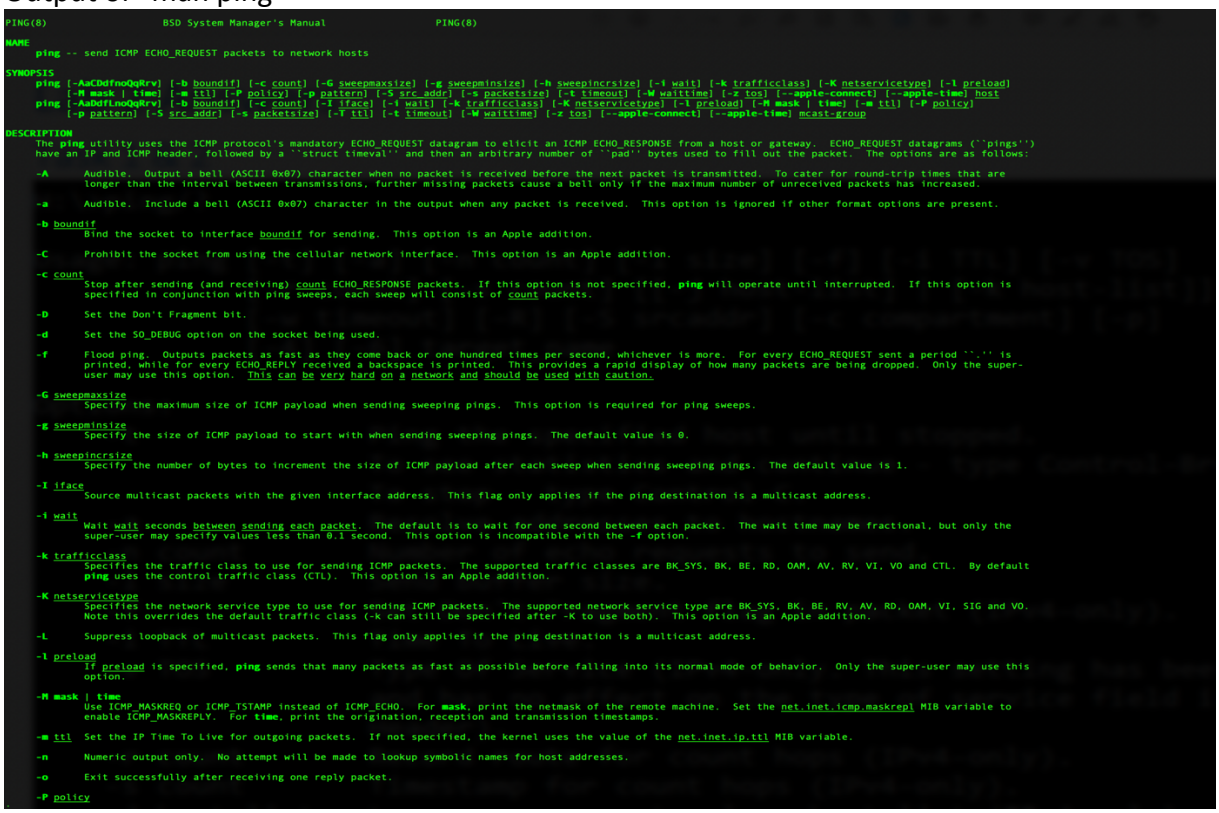
Lab 2 Answers (Mac)

