Windows TCP/IP utilities and services

TCP/IP utilities offer network connections to other computers, such as UNIX workstations. You must have the TCP/IP network protocol installed to use the TCP/IP utilities.

MAC:

In computer networking a **Media Access Control address** (**MAC address**) is a unique identifier attached to most network adapters (NICs). It is a number that acts like a name for a particular network adapter, so, for example, the network cards (or built-in network adapters) in two different computers will have different names, or MAC addresses, as would an Ethernet adapter and a wireless adapter in the same computer, and as would multiple network cards in a router. However, it is possible to change the MAC address on most of today's hardware.

ARP is commonly used to convert from addresses in a layer 3 protocol such as Internet Protocol (IP) to the layer 2 MAC address. On broadcast networks, such as Ethernet, the MAC address allows each host to be uniquely identified and allows frames to be marked for specific hosts. It thus forms the basis of most of the layer 2 networking upon which higher OSI Layer protocols are built to produce complex, functioning networks.

The original IEEE 802 **MAC address**, now officially called "MAC-48", comes from the Ethernet specification. Since the original designers of Ethernet had the foresight to use a 48-bit address space, there are potentially 2^{48} or 281,474,976,710,656 possible MAC addresses.

The standard (IEEE 802) format for printing MAC-48 addresses in human-readable media is six groups of two hexadecimal digits, separated by hyphens (`-`) in transmission order, e.g. `01-23-45-67-89-ab`. Other conventions include six groups of two separated by colons (`:`), e.g. `01:23:45:67:89:ab`; or three groups of four hexadecimal digits separated by dots (`.`), e.g. `0123.4567.89ab`; again in transmission order.

Arp Command

Displays and modifies entries in the Address Resolution Protocol (ARP) cache, which contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses. There is a separate table for each Ethernet or Token Ring network adapter installed on your computer. Used without parameters, **arp** displays help.

Syntax

arp [**-a** [*InetAddr*] [**-N** *IfaceAddr*]] [**-g** [*InetAddr*] [**-N** *IfaceAddr*]] [**-d** *InetAddr* [*IfaceAddr*]] [**-s** *InetAddr EtherAddr* [*IfaceAddr*]]

Parameters

-a [*InetAddr*] [-N *IfaceAddr*] : Displays current ARP cache tables for all interfaces. To display the ARP cache entry for a specific IP address, use **arp -a** with the *InetAddr* parameter, where *InetAddr* is an IP address. To display the ARP cache table for a specific interface, use the **-N** *IfaceAddr* parameter where *IfaceAddr* is the IP address assigned to the interface. The **-N** parameter is case-sensitive.

-g [*InetAddr*] [-N *IfaceAddr*] : Identical to **-a**.

-d *InetAddr* [*IfaceAddr*] : Deletes an entry with a specific IP address, where *InetAddr* is the IP address. To delete an entry in a table for a specific interface, use the *IfaceAddr* parameter where *IfaceAddr* is the IP address assigned to the interface. To delete all entries, use the asterisk (*) wildcard character in place of *InetAddr*.

-s *InetAddr EtherAddr* [*IfaceAddr*] : Adds a static entry to the ARP cache that resolves the IP address *InetAddr* to the physical address *EtherAddr*. To add a static ARP cache entry to the table for a specific interface, use the *IfaceAddr* parameter where *IfaceAddr* is an IP address assigned to the interface.

/? : Displays help at the command prompt.

Remarks

- The IP addresses for *InetAddr* and *IfaceAddr* are expressed in dotted decimal notation.
- The physical address for *EtherAddr* consists of six bytes expressed in hexadecimal notation and separated by hyphens (for example, 00-AA-00-4F-2A-9C).
- Entries added with the **-s** parameter are static and do not time out of the ARP cache. The entries are removed if the TCP/IP protocol is stopped and started. To create permanent static ARP cache entries, place the appropriate **arp** commands in a batch file and use **Scheduled Tasks** to run the batch file at startup.
- This command is available only if the **Internet Protocol (TCP/IP)** protocol is installed as a component in the properties of a network adapter in Network Connections

Examples

To display the ARP cache tables for all interfaces, type:

```
arp -a
```

To display the ARP cache table for the interface that is assigned the IP address 10.0.0.99, type:

```
arp -a -N 10.0.0.99
```

To add a static ARP cache entry that resolves the IP address 10.0.0.80 to the physical address 00-AA-00-4F-2A-9C, type:

```
arp -s 10.0.0.80 00-AA-00-4F-2A-9C
```

ICMP

The **Internet Control Message Protocol** (**ICMP**) is one of the core protocols of the Internet protocol suite. It is chiefly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached.

