Fundamental of Information Security and Blockchain

B. Tech CSE III Semester

Instructor:

Dr Mohammad Wazid

Professor, Department of CSE

Graphic Era (Deemed to be University), Dehradun, India

Email: wazidkec2005@gmail.com

Homepage: https://sites.google.com/site/mwazidiiith/home

ping command

- The ping command is one of the most often used networking utilities (tool/command) for troubleshooting network problems.
- You can use the ping command to test the availability of a networking device (usually a computer) on a network.
- When you ping a device you send that device a short message, which it then sends back (the echo).
- If you receive a reply then the device is working OK , if you don’t then the device is **faulty, disconnected, switched off, incorrectly configured.**

ping command

- The ping command **operates by sending Internet Control Message Protocol (ICMP) Echo Request messages** to the destination computer and waiting for a response.
- How many of those responses are returned, and how long it takes for them to return, are the two major pieces of information that thping e ping command provides.
- To use the ping command you go to the command line.
- On Windows -Start Menu>Run and enter cmd to open a command prompt. Then type:

ping IP Address e.g. ping 192.169.0.1 or to ping a web address e.g. ping www.google.com

ping command

- **Output will be as follows:**

```
Pinging www.google.com [172.217.166.196] with 32 bytes of data:
Reply from 172.217.166.196: bytes=32 time=51ms TTL=56
Reply from 172.217.166.196: bytes=32 time=51ms TTL=56
Reply from 172.217.166.196: bytes=32 time=52ms TTL=56
Reply from 172.217.166.196: bytes=32 time=51ms TTL=56
Ping statistics for 172.217.166.196:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 51ms, Maximum = 52ms, Average = 51ms
```

ping command options

- **Item** **Explanation**
- **-t** Using this option will ping the target until you force it to stop by using Ctrl-C.
- **-n count** This option sets the number of ICMP Echo Requests to send, from 1 to 4294967295. The ping command will send 4 by default if -n isn't used.

```
ping -n 8 www.google.com
```

- **-l size** Use this option to set the size, in bytes, of the echo request packet from 32 to 65,527. The ping command will send a 32-byte echo request if you don't use the -l option.

```
ping -l 64 www.google.com
```

ping command options

- **Item Explanation**
- -f Use this ping command option to prevent ICMP Echo Requests from being fragmented by routers between you and the target. The -f option is most often used to troubleshoot Path Maximum Transmission Unit (PMTU) issues.
- -i TTL This option sets the Time to Live (TTL) value, the maximum of which is 255.

```
ping -i 100 www.google.com
```

- -r count Use this ping command option to specify the number of hops between your computer and the target computer or device that you’d like to be recorded and displayed. The maximum value for count is 9.

```
ping -r 6 www.google.com
```

Ping using wireshark

-
  ```
  C:\Users\MWazid>ping www.google.com
  Pinging www.google.com [172.217.167.36] with 32 bytes of data:
  Reply from 172.217.167.36: bytes=32 time=54ms TTL=56
  Reply from 172.217.167.36: bytes=32 time=54ms TTL=56
  Reply from 172.217.167.36: bytes=32 time=54ms TTL=56
  Reply from 172.217.167.36: bytes=32 time=54ms TTL=56
  Ping statistics for 172.217.167.36:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
  Minimum = 54ms, Maximum = 54ms, Average = 54ms
  ```

Ping using wireshark

- Query: The query messages are the information we get from a router or another destination host.
- For example, given below message types are some ICMP query codes:
- Type 0 = Echo Reply
- Type 8 = Echo Request
- Type 9 = Router Advertisement
- Type 10 = Router Solicitation
- Type 13 = Timestamp Request
- Type 14 = Timestamp Reply
- A ping command sends an ICMP echo request to the target host. The target host responds with an echo Reply which means the target host is alive.

ICMP

- ICMP (Internet Control Message Protocol) is a protocol that network devices (e.g. routers) use to generate error messages when network issues are preventing IP packets to move forward.
- The Internet Control Message Protocol is one of the fundamental systems that makes the internet work.
- Although you may not have heard of ICMP, you probably have heard of one of its features: Ping

