

Packet Tracer Lab 15

Internal Portal Access Failure Investigation

Incident ID: INC-1015

Difficulty

Intermediate

Estimated Time

20–40 Minutes

Skills Covered

- Extended ACL Troubleshooting
- Router-on-a-Stick Verification
- Inter-VLAN Routing
- DNS Validation
- HTTP Connectivity Testing
- Ping Testing
- Layer 3 Connectivity Verification
- Structured Troubleshooting Methodology

Scenario

Following scheduled security policy updates performed earlier in the day, multiple employees have reported they are unable to access the company's internal web portal.

Users report that internet access appears to be functioning normally and external websites remain accessible. Internal DNS resolution also appears to be working correctly.

BridgeOpsOne

The issue appears isolated to the internal BridgeOpsOne Corporate Portal.

You have been assigned to investigate the issue, restore access to the internal application, and validate that normal operations have been restored.

Customer Report

Reported By: Operations Department

Users Affected: Corporate Users

Business Impact:

Employees are unable to access the internal BridgeOpsOne Corporate Portal, preventing access to operational documentation, internal resources, and status information.

Issue Started:

Shortly after scheduled security policy changes.

Priority: Medium

Goal

- Identify the cause of the application access issue.
- Restore access to the internal BridgeOpsOne Corporate Portal.
- Validate internal and external web access.
- Document your findings.

Environment

The lab environment includes:

- Corporate User VLAN (VLAN 10)
- Internal Server VLAN (VLAN 20)
- Core Switch
- Router-on-a-Stick Gateway
- Internal DNS/Web Server
- Remote Office

BridgeOpsOne

- Public Web Server

Known Variables

- User workstations have valid IP configurations.
- Users can successfully reach their default gateway.
- Internet connectivity is operational.
- Public website access is functioning normally.
- DNS resolution is functioning correctly.
- The issue affects only the internal web application.
- Follow a structured troubleshooting methodology before making configuration changes.

Troubleshooting Mindset

During troubleshooting, think through the following questions:

- Does DNS resolve the internal website correctly?
- Can users communicate with their default gateway?
- Can users reach the internal server with ICMP?
- Is the issue affecting all network traffic or only one application?
- Could a security policy be blocking specific traffic?
- Have any recent security configuration changes impacted access?

Focus on identifying **which protocol is failing** instead of assuming the entire network is down.

Expected Outcome

By the end of this lab, users should successfully restore access to the internal BridgeOpsOne Corporate Portal.

BridgeOpsOne

Users should also be able to explain how an ACL can impact application traffic while allowing other network traffic to function normally.

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:

- Users unable to access the internal portal
 - External websites functioning normally
 - Investigation underway
-

2. Save Timeline Updates

Provide 2–3 operational updates describing:

- Investigation progress
- Validation performed
- Findings

Add updates to your Command Center timeline.

3. Create a Final Resolution Statement

Summarize:

- Root cause
- Corrective actions
- Current environment status
- Validation completed

BridgeOpsOne

Real-World Relevance

This issue simulates realistic troubleshooting commonly encountered in:

- Network Operations Centers (NOC)
- Enterprise IT
- Security Operations
- Network Engineering
- Help Desk Escalations

The purpose of this lab is to develop:

- Application troubleshooting skills
- Security policy validation
- Layer 3 troubleshooting
- Structured operational thinking
- Operational communication

Deliverables

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

- Explain the issue.
- Describe the troubleshooting methodology.
- Restore application access.
- Validate successful HTTP connectivity.
- Communicate findings clearly.

Hints

If you become stuck during troubleshooting, consider the following:

- Verify DNS resolution before assuming a web server failure.

BridgeOpsOne

- Compare internal and external website functionality.
- Verify gateway connectivity.
- Determine whether ICMP and HTTP behave differently.
- Review router security policies.
- Follow a structured troubleshooting methodology instead of guessing.