מטלה 5 תקשורת ומחשוב

מגישים
בר גולדנברג 209894286
ספיר בוחבוט 316416429

Part 1

MyPing.c

The code has comments.

How it works:

First off, we fill the ICMP header before sending, we copy the ICMP header + ICMP Data that we want to send into the computers memory (memcpy) later we calculate the checksum and add it to the packet.

```
// Calculate the ICMP header checksum
icmphdr.icmp_cksum = calculate_checksum((unsigned short *) (packet), ICMP_HDRLEN + datalen);
memcpy ((packet), &icmphdr, ICMP_HDRLEN);
```

After that we initialize socket address information using the sockaddr_in struct

```
struct sockaddr_in dest_in;
memset (&dest_in, 0, sizeof (struct sockaddr_in));
dest_in.sin_family = AF_INET;
inet_pton(AF_INET,DESTINATION_IP,&(dest_in.sin_addr));
```

we create a Raw Socket

IPPROTO_ICMP instead of IPPROTO_RAW for icmp response

```
// Create raw socket for IP-RAW (make IP-header by yourself)
int sock = -1;
if ((sock = socket (AF_INET, SOCK_RAW, IPPROTO_ICMP)) == -1)
```

finally after setting everything up we send the ECHO REQUEST and start the timer

```
struct timeval  start,stop;
//Get time of send
gettimeofday(&start, NULL);
// Send the packet using sendto() for sending datagrams.
if (sendto (sock, packet, ICMP_HDRLEN + datalen, 0, (struct sockaddr *) &dest_in, sizeof (dest_in)) == -1)
```

after sending we receive the ECHO reply and close the timer

```
int bytes = recvfrom (sock,buff,sizeof(buff),0, (struct sockaddr*) &dest_in,&length);
if(bytes==-1){
    fprintf (stderr, "recvfrom() failed with error: %d",errno);
}
//Get time of receive
 gettimeofday(&stop, NULL);
```

How to run the program (MyPing.c):
we have included a makefile to make everything easier

run the command “make all”

```
(base) bar@bar:~/Desktop/dev/Networks_Ex5$ make all
gcc MyPing.c -o MyPing
gcc Sniffer.c -o Sniffer -lpcap
(base) bar@bar:~/Desktop/dev/Networks_Ex5$
```

run the command “sudo ./MyPing”
the program will ping google “8.8.8.8”

as seen in the screenshot we sent received 47 bytes from 8.8.8.8 (google) and the Round Trip Time is 85.411000 ms

Part 2

Sniffer.c

The code has comments.

How it works:

First we build the ethernet header struct and the ip header struct so we can access the sniffed packets feilds.

“got_packet” function:

in this function we access the sniffed packets feilds and print them to the screen. (SRC_IP,DEST_IP)

“main” function:

first we initialize a packet capture struct
and initialize a ICMP filter for packet capture.

```
pcap_t *handle;
char errbuf[PCAP_ERRBUF_SIZE];

struct bpf_program fp;
char filter_exp[] = "ip proto ICMP";
bpf_u_int32 net;
```

Then we open a live pcap session with the computers NIC in my case its called “wlo1”
feel free to change it to the NIC you want to capture packets with.

```
handle = pcap_open_live("wlo1", BUFSIZ, 1, 1000, errbuf);
//Error Detection
if (handle == NULL) {
  printf("Can't open wlo1: %s\n", errbuf);
  exit(1);
```

Now we compile filter_exp into bpf psuedo-code and add filter to pcap struct

```
// Step 2: Compile filter_exp into BPF psuedo-code
int pcaperr;
pcaperr=pcap_compile(handle, &fp, filter_exp, 0, net);
//Error Detection
if(pcaperr==-1){
  printf("%s\n",pcap_geterr(handle));
}
pcap_setfilter(handle, &fp);
```

Finally, we start capturing packets:

```
// Step 3: Capture packets
printf("Initialization Successful!\n");
printf("Capturing ICMP packets...\n");
printf("\n");
pcap_loop(handle, -1, got_packet, NULL);
```

How to run the program(Sniffer.c):

we have included a makefile to make everything easier

run the command “make all”

```
(base) bar@bar:~/Desktop/dev/Networks_Ex5$ make all
gcc MyPing.c -o MyPing
gcc Sniffer.c -o Sniffer -lpcap
(base) bar@bar:~/Desktop/dev/Networks_Ex5$
```

run the command “sudo ./Sniffer”

```
(base) bar@bar:~/Desktop/dev/Networks_Ex5$ sudo ./Sniffer
Initialization Successful!
Capturing ICMP packets...
```

open a different terminal and run MyPing to send ICMP packet

```
(base) bar@bar:~/Desktop/dev/Networks_Ex5$ sudo ./MyPing
47 bytes received from 8.8.8.8 RTT: 85.411000 ms
```

Captured Packets:

```
(base) bar@bar:~/Desktop/dev/Networks_Ex5$ sudo ./Sniffer
Initialization Successful!
Capturing ICMP packets...

From: 192.168.14.189
To: 8.8.8.8
Protocol: ICMP

From: 8.8.8.8
To: 192.168.14.189
Protocol: ICMP
```