

Network / Port Address Translation

Overview

This lab exercise will introduce you to both network and port address translation (NAT and PAT) and how they are used to allow private internal IP addressing while providing access to the Internet for both client and server systems.

Objectives

Upon successful completion of this lab, you should be able to:

- Configure dynamic PAT on a router using an access list.
- Configure static PAT on a router.
- Examine and troubleshoot NAT and PAT operation.

Prerequisites

This lab builds on the skills covered in “Access Control Lists”. You should have successfully completed all of the tasks and procedures, and understood all of the commands and concepts introduced in that lab before attempting this lab.

Topology

Figure 1 illustrates the network topology that this lab will use.

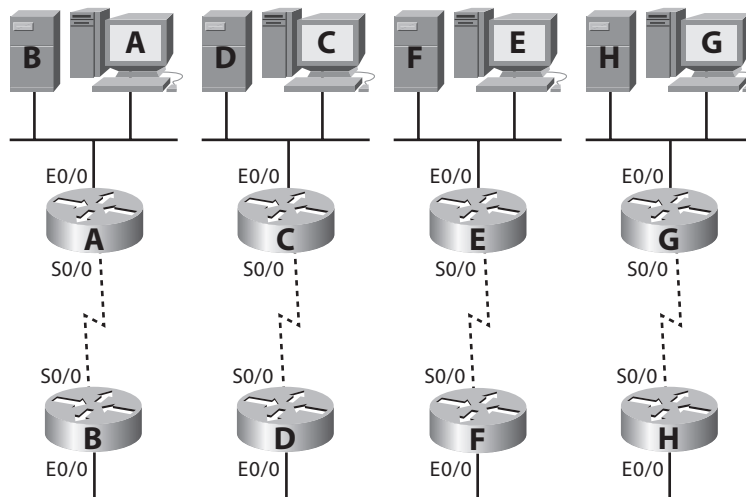


Figure 1 – Topology Diagram

Scenario

You will first attach your router to the lab network according to the specified topology. You will then configure your router’s interfaces with the specified IP addresses so you can communicate with the routers that are directly connected to you. After confirming that functionality, customer routers will be configured with a static default route and ISP routers will be configured with OSPF. You will then place one of your station workstations on your customer network and configure

the customer router with dynamic PAT to allow access to the lab Internet. Finally, you will configure your customer router with static PAT to allow access to the web server on one of your customer network workstations.

IP Addressing

Table 1 indicates the IP addressing that the systems in this lab will use.

Station	System	Role	Interface	IP Address	Subnet Mask
1 – Atlanta	2600 Router	Customer	Ethernet 0/0	192.168.1.1	255.255.255.0
			Serial 0/0	30.1.2.2	255.255.255.252
	Workstation	Client	Ethernet	192.168.1.200	255.255.255.0
2 – Burlington	2600 Router	ISP	Ethernet 0/0	150.10.10.2	255.255.255.0
			Serial 0/0	30.1.2.1	255.255.255.252
	Loopback 0	200.1.1.2	255.255.255.255		
Workstation	Server	Ethernet	192.168.1.100	255.255.255.0	
3 – Chicago	2600 Router	Customer	Ethernet 0/0	192.168.1.1	255.255.255.0
			Serial 0/0	30.3.4.2	255.255.255.252
	Workstation	Client	Ethernet	192.168.1.200	255.255.255.0
4 – Denver	2600 Router	ISP	Ethernet 0/0	150.10.10.4	255.255.255.0
			Serial 0/0	30.3.4.1	255.255.255.252
	Loopback 0	200.1.1.4	255.255.255.255		
Workstation	Server	Ethernet	192.168.1.100	255.255.255.0	
5 – Eugene	2600 Router	Customer	Ethernet 0/0	192.168.1.1	255.255.255.0
			Serial 0/0	30.5.6.2	255.255.255.252
	Workstation	Client	Ethernet	192.168.1.200	255.255.255.0
6 – Flagstaff	2600 Router	ISP	Ethernet 0/0	150.10.10.6	255.255.255.0
			Serial 0/0	30.5.6.1	255.255.255.252
	Loopback 0	200.1.1.6	255.255.255.255		
Workstation	Server	Ethernet	192.168.1.100	255.255.255.0	
7 – Gorham	2600 Router	Customer	Ethernet 0/0	192.168.1.1	255.255.255.0
			Serial 0/0	30.7.8.2	255.255.255.252
	Workstation	Client	Ethernet	192.168.1.200	255.255.255.0
8 – Houston	2600 Router	ISP	Ethernet 0/0	150.10.10.8	255.255.255.0
			Serial 0/0	30.7.8.1	255.255.255.252
	Loopback 0	200.1.1.8	255.255.255.255		
Workstation	Server	Ethernet	192.168.1.100	255.255.255.0	

Table 1 – Lab IP Addressing

Procedure

The following tasks and steps will guide you through completion of this lab.

Task 1 Attach your 2600 router to the lab network according to the specified topology.

Step 1 Examine the topology diagram outlined in Figure 1 and determine who your directly connected neighbor routers are.

Step 2 Using the lab patch panels and the various types of data cables available, connect your router's Ethernet interface to the 2900 switch that the instructor specifies.

Step 3 Using the lab patch panels and the various types of data cables available, connect your router's serial interface to the appropriate neighbor router.

Task 2 Configure your router with IP addresses.

Step 1 Gain access to enable mode on your router and enter global configuration mode.

Step 2 Set your router's hostname to correspond with your station name as listed in Table 1.

Step 3 Enter interface configuration mode for each of the interfaces specified in Table 1 and set the IP address accordingly.

Step 4 Confirm connectivity by pinging your directly connected neighbor routers.

