Investigating TCP/IP, HTTP, ARP, ICMP Packets Using Wireshark

Amanpreet Kaur¹, Monika Saluja²
¹Student of M.Tech in Computer Science and Engg., ²H.O.D CSE Deptt., Shaheed Bhagat Singh College of Engg. and Technology, Ferozepur

Abstract— The effect of increasing changes in the network led to threats and security issues that has made monitoring and analysis a challenging task. A good understanding of network, type of network traffic is the good way of solving problems on the network like congestion, bandwidth. In this paper architecture of network traffic of an institute is taken, monitored and analysed using various protocols like TCP/IP, HTTP, ARP, ICMP comes under capturing packets. Detailed analysis of protocols is done, problems/issues comes under troubleshooting that network and various graphical representations are produced through captured packets on real time analysis basis. This network system from where capturing is done is in use at MIMIT college of Engg. and technology Malout.

Keywords— Wireshark, Protocol Dissector, Filtering, Log analysis.

I. INTRODUCTION

Wireshark [1] is a network protocol analyzer. It is formerly known as Ethereal. It reads packet from the network, decodes them and presents them in an easy to understand format. It is an open source network analyzer and is freely available. It works in Promiscuous as well as Non-promiscuous mode. In Promiscuous mode NIC can see conversation to and from all of its neighbours. Wireshark displays capture information in three main panes. Its default fields include: Packet number, Time, Source address, Destination address, Name and information about protocols.

II. HISTORY

Wireshark was first developed by Gerald Combs in 1997 for network troubleshooting. Its first version was released in July 1998 [1]. He and other members of his team use dissectors that allow Wireshark to decode individual protocols and present them in readable format. It has the ability to read captures in a variety of other formats. Protocol Dissector allows Wireshark to break down a packet into various sections so that it can be decoded, can be easily readable and can be analyzed. Another name for this is Protocol Decoding.

A. Traffic types

1. Unicast:- In this traffic type packets are transmitted from one computer to another.
2. Broadcast:- In this packet is one that is sent to all ports on a network segment. Hubs only are capable of broadcast traffic.
3. Multicast:- It transmit packets from single source to multiple destinations. It also uses special addressing schemes to send packets to which it is destined [2].

B. Capture Modes

1. By using Hub:- By this mode you can localize target device and your analyzer system on same network segment by plugging them directly into hub. Hub works on Physical layer and is half duplexed.
2. By Port Mirroring:- It duplicates the traffic between one or more switch ports and mirror it to the port that you want.
3. ARP cache Poisoning:- It translate layer 2 address through layer 3 protocols in ARP. It is the advanced form of tapping into wire on a switched network. This is also known as ARP Spothing, which is a process of sending ARP messages to Ethernet or router with fake MAC address in order to intercept the traffic to another computer. It causes DOS attack [5].

III. EXPERIMENTAL SETUP

Various cable taps, hubs, switches etc. can be used to attach a sniffer to a network [4]. Use laptop to run wireshark and a small hub attached to it and some network cables for troubleshooting. Install a small hub between server and the switch and connect the wireshark laptop to it. Wireshark will then see all the traffic going to and coming from the server. Use a sniffer at various points in the network. By this you will be familiar with various protocols running on your network. And also detect problems on network and resolve them.
It is a layer 4 protocol and provide bi directional communication. IP is a layer 3 protocol and provides addressing system that allows communication on network. It is a connectionless protocol [3].

TCP/IP session is a three way handshake process. In which SYN/ACK message is send and received at the start. SYN packet segment number is 0. This is shown in packet no. 95 in Figure 3. below whose seq. No. is 0 and after that in packet 96 when it gets acknowledgment from destination its sequence no. Is changed from 0 to 1. When same destination is called by same source again then port reused message is displayed with sequence no 0 as shown in packet 100.