ICMP differs in purpose from TCP and UDP in that it is usually *not* used directly by user network applications. One exception is the ping tool, which sends ICMP Echo Request messages (and receives Echo Response messages) to determine whether a host is reachable and how long packets take to get to and from that host.

Internet control message protocol is part of the Internet protocol suite as defined in RFC 792. ICMP messages are typically generated in response to errors in IP datagrams (as specified in RFC 1122) or for diagnostic or routing purposes.

Ping Command

Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, **ping** displays help.

Syntax

ping [**-t**] [**-a**] [**-n** *Count*] [**-l** *Size*] [**-f**] [**-i** *TTL*] [**-v** *TOS*] [**-r** *Count*] [**-s** *Count*] [{**-j** *HostList* | **-k** *HostList*}] [**-w** *Timeout*] [*TargetName*]

Parameters

-t : Specifies that ping continue sending Echo Request messages to the destination until interrupted. To interrupt and display statistics, press CTRL-BREAK. To interrupt and quit ping, press CTRL-C.

-a : Specifies that reverse name resolution is performed on the destination IP address. If this is successful, ping displays the corresponding host name.

-n *Count* : Specifies the number of Echo Request messages sent. The default is 4.

-l *Size* : Specifies the length, in bytes, of the Data field in the Echo Request messages sent. The default is 32. The maximum *size* is 65,527.

-f : Specifies that Echo Request messages are sent with the Don't Fragment flag in the IP header set to 1. The Echo Request message cannot be fragmented by routers in the path to the destination. This parameter is useful for troubleshooting path Maximum Transmission Unit (PMTU) problems.

-i *TTL* : Specifies the value of the TTL field in the IP header for Echo Request messages sent. The default is the default TTL value for the host. For Windows XP hosts, this is typically 128. The maximum *TTL* is 255.

-v *TOS* : Specifies the value of the Type of Service (TOS) field in the IP header for Echo Request messages sent. The default is 0. *TOS* is specified as a decimal value from 0 to 255.

-r *Count* : Specifies that the Record Route option in the IP header is used to record the path taken by the Echo Request message and corresponding Echo Reply message. Each hop in the path uses an entry in the Record Route option. If possible, specify a *Count* that is equal to or greater than the number of hops between the source and destination. The *Count* must be a minimum of 1 and a maximum of 9.

-s *Count* : Specifies that the Internet Timestamp option in the IP header is used to record the time of arrival for the Echo Request message and corresponding Echo Reply message for each hop. The *Count* must be a minimum of 1 and a maximum of 4.

-j *HostList* : Specifies that the Echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in *HostList*. With loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the host list is 9. The host list is a series of IP addresses (in dotted decimal notation) separated by spaces.

-k *HostList* : Specifies that the Echo Request messages use the Strict Source Route option in the IP header with the set of intermediate destinations specified in *HostList*. With strict source routing, the next intermediate destination must be directly reachable (it must be a neighbor on an interface of the router). The maximum number of addresses or names in the host list is 9. The host list is a series of IP addresses (in dotted decimal notation) separated by spaces.

-w *Timeout* : Specifies the amount of time, in milliseconds, to wait for the Echo Reply message that corresponds to a given Echo Request message to be received. If the Echo Reply message is not received within the time-out, the "Request timed out" error message is displayed. The default time-out is 4000 (4 seconds).

***TargetName* :** Specifies the destination, which is identified either by IP address or host name.

/? : Displays help at the command prompt.

