Basic network commands

ping

The ping command (named after the sound of an active sonar system) sends echo requests to the host specified on the command line, and lists the responses received.

$ ping ipAddress or hostname

e.g

$ ping www.vit.ac.in

• ping - sends an ICMP *ECHO_REQUEST* packet to the specified host. If the host responds, an ICMP packet is received.

• One can “ping” an IP address to see if a machine is alive.

• It provides a very quick way to see if a machine is up and connected to the network.

netstat

• It works with the LINUX Network Subsystem, it will tell you what the status of ports are ie. open, closed, waiting connections. It is used to display the TCP/IP network protocol statistics and information.

tcpdump

This is a sniffer, a program that captures packets off a network interface and interprets them.

hostname

Tells the user the host name of the computer they are logged into.

traceroute

traceroute will show the route of a packet. It attempts to list the series of hosts through which your packets travel on their way to a given destination.

Command syntax:

traceroute machine_name_or_ip

e.g traceroute www.vit.ac.in

Each host will be displayed, along with the response times at each host.

`finger`

Retrieves information about the specified user.

e.g finger bit50001

ifconfig (In Windows use ipconfig)

This command is used to configure network interfaces, or to display their current configuration.

dig

The "domain information groper" tool. If you give a hostname as an argument to output information about that host, including it's IP address, hostname and various other information.

e.g dig vitlinux

`telnet`

`telnet` allows you to log in to a computer, just as if you were sitting at the terminal. Once your username and password are verified, you are given a shell prompt. From here, you can do anything requiring a text console.

`ftp`

To connect to an FTP server use

`ftp ipaddress`

netstat

Displays contents of /proc/net files. It works with the LINUX Network Subsystem, it will tell you what the status of ports are ie. open, closed, waiting, masquerade connections. It will also display various other things. It has many different options.

tcpdump

This is a sniffer, a program that captures packets off a network interface and interprets them for you. It understands all basic internet protocols, and can be used to save entire packets for later inspection.

ping

The ping command (named after the sound of an active sonar system) sends echo requests to the host you specify on the command line, and lists the responses received their round trip time.

You simply use ping as:

```
ping ip_or_host_name
```

hostname

Tells the user the host name of the computer they are logged into. Note: may be called *host.*

traceroute

traceroute will show the route of a packet. It attempts to list the series of hosts through which your packets travel on their way to a given destination. Also have a look at *xtraceroute* (one of several graphical equivalents of this program).

Command syntax:

```
traceroute machine_name_or_ip
```

tracepath

tracepath performs a very simlar function to *traceroute* the main difference is that *tracepath* doesn't take complicated options.

Command syntax:

```
tracepath machine_name_or_ip
```

findsmb

findsmb is used to list info about machines that respond to SMB name queries (for example windows based machines sharing their hard disk's).

Command syntax:

```
Findsmb
```

This would find all machines possible, you may need to specify a particular subnet to query those machines only...

nmap

“ network exploration tool and security scanner”. *nmap* is a very advanced network tool used to query machines (local or remote) as to whether they are up and what ports are open on these machines.

A simple usage example:

```
nmap machine_name
```

This would query your own machine as to what ports it keeps open. *nmap* is a very powerful tool, documentation is available on the nmap site as well as the information in the manual page.

telnet

Someone once stated that telnet(1) was the coolest thing he had ever seen on computers. The ability to remotely log in and do stuff on another computer is what separates Unix and Unix-like operating systems from other operating systems.

telnet allows you to log in to a computer, just as if you were sitting at the terminal. Once your username and password are verified, you are given a shell prompt. From here, you can do anything requiring a text console. Compose email, read newsgroups, move files around, and so on. If you are running X and you telnet to another machine, you can run X programs on the remote computer and display them on yours.

To login to a remote machine, use this syntax:

```
% telnet <hostname>
```

If the host responds, you will receive a login prompt. Give it your username and password. That's it. You are now at a shell. To quit your telnet session, use either the exit command or the logout command.

> telnet does not encrypt the information it sends. Everything is sent in plain text, even passwords. It is not advisable to use telnet over the Internet. Instead, consider the Secure Shell. It encrypts all traffic and is available for free.

The other use of telnet

Now that we have convinced you not to use the telnet protocol anymore to log into a remote machine, we'll show you a couple of useful ways to use telnet.

You can also use the telnet command to connect to a host on a certain port.

```
% telnet <hostname> [port]
```

This can be quite handy when you quickly need to test a certain service, and you need full control over the commands, and you need to see what exactly is going on. You can interactively test or use an SMTP server, a POP3 server, an HTTP server, etc. this way.

