Lab 08: Action at Network Layer

OSL, Thu Mar 19, 2015

Objective:

1. Understand the operation of various mechansims/protocols that operate at network layer: IP fragmentation, ARP, DHCP, ICMP.

General instructions:

1. This lab is to be done in **groups of two students**
2. Download relevant files needed for this lab, available under "student-files.tgz"
3. Create a directory called <rollnumber1>_<rollnumber2>_lab08. As you proceed with the lab instructions below, note down observations or relevant output from whatever you do in a file named "lab08.txt" using a text editor.
4. **Also add to this directory any log files collected.** Name the files appropriately.
5. Read the exercise fully before experimenting
6. ***This lab has many exercises, but each exercise is rather small. Focus, to get it done on time.***
7. See below. I don't want you exploiting loopholes in the way questions are asked in this lab :)

Reference:

1. Man pages of the commands.
2. Man page of a new tool 'arping'
3. Video/slides of 'IP packet format', 'Obtaining IP Addresses' and 'Supporting Protocols', all under 'Network Layer'.

Lab Instructions:

Col. Protozoa wants to counter cyber attacks and has read up on network layer protocols. He wants to relate theory to practice. He has many questions, help him design the right experiments that will answer his questions. The colonel has little patience with irrelevant details, so ensure in each experiment that you capture the right set of packets.

Exercise 1: Adress Resolution Protocol (ARP) [30 min]

When Col. Protozoa read up on how packet forwarding is done at a host, he came to know that in cases where the destination IP address belongs to the host's own subnet, the packet goes directly, otherwise it goes via a router. He wants to check this out. Can you design an experiment that illustrates this. Also, he wants to know what happens if you try to send a packet to "a non existent host within the same subnet". Help him with that as well.

Guidance:

1. As the name of the exercise suggests, this experiment is about exploring the ARP protocol in the context of forwarding. You do not have permissions to delete or set the arp entries but you should be able to view the arp entries currently in the cache.
2. In all cases, you do NOT want the arp entry of the target in the cache. So, ensure this is the case.
3. When you are sending packets to a 'non existent host within the same subnet', do wait for atleast 10 sec before closing your packet capture tool. The underlying action in this case, takes time.
4. “Within subnet” -- hosts within OSL. “Outside subnet” -- hostel machines

Questions:

1. For the first case, where you sent packets to a host within the same subnet, specify the command sequence used. How many arp messages were exchanged? Does the arp entry correspond to the remote host IP address you contacted? Explain your observations.
2. For the second case, where you sent packets to a remote host outside the same subnet, specify the command sequence used. How many arp messages were exchanged? Does the arp entry correspond to the remote host IP address you contacted? Explain your observations.
3. For the third case where you sent packets to a non-existing host, specify the command sequence used. How many ARP attempts were made to resolve the non-existing IP address? After what time did ARP give up?

Exercise 2: Gratuitous ARP **[20 min]**

Col. Protozoa read that ARP is a good candidate for spoofing. An intruder can generate a gratuitous ARP advertising his MAC address and some one else's IP address and capture the some one's traffic. Given its relevance to security, he wants to know more about this aspect of ARP. Design an experiment to capture gratuitous ARPs.

Guidance:

1. 'arping' is a tool that generates gratuitous ARPs. Understand how this works.
2. Gratuitous ARPs can be sent as both ARP requests and ARP replies. Capture both types of packets via appropriate arguments.
3. Note, I am not asking you to implement the APR spoofing attack. You don't have permissions for that. Just play with gratuitous ARPs : MAC address and IP adress both will belong to your machine only.
4. The operation as you see in practice differs slightly from what was covered in the video. This is an implementation artifact, what matters is the concept.

Questions:

1. What command did you use to generate the required traces?
2. How is it ensured that the gratuitous ARPs reach all hosts within the physical network?
3. What difference did you observe when gratuitous ARP was sent as a request vs it being sent as a reply?

Exercise 3: IP Fragmentation **[20 min]**

The Colonel saw the IP packet format and is particularly fascinated by the fragmentation fields and wants to see it in action. Design an experiment where 1) No fragmentation occurs and 2) Fragmentation occurs.

Guidance:

1. "sendUDP.c" is a simple socket program (provided in the directory) that generates a single IP packet of a given size and sends it to the specified destination IP address. Compile the program and use it in your experiments.

Questions:

Answer the following questions in your report.

1. For the case when no fragmentation happened, note down the values corresponding to the following fields: Total length, Identifier, flags and fragment offset in your report.
2. For the case when fragmentation happened, for each fragment, note down the values corresponding to the following fields: Total length, Identifier, flags and fragment offset.

Exercise 4: Dynamic Host Configuration Protocol (DHCP) **[30 min]**

The Colonel is equally fascinated by how hosts obtain IP address and wants to look at the message exchange of this process. One of his staff already procured such a trace, help him interpret the trace.

Guidance:

1. Configuring IP addresses requires root permission. Since you do not have these privileges, for this exercise you will have to make do with a generated trace file "dhcp.out". This trace file was generated using tcpdump and running "dhclient" on a terminal with root permissions. Explore it via wireshark.

Questions:

Answer the following questions

1. What is the IP address of the DHCP server and on what port is it listening on?
2. Was any DHCP relay involved in forwarding the DHCP packets? How did you determine the answer.
3. When the DHCP server replied, which IP address did it reply to? And why?
4. What is the offered IP address to the client and for how long is this address valid?
5. Apart from the IP address, what additional information has the client received from the dhcp server?

Exercise 5: Internet Control Message Protocol (ICMP) **[30 min]**

The Colonel read about the different types of ICMP messages and wants to look at them in a packet trace. He wants to look at the following 3 types.

- Type 0, code 0
- Type 3, code 3
- Type 8, code 0

Design experiments that will produce ICMP messages of the above type in a packet trace.

Question: Which commands did you use to generate the above ICMP message types.

Exercise 6: More Internet Control Message Protocol (ICMP) [30 min]

The Colonel's collegue (who in far away as an undercover agent) often complains that he doesn't get time-critical messages on time. The colonel who now knows enough theory wants to debug this. He feels its likely due to too many routers in between and feels 'traceroute' is the right command to use. Help him interpret the output of the command.

Guidance:

1. When tracing the path to a host, select a host that is not on the same physical network as your machine. Otherwise, its too trivial with a hop count of 1.

Questions:

1. Specify the command used and cut/paste the output you saw.
2. What ICMP message type/code is involved in the process?
3. Explain how this command works by looking at the trace file and the output produced by running the command.
4. What is the IP address of your machine's default router?

Homework:

If you have root permissions and traceroute on your laptop try the following. Traceroute to say www.iitb.ac.in, you will not be able to, since intermediate routers drop these packets. Explore options of traceroute to see if you can make it work. Don't forget to collect the packet trace and explore what is happening.

Submission instructions

The directory named <rollnumber1>_<rollnumber2>_lab08 that you will submit should contain the files lab08.txt and the trace files corresponding to exercises 1, 2, 3, 5 and 6.

Tar the folder and upload it on moodle.