Task 1&2

Output of “man ping”



```
PING(8)                   BSD System Manager's Manual                  PING(8)

NAME
     ping -- send ICMP ECHO_REQUEST packets to network hosts

SYNOPSIS
     ping [-AaCDdfnoQqRrv] [-b boundif] [-c count] [-G sweepmaxsize] [-g sweepminsize] [-h sweepincrsize] [-i wait] [-k trafficclass] [-K netservicetype] [-l preload]
          [-M mask | time] [-m ttl] [-P policy] [-p pattern] [-S src_addr] [-s packetsize] [-t timeout] [-W waittime] [-z tos] [--apple-connect] [--apple-time] host
     ping [-AaDdfLnoQqRrv] [-b boundif] [-c count] [-I iface] [-i wait] [-k trafficclass] [-K netservicetype] [-l preload] [-M mask | time] [-m ttl] [-P policy]
          [-p pattern] [-S src_addr] [-s packetsize] [-T ttl] [-t timeout] [-W waittime] [-z tos] [--apple-connect] [--apple-time] mcast-group

DESCRIPTION
     The ping utility uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway.  ECHO_REQUEST datagrams (``pings'')
     have an IP and ICMP header, followed by a ``struct timeval'' and then an arbitrary number of ``pad'' bytes used to fill out the packet.  The options are as follows:

     -A      Audible.  Output a bell (ASCII 0x07) character when no packet is received before the next packet is transmitted.  To cater for round-trip times that are
             longer than the interval between transmissions, further missing packets cause a bell only if the maximum number of unreceived packets has increased.

     -a      Audible.  Include a bell (ASCII 0x07) character in the output when any packet is received.  This option is ignored if other format options are present.

     -b boundif
             Bind the socket to interface boundif for sending.  This option is an Apple addition.

     -C      Prohibit the socket from using the cellular network interface.  This option is an Apple addition.

     -c count
             Stop after sending (and receiving) count ECHO_RESPONSE packets.  If this option is not specified, ping will operate until interrupted.  If this option is
             specified in conjunction with ping sweeps, each sweep will consist of count packets.

     -D      Set the Don't Fragment bit.

     -d      Set the SO_DEBUG option on the socket being used.

     -f      Flood ping.  Outputs packets as fast as they come back or one hundred times per second, whichever is more.  For every ECHO_REQUEST sent a period ``.'' is
             printed, while for every ECHO_REPLY received a backspace is printed.  This provides a rapid display of how many packets are being dropped.  Only the super-
             user may use this option.  This can be very hard on a network and should be used with caution.

     -G sweepmaxsize
             Specify the maximum size of ICMP payload when sending sweeping pings.  This option is required for ping sweeps.

     -g sweepminsize
             Specify the size of ICMP payload to start with when sending sweeping pings.  The default value is 0.

     -h sweepincrsize
             Specify the number of bytes to increment the size of ICMP payload after each sweep when sending sweeping pings.  The default value is 1.

     -I iface
             Source multicast packets with the given interface address.  This flag only applies if the ping destination is a multicast address.

     -i wait
             Wait wait seconds between sending each packet.  The default is to wait for one second between each packet.  The wait time may be fractional, but only the
             super-user may specify values less than 0.1 second.  This option is incompatible with the -f option.

     -k trafficclass
             Specifies the traffic class to use for sending ICMP packets.  The supported traffic classes are BK_SYS, BK, BE, RD, OAM, AV, RV, VI, VO and CTL.  By default
             ping uses the control traffic class (CTL).  This option is an Apple addition.

     -K netservicetype
             Specifies the network service type to use for sending ICMP packets.  The supported network service type are BK_SYS, BK, BE, RV, AV, RD, OAM, VI, SIG and VO.
             Note this overrides the default traffic class (-k can still be specified after -K to use both).  This option is an Apple addition.

     -L      Suppress loopback of multicast packets.  This flag only applies if the ping destination is a multicast address.

     -l preload
             If preload is specified, ping sends that many packets as fast as possible before falling into its normal mode of behavior.  Only the super-user may use this
             option.

     -M mask | time
             Use ICMP_MASKREQ or ICMP_TSTAMP instead of ICMP_ECHO.  For mask, print the netmask of the remote machine.  Set the net.inet.icmp.maskrepl MIB variable to
             enable ICMP_MASKREPLY.  For time, print the origination, reception and transmission timestamps.

     -m ttl  Set the IP Time To Live for outgoing packets.  If not specified, the kernel uses the value of the net.inet.ip.ttl MIB variable.

     -n      Numeric output only.  No attempt will be made to lookup symbolic names for host addresses.

     -o      Exit successfully after receiving one reply packet.

     -P policy
```