In the next figure you'll see how you can telnet to a HTTP server on port 80, and get some basic information from it.

Figure 13-1. Telnetting to a webserver

```
% telnet store.slackware.com 80

Trying 69.50.233.153...

Connected to store.slackware.com.

Escape character is '^]'.

HEAD / HTTP/1.0



HTTP/1.1 200 OK

Date: Mon, 25 Apr 2005 20:47:01 GMT

Server: Apache/1.3.33 (Unix) mod_ssl/2.8.22 OpenSSL/0.9.7d

Last-Modified: Fri, 18 Apr 2003 10:58:54 GMT

ETag: "193424-c0-3e9fda6e"

Accept-Ranges: bytes

Content-Length: 192

Connection: close

Content-Type: text/html
```

Connection closed by foreign host.

%

1-)arp :

When we need an Ethernet (MAC) address we can use arp(address resolution protocol).

In other words it shows the physical address of an host.

Example:

C:\Documents and Settings\sysadm>arp -a

Interface: 169.254.195.199 --- 0x2

Internet Address Physical Address Type

216.109.127.60 00-53-45-00-00-00 static

2-)nslookup:

Displays information from Domain Name System (DNS) name servers.

Example:

C:\Documents and Settings\sysadm>nslookup itu.dk

Server: ns3.inet.tele.dk

Address: 193.162.153.164

Non-authoritative answer:

Name: itu.dk

Address: 130.226.133.2

NOTE :If you write the command as above it shows as default your pc's server name firstly.

C:\Documents and Settings\sysadm>nslookup mail.yahoo.com itu.dk

Server: superman.itu.dk

Address: 130.226.133.2

Non-authoritative answer:

Name: login.yahoo.akadns.net

Address: 216.109.127.60

Aliases: mail.yahoo.com, login.yahoo.com

NOTE:Remark that in the second example we do not see the default server name.

There are many nslookup with optional commands.To read them type nslookup and enter

then type help and enter.

3-)finger:

Displays the information about a user on the system.

Example:

NOTE :I could not find out the name of the server that we log on (windows) at the school.

Sysadmin does not know that either:o)

But as an example I tried it on the our unix server.

[hilmiolgun@ssh hilmiolgun]$ finger

Login Name Tty Idle Login Time Office Office Phone

adel Adel Abu-Sharkh pts/1 7 Sep 10 00:11 (cpe.atm2-0-1091080.0x50a0bcb2.albnxx13.customer.tele.dk)

adel Adel Abu-Sharkh pts/2 9 Sep 9 23:56 (cpe.atm2-0-1091080.0x50a0bcb2.albnxx13.customer.tele.dk)

hilmiolgun Hilmi Olgun pts/9 Sep 10 00:20 (0x3ef3e2fe.albnxx8.adsl.tele.dk)

hm Hanne Munkholm pts/6 1:56 Sep 8 21:27 (off180.palombia.dk)

jcg Jens Christian Godsk pts/4 1d Sep 8 10:28 (toscana.itu.dk)

kaj Kenneth Ahn Jensen pts/7 Sep 10 00:11 (cpe.atm2-0-54493.0x50a4ad32.boanxx12.customer.tele.dk)

root root pts/8 1 Sep 10 00:12 (sysadm2.itu.dk)

troels Troels Arvin pts/5 3:49 Sep 9 20:31 (62.79.119.132.adsl.vbr.worldonline.dk)

webclaus Claus Bech Rasmussen pts/0 6 Sep 10 00:11 (port967.ds1-khk.adsl.cybercity.dk)

NOTE :What I did is :I first check the online users,and get a list of them(above).

Then i just choosed one user to get information about him(below)

[hilmiolgun@ssh hilmiolgun]$ finger hm

Login: hm Name: Hanne Munkholm

Directory: /import/home/hm Shell: /bin/bash

On since Mon Sep 8 21:27 (CEST) on pts/6 from off180.palombia.dk

1 hour 56 minutes idle

Last login Tue Sep 9 11:05 (CEST) on pts/12 from stud127.itu.dk

New mail received Mon Nov 11 23:01 2002 (CET)

Unread since Sat Oct 5 00:00 2002 (CEST)

Plan:

World Domination... fast.

[hilmiolgun@ssh hilmiolgun]$

4-)ping:

Simpy shows if the remote machine is available or not....

