

PAT (Port Address Translation)

PAT is a type of NAT. While NAT typically manages IP addresses, PAT goes a step further by managing both IP addresses and port numbers. This is why PAT is sometimes called "NAT overload." Here's how it works:

Port Number Usage: PAT uses unique port numbers on the outgoing public IP address to distinguish between different private IP addresses and sessions initiated by multiple devices within the local network.

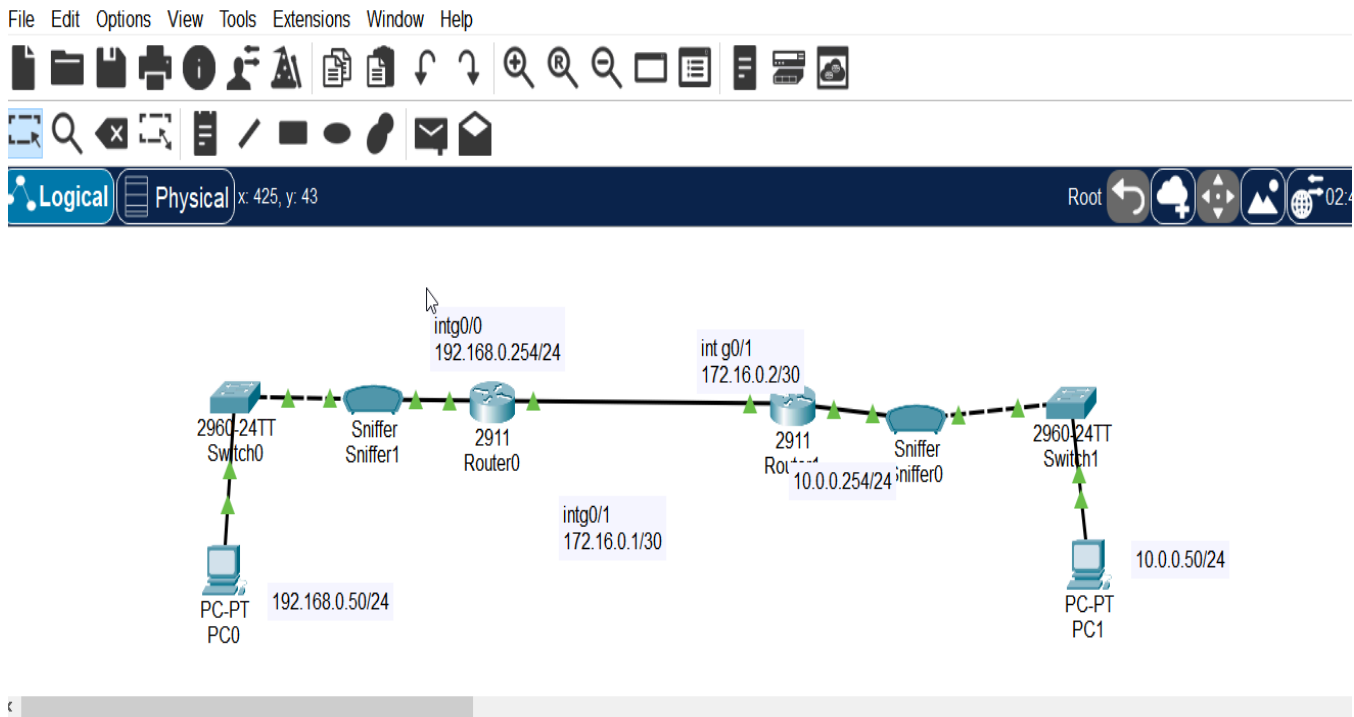
Efficiency: With PAT, many devices can use one public IP address, but they are differentiated by their port numbers. For example, your laptop and phone could both access different websites from the same public IP address. The router uses different port numbers to keep track of which traffic belongs to which device.

Practical Example

Imagine you have several smartphones, laptops, and smart devices in your home, all connected to the internet via one router. When any of these devices access the internet, the router uses NAT to translate the private IP addresses to its single public IP address. With PAT, it also assigns different port numbers to each device's internet session. Thus, when data returns to the router, it knows exactly which device to send it to based on these port numbers.

In summary, NAT and PAT are essential for efficient and secure internet connectivity in networks with limited public IP addresses. They allow multiple devices to share a single public IP address, help conserve the limited number of available public IP addresses, and enhance privacy by hiding internal network details from the external world.