HTTP request and transmission:- Now actual request and transmission on web page are to be viewed. This involves HTTP and TCP protocol and seen by GET command and after that OK message response comes. FIN/ACK messages are send and received when packets are to be transmitted. As shown in Figure 4. at packet 951 source sends a request to destination for http and in response it receives GET message in packet 954 after receiving acknowledgement. And at packet 972 conversation is completed by HTTP/1.0 OK message. The Web server responds in HTTP/1.1 with status code ―200 OK‖ which indicates to the browser that the object was successfully fetched. Other codes are ―403 Forbidden,‖ (the server does not have permission to send the object to the client, and ―404,‖ (the server cannot find the object that the client requested).
Another trace shows HTTP request and transmission from one source to destination starting with sequence no. 0 in packet 974 in Figure 5. and GET message in packet 980. But this is not found by particular destination so it sends HTTP/1.0 Not found message to source and end this conversation with FIN/ACK message in packet 987.

![Figure 5. HTTP Protocol showing conversation between two end points](image)

**ARP Protocol:**
- It is used to translate layer 3 address into layer 2 address that are IP addresses to MAC addresses which allows devices to determine where other devices are located on each port. It actually provides services to network and data link layer. Switch or router is used to know the location of computer to transmit data [3]. On seeing the capture file seen below in Figure 6, packets collected by it shows in packet no. 19 source computer is sending packet to IP address 192.168.24.9 asking who has 192.168.26.136 address?

![Figure 6. ARP Protocol asking who has 192.168.26.136 address](image)

It also provides functionality to find client’s layer 3 address by allowing transmitting computer to send ARP broadcast. Computer that has IP address will identify itself by sending response containing its layer 2 address back to transmitting computer. Second packet in Figure 6 shows destination computer’s ARP response to first packet. In response packet no. 20 shows that the above address 192.168.26.136 is at f0:4d:a2:a3:82:b8 machine (MAC address). This way computer will be able to send data directly to it. If there is no response from the host, it may not be on the network.

**ICMP Protocol:**
- Internet Control Message Protocol. It is a part of IP protocol and seen by Type 8 echo (ping) request in the window pane.

Computer sends echo request, it should receive echo reply in response as shown in Figure 7. Next Packet is transmitted back from remote computer and is marked as type 0, an echo (ping) reply.

![Figure 7. ICMP Protocol showing request /reply response](image)

**Common Problems Encountered When Troubleshooting Network**

**A. Unreachable Destinations and ICMP codes**
- When the target you are pinging is not responding, you will receive a Destination unreachable message. You are seeing that in packet there is Echo (ping) request from 192.168.26.136 to 192.168.25.1 as shown in Figure 8.

![Figure 8. ICMP Request/Reply](image)

**You receive a Echo (ping) reply in response.** Examine in packet display pane you will see it is a Type 0 packet in Figure 9.

![Figure 9. Packet Display Pane for Ping reply](image)

But if the destination is unreachable Figure 10, it is of Type 3 packet Figure 11.

![Figure 10. Destination/Host Unreachable](image)
Figure 11. Host Unreachable

B. Unreachable Port: - Another task is to ping on a specific port. This is done to ensure ports that are required are running and accepting the data Figure 12.

Figure 12. Unreachable Port

C. Fragmented Packets: - Fragmentation allows the IP protocol to breakdown large amount of data into chunks that can be sent across and reassembled at receiver. Each request and reply requires three packets instead of only one and by default a ping only sends 32 bytes of data to its destination. To determine whether a packet is fragmented or not see the Packet detail pane as shown in Figure 13.

Figure 13. Fragmented Packet, Packet detail pane

In the capture file select any one packet and then expand the Internet Protocol section of the packet’s Details pane. It has a section called Flags. By expanding it we see three fields One among them is More Fragments section. If its value is 0 then it is not fragmented further but if its value is 1 then it has more fragments.

D. Keeping Things in order: - These fragmented packets should stay in order. For this IP provides an offset value so that receiving system knows the order in which to sequence the fragmented packets. If in Packet Detail pane offset value is 0 this means this is the first packet in series of fragmented packet. If you see second packet it rises to 1480 value. (payload(data) size). Then for next packet it is 2960 and so on....This way it keeps packets in order.

