

Packet Tracer Lab 18 Solution Guide

Routing Loop Investigation

Incident ID: INC-1018

Objective

This lab focuses on identifying and resolving a routing loop affecting communication from headquarters to the branch office after scheduled WAN maintenance.

The environment retains operational interfaces and healthy OSPF neighbor relationships, but traffic destined for the branch network repeatedly circulates between R-EDGE and R-WAN-HQ instead of continuing toward R-BRANCH.

The objective is to use a structured troubleshooting methodology, identify the route-selection problem, remove the incorrect configuration, and validate the restored forwarding path.

Root Cause

A temporary static route remained configured on R-WAN-HQ after the maintenance window:

```
ip route 192.168.60.0 255.255.255.0 10.10.2.1
```

This route directs branch-bound traffic from R-WAN-HQ backward to R-EDGE. R-EDGE still uses its valid OSPF route and forwards the same traffic to R-WAN-HQ. The packet therefore loops between the two routers until its TTL expires.

The static route has an administrative distance of 1, so it is preferred over the OSPF route, which has an administrative distance of 110.

BridgeOpsOne

Symptoms Observed

- Headquarters users can access local VLANs and SERVER01.
- Headquarters users cannot reach the branch LAN.
- Branch workstations can communicate locally.
- Router interfaces remain up.
- OSPF neighbors remain in the FULL state.
- Pings from headquarters to the branch time out.
- Traceroute alternates repeatedly between R-EDGE and R-WAN-HQ.
- R-WAN-HQ installs a static route for 192.168.60.0/24 instead of the OSPF route.

Troubleshooting Process

Step 1 - Verify Headquarters Local Connectivity

From HR-PC1, test the internal server:

```
ping 192.168.50.10
```

This should succeed. The first packet may time out while ARP resolves, but subsequent replies should be successful.

This confirms that HR-PC1, VLAN 10, trunking, router-on-a-stick, inter-VLAN routing, and the server VLAN remain operational.

Step 2 - Test Branch Connectivity

From HR-PC1, test BRANCH-PC1:

```
ping 192.168.60.10
```

This should fail, confirming that the issue is isolated to traffic traveling toward the branch network rather than a complete headquarters outage.

BridgeOpsOne

Step 3 - Trace the Packet Path

From HR-PC1, run:

```
tracert 192.168.60.10
```

The output should repeatedly alternate between the headquarters gateway and R-WAN-HQ, similar to:

```
192.168.10.1
10.10.2.2
192.168.10.1
10.10.2.2
```

The repeating hops identify a routing loop. Traffic reaches R-EDGE, is forwarded to R-WAN-HQ, and is then sent back to R-EDGE.

Step 4 - Verify Interface and OSPF Health

On the routers, review interface state and OSPF neighbors:

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

Interfaces should be operational, and R-WAN-HQ should show neighbors 1.1.1.1 and 3.3.3.3 in the FULL state.

This rules out a physical WAN failure and an OSPF adjacency failure. It also reinforces that a healthy routing protocol does not guarantee that the preferred route is correct.

Step 5 - Inspect the Selected Route

On R-WAN-HQ, run:

```
show ip route 192.168.60.0
```

The output identifies the route as static and points to the incorrect next hop:

```
Known via "static", distance 1
* 10.10.2.1
```

A full routing-table review also shows:

```
S 192.168.60.0/24 [1/0] via 10.10.2.1
```

BridgeOpsOne

Step 6 - Review the Running Configuration

On R-WAN-HQ, run:

```
show running-config
```

Locate the following line:

```
ip route 192.168.60.0 255.255.255.0 10.10.2.1
```

This is the primary indicator of the root cause. The next hop 10.10.2.1 is R-EDGE, which sends branch traffic back toward R-WAN-HQ using OSPF.

Commands Used

```
ping 192.168.50.10
ping 192.168.60.10
tracert 192.168.60.10
show ip interface brief
show ip ospf neighbor
show ip route
show ip route 192.168.60.0
show running-config
configure terminal
no ip route 192.168.60.0 255.255.255.0 10.10.2.1
copy running-config startup-config
```

Resolution

Access R-WAN-HQ and remove the incorrect temporary static route:

```
enable
configure terminal
no ip route 192.168.60.0 255.255.255.0 10.10.2.1
end
copy running-config startup-config
```

After removal, R-WAN-HQ should reinstall the valid OSPF route toward R-BRANCH:

```
O 192.168.60.0/24 [110/65] via 10.10.3.2, Serial0/0/0
```

BridgeOpsOne

Validation

Successful resolution should include:

- Successful ping from HR-PC1 to 192.168.50.10.
- Successful ping from HR-PC1 to 192.168.60.10.
- Successful ping from headquarters workstations to BRANCH-PC2 at 192.168.60.11.
- Successful bidirectional communication between headquarters and branch systems.
- OSPF neighbors remaining FULL.
- The branch route appearing as OSPF rather than static on R-WAN-HQ.
- Traceroute following the intended path without repeated hops.

Expected healthy traceroute from HR-PC1 to BRANCH-PC1:

```
1  192.168.10.1
2  10.10.2.2
3  10.10.3.2
4  192.168.60.10
```

Key Takeaways

- Static routes normally have a lower administrative distance than OSPF routes and therefore take precedence.
- An OSPF neighbor relationship can remain healthy while traffic follows an incorrect route.
- Traceroute is one of the clearest tools for recognizing a forwarding loop.
- Repeated router addresses indicate that packets are returning to devices they have already visited.
- Local connectivity should be validated before assuming a complete network outage.
- Route source codes and next-hop addresses must be reviewed together.
- Temporary maintenance configurations should be documented, removed, and validated before a maintenance window is closed.
- Always perform end-to-end testing after a routing change.

Real-World Relevance

This failure pattern is common in enterprise networks when temporary routes, legacy routes, or incorrect next-hop entries override a dynamic routing protocol. Network engineers must distinguish between protocol health and forwarding correctness, especially after maintenance activity.