Example:

C:\Documents and Settings\sysadm>ping webmail.itu.dk

Pinging tarzan.itu.dk [130.226.133.3] with 32 bytes of data:

Reply from 130.226.133.3: bytes=32 time=29ms TTL=55

Reply from 130.226.133.3: bytes=32 time=30ms TTL=55

Reply from 130.226.133.3: bytes=32 time=30ms TTL=55

Reply from 130.226.133.3: bytes=32 time=30ms TTL=55

Ping statistics for 130.226.133.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 29ms, Maximum = 30ms, Average = 29ms

NOTE :Remark that the remote machine is replying.Otherwise the output will be "Request time out" which means the

remote machine is not working well.(Not answering)

5-)tracert:

It simply shows the path between source and destination address.

Example:

C:\Documents and Settings\sysadm>tracert webmail.itu.dk

Tracing route to tarzan.itu.dk [130.226.133.3]

over a maximum of 30 hops:

1	*	*	*	Request timed out.
2	29 ms	19 ms	29 ms	ge-0-2-1-2.1000M.albnxu1.ip.tele.dk [195.249.1.2 9]
3	29 ms	29 ms	19 ms	pos1-0.622M.lynxg1.ip.tele.dk [195.249.2.46]
4	29 ms	19 ms	29 ms	herman.fsknet.lyngby.forskningsnettet.dk [192.38 .7.1]
5	29 ms	29 ms	19 ms	130.225.244.214
6	29 ms	29 ms	29 ms	1.ku.forskningsnettet.dk [130.225.245.90]
7	29 ms	29 ms	29 ms	rk.itu.forskningsnettet.dk [130.226.249.30]
8	29 ms	29 ms	29 ms	130.225.245.86
9	29 ms	29 ms	29 ms	tarzan.itu.dk [130.226.133.3]

Trace complete.

6-)ftp:

For file transferring..(File transfer protocol)

Example: Lets you dont have an ftp software and you want to get a file from your school harddisk.

So to do that:

C:\Documents and Settings\sysadm>ftp

ftp> open

To ftp.itu.dk

Connected to ssh.itu.dk.

220 ProFTPD 1.2.8rc2 Server (ProFTPD Default Installation) [ssh.it-c.dk]

NOTE: What am I doing is simply:typing them one-by-one(after each typing remember to enter)

ftp,open,ftp.itu.dk

User (ssh.itu.dk:(none)): hilmiolgun

331 Password required for hilmiolgun.

Password:

230 User hilmiolgun logged in.

NOTE:The server will require username and password..

ftp> help

Commands may be abbreviated. Commands are:

! delete literal prompt send

? debug ls put status

append dir mdelete pwd trace

ascii disconnect mdir quit type

bell get mget quote user

binary glob mkdir recv verbose

bye hash mls remotehelp

cd help mput rename

close lcd open rmdir

ftp> help dir

dir List contents of remote directory

NOTE: If it is your first time to those commands just type help and get the commands.If you dont know how to use

them type help commandname..

ftp> dir

200 PORT command successful

150 Opening ASCII mode data connection for file list

drwx------ 4 hilmiolgun hilmiolgun 155 Jul 1 14:02 Desktop

drwx------ 2 hilmiolgun hilmiolgun 4096 May 30 10:21 Mail

drwxr-xr-x 5 hilmiolgun hilmiolgun 90 Sep 2 02:59 MobilePositionSDK

drwx------ 7 hilmiolgun hilmiolgun 4096 Aug 8 2002 NTnetscape

drwxr--r-- 13 hilmiolgun hilmiolgun 4096 Sep 4 01:56 New Folder

-rw-rw-r-- 1 hilmiolgun hilmiolgun 74 Sep 9 12:56 TTI409B

drwx------ 2 hilmiolgun hilmiolgun 6 Jan 21 2002 cgi-bin

-rw-rw-r-- 1 hilmiolgun hilmiolgun 74 Sep 9 12:56 geu

-rw-rw-r-- 1 hilmiolgun hilmiolgun 74 Sep 9 12:56 hilmiolgun

drwxr-xr-x 6 hilmiolgun hilmiolgun 4096 Aug 14 15:59 image

drwxr-xr-x 3 hilmiolgun hilmiolgun 4096 Jul 29 16:03 jmf20-apidocs

drwxr-xr-x 4 hilmiolgun hilmiolgun 4096 Sep 9 14:10 NOTEsieee

drwx------ 2 hilmiolgun hilmiolgun 6 Feb 21 2002 nsmail

drwx------ 3 hilmiolgun hilmiolgun 103 Feb 21 2002 office52

drwx------ 2 hilmiolgun hilmiolgun 6 Jan 21 2002 private

drwxr--rwx 2 hilmiolgun hilmiolgun 4096 Aug 23 12:02 public_html

drwxr-xr-x 5 hilmiolgun hilmiolgun 4096 Sep 6 03:30 speech

-rw-rw-r-- 1 hilmiolgun hilmiolgun 2630 Sep 9 13:58 test.txt

-rw-rw-r-- 1 hilmiolgun hilmiolgun 148 Sep 9 14:03 testing.txt

226 Transfer complete.

ftp: 1318 bytes received in 0,24Seconds 5,49Kbytes/sec.

ftp> get testing.txt

200 PORT command successful

150 Opening ASCII mode data connection for testing.txt (148 bytes)

226 Transfer complete.

ftp: 161 bytes received in 0,02Seconds 8,05Kbytes/sec.

