

CS 145 Lab Exercise 2: Wireshark Lab –Layer 2 Addresses

1.

Wireshark packet capture showing HTTP traffic. The packet list shows packet 133 (GET / HTTP/1.1) from source 64.207.139.127 to destination 192.168.1.4. The packet details pane shows the full request URI: http://www.cbtl.com.ph/. The packet bytes pane shows the raw data of the request.

Frame 133: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits) on interface 0
Ethernet II, Src: Tp-LinkT_13:1e:c1 (84:16:f9:13:1e:c1), Dst: Shenzhen_2b:1f:8d (bc:96:80:2b:1f:8d)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 64.207.139.127
Transmission Control Protocol, Src Port: 57331, Dst Port: 80, Seq: 1, Ack: 1, Len: 326
Hypertext Transfer Protocol
GET / HTTP/1.1\r\nHost: www.cbtl.com.ph\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: en-us\r\nConnection: keep-alive\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/601.6.17 (KHTML, like Gecko) Version/9.1.1 Safari/601.6.17\r\n\r\n[Full request URI: http://www.cbtl.com.ph/]
[HTTP request 1/1]
[Response in frame: 157]

This is the first GET message associated with cbtl.com.ph. This is the first GET request that has the host of www.cbtl.com.ph

2.

Wireshark packet capture showing HTTP traffic. The packet list shows packet 3653 (GET / HTTP/1.1) from source 66.85.130.13 to destination 192.168.1.4. The packet details pane shows the full request URI: http://www.philstar.com/. The packet bytes pane shows the raw data of the request.

Frame 3653: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface 0
Ethernet II, Src: Tp-LinkT_13:1e:c1 (84:16:f9:13:1e:c1), Dst: Shenzhen_2b:1f:8d (bc:96:80:2b:1f:8d)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 66.85.130.13
Transmission Control Protocol, Src Port: 57400, Dst Port: 80, Seq: 1, Ack: 1, Len: 327
Hypertext Transfer Protocol
GET / HTTP/1.1\r\nHost: www.philstar.com\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: en-us\r\nConnection: keep-alive\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/601.6.17 (KHTML, like Gecko) Version/9.1.1 Safari/601.6.17\r\n\r\n[Full request URI: http://www.philstar.com/]
[HTTP request 1/2]
[Next request in frame: 4950]

First GET request with a host of www.philstar.com

Gerard Montemayor

2014-56725

THWMXYHONOR

3.

Wireshark packet capture showing an HTTP GET request. The packet list shows a GET request from 192.168.1.4 to 64.207.139.127. The packet details pane shows the destination address as bc:96:80:2b:1f:8d and the source address as 84:16:f9:13:1e:c1.

Destination address is bc:96:80:2b:1f:8d

Source address is 84:16:f9:13:1e:c1

4.

Wireshark packet capture showing an HTTP GET request. The packet list shows a GET request from 192.168.1.4 to 66.85.130.13. The packet details pane shows the destination address as bc:96:80:2b:1f:8d and the source address as 84:16:f9:13:1e:c1.

Destination address is bc:96:80:2b:1f:8d

Source address is 84:16:f9:13:1e:c1

Gerard Montemayor

2014-56725

THWMXYHONOR

5. It is the Ethernet address of the network interface card that my computer is using to connect to the network.
6. It is the address of the router that the computer is connected to through the network interface card. It is not the HTTP server that the webpage is hosted.
7. The two addresses are the same. It makes sense since the GET requests from the computer should pass the same network interface card before going to the router. It wouldn't make sense if I was connected to the same network with the same network interface card but got two different source addresses.
8. The two addresses are the same. It also makes sense since the GET requests from the computer to the webpage should pass through the same router from the network interface card that the computer is using. It wouldn't make sense if I am connected to the same router where the computer sent the two GET requests, and get a different destination address for each one.
9. "*ifconfig* is used to configure, or view the configuration of, a network interface. *ifconfig* stands for "interface configuration". It is used to view and change the configuration of the network interfaces on your system."

Source: <http://www.computerhope.com/unix/uifconfi.htm>

```
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 84:16:f9:13:1e:c1
    inet6 fe80::8616:f9ff:fe13:1ec1%en1 prefixlen 64 scopeid 0x5
    inet 192.168.1.4 netmask 0xffffff00 broadcast 192.168.1.255
    nd6 options=1<PERFORMNUD>
    media: autoselect
    status: active
```

As we can see above, *en1* and the source addresses of the packets are the same, thus supporting that the network interface card address is the source address of the packets.