Output of “man traceroute”

```
TRACEROUTE(8)             BSD System Manager's Manual            TRACEROUTE(8)

NAME
     traceroute -- print the route packets take to network host

SYNOPSIS
     traceroute [-adeFISdNnrvx] [-A as_server] [-f first_ttl] [-g gateway] [-i iface] [-M first_ttl] [-m max_ttl] [-P proto] [-p port] [-q nqueries] [-s src_addr] [-t tos] [-w waittime]
                [-z pausemsecs] host [packetsize]

DESCRIPTION
     The Internet is a large and complex aggregation of network hardware, connected together by gateways.  Tracking the route one's packets follow (or finding the miscreant gateway that's dis-
     carding your packets) can be difficult.  traceroute utilizes the IP protocol `time to live' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to
     some host.

     The only mandatory parameter is the destination host name or IP number.  The default probe datagram length is 40 bytes, but this may be increased by specifying a packet size (in bytes)
     after the destination host name.

     Other options are:

     -a      Turn on AS# lookups for each hop encountered.

     -A as_server
             Turn  on  AS#  lookups  and  use the given server instead of the default.

     -d      Enable socket level debugging.

     -D      When an ICMP response to our probe datagram is received, print the differences between the transmitted packet and the packet quoted by the ICMP response.  A key showing the loca-
             tion of fields within the transmitted packet is printed, followed by the original packet in hex, followed by the quoted packet in hex.  Bytes that are unchanged in the quoted
             packet are shown as underscores.  Note, the IP checksum and the TTL of the quoted packet are not expected to match.  By default, only one probe per hop is sent with this option.

     -e      Firewall evasion mode.  Use fixed destination ports for UDP and TCP probes.  The destination port does NOT increment with each packet sent.

     -f first_ttl
             Set the initial time-to-live used in the first outgoing probe packet.

     -F      Set the "don't fragment" bit.

     -g gateway
             Specify a loose source route gateway (8 maximum).

     -i iface
             Specify a network interface to obtain the source IP address for outgoing probe packets. This is normally only useful on a multi-homed host. (See the -s flag for another way to do
             this.)

     -I      Use ICMP ECHO instead of UDP datagrams.  (A synonym for "-P icmp").

     -M first_ttl
             Set the initial time-to-live value used in outgoing probe packets.  The default is 1, i.e., start with the first hop.

     -m max_ttl
             Set the max time-to-live (max number of hops) used in outgoing probe packets.  The default is net.inet.ip.ttl hops (the same default used for TCP connections).

     -n      Print hop addresses numerically rather than symbolically and numerically (saves a nameserver address-to-name lookup for each gateway found on the path).

     -P proto
             Send packets of specified IP protocol. The currently supported protocols are: UDP , TCP , GRE and ICMP Other protocols may also be specified (either by name or by number), though
             traceroute does not implement any special knowledge of their packet formats. This option is useful for determining which router along a path may be blocking packets based on IP
             protocol number. But see BUGS below.

     -p port
             Protocol specific. For UDP and TCP, sets the base port number used in probes (default is 33434).  traceroute hopes that nothing is listening on UDP ports base to base+nhops-1 at
             the destination host (so an ICMP PORT_UNREACHABLE message will be returned to terminate the route tracing).  If something is listening on a port in the default range, this option
             can be used to pick an unused port range.

     -q nqueries
             Set the number of probes per ``ttl'' to nqueries (default is three probes).

     -r      Bypass the normal routing tables and send directly to a host on an attached network.  If the host is not on a directly-attached network, an error is returned.  This option can be
             used to ping a local host through an interface that has no route through it (e.g., after the interface was dropped by routed(8)).

     -s src_addr
             Use the following IP address (which must be given as an IP number, not a hostname) as the source address in outgoing probe packets.  On hosts with more than one IP address, this
             option can be used to force the source address to be something other than the IP address of the interface the probe packet is sent on.  If the IP address is not one of this
             machine's interface addresses, an error is returned and nothing is sent.  (See the -i flag for another way to do this.)

     -S      Print a summary of how many probes were not answered for each hop.

     -t tos  Set the type-of-service in probe packets to the following value (default zero).  The value must be a decimal integer in the range 0 to 255.  This option can be used to see if dif-
```