NOTE :After taking a look to the school harddisk ,I copied a file "testing.txt" to my local harddisk....

```
ftp> !dir

 Volume in drive C has no label.

 Volume Serial Number is 0868-D52D

  Directory of C:\Documents and Settings\sysadm

 10-09-2003  00:21    <DIR>          .

10-09-2003  00:21    <DIR>          ..

31-08-2003  07:28    <DIR>          .java

25-04-2003  12:18    <DIR>          .javaws

23-04-2003  15:26    <DIR>          .jpi_cache

26-08-2003  04:59    <DIR>          .Nokia

07-09-2003  01:46            12.546 .plugin140_03.trace

07-09-2003  04:46               693 .plugin141_02.trace

07-09-2003  01:20               164 .saves-3824-IBMR31IMAGE

07-09-2003  01:20    <DIR>          Desktop

07-09-2003  08:05    <DIR>          Favorites

06-09-2003  05:29            80.140 love.wav

09-09-2003  23:45    <DIR>          mindterm

09-09-2003  11:02    <DIR>          My Documents

10-09-2003  00:21             2.903 plugin131_08.trace

25-04-2003  11:44    <DIR>          Start Menu

06-09-2003  21:21    <DIR>          studio5se_user
```

06-09-2003 05:32   18 test.txt

06-09-2003 05:20   70 testing

10-09-2003 00:37   161 testing.txt

26-08-2003 03:46   <DIR>   WINDOWS

               8 File(s)   96.695 bytes

              13 Dir(s)   3.842.056.192 bytes free

ftp> send love.wav

200 PORT command successful

150 Opening ASCII mode data connection for love.wav

226 Transfer complete.

ftp: 80140 bytes sent in 3,97Seconds 20,21Kbytes/sec.

ftp> dir

200 PORT command successful

150 Opening ASCII mode data connection for file list

drwx------   4 hilmiolgun hilmiolgun   155 Jul 1 14:02 Desktop

drwx------   2 hilmiolgun hilmiolgun   4096 May 30 10:21 Mail

drwxr-xr-x   5 hilmiolgun hilmiolgun   90 Sep 2 02:59 MobilePositionSDK

drwx------   7 hilmiolgun hilmiolgun   4096 Aug 8 2002 NTnetscape

drwxr--r-- 13 hilmiolgun hilmiolgun   4096 Sep 4 01:56 New Folder

-rw-rw-r--   1 hilmiolgun hilmiolgun   74 Sep 9 12:56 TTI409B

drwx------   2 hilmiolgun hilmiolgun   6 Jan 21 2002 cgi-bin

-rw-rw-r-- 1 hilmiolgun hilmiolgun 74 Sep 9 12:56 geu

-rw-rw-r-- 1 hilmiolgun hilmiolgun 74 Sep 9 12:56 hilmiolgun

drwxr-xr-x 6 hilmiolgun hilmiolgun 4096 Aug 14 15:59 image

drwxr-xr-x 3 hilmiolgun hilmiolgun 4096 Jul 29 16:03 jmf20-apidocs

-rw-rw-r-- 1 hilmiolgun hilmiolgun 80137 Sep 9 22:36 love.wav

drwxr-xr-x 4 hilmiolgun hilmiolgun 4096 Sep 9 14:10 NOTEsieee

drwx------ 2 hilmiolgun hilmiolgun 6 Feb 21 2002 nsmail

drwx------ 3 hilmiolgun hilmiolgun 103 Feb 21 2002 office52

drwx------ 2 hilmiolgun hilmiolgun 6 Jan 21 2002 private

drwxr--rwx 2 hilmiolgun hilmiolgun 4096 Aug 23 12:02 public_html

drwxr-xr-x 5 hilmiolgun hilmiolgun 4096 Sep 6 03:30 speech

-rw-rw-r-- 1 hilmiolgun hilmiolgun 2630 Sep 9 13:58 test.txt

-rw-rw-r-- 1 hilmiolgun hilmiolgun 148 Sep 9 14:03 testing.txt

226 Transfer complete.

ftp: 1387 bytes received in 0,07Seconds 19,81Kbytes/sec.

ftp>

NOTE:At the end first looking at the local working directory and sending a file "love.wav" to the school harddisk.

