Basic UNIX Networking SysAdmin Files/Commands

Focus is on getting information from system

Files

/etc/hosts - ip address/DNS names
/etc/networks - net ip addr/local names
/etc/protocols - protocol constants
/etc/services - port assignments

Commands - gathering info

netstat -a - print udp/tcp ports in use
netstat -i - print network i/f info
ifconfig ifname etc... - i/f setup info
netstat -r - routing table
netstat -s - tcp stack stats
netstat -m- network buf usage
arp - print arp table
NFS
    rpcinfo/nfsstat
    showmount/df (not shown below)
ps -ax - network daemons

 # /etc/hosts

```
127.0.0.1          localhost
131.252.20.183     sirius.cs.pdx.edu sirius
131.252.21.183     sirius-suncs.cs.pdx.edu
sirius-suncs
131.252.20.10      psur1.cs.pdx.edu psur1
```

 # /etc/networks

```
loopback-net   127          software-
    loopback-net loopback
cs-pdx-net 131.252.20     cs-lan
suncs-pdx-net  131.252.21      suncs-lan
```

 # /etc/protocols

```
ip   0    IP   # internet protocol, pseudo
protocol number
icmp    1    ICMP  # internet control message
protocol
tcp 6    TCP     # transmission control
protocol
udp      17  UDP    # user datagram protocol
```

 # /etc/services

tcpmux	1/tcp	# rfc-1078
echo	7/tcp	
echo	7/udp	
discard	9/tcp	sink null
discard	9/udp	sink null
ftp-data	20/tcp	
ftp	21/tcp	
telnet	23/tcp	
smtp	25/tcp	mail
domain	53/udp	
domain	53/tcp	
sunrpc	111/udp	
sunrpc	111/tcp	
who	513/udp	whod
route	520/udp	router routed

AND MORE...

 # netstat -a

```
Active Internet connections (including
servers)
Proto Recv-Q Send-Q  Local Address
Foreign Address        (state)
udp        0      0  *.1614                 *.*
udp        0      0  *.echo                 *.*
udp        0      0  *.syslog               *.*
udp        0      0  *.domain                 *.*
udp        0      0  *.route                *.*
udp        0      0  *.sunrpc                *.*
tcp        0      0  rigel.cs.pdx.edu.telne
crg8.sequent.com.51126 ESTABLISHED
tcp        0      0  *.echo                 *.*
LISTEN
tcp        0      0  *.telnet               *.*
LISTEN
tcp        0      0  *.ftp                *.*
LISTEN
tcp        0      0  *.sunrpc               *.*
LISTEN
```

 # netstat -i(n)

```
Name  Mtu  Net/Dest      Address        Ipkts
      Ierrs Opkts  Oerrs Collis Queue
le0   1500 cs-pdx-net    rigel.cs.pdx.edu
      3415184 1    3217316 14   101489 0
le1   1500 suncs-pdx-net rigel-
      suncs.cs.pdx.edu 323426  0    478075
      9162    0
lo0   1536 127.0.0.0     localhost.cs.pdx.edu
      593555  0    593555  0    0      0
```

 # ifconfig le0

```
le0:
flags=63<UP,BROADCAST,NOTRAILER
S,RUNNING>
inet 131.252.20.183 netmask ffffff00
broadcast 131.252.20.0
```

note: ifconfig used to set ip addrs at boot

 # netstat -r

```
Routing tables
Destination      Gateway          Flags   Refcnt
    Use      Interface
localhost.cs.pdx.edu localhost.cs.pdx.edu
    UH1    7878    lo0
131.252.56.0   psur1.cs.pdx.edu        UG0
    0    le0
131.252.80.0   psur1.cs.pdx.edu        UG0
    0    le0
default        psur1.cs.pdx.edu        UG0    0
    le0
cc-pdx-net psur1.cs.pdx.edu        UG0
    43932  le0
cs-pdx-net rigel.cs.pdx.edu        U    69
    3487675    le0
suncs-pdx-net  rigel-suncs.cs.pdx.e    U    6
    256156      le1
```

#netstat -s

udp:
    0 incomplete headers
    0 bad data length fields
    0 bad checksums
    0 socket overflows
tcp:
    3241529 packets sent
        2610326 data packets (1068380133 bytes)
        5458 data packets (3331016 bytes) retransmitted
    3304840 packets received
        2147382 acks (for 1070487523 bytes)
        10484 duplicate acks
        0 acks for unsent data
        2175326 packets (173167748 bytes) received in-sequence
        13053 completely duplicate packets (222443 bytes)

558 packets with some dup. data (22753 bytes duped)
6729 out-of-order packets (1082423 bytes)
99 packets (69 bytes) of data after window
69 window probes
47026 window update packets
149 packets received after close
24 discarded for bad checksums
0 discarded for bad header offset fields
0 discarded because packet too short
4330 connection requests
2282 connection accepts
6534 connections established (including accepts)
7230 connections closed (including 206 drops)
82 embryonic connections dropped
2139678 segments updated rtt (of 2146340 attempts)

icmp:
    1309 calls to icmp_error
    0 errors not generated 'cuz old message too short
    0 errors not generated 'cuz old message was icmp
    Output histogram:
        echo reply: 10
        destination unreachable: 1297
        routing redirect: 41
        time exceeded: 12
        address mask reply: 4
    20 messages with bad code fields
    0 messages with bad length
    Input histogram:
        echo reply: 2
        destination unreachable: 2515
        source quench: 31
        echo: 10
        time exceeded: 25
        address mask request: 4
    14 message responses generated

ip:

4342156 total packets received

1 bad header checksum

0 with size smaller than minimum

0 with data size < data length

0 with header length < data size

0 with data length < header length

28991 fragments received

2 fragments dropped (dup or out of space)

