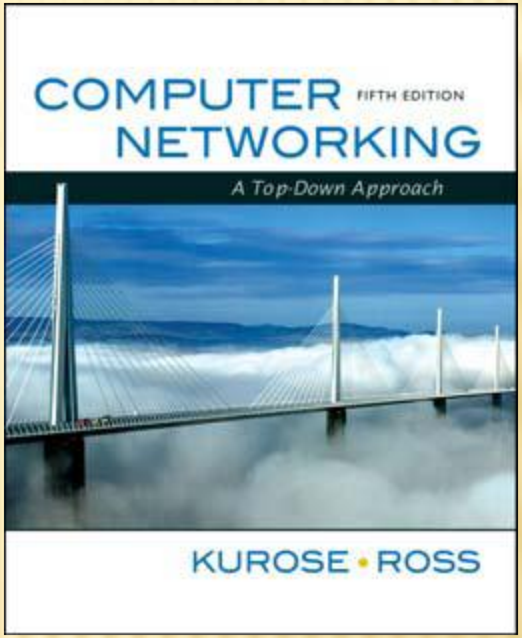

Computer Networking

LAB 6 - IP

1. CAPTURING PACKETS FROM AN EXECUTION OF TRACEROUTE

- first sending one or more datagrams with the TTL field in the IP header set to 1
- then sends a series of one or more datagrams towards the same destination with a TTL value of 2
- then sends a series of datagrams towards the same destination with a TTL value of 3
- and so on.

TRACEROUTE

- **Windows:** *pingplotter*, available both in free version and shareware versions at http://www.pingplotter.com.
- **Linux/Unix:** *traceroute* command, the size of the UDP datagram sent towards the destination can be explicitly set:
  - `%traceroute gaia.cs.umass.edu 2000`

STEPS

- Start up Wireshark and begin packet capture
- If you are using a Windows platform, start up *pingplotter* and enter the name of a target destination in the “Address to Trace Window.”
- Enter 3 in the “# of times to Trace” field
- Select the menu item *Edit->Advanced Options->Packet Options* and enter a value of 56 in the *Packet Size* field
- Then press the Trace button
- Stop Wireshark tracing.

2. A LOOK AT THE CAPTURED TRACE

- Select the first ICMP Echo Request message sent by your computer:

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?
4. Has this IP datagram been fragmented?

STEPS

- Sort the traced packets according to IP source address by clicking on the *Source* column header
- Select the first ICMP Echo Request message sent by your computer
- Expand the Internet Protocol portion in the “details of selected packet header” window
- Use the down arrow to move through the ICMP messages sent by your computer

QUESTIONS

5. Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by your computer?
6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?
7. Describe the pattern you see in the values in the Identification field of the IP datagram

QUESTIONS

- Find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router:

8. What is the value in the Identification field and the TTL field?
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

FRAGMENTATION

- Sort the packet listing according to time again by clicking on the *Time* column

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 2000. Has that message been fragmented across more than one IP datagram?

QUESTIONS

11. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?
12. What information in the second IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?
13. What fields change in the IP header between the first and second fragment?

QUESTIONS

- Now find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 3500

14. How many fragments were created from the original datagram?
15. What fields change in the IP header among the fragments?