you have verified which component is actually failing.

BridgeOpsOne

Expected Outcome

By the end of this lab, users should restore communication between headquarters and the branch office and verify that traffic follows the intended WAN path.

Users should also be able to explain how an incorrect route can override otherwise healthy dynamic routing and create a forwarding loop.

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:

- Headquarters users unable to access branch-hosted services
- Local headquarters resources remain available
- Network investigation underway

2. Save Timeline Updates

Provide 2-3 operational updates describing:

- Connectivity tests completed
- Routing and WAN components validated
- The point in the traffic path where abnormal behavior is observed

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

3. Create a Final Resolution Statement

After service restoration, summarize:

- The confirmed cause
- The corrective action
- The current network status
- Post-repair validation and monitoring

BridgeOpsOne

Real-World Relevance

This issue simulates routing failures commonly encountered in:

- Network Operations Centers (NOC)
- Enterprise WAN Operations
- MSP Network Support
- Enterprise IT
- Network Engineering

Temporary maintenance routes, legacy static routes, and incorrect next-hop selections can override dynamic routing and produce failures that are difficult to recognize because physical links and routing adjacencies remain healthy.

Deliverables

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

- Explain the incident and business impact.
- Describe the troubleshooting methodology.
- Identify abnormal packet forwarding behavior.
- Restore headquarters-to-branch communication.
- Validate the intended routing path.
- Communicate findings clearly.

Hints

- Confirm that headquarters-local services remain reachable before focusing on the WAN.
- Use ping to compare reachable and unreachable destinations.
- Use tracer from HR-PC1 to BRANCH-PC1 and carefully review every hop.
- Repeated router addresses are an important clue.
- Use show ip interface brief to verify interface state.
- Use show ip ospf neighbor to determine whether OSPF adjacency is actually down.
- Use show ip route 192.168.60.0 to identify how the branch network is being reached.
- Pay attention to the route source code and the selected next hop.
- Review recent configuration changes only after isolating the traffic path.