Task 3&4

Output of “ping www.bbc.co.uk”

```
(base) Angeloss-iMac:Labs akm$ ping www.bbc.co.uk
PING www.bbc.net.uk (212.58.237.253): 56 data bytes
64 bytes from 212.58.237.253: icmp_seq=0 ttl=53 time=21.775 ms
64 bytes from 212.58.237.253: icmp_seq=1 ttl=53 time=23.251 ms
64 bytes from 212.58.237.253: icmp_seq=2 ttl=53 time=40.008 ms
64 bytes from 212.58.237.253: icmp_seq=3 ttl=53 time=21.846 ms
64 bytes from 212.58.237.253: icmp_seq=4 ttl=53 time=34.691 ms
64 bytes from 212.58.237.253: icmp_seq=5 ttl=53 time=22.613 ms
64 bytes from 212.58.237.253: icmp_seq=6 ttl=53 time=21.559 ms
64 bytes from 212.58.237.253: icmp_seq=7 ttl=53 time=22.450 ms
64 bytes from 212.58.237.253: icmp_seq=8 ttl=53 time=25.383 ms
64 bytes from 212.58.237.253: icmp_seq=9 ttl=53 time=25.245 ms
64 bytes from 212.58.237.253: icmp_seq=10 ttl=53 time=21.578 ms
64 bytes from 212.58.237.253: icmp_seq=11 ttl=53 time=21.498 ms
64 bytes from 212.58.237.253: icmp_seq=12 ttl=53 time=21.279 ms
64 bytes from 212.58.237.253: icmp_seq=13 ttl=53 time=23.903 ms
64 bytes from 212.58.237.253: icmp_seq=14 ttl=53 time=21.834 ms
64 bytes from 212.58.237.253: icmp_seq=15 ttl=53 time=24.205 ms
64 bytes from 212.58.237.253: icmp_seq=16 ttl=53 time=22.026 ms
64 bytes from 212.58.237.253: icmp_seq=17 ttl=53 time=21.994 ms
64 bytes from 212.58.237.253: icmp_seq=18 ttl=53 time=21.707 ms
^C
--- www.bbc.net.uk ping statistics ---
19 packets transmitted, 19 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 21.279/24.150/40.008/4.765 ms
(base) Angeloss-iMac:Labs akm$
```

Output from “ping www.gla.ac.uk”

```
(base) Angeloss-iMac:Labs akm$ ping www.gla.ac.uk
PING www.gla.ac.uk (130.209.16.90): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
^C
--- www.gla.ac.uk ping statistics ---
9 packets transmitted, 0 packets received, 100.0% packet loss
```

The reason for not being able to ping the Glasgow host (www.gla.ac.uk) is because of group policies invoked by the network administrators on the University network to prevent ICMP Echo request and/or response packets to travel into and/or out of the University network. If you check the other solution sample sheet assuming we are in the SoCS lab with a windows machine you will see that internal pings are allowed and you would get a response. On the other hand, pinging a globally accessed host such as www.bbc.co.uk is successful.

Also, in contrast to Windows machines, any *BSD/Unix machine running the default ping command on a host, would continue to ping a given host until a manual keyboard interruption of the process is initiated by you (i.e. “^C” → Control-C). If you want to ping for a given period of time or send a pre-defined number of ping request packets you should use “ping -t <time in seconds> <host>” or “ping -c <number of packets> <host>” as shown next.

```
(base) Angeloss-iMac:Labs akm$ ping -t 10 www.bbc.co.uk
PING www.bbc.net.uk (212.58.233.252): 56 data bytes
64 bytes from 212.58.233.252: icmp_seq=0 ttl=52 time=30.218 ms
64 bytes from 212.58.233.252: icmp_seq=1 ttl=52 time=21.908 ms
64 bytes from 212.58.233.252: icmp_seq=2 ttl=52 time=23.171 ms
64 bytes from 212.58.233.252: icmp_seq=3 ttl=52 time=22.615 ms
64 bytes from 212.58.233.252: icmp_seq=4 ttl=52 time=30.896 ms
64 bytes from 212.58.233.252: icmp_seq=5 ttl=52 time=28.587 ms
64 bytes from 212.58.233.252: icmp_seq=6 ttl=52 time=30.415 ms
64 bytes from 212.58.233.252: icmp_seq=7 ttl=52 time=23.593 ms
64 bytes from 212.58.233.252: icmp_seq=8 ttl=52 time=22.265 ms
64 bytes from 212.58.233.252: icmp_seq=9 ttl=52 time=36.607 ms

--- www.bbc.net.uk ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 21.908/27.027/36.607/4.752 ms
```

```
(base) Angeloss-iMac:Labs akm$ ping -c 15 www.bbc.co.uk
PING www.bbc.net.uk (212.58.233.252): 56 data bytes
64 bytes from 212.58.233.252: icmp_seq=0 ttl=52 time=23.590 ms
64 bytes from 212.58.233.252: icmp_seq=1 ttl=52 time=23.653 ms
64 bytes from 212.58.233.252: icmp_seq=2 ttl=52 time=22.925 ms
64 bytes from 212.58.233.252: icmp_seq=3 ttl=52 time=22.688 ms
64 bytes from 212.58.233.252: icmp_seq=4 ttl=52 time=23.231 ms
64 bytes from 212.58.233.252: icmp_seq=5 ttl=52 time=27.057 ms
64 bytes from 212.58.233.252: icmp_seq=6 ttl=52 time=22.446 ms
64 bytes from 212.58.233.252: icmp_seq=7 ttl=52 time=23.167 ms
64 bytes from 212.58.233.252: icmp_seq=8 ttl=52 time=31.744 ms
64 bytes from 212.58.233.252: icmp_seq=9 ttl=52 time=22.488 ms
64 bytes from 212.58.233.252: icmp_seq=10 ttl=52 time=22.205 ms
64 bytes from 212.58.233.252: icmp_seq=11 ttl=52 time=22.414 ms
64 bytes from 212.58.233.252: icmp_seq=12 ttl=52 time=22.416 ms
64 bytes from 212.58.233.252: icmp_seq=13 ttl=52 time=23.765 ms
64 bytes from 212.58.233.252: icmp_seq=14 ttl=52 time=23.186 ms

--- www.bbc.net.uk ping statistics ---
15 packets transmitted, 15 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 22.205/23.798/31.744/2.406 ms
```