1 fragment dropped after timeout

128411 packets forwarded

0 packets not forwardable

41 redirects sent

0 ip input queue drops

 # netstat -m

509/1024 mbufs in use:
    49 mbufs allocated to packet headers
    156 mbufs allocated to socket structures
    233 mbufs allocated to protocol control blocks
    65 mbufs allocated to routing table entries
    3 mbufs allocated to socket names and addresses
    3 mbufs allocated to interface addresses
0/28 cluster buffers in use
156 Kbytes allocated to network (40% in use)
0 requests for memory denied
0 requests for memory delayed
0 calls to protocol drain routines

 # arp -a (SunOs)

banshee.cs.pdx.edu (131.252.20.128) at
    0:0:a7:0:2d:a0
pdx-gwy.cs.pdx.edu (131.252.20.1) at
    0:0:c:0:f9:17
longshot.cs.pdx.edu (131.252.20.129) at
    8:0:11:1:44:68
walt-suncs.cs.pdx.edu (131.252.21.2) at
    8:0:20:e:21:25
walt-cs.cs.pdx.edu (131.252.20.2) at
    8:0:20:e:21:25
connor.cs.pdx.edu (131.252.21.179) at
    0:0:c0:c5:57:10
dazzler.cs.pdx.edu (131.252.21.132) at
    8:0:11:1:12:82
sprite.cs.pdx.edu (131.252.21.133) at
    8:0:11:1:12:e7
eecs.cs.pdx.edu (131.252.20.118) at
    8:0:47:0:25:11
thunderbird.cs.pdx.edu (131.252.20.166) at
    8:0:11:1:44:69

 # rpcinfo -p

```
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100004    2   udp    672  ypserv
    100004    2   tcp    673  ypserv
    100004    1   udp    672  ypserv
    100004    1   tcp    673  ypserv
    100007    2   tcp   1024  ypbind
    100007    2   udp   1027  ypbind
    100007    1   tcp   1024  ypbind
    100007    1   udp   1027  ypbind
    100028    1   tcp    677  ypupdated
    100028    1   udp    679  ypupdated
    100003    2   udp   2049  nfs
    100005    1   udp    720  mountd
    100005    2   udp    720  mountd
    100005    1   tcp    723  mountd
    100005    2   tcp    723  mountd
    100026    1   udp    733  bootparam
    100021    1   tcp    736  nlockmgr
```

 # nfsstat

Server rpc:
calls badcalls nullrecv badlen
xdrcall
288507 0 0 0 0

Server nfs:
calls badcalls
288507 50
null getattr setattr root lookup
readlink read
139 0% 36413 12% 3705 1% 0 0%
187621 65% 1460 0% 22846 7%
wrcache write create remove
rename link symlink
0 0% 10554 3% 6939 2% 916 0%
491 0% 19 0% 14 0%
mkdir rmdir readdir fsstat
153 0% 23 0% 15999 5% 1215 0%

Client rpc:
calls badcalls retrans badxid timeout wait newcred timers
17069 440 16 47 444 0 0 526

Client nfs:
calls badcalls nclget nclsleep
16644 15 16644 0
null getattr setattr root lookup readlink read
0 0% 2896 17% 19 0% 0 0% 8215 49% 2877 17% 1595 9%
wrcache write create remove rename link symlink
0 0% 27 0% 27 0% 28 0% 4 0% 1 0% 1 0%
mkdir rmdir readdir fsstat
1 0% 0 0% 780 4% 173 1%

 # ps ax

```
  PID TT STAT  TIME COMMAND
    0 ?  D     1:09 swapper
    1 ?  IW    0:04 /sbin/init -
    2 ?  D     0:01 pagedaemon
   68 ?  IW    0:31 portmap
   71 ?  IW   17:24 ypserv
   73 ?  IW    0:00 ypbind
   76 ?  IW    0:00 rpc.ypupdated
   83 ?  S     2:35 in.routed
   89 ?  S     3:51 /usr/local/lib/named/named
   91 ?  I     0:00  (biod)
   92 ?  I     0:00  (biod)
   93 ?  I     0:00  (biod)
   94 ?  I     0:00  (biod)
  104 ?  IW    0:11 syslogd
  111 ?  IW    0:05 /usr/lib/sendmail -bd -q1h
  117 ?  I     2:11  (nfsd)
  118 ?  IW    0:04 rpc.mountd -n
  119 ?  I     2:11  (nfsd)
  120 ?  I     2:17  (nfsd)
  121 ?  I     2:19  (nfsd)
```

```
  123 ?  I     2:16  (nfsd)
  124 ?  I     2:20  (nfsd)
  125 ?  I     2:15  (nfsd)
  126 ?  I     2:13  (nfsd)
  127 ?  IW    0:00 rarpd -a
  128 ?  IW    0:00 rarpd -a
  129 ?  IW    0:00 rarpd -a
  130 ?  IW    0:00 rarpd -a
  132 ?  IW    0:00 rpc.bootparamd
  135 ?  IW    0:00 rpc.lockd
  136 ?  IW    0:00 rpc.statd
  141 ?  S     1:16 automount -m -f
/etc/auto.master
  155 ?  IW   11:08
/usr/local/lib/nn/nnmaster -l -C -r
  172 ?  IW    7:57 update
  175 ?  IW    0:04 cron
  184 ?  IW    0:11 inetd -r 60 60
  187 ?  IW    0:00 /usr/lib/lpd
 3991 ?  IW    0:00 in.telnetd
 4543 ?  IW    0:00 /usr/lib/lpd
```

```
 4876 ?  TW    0:00 -sendmail hford
(sendmail)
 4877 ?  TW    0:00 mail -d hford
```