Unix Networking Commands

The following information consists of various UNIX networking and system administration commands that you may wish to learn. This is not a formal homework, it is just something I suggest you investigate at least a little for your own edification.

Please read the man pages and try to experiment with the commands when possible. You need root access to do some of the commands, but you can at least look at the man pages to see how the programs operate. For example, use

```
> man arp
```

to read the man page on arp.

For now I just want you to be aware of the commands and have an idea of what they do. If you need to learn a program in more detail you at least have a place to start. Being a sysadmin is tough and it can take a long time to really learn how everything works.

Most of the programs for the UAA math system (i.e. saturn, mazzy) are stored in

```
/usr/sbin.
```

This will be different for other operating systems. For example, SunOS stores most of these in /usr/etc instead.

You might want to add /usr/sbin to your path if you can't execute them. If you are using saturn with bash, then add :/usr/sbin to the end of your PATH in your .profile file.

Common System Administrator files and commands

Network Status commands

- netstat <seconds>
  running error stats + counts on config interface every N seconds
- netstat –a
  socket ports and state
- netstat -s
  protocol (tcp etc.) counts and errors
- netstat -r
  routing table dump
- netstat –i
  list of interfaces and gives 3 letter interface names

If you use the –n flag, host addressed will be numeric and avoid a DNS lookup, which might be faster in some cases. Combine with the other switches.

Network interfaces commands

- ifconfig –a
  Show all interfaces
- ifconfig <interface name>
  setup for a particular interface, e.g. ln0

- ifconfig <interface name> <params>
  Set params of the interface. Root only. Typically IP address, subnet, are set upon bootup in /etc/rc*
  ROOT ONLY

Connectivity

- ping <host>
  send an ICMP echo message (one packet) to a host.
  This may go continually until you hit Control-C.
  Ping means a packet was sent from your machine via ICMP, and echoed at the IP level. ping tells you if the OS is up; but doesn't tell you if inetd or other daemons are running.

- telnet host <port>
  talk to "hosts" at the given port number. By default, the telnet port is port 23. See the file /etc/services for a list of what services are in use at what ports. A few samples:

  7 – echo port, use control-] to get out
  25 – SMTP, use to send mail
  79 - Finger

- telnet ip-number
  Can tell if inetd is functioning. With telnet you can use the ip number instead of the host name. If ip-number as opposed to telnet hostname works, you have problems with the name server. If you can ping, but you can't telnet, you have problems with getting processes running and possibly inetd configuration problems.

Routing

- netstat –r
  Print routing tables. The routing tables are stored in the kernel and used by ip to route packets to non-local networks.

- route ... params
  The route command is used for setting a static (non-dynamic by hand route) route path in the route tables. It is typically used at boot in the /etc/rc scripts. It can be used for setting a default route; i.e., when in doubt send all packets to a particular local gateway. Generally **ROOT ONLY**.
- routed
  The BSD daemon that does dynamic routing. Started at boot. This runs the RIP routing protocol. **ROOT ONLY**. You won't be able to run this without root access.
- gated
  Gated is an alternative routing daemon to RIP. It uses the OSPF, EGP, and RIP protocols in one place. **ROOT ONLY**.
- traceroute <host>
  Useful for tracing route of IP packets. The packet causes message to be sent back from all gateways in between the source and destination.

Arp

- arp –a
  Print the arp table. Arp is used to translate IP addresses into Ethernet addresses. Root can add and delete arp entries. Deleting them can be useful if an arp entry is malformed or just wrong. Arp entries explicitly added by root are permanent -- they can also be by proxy. The arp table is stored in the kernel and manipulated dynamically. Arp entries are cached and will time out and are deleted normally in 20 minutes.

NFS/NIS

Network file system/yellow pages

- df .
  Shows your filesystem and mount for the current directory
- df -t nfs
  Show nfs mounts.
- mount
  Use to mount a file system, **ROOT ONLY**.
  /etc/fstab contains the mounts done at boot time.
  /etc/exports contains mount points exported on a suste,/
  /etc/mtab contains the mount table built by mount.

Other Useful Commands

- ps aux or ps alx

  List of processes in action, usage varies from system to system.

  "ps -aux | grep <string> " often useful to filter output by string

- ps

  List your processes in the foreground.

- nslookup (or nslookup <host>)

  Makes queries to the DNS server to translate IP to a name, or vice versa.

- ftp <host>

  Transfer files to host. Often can use login="anonymous" , p/w="guest"

- rcp <switches> system:file system:file

  Rcp performs a remote copy from one system to another, and is used much like Unix cp. Rcp and rsh use rshd which is controlled by inetd. The rshd security protocol is very weak, and uses the .rhosts and /etc/hosts.equiv files. Since security is so weak these protocols are often banned from systems (e.g., add "*" to rhosts and anyone could log into your account).
- rsh host <command>

  BSD remote shell.

- rlogin <host> -l <login>

  Logs into the host with a virtual terminal like telnet.

Important Files

/etc/hosts - names to ip addresses
/etc/networks - network names to ip addresses
/etc/protocols - protocol names to protocol numbers
/etc/services - tcp/udp service names to port numbers

Not all programs use these services.

ROOT ONLY *daemons started at boot:*

inetd

> inetd is the BSD mother daemon that listens on the apps in /etc/inetd.conf and makes connections for these other daemons.

sendmail

> Sendmail runs the SMTP mail protocol on tcp port 25. If you telnet to port 25, you are talking directly to sendmail. Some old configurations allowed forgeries to be made in this fashion (mail relaying) but that has been mostly disabled today.