7-)net:

It has many options,which are for checking/starting/stopping nt services,users,messaging,configuration and so on...

Some of those options require administration privileges..

Example:

NOTE: To have an overview of commands options....

C:\Documents and Settings\sysadm>net

The syntax of this command is:

NET COMMANDS

NET [ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |

HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |

SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW]

NOTE: And furthermore to get an overview of a specific option ...

C:\Documents and Settings\sysadm>net help print

The syntax of this command is:

NET PRINT

\\computername\sharename

[\\computername] job# [/HOLD | /RELEASE | /DELETE]

NET PRINT displays print jobs and shared queues.

For each queue, the display lists jobs, showing the size

and status of each job, and the status of the queue.

\\computername Is the name of the computer sharing the printer

queue(s).

sharename Is the name of the shared printer queue.

job# Is the identification number assigned to a print job. A computer with one or more printer queues assigns each print job a unique number.

/HOLD Prevents a job in a queue from printing. The job stays in the printer queue, and other jobs bypass it until it is released.

/RELEASE Reactivates a job that is held.

/DELETE Removes a job from a queue.

NET HELP command | MORE displays Help one screen at a time.

Finally in addition to above there are also those commands: **hostname ,lpq, lpr ,rsh ,tftp ,nbstat ,netstat.**

To get familiar with those commands simply type **commandname /?** at the command line.

C:\>net

The syntax of this command is:

NET [ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW]

C:\>net use

New connections will not be remembered.

Status Local Remote Network

OK F: \\cse-sec\fac Microsoft Windows Network

C:\>net user

User accounts for \\CSE-DEPT-05

Administrator Guest

C:\>net statistics

Statistics are available for the following running services:

Server

Workstation

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

-a Displays all connections and listening ports.

-e Displays Ethernet statistics. This may be combined with the -s option.

-n Displays addresses and port numbers in numerical form.

-p proto Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display

per-protocol statistics, proto may be TCP, UDP, or IP.

-r Displays the routing table.

-s Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.

interval Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

C:\>net name

Name

CSE-DEPT-05

C:\>net session

Computer User name Client Type Opens Idle time

\\ENGLISH-03 Windows NT 1381 0 00:10:47

\\ENGLISHBDC Windows NT 1381 0 00:02:01

C:\>net accounts

Force user logoff how long after time expires?: Never

Minimum password age (days): 0

Maximum password age (days): 42

Minimum password length: 0

Length of password history maintained: None

Lockout threshold: Never

Lockout duration (minutes): 30

Lockout observation window (minutes): 30

Computer role: WORKSTATION

C:\>net localgroup

Aliases for \\CSE-DEPT-05

---

*Administrators *Backup Operators *Guests

*Power Users *Replicator *Users

C:\>net config server

Server Name \\CSE-DEPT-05

Server Comment

Software version Windows NT 4.0

Server is active on NetBT_DLKRTS1 (0050ba8b326b) NetBT_DLKRTS1

(0050ba8b326b) NwlnkIpx (0050ba8b326b) NwlnkNb (0050ba8b326b) Nbf_DLKRTS1 (0050

ba8b326b)

Server hidden No

Maximum Logged On Users 10

Maximum open files per session 2048

Idle session time (min) 15

C:\>net config workstation

Computer name \\CSE-DEPT-05

User name Administrator

Workstation active on NwlnkNb (0050BA8B326B) NetBT_DLKRTS1 (0050B

A8B326B) Nbf_DLKRTS1 (0050BA8B326B)

Software version Windows NT 4.0

Workstation domain WORKGROUP

Logon domain CSE-DEPT-05

COM Open Timeout (sec) 3600

COM Send Count (byte) 16

COM Send Timeout (msec) 250

C:\>net share

Share name Resource Remark

D$ D:\ Default share

IPC$ Remote IPC

C$ C:\ Default share

ADMIN$ C:\WINNT Remote Admin

E$ E:\ Default share

abishek E:\abishek

akshu E:\akshu

HARSHINI D:\ HARSHINI

DHARSHINI E:\ DHARSHINI

C:\>net stop messenger

The Messenger service is stopping.

The Messenger service was stopped successfully.

C:\>net start messenger

The Messenger service is starting...

The Messenger service was started successfully.

Network Configuration commands

ifconfig

This command is used to configure network interfaces, or to display their current configuration. In addition to activating and deactivating interfaces with the “up” and “down” settings, this command is necessary for setting an interface's address information if you don't have the *ifcfg* script.

