1 Lab Preparation

It is assumed that students already have Wireshark installed on their Linux VM. Wireshark does run on Windows, however the command line tools, such as tshark use a different syntax. Additionally, if you wish to capture using Wireshark you must install separate drivers to capture on a Windows host. The Linux and Windows GUI capabilities and layouts are largely similar. If you need to install Wireshark to your Linux VM, from the command line use the following command:

sudo apt-get install wireshark wireshark-common tshark

- Download the following trace files to your working directory:
  - arp-bootup.pcapng
- Use the Layer 2/3 Reference Sheet - Header Format (Ehternet, IPv4, ARP & ICMP Echo), located on the course website, for use in analyzing the Wireshark packets throughout this lab

Submit all of your work in neatly hand-written format. Ensure you show all your work and steps you took to solve the problem, as needed.

What to turn in:

- The completed answer sheet

2 Lab Assignment

1. Open the trace file: arp-bootup.pcapng in Wireshark. (a) What is the display filter for ARP?

The display filter for ARP is arp to display all the ARP frames.

2. Use the display filter for ARP, analyze the resulting ARP messages. (a) What is happening in packets 3, 4, and 5? Using the display filter for ARP, in frames 3,4, and 5, the frames are sending three duplicates address tests. This is done to ensure that IPv4 is using gratuitous ARPs for the test.

(b) What unique feature of a gratuitous ARP message allows Wireshark (and you) to determine whether or not an ARP message is ‘gratuitous’ (Note: “Wireshark tells you under info” is not an acceptable answer as Wireshark fills out this column based on information it can parse from the packet.)
The unique feature of a gratuitous ARP message is that a gratuitous Arp is sent as a broadcast, this way for a node to announce or update the IP address.

(c) How did Wireshark know that these were ARP messages? What field-value pair within the packet tells

Wireshark that the packets were ARP messages.
Wireshark knows that there are ARP messages because it is used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.

(d) What are the display filters for the ARP's hardware type and protocol type? What are the values and types associated with these messages?
Ipconfig.all is a display filter for the ARP's hardware type, a protocol type that uses the network layer. The specific protocol is IPv4 (0x0800).

(e) Using packet 23, what do the hardware size and protocol size fields represent? Be specific.

For packet 23 the hardware size is 6 and the protocol size is 4, this represents what types of addresses are being mapped to each other. The Hardware size and the Protocol size refer to the amount of bytes in each of the aforementioned types of addresses: a MAC address is 6 bytes , and an IPv4 address is 4 bytes which is the results we see in wireshark.

(f) What is the display filter for ARP requests? ARP replies?

The display filter for an ARP request is one, for an ARP reply it is two.

(g) Research why packet 22, an ARP packet, would specify a target MAC address field that contains all zeros.

Packet 22 is an ARP request packet, this means that the target MAC address needs to be all zeros in order to send the request.

(h) Based on what you learned about packet 22 what is happening in packet 23?

Based on packet 22 being a ARP request packet. Packet 23 is an ARP reply packet.

(i) In the ARP messages 3, 4, 5, and 22, the destination MAC addresses were ff:ff:ff:ff:ff:ff, why? Explain in detail.

Since all four frames are considered ARP requests they will alway have the destination MAC address to be a broadcast address of FF:FF:FF:FF:FF. This is because an ARP request is considered a broadcast signal, this is why we must have the destination MAC be a broadcast address.

(j) Using only the ARP packets, list all known hosts on the network. Include all the relevant layer 2 and 3 addresses of the hosts. Extra Credit: Using any part of the trace, identify the type of network device of the host with an IP address of 24.6.168.1.

Using only the ARP packets we have two IP addresses that are sending information back and forth. For all of the ARP requests the Sender MAC address is: ASUSTekC_69:8f:58 and the sender's IP address is: 24.6.170.101. The other user that is sending the ARP reply has a MAC address of: Cadant_31:bb:c1 and has an IP address of: 24.6.168.1.

(k) Would it be valid to assume that this network is a /24 based on the information gleaned from these ARP packets.

This assumption is not valid because based on the IP address of the packets the information that was gained from this shows the the network is a /12.

3. Answer the following questions using display filters. *Always list your display filter as part of your answer.*

(a) Filter for all traffic with a layer 2 source address of 00:23:54:69:8f:58. List the other types of protocol traffic seen from this device.

The filter used for this information is **eth.src == 00:23:54:69:8f:58**. The other types of protocols that are seen other than ARP are, **DHCP, NBNS, ICMP, and BROWSER.**

(b) How many packets are in the trace with a destination address of 00:23:54:69:8f:58?

There are **21** packets that are in the trace with a destination address of 00:23:54:69:8f:58

Review Questions

1. What is the purpose of ARP?

The main purpose of ARP is that it acts as a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite.

2. Why are ARP packets not forwarded via routers?

ARP packets are not forwarded via a router because ARP requests will be broadcast first for the target IP address within the network because routers do not forward broadcast packet.

3. Research two additional hardware types and two additional protocol types supported by ARP? List with the hex values.

Two additional Hardware types for ARP are Ethernet and Amateur Radio. Two additional protocol types are Reserved and Unassigned.

4. List three reasons ARP is vulnerable.

a) Since it is a stateless protocol, ARP is vulnerable to ARP spoofing, which is a method of exploiting the interaction of IP and Ethernet Protocols, by making a fake ARP request and reply.
b) ARP protocol design mechanism, there is an obvious loophole: when a host receives an

ARP request or response packet, it does not verify the authenticity of the packet, but directly to the ARP packet IP / MAC correspondence into the ARP cache table.

c) Spoofing can cause a denial of service.

5. What is ARP poisoning?

ARP poisoning is when an attacker sends falsified ARP messages over a local area network (LAN) to link an attacker's MAC address with the IP address of a legitimate computer or server on the network.