(1) Microsoft DOS `hostname` command

About hostname

Display the hostname of the machine the command is being run on.

Availability

The hostname command is an external command and is available in the below Microsoft operating systems.

Windows 2000, Windows XP, Windows Vista, Windows 7

Syntax

hostname

sethostname: Use the Network Control Panel Applet to set hostname. hostname -s is not supported.

Examples

hostname

Running the command would display the hostname for the computer.

(2) Microsoft DOS `arp` command

About arp

Displays, adds and removes `arp` information from network devices.

The arp.exe command is an external command accessed through the C:\Windows or C:\Winnt\System32 directory and is available in the below Microsoft operating systems.

Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7

Syntax

```
ARP -s inet_addr eth_adr [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 seperated 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.

Examples

`arp -a`

Interface 220.0.0.80

Internet Address	Physical Address	Type
220.0.0.160	00-50-04-62-F7-23	static

The Physical Address or MAC address as shown above in the format aa-bb-cc-dd-ee-ff is the unique manufacturer identification number. This number should always be a unique address.

An example of how to change the above IP address 220.0.0.160 to 220.0.0.161 in this case would be:

`arp -s 220.0.0.161 00-50-04-62-F7-23`

If an IP address has already been assigned to the specific network adapter it is not possible to change that assigned IP address to a new address. In addition, networks italicizing DHCP, BOOTP or RARP will automatically assign the card an IP address; therefore, this command would not be utilized.

(3) Microsoft DOS `ipconfig` command

About ipconfig

Ipconfig is a DOS utility that can be used from MS-DOS and a MS-DOS shell to display the network settings currently assigned and given by a network. This command can be utilized to verify a network connection as well as to verify your network settings.

Availability

The ipconfig.exe command is an external command and is available in the below Microsoft operating systems.

Windows 95, Windows 98, Windows ME, Windows 2000, Windows XP, Windows Vista, Windows 7.

Windows 95, 98, and ME syntax

/All	Display detailed information.
/Batch [file]	Write to file or ./WINIPCFG.OUT
/renew_all	Renew all adapters.
/release_all	Release all adapters.
/renew N	Renew adapter N.
/release N	Release adapter N.

Windows 2000 and XP syntax

```
ipconfig [/? | /all | /release [adapter] | /renew
[adapter] | /flushdns | /registerdns | /showclassid
adapter | /setclassid adapter [classidtoset] ]
```

/all	Display full configuration information.
/release	Release the IP address for the specified adapter.
/renew	Renew the IP address for the specified adapter.
/flushdns	Purges the DNS Resolver cache.
/registerdns	Refreshes all DHCP leases and re-registers DNS names
/displaydns	Display the contents of the DNS Resolver Cache.
/showclassid	Displays all the dhcp class IDs allowed for adapter.
/setclassid	Modifies the dhcp class id.

The default is to display only the IP address, subnet mask and default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address leases for all adapters bound to TCP/IP will be released or renewed.

For SetClassID, if no class id is specified, then the classid is removed.

Examples

To get your computers local network IP address, subnet mask, and default gateway typing ipconfig alone will display this information as shown below. Keep in mind this is only your local network information.

ipconfig

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : hsd1.ut.comcast.net.
IP Address. . . . . : 192.168.201.245
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.201.1

To get all local network information for your computer use the /all switch as shown below, followed by the results that would be seen when using this command.

ipconfig /all

Windows IP Configuration

Host Name . . . . . : COMPUTERH1
DNS Servers . . . . . : 123.45.67.8
111.111.111.1
111.111.111.1
Node Type . . . . . : Broadcast
NetBIOS Scope ID. . . . . :
IP Routing Enabled. . . . : No
WINS Proxy Enabled. . . . : No
NetBIOS Resolution Uses DNS : No

0 Ethernet adapter :

Description . . . . . .: PPP Adapter.
Physical Address. . . . . .: 44-44-44-54-00-00
DHCP Enabled. . . . . : Yes
IP Address. . . . . . : 123.45.67.802
Subnet Mask . . . . . .: 255.255.0.0
Default Gateway . . . . . .: 123.45.67.801
DHCP Server . . . . . .: 255.255.255.255
Primary WINS Server . . . .:
Secondary WINS Server . . :
Lease Obtained. . . . . .: 01 01 80 12:00:00 AM
Lease Expires . . . . . : 01 01 80 12:00:00 AM

1 Ethernet adapter :

Description . . . . . : 3Com 3C90x Ethernet Adapter
Physical Address. . . . . : 00-50-04-62-F7-23