As shown, in the first figure we ping for 10 seconds using the “-t” flag, whereas in the second ping with the “-c” flag we pre-define to send 15 ping request packets. You can use this to get a more accurate picture of the network with regards to round-trip times to your target host, but please bear in mind that ICMP packets may be arbitrarily delayed for a number of reasons and all such measurements should be taken with a pinch of salt.

TTL, or Time-To-Live, is one of the fields of the IP header. Specifically, it is an 8-bit number (taking values in 0-255 inclusive) that is initialised to the maximum number of hops a packet can travel; in other words, the maximum number of routers through which the packet will be routed/forwarded. Every router along the route decreases the TTL value on the packet by 1, with the router that decreases it to 0 dropping the packet and not forwarding it any further. The default initial value used for ping (and other similar utilities) is OS-dependent; Linux, *BSD, and other modern Unix-based operating systems use a value of 64, while newer versions of Windows use a value of 128, but this limit is in any case configurable at the system level (i.e., the systems administrator may have changed the default to some other value).

When ping is finished sending/receiving packets, it prints out some statistics on its observations. These include the number of packets sent/received and the resulting packet loss, as well as the minimum, maximum and average (mean) values for the amount of time between sending an ICMP Echo request packet to the target host and receiving the matching ICMP Echo response packet.

Task 5

Tracert is a command used for revealing the path that a packet takes from the computer sending request to the desired destination. As discussed in the lab sheet, tracert uses ICMP Echo packets by default. As such, the limitations on ICMP traffic imposed by the ISP/group policy still apply. Keep in mind that each hop could represent a different network (in some cases on a different AS) and policies employed cannot give you the necessary output to get the full path from your machine to an end host. Commonly, the most easily obtained paths are when traceroute is employed within single domains (check the other solution sheet in which we traceroute the university server from our SoCS lab machines and it works). In the below snippets we traceroute first the BBC server and then the UofG server. By default traceroute will aim to get information up to 64 hops, thus you will receive 64 entries. As evidenced many of them do not show anything (i.e. "* * *") indicating that these hosts are members of networks in which policies for not responding back to ICMP ping requests. Hence, the result is that in many cases we are unable to receive responses from hosts outside our network, hence only the responses from the first few hops en route to www.bbc.co.uk and www.gla.ac.uk are received and printed.

