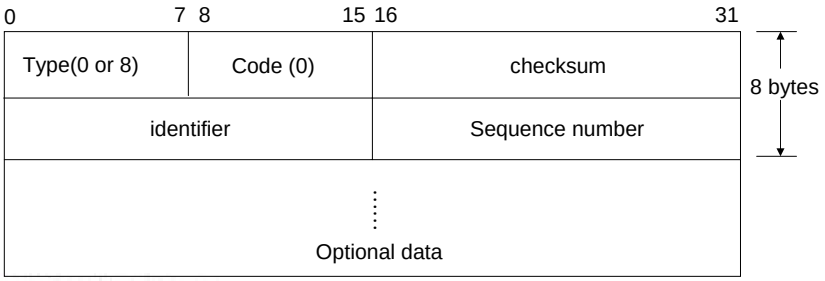
Chapter 7:
Ping Program

Introduction

- The Ping program was written by Mike Muuss and it tests whether another host is reachable.
- The program sends an ICMP echo request message to a host, expecting an ICMP echo reply to be return.
- If you can't Ping a host, you won't be able to Telnet or FTP to that host. Conversely, if you can't Telnet to a host, Ping is often the starting point to determine what the problem is.
- Ping also measures the round-trip time to the host, giving us some indication of how "far away" that host is.

Ping program

- **Client: the ping program that sends the echo requests**
  Server: the host be pinged
- **Most TCP/IP implementations support the Ping server directly in the kernel --- the server is not a user process.**
- **Format:**



Ping program (Cont.)

- **Unix implementations of ping set the *identifier* field in the ICMP massage to the process ID of the sending process.**
- **The sequence number starts at 0 and is increased every time a new echo request is sent.**
  - Ping prints the sequence number of each returned packet, allowing us to see if packets are missing, reordered, or duplicated.

Ping program (Cont.)

❑ Example: LAN Output

```
bsdi % ping svr4
PING svr4 (140.252.13.34): 56 data byres
64 bytes from 140.252.13.34: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 140.252.13.34: icmp_seq=1 ttl=255 time=0 ms
64 bytes from 140.252.13.34: icmp_seq=2 ttl=255 time=0 ms
64 bytes from 140.252.13.34: icmp_seq=3 ttl=255 time=0 ms
64 bytes from 140.252.13.34: icmp_seq=4 ttl=255 time=0 ms
64 bytes from 140.252.13.34: icmp_seq=5 ttl=255 time=0 ms
64 bytes from 140.252.13.34: icmp_seq=6 ttl=255 time=0 ms
64 bytes from 140.252.13.34: icmp_seq=7 ttl=255 time=0 ms
^?
--- svr4 ping statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

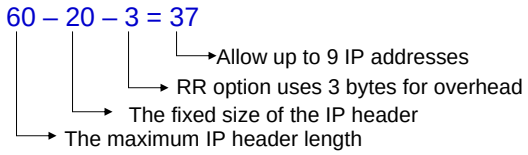
Ping program (Cont.)

- Shows the tcpdump output for this example:

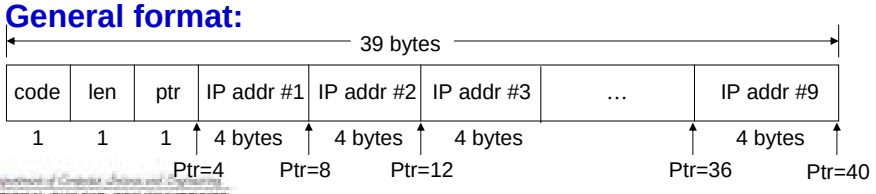
1	0.0	bsdi>svr4: icmp: echo request
2	0.003733(0.0037)	svr4>bsdi: icmp: echo reply
3	0.998045(039943	bsdi>svr4: icmp: echo request
4	1.001747(0.0037)	svr4>bsdi: icmp: echo reply
5	1.997818(039961)	bsdi>svr4: icmp: echo request
6	2.001542(0.0037)	svr4>bsdi: icmp: echo reply
7	2.997610(0.9961)	bsdi>svr4: icmp: echo request
8	3.001311(0.0037)	svr4>bsdi: icmp: echo reply
9	3.997390(0.9961)	bsdi>svr4: icmp: echo request
10	4.001115(0.0037)	svr4>bsdi: icmp: echo reply
11	4.997201(0.9961)	bsdi>svr4: icmp: echo request
12	5.000904(0.0037)	svr4>bsdi: icmp: echo reply
13	5.996977(0.9961)	bsdi>svr4: icmp: echo request
14	6.000708(0.0037)	svr4>bsdi: icmp: echo reply
15	6.996764(0.9961)	bsdi>svr4: icmp: echo request
16	7.000479(0.0037)	svr4>bsdi: icmp: echo reply

IP Record Route Option

- Most versions of ping provide the *–R* option that enables the record route (RR) feature.
- The big problem is the limited room in the IP header for the list of IP addresses.



- General format:



IP Record Route Option (Cont.)

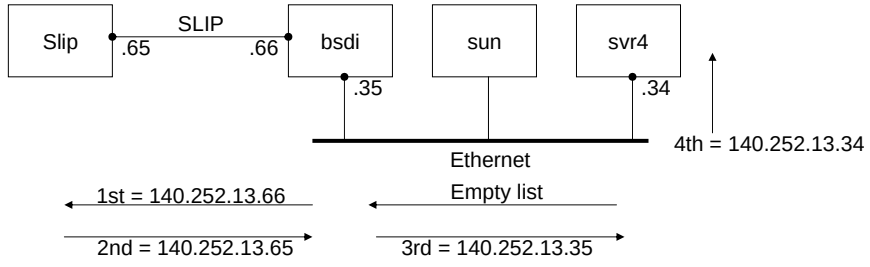
- ***Code***: a 1-byte field specifying the type of IP option.
- ***Len***: the total number of bytes of the RR option.
- ***Prt***: pointer field.
  - It is a 1-based index into the 39-byte option of where to store the next IP address. Its minimum value is 4, which is the pointer to the first IP address.
- RFC 791 [Postel 1981a] specifies that the router records the outgoing IP address.

IP Record Route Option (Cont.)

- **Normal Example**