```
DHCP Enabled. . . . . . . . : Yes
IP Address. . . . . . . . . : 111.111.111.108
Subnet Mask . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . : 111.111.111.1
DHCP Server . . . . . . . . : 111.111.111.1
Primary WINS Server . . . . :
Secondary WINS Server . . . :
Lease Obtained. . . . . . . : 11 16 00 12:12:44 AM
Lease Expires . . . . . . . :
```

ipconfig /displaydns

Running the above command would display all the DNS information.

ipconfig /flushdns

Delete all DNS entries.

(4) Microsoft DOS ping command

About ping

Helps in determining TCP/IP Networks IP address as well as determine issues with the network and assists in resolving them.

Availability

The ping.exe command is an external command that is available in the below Microsoft operating systems.

Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7.

Syntax

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	Pings the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.
-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.

Examples

`ping localhost`

Pings the local host, this will allow you to see if the computer is able to send information out and receive the information back. Note that this does not send information over a network but may allow you to see if the card is being seen.

`ping xxx.xxx.xxx.xxx`

Allows you to ping another computer where the *x*'s are located are where you would place the IP address of the computer you are attempting to ping. If this is not able to complete, this should relay back an unsuccessful message, which could be an indication of cable issues, network card issues, hub issue, etc.

`ping computerhope.com`

```
PING computerhope.com (204.228.150.3) 56(84) bytes of data.
64 bytes from www.computerhope.com (204.228.150.3): icmp_seq=1 ttl=63
time=0.267 ms

--- computerhope.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.267/0.267/0.267/0.000 ms
```

Additional information

- Information about why pinging a website such as microsoft.com may not return a response can be found on document CH001054.
- See document CH001055 for additional information about determining the IP address of a web page.
- Ping a website or check if it's online through our free is it up utility.

(5) Microsoft DOS `netstat` command

About netstat

The `netstat` command is used to display the TCP/IP network protocol statistics and information.

Availability

The netstat.exe command is an external command available in the below Microsoft operating systems.

Windows 95, Windows 98, Windows NT, Windows ME, Windows 2000, Windows XP, Windows Vista, Windows 7.

Syntax

```
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	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.

Examples

`netstat`

Displays all local network information. Below is an example of what may be displayed.

```
  Proto Local Address  Foreign Address               State
  TCP   hope:4409      www.computerhope.com:telnet   ESTABLISHED
  TCP   hope:3708      multicity.com:80              CLOSE_WAIT
  TCP   hope:4750      www.google.com:80             CLOSE_WAIT
```

`netstat 5`

Running `netstat` with a number after the command will continue to run the command until stopped. In this case `netstat` would be refreshed ever five seconds. To cancel press CTRL + C.

Notice: Keep in mind that if you have network applications open, such as the browser you're using to view this page, additional items will be listed when you run "`netstat`" and/or the "`netstat -a`" command. So you may see items from Computer Hope in your list; if you want a true listing of what is running in the background, close all programs and run the command.

(6) Microsoft DOS `tracert` command

About tracert

The `tracert` command is used to visually see a network packet being sent and received and the amount of hops required for that packet to get to its destination.

Users with Microsoft Windows 2000 and Windows XP who need additional information network latency and network loss should also consider using the `pathping command`.

Availability

The `tracert.exe` command is an external command that is available in the below Microsoft operating systems.

MS-DOS 6.2, Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7.

Syntax

`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.

Examples

Below is an example when we used `tracert` on www.computerhope.com. As you can see in the below example, we had a very short list and time to get to its destination because of the location we are.

`tracert computerhope.com`


```
1   169 ms   190 ms   160 ms      slc1-tc.xmission.com [166.70.1.20]
2   159 ms   160 ms   190 ms      cisco0-tc.xmission.com [166.70.1.1]
3   165 ms   189 ms   159 ms      www.computerhope.com [166.70.10.23]
```

(7) Microsoft DOS `pathping` command

About pathping

Similar to the `tracert command`, `pathping` provides users with the ability of locating spots that have network latency and network loss.

Availability

The pathping.exe command is an external command that is available in the below Microsoft operating systems.

Windows 2000, Windows XP, Windows Vista, Windows 7.

Syntax

Windows 2000 Syntax

```
Usage:pathping [-n] [-h maximum_hops] [-g host-list] [-p period]
               [-q num_queries] [-w timeout] [-t] [-R] [-r] target_name
```

Options:

-n	Do not resolve addresses to hostnames.
-h maximum_hops	Maximum number of hops to search for target.
-g host-list	Loose source route along host-list.
-p period	Wait period milliseconds between pings.
-q num_queries	Number of queries per hop.
-w timeout	Wait timeout milliseconds for each reply.
-T	Test connectivity to each hop with Layer-2 priority tags.
-R	Test if each hop is RSVP aware.