PAT Lab Configuration



The detailed explanation provided is a walkthrough of setting up a basic network configuration using Cisco's Packet Tracer, a simulation tool for networking practice. Here, the setup includes two routers, two switches, PCs, and network sniffers to monitor traffic. This initial configuration serves as a foundation for future Network Address Translation (NAT) tutorials. Let's break down the key steps and elements in simpler terms:

1. Choosing Devices

- Routers: Two Cisco 2911 routers are selected for directing traffic between networks.
- Switches: Two Cisco 2960 switches are used, allowing devices on the same network to communicate efficiently.

- PCs: Two PCs are included, each representing a different local area network (LAN).
- Sniffers: Network sniffers are set up to analyze and debug network traffic.

2. Setting IP Schemes

- Each LAN has a unique IP address scheme to avoid overlaps and ensure clear network segmentation:
 - LAN on the left uses IP addresses starting with 192.168.0.x.
 - The other LAN uses the 10.0.0.x range.

3. Interface Configuration

- Each router has multiple interfaces configured:
 - Router 1: One interface set to 192.168.0.254 (acting as a gateway for the first LAN) and another set to 172.16.0.2/30 (connecting to Router 2).
 - Router 2: One interface set to 172.16.0.1/30 (connecting to Router 1) and another set to 10.0.0.254 (gateway for the second LAN).

4. Connection Setup

- Devices are physically linked using appropriate cabling in Packet Tracer, symbolized by the lightning bolt tool. PCs are connected to their respective switches, and routers are interconnected.

5. Configuring IP Addresses

- Each PC's network settings are configured with an IP address and a default gateway matching its network's scheme.

6. Routing Protocol Configuration

- IBGP (Internal Border Gateway Protocol): A simple routing protocol setup allows the routers to exchange information about the networks they are connected to, ensuring that devices across different LANs can communicate.

7. Testing Connectivity

- By using the command prompt on the PCs, you can ping devices across LANs to test connectivity and ensure that the routing protocol is functioning as expected.

8. Saving the Configuration

- The entire setup is saved in Packet Tracer. This saved file acts as a template for future NAT configuration exercises, allowing you to reuse the setup without reconfiguring from scratch.

Prerequisites

- Ensure Cisco Packet Tracer is installed and open the necessary project file.
- Prepare at least two PCs and a router in your Packet Tracer topology.

Step 1: Disable ARP for the Network

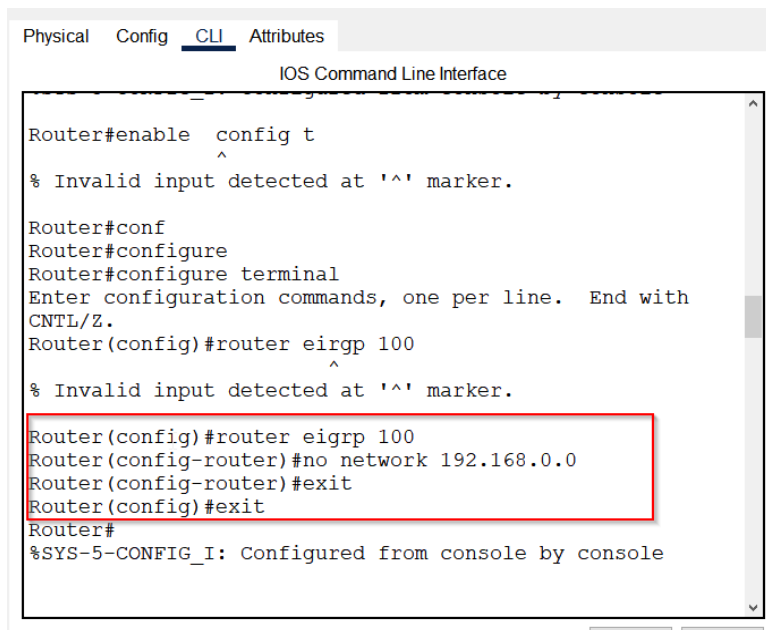
Select the router in your Packet Tracer topology.