Remarks

- You can use **ping** to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name is not, you might have a name resolution problem. In this case, ensure that the computer name you are specifying can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.
- This command is available only if the **Internet Protocol (TCP/IP)** protocol is installed as a component in the properties of a network adapter in Network Connections

Examples

The following example shows **ping** command output:

```
C:\>ping example.microsoft.com

Pinging example.microsoft.com [192.168.239.132] with 32 bytes of data:

Reply from 192.168.239.132: bytes=32 time=101ms TTL=124

Reply from 192.168.239.132: bytes=32 time=100ms TTL=124

Reply from 192.168.239.132: bytes=32 time=120ms TTL=124

Reply from 192.168.239.132: bytes=32 time=120ms TTL=124
```

To ping the destination 10.0.99.221 and resolve 10.0.99.221 to its host name, type:

ping -a 10.0.99.221

To ping the destination 10.0.99.221 with 10 Echo Request messages, each of which has a Data field of 1000 bytes, type:

ping -n 10 -l 1000 10.0.99.221

To ping the destination 10.0.99.221 and record the route for 4 hops, type:

ping -r 4 10.0.99.221

To ping the destination 10.0.99.221 and specify the loose source route of 10.12.0.1-10.29.3.1-10.1.44.1, type:

ping -j 10.12.0.1 10.29.3.1 10.1.44.1 10.0.99.221

Tracert Command

Determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live (TTL) field values. The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination. The near-side interface is the interface of the router that is closest to the sending host in the path. Used without parameters, **tracert** displays help.

Syntax

tracert [**-d**] [**-h** *MaximumHops*] [**-j** *HostList*] [**-w** *Timeout*] [*TargetName*]

Parameters

-d : Prevents **tracert** from attempting to resolve the IP addresses of intermediate routers to their names. This can speed up the display of **tracert** results.

-h ***MaximumHops*** **:** Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.

-w ***Timeout*** **:** Specifies the amount of time in milliseconds to wait for the ICMP Time Exceeded or Echo Reply message corresponding to a given Echo Request message to be received. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds).

TargetName **:** Specifies the destination, identified either by IP address or host name.

-? : Displays help at the command prompt.

Remarks

- This diagnostic tool determines the path taken to a destination by sending ICMP Echo Request messages with varying Time to Live (TTL) values to the destination. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP Time Exceeded message to the source computer. Tracert determines the path by sending the first Echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 30 by default and can be specified using the **-h** parameter. The path is determined by examining the ICMP Time Exceeded messages returned by intermediate routers and the Echo Reply message returned by the destination. However, some routers do not return Time Exceeded messages for packets with expired TTL values and are invisible to the tracert command. In this case, a row of asterisks (*) is displayed for that hop.
- To trace a path and provide network latency and packet loss for each router and link in the path, use the **pathping** command.
- This command is available only if the **Internet Protocol (TCP/IP)** protocol is installed as a component in the properties of a network adapter in Network Connections

Examples

To trace the path to the host named corp7.microsoft.com, type:

tracert corp7.microsoft.com

To trace the path to the host named corp7.microsoft.com and prevent the resolution of each IP address to its name, type:

tracert -d corp7.microsoft.com

Netstat

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, **netstat** displays active TCP connections.

Syntax

netstat [**-a**] [**-e**] [**-n**] [**-o**] [**-p** *Protocol*] [**-r**] [**-s**] [*Interval*]

Parameters

-a : Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

-e : Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with **-s**.

-n : Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.

-o : Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the **Processes** tab in Windows Task Manager. This parameter can be combined with **-a**, **-n**, and **-p**.

-p *Protocol* : Shows connections for the protocol specified by *Protocol*. In this case, the *Protocol* can be **tcp**, **udp**, **tcpv6**, or **udpv6**. If this parameter is used with **-s** to display statistics by protocol, *Protocol* can be **tcp**, **udp**, **icmp**, **ip**, **tcpv6**, **udpv6**, **icmpv6**, or **ipv6**.

-s : Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The **-p** parameter can be used to specify a set of protocols.

-r : Displays the contents of the IP routing table. This is equivalent to the **route print** command.