Windows XP Syntax

```
Usage:pathping [-g host-list][-h maximum_hops][-i address][-n]
               [-p period][-q num_queries][-w timeout][-P][-R]
               [-T]
```



```
[-4] [-6] target_name
```

Options:

-g host-list	Loose source route along host-list.
-h maximum_hops	Maximum number of hops to search for target.
-i address	Use the specified source address.
-n	Do not resolve addresses to hostnames.
-p period	Wait period milliseconds between pings.
-q num_queries	Number of queries per hop.
-w timeout	Wait timeout milliseconds for each reply.
-P	Test for RSVP PATH connectivity.
-R	Test if each hop is RSVP aware.
-T	Test connectivity to each hop with Layer-2 priority tags.
-4	Force using IPv4.
-6	Force using IPv6.

Examples

`pathping computerhope.com`

```
Tracing route to computerhope.com [204.228.150.3]
over a maximum of 30 hops:
0 Hope [192.168.120.101]
1 192.168.120.254
2 ...
Computing statistics for 50 seconds...

                    Source to Here   This Node/Link
Hop  RTT            Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                                  0 Hope [192.168.120.101]
                                     0/100 = 0%         |
  1    0ms          0/ 100 = 0%      0/100 = 0%       192.168.120.254
                                     100/100 = 100%     |
  2    ---          100/100 = 100%   0/100 = 0%       Hope [0.0.0.0]

Trace complete.
```

(8) Microsoft DOS `nbtstat` command

About nbtstat

MS-DOS utility that displays protocol statistics and current TCP/IP connections using NBT.

Availability

The nbtstat command is an external command that is available in the below Microsoft operating systems.

Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7.

Syntax

NBTSTAT [[-a RemoteName][-A IP address][-c][-n][-r][-R][-RR][-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 NBT's cache of remote [machine] names and their 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 computer NETBIOS names.
-RR	(ReleaseRefresh) Sends Name Release packets to WINs and then, starts Refresh
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.

Examples

nbtstat -a 204.224.150.3

```
Local Area Connection:
Node IpAddress: [204.224.150.3] Scope Id: []

NetBIOS Remote Machine Name Table

Name Type Status
---------------------------------------------
HOPE4           <00> UNIQUE Registered
CHGROUP         <00> GROUP Registered
HOPE4           <20> UNIQUE Registered
```



```
HOPE4           <03> UNIQUE Registered
CHGROUP         <1E> GROUP Registered
CHGROUP         <1D> UNIQUE Registered
..__MSBROWSE__.<01> GROUP Registered
ADMINISTRATOR   <03> UNIQUE Registered

MAC Address = 00-00-00-00-00-00
```

(9) Microsoft DOS nslookup command

About nslookup

MS-DOS utility that enables a user to look up an IP address of a domain or host on a network.

Users who are using earlier versions of Microsoft Windows 95, Windows 98, or Windows ME and need the options available with the nslookup command will need to download an alternative, third-party program.

Availability

The nslookup.exe command is an external command that is available in the below Microsoft operating systems.

Windows NT, Windows 2000, Windows XP, Windows 7.

Syntax

Commands: (identifiers are shown in uppercase, [] means optional)

NAME	print info about the host/domain NAME using default server
NAME1 NAME2	as above, but use NAME2 as server
help or ?	print info on common commands
set OPTION	set an option **all** print options, current server and host **[no]debug** print debugging information **[no]d2** print exhaustive debugging information **[no]defname** append domain name to each query **[no]recurse** ask for recursive answer to query **[no]search** use domain search list **[no]vc** always use a virtual circuit **domain=NAME** set default domain name to NAME **srchlist=N1[/N2/.../N6]** set domain to N1 and search list to N1,N2, etc. **root=NAME** set root server to NAME **retry=X** set number of retries to X **timeout=X** set initial time-out interval to X seconds **type=X** set query type (ex.

	querytype=X	A,ANY,CNAME,MX,NS,PTR,SOA,SRV) same as type
	class=X	set query class (ex. IN (Internet), ANY)
	[no]msxfr	use MS fast zone transfer
	ixfrver=X	current version to use in IXFR transfer request
server NAME	set default server to NAME, using current default server	
lserver NAME	set default server to NAME, using initial server	
finger [USER]	finger the optional NAME at the current default host	
root	set current default server to the root	
ls [opt] DOMAIN [> FILE]	list addresses in DOMAIN (optional: output to FILE) **-a** list canonical names and aliases **-d** list all records **-t TYPE** list records of the given type (e.g. A,CNAME,MX,NS,PTR etc.)	
view FILE	sort an 'ls' output file and view it with pg	
exit	exit the program	

Examples

This command is often used to perform a reverse lookup on an IP address as shown in the below example. The first section specifies the server and address of that server that provided you with the domain name and IP address displayed in the second section.