Enter Global Configuration Mode:

enable

configure terminal

Disable ARP for the specific interface connected to the internal network:



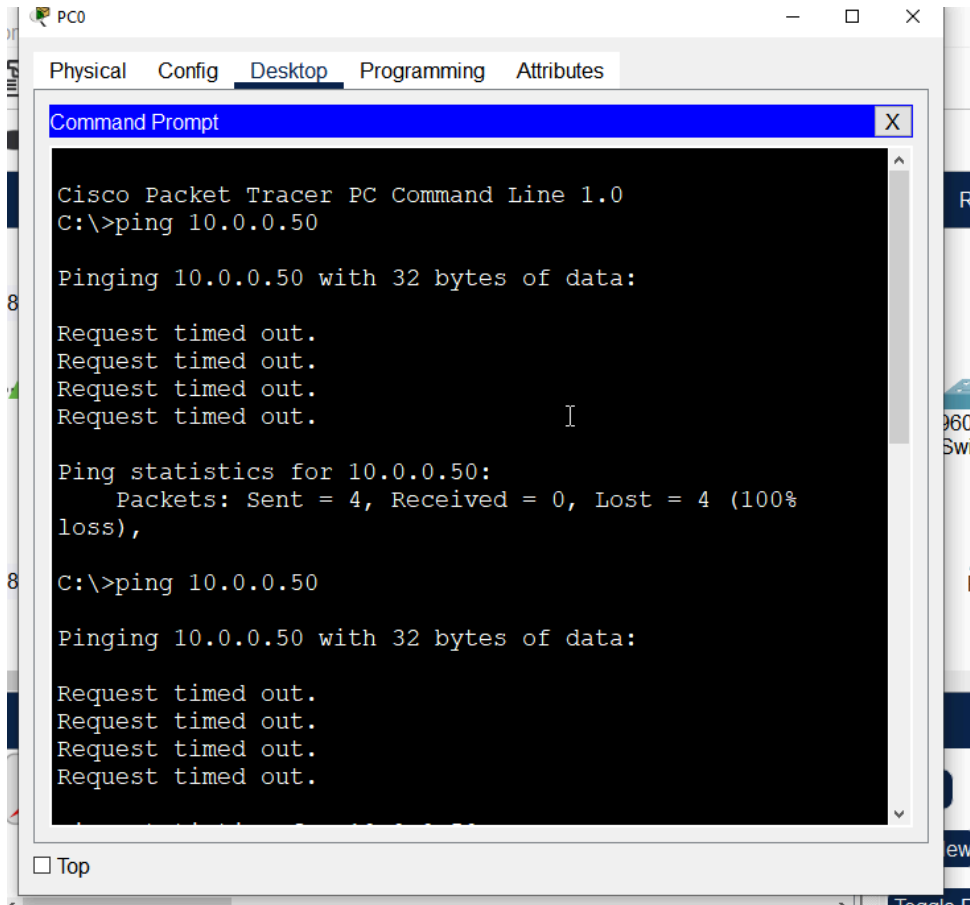
```
Physical  Config  CLI  Attributes
IOS Command Line Interface

Router#enable  config t
      ^
% Invalid input detected at '^' marker.

Router#conf
Router#configure
Router#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#router eigrp 100
      ^
% Invalid input detected at '^' marker.

Router(config)#router eigrp 100
Router(config-router)#no network 192.168.0.0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Verify that ARP is disabled by trying to ping another internal device and ensuring it fails.



Step 2: Configure NAT/PAT on the Router

Define the inside and outside interfaces for NAT:

```
Router>
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip nat inside
      ^
% Invalid input detected at '^' marker.

Router(config-if)#ip nat inside
Router(config-if)#int g0/01
Router(config-if)#ip nat outside
Router(config-if)#exit
```

Step 3: Create an Access List

Adjust the IP range and wildcard mask as necessary for your network.

```
Router(config)#ip access-list standard INSIDE-NET
Router(config-std-nacl)#permit 192.168.0.0 0.0.0.255
Router(config-std-nacl)#exit
```

T

Step 4: Configure NAT Pool

Define a NAT pool with a single IP address (the external IP used for PAT):