Output from home machine when "traceroute www.bbc.co.uk"

```
(base) Angeloss-iMac:Labs akm$ traceroute www.bbc.co.uk
traceroute: Warning: www.bbc.co.uk has multiple addresses; using 212.58.233.253
traceroute to www.bbc.net.uk (212.58.233.253), 64 hops max, 52 byte packets
 1  * bthomehub (191.167.1.254)  2.205 ms  1.963 ms
 2  * * *
 3  * * *
 4  81.139.56.168 (81.139.56.168)  33.582 ms  24.023 ms  24.015 ms
 5  213.121.192.142 (213.121.192.142)  23.137 ms
    core1-hu0-6-0-6.colindale.ukcore.bt.net (213.121.192.0)  24.237 ms
    213.121.192.136 (213.121.192.136)  24.663 ms
 6  194.72.16.72 (194.72.16.72)  24.241 ms
    peer7-et-4-1-1.telehouse.ukcore.bt.net (194.72.16.134)  36.185 ms
    peer8-et-0-0-4.telehouse.ukcore.bt.net (109.159.252.158)  24.831 ms
 7  109.159.253.15 (109.159.253.15)  32.081 ms
    109.159.253.13 (109.159.253.13)  37.112 ms
    195.99.126.71 (195.99.126.71)  33.985 ms
 8  * * *
 9  * * *
10  ae2.er01.lbh.bbc.co.uk (132.185.249.7)  26.848 ms  25.484 ms  25.055 ms
11  132.185.252.126 (132.185.252.126)  39.002 ms  35.878 ms  34.077 ms
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
31  * * *
32  * * *
33  * * *
34  * * *
35  * * *
36  * * *
37  * * *
38  * * *
39  * * *
40  * * *
41  * * *
42  * * *
43  * * *
44  * * *
45  * * *
46  * * *
47  * * *
48  * * *
49  * * *
50  * * *
51  * * *
52  * * *
53  * * *
54  * * *
55  * * *
56  * * *
57  * * *
```

```
58  * * *
59  * * *
60  * * *
61  * * *
62  * * *
63  * * *
64  * * *
(base) Angeloss-iMac:Labs akm$
```

Output from home machine when “traceroute www.gla.ac.uk ”

```
(base) Angeloss-iMac:Labs akm$ traceroute www.gla.ac.uk
traceroute to www.gla.ac.uk (130.209.16.90), 64 hops max, 52 byte packets
 1  bthomehub (191.167.1.254)  5.502 ms  2.081 ms  2.041 ms
 2  * * *
 3  81.139.56.169 (81.139.56.169)  24.867 ms  23.381 ms  23.343 ms
 4  81.139.56.168 (81.139.56.168)  25.000 ms  24.309 ms  23.729 ms
 5  core1-hu0-15-0-6.colindale.ukcore.bt (213.121.192.8)  22.594 ms
    core2-hu0-12-0-1.colindale.ukcore.bt.net (195.99.127.118)  23.705 ms
    core2-hu0-16-0-9.colindale.ukcore.bt.net (213.121.192.46)  24.084 ms
 6  peer7-et-7-0-4.telehouse.ukcore.bt.net (62.172.103.164)  23.709 ms
    peer2-et-3-0-4.slough.ukcore.bt.net (109.159.252.122)  26.895 ms
    peer7-et-4-1-1.telehouse.ukcore.bt.net (194.72.16.134)  23.858 ms
 7  195.99.126.63 (195.99.126.63)  23.719 ms  37.406 ms
    linx-gw1.ja.net (195.66.224.15)  28.214 ms
 8  ae23.londtt-sbr1.ja.net (146.97.35.169)  23.693 ms  24.172 ms  23.854 ms
 9  ae28.londtw-sbr2.ja.net (146.97.33.62)  23.893 ms  28.233 ms  25.745 ms
10  ae31.lowdss-sbr1.ja.net (146.97.33.29)  26.394 ms  27.313 ms  25.944 ms
11  ae29.leedaq-sbr2.ja.net (146.97.33.49)  29.030 ms  31.134 ms  29.619 ms
12  ae28.glasss-sbr1.ja.net (146.97.33.57)  33.526 ms  32.409 ms  32.354 ms
13  ae26.glasjw-rbr1.ja.net (146.97.38.26)  37.648 ms  33.735 ms  34.553 ms
14  146.97.154.2 (146.97.154.2)  34.543 ms  41.501 ms  43.808 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
31  * * *
32  * * *
33  * * *
34  * * *
35  * * *
36  * * *
37  * * *
38  * * *
39  * * *
40  * * *
41  * * *
42  * * *
43  * * *
44  * * *
45  * * *
46  * * *
47  * * *
48  * * *
49  * * *
50  * * *
51  * * *
52  * * *
53  * * *
54  * * *
55  * * *
56  * * *
57  * * *
58  * * *
59  * * *
60  * * *
61  * * *
62  * * *
63  * * *
64  * * *
(base) Angeloss-iMac:Labs akm$
```