University of Victoria

CENG 460

Computer Communication Networks

Lab 3 - ARP, IP, and ICMP

Instructor:
Dr. Lin Cai

Teaching Assistant:
Amir Andaliby

Tyler Stephen V00812021
A01 - B04

March 18, 2016

1 Introduction

This lab will investigate Address Resolution Protocol (ARP), Internet Protocol (IP) and Internet Control Message Protocol (ICMP). ARP allows known IP addresses to be associated to unknown MAC addresses. Wireshark will be used to examine Ethernet frames for ARP messages. The contents of IP frames and content of ICMP messages will be examined. ICMP allows core IP functionality to be exposed as thought it were a higher level service and provide information about a network's functionality and structure.

2 Procedure

2.1 ARP Functions

`ethernet-trace-1.pcap` was downloaded from the course lab website and opened in Wireshark. The trace contains traffic generated by a source requesting a large document from a host. The trace begins with ARP discovery, where the source requests the MAC address from an IP. Both the request and reply headers for the ARP messages are examined in depth.

2.2 Analyzing IP frames

`ethernet-trace-1.pcap` also contains an HTTP GET request to initiate the transfer of the large document. The contents and size of the IP header corresponding to the request are examined in detail.

2.3 ICMP Functions: Ping & Traceroute

`ping-trace-1.pcap` contains traffic from ten ping requests between hosts on a local network. The round trip time (RTT) between two hosts is determined as the difference in wall clock time between the sending of a request and receiving its reply.

`tracert-trace-2.pcap` contains traffic from the `traceroute` command for a source and destination on the UVic network. `traceroute` sends requests to the destination with staggered time-to-live (TTL) values. If the requests expire before they reach the destination the intermediate router will send back an error message wrapped around the original request header.

The order of intermediate routers can be determined by cross-referencing the sender IP of the error message with the original request's TTL.

3 Discussion

3.1 ARP Functions

3.1.1 ARP Request (Packet 1)

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

Source address: `00:d0:59:a9:3d:68`
Destination address: `ff:ff:ff:ff:ff:ff` (broadcast)

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

The hex value is `0x0806`, which corresponds to an ARP message.

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?

The ARP message contains, in order: Hardware type (2 bytes); Protocol type (2 bytes); Hardware size (1 byte); Protocol size (1 byte), and; Opcode (2 bytes). Hence, the opcode is 6 bytes from the start the the ARP message.

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?

The opcode is `0x0001`, which corresponds to an ARP request.

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

Yes, the IP is `192.168.1.105`.

3.1.2 ARP Response (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?

As with the request, the opcode is 6 bytes from the start of the ARP message.

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?

The opcode is `0x0002`, which corresponds to an ARP reply.

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

The sender of the reply returns its MAC address: `00:06:25:da:af:73`.

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)?

The query goes unanswered either because the owner is unreachable or the IP is not owned by anyone on the local network.

3.2 Analyzing IP frames

3.2.1 HTTP GET (Packet 10)

1. Sketch a figure of the packet you selected (packet 10) 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">Offset</td><td colspan="16">Bit Position
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15</td></tr>
<tr><td>0</td><td colspan="4">Version</td><td colspan="4">IHL</td><td colspan="8">DSCP</td><td colspan="2">ECN</td></tr>
<tr><td></td><td colspan="4">0x4</td><td colspan="4">0x5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td rowspan="2">16</td><td colspan="16">Total Length</td></tr>
<tr><td colspan="16">0x02a0</td></tr>
<tr><td rowspan="2">32</td><td colspan="16">Identification</td></tr>
<tr><td colspan="16">0x00fa</td></tr>
<tr><td rowspan="2">48</td><td colspan="3">Flag</td><td colspan="13">Fragment Offset</td></tr>
<tr><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td rowspan="2">64</td><td colspan="8">Time To Live</td><td colspan="8">Protocol</td></tr>
<tr><td colspan="8">0x08</td><td colspan="8">0x06</td></tr>
<tr><td rowspan="2">80</td><td colspan="16">Header Checksum</td></tr>
<tr><td colspan="16">0xbfc8</td></tr>
<tr><td rowspan="2">96</td><td colspan="16">Source IP Address</td></tr>
<tr><td colspan="16">0xc0a80169</td></tr>
<tr><td rowspan="2">128</td><td colspan="16">Destination IP Address</td></tr>
<tr><td colspan="16">0x8077f50c</td></tr>
</table>

Since number of bits for the DSCP, ECN, Flags, and Fragment Offset fields are not divisible by 4 they have no unpadded hexadecimal equivalent. The raw bit values have been displayed instead.

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

The source has IP `192.168.1.105` and MAC `00:d0:59:a9:3d:68`. The destination has IP `128.119.245.12` and MAC `00:06:25:da:af:73`.

3.2.2 All packets

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?

The ID field corresponds to a counter set by each host. Every time a host sends a message its counter is incremented by one. The two counters do not have the same value.

4. How can you tell from looking at a packet that it has not been fragmented?

The value of the "Don't Fragment" flag is 1.