```
|Router(config)#ip nat pool SHARED-IP 172.16.0.1 172.16.0.1 netmask 255.255.255.255
```

Step 5: Enable PAT

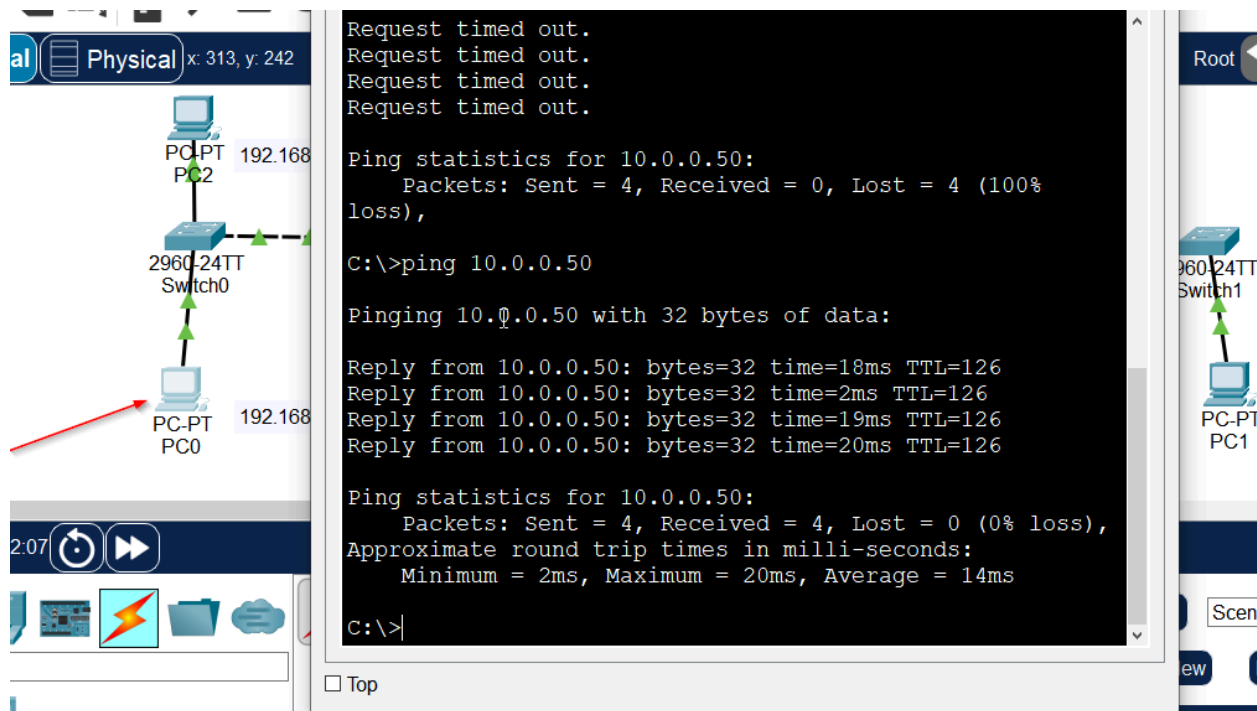
Link the access list and the NAT pool with overload to enable PAT:

```
|Router(config)#ip nat inside source list INSIDE-NET pool SHARED-IP overload
```

Step 6: Verify Configuration

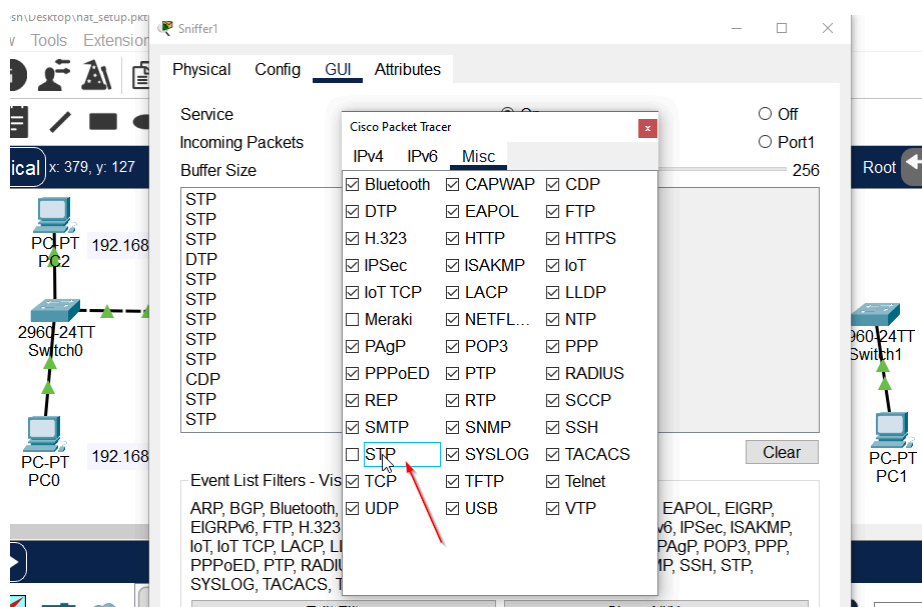
Test connectivity from your internal devices to an external address

Use an IP address that represents an external server.



Step 7: Adjust Monitoring Tools

Disable Spanning Tree Protocol (STP) and any sniffers or monitoring devices to reduce noise:



Conclusion

By following these steps, you've configured PAT on a Cisco router using Packet Tracer, allowing multiple devices in your network to share a single external IP address while maintaining unique sessions. This setup is crucial for conserving IP addresses and managing internal traffic outward to the Internet. Always verify your configuration to ensure everything is working as intended.