Intro to Data Communications   
Understanding ARP and ICMP

Last Updated: 1/19/2023 3:11 PM Version 2  
Document Prepared for: Professor Lindstrom's Student

# Name Peter Sanford ID 10934984

# Overview

This lab will introduce you to packet capture and analysis using the free Wireshark protocol analyzer. Wireshark is a multiplatform protocol analyzer. A protocol analyzer interprets data packets that are captured from a network interface. It decodes and displays the data in a human readable form.

# Setup

Complete/Confirm the following setup

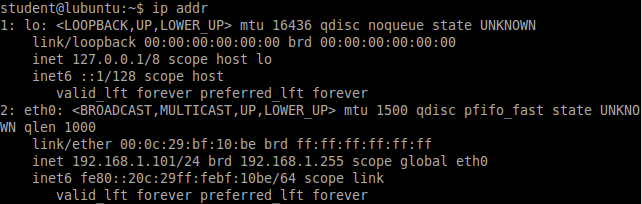
1. Start your pfsense, Debian-1 and Debian-2 virtual machines.
2. Ensure Debian-1 and 2’s Network adapters are connected to **VMNet11**

# Task 1—configure static IP addresses for Debian-1 and Debian-2

The first thing you will need to do is set IP addresses on your Debian-1 and 2 VMs to addresses that you control rather than addresses that are automatically configured. The information you will need is as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VM | IP Address | Subnet Mask | Gateway | DNS Server |
| Debian-1 | 192.168.1.11 | 255.255.255.0 | 192.168.1.1 | 192.168.1.1 |
| Debian-2 | 192.168.1.12 | 255.255.255.0 | 192.168.1.1 | 192.168.1.1 |

## Steps

1. Configure a static IP address on your Debian-1 VM
   1. Open the Wicd Network Manager, **Start Menu🡪Internet🡪Wicd Network Manager.** You should see the Wicd Network Manager dialog.
   2. Open the properties for the wired-default network.
   3. Configure your adapter to use static IPs and DNS servers.
   4. Enter the IP, Netmask (Subnet Mask), Gateway, and DNS server 1 from the table above.
   5. Click OK to save the settings
2. Disconnect then reconnect the network to apply the changes.
3. Verify your changes
   1. Open a terminal window, enter the command   
      **ifconfig eth0**Verify the IP Address (inet addr) and Subnet mask (Mask) are correct. If they are not fix them
   2. Alternatively you could us the ip command. Enter the command   
      **ip addr**  
        
      we are interested in interface eth0, notice the Subnet Mask is displayed in shorthand “/” notation. So the IP address in this output is 192.168.1.101 with the subnet /24.
   3. You can verify your name server by looking in the file /etc/resolv.conf. Enter the command  
      cat /etc/resolv.conf  
      You should see something like this:  
        
      the address on the nameserver line(s) is/are your DNS server’s IP address.
   4. To verify the Gateway was entered correctly enter the command:   
      **ip route**.   
      You should see output like this  
      
      1. the "default via" address
4. Repeat the above steps to configure and verify the IP settings on your Debian-2 VM.
5. Test connectivity with your new IP address.
   1. Ping from Debian-1 to pfsense with the command:  
      **ping –c 3 192.168.1.1**  
      If it does not work troubleshoot.
   2. Ping from Debian-2 to pfsense with the command:  
      **ping –c 3 192.168.1.1**  
      If it does not work troubleshoot.

# Task 2—exploring the ARP table

Remember ARP is used to translate IP addresses to MAC addresses. To communicate between hosts the hardware (MAC) address must be known. IP knows nothing of MAC addresses and Ethernet knows nothing of IP addresses so a translation table must be create to send data to the desired IP address over a protocol (Ethernet) that knows nothing of IP. In this task you will view and manage the ARP table.