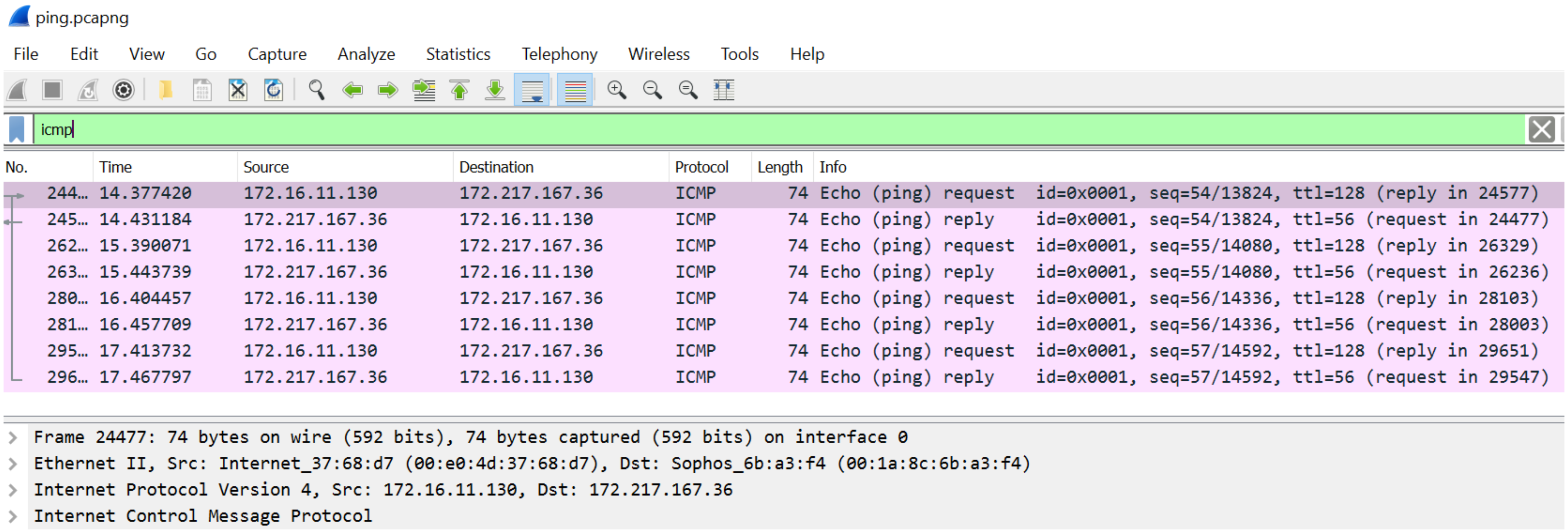
Purpose of ICMP

- Lower level Internet Layer is not supposed to be concerned with connection assurance, ICMP gives a little bit of feedback on communications when things go wrong.
- So, even if we use UDP, which has a connectionless communications model, it is still possible to find out why the transmission failed.

Ping using wireshark

- In the provided image (on next slide) you can see a reply from the host; now notice a few more things as given below:
- The default size of payload sent by source machine is 32 bytes (request)
- The same size of payload received by source machine is 32 bytes from Destination machine (reply)
- TTL = 56 which means host machine is windows system (see ICMP reply).
- Total packets are 8, 4 packets of the request and 4 of reply.

Ping using wireshark



icmp

```
No.    Time       Source          Destination     Protocol  Length  Info
244…   14.377420  172.16.11.130   172.217.167.36  ICMP          74  Echo (ping) request  id=0x0001, seq=54/13824, ttl=128 (reply in 24577)
245…   14.431184  172.217.167.36  172.16.11.130   ICMP          74  Echo (ping) reply    id=0x0001, seq=54/13824, ttl=56 (request in 24477)
262…   15.390071  172.16.11.130   172.217.167.36  ICMP          74  Echo (ping) request  id=0x0001, seq=55/14080, ttl=128 (reply in 26329)
263…   15.443739  172.217.167.36  172.16.11.130   ICMP          74  Echo (ping) reply    id=0x0001, seq=55/14080, ttl=56 (request in 26236)
280…   16.404457  172.16.11.130   172.217.167.36  ICMP          74  Echo (ping) request  id=0x0001, seq=56/14336, ttl=128 (reply in 28103)
281…   16.457709  172.217.167.36  172.16.11.130   ICMP          74  Echo (ping) reply    id=0x0001, seq=56/14336, ttl=56 (request in 28003)
295…   17.413732  172.16.11.130   172.217.167.36  ICMP          74  Echo (ping) request  id=0x0001, seq=57/14592, ttl=128 (reply in 29651)
296…   17.467797  172.217.167.36  172.16.11.130   ICMP          74  Echo (ping) reply    id=0x0001, seq=57/14592, ttl=56 (request in 29547)
```

```
> Frame 24477: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Internet_37:68:d7 (00:e0:4d:37:68:d7), Dst: Sophos_6b:a3:f4 (00:1a:8c:6b:a3:f4)
> Internet Protocol Version 4, Src: 172.16.11.130, Dst: 172.217.167.36
> Internet Control Message Protocol
```

Ping using wireshark

- Below message types are some of the ICMP error codes:
- Type 3 = Destination Unreachable
- Type 4 = Source Quench
- Type 5 = Redirect
- Type 11 = Time Exceeded
- Type 12 = Parameter Problems