

BridgeOpsOne

Packet Tracer Lab 22 Solution Guide

Network Segmentation Failure Investigation

Incident ID: INC-1022

Objective

This lab focuses on identifying and resolving a department-specific communication failure following scheduled network policy maintenance.

Finance users can reach their local gateway and other departmental networks, but they cannot access centralized DNS and file services. Other departments and branch offices remain fully operational.

The objective is to use comparative testing and structured troubleshooting to distinguish a traffic-policy problem from a routing, VLAN, server, or WAN failure.

Root Cause

An incorrect extended access control list entry was configured on SW-HQ-CORE and applied inbound to the Finance VLAN 10 interface.

```
deny ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
```

The rule blocked all IP traffic originating from the Finance network (192.168.10.0/24) and destined for the headquarters server network (192.168.40.0/24).

Because the ACL was applied inbound on VLAN 10, Finance traffic was denied as it entered the multilayer switch. Routing, OSPF, VLAN interfaces, and the destination servers remained operational.

Symptoms Observed

- Finance default gateway reachable at 192.168.10.1.
- Finance communication with HR and IT remains operational.
- Finance cannot reach DNS server 192.168.40.10.
- Finance cannot reach file server 192.168.40.20.
- HR, IT, and branch users can reach the same servers.
- All VLAN interfaces remain up/up.
- OSPF neighbor relationships and routing entries remain healthy.

Troubleshooting Process

Step 1 — Verify Finance IP Configuration

From PC-FINANCE, review the workstation configuration:

```
ipconfig
```

Verify the expected address, subnet mask, and default gateway:

BridgeOpsOne

- IP address: 192.168.10.10
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.10.1

Step 2 — Verify Local and Cross-Department Connectivity

```
ping 192.168.10.1
ping 192.168.20.10
ping 192.168.30.10
```

These tests should succeed, confirming that Finance switching, its gateway, and general inter-VLAN routing are operational.

Step 3 — Test Centralized Services from Finance

```
ping 192.168.40.10
ping 192.168.40.20
```

Both tests should fail. The response may originate from 192.168.10.1, indicating the Finance gateway is reachable but cannot forward the denied traffic to the server network.

Step 4 — Compare with an Unaffected Department

From PC-HR or PC-IT, test the same file server:

```
ping 192.168.40.20
```

This should succeed. The destination server and server VLAN are therefore operational, and the issue is isolated to Finance-originated traffic.

Step 5 — Validate Interfaces and Routing

On SW-HQ-CORE and R-HQ, review infrastructure health:

```
show ip interface brief
show ip route
show ip ospf neighbor
```

The relevant VLAN interfaces should be up/up, the server route should be present, and OSPF relationships should remain established.

Step 6 — Review Access Control Policies

On SW-HQ-CORE:

```
show access-lists
show ip interface vlan 10
```

Identify SERVER_ACCESS as the inbound ACL on VLAN 10 and locate the incorrect deny entry. Match counters may increase as Finance tests the blocked destinations.

Commands Used

```
ipconfig
ping
show ip interface brief
show ip route
```

BridgeOpsOne

```
show ip ospf neighbor
show access-lists
show ip interface vlan 10
show running-config
configure terminal
ip access-list extended SERVER_ACCESS
no 10
write memory
```

Resolution

Remove the incorrect deny entry while preserving the named ACL and its remaining permitted traffic policy.

On SW-HQ-CORE:

```
configure terminal
ip access-list extended SERVER_ACCESS
no 10
exit
end
write memory
```

The existing permit ip any any entry remains in place, allowing Finance traffic to reach the server network again.

Validation

Successful resolution should include:

- Finance can ping its default gateway 192.168.10.1.
- Finance can ping DNS server 192.168.40.10.
- Finance can ping file server 192.168.40.20.
- Finance retains communication with HR and IT.
- HR, IT, and branch connectivity remains operational.
- All VLAN interfaces remain up/up.
- OSPF neighbors remain established and routes remain present.
- show access-lists no longer displays the incorrect Finance-to-server deny entry.

Key Takeaways

- Healthy routing does not guarantee that traffic is permitted.
- Compare affected and unaffected users to narrow the scope quickly.
- Extended ACL placement and direction determine which traffic is evaluated.
- A source-specific policy can block one department while all other networks remain healthy.

BridgeOpsOne

- Do not remove an entire security control when only one incorrect entry requires correction.
- Validate both service restoration and the continued operation of unaffected networks.
- Follow a structured troubleshooting methodology before changing policy.

Real-World Relevance

This type of issue is commonly encountered after firewall, ACL, microsegmentation, or network-access policy changes in enterprise environments.

Network and security teams must distinguish intended segmentation from accidental service disruption, verify the exact source and destination affected, and correct only the improper policy entry.