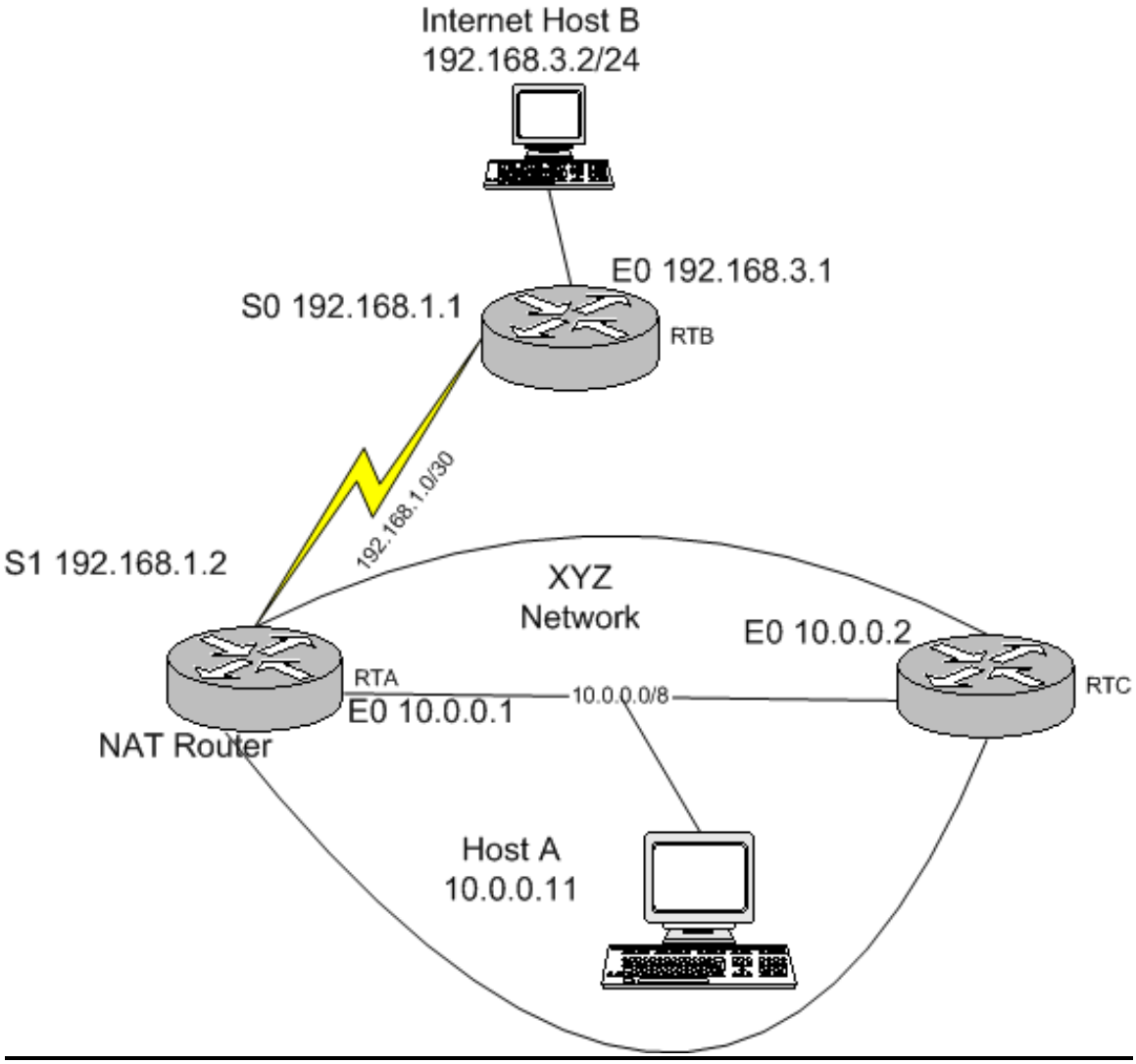
How NAT Utilizes ACLs



Objective:

In this lab you will configure dynamic NAT with overload on a Cisco router. You will also configure TCP Load Distribution.

