IT304
LAB 8
Analysis of IP packets through Wireshark and Introduction to static routing through packet tracer

1 To study and analyze IP Packets through Wireshark.

The Internet Protocol (IP) is the principal communications protocol used for relaying datagrams (packets) across an internetwork using the Internet Protocol Suite. Responsible for routing packets across network boundaries, it is the primary protocol that establishes the Internet. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering datagrams from the source host to the destination host solely based on their addresses. For this purpose, IP defines addressing methods and structures for datagram encapsulation.

IP packet header format is as shown in figure 1.

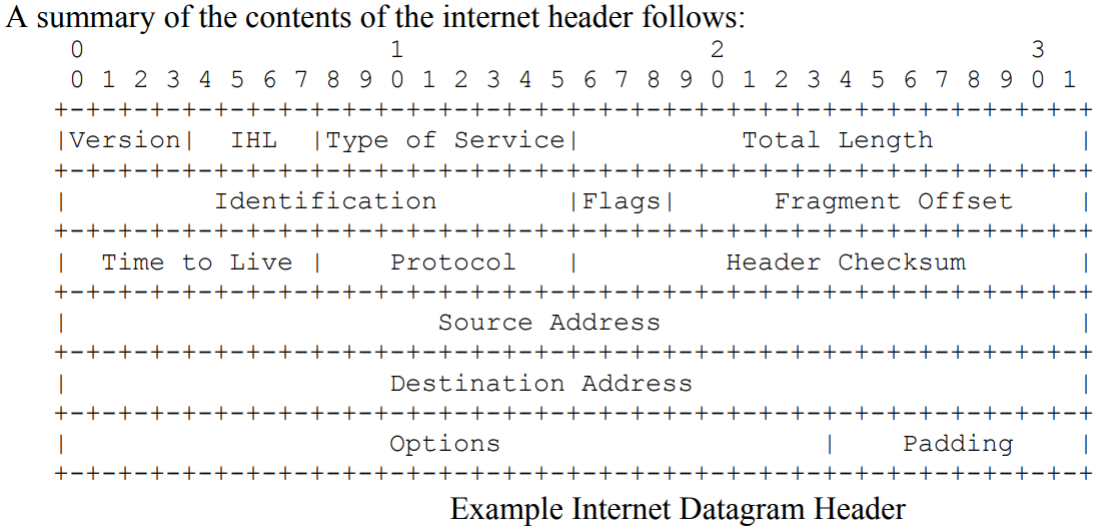

Figure 1: IP packet header format

1.1 Exercise

1. Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file ipethereal- trace-1.

2. In your trace, you should be able to see the series of ICMP Echo Request (in the case of Windows machine) or the UDP segment (in the case of Unix) sent by your computer and the ICMP TTL-exceeded messages returned to your computer by the intermediate routers.

3. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.

1.2 Questions

1. What is the IP address of your computer?
2. Within the IP packet header, what is the value in the upper layer protocol field?
3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

1.3 Exercise

1. Sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the "details of selected packet header" window. In the "listing of captured packets" window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent my other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

1.4 Questions

1. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?
2. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?
3. Describe the pattern you see in the values in the identification field of the IP datagram.
4. Next (with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to your computer by the nearest (first hop) router.
5. What is the value in the Identification field and the TTL field?
6. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

"Open the http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file ICMP-ethereal-trace-1.

1.5 Questions:

1. What is the IP address of your host? What is the IP address of the destination host?
2. Why is it that an ICMP packet does not have source and destination port numbers?
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Open http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file ICMP-ethereal-trace-2.

1.6 Questions

1. What is the IP address of your host? What is the IP address of the target destination host?
2. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?
3. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?
4. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?
5. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

2 Understanding IP addressing and static routing using packet tracer

Implement following topology in packet tracer.

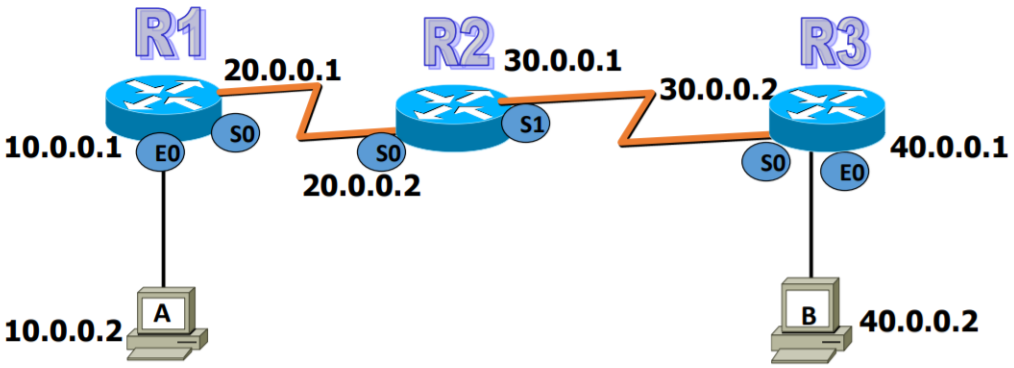

Figure 2: Caption

Steps to follow

1. drag and drop devices
2. configure IP addresses of PCs and also assign default gateway
3. Assign IP address to routers
4. Turn port ON for all routers

