

Packet Tracer Lab 16 Solution Guide

External Service Connectivity Problem

Incident ID: INC-1016

Objective

This lab focuses on identifying and restoring outbound connectivity following scheduled network maintenance.

Although users can successfully access internal resources and communicate with internal servers, all attempts to access external/public services fail.

The objective is to troubleshoot the issue using a structured methodology, identify the root cause, restore external connectivity, and validate successful communication with public resources.

Root Cause

The NAT overload (PAT) configuration on **R-EDGE** was removed during scheduled maintenance.

Specifically, the following command was missing:

`ip nat inside source list 1 interface GigabitEthernet0/1 overload`

Without NAT overload configured:

- Internal devices could communicate with local resources.
- Traffic destined for public networks was not translated.
- External devices could not return traffic to private IP addresses.
- Users were unable to access public services.

Symptoms Observed

- Internal resources accessible.
- Internal DNS functioning normally.
- Users can reach their default gateway.
- Users can communicate with internal servers.

BridgeOpsOne

- Public website inaccessible.
- External IP addresses unreachable.
- No active NAT translations generated.

Troubleshooting Process

Step 1 — Verify Internal Connectivity

From PC-HR:

```
ping 192.168.20.100
```

This should succeed.

This confirms:

- Local switching is operational.
- Internal routing is functioning.
- Internal server connectivity is available.

Step 2 — Verify External Connectivity

Attempt to reach the public web server.

Example:

```
ping 203.0.113.10
```

or

```
ping bridgeopsone.com
```

Both tests should fail.

This confirms the issue is isolated to outbound/public communication.

Step 3 — Verify Routing

On R-EDGE verify routing information.

Example:

```
show ip route
```

BridgeOpsOne

Users should observe that routing appears normal.

This helps eliminate routing as the primary issue.

Step 4 — Verify NAT Configuration

Review the NAT configuration on **R-EDGE**.

Example:

```
show running-config
```

Verify the NAT overload configuration is present.

Users should identify that the following command is missing:

```
ip nat inside source list 1 interface GigabitEthernet0/1 overload
```

This is the primary indicator of the issue.

Step 5 — Verify NAT Operation

Example commands:

```
show ip nat translations
```

```
show ip nat statistics
```

Users should observe:

- No active translations.
- Little or no NAT activity.

This confirms outbound traffic is not being translated.

Commands Used

BridgeOpsOne

ping

show ip route

show running-config

show ip nat translations

show ip nat statistics

configure terminal

write memory

Resolution

Restore the missing NAT overload configuration.

On **R-EDGE**:

conf t

ip nat inside source list 1 interface GigabitEthernet0/1 overload

end

write memory

Validation

Successful resolution should include:

- Successful communication with internal resources.
- Successful ping to **203.0.113.10**.
- Successful ping to **bridgeopsone.com**.
- Active NAT translations displayed.
- External connectivity restored for corporate users.

BridgeOpsOne

- Successful DNS resolution of bridgeopsone.com.

Key Takeaways

- NAT is required for private networks to communicate with public networks.
- Internal connectivity does not guarantee Internet connectivity.
- Compare working services with non-working services before making assumptions.
- Verify NAT translations when troubleshooting outbound connectivity.
- Follow a structured troubleshooting methodology.
- Validate successful connectivity after completing repairs.