`nslookup 204.228.150.3`

```
Server: ns.computerhope.com
Address: 1.1.1.1

Name: www.computerhope.com
Address: 204.228.150.3
```

`nslookup`

Running nslookup without specifying an IP address or domain name will s

(10) Microsoft DOS `route` command

About route

The function and syntax of the Windows ROUTE command is similar to the UNIX or `Linux route` command. Use the command to manually configure the routes in the routing table.

Availability

The `route.exe` command is an external command that is available in the below Microsoft operating systems.

Windows 95, Windows 98, Windows ME, Windows 2000, Windows XP, Windows Vista and Windows 7

Syntax

`ROUTE [-f] [-p] [command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]`

-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.
-p	When used with the ADD command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. When used with the PRINT command, displays the list of registered persistent routes. Ignored for all other commands, which always affect the appropriate persistent routes. This option is not supported Windows'95. command
command	One of these: PRINT Prints a route ADD Adds a route DELETE Deletes a route CHANGE Modifies an existing route destination
destination	Specifies the host.
MASK	Specifies that the next parameter is the 'netmask' value.
netmask	Specifies a subnet mask value for this route entry. If not specified, it defaults to 255.255.255.255.
gateway	Specifies gateway.
interface	the interface number for the specified route.
METRIC	Specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database file NETWORKS. The symbolic names for gateway are looked up in the host name database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard, (wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only matching destination routes are printed. The '*' matches any string, and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Diagnostic Notes:
Invalid MASK generates an error, that is when (DEST & MASK) != DEST.

Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
The route addition failed: The specified mask parameter is invalid.
(Destination & Mask) != Destination.

Examples

Examples:

```
> route PRINT

>route  ADD 157.0.0.0   MASK                    METRIC 3        IF 2
                        255.0.0.0     157.55.80.1
^destination                            ^gateway    ^metric         ^Interface
                        ^mask
```

If IF is not given, it tries to find the best interface for a given gateway.

```
> route PRINT
> route PRINT 157* .... Only prints those matching 157*
> route DELETE 157.0.0.0
> route PRINT
```

One way to use this would be as follows: You can't ping the server that you are connecting to, but you know the ip address to be 127.16.16.10

```
>route PRINT
```

Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 14 a4 c3 44 20 ..... Xircom CardBus Ethernet 10/100 Adapter
0x3 ...00 b0 d0 43 55 a5 ..... 3Com EtherLink PCI
0x4 ...00 01 b0 8f 8f 80 ..... NdisWan Adapter

Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 127.16.8.14 127.16.8.14 1
127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
127.16.0.0 255.255.0.0 127.16.8.14 127.16.8.14 1
127.16.8.14 255.255.255.255 127.0.0.1 127.0.0.1 1
192.168.50.0 255.255.255.0 192.168.50.65 192.168.50.65 2
192.168.50.65 255.255.255.255 127.0.0.1 127.0.0.1 1
192.168.50.255 255.255.255.255 192.168.50.65 192.168.50.65 1
224.0.0.0 224.0.0.0 127.16.8.14 127.16.8.14 1
224.0.0.0 224.0.0.0 192.168.50.65 192.168.50.65 1
255.255.255.255 255.255.255.255 192.168.50.65 192.168.50.65 1

** notice that no gateway for the current ip goes to 255.255.255.0, so it must be added. Now do the below command.

```
>route ADD 127.16.0.0 MASK 255.255.255.0 <your current ip from
winntcfg or winipcfg> METRIC 1
```


**Then do the below command:

```
>route print
```

Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 127.16.8.14 127.16.8.14 1
127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
127.16.0.0 255.255.0.0 127.16.8.14 127.16.8.14 1
** 127.16.0.0 255.255.255.0 127.16.8.14 127.16.8.14 1
127.16.8.14 255.255.255.255 127.0.0.1 127.0.0.1 1
192.168.50.0 255.255.255.0 192.168.50.65 192.168.50.65 2
192.168.50.65 255.255.255.255 127.0.0.1 127.0.0.1 1
192.168.50.255 255.255.255.255 192.168.50.65 192.168.50.65 1
224.0.0.0 224.0.0.0 127.16.8.14 127.16.8.14 1
224.0.0.0 224.0.0.0 192.168.50.65 192.168.50.65 1
255.255.255.255 255.255.255.255 192.168.50.65 192.168.50.65 1

**Notice the ** ip address gives me the default gateway.

Find All Active/Used IP Addresses on Your Network?

There is a really neat way that you can quite easily find all active/used IP Addresses on your network without the need for any third party applications or worse, pinging each IP Address individually.

Open the Command Prompt and type in the following:

```
FOR /L %i IN (1, 1,254) DO ping -n 1 192.168.10. %i | FIND /I
Reply">>c:\ipaddresses.txt
```

Change 192.168.10 to match you own network.