Use *ifconfig* as either:

ifconfig

This will simply list all information on all network devices currently up.

ifconfig eth0 down

This will take eth0 (assuming the device exists) down, it won't be able to receive or send anything until you put the device back “up” again.

Clearly there are a lot more options for this tool, you will need to read the manual/info page to learn more about them.

ifup

Use *ifup device-name* to bring an interface up by following a script (which will contain your default networking settings). Simply type *ifup* and you will get help on using the script.

For example typing:

ifup eth0

Will bring eth0 up if it is currently down.

ifdown

Use *ifdown device-name* to bring an interface down using a script (which will contain your default network settings). Simply type *ifdown* and you will get help on using the script.

For example typing:

ifdown eth0

Will bring eth0 down if it is currently up.

ifcfg

Use *ifcfg* to configure a particular interface. Simply type ifcfg to get help on using this script.

For example, to change eth0 from 192.168.0.1 to 192.168.0.2 you could do:

ifcfg eth0 del 192.168.0.1

ifcfg eth0 add 192.168.0.2

The first command takes eth0 down and removes that stored IP address and the second one brings it back up with the new address.

route

The *route* command is the tool used to display or modify the routing table. To add a gateway as the default you would type:

route add default gw some_computer

INTERNET SPECIFIC COMMANDS

host

Performs a simple lookup of an internet address (using the Domain Name System, DNS). Simply type:

host ip_address

or

host domain_name

dig

The "domain information groper" tool. More advanced then *host*... If you give a hostname as an argument to output information about that host, including it's IP address, hostname and various other information.

For example, to look up information about “www.amazon.com” type:

dig www.amazon.com

To find the host name for a given IP address (ie a reverse lookup), use *dig* with the `*-x*' option.

dig -x 100.42.30.95

This will look up the address (which may or may not exist) and returns the address of the host, for example if that was the address of “http://slashdot.org” then it would return “http://slashdot.org”.

dig takes a huge number of options (at the point of being too many), refer to the manual page for more information.

whois

(now BW whois) is used to look up the contact information from the “whois” databases, the servers are only likely to hold major sites. Note that contact information is likely to be hidden or restricted as it is often abused by crackers and others looking for a way to cause malicious damage to organisation's.

wget

(GNU Web get) used to download files from the World Wide Web.

To archive a single web-site, use the *-m* or *--mirror* (mirror) option.

Use the *-nc* (no clobber) option to stop *wget* from overwriting a file if you already have it.

Use the *-c* or *--continue* option to continue a file that was unfinished by wget or another program.

Simple usage example:

wget url_for_file

This would simply get a file from a site.

wget can also retrieve multiple files using standard wildcards, the same as the type used in bash, like *, [ ], ?. Simply use *wget* as per normal but use single quotation marks (' ') on the URL to prevent bash from expanding the wildcards. There are complications if you are retrieving from a http site (see below...).

Advanced usage example, (used from *wget* manual page):

wget --spider --force-html -i bookmarks.html

This will parse the file bookmarks.html and check that all the links exist.

Advanced usage: this is how you can download multiple files using http (using a wildcard...).

Notes: http doesn't support downloading using standard wildcards, ftp does so you may use wildcards with ftp and it will work fine. A work-around for this http limitation is shown below:

wget -r -l1 --no-parent -A.gif http://www.website.com[1]

This will download (recursively), to a depth of one, in other words in the current directory and not below that. This command will ignore references to the parent directory, and downloads anything that ends in ".gif". If you wanted to download say, anything that ends with ".pdf" as well than add a *-A.pdf* before the website address. Simply change the website address and the type of file being downloaded to download something else. Note that doing *-A.gif* is the same as doing *-A "*.gif*" (double quotes only, single quotes will not work).

wget has many more options refer to the examples section of the manual page, this tool is very well documented.

Alternative website downloaders: You may like to try alternatives like httrack. A full GUI website downloader written in python and available for GNU/Linux

curl

curl is another remote downloader. This remote downloader is designed to work without user interaction and supports a variety of protocols, can upload/download and has a large number of tricks/work-arounds for various things. It can access dictionary servers (dict), ldap servers, ftp, http, gopher, see the manual page for full details.

