**COMP416 – Project3**

**Part-1: Network Layer Analysis**

**Network Interface Analysis**

1. Graphical user interface, text, application

   Description automatically generatedText

   Description automatically generatedView the interface information on your system. Differentiate the interfaces that you see and **explain the parameters provided in the output.** Provide the command to view the information for the wireless interface of your machine.

**Interfaces:**

* lo0: Loopback interface
* gif0: Software network interface
* stf0: IPv6 to IPv4 tunnel interface
* anpi1, anpi0
* ap1: Access point interface
* en3, en4: Ethernet adapters
* en1, en2: Thunderbolt interfaces
* en0: Wi-fi interface
* awdl0: Apple wireless direct link (Bluetooth) to iOS devices, which is for a peer-to-peer connection
* bridge0: Thunderbolt bridge
* llw0: WLAN low-latency interface
* utun0, utun1, utun2, utun3, utun4, utun5: VPN connection interfaces

The command is “inconfig en0” or “netstat -I en0”.

**Parameters:**

* mtu: Maximum Transmission Unit sizes
* ether: The hardware address of the interface, MAC address
* inet: INET address of the interface
* netmask: Network mask of the interface
* broadcast: Protocol broadcast address
* inet6: INET6 address of the interface
* prefixlen: The length of the prefix
* media: Media type of the interface
* status: Active or inactive status of the interface

1. What are table routes? Find the routing table using the ‘ip’ command. Examine the output and explain the parameters comparing the current output with that of ‘netstat -r’.

Graphical user interface, application

Description automatically generatedRouting table keeps the information of where the data packets will be directed over an IP.

Text

Description automatically generated

**Parameters:**

* Destination: The address of the destination network.
* Gateway: Next hop
* Flags: U: Up, the route is up. G: Gateway,

the route is via a gateway. L: Local address for the host. C: Clones the interface host route entries. H: Destination route is a specific host.

* Netif Expire: Network interface that route uses.

The outputs of the two commands are different. The first line of the ip route means that the default route for any packet is through en0 and via the default gateway (192.168.0.1). The second line means that any packet that will be sent to any IP address within the network 127.0.0.0/8 should be send through lo0 with 127.0.0.1.

1. What is multicast? View the list of multicast addresses for the wireless interface. Provide an explanation for the various fields you observe during the process.

Graphical user interface

Description automatically generatedGraphical user interface

Description automatically generatedMulticast is used for sending the data to multiple receivers. We can see the multicast addresses with the command “netstat -g”. And can see the addresses for wireless interface with the command “netstat -I en0”. But I couldn’t combine them. Multicast addresses list is below.

**ICMP Analysis**

*I used a different address from my URL since it was not terminating and returning “\* \* \*” infinitely. I used “ucla.edu” rather than “tufts.edu”.*

1. What is TTL and its significance? Under which layer header can you find the value of TTL?

Graphical user interface

Description automatically generatedGraphical user interface

Description automatically generatedTTL (time-to-live) is the time that a packet is available and valid within a network before the router discards it. This mechanism prevents the packets to circulate infinitely.

The TTL value can be found under Internet Control Message Protocol -> Internet Protocol Version 4 -> Time to Live.

1. Why is it that an ICMP packet does not have source and destination port numbers?

ICMP packets do not communicate between application layer processes. It communicates between hosts and routers in the network layer, therefore there is no need for destination and source port numbers. It does not need to be recognized.

1. What does the Type and Code under the ICMP header signify? Observe these fields for the various packets captured in Wireshark and explain the significance of these fields.

ICMP packets provides the information to the recipient. The error data contains two fields: type and code. They carry the necessary information together.

Packet 317 could not reach to its destination therefore its type is 3 and code is also 3.

A screenshot of a computer

Description automatically generated with medium confidence

Packet 173 exceeded TTL, therefore the type is 11 and code is 0.A screenshot of a computer

Description automatically generated with medium confidence

1. Find the minimum TTL below which the traceroute messages do not reach your particular URL destination.

All the packets except packet 317 have TTL = 1 which is the minimum TTL.

1. How does your computer (the source) learn the IP address of a router along the path from a TTL exceeded packet?

My computer sends echo requests to the destination and the path is probed by the traceroute. The routers send TTL exceeded messages along the path to the source (my computer) as a response. The router put its IP address in the source field of the TTL Exceeded packet.

1. How many times is each router along the path probed by traceroute?

It probes more than once (generally three times) in case of a packet loss.

1. What is the default number of probes used by the traceroute? Run multiple traceroutes increasing the number of probes progressively. Explain your observation regarding the resolution of the route to your destination ip address.

Graphical user interface

Description automatically generatedThe default number is 3 times. Number of probes can be specified with the -q flag. We can see the time of each probe sent for each packet.

1. Graphical user interface

   Description automatically generatedFind the route to the IP Address: 18.31.0.200. What is different about the results for this address?

Traceroute does not return anything with this address. It starts to return “\* \* \*” infinitely. This is called a black hole in networking.

1. What is a Routing Blackhole? Provide a scenario where Routing Blackholes may be used beneficially.

Routing black hole means the traffic between the source and destination is dropped unintentionally because of a missing routing information. It can be set intentionally and can be useful. A router can create a black hole and it forwards the traffic to the null device (bit bucket) which discards any data you send to it. It can be used for security e.g., preventing the DDoS attacks. When the attack is detected, the traffic can be dropped by routing it to a blackhole.

1. Can you provide of another command which uses ICMP protocol? If so, use that to corroborate the minimum TTL obtained in 7.

Ping command uses ICMP protocol. Its minimum TTL is 50.

1. Use ‘mtr *yourURL*’ to find continuous statistics of the traceroute. Run the mtr command with three different sets of 4 fields each (you can find the information from ‘man’ pages) and explain the output.
2. Record the packets using ‘mtr yourURL’ through Wiresh Wireshark. What is the difference between the Wireshark capture of traceroute and ‘mtr’?

**Part-2: DV-Route Simulator**

**Sources**

[1] <http://linux-ip.net/html/tools-ip-route.html>

[2] <https://diego.assencio.com/?index=d71346b8737ee449bb09496784c9b344>

[3] <https://resources.infosecinstitute.com/topic/icmp-protocol-with-wireshark/>