3.3 ICMP Functions

3.3.1 Ping

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

Source IP: `142.104.115.34`
Destination IP: `142.104.96.10`

What is the average Round Trip Time (RTT)?

Wireshark computes a single RTT for each reply packet. Summing the times of all 10 reply packets gives an average RTT of 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?

For the ping request in packet number 634, the ICMP type is 8 and the code number is 0. Other fields in the packet, with length, 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?

For the corresponding ping reply in packet number 635, the ICMP type is 0 and the code number is 0. Other fields in the packet, with length, are: Checksum (2 bytes), Sequence number (2 bytes), Identifier fields (2 bytes), Timestamp from ICMP data (8 bytes).

3.3.2 Traceroute

5. What is the IP address of the source host (client)? What is the IP address of the destination host (server)?

Source IP: `142.104.115.34`

Destination IP: `142.104.193.247`

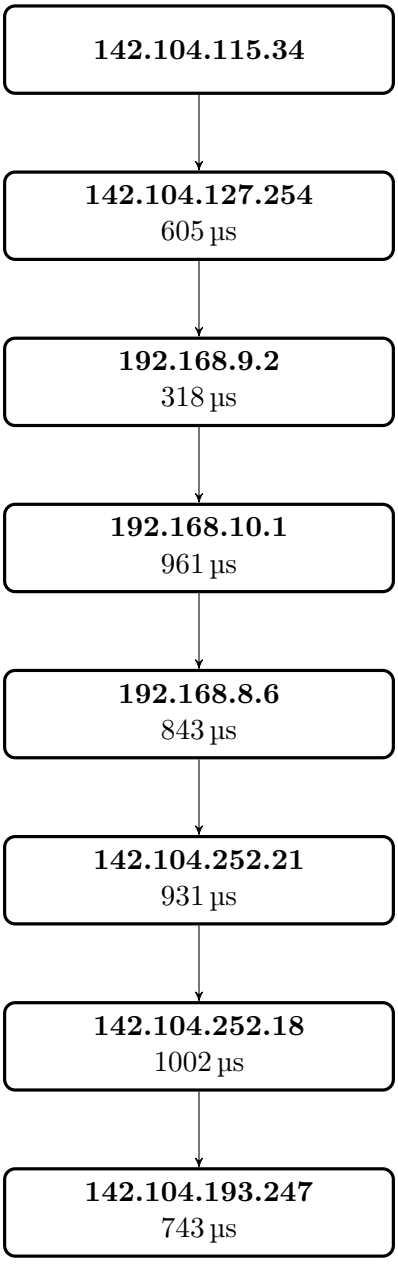
6. Examine the ICMP error packet, which could be found in the packets from tracert-trace-2. It has more fields than the ICMP echo packet. What are included in those fields? Find the TTL field, and explain what it is.

Examining packet 365, it 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 indicates the number of hops that a packet can make before it is invalidated. Each time a hope occurs the TTL value is decremented by one. When the TTL field is one and it reaches a host different from the destination, an error reply is generated and returned to the source.

7. 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 → ⋯ → router last → destination.

The order of routers along the route can be constructed by examining the original ping request wrapped in the error message. The wrapped request has a sequence number that can be cross-referenced to the original ping request to find the original TTL. In this trace, the first error response to reach the source is *not* from its nearest neighbor. It could be the case that the nearest neighbor is able to pass traffic faster than it can generate an error message as a result of

task priorities or dynamic load. Hence, it is absolutely necessary to cross-reference the sequence number to the original TTL to determine distance.



8. What are the average RTT between the source host and each router?

The average RTT is shown in the previous diagram. The time associated with each router is the RTT *to the source*. It is calculated by comparing the difference between the request and error response timestamps in Wireshark. Observe that the distance between the source and the router does not guarantee an identical ordering in response times.

4 Conclusion

The document request trace demonstrated that ARP requests are broadcast but their replies are unicast. ARP requests are not guaranteed a reply, and will not receive one if the destination IP is unavailable or unassigned. By analyzing all the packets, it is clear that the identification field is tied to unique counters for each host that increments each time a message is sent.

Ping and Traceroute are ICMP functions that yield information about the speed and topology of a network. Ping determines network speed by finding the time elapsed between request and reply message. Traceroute determines network topology by sending out multiple requests with staggered TTLs and uses the TTL Expired error messages to determine distances.

5 Feedback

- Capture traffic from a network with three hosts: A, B, C. A sends an ARP request for B's IP and B sends a response. C sends a message to A without a corresponding ARP request. Investigate why. (C knows A's MAC address from A's broadcast to find B.)
- Execute two `traceroutes`: one between local hosts and one from local-to-WAN. Does the mismatch between distance and reply time that exists for the local hosts also exist for the local-to-WAN case?
- Use `traceroute` for multiple websites in different countries. Where do the routes overlap? Construct a composite graph based on the routes that were obtained. Routes can be determined via the command line instead of through packet inspection in Wireshark.