To access the full manual (which is huge) for this command type:

curl -M

For general usage you can use it like *wget*. You can also login using a user name by using the *-u* option and typing your username and password like this:

curl -u username:password http://www.placetodownload/file

To upload using ftp you the *-T* option:

curl -T file_name ftp://ftp.uploadsite.com

To continue a file use the *-C* option:

curl -C - -o file http://www.site.com

View and modify network interfaces

ifconfig -a Show information about all network interfaces

ifconfig eth0 Show information only about the interface eth0

ifconfig eth0 up Bring up the interface eth0

ifconfig eth0 down Take down the interface eth0

Simple network diagnostic commands

ping hostname Send ICMP echo requests to the host hostname

traceroute hostname Trace the network path to hostname

View open network connections

netstat -a Show information about all open network connections

netstat -a | grep LISTEN Show information about all open network ports

Set/view routing information

netstat -r View system routing tables

route View system routing tables

The command route can also be used to add or delete routes. Examples:

route add -host 192.168.3.4 gw 192.168.3.1 netmask 255.255.0.0

route del -host 192.168.3.4

NETSTAT.exe **TCP/IP Network Statistics**

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

-a **Displays all connections and listening ports.**

-e **Displays Ethernet statistics. This may be combined with the -s option.**

-n **Displays addresses and port numbers in numerical form.**

-p proto **Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.**

-r **Displays the routing table.**

-s **Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.**

interval **Redisplays selected statistics, pausing interval seconds between each display. Press**

CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

C:\WINDOWS>netstat -a

Active Connections

Proto	Local Address	Foreign Address	State
TCP	My_Comp:ftp	localhost:0	LISTENING
TCP	My_Comp:80	localhost:0	LISTENING

Or with the "-an" parameters:

C:\WINDOWS>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING

By simply opening a browser connection to both the HTTP (port 80) and FTP (port 21) servers (while still offline!), I saw the following:

C:\WINDOWS>netstat -a

Active Connections

Proto	Local Address	Foreign Address	State
TCP	My_Comp:ftp	localhost:0	LISTENING
TCP	My_Comp:80	localhost:0	LISTENING
TCP	My_Comp:1104	localhost:0	LISTENING
TCP	My_Comp:ftp	localhost:1104	ESTABLISHED
TCP	My_Comp:1102	localhost:0	LISTENING
TCP	My_Comp:1103	localhost:0	LISTENING
TCP	My_Comp:80	localhost:1111	TIME_WAIT
TCP	My_Comp:1104	localhost:ftp	ESTABLISHED
TCP	My_Comp:1107	localhost:0	LISTENING
TCP	My_Comp:1112	localhost:80	TIME_WAIT
UDP	My_Comp:1102	*:*	

```
  UDP    My_Comp:1103           *:*
  UDP    My_Comp:1107           *:*
```

This may be a bit confusing to some people, but remember I'm running BOTH the servers and clients on the same machine in these examples. A little later (using both 'a' and 'n') I got this:

C:\WINDOWS>netstat -an

Active Connections

```
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1104           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:21           127.0.0.1:1104         FIN_WAIT_2
  TCP    127.0.0.1:1102         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1103         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1104         127.0.0.1:21           CLOSE_WAIT
  TCP    127.0.0.1:1107         0.0.0.0:0              LISTENING
  UDP    127.0.0.1:1102         *:*
  UDP    127.0.0.1:1103         *:*
  UDP    127.0.0.1:1107         *:*
```

After turning off my server, I ended up with this for a while:

C:\WINDOWS>netstat -an

Active Connections

```
  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:80           127.0.0.1:1150         TIME_WAIT
  TCP    127.0.0.1:80           127.0.0.1:1151         TIME_WAIT
```

PING.exe

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]

[-w timeout] destination-list

Options:

-t **Ping the specifed host until interrupted.**
-a **Resolve addresses to hostnames.**
-n count **Number of echo requests to send.**
-l size **Send buffer size.**
-f **Set "Don't Fragment" flag in packet.**
-i TTL **Time To Live.**
-v TOS **Type Of Service.**
-r count **Record route for count hops.**
-s count **Timestamp for count hops.**
-j host-list **Loose source route along host-list.**
-k host-list **Strict source route along host-list.**
-w timeout **Timeout in milliseconds to wait for each reply.**

There's one special IP number everyone should know about:

127.0.0.1 - localhost (or loopback).
This is used to connect (through a browser, for example) to a Web server on your own computer. (127 being reserved for this purpose.) You can use this IP number **at all times**. It doesn't matter if you're connected to the Internet or not.

