**Lab1 Report**

**Student name: Wei Lin (999595193)**

**Student name: Shenglin Meng ()**

Exercise 5

**Which files must be edited to change the name of a Linux PC, e.g., from `PC1’ to `machine1’?**

Edit the file /etc/sysconfig/network”, change “HOSTNAME=PC1” to “HOSTNAME=machine1”

**Which files include information that determines whether a Linux PC performs IP forwarding?**

In the file “/etc/sysctl.conf” that has “net.ipv4.ip\_forward = $boolean”.

**Attach the content of the file /etc/sysconfig/network-scripts/ifcfg-eth0 to your lab report.**

Exercise 6

**Include the output you saved in this exercise.**

6.1

PING 10.0.1.12 (10.0.1.12) 56(84) bytes of data.

64 bytes from 10.0.1.12: icmp\_seq=1 ttl=64 time=4.60 ms

64 bytes from 10.0.1.12: icmp\_seq=2 ttl=64 time=0.101 ms

64 bytes from 10.0.1.12: icmp\_seq=3 ttl=64 time=0.103 ms

64 bytes from 10.0.1.12: icmp\_seq=4 ttl=64 time=0.098 ms

64 bytes from 10.0.1.12: icmp\_seq=5 ttl=64 time=0.105 ms

--- 10.0.1.12 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4000ms

rtt min/avg/max/mdev = 0.098/1.002/4.606/1.802 ms

6.2

PING 10.0.1.11 (10.0.1.11) 56(84) bytes of data.

64 bytes from 10.0.1.11: icmp\_seq=1 ttl=64 time=0.112 ms

64 bytes from 10.0.1.11: icmp\_seq=2 ttl=64 time=0.099 ms

64 bytes from 10.0.1.11: icmp\_seq=3 ttl=64 time=0.101 ms

64 bytes from 10.0.1.11: icmp\_seq=4 ttl=64 time=0.101 ms

64 bytes from 10.0.1.11: icmp\_seq=5 ttl=64 time=0.108 ms

--- 10.0.1.11 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 3997ms

rtt min/avg/max/mdev = 0.099/0.104/0.112/0.008 ms

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

64 bytes from 127.0.0.1: icmp\_seq=1 ttl=64 time=0.033 ms

64 bytes from 127.0.0.1: icmp\_seq=2 ttl=64 time=0.025 ms

64 bytes from 127.0.0.1: icmp\_seq=3 ttl=64 time=0.025 ms

64 bytes from 127.0.0.1: icmp\_seq=4 ttl=64 time=0.021 ms

64 bytes from 127.0.0.1: icmp\_seq=5 ttl=64 time=0.024 ms

--- 127.0.0.1 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 3998ms

rtt min/avg/max/mdev = 0.021/0.025/0.033/0.006 ms

**Explain the difference between pinging the local Ethernet interface and the loopback interface. Specifically, on PC1, what is the difference between typing “ping 10.0.1.11” and “ping 127.0.0.1”. (This is a conceptual question on the role of the loopback interface. The response to the ping command does not provide you with the answer to this question.)**

127.0.0.1 is a local loopback address, an virtual address, that the host uses to communicate with itself while 10.0.1.11 is an ip address assigned to the physical ethernet interface. Therefore, if the ethernet interface is not connected, ping 10.0.1.11 will fail while ping 127.0.0.1 will succeed.

**(To be completed after the lab). Find a host connected to the Internet. Send ping messages to a number of web servers on the Internet and collect statistics on the maximum round-trip delay of the ICMP Echo Request/Echo Reply. Try to find a host with a very long round-trip time. To avoid overloading the destination, do not send more than 3 ping packets to any destination machine. Save the output data and include it in your lab report.**

Pinging www.mingwangdao.com [211.149.206.190] with 32 bytes of data:

Reply from 211.149.206.190: bytes=32 time=266ms TTL=46

Reply from 211.149.206.190: bytes=32 time=265ms TTL=46

Reply from 211.149.206.190: bytes=32 time=265ms TTL=46

Ping statistics for 211.149.206.190:

Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 265ms, Maximum = 266ms, Average = 265ms

Exercise 7

**7-a:** **Include the saved output in your lab report. Explain the meaning of each field in the captured data.**

04:25:00.330294 IP 10.0.1.11 > 10.0.1.12: ICMP echo request, id 54368, seq 1, length 64

04:25:00.336191 arp who-has 10.0.1.11 tell 10.0.1.12

04:25:00.336213 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25

04:25:00.336279 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 54368, seq 1, length 64

Meaning:

Each line standards for a packet contains the ip address: 10.0.1.12. Each line starts with the time that packet is observed followed by the protocol type and information inside the packet.