```
Svr4 % ping –R slip
PING slip (140.252.13.65): 56 data bytes
64 bytes from 140.252.13.65: icmp_seq=0 ttl=254 time=280 ms
RR:     bsdi     (140.252.13.66)
        slip     (140.252.13.65)
        bsdi     (140.252.13.35)
        svr4     (140.252.13.34)
64 bytes from 140.252.13.65: icmp_seq=1 ttl=254 time=280 ms (same route)
64 bytes from 140.252.13.65: icmp_seq=2 ttl=254 time=270 ms (same route)
^?
--- slip ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
Round-trip min/avg/max = 270/276/280 ms
```


IP Record Route Option (Cont.)



IP Record Route Option (Cont.)

- We can watch this exchange of packets from the host sun, running tcpdump with its –v option (to see the IP options).

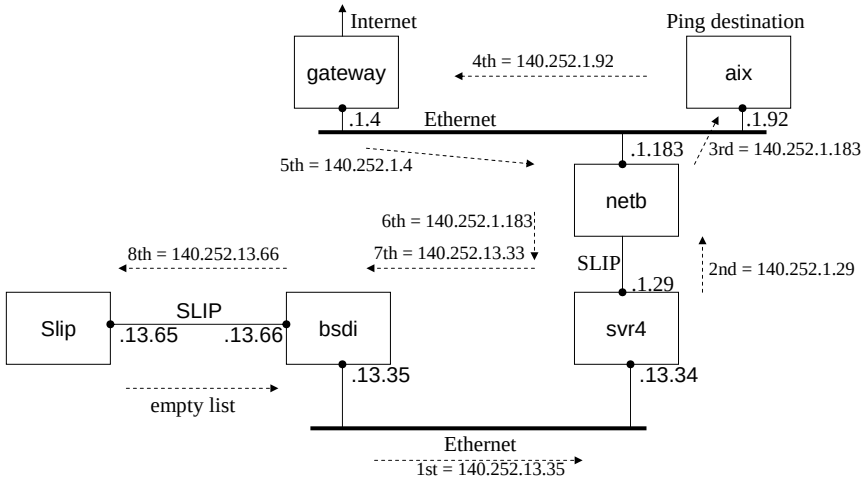
1 0.0	svr4>slip: icmp: echo request (ttl 32, id 35835, optlen=40 RR{39}=RR{#0.0.0.0/0.0.0.0/0.0.0.0/ 0.0.0.0/0.0.0.0/0.0.0.0/0.0.0.0/0.0.0.0/0.0.0.0/} EOL)
0.267746 (0.2677)	slip>svr4: icmp: echo reply (ttl 254, id 1976, optlen=40 RR{39}=RR{140.252.13.66/140.252.13.65/ 140.252.13.35/#0.0.0.0/0.0.0.0/0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0/} EOL}

IP Record Route Option (Cont.)

- **Abnormal Output**

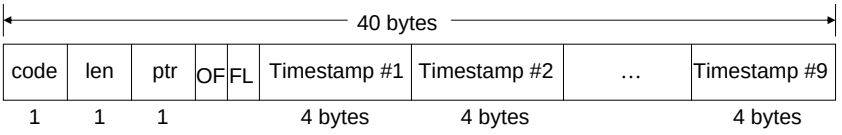
```
Slip % ping –R aix
PING aix (140.252.1.92): 56 data bytes
64 bytes from 140.252.1.92: icmp_seq=0 ttl=251 time=650 ms
RR:         bsdi (140.252.13.35)
            sun (140.252.1.29)
            netb (140.252.1.183)
            aix (140.252.1.92)
            gateway (140.252.1.4)
            netb (140.252.1.183)
            sun (140.252.1.33)
            bsdi (140.252.1.66)
            slip (140.252.1.65)
64 bytes from aix: icmp_seq=1 ttl=251 time=610 ms (same route)
64 bytes from aix: icmp_seq=2 ttl=251 time=600 ms (same route)
^?
--- aix ping statistics ---
4 packets transmitted, 3 packets received, 25% packet loss
round-trip min/avg/max = 600/652/650 ms
```

IP Record Route Option (Cont.)



IP Timestamp Option

- **The IP timestamp option is similar to the record route option.**
- **Format:**



  - len: the total length of option (normally 36 or 40)
  - ptr: a pointer to the next available entry (5, 9, 13, etc.)
  - OF: overflow, if a router can't add a timestamp because there's no room left, it just increments the overflow field.
  - FL: flag, the operation of the timestamp option is driven by the flags field

IP Timestamp Option (Cont.)

Flags	Description
0	Record only timestamps.
1	Each router records its IP address and its timestamp. There is room for only four of these pairs in the options list.
3	The sender initializes the options list with up to four of IP address and a 0 timestamp. A router records its timestamp only if the next IP address in the list matches the router's.

Summary

- The Ping program is the basic connectivity test between two systems running TCP/IP.
- It uses the ICMP echo request and echo reply messages and does not use a transport layer.
- The Ping server is normally part of the kernel's ICMP implementation.
- We looked at the normal ping output for a LAN, WAN, and SLIP links, and performed some serial line throughput calculations for a dedicated SLIP link.
- Ping also let us examine and use the IP record route option.
- We also looked at the IP timestamp option, but it is of limited practical use.