

Lab7 Networking

Haorui Chen chenhr@bu.edu

Task1

input command ip addr

```
blenguin@blenguin-virtual-machine:~/Desktop$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c9:1c:ca brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.118.128/24 brd 192.168.118.255 scope global dynamic noprefixroute ens33
        valid_lft 1156sec preferred_lft 1156sec
    inet6 fe80::42c6:f0be:f51e:12f0/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:36:b7:5a:83 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
```

ip addr

trace ping www.bu.edu

The image shows a Wireshark packet capture of a ping command. The packet list on the left shows 25 packets. The packet details pane on the right shows the selected packet (No. 25) as a Standard query response (PTR) from 192.168.118.2 to 192.168.118.128. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.118.128	192.168.118.2	DNS	81	Standard query 0x08ca A www.bu.edu OPT
2	0.000144138	192.168.118.128	192.168.118.2	DNS	81	Standard query response 0xf203 AAAA www.bu.edu OPT
3	0.015224771	192.168.118.2	192.168.118.128	DNS	187	Standard query response 0x08ca A www.bu.edu CNAME d6c88qfbxvnm.cloudfront.net A 18.239.183.41 ...
4	0.037029777	192.168.118.2	192.168.118.128	DNS	208	Standard query response 0xf203 AAAA www.bu.edu CNAME d6c88qfbxvnm.cloudfront.net SOA ns-1246.a...
5	0.037482968	192.168.118.128	192.168.118.2	DNS	99	Standard query 0x2262 AAAA d6c88qfbxvnm.cloudfront.net OPT
6	0.039398346	192.168.118.2	192.168.118.128	DNS	99	Standard query response 0x2262 AAAA d6c88qfbxvnm.cloudfront.net OPT
7	0.040632483	192.168.118.128	18.239.183.41	ICMP	98	Echo (ping) request id=0x0003, seq=1/256, ttl=64 (reply in 8)
8	0.056283176	18.239.183.41	192.168.118.128	ICMP	98	Echo (ping) reply id=0x0003, seq=1/256, ttl=128 (request in 7)
9	0.057199097	192.168.118.128	192.168.118.2	DNS	97	Standard query 0x52c7 PTR 41.183.239.18.in-addr.arpa OPT
10	0.115687788	192.168.118.2	192.168.118.128	DNS	154	Standard query response 0x52c7 PTR 41.183.239.18.in-addr.arpa PTR server-18-239-183-41.bos50.r...
11	1.041543051	192.168.118.128	18.239.183.41	ICMP	98	Echo (ping) request id=0x0003, seq=2/512, ttl=64 (reply in 12)
12	1.056327328	18.239.183.41	192.168.118.128	ICMP	98	Echo (ping) reply id=0x0003, seq=2/512, ttl=128 (request in 11)
13	2.043178409	192.168.118.128	18.239.183.41	ICMP	98	Echo (ping) request id=0x0003, seq=3/768, ttl=64 (reply in 14)
14	2.056614169	18.239.183.41	192.168.118.128	ICMP	98	Echo (ping) reply id=0x0003, seq=3/768, ttl=128 (request in 13)
15	3.045585791	192.168.118.128	18.239.183.41	ICMP	98	Echo (ping) request id=0x0003, seq=4/1824, ttl=64 (reply in 16)
16	3.057293125	18.239.183.41	192.168.118.128	ICMP	98	Echo (ping) reply id=0x0003, seq=4/1824, ttl=128 (request in 15)
17	4.047823328	192.168.118.128	18.239.183.41	ICMP	98	Echo (ping) request id=0x0003, seq=5/1280, ttl=64 (reply in 18)
18	4.059501689	18.239.183.41	192.168.118.128	ICMP	98	Echo (ping) reply id=0x0003, seq=5/1280, ttl=128 (request in 17)
19	5.049953994	192.168.118.128	18.239.183.41	ICMP	98	Echo (ping) request id=0x0003, seq=6/1536, ttl=64 (reply in 20)
20	5.068018304	18.239.183.41	192.168.118.128	ICMP	98	Echo (ping) reply id=0x0003, seq=6/1536, ttl=128 (request in 19)
21	5.175261893	VMware_c9:1c:ca	VMware_e4:6e:46	ARP	42	Who has 192.168.118.2? Tell 192.168.118.128
22	5.175412305	VMware_e4:6e:46	VMware_c9:1c:ca	ARP	60	192.168.118.2 is at 00:50:56:e4:6e:46
23	6.051444287	192.168.118.128	18.239.183.41	ICMP	98	Echo (ping) request id=0x0003, seq=7/1792, ttl=64 (reply in 24)
24	6.065890492	18.239.183.41	192.168.118.128	ICMP	98	Echo (ping) reply id=0x0003, seq=7/1792, ttl=128 (request in 23)
25	6.066786999	192.168.118.128	192.168.118.2	DNS	97	Standard query 0xdata PTR 41.183.239.18.in-addr.arpa OPT

Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface ens33, id 0
Ethernet II, Src: VMware_c9:1c:ca (00:0c:29:c9:1c:ca), Dst: VMware_e4:6e:46 (00:50:56:e4:6e:46)
Internet Protocol Version 4, Src: 192.168.118.128, Dst: 192.168.118.2
User Datagram Protocol, Src Port: 34148, Dst Port: 53
Domain Name System (query)
0000 00 50 56 e4 6e 46 00 c9 29 c9 1c ca 00 00 45 00 PV nF...).....E
0010 c0 43 7a 52 00 00 40 11 92 84 c0 a5 76 80 c0 08 CZR @...v...
0020 76 02 85 64 00 35 00 2f 6e 14 08 ca 01 00 00 01 v...d 5 / n...v...
0030 00 00 00 00 00 01 03 77 77 77 02 62 75 03 65 64w ww-bu-ed
0040 75 00 00 01 00 00 00 00 29 05 c0 00 00 00 00 00 u... ..).....
0050 00

trace ping

Q1:What kind of protocol is used when performing a ping command?

