

Packet Tracer Lab 3

Inter-VLAN Routing Failure Investigation

Incident ID: INC-1003

Difficulty

Intermediate

Estimated Time

20–40 Minutes

Skills Covered

- VLAN Troubleshooting
- Inter-VLAN Routing
- Ping Testing
- Traceroute Analysis
- Default Gateway Verification
- Router-on-a-Stick Concepts
- Structured Troubleshooting Methodology

Scenario

Users across multiple departments have reported connectivity issues following network changes performed during a scheduled maintenance window.

Initial reports indicate that devices can communicate successfully with systems located within their own department. However, users are unable to access resources located in other parts of the network.

Several internal business applications hosted on centralized servers have become inaccessible for affected users.

You have been assigned as the technician responsible for identifying the issue, restoring connectivity, and validating that normal operations have been restored.

BridgeOpsOne

Customer Report

Reported By: Sales Department

Users Affected: Sales Department

Business Impact: Sales users are unable to access resources located in other network segments. Internal applications and shared services are unavailable for affected users.

Issue Started: Shortly after scheduled network maintenance.

Priority: Medium

Goal

- Identify the root cause of the connectivity issue
- Restore communication between network segments
- Validate access to shared resources
- Document your findings

Environment

- HR Department VLAN
- Finance Department VLAN
- Internal Server VLAN
- Layer 2 Access Switch
- Branch Router
- Multiple Workstations
- Internal Application Server

Troubleshooting Mindset

During troubleshooting, think through the following questions:

BridgeOpsOne

- Do devices have valid IP configurations?
- Can devices communicate with their default gateway?
- Is local VLAN communication functioning properly?
- Can devices communicate with resources located in other VLANs?
- Where does connectivity stop?
- Is routing between VLANs functioning correctly?
- Have any recent configuration changes impacted traffic flow?

Focus on isolating the issue step-by-step rather than immediately assuming the problem.

Expected Outcome

By the end of this lab, users should successfully regain connectivity to resources located in other VLANs.

Users should also be able to explain the troubleshooting process used to identify and resolve the issue.

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 an initial customer-safe incident update describing the issue.

Example topics:

- Multiple departments reporting connectivity issues
- Internal applications inaccessible
- Investigation in progress

Use the Generate feature if needed to clean and professionalize your update.

BridgeOpsOne

2. Save Timeline Updates

During troubleshooting, provide 2–3 operational updates describing:

- What you are investigating
- What has been ruled out
- Progress toward resolution

Add these updates to your incident timeline within the Command Center.

Focus on keeping updates:

- Professional
- Concise
- Customer safe

3. Create a Final Resolution Statement

Once connectivity has been restored, create a final resolution update summarizing:

- What caused the issue
- Actions taken
- Current environment status
- Monitoring and validation steps

Real-World Relevance

This issue simulates realistic troubleshooting commonly encountered in:

- NOC Environments
- Network Operations
- MSP Support
- Enterprise IT
- Junior Network Engineer Roles

BridgeOpsOne

Deliverables

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

- Explain the issue
- Describe the troubleshooting process
- Demonstrate the fix
- Validate successful inter-VLAN communication
- Restore access to shared resources
- Communicate findings clearly

Hints

- Verify local connectivity before testing remote networks.
- Compare the results of connectivity tests within the same VLAN and across different VLANs.
- Use: ipconfig to review workstation network settings.
- Use: ping to identify where communication is failing.
- Use: tracert to determine how far traffic is traveling.
- Verify that default gateways are reachable.
- Consider which device is responsible for forwarding traffic between VLANs.
- Compare the behavior of working VLANs with the affected VLAN before making configuration changes.
- Follow a structured troubleshooting process and avoid making assumptions too early.