## Steps

1. View the current arp table containing IP to MAC translation on both your Debian VMs. From each of your Debian-1 and Debian-2 VMs enter the following command:  
   **arp –n**  
   Record the ARP entries for each Machine (add rows to table if necessary)  
     
   Debian-1 Results (add rows as necessary)

|  |  |  |  |
| --- | --- | --- | --- |
| Address | HWtype | HWaddress | Iface |
| 192.168.1.1 | ether | 00:0c:29:bc:64:97 | Ens33 |

Debian-2 Results

|  |  |  |  |
| --- | --- | --- | --- |
| Address | HWtype | HWaddress | Iface |
| 192.168.1.1 | ether | 00:0c:29:bc:64:97 | Ens33 |

1. Ping from Debian-1 to Debian-2 with the command:  
   **ping –c 3 192.168.1.12**  
   View the arp tables again and record the results  
   Debian-1 Results (add rows as necessary)

|  |  |  |  |
| --- | --- | --- | --- |
| Address | HWtype | HWaddress | Iface |
| 192.168.1.1 | ether | 00:0c:29:bc:64:97 | Ens33 |
| 192.168.1.12 | ether | 00:0c:29:5e:c7:48 | Ens33 |

Debian-2 Results

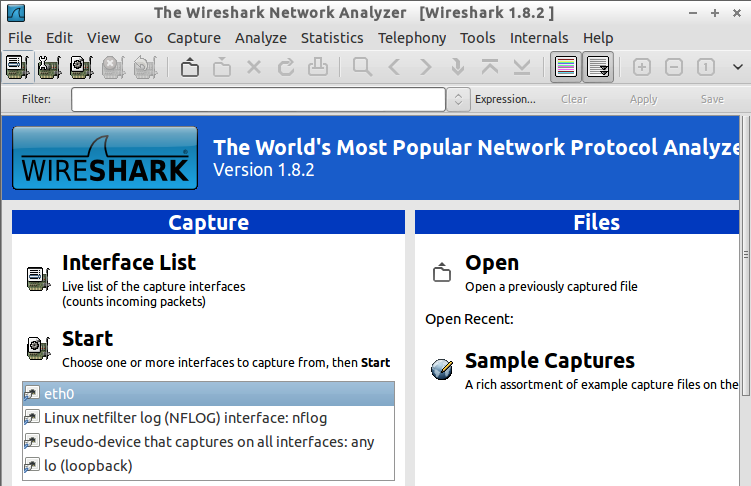
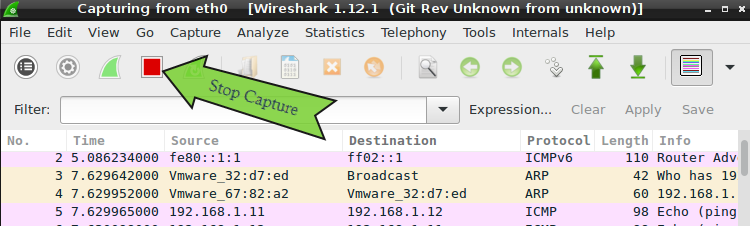
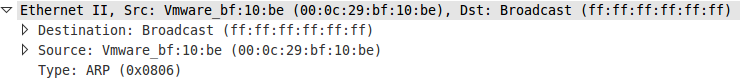
|  |  |  |  |
| --- | --- | --- | --- |
| Address | HWtype | HWaddress | Iface |
| 192.168.1.1 | ether | 00:0c:29:bc:64:97 | Ens33 |
| 192.168.1.11 | ether | 00:0c:29:73:aa:39 | Ens33 |

1. Deleting arp entries. You can manually remove an arp entery with the arp command.
   1. *From Debian-1* remove the ARP entry for Debian-2’s IP address. To modify the ARP table you must have root privileges, if you are not logged in as root you will need to run the command as root, to run a Linux command as root preface the command with “sudo”:  
      **arp –d 192.168.1.12**  
      enter your password when necessary.
   2. View the ARP table to ensure the entry was removed. (if you see the word incomplete in the HWaddress the command worked properly)
   3. *From Debian-2* remove the ARP entry for Debian-1’s IP address, enter the command:  
      **arp –d 192.168.1.11**
   4. View the ARP table to ensure the entry was removed.

# Task 4-Exploring the ARP protocol

Now you will capture network traffic to see the ARP protocol in action. Read through all the steps to familiarize yourself with the process. You will want to Start the Capture, ping, then stop capturing as quickly as possible to limit the extraneous network packets.