A1: ICMP (Internet Control Message Protocol) .ICMP (Internet Control Message Protocol) is a network layer protocol used for sending error messages and operational information, primarily for network diagnostics. It helps determine whether data is reaching its intended destination by sending "echo request" and receiving "echo reply" messages, commonly seen in commands like `ping`. Unlike TCP or UDP, ICMP is not used for exchanging user data but for troubleshooting and reporting network issues.

Q2: What information is transferred in this protocol?

A2: In the ICMP (Internet Control Message Protocol), the following types of information are transferred:

1. **Error Messages:** ICMP communicates errors that occur when packets cannot be delivered. For example, "Destination Unreachable" messages inform the sender that a destination is unreachable due to network issues or configuration problems.
2. **Diagnostic Messages:** ICMP is used for diagnostic purposes, such as with `ping` or `traceroute`. These tools send Echo Request and Echo Reply messages to check if a host is reachable and measure the round-trip time.
3. **Control and Status Messages:** ICMP also provides information about the status of the network. This includes messages like Time Exceeded, which indicates that a packet's time-to-live (TTL) expired in transit, or Redirect messages, which inform a host of a better route for sending packets.

Task2

wget www.bu.edu

The image shows a Wireshark packet capture of a successful HTTP GET request to www.bu.edu. The packet list shows a standard query for www.bu.edu and a successful HTTP 200 OK response. The packet details pane shows the Hypertext Transfer Protocol section with status 200 OK.

HTTP GET

Q1: Specify the source and destination IP address

A1: Source IP Address: 192.168.118.128

Destination IP Address: 18.239.183.111

Q2: Source and Destination MAC Address

A2: Source MAC Address: 00:0c:29:e4:6e:46 (VMware virtual adapter)

Destination MAC Address: 00:50:56:e4:6e:46

Q3: Internet Protocol Version

A3: IPv4

Q4: Source and Destination Port

A4: Source Port: 53152

Destination Port: 80

Q5: Version of wget

A5: Wget/1.21.2.

Q6: TCP Flags

A6: ACK

Task3

wget <https://www.bu.edu>

The image shows a Wireshark packet capture of a TLS handshake and data transfer. The top pane shows the packet list with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
10	0.373017914	192.168.118.128	18.239.183.101	TLSv1.3	458	Client Hello
12	0.388085984	18.239.183.101	192.168.118.128	TLSv1.3	6550	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application D...
14	0.405710714	192.168.118.128	18.239.183.101	TLSv1.3	118	Change Cipher Spec, Application Data
16	0.406021123	192.168.118.128	18.239.183.101	TLSv1.3	201	Application Data
18	0.410925798	18.239.183.101	192.168.118.128	TLSv1.3	200	Application Data
24	0.526202776	18.239.183.101	192.168.118.128	TLSv1.3	8246	Application Data [TCP segment of a reassembled PDU]
28	0.526456396	18.239.183.101	192.168.118.128	TLSv1.3	8246	Application Data [TCP segment of a reassembled PDU]
31	0.536175750	18.239.183.101	192.168.118.128	TLSv1.3	5270	Application Data [TCP segment of a reassembled PDU]
38	0.541327741	18.239.183.101	192.168.118.128	TLSv1.3	7254	Application Data [TCP segment of a reassembled PDU]
41	0.544455562	18.239.183.101	192.168.118.128	TLSv1.3	6262	Application Data [TCP segment of a reassembled PDU]
45	0.545318457	18.239.183.101	192.168.118.128	TLSv1.3	3382	Application Data [TCP segment of a reassembled PDU]
54	0.561815587	18.239.183.101	192.168.118.128	TLSv1.3	8246	Application Data [TCP segment of a reassembled PDU]
55	0.561816048	18.239.183.101	192.168.118.128	TLSv1.3	6237	Application Data

The bottom pane shows the details of the selected packet (Packet 10, Client Hello). The Cipher Suites section is expanded, showing the following details:

- Session ID: 620fc43ff21c9e13cab238580cddc382a848561708d5e3e17952b19a3acfd0d
- Cipher Suites Length: 150
- Cipher Suites (75 suites)
- Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
- Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)

The packet bytes pane shows the raw data of the Client Hello packet, including the TLS record structure and the Client Hello message.

wget <https://www.bu.edu>

Q1: List the packets sent between two machines and the purpose of each packet.

A1:

- **Client Hello (Packet 10):** The client initiates the TLS handshake by proposing encryption settings.
- **Server Hello, Change Cipher Spec, Application Data (Packet 12):** The server selects encryption settings, notifies that future communication will be encrypted, and starts sending encrypted data.
- **Change Cipher Spec, Application Data (Packet 14):** The client acknowledges the encryption setup and starts sending encrypted data.

- **Application Data (Packets 16-55):** Encrypted data is exchanged between the client and server.

Task4

Q1: Which IP addresses are in the trace?

A1:

1. **192.168.1.17** (Client)
2. **192.168.1.1** (Local Gateway)
3. **74.125.29.189** (Google Server)
4. **216.58.219.238** (Google Server)
5. **128.197.26.34, 128.197.26.35, 128.197.26.4, 128.197.26.3** (Boston University Servers)

Q2: Which IP is the client?

A2: **192.168.1.17** is the client IP address.

Q3: What domains are being accessed?

A3:

1. **goo.gl** (Google's URL shortening service)
2. www.bu.edu (Boston University official website)

Q4: Using Wireshark, get a copy of the image file and include it in the write-up

A4:



BUPC-Logo-black