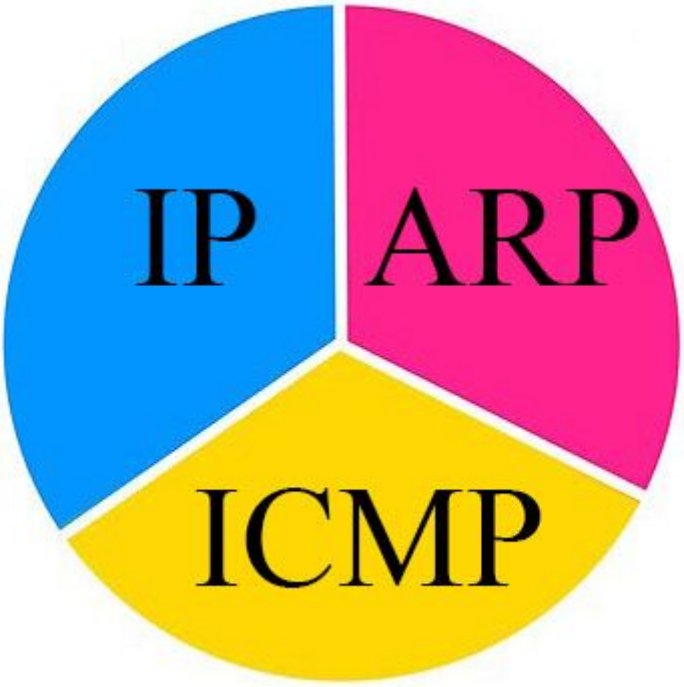

Address Resolution Protocol (ARP), Internet Protocol (IP), and The Internet Control Message Protocol (ICMP)

Dept. of CS, University of Victoria

March 2019

1 Introduction

This lab will focus on examining Address Resolution Protocol (ARP), which determines another computer's MAC address using their IP Address and an ARP table. Also, Internet Protocol and (IP) and Internet Control Message Protocol (ICMP) will be discussed. WireShark will be used to display the contents of frames for each of these 3 different protocols and provide us with information in regards to how the network is structured and operated.

2 Procedure

2.1 ARP Service

In the ethernet-trace-1.pcap trace, the source/client makes a broadcast to all listening nodes requesting the MAC address of the given IP Address. Source sends its MAC and IP address as well as the target IP Address. The target MAC Address is unknown at this point. Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

2.2 Analyzing IP frames

This section of the trace ethernet-trace-1.pcap, looks into the HTTP GET and RESPONSE requests which are used to transfer the following file:
/ethereal-labs/HTTP-ethereal-lab-file3.html

2.3 ICMP Functionality

Tracert is a program/command line that displays path a packet takes and measures any delays. Traceroute sends a packet to the first router with time to live = 1 which gets decremented to zero then dropped and information is sent back to the source such as IP addresses. tracert-trace-2.pcap displays this traffic in WireShark. Also, Ping is a tool that determines whether a device is reachable or not. ping-trace-1.pcap displays this traffic.

3 Discussion

3.1 ARP Analysis (Ethernet-trace)

1. **What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?**

Source address: ambitmic 00:d0:59:a9:3d:68

Destination address: ff:ff:ff:ff:ff:ff (broadcast)

This is in the first ARP request packet.

2. **Find the hexadecimal value for the two-byte Ethernet Frame type field.**

Type: ARP (0x0806)

3. **Where the ARP opcode (operation code) field is located, i.e., how many bytes are there between the first bit of the opcode and the first bit of the ARP message?**

Opcode is placed 6 bytes away from the start.

ARP message has:

Hardware type (2 bytes)

Protocol type (2 bytes)

Hardware size (1 byte)

Protocol size (1 byte)

Opcode (2 bytes)

4. **What is the value of the opcode field within the ARP-payload part of the Ethernet frame, in which an ARP request is made?**

Opcode: request (1)

5. **Does the ARP message contain the IP address of the sender?**

Yes, the IP is 192.168.1.105

ARP Packet #2

6. **Where the ARP opcode (operation code) field is located, i.e., how many bytes are there between the first bit of the opcode and the first bit of the ARP message?**

opcode is 6 bytes away from the start of the ARP message.

This is from the 2nd ARP response packet.

7. **What is the value of the opcode field within the ARP-payload part of the Ethernet frame, in which an ARP request is made?**

Opcode: reply (2) which means reply

8. **What is the MAC address answered to the earlier ARP query?**

Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)

Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) this is the MAC address requested by the source

9. **What are the hexadecimal values for the source and destination ad- dresses in the Ethernet frame containing the ARP reply message?**

Source address: 00:06:25:da:af:73

Destination address: 00:d0:59:a9:3d:68

10. **Why there is no ARP reply for the second ARP query (in packet No. 6)?**

Maybe because the IP address is not found and no node recognizes it or the device cannot be reached.

