

Packet Tracer Lab 25

Major Incident Management Exercise

Incident ID: INC-1025

Difficulty

Advanced

Estimated Time

45–60 Minutes

Skills Covered

- Enterprise Incident Management
- Major Incident Communication
- Root Cause Analysis
- Enterprise Routing Validation
- Infrastructure Troubleshooting
- Service Restoration
- Executive Communication
- Customer Communication
- Timeline Documentation
- Incident Closure
- Structured Troubleshooting Methodology

Scenario

BridgeOpsOne

Major Incident Ticket

Priority

P1 (Critical)

Incident Title

Major Enterprise Services Outage

Status

Bridge Open

Reported By

Operations Monitoring Center (OMC)

Time Opened

08:17 AM

Incident Commander

You

Executive Summary

At approximately **08:17 AM**, multiple regional offices began reporting loss of access to centralized corporate services hosted at headquarters.

Although branch office users remain operational within their local environments, users are unable to access headquarters resources, business applications, and centralized services.

Due to the widespread impact across multiple sites, Operations has declared a **Priority 1 Major Incident**.

BridgeOpsOne

You have been assigned as the Incident Commander responsible for:

- Technical investigation
- Operational communication
- Service restoration
- Validation
- Incident closure

Customer Report

Reported By: Operations Monitoring Center

Users Affected:

Enterprise-wide

Business Impact

- Headquarters resources unavailable
- Corporate applications unavailable
- Internal file services unavailable
- Multiple departments impacted

Success Criteria

This incident is **NOT** considered complete until ALL of the following have been completed.

- ✓ Root Cause Identified
- ✓ Service Restored
- ✓ Enterprise Validation Completed
- ✓ Executive Update Created

BridgeOpsOne

- ✓ Customer Update Created
- ✓ Timeline Completed
- ✓ Resolution Summary Completed
- ✓ Incident Closed

Environment

- Headquarters Core Infrastructure
- Enterprise WAN
- Three Regional Branch Offices
- Layer 3 Core Switch
- Internal DNS Server
- Corporate File Server
- OSPF Dynamic Routing
- Multiple Workstations

Known Variables

- Branch office local connectivity remains operational.
- Users successfully communicate with their local default gateways.
- Headquarters resources are currently unavailable.
- Headquarters Server Network: **192.168.40.0/24**
- DNS Server: **192.168.40.10**
- File Server: **192.168.40.20**
- Finance Gateway: **192.168.10.1**
- HR Gateway: **192.168.20.1**

BridgeOpsOne

- IT Gateway: **192.168.30.1**
- Multiple regional offices report identical symptoms.
- Scheduled infrastructure maintenance completed immediately prior to the incident.
- Executive leadership has requested updates every **30 minutes**.
- Follow a structured troubleshooting methodology before making configuration changes.

Incident Expectations

This lab is designed to simulate a real enterprise Major Incident.

Students are expected to investigate the technical issue while maintaining operational communication throughout the incident lifecycle.

Successful completion includes both restoring service **and** communicating effectively with stakeholders.

Required BridgeOpsOne Workflow

Phase 1

Create an Initial Customer Update

Phase 2

Create an Executive Update

Phase 3

Document Timeline Updates

Minimum:

- Investigation Started

BridgeOpsOne

- Infrastructure Validated
 - Root Cause Identified
 - Service Restored
-

Phase 4

Create Resolution Summary

Phase 5

Close Incident

Real-World Relevance

This scenario simulates real incidents commonly encountered within:

- Enterprise Operations Centers
- Network Operations Centers
- Critical Infrastructure Teams
- Data Center Operations
- Enterprise Network Engineering
- Major Incident Management Teams

Deliverables

Students should submit:

- Initial Incident Update
- Executive Update
- Customer Update
- Timeline

BridgeOpsOne

- Root Cause Analysis
- Validation Results
- Resolution Summary
- Incident Closure Notes

Hints

- Validate local connectivity before assuming enterprise failure.
- Compare operational services with unavailable services.
- Verify interface status.
- Validate routing.
- Review recent maintenance activities.
- Use a structured troubleshooting methodology.
- Communicate throughout the investigation.