Packet Tracer - Examine NAT on a Wireless Router

Objectives

- Examine NAT configuration on a wireless router
- Set up 4 PCs to connect to a wireless router using DHCP
- Examine traffic that crosses the network using NAT

Instructions

Part 1: Examine the configuration for accessing external network.

1. Add 1 PC and connect it to the wireless router with a straight-through cable. Wait for all link lights to turn green before moving onto the next step or click Fast Forward.
2. On the PC, click Desktop. Select IP Configuration. Click DHCP to enable each device to receive an IP address via the DHCP on the wireless router.
3. Note the IP address of the default gateway. Close the IP Configuration when done.
4. Navigate to the web browser and enter the IP address of the default gateway in the URL field. Enter the username admin and password admin when prompted.
5. Click Status menu option in the upper right-hand corner. When selected, it displays the Router sub-menu page.
6. Scroll down the router page to the internet connection option. The IP address assigned here is the address assigned by the ISP. If no IP address is present (0.0.0.0 appears), close the window, wait for a few seconds and try again. The wireless router is in the process of obtaining an IP address from the ISP DHCP server.

Is this a private or public address?

Answer Area
Private IP address
Show Answer

Part 2: Examine the configurations for accessing the internal network.

1. Click Local Network within the Status sub-menu bar.
2. Scroll down to examine the Local Network information. This is the address assigned to the internal network.
3. Scroll down further to examine the DHCP server information, and range of IP addresses that can be assigned to connected hosts.

Are these private or public addresses?

Answer Area
Public IP address
Show Answer

1. Close the wireless router configuration window.

Part 3: Connect 3 PCs to the wireless router.

1. Add 3 more PCs and connect them to the wireless router with straight-through cables. Wait for all link lights to turn green before moving onto the next step or click Fast Forward.
2. On each PC, click Desktop. Select IP Configuration. Click DHCP to enable each device to receive an IP address via the DHCP on the wireless router. Close the IP Configuration when done.
3. Click Command Prompt to verify each device IP configuration using ipconfig /all command. Note: These devices will receive a private address. Private addresses are not able to cross the internet, therefore, NAT translation must occur.

Part 4: View NAT translation across the wireless router.

1. Enter Simulation mode by clicking the Simulation tab in the lower right-hand corner. The Simulation tab is located next to the Realtime tab and has a stopwatch symbol.
2. View traffic by creating a Complex PDU in Simulation mode:

   o From the Simulation Panel, click Show All/None to change visible events to none. Now click Edit Filters and under the Misc tab checkmark the boxes for TCP and HTTP. Close the window when done.
   o Add a Complex PDU by clicking on the opened envelope located in upper menu.
   o Click one of the PCs to specify it as the source.

3. Specify the Complex PDU settings by changing the following within the complex PDU window:

   o Under PDU Settings > Select Application should be set to: HTTP.
   o Click ciscolearn.nat.com server to specify it as the destination device.
   o For the Source Port, enter 1000.
   o Under Simulation Settings, select Periodic. Enter 120 seconds for the Interval.
   o Click Create PDU in the Create Complex PDU window.

Part 5: View the header information of the packets that traveled across the network.

1. Examine the headers of the packets sent between a PC and the web server.

   1. In the Simulation Panel, double click the 3rd line down in the event list. This displays an envelope in the work area that represents that line.
   2. Click the envelope in the work area window to view the packet and header information.
2. Click the Inbound PDU details tab. Examine the packet information for the source (SRC) IP address and destination IP address.
3. Click the Outbound PDU details tab. Examine the packet information for the source (SRC) IP address and destination IP address.
   Notice the change in SRC IP address.
4. Click through other event lines to view those headers throughout the process.
5. When finished, click Check Results to check your work.