The 1st line means host 10.0.1.11 sends an ICMP request to host 10.0.1.12. It also prints out the id, sequence number and length of the packet.

The 2nd line means host 10.0.1.11 sends an ARP request for the MAC address of host 10.0.1.12.

The 3rd line means host 10.0.1.11 gets an ARP reply that containing the host 10.0.1.12’s MAC address: 00:04:5a:7a:c8:25.

The 4th line means host 10.0.1.11 receives an ICMP reply from host 10.0.1.12. It also prints out the id, sequence number and length of the packet.

**7-b: Include the saved output in your lab report and interpret the results. How many of the Linux PCs responded to the broadcast ping?**

Missing ping info

04:30:04.807672 IP 10.0.1.11 > 10.0.1.255: ICMP echo request, id 7777, seq 1, length 64

04:30:04.807778 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 7777, seq 1, length 64

04:30:04.810936 arp who-has 10.0.1.11 tell 10.0.1.13

04:30:04.810964 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25

04:30:04.811030 IP 10.0.1.13 > 10.0.1.11: ICMP echo reply, id 7777, seq 1, length 64

04:30:04.814185 arp who-has 10.0.1.11 tell 10.0.1.14

04:30:04.814211 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25

04:30:04.814276 IP 10.0.1.14 > 10.0.1.11: ICMP echo reply, id 7777, seq 1, length 64

04:30:05.807187 IP 10.0.1.11 > 10.0.1.255: ICMP echo request, id 7777, seq 2, length 64

04:30:05.807274 IP 10.0.1.13 > 10.0.1.11: ICMP echo reply, id 7777, seq 2, length 64

04:30:05.807287 IP 10.0.1.12 > 10.0.1.11: ICMP echo reply, id 7777, seq 2, length 64

04:30:05.807291 IP 10.0.1.14 > 10.0.1.11: ICMP echo reply, id 7777, seq 2, length 64

04:30:09.809004 arp who-has 10.0.1.11 tell 10.0.1.12

04:30:09.809034 arp reply 10.0.1.11 is-at 00:04:5a:7a:c8:25

Interpret: each short paragraph below explains each line in above tcpdmup output.

host 10.0.1.11 sends an ICMP request to broadcast address 10.0.1.255. Packet id is 7777, sequence number is 1 and length is 64 bytes.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.12. Packet id is 7777, sequence number is 1 and length is 64 bytes.

host 10.0.1.11 receives ARP request for the MAC address of host 10.0.1.11 from host 10.0.1.13.

host 10.0.1.11 sends an ARP reply that containing the host 10.0.1.11’s MAC address: 00:04:5a:7a:c8:25.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.13. Packet id is 7777, sequence number is 1 and length is 64 bytes.

host 10.0.1.11 receives an ARP request for the MAC address of host 10.0.1.11 from host 10.0.1.14.

host 10.0.1.11 sends an ARP reply that containing the host 10.0.1.11’s MAC address: 00:04:5a:7a:c8:25.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.14. Packet id is 7777, sequence number is 1 and length is 64 bytes

host 10.0.1.11 sends an 2nd ICMP request to broadcast address 10.0.1.255. Packet id is 7777, sequence number is 2 and length is 64 bytes.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.13. Packet id is 7777, sequence number is 2 and length is 64 bytes.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.12. Packet id is 7777, sequence number is 2 and length is 64 bytes.

host 10.0.1.11 receives an ICMP reply from host 10.0.1.14. Packet id is 7777, sequence number is 2 and length is 64 bytes.

All 4 PCs response to the broadcast ping, which is 10.0.1.11, 10.0.1.12, 10.0.1.13 and 10.0.1.14, because they are all in same network.

Exercise 8

**Include the file with the captured data in your lab report. Save the details of the captured traffic, using the “Print detail” option in the Print window . Describe the differences between the files saved by tcpdump (in Part 7) and by wireshark (in this part).**

Differences:

Wireshark contains much more information about the network traffic while tcpdump only provides simple description about the packet content.

In Wireshark, all the header is shown, such as IP header, ARP header and Ethernet header, etc. In addition, information inside the header is also exhibited in Wireshark.

For example, we can see the version, header length, differentiated Services Field, Total Length, Identification, Flags, Fragment offset, Time to live, Protocol, Header checksum, Source and Destination in the IP header; the MAC address of source and destination in the Ethernet header.