Scenario:

Company XYZ's network consists of tow routers, RTA, and RTC. RTA is the boundary router that connects to the ISP. Only a single subnet has been allocated to address XYZ's network, 192.168.1.32/27. Because this subnet allows for only 30 hosts, XYZ decides to run NAT overload inside its network so that hundred of nodes can share those 30 addresses. In addition to configuring NAT overload, the company asked you to implement TCP load distribution so that outside web requests are distributed to different internal web servers.

Step 1:

Build and configure the network according to the diagram. This configuration requires the use of subnet zero, so you may need to enter the **IP subnet-Zero** command. Be sure to configure host A, and host B with static IP address according to the map.
Because RTA and RTB do not belong to the same autonomous system, you will not enable a routing protocol between them. Configure RTA to route all non local traffic to the ISP router (RTB):
RTA(config)#**IP route 0.0.0.0 0.0.0.0 192.168.1.1**
Also configure RTB with a static route to 192.168.1.32/27, the address block allocated to the company.
RTB(config)#**IP route 192.168.1.32 255.255.255.224 192.168.1.2**
Also configure RTC to use a default route to RTA:
RTC(config)# **IP route 0.0.0.0 0.0.0.0 10.0.0.1**

Verify that RTA can ping all devices. (At this point RTC should not be capable of pinging RTB, and vise versa. Why??).

Step 2:

You will configure RTA as a NAT router. RTA will translate addresses internal to XYZ (10.0.0.0/8)in to addresses allocated by the ISP (192.168.1.32/27). Because the company wants to maximize its allocated address space, a one-to-one static mapping will not suffice. You must configure dynamic NAT with overload

- Configure a NAT pool that will assign up to 25 addresses from the company allocated block (192.168.1.32/27): **RTA(config)#IP nat pool globalxyz 192.168.1.33 192.168.1.57 netmask 255.255.255.224.**
- You must also configure an ACL that will determine whether a received packet should be translated: RTA(config)# **access-list 1 permit 10.0.0.0 0.255.255.255**
- Finally assign this access list to the NAT pool and configure it for overload: **RTA(config)# IP nat inside source list 1 pool globalxyz overload**
- Configure e0 on RTA with the command **Ip nat inside**
- Configure s1 on RTA with the command **IP nat outside**

Step 3:

Test your dynamic NAT configuration. From xyz's host A, ping the ISP's host B. From RTC, also ping host B. Both pings should be successful. Troubleshoot if necessary
Next telnet to RTB on S1 from both RTC and XYZ's host A. Leave both sessions open and return to RTA's console. On RTA, enter the show **IP nat translations** command.

- Which global IP address is RTC using to reach RTB?
- Which address is Host A using to reach RTB?
- From RTB's perspective, how many different IP hosts is it communicating with?
- From RTA, issue the show **IP nat statistic**s command. What percentage of the available addresses are in use?

Step 4:

Your final configuration task is to set up NAT to use TCP load distribution. Company XYZ wants outside Web users directed in a round-robin fashion to two mirrored Web servers. For the purpose of this lab, RTA, and RTC will act as the redundant Web servers. Configure HTTP services on each using the following command: IP http server.

On RTA, configure a NAT pool and access list for TCP load distribution. The key word rotary is used to configure the round-robin distribution. The access list will identify the virtual address the outside browsers will request Web pages from, 192.168.1.60.

RTA(config)# **IP nat pool webservers 10.0.0.1 10.0.0.2 netmask 255.0.0.0 type rotary**
RTA(config)# **access-list 2 permit host 192.168.1.60**
RTA(config)#**IP nat inside destination list 2 pool webservers**

Test your configuration by running a web browser on host B, which is outside XYZ network. Point the browser to 192.168.1.60.

Not which router's web page loads in the browser window (look for its host name).

Click your Web browser refresh button. Which router's Web page appears after the refresh?