It's also called the **loopback** address because you can **ping** it and get ***returns*** even when you're ***offline*** (not connected to *any* network). If you don't get any valid replies, then there's a problem with the computer's Network settings. Here's a typical response to the 'ping' command:

Here's another recent example using the name of my computer which I have tied to the IP number 127.0.0.1 in my C:\WINDOWS\HOSTS file:

C:\WINDOWS>**ping My_Comp**

Pinging My_Comp [127.0.0.1] with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time=1ms TTL=128

Reply from 127.0.0.1: bytes=32 time=1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<10ms TTL=128

Reply from 127.0.0.1: bytes=32 time=1ms TTL=128

Ping statistics for 127.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

TRACERT.exe **Trace Route**

Usage:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:

-d **Do not resolve addresses to hostnames.**

-h maximum_hops **Maximum number of hops to search for target.**

-j host-list **Loose source route along host-list.**

-w timeout **Wait timeout milliseconds for each reply.**

Here's an example which traces the route from some ISP in Los Angeles to the main server at UCLA in California (note how two computers relatively close to each other may be routed way round about!):

C:\WINDOWS>**tracert www.ucla.edu**

Tracing route to www.ucla.edu [169.232.33.129]

over a maximum of 30 hops:

1	141 ms	132 ms	140 ms	wla-ca-pm6.icg.net [165.236.29.85]
2	134 ms	131 ms	139 ms	whv-ca-gw1.icg.net [165.236.29.65]
3	157 ms	132 ms	143 ms	f3-1-0.lai-ca-gw1.icg.net [165.236.24.89]
4	194 ms	193 ms	188 ms	a0-0-0-1.dai-tx-gw1.icg.net [163.179.235.61]

5 300 ms 211 ms 214 ms a1-1-0-1.ati-ga-gw1.icg.net [163.179.235.186]

6 236 ms 237 ms 247 ms a5-0-0-1.was-dc-gw1.icg.net [163.179.235.129]

7 258 ms 236 ms 244 ms 163.179.243.205

8 231 ms 233 ms 230 ms wdc-brdr-03.inet.qwest.net [205.171.4.153]

9 240 ms 230 ms 236 ms wdc-core-03.inet.qwest.net [205.171.24.69]

10 262 ms 264 ms 263 ms hou-core-01.inet.qwest.net [205.171.5.187]

11 281 ms 263 ms 259 ms hou-core-03.inet.qwest.net [205.171.23.9]

12 272 ms 229 ms 222 ms lax-core-02.inet.qwest.net [205.171.5.163]

13 230 ms 217 ms 230 ms lax-edge-07.inet.qwest.net [205.171.19.58]

14 228 ms 219 ms 220 ms 63-145-160-42.cust.qwest.net [63.145.160.42]

15 218 ms 222 ms 218 ms ISI-7507--ISI.POS.calren2.net [198.32.248.21]

16 232 ms 222 ms 214 ms UCLA--ISI.POS.calren2.net [198.32.248.30]

17 234 ms 226 ms 226 ms cbn5-gsr.calren2.ucla.edu [169.232.1.18]

18 245 ms 227 ms 235 ms www.ucla.edu [169.232.33.129]

Trace complete.

Net Bios Stats

NBTSTAT.exe

Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP).

NBTSTAT [-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-s] [S] [interval]

-a (adapter status) Lists the remote machine's name table given its name.

-A (Adapter status) Lists the remote machine's name table given its IP address.

-c (cache) Lists the remote name cache including the IP addresses.

-n (names) Lists local NetBIOS names.

-r (resolved) Lists names resolved by broadcast and via WINS

-R (Reload) Purges and reloads the remote cache name table

-S (Sessions) Lists sessions table with the destination IP addresses.

-s (sessions) Lists sessions table converting destination IP addresses to host names via the hosts file.

RemoteName Remote host machine name.
IP address Dotted decimal representation of the IP address.

interval Redisplays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop redisplaying statistics.

ROUTE.exe

Manipulates network routing tables.

ROUTE [-f] [command [destination] [MASK netmask] [gateway]]

-f Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command.

command Specifies one of four commands

PRINT Prints a route
ADD Adds a route
DELETE Deletes a route
CHANGE Modifies an existing route

destination Specifies the host to send command.

MASK If the MASK keyword is present, the next parameter is interpreted as the netmask parameter.

netmask If provided, specifies a sub-net mask value to be associated with this route entry. If not specified, if defaults to 255.255.255.255.

gateway Specifies gateway.

All symbolic names used for destination or gateway are looked up in the network and host name database files NETWORKS and HOSTS, respectively.

If the command is print or delete, wildcards may be used for the destination and gateway, or the gateway argument may be omitted.

ARP.exe Address Resolution Protocol

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.

-g (Same as -a)

inet_addr Specifies an internet address.

-N if_addr Displays the ARP entries for the network interface specified by if_addr.

-d Deletes the host specified by inet_addr.

-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

eth_addr Specifies a physical address.

if_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.