David Bozarth
CES 440 – Sonoma State University
11 October 2004

Experiment 1: Basics

The objective and setup are described in the “Basics-Lab” section of CES 440 Data Communication Lab.

A primary workstation (Lab# 2B) and secondary workstation (Lab# 2C), each connected to the private lab network and to the lab internet firewall, were running in **itl-linux**. From the primary workstation, the command `ifconfig` returned interface values as follows:

```
eth0  Link encap:Ethernet  HWaddr 00:06:5B:99:7E:7F
      inet addr:130.157.166.138  Bcast:130.157.166.255  Mask:255.255.255.0

eth1  Link encap:Ethernet  HWaddr 00:00:B4:91:D9:F4
      inet addr:192.168.200.106  Bcast:192.168.200.255  Mask:255.255.255.0

lo     (Loopback)
      inet addr:127.0.0.1  Mask:255.0.0.0
```

From the subnet mask 255.255.255.0 – we see that the lower-order 8 bits are zeros. This leaves room for 255 hosts on that subnet. (Perhaps one or more of these is reserved for something, but basically, that’s the amount of space available for use within the subnet, for whatever purpose.)

Pinging `eth1` five times, returned a long first response (2746 μs) and 4 shorter responses. The reported statistics were:

```
      round-trip min/avg/max/mdev = 0.057/0.605/2.746/1.070 ms
```

Setup and behavior of eth2

Using the `ifconfig` command, `eth2` was attached to IP address 192.168.0.43. A subsequent `ifconfig` query returned the following information on `eth2`:

```
eth2      Link encap:Ethernet  HWaddr 00:00:B4:91:D8:F3
          inet addr:192.168.0.43  Bcast:192.168.0.255  Mask:255.255.255.0
```

Running `ifup eth2`, however, returned the following message:

```
      SIOCDELRT: No such process
```

On the secondary workstation, assignment of `eth2` to IP address 192.168.0.44 yielded the same result: reported as attached by `ifconfig`, but reported as “no such process” by `ifup`.

Connection with the secondary workstation

Ping to the `eth1` port of the secondary workstation returned:

```
PING 192.168.200.107 (192.168.200.107) from 192.168.200.106 : 56(84) bytes of
data.
Warning: time of day goes back, taking countermeasures.
64 bytes from 192.168.200.107: icmp_seq=0 ttl=255 time=2.801 msec
64 bytes from 192.168.200.107: icmp_seq=1 ttl=255 time=232 usec
64 bytes from 192.168.200.107: icmp_seq=2 ttl=255 time=172 usec
64 bytes from 192.168.200.107: icmp_seq=3 ttl=255 time=208 usec
64 bytes from 192.168.200.107: icmp_seq=4 ttl=255 time=170 usec


--- 192.168.200.107 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.170/0.716/2.801/1.042 ms
```

Ping to `eth2` of the secondary workstation returned:

```
PING 192.168.0.44 (192.168.0.44) from 192.168.0.43 : 56(84) bytes of data.
From 192.168.0.43: Destination Host Unreachable
From 192.168.0.43: Destination Host Unreachable
From 192.168.0.43: Destination Host Unreachable
From 192.168.0.43: Destination Host Unreachable
From 192.168.0.43: Destination Host Unreachable
From 192.168.0.43: Destination Host Unreachable

--- 192.168.0.44 ping statistics ---
8 packets transmitted, 0 packets received, +6 errors, 100% packet loss
```

Using ethereal

The `ethereal` application was started, and set up to capture icmp packets at the `eth1` port, while a series of two ping request/response cycles was initiated from the secondary workstation.

The application window has 3 panels. The top panel shows a list of the icmp packets received and sourced at `eth1`, with sequence numbers, times, and addresses. Selecting a line item (packet) in this window, activates the packet for analysis in the other two windows.

The center panel gives description details for the selected packet. It is divided into sections. The Frame section gives arrival date and time, times relative to the first and previous packets, sequence number, packet length and capture length in bytes. Another section gives MAC address and port info for the destination and source. Another section gives IP information including checksum and flags. The ICMP section gives more info including checksums.

Some differences between the descriptions for Request and Reply packets.

In the IP Differentiated Services field, the Request ID is 0x0000, but the Reply ID is non-zero. In the Flags field, the "Don't Fragment" bit is set for the Request packet, but not set for the Reply packet. Likewise, "Time to Live" is 64 for Request, 255 for Reply. The ICMP Type is 8 for Request, 0 for Reply.

The bottom panel shows the packet data represented both in hex and in ASCII. The data from the first request/reply pair is shown below:

```
0000  a1 e6 66 41 96 48 08 00 ff ff ff ff ff ff ff ff   ..fA.H..........
0010  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
0020  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
0030  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
0040  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
0050  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
0060  ff ff ff ff                                       ....
```

```
0000  a1 e6 66 41 96 48 08 00 ff ff ff ff ff ff ff ff   ..fA.H..........
0010  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
0020  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
0030  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
0040  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
0050  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff   ................
0060  ff ff ff ff                                       ....
```

It was reasonable to expect that the content of the Reply ICMP packet would be identical with that of its Request.

The outside world.

Packets were also sent from `eth0` to the www.cisco.com website, whose IP address is contained below in a portion of the description of one of the packets:

```
Internet Protocol, Src Addr: SSU37801.cs.sonoma.edu (130.157.166.155), Dst
Addr: www.cisco.com (198.133.219.25)
```

A different packet that was captured, has a source address at Sonoma State and a Broadcast destination (255.255.255.255). This packet contains as data, a partial host address at Sonoma State:

```
0000  dc 84 00 00 bc a4 a1 21 da 39 a3 ee 5e 6b 4b 0d   .......!.9..^kK.
0010  32 55 bf ef 95 60 18 90 af d8 07 09 53 53 55 33   2U...`......SSU3
0020  38 36 39 31 00                                    8691.
```

The above packet was not an ICMP packet, thus not technically part of the ping transaction between the host and remote server. It was a UDP (User Datagram Protocol) packet, likely meant for network housekeeping on the local subnet.

Most of the other packets captured from this session, had data very much like a standard “empty” `ping` packet sent from one local workstation to another. The metadata for these packets were similar also, tending to differ mostly in source vs. destination addressing, corresponding to Request and Reply packets. The data from one such packet is shown below:

```
0000  b3 e1 66 41 4c 2d 0a 00 08 09 0a 0b 0c 0d 0e 0f   ..fAL-..........
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
```

Again, it was reasonable to expect that the content of these packets would be “nothing special”, since data was not specified for this `ping` transaction.