Wireshark ip routing

Technology, Computer

Introduction

To complete this study, I have had three Virtual machines running at once. Two of these Virtual Machines were running Ubuntu and one was running FREEBSD acting like a router between the two Ubuntu machines. Configured Each machine to the specified IP addresses beforehand and set two NAT Networks up as required in the study. Once all was set up I double checked IP addresses of both Ubuntu machines by opening terminal and typing inifconfigwhich then confirmed that both machines networks were working correctly. Furthermore, I have used thepingcommand to send an ICMP packet to NAT Networks to confirm both Ubuntu machines are connected to the right network. (See below) A

Fig. 1 ifconfig

Fig. 2 ping NAT Network

Fig. 3 ICMP Echo Request message IP information

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. What is the IP address of your computer?

The IP Address of my computer is 10. 0. 3. 4 . I found this out by looking at the “ Source” and that’s where packets were sent from so I know that will be my IP address also in the Internet Protocol version 4 it says “ Src: 10. 0. 3. 4”.

Within the IP packet header, what is the value in the upper layer protocol field?

Within the header, the value in the upper layer protocol field is ICMP(1).

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.

There are 20 bytes in the IP header and 60 bytes total length this gives 40 bytes in the payload of the IP datagram. To determine the number of payload bytes all you need to do is take away the IP header size which in this case is 20bytes from the total length which in this case is 60 bytes and the remainder is the number of payload bytes.

Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

The more fragments is= 0 so the data is not fragmented. I looked at the " Flags" drop down and there it determines if a packet is fragmented or not and in this case " more fragments" was 0 also Fragment offset is also = 0.

Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by your computer?

Time to live, Identification and Header checksum always change. The identification is a unique number assigned to each packet so it always has to change as a result of this the Header checksum will change and the Time to live will change with it too.

Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?

The fields that stay constant across the IP datagrams are:

Version (since we are using IPv4 for all packets)

Header length (since these are ICMP packets)

Source IP (since we are sending from the same source)

Destination IP (since we are sending to the same destination)

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

Upper Layer Protocol (since these are ICMP packets)

The fields that must stay constant are:

Version (since we are using IPv4 for all packets)

Header length (since these are ICMP packets)

Source IP (since we are sending from the same source)

Destination IP (since we are sending to the same dest)

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

Upper Layer Protocol (since these are ICMP packets)

The fields that must change are:

Identification(IP packets must have different ids)

Time to live (traceroute increments each subsequent packet)

Header checksum (since header changes, so must checksum)

Describe the pattern you see in the values in the Identification field of the IP datagram

IP header Identification fields increment with each ICMP Echo (ping) request.

I found this out by scrolling through each ICMP Echo request (ping) and looking at how Identification field values change.

Fig. 4 ICMP TTL exceeded reply, IP Info

What is the value in the Identification field and the TTL field?

Identification: 0x01a9(425)

TTL: 64

Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

The TTL will remain unchanged because the first hop router is always the same. Identification field for all ICMP TTL-exceeded replies will change because it is assigned a unique value. When two or more IP datagrams have the same identification value that means that these IP datagrams are fragments of a single large IP datagram.

Fig. 5 ICMP Echo Request packet size = 2000, First segment

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?

Yes, this packet has been fragmented across more than one IP datagram. I found this out by looking at the info tab on my Wireshark as it clearly states Fragmented IP also, I checked each one to see under Flags if the More segments is set to a value or not.

11. Print out the first fragment of the fragmented IP datagram. 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?

Under the Flags bit for “ More Fragments” it is showing that the datagram has been fragmented. Since the fragment offset is 0, we know that this is the first fragment. This first datagram has a total length of 1500 including the header.

Fig. 6 ICMP Echo Request packet size= 2000, second fragment

Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?
I can tell that this is not the first fragment since the fragment offset is 1480. It is the last fragment since the “ more fragments flag” is not set.
What fields change in the IP header between the first and second fragment?
The IP header fields that changed between the fragments are: total length, flags, fragment offset and checksum.

Fig. 7 ICMP Echo Request packet size= 3500, first fragment

How many fragments were created from the original datagram?
After switching to 3500, there are 3 packets created from original datagram.
What fields change in the IP header among the fragments?
The IP header fields that changed between all of the packets are: fragment offset and checksum. Between the first two packets and the last packet, we

see a change in total length also in the flags. The first two packets have the total length of 1500 with more fragments bit set to 1 and the last packet has a total length of 540 with more fragments bit set to 0.