Ellie Parobek
NSSA 290 Network Essentials for Developers
Lab Exercise – IP and Host Routing and Tracert

Lab Overview

We've talked about IP addressing and subnetting as well as network topologies. Using that knowledge, you will examine how a host determines where to send a packet on the network and what that packet looks like as it is encapsulated for the next hop.

What to Submit

Submit an individual set of answers to all the questions to the MyCourses dropbox.

Working Together

Please work with a partner for this lab, but submit your individual responses to the questions to the dropbox in MyCourses. Be sure to reference the guidelines for working together in groups that we previously discussed during class to help you.

Lab Setup and Nomenclature – Recall from Previous Lab Experiences

Each group of benches is identified as a Pod with a number; i.e. Pod 2. Each pod consists of two benches with a total of six machines. On one bench the PCs are numbered 1, 2, and 3. On the other bench the PCs are numbered 4, 5, and 6.

Activity 1: Host Routing Table Comparison to Predictions

Before beginning this exercise, reboot Windows on all three PCs. This will reset the machines in case anyone was using them before us.

- You can do this by clicking on the Windows icon  and then the restart button.

Verify the network settings for each of the three workstations on your bench using the ipconfig command in a dos window:
IP address: 10.140.100.table_host
Subnet mask: 255.255.255.0
Gateway: 10.140.100.254

- Use the command route print in the dos command window to look at the routing table for your workstation.
- Ignoring all of the lines for the virtual adapter (192.168.x.y), examine how your prediction table compares to what you are seeing on your PC.

Activity 1: Questions

1. Explain any differences between your predicted routing table and what you see on your workstation.

The metric numbers are very different along with many more network destinations also the gateway column all says "on-link"

2. What is the default route in the routing table on your workstation?

   10.140.100.254

3. What does “on-link” in the gateway field mean?

   Addresses that don’t need a gateway because they can be resolved locally.

   a. If you were to replace this with an IP address what would it be?

   127.0.0.1

4. What is the purpose of the metric field? Explain the numbers you are seeing in the table and how they relate to the routes in the routing table (provide your resource).

   The router will choose the direction of the gateway with the lowest metric. The number can be thought of as the ‘cost’ of the route.

Activity 2: Examining the Host Routing Table with a Local Destination

Next you will examine the encapsulation and routing table decisions by examining error messages resulting from your tests as well as packets in Wireshark.

- Start Wireshark and be sure to select the appropriate adapter to capture traffic.
- Ping the IP for a host that is on your own network while running Wireshark.
- Afterward you can stop the traffic capture to examine the messages and answer the questions below.

When looking at the Wireshark capture, expand the layers to see both the Ethernet header and the IPv4 packet and headers.

Activity 2: Questions

5. In the echo request, which destination MAC address is in the **Ethernet** header?
   broadcast ff:ff:ff:ff:ff:ff

6. In the echo request, which source MAC address is in the **Ethernet** header?
   HewlettP_45:11:26 ec:b1:d7:45:11:26

7. In the echo request, which destination IP address is in the **IP packet** header?

   10.140.100.255 (broadcast)

8. In the echo request, which source IP address is in the **IP packet** header?

   10.140.100.81

Activity 3: Examining the Host Routing Table with a Non-local Destination

- Ping cnn.com (noting that this IP address is off your local network).
- Examine the Wireshark capture and again look at the Ethernet header versus the IPv4 packet.

Activity 3: Questions

9. In the echo request, which destination MAC address is in the Ethernet header?

   IPv4mcast_7f:ff:fa 01:00:5e:7f:ff:fa

10. In the echo request, which source MAC address is in the Ethernet header?

    HewlettP_40:d9:fb ec:b1:d7:40:d9:fb

11. In the echo request, which destination IP address is in the IP packet header?

    239.255.255.250

12. In the echo request, which source IP address is in the IP packet header?
    10.140.100.83

Activity 4: Using Traceroute

From the dos command window use the tracert tool to examine the path from your computer to a destination.

- Tracert cnn.com
- Examine the output in the dos window.
- Examine the activity in Wireshark.

Activity 4: Questions

13. What is the purpose of tracert?

    Displaying the route and packet delays across an IP network.

14. Explain how tracert works?

Tracert sends ICMP echo packets to its destination and uses incrementing time to live values until the destination responds (or maximum TTL is reached). “Time Exceeded” messages are received which show the route.

15. What is the path that the packets took to get to cnn.com?

1 syscore-gw-netlab-vlan140.istlabs.rit.edu [10.140.100.254]
2 warpcore-pp-syscore.istlabs.rit.edu [10.255.4.1]
3 worf.istlabs.rit.edu [10.255.1.1]
4 129.21.26.254
5 rit-rtr001-pp-rtr070-vlan852.rit.edu [129.21.8.113]
6 rit-rit1-100g-pp-rtr001-vlan856.rit.edu [129.21.8.126]
7 xe-8-1-2.bar1.buffalo1.level3.net [4.59.214.21]
8 ae-0-11.bar1.cleveland1.level3.net [4.69.136.185]
9 4.14.76.50
10 151.101.193.67

16. Do another tracert to some other favorite site of yours. Explain the path, noting if it is different or the same as the previous path to cnn.com.

The first 6 routes were the same until it exits RIT’s network.