***Interval* :** Redisplays the selected information every *Interval* seconds. Press CTRL+C to stop the redisplay. If this parameter is omitted, **netstat** prints the selected information only once.

/? : Displays help at the command prompt.

Remarks

- Parameters used with this command must be prefixed with a hyphen (**-**) rather than a slash (**/**).
- **Netstat** provides statistics for the following:
  - Proto

    The name of the protocol (TCP or UDP).
  - Local Address

    The IP address of the local computer and the port number being used. The name of the local computer that corresponds to the IP address and the name of the port is shown unless the **-n** parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).

- Foreign Address

  The IP address and port number of the remote computer to which the socket is connected. The names that corresponds to the IP address and the port are shown unless the **-n** parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).
- (state)

  Indicates the state of a TCP connection. The possible states are as follows:

  CLOSE_WAIT

  CLOSED

  ESTABLISHED

  FIN_WAIT_1

  FIN_WAIT_2

  LAST_ACK

  LISTEN

  SYN_RECEIVED

  SYN_SEND

  TIMED_WAIT

  For more information about the states of a TCP connection, see RFC 793.
- This command is available only if the **Internet Protocol (TCP/IP)** protocol is installed as a component in the properties of a network adapter in Network Connections

Examples

To display both the Ethernet statistics and the statistics for all protocols, type the following command:

netstat -e -s

To display the statistics for only the TCP and UDP protocols, type the following command:

netstat -s -p tcp udp

To display active TCP connections and the process IDs every 5 seconds, type the following command:

nbtstat -o 5

To display active TCP connections and the process IDs using numerical form, type the following command:

```
nbtstat -n –o
```

DNS

On the Internet, the **Domain Name System** (DNS) stores and associates many types of information with domain names; most importantly, it translates domain names (computer hostnames) to IP addresses. It also lists mail exchange servers accepting e-mail for each domain. In providing a worldwide keyword-based redirection service, DNS is an essential component of contemporary Internet use.

The most basic use of DNS is to translate hostnames to IP addresses. It is in very simple terms like a phone book. For example, if you want to know the internet address of en.wikipedia.org, DNS can be used to tell you it's 66.230.200.100. DNS also has other important uses.

Pre-eminently, the DNS makes it possible to assign Internet destinations to the human organization or concern they represent, independently of the physical routing hierarchy represented by the numerical IP address. Because of this, hyperlinks and Internet contact information can remain the same, whatever the current IP routing arrangements may be, and can take a human-readable form (such as "`wikipedia.org`") which is rather easier to remember than an IP address (such as 66.230.200.100). People take advantage of this when they recite meaningful URLs and e-mail addresses without caring how the machine will actually locate them.

Nslookup Command

Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The Nslookup command-line tool is available only if you have installed the TCP/IP protocol.

Syntax

nslookup [-*SubCommand* ...] [{*ComputerToFind*| [-*Server*]}]

Nslookup Command

Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The Nslookup command-line tool is available only if you have installed the TCP/IP protocol.

Syntax

nslookup [-*SubCommand* ...] [{*ComputerToFind*| [-*Server*]}]

Parameters

***-SubCommand* ... :** Specifies one or more **nslookup** subcommands as a command-line option. For a list of subcommands, see Related Topics.

***ComputerToFind* :** Looks up information for *ComputerToFind* using the current default DNS name server, if no other server is specified. To look up a computer not in the current DNS domain, append a period to the name.

***-Server* :** Specifies to use this server as the DNS name server. If you omit -*Server*, the default DNS name server is used.

{help|?} : Displays a short summary of **nslookup** subcommands.

Remarks

- If *ComputerToFind* is an IP address and the query is for an A or PTR resource record type, the name of the computer is returned. If *ComputerToFind* is a name and does not have a trailing period, the default DNS domain name is appended to the name. This behavior depends on the state of the following **set** subcommands: **domain**, **srchlist**, **defname**, and **search**.
- If you type a hyphen (-) instead of *ComputerToFind*, the command prompt changes to **nslookup** interactive mode.
- The command-