Network toolbox
Utilities to Configure and Troubleshoot Network Connections

The following list shows common networking tools and files you should be familiar with as a networking professional.

When using these utilities the output may occupy more than one screen. If that happens, you will need to pipe your terminal output to a pager { more | less } to view everything.

Unfortunately, there are minor variations in the tool options and syntax between operating systems. They may even vary between Linux distros or BSD flavors (and will certainly be different in MS-Windows). The man pages should be consulted for details of each tool or file on your system.

Tools and Files:

ifconfig – configure network interfaces, (lo, eth0)
ping – test network connectivity, uses ICMP
traceroute – show the route packets take to a network host, ttl and ICMP
host – dns lookup (also nslookup)
dig – dns lookup (reverse lookup = dig -x ipaddr), “domain internet groper”
netstat – network status
route – view and manipulate the routing tables
whois – Internet domain name and network number directory service

ssh – secure shell access to a remote system, used for network administration
nc (netcat) – tool for working with sockets
nmap – network exploration and security auditing tool (NOT available on cs server)

> WARNING: Do not use nmap on networks you do not administer. Administrators view traffic generated by this tool as attack traffic. You could lose your network privileges, your ISP may disconnect you, and the FBI may invite you on a free trip to a foreign country for questioning.

/etc/hosts – maps hostnames to IP addresses, must include reference to localhost
/etc/resolv.conf – name resolver configuration
/etc/services – network service name database
/etc/protocols – network protocol database

Finally, you should be aware of any packet filtering on the machine you are working from. Firewalls (packet filters) often create problems or interfere with troubleshooting. Also, do NOT disable or block ICMP on your hosts, it is a vital part of networking. The extremely paranoid may do some filtering of inbound ICMP, but outright blocking all ICMP traffic will cause you headaches.

Run the following commands on the CS Server and describe what they do.

Command	Purpose (what it tells you) and Output of command
> host www.una.edu	
> ping -c 4 www.yahoo.com	
> ifconfig em0	
> route show -inet	

> netstat =anf inet	
> netstat -anf inet6	
> dig www.una.edu	
> dig -t MX backwoods.science	

> dig -t RRSIG isc.org	
> traceroute -I caida.org	
> host undeadly.org	
> cat /etc/resolv.conf	

> less /etc/services	
> less /etc/protocols	
> echo “GET / HTTP/1.0\r\n\r\n” | nc www.una.edu 80	
> whois una.edu	