Wire-shark IP Routing

Overview

I had three virtual computers operating simultaneously to do this investigation. Two Virtual Computers ran Ubuntu, while the third ran FREEBSD and served as a router between the two Ubuntu machines. Configured Set up two NAT Networks as required in the research and assigned each machine to the specified IP addresses. After everything was set up, I double-checked the IP addresses of both Ubuntu PCs by opening the terminal and entering ifconfig, which confirmed that both machines' networks were operational. I also used the ping command to send an ICMP packet to NAT Networks to ensure that both Ubuntu workstations were connected to the correct network. (See the list below.)

1. In the packet details window, expand the Internet Protocol section of the initial ICMP Echo Request message delivered by your machine. What is your computer's IP address?

• My computer's IP address is 10.0.3.4. I discovered this by looking at the "Source," where packets were transmitted from, so I know that's my IP address. "Src: 10.0.3.4" is also stated in the Internet Protocol version 4.

2. What is the value of the upper layer protocol field in the IP packet header?

• The value of the upper layer protocol field in the header is ICMP (1).

3. What is the size of the IP header in bytes? How many bytes are in the IP datagram's payload? Describe how you came up with the number of payload bytes.

• Because the IP header is 20 bytes long and the IP datagram is 60 bytes long, the payload is 40 bytes long. To find the number of payload bytes, subtract the IP header size, which is 20 bytes, from the entire length, which is 60 bytes, and the number of payload bytes remains.

4. Is it possible that this IP datagram has been fragmented? Describe how you decided if the datagram was fragmented or not.

• If the number of pieces equals zero, the data is not fragmented. I looked at the "Flags" drop-down, which controls whether a packet is fragmented or not, and "more fragments" was 0 in this case, as was Fragment offset.

5. In this series of ICMP signals generated by your computer, which fields in the IP datagram always change from one to the next?

• The time to live, the identification, and the header checksum are all constantly changing. Because the identifier is a unique number issued to each packet, it must vary regularly, causing the Header checksum and the Time to Live to change.

6. Which fields do not change? Which fields must remain constant? Which fields must be updated? Why?

The Following Fields Are Consistent Throughout IP Datagrams:

• Version (meanwhile we use IPv4 for all packs)

• The width of the header (since these are ICMP packets)

• IP address of the source (since we are sending from the same source)

• IP address of the destination (since we are sending to the same destination)

• Distinct Services (since all packets are ICMP, they use the same Type of Service class)

• Protocol for the Upper Layer (since these are ICMP packets)

The Following Fields Must Remain Constant:

• Version (meanwhile we use IPv4 for all packs)

• Source IP (because these are ICMP packets)

• Header length (since we are sending from the same source)

• IP address of the destination (since we are sending to the same dest)

• Distinct Services (since all packets are ICMP, they use the same Type of Service class)

• Protocol for the Upper Layer (since these are ICMP packets)

The Following Are The Fields That Need Change:

• Identifying you (IP packets must have different ids)

• It's time to live (traceroute increments each subsequent packet)

• Checksum in the header (since header changes, so must checksum)

7. Describe the pattern you detect in the IP datagram's Identification field's values.

• Every ICMP Echo (ping) query causes the IP header identifying fields to grow in length. I discovered this by browsing through each ICMP Echo request (ping) and observing the changes in the Identification field values.

8. What is the value of the TTL field and the Identification field?

- TTL:64
- Identification: 0x01a9(425)

9. Are these values consistent across all ICMP TTL-exceeded answers provided to your PC by the nearest (first hop) router? Why?

• Because the first-hop router is always the same, the TTL will not change. Because it has been allocated a unique value, the identification field for all ICMP TTL-exceeded answers will change. When two or more IP datagrams share the same identification value, they are fragments of a larger IP datagram.

10. Track down your machine's first ICMP Echo Request message after setting the Packet Size to 2000 in the ping plotter. Has the message been split up into many IP datagrams?

• This packet was split among many IP datagrams, yes. I discovered this by checking the data tab on my Wire shark, which displays Fragmented IP. I then examined each one to see whether the more segments are set to a value or not under Flags.

11. Print the first fragment of the IP datagram that has been fragmented. What does IP header information indicate that the datagram has been fragmented? What information does the IP header contains that indicates if this is the first or second fragment? What is the length of this IP datagram?

• The datagram has been fragmented, as indicated by the Flags bit for "More Fragments." We know this is the first fragment since the fragment offset is 0. This initial datagram is 1500 bytes long, including the header.

12. Print the second fragment of the IP datagram that has been fragmented.

What information in the IP header shows that this datagram fragment is not the first? Are there a greater number of fragments? How do you know?

• Because the fragment offset is 1480, I know this isn't the initial piece. Because the "additional fragments flag" is not set, it is the last fragment.

13. What fields change between the first and second fragments in the IP header?

• Total length, flags, fragment offset, and checksum are the IP header fields that changed across pieces.

14. From the original datagram, how many pieces were created?

• From the initial datagram, three packets are produced after switching to 3500.

15. What fields in the IP header differ across the fragments?

We can detect a change in the overall length of the flags between the first two packets and the last packet. The first two packets are 1500 bytes long, with the more fragments bit set to 1, while the last packet is 540 bytes long, with the more fragments bit set to 0.

Get LiveWebTutors Help!

If you need assistance with any type of academic writing, our team of academic writers is standing by. We offer a service to suit your demands, from easy **essay help** proposals to complete dissertations.