Step 5 If you are an ISP, confirm loopback connectivity by pinging your router's loopback interface.

Step 6 Confirm Ethernet connectivity by pinging your router's Ethernet interface.



Don't continue to the next task until you are able to ping all of your directly connected neighbor routers, your router's loopback interface (if applicable), and your router's Ethernet interface.

Task 3 If you are an ISP, configure your router to use OSPF.

Step 1 Enable OSPF on all of your router's interfaces (including loopback), place them in Area 0, and force the OSPF router ID to be your loopback interface.

Step 2 Ensure that your router's serial interface does not send out OSPF Hello messages.

Step 3 If you are confident that you have configured OSPF correctly, confirm that your router has full connectivity within the lab network by pinging every public IP address.

Task 3 If you are a customer, configure your router with a static default route.

Step 1 In global configuration mode, enter a static default route with your ISP as the next hop interface or IP address.

Step 2 If you are confident that you have configured your default route correctly, confirm that your router has full connectivity within the lab network by pinging every public IP address.



Don't continue to the next step until you are able to ping every public IP address within the lab network. If you are unable to ping some public IP addresses, use the troubleshooting skills you learned in previous labs to determine the issue. If other stations haven't reached this point yet, feel free to assist them.

Task 4 Attach one of your workstations to the lab network.

- Step 1** Using the lab patch panels and the various types of data cables available, connect your workstation's Ethernet interface to the 2900 switch that the instructor specifies.
- Step 2** Configure your workstation's Ethernet interface with the IP address specified in Table 1.
- Step 3** Set your workstation's default gateway to be the IP address of your router's Ethernet interface.
- Step 4** Confirm that your workstation has LAN connectivity by pinging your router's Ethernet interface and your neighbor workstation.
- Step 5** If your LAN connectivity test is successful, confirm that your workstation has its default gateway configured correctly by pinging your LAN router's serial IP address.



Don't continue to the next step until your workstation is able to ping every device on its LAN and its LAN router's serial IP address. If some pings are unsuccessful, use the troubleshooting skills you learned in previous labs to determine the issue. If other stations haven't reached this point yet, feel free to assist them.

Task 5 If you are a customer, configure your router with dynamic PAT.

- Step 1** Configure your router with a standard named ACL called **NAT-THIS** that permits all IP traffic from your LAN and denies all other traffic.
- Step 2** Type `ip nat inside` within interface configuration mode for your router's Ethernet interface.
- Step 3** Type `ip nat outside` within interface configuration mode for your router's serial interface.
- Step 4** Type `ip nat inside source list NAT-THIS interface Serial 0/0 overload` in global configuration mode to enable dynamic PAT using your router's serial IP address for any LAN-originated traffic.

Task 6 Test and examine dynamic PAT.

- Step 1** Confirm that dynamic PAT is working by pinging every public IP address from your workstation.
- Step 2** If you are a customer, type `show ip nat translations` at the enable prompt to view the NAT/PAT translation table.

Task 7 If you are a customer, configure your router with static PAT.

- Step 1** Type `ip nat inside source static tcp 192.168.1.100 80 interface Serial 0/0 80` in global configuration mode to enable static PAT that will forward any traffic sent to your router's serial IP address on the HTTP port to your LAN's web server.
- Step 2** Once again, type `show ip nat translations` at the enable prompt and examine the resulting output.

Task 8 Test and examine static PAT.

Step 1 Confirm that static PAT is working by using your workstation to browse to the web server at every customer's serial IP address.

Step 2 If you are a customer, examine the NAT/PAT table again.

Step 3 Your instructor will lead you through the installation and configuration of various network services on your workstation.

Task 9 Submit your work to the instructor (one email per station.)

Step 1 Attach a text file with your 2600 configuration to an email to your instructor with a subject of **Lab 9 - Station-Name Configuration**. The body should contain the date, your station name, the lab name, and the names of anyone at your station.



If your station does not email your configurations to the instructor along with the information specified, you and your lab partners will receive a zero for the lab.

Discussion

Network and port address translation allow the conservation of public IP addresses by providing a means to arbitrarily translate traffic based on a wide variety of criteria. NAT and PAT can also be used to obfuscate and firewall systems that shouldn't be directly connected to the Internet for security reasons. Although most consumer-grade routers perform this functionality by default, on a Cisco router there is a bit more work involved. However, the increased level of control and flexibility available with enterprise-class routers far outweighs the inherent complexity required to configure NAT and PAT when compared to consumer-grade equipment.

Questions

1. How does dynamic PAT differ from static PAT?

2. In this lab we only performed source address translation. Can you think of a real-world scenario where destination address translation would be required?

3. If you enabled dynamic PAT on a Cisco router, would you need to apply an ACL to the interface connected to the Internet for filtering purposes?

Command Summary

The following table outlines the commands introduced in this lab.

Command	Description
<code>ip nat {inside outside}</code>	Designate an interface as either part of the inside group of NAT interfaces or the outside group of NAT interfaces.
<code>ip nat inside source list <i>ACL</i> interface <i>interface</i> [overload]</code>	Perform dynamic inside source network or port address translation. When traffic matches <i>ACL</i> it will be translated to the IP address associated with <i>interface</i> . If overload is specified, PAT will occur rather than NAT.
<code>show ip nat translations</code>	Display the NAT/PAT translation table.
<code>ip nat inside source static {tcp udp} <i>source-ip</i> <i>source-port</i> interface <i>interface</i> <i>dest-port</i></code>	Perform static inside source port address translation. Traffic sent to <i>dest-port</i> on the IP address associated with <i>interface</i> will be translated to <i>source-ip</i> and <i>source-port</i> and forwarded according to the routing table.