## Steps

1. From your Debian-1 VM start Wireshark from the desktop icon or from **Start🡪Internet🡪Wireshark**. If you run Wireshark as root you will get a couple of error messages,m you can click through them. Eventually you should see the Wireshark start screen  
   
2. In the list of network adapters click on **eth0**
3. Click the **start** link to start capturing network traffic.
4. From Debian-1 Ping your Debian-2 computer with the following command:  
   **ping –c 1 192.168.1.12**
5. Go back to Wireshark and stop the capture  
   
6. After you stop the capture you should see several captured frames. If all went well you should see some ARP and ICMP traffic. Wireshark lists the network frames in the order they were received. Near the top of your list you should see a frame with the protocol type of ARP. The info section should say “Who has 192.168.1.12? Tell 192.168.1.11” Click on that frame.
7. The wire shark display has three main windows, the top lists the frames captured, the middle decodes the frames by data field, and the bottom lists the data that was captured in hex. Once you select a frame, Wireshark decodes the frame and fills in the middle and bottom windows. The middle window is the most interesting. The middle window displays the frame as decoded data fields. The first node in the tree is the frame capture statistics, you can ignore that most of the time. The interesting stuff starts after the frame info.
   1. The second node in our example is an **Ethernet II** node. Click on the  icon to expand the node. Mine looks like this after the node is expanded.  
      
   2. What is the destination MAC address in your capture? Destination: Broadcast (ff:ff:ff:ff:ff:ff)   
      Is there anything special about that address? It’s the broadcast address
   3. What is the source MAC address? Source: VMware\_   
      What computer does that MAC address belong to? Debian1
   4. The last bit of information identifies this frame as an ARP frame type
8. Now that Wireshark has determined that it was an Ethernet II frame containing ARP it can decode the ARP data. The third node  is the ARP data decoded, expand the node and answer the following questions:
   1. What is the sender’s MAC address? 00:0c:29:73:aa:39
   2. What is the sender’s IP address? 192.168.1.11
   3. What is the Target’s MAC address? Receiver MAC address: 00:00:00 00:00:00 (00:00:00:00:00:00)   
      Why is that that value? I doesn’t know where it’s going, it’s going to everyone
   4. What is the Target’s IP address? 192.168.1.12
   5. What is the opcode? Opcode: Request (1)
9. Now select the ARP reply frame it should be very close behind the frame you just examined. The protocol will be ARP the info will be “192.168.1.12 is at …”
   1. From the ARP data answer the following questions
      1. What is the sender’s MAC address? 00:0c:29:5e:c7:48   
         Is that the same as the Sender’s MAC address in the ARP request frame no   
         Explain This is Debian2 replying back
      2. What is the sender’s IP address? 192.168.1.12
      3. What is the Target’s MAC address? 00:0c:29:73:aa:39   
         Why is that that value? Debian1’s address since it’s a reply
      4. What is the Target’s IP address? 192.168.1.11
      5. What is the opcode? Opcode: reply (2)

# Task 5—exploring ICMP

Now you will explore the ICMP protocol.

## Steps

1. Select the first ICMP (Not ICMP6)protocol frame after the ARP frame. What top level nodes are listed in the middle window? Frame, Ethernet II, Internet Protocol Version 4, Internet Control Message Protocol
2. Select the IP protocol node  expand that node.
   1. What is the time to live? 64
   2. What protocol is being encapsulated in this node (hint look at the node below the IP node)? ICMP (1)
3. Select and expand the  node in the middle window.
   1. What is the type? Type: 8 (Echo (ping) request)
   2. What is the protocol code? Code: 0
   3. Select the last node 
      1. How much data was sent in the echo request? 48 bytes
   4. Notice if you select the data field, the bytes representing that data will be highlighted in the bottom window. Select other fields and notice how the data is highlighted in the bottom window.
4. Find the response to this echo request. In the ICMP node you should see a link something like [Response frame: <somenumber>], this is a link to another frame. Double click the link to take you to that frame.
   1. What type is this ICMP packet? Type: 0 (Echo (ping) reply)
   2. Did the response send the same data back as it received? Yes

# Wrap-up

Congratulations you are now a network packet sniffing guru! Shutdown your VMs and ponder what you have learned.

# Deliverable

Upload this document with completed answers to canvas.