E. An Evil Program: - In this type of problem your browser changes your home page everyday to any website. This is a spyware problem. This is seen in TCP packet where packet has sequence no. 0 and Len=0 and MSS value 1440 in Figure 14.

Figure 14. TCP packets for PSH, ACK messages

Evil program can also be checked in ARP packet, where there is a message of “Who has gratuitious ARP”? This is an evil program.

F. Malformed BOOTP/DHCP: - When source address is 0.0.0.0 then that packet is malformed.

VI. FILTERING THE TRAFFIC

Traffic filters basically provide a “search” functionality that limits the amount of data appearing on the screen to that matching a user’s customized criteria [6]. In order to filter out the abnormal traffic we will use Expert Infos in Analyze menu as shown in Figure 15. By selecting this option we see Errors, Warning, Chats, Notes and Details options. In Notes section we see when TCP previous segment lost packet is seen in the capture file a packet was suddenly dropped, for this Duplicate ACK packet is send to the server, in response requesting that lost packet be sent again. Client continues to send Duplicate ACK until it receives the requested packet. After it see TCP Retransmission in the Expert Infos window. In Error option we can see various Malformed packet received during capturing and in chats field we see all the conversation on TCP/IP and HTTP protocols.
Wireshark also give facility of reading the content of packets or segments sent. It provides facility of Follow TCP stream and shows the internal contents. As shown in Figure 16. One packet has data as shown in dark by opening Follow TCP Stream.

We can also draw graphs of packets captured in capture file. Click on Statistics menu and then TCP Stream Graph and then choose any graph type out of five graphs shown in option but first select packet for which you want to draw graph.

I select one of the packet and for this Time Sequence graph (tcp-trace) graph displayed is as shown in Figure 17.

This graph is for another packet, it has mark for transmitted segments and region of discontinuity where packet loss occurred Figure 18.

Wireshark also has facility of displaying object list. It will display Host name, its content type, bytes consumed and file name of that. This is shown in Figure 19.
If you want to see the summary of the captured file which you have capture then Figure 20. Shows all the summary of packets included First packet start time and last packet ending time. How many packets are captured and how many are displayed. Average packets/sec ,Average packet size and average bytes/sec etc..

Figure 20. Summary Window

A. Conversation :- Conversation between two packets can be seen by selecting any protocol and you can see packets transmitted and received and in percentage also as shown in Figure 21. In This TCP protocol conversation is shown.

B. I/O Graph :- Most important facility provided by Wireshark is to draw I/O graph of the captured packets. At a time we can draw graph of Five protocols of different colors with different tick interval and pixels per tick on X-axis and units and scale on Y-axis. Styles can also be changed instead of lines shown you can select impulse, Fbar, dot from the drop down and you get a different look of the graph. A line graph of TCP,HTTP,ARP protocol is shown to you in Figure 22.
VII. Graphs Related To Captured Packets (Time-Sequence Graphs)

Figure 23. Time Sequence Graph of captured packet

Figure 24. Time Sequence Graph of captured packet

Figure 25. Time Sequence Graph of captured packet

Figure 26. Time Sequence Graph of captured packet

Figure 27. Time Sequence Graph of captured packet
VIII. CONCLUSION

In this paper network traffic from a live network is shown by taking various traces and monitoring and analysis is done on that captured files and then statistics is built. Detailed analysis and summary as well as conversations between two end points are shown. One interesting option which Wireshark give is objects which we captured or say user who are on the network using whatever sites can be listed in this object list. Graphs of captured files are shown and other attractive features are shown which make Wireshark a great tool for network analysis. The Output graphs generated through captured packets provides details of network dynamics and insight into the problems that lead to network slowness, network performance etc.

Acknowledgement

The authors will like to express our gratitude to MIMIT college, Malout for providing infrastructure for capturing traces conducted in the study.

REFERENCES