

BridgeOpsOne

Packet Tracer Lab 22

Network Segmentation Failure Investigation

Incident ID: INC-1022

Difficulty

Advanced

Estimated Time

20–40 Minutes

Skills Covered

- Extended ACL Troubleshooting
- Network Segmentation Analysis
- Inter-VLAN Routing Verification
- Policy-Based Traffic Control
- Ping and Comparative Testing
- Interface and Routing Validation
- Structured Troubleshooting Methodology
- Operational Validation

Scenario

Following scheduled network policy maintenance, users in the Finance department have reported that centralized corporate services are no longer accessible.

Finance workstations remain connected to the local network and can communicate with their default gateway and users in other departments. However, attempts to reach the internal DNS and file servers fail. HR, IT, and regional branch users continue accessing the same server resources normally.

You have been assigned to identify the source of the department-specific communication failure, restore the intended access, and validate that network segmentation policies are functioning correctly.

Customer Report

Reported By: Finance Department

Users Affected: Finance users

Business Impact: Finance personnel cannot access centralized DNS and file services required for daily operations.

BridgeOpsOne

Issue Started: Shortly after scheduled network policy maintenance.

Priority: High

Goal

- Identify the cause of the Finance-to-server communication failure.
- Restore Finance access to approved centralized services.
- Confirm that other departments and branch offices remain operational.
- Validate the intended segmentation policy after the repair.
- Document your findings.

Environment

- Headquarters multilayer core switch
- Finance VLAN 10
- HR VLAN 20
- IT VLAN 30
- Server VLAN 40
- Enterprise WAN with three regional branch offices
- OSPF dynamic routing
- Internal DNS and file servers
- Department and branch workstations

Known Variables

- Finance workstation: 192.168.10.10/24
- Finance default gateway: 192.168.10.1
- HR workstation: 192.168.20.10/24
- IT workstation: 192.168.30.10/24
- Headquarters server network: 192.168.40.0/24
- DNS server: 192.168.40.10
- File server: 192.168.40.20
- Finance users can communicate with their local default gateway.
- Finance users can communicate with HR and IT resources.
- HR, IT, and regional branch users can access the headquarters servers.
- All relevant VLAN interfaces and WAN links remain operational.
- OSPF neighbor relationships remain established and enterprise routes remain present.
- Scheduled network policy maintenance occurred before the incident began.
- Follow a structured troubleshooting methodology before making configuration changes.

BridgeOpsOne

Troubleshooting Mindset

During troubleshooting, think through the following questions:

- Is the issue isolated to Finance or affecting multiple networks?
- Can Finance reach its default gateway and other departmental networks?
- Can unaffected users reach the same server destinations?
- Are VLAN interfaces, routing entries, and OSPF relationships healthy?
- Is traffic being filtered differently based on its source network?
- Have recent policy changes altered permitted communication paths?
- Where does communication stop?

Compare working and non-working traffic paths. Focus on isolating what is different before changing the configuration.

Expected Outcome

By the end of this lab, Finance users should regain access to approved centralized services while all other enterprise connectivity remains operational.

Users should also be able to explain how routing and interface health can remain normal while a traffic-filtering policy prevents communication.

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 update describing:

- Finance users unable to access centralized services
- Other departments remain operational
- Investigation underway

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

2. Save Timeline Updates

Provide 2–3 operational updates describing:

- Connectivity tests completed
- Working and non-working traffic paths compared
- Routing, interface, and policy findings
- Progress toward restoration

Add the updates to your Command Center timeline. Keep them professional, concise, and customer safe.

3. Create a Final Resolution Statement

Summarize:

BridgeOpsOne

- Root cause
- Corrective action
- Current service status
- Validation completed

Real-World Relevance

This issue simulates realistic troubleshooting commonly encountered in:

- Network Operations Centers (NOC)
- Enterprise Network Engineering
- Security and Segmentation Operations
- MSP Support
- Enterprise IT

The lab develops policy troubleshooting, differential testing, routing validation, and operational communication skills.

Deliverables

- Explain the issue and affected traffic path.
- Describe the troubleshooting methodology.
- Identify the misconfigured policy.
- Restore Finance access to centralized services.
- Validate unaffected networks remain operational.
- Communicate findings clearly.

Hints

- Verify local connectivity before assuming a complete outage.
- Compare Finance results with HR or IT results.
- Confirm the destination servers are reachable from an unaffected network.
- Verify interface and routing health.
- Consider whether a policy can affect one source network while allowing others.
- Review traffic-filtering configuration only after narrowing the scope.
- Avoid removing security controls without first identifying the incorrect entry.