3.2 Analyzing IP frames

Ethernet trace - HTTP GET packet#10

1. **Sketch a figure of the packet you selected to show the position and size in bytes of the IP header fields, as well as the values in hexadecimal. Your figure can simply show the frame as a long, thin rectangle.**

<table>
<tr><td rowspan="2">0 offset</td><td>Version</td><td>Header length</td><td colspan="2">DSCP</td><td>ECN</td></tr>
<tr><td>0x4</td><td>0x5
20 bytes (5)</td><td colspan="2">0 0 0 0 0 0</td><td>0 0</td></tr>
<tr><td rowspan="2">16</td><td colspan="5">Total Length</td></tr>
<tr><td colspan="5">0x02a0 - Total Length: 672</td></tr>
<tr><td rowspan="2">32</td><td colspan="5">Identification</td></tr>
<tr><td colspan="5">0x00fa (250)</td></tr>
<tr><td rowspan="2">48</td><td colspan="2">Flag</td><td colspan="3">Fragment Offset</td></tr>
<tr><td colspan="2">0 1 0</td><td colspan="3">...0 0000 0000 0000 = Fragment offset: 0</td></tr>
<tr><td rowspan="2">64</td><td colspan="3">TTL</td><td colspan="2">Protocol</td></tr>
<tr><td colspan="3">0x08 (128)</td><td colspan="2">0x06 (TCP)</td></tr>
<tr><td rowspan="2">80</td><td colspan="5">Header Checksum</td></tr>
<tr><td colspan="5">0xbfc8</td></tr>
<tr><td rowspan="2">96</td><td colspan="5">Source IP Address</td></tr>
<tr><td colspan="5">0xc0a80169 (Source: 192.168.1.105)</td></tr>
<tr><td rowspan="2">128</td><td colspan="5">Destination IP Address</td></tr>
<tr><td colspan="5">0x8077f50c (Destination: 128.119.245.12)</td></tr>
</table>

2. **What are the IP and MAC addresses of the source and destination, respectively?**

Source is IP 192.168.1.105 and MAC 00:d0:59:a9:3d:68.

Destination is IP 128.119.245.12 and MAC 00:06:25:da:af:73

3. **How does the value of the Identification field change or stay the same for different packets? Is there any pattern if the value does change?**

This is for all packets.. The ID field changes every time a device sends a message. It uses a counter that increases by one and hence it changes every time.

4. **How to judge a packet has been fragmented or not?**

Flags: 0x4000, Don't fragment meaning it`s set to no fragment.

3.3 ICMP Functions (ping trace)

1. **What is the IP address of the source host (client)? What is the IP address of the destination host (server)? (PING)**

Source IP: 142.104.115.34

Destination IP: 142.104.96.10

2. **What is the average Round Trip Time (RTT)?**

(2.364+0.255+0.254+0.247+0.250+0.251+0.252+0.250+0.251+0.253)/10

= 0.4672 ms.

3. **Examine one of the ping request packets. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are in the checksum, sequence number and identifier fields?**

packet number 679, the ICMP type is 8 and the code number is 0. Other fields in the packet are: Checksum (2 bytes), Sequence number (2 bytes), Identifier fields (2 bytes), Timestamp from ICMP data (8 bytes).

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 in the checksum, sequence number and identifier fields?**

Corresponding packet number 680, the ICMP type is 0 and the code number is 0. Other fields in the packet are Checksum (2 bytes), Sequence number (2 bytes), Identifier fields (2 bytes), Timestamp from ICMP data (8 bytes).

5. **Examine the ICMP error packet, which could be found in the packets from tracert-trace-2. It has more fields than the ICMP echo packet. What are included in those fields? Find the TTL field, and explain what it is.**

Packet 366 contains the original ICMP request fields plus another Type, Code and Checksum. The error packet has Type 11, corresponding to "TTL exceeded". The Time-To-Live (TTL) field means this time is decreased by one as it jumps from one hop to another hop until it reaches to zero and the packet is dropped and returns to the sender with information about the hop.

6. **How many routers are between the source and the destination (www.engr.uvic.ca) from the trace file? Please draw a figure to show the sequences of these routers, i.e, source → router first**

the following is the sequence of routers (start from top to bottom)

Address	**Sequence number**
142.104.115.34	
142.104.127.254	1
192.168.9.2	4
192.168.10.1	7
192.168.8.6	10
142.104.252.21	13
142.104.252.18	16
142.104.193.247	

7. **How long are the average RTT between the source host and each router?**

By subtracting timestamps in wireshark:

142.104.127.254 = 605 ms

192.168.9.2 = 318 ms

192.168.10.1 = 961 ms

192.168.8.6 = 843 ms

142.104.252.21 = 931 ms

142.104.252.18 = 1002 ms

142.104.193.247 = 743 ms

4 Conclusion

When an ARP broadcasts a request asking whose MAC address has this given IP address, this usually is sent to all listening nodes or nodes within range of the device's network. When the IP address is not found, the packet is discarded at the receiver and when the IP address is found, the receiver sends a unicast reply to the sender with its IP and MAC addresses. Moreover, in this report commands such as PING and Traceroute have been discussed. It has been observed that Ping not only sheds light on the reachability of the host but it also provides information in regards to the network speed. Traceroute, on the other hand, helps find out how many nodes in the network by sending out request with TTLs and expired error messages.

5 Feedback

- Is there a limit to the number of hops used in Traceroute?