/etc/services text file

```
ftp             21/tcp
ftp             21/udp
ssh             22/tcp  # SSH Remote Login Protocol
ssh             22/udp  # SSH Remote Login Protocol
telnet          23/tcp
telnet          23/udp
smtp            25/tcp          mail
smtp            25/udp          mail
time            37/tcp          timserver
time            37/udp          timserver
```

ping boron.cs.washington.edu

PING boron.cs.washington.edu (128.95.2.210) from 216.39.173.24 : 56(84) bytes of data.
64 bytes from boron.cs.washington.edu (128.95.2.210): icmp_seq=0 ttl=238 time=74.712 msec
64 bytes from boron.cs.washington.edu (128.95.2.210): icmp_seq=1 ttl=238 time=70.264 msec
64 bytes from boron.cs.washington.edu (128.95.2.210): icmp_seq=2 ttl=238 time=68.630 msec
64 bytes from boron.cs.washington.edu (128.95.2.210): icmp_seq=3 ttl=238 time=69.668 msec
64 bytes from boron.cs.washington.edu (128.95.2.210): icmp_seq=4 ttl=238 time=70.079 msec

tcpdump –i eth1 -d

Kernel filter, protocol ALL, datagram packet socket
tcpdump: listening on eth0

Ping boron(using a known hostname)
22:41:55.042138 > 216.39.173.24 > 128.95.2.210: icmp: echo request (DF)
22:41:55.116489 < 128.95.2.210 > 216.39.173.24: icmp: echo reply

Try to connect to http://boron
22:42:02.748659 > 216.39.173.24.55771 > 128.95.2.210.http:
S 2975078981:2975078981(0) win 5840 <mss 1460,sackOK,timestamp 267274664 0,nop,wscale 0> (DF)
22:42:02.824161 < 128.95.2.210.http > 216.39.173.24.55771:
R 0:0(0) ack 2975078982 win 0 (DF)

Connecting

Send the SYN

22:42:11.682308 > 216.39.173.24.55772 > 207.25.71.5.http: S 2988657107:2988657107(0) win 5840 <mss 1460,sackOK,timestamp 267275557 0,nop,wscale 0> (DF)

Receive the SYN ACK

them > : S 2559467560:2559467560(0) ack 2988657108 win 10136 <nop,nop,timestamp 1085015529 267275557,nop,wscale 0,nop,nop,sackOK,mss 1460>

Ack the syn ack

me: . 1:1(0) ack 1 win 5840 <nop,nop,timestamp 267275569 1085015529> (DF)

Sending data

me: . 1:1449(1448) ack 1 win 5840

me: P 1449:1697(248) ack 1 win 5840

cnn: . 1:1(0) ack 1449 win 10136

cnn: P 1:255(254) ack 1697 win 10136

me: . 1697:1697(0) ack 255 win 6432

cnn: P 255:1547(1292) ack 1697 win 10136

me: . 1697:1697(0) ack 1547 win 9044

cnn: P 1547:1841(294) ack 1697 win 10136

Arp the address

bash$ /sbin/arp -n

Address	HWtype	HWaddress	Flags Mask	Iface
128.95.2.1	ether	00:00:C0:38:2D:E4	C	eth0
128.95.2.100	ether	00:E0:52:A6:E9:25	C	eth0

TCPDUMP of an arp request:

09:41:07.964893 > arp who-has 216.39.173.1 tell 216.39.173.24 (0:0:c0:9e:15:d8)

09:41:08.001051 < arp reply 216.39.173.1 is-at 0:10:67:0:3b:e2 (0:0:c0:9e:15:d8)

/sbin/route -n

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
216.39.173.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
10.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	eth1
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	216.39.173.1	0.0.0.0	UG	0	0	0	eth0

/sbin/ifconfig

```
eth0  Link encap:Ethernet  HWaddr 00:00:C0:9E:15:D8
      inet addr:216.39.173.24  Bcast:216.39.173.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:2590813 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3115512 errors:0 dropped:0 overruns:0 carrier:0
      collisions:132 txqueuelen:100
      Interrupt:10 Base address:0x250 Memory:c8000-ca000
```

```
 /usr/sbin/traceroute news.oz.net
traceroute: Warning: news.oz.net has multiple addresses; using 207.14.113.10
traceroute to news.alt.net (207.14.113.10), 30 hops max, 38 byte packets
 1  sense-sea-dsl-173-1.oz.net (216.39.173.1)  17.691 ms  16.800 ms  17.125 ms
 2  core.sea.theriver.com (216.39.128.1)  17.738 ms  17.546 ms  18.426 ms
 3  routerB.sea.theriver.com (216.39.128.41)  20.401 ms  18.999 ms  19.028 ms
 4  six.alt.net (198.32.180.10)  19.146 ms  19.456 ms  19.078 ms
 5  dosa.alt.net (207.14.113.10)  20.398 ms  18.235 ms  19.124 ms
```

Limitation

- Can only find the path from your node to someone else, not between arbitrary nodes
  - Partial solution: traceroute.org
    - A site listing MANY sites around the world that let you conduct traceroute queries from their location

Bugs

```
 1  helios.ee.lbl.gov (128.3.112.1)  0 ms  0 ms  0 ms
2  lilac-dmc.Berkeley.EDU (128.32.216.1)  39 ms  19 ms  39 ms
3  lilac-dmc.Berkeley.EDU (128.32.216.1)  19 ms  39 ms  19 ms
4  ccngw-ner-cc.Berkeley.EDU (128.32.136.23)  39 ms  40 ms  19 ms
5  ccn-nerif35.Berkeley.EDU (128.32.168.35)  39 ms  39 ms  39 ms
6  csgw.Berkeley.EDU (128.32.133.254)  39 ms  59 ms  39 ms
7  * * *
8  * * *
9  * * *
10  * * *
11  * * *
12  * * *
13  rip.Berkeley.EDU (128.32.131.22)  59 ms !  39 ms !  39 ms !
```

netstat

Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	sense-elemar-24.o:53254	ceylon.cs.washingto:ssh	ESTABLISHED
tcp	0	1	sense-elemar-24.o:55755	23.234.2.34:telnet	SYN_SENT
tcp	1	0	sense-elemar-24.o:55754	www5.cnn.com:http	CLOSE_WAIT
tcp	0	0	sense-elemar-24.o:59939	boron.cs.washington:ssh	ESTABLISHED
tcp	0	0	sense-elemar-24.o:59935	boron.cs.washington:ssh	ESTABLISHED
tcp	0	0	sense-elemar-24.o:42626	bald.cs.was:netbios-ssn	ESTABLISHED
tcp	0	0	sense-elemar-24.o:55753	i1.cnn.net:http	ESTABLISHED
tcp	0	0	sense-elemar-24.o:55752	ads.web.aol.com:http	ESTABLISHED