Try to ping from 10.0.0.2 to 40.0.0.2. Are you able to do it?
Now add static routes as shown in following image

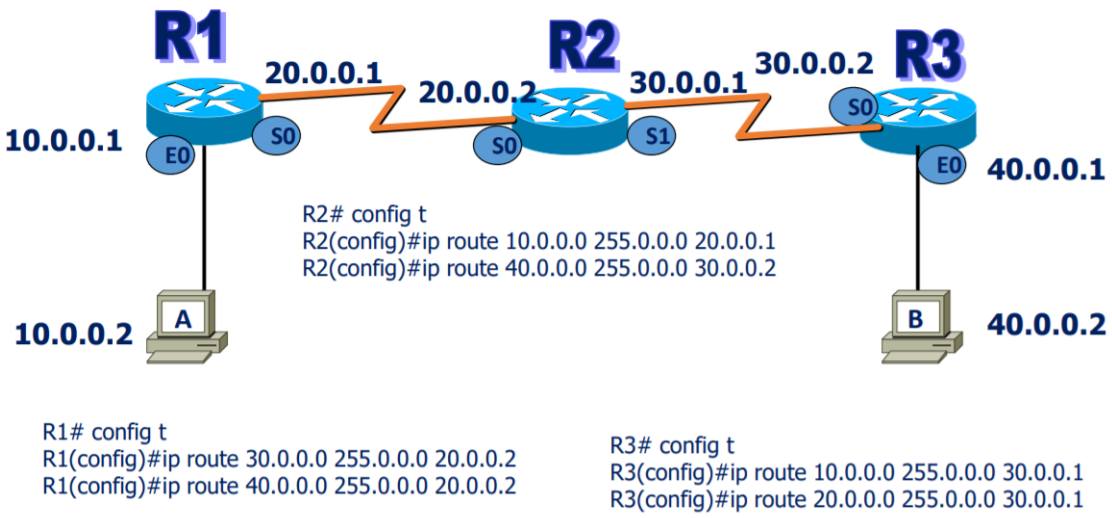

Figure 3: Caption

Now try to ping from 10.0.0.2 to 40.0.0.2
You can **see routing table** on each router by following command in CLI
Router#show ip route
if you are in config mode in CLI, exit from config mode and then run the above mentioned command
To remove a static route:

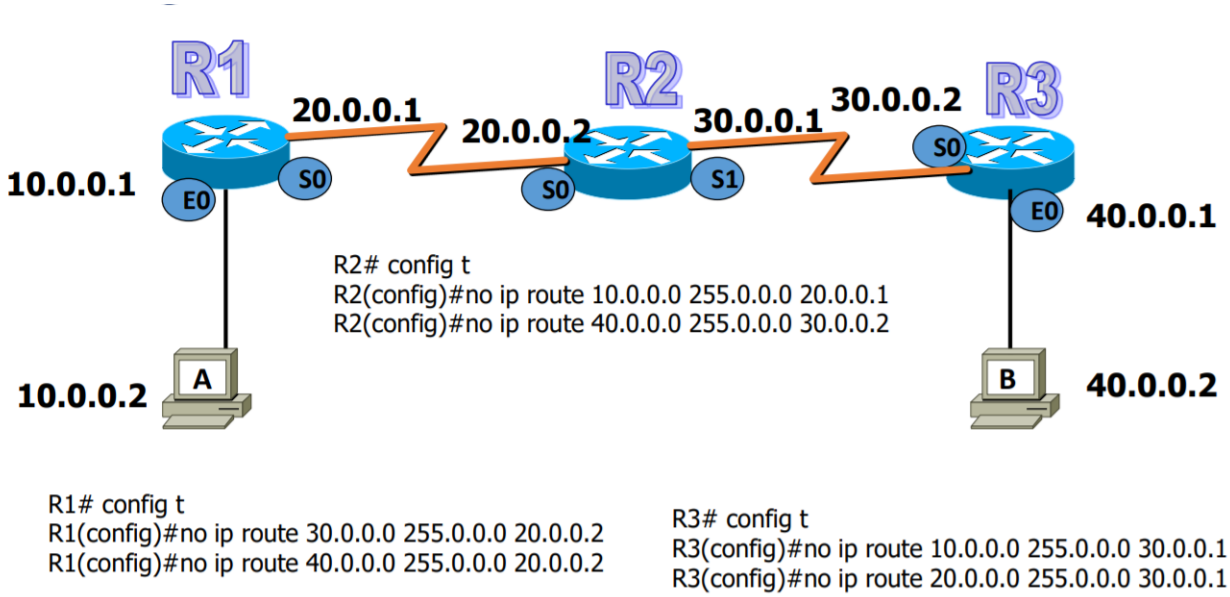

Figure 4: Caption

2.1 Exercise

Design a topology which have three networks. Each network has 4 PCs and all three network are connected to each other. The suggested IP ranges are 192.168.0.1 to 192.168.2.4. All IP addresses of all network should be from the given range. Run the experiment and ping from each network to every other Network. Take a snapshot and submit. Also submit the snapshot of topology with IP assigned to each PC.

3 Suggested reading

- `https://www.computernetworkingnotes.com/ccna-study-guide/static-routing-configuration-guide-wi`
  `html`