Below is the output:

No. Time Source Destination Protocol Info

1 0.000000 00:04:5a:7a:c8:25 ff:ff:ff:ff:ff:ff ARP Who has 10.0.1.13? Tell 10.0.1.11

Frame 1 (42 bytes on wire, 42 bytes captured)

Arrival Time: Jun 7, 2007 04:34:46.936353000

[Time delta from previous packet: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

Packet Length: 42 bytes

Capture Length: 42 bytes

[Frame is marked: False]

[Protocols in frame: eth:arp]

[Coloring Rule Name: ARP]

[Coloring Rule String: arp]

Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

Address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

.... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)

.... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)

Source: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Type: ARP (0x0806)

Address Resolution Protocol (request)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (0x0001)

Sender MAC address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Sender IP address: 10.0.1.11 (10.0.1.11)

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 10.0.1.13 (10.0.1.13)

No. Time Source Destination Protocol Info

2 0.000082 00:04:5a:7a:c6:64 00:04:5a:7a:c8:25 ARP 10.0.1.13 is at 00:04:5a:7a:c6:64

Frame 2 (60 bytes on wire, 60 bytes captured)

Arrival Time: Jun 7, 2007 04:34:46.936435000

[Time delta from previous packet: 0.000082000 seconds]

[Time since reference or first frame: 0.000082000 seconds]

Frame Number: 2

Packet Length: 60 bytes

Capture Length: 60 bytes

[Frame is marked: False]

[Protocols in frame: eth:arp]

[Coloring Rule Name: ARP]

[Coloring Rule String: arp]

Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64), Dst: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Destination: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Source: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Type: ARP (0x0806)

Trailer: 000000000000000000000000000000000000

Address Resolution Protocol (reply)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (0x0002)

Sender MAC address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Sender IP address: 10.0.1.13 (10.0.1.13)

Target MAC address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Target IP address: 10.0.1.11 (10.0.1.11)

No. Time Source Destination Protocol Info

3 0.000095 10.0.1.11 10.0.1.13 ICMP Echo (ping) request

Frame 3 (98 bytes on wire, 98 bytes captured)

Arrival Time: Jun 7, 2007 04:34:46.936448000

[Time delta from previous packet: 0.000013000 seconds]

[Time since reference or first frame: 0.000095000 seconds]

Frame Number: 3

Packet Length: 98 bytes

Capture Length: 98 bytes

[Frame is marked: False]

[Protocols in frame: eth:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp]

Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Destination: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Source: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)

Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.1.13 (10.0.1.13)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

.... ...0 = ECN-CE: 0

Total Length: 84

Identification: 0x0000 (0)

Flags: 0x04 (Don't Fragment)

0... = Reserved bit: Not set

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: ICMP (0x01)

Header checksum: 0x2492 [correct]

[Good: True]

[Bad : False]

Source: 10.0.1.11 (10.0.1.11)

Destination: 10.0.1.13 (10.0.1.13)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0xe640 [correct]

Identifier: 0x2461

Sequence number: 1 (0x0001)

Data (56 bytes)

0000 36 d1 67 46 56 42 0e 00 08 09 0a 0b 0c 0d 0e 0f 6.gFVB..........

0010 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ................

0020 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#$%&'()\*+,-./

0030 30 31 32 33 34 35 36 37 01234567

No. Time Source Destination Protocol Info

4 0.000176 10.0.1.13 10.0.1.11 ICMP Echo (ping) reply

Frame 4 (98 bytes on wire, 98 bytes captured)

Arrival Time: Jun 7, 2007 04:34:46.936529000

[Time delta from previous packet: 0.000081000 seconds]

[Time since reference or first frame: 0.000176000 seconds]

Frame Number: 4

Packet Length: 98 bytes

Capture Length: 98 bytes

[Frame is marked: False]

[Protocols in frame: eth:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp]

Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64), Dst: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Destination: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Source: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)

Internet Protocol, Src: 10.0.1.13 (10.0.1.13), Dst: 10.0.1.11 (10.0.1.11)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

.... ...0 = ECN-CE: 0

Total Length: 84

Identification: 0x1a4a (6730)

Flags: 0x00

0... = Reserved bit: Not set

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: ICMP (0x01)

Header checksum: 0x4a48 [correct]

[Good: True]

[Bad : False]

Source: 10.0.1.13 (10.0.1.13)

Destination: 10.0.1.11 (10.0.1.11)

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0xee40 [correct]

Identifier: 0x2461

Sequence number: 1 (0x0001)

Data (56 bytes)

0000 36 d1 67 46 56 42 0e 00 08 09 0a 0b 0c 0d 0e 0f 6.gFVB..........

0010 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ................

0020 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#$%&'()\*+,-./

0030 30 31 32 33 34 35 36 37 01234567

No. Time Source Destination Protocol Info

5 0.997150 10.0.1.11 10.0.1.13 ICMP Echo (ping) request

Frame 5 (98 bytes on wire, 98 bytes captured)

Arrival Time: Jun 7, 2007 04:34:47.933503000

[Time delta from previous packet: 0.996974000 seconds]

[Time since reference or first frame: 0.997150000 seconds]

Frame Number: 5

Packet Length: 98 bytes

Capture Length: 98 bytes

[Frame is marked: False]

[Protocols in frame: eth:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp]

Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Destination: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Source: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)

Internet Protocol, Src: 10.0.1.11 (10.0.1.11), Dst: 10.0.1.13 (10.0.1.13)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

.... ...0 = ECN-CE: 0

Total Length: 84

Identification: 0x0000 (0)

Flags: 0x04 (Don't Fragment)

0... = Reserved bit: Not set

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: ICMP (0x01)

Header checksum: 0x2492 [correct]

[Good: True]

[Bad : False]

Source: 10.0.1.11 (10.0.1.11)

Destination: 10.0.1.13 (10.0.1.13)

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0xcb43 [correct]

Identifier: 0x2461

Sequence number: 2 (0x0002)

Data (56 bytes)

0000 37 d1 67 46 70 3e 0e 00 08 09 0a 0b 0c 0d 0e 0f 7.gFp>..........

0010 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ................

0020 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#$%&'()\*+,-./

0030 30 31 32 33 34 35 36 37 01234567

No. Time Source Destination Protocol Info

6 0.997235 10.0.1.13 10.0.1.11 ICMP Echo (ping) reply

Frame 6 (98 bytes on wire, 98 bytes captured)

Arrival Time: Jun 7, 2007 04:34:47.933588000

[Time delta from previous packet: 0.000085000 seconds]

[Time since reference or first frame: 0.997235000 seconds]

Frame Number: 6

Packet Length: 98 bytes

Capture Length: 98 bytes

[Frame is marked: False]

[Protocols in frame: eth:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp]

Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64), Dst: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Destination: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Source: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)

Internet Protocol, Src: 10.0.1.13 (10.0.1.13), Dst: 10.0.1.11 (10.0.1.11)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

.... ...0 = ECN-CE: 0

Total Length: 84

Identification: 0x1a4b (6731)

Flags: 0x00

0... = Reserved bit: Not set

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: ICMP (0x01)

Header checksum: 0x4a47 [correct]

[Good: True]

[Bad : False]

Source: 10.0.1.13 (10.0.1.13)

Destination: 10.0.1.11 (10.0.1.11)

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0xd343 [correct]

Identifier: 0x2461

Sequence number: 2 (0x0002)

Data (56 bytes)

0000 37 d1 67 46 70 3e 0e 00 08 09 0a 0b 0c 0d 0e 0f 7.gFp>..........

0010 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ................

0020 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f !"#$%&'()\*+,-./

0030 30 31 32 33 34 35 36 37 01234567

No. Time Source Destination Protocol Info

7 5.000016 00:04:5a:7a:c6:64 00:04:5a:7a:c8:25 ARP Who has 10.0.1.11? Tell 10.0.1.13

Frame 7 (60 bytes on wire, 60 bytes captured)

Arrival Time: Jun 7, 2007 04:34:51.936369000

[Time delta from previous packet: 4.002781000 seconds]

[Time since reference or first frame: 5.000016000 seconds]

Frame Number: 7

Packet Length: 60 bytes

Capture Length: 60 bytes

[Frame is marked: False]

[Protocols in frame: eth:arp]

[Coloring Rule Name: ARP]

[Coloring Rule String: arp]

Ethernet II, Src: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64), Dst: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Destination: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Source: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Type: ARP (0x0806)

Trailer: 000000000000000000000000000000000000

Address Resolution Protocol (request)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (0x0001)

Sender MAC address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Sender IP address: 10.0.1.13 (10.0.1.13)

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 10.0.1.11 (10.0.1.11)

No. Time Source Destination Protocol Info

8 5.000034 00:04:5a:7a:c8:25 00:04:5a:7a:c6:64 ARP 10.0.1.11 is at 00:04:5a:7a:c8:25

Frame 8 (42 bytes on wire, 42 bytes captured)

Arrival Time: Jun 7, 2007 04:34:51.936387000

[Time delta from previous packet: 0.000018000 seconds]

[Time since reference or first frame: 5.000034000 seconds]

Frame Number: 8

Packet Length: 42 bytes

Capture Length: 42 bytes

[Frame is marked: False]

[Protocols in frame: eth:arp]

[Coloring Rule Name: ARP]

[Coloring Rule String: arp]

Ethernet II, Src: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25), Dst: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Destination: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Source: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Type: ARP (0x0806)

Address Resolution Protocol (reply)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (0x0002)

Sender MAC address: 00:04:5a:7a:c8:25 (00:04:5a:7a:c8:25)

Sender IP address: 10.0.1.11 (10.0.1.11)

Target MAC address: 00:04:5a:7a:c6:64 (00:04:5a:7a:c6:64)

Target IP address: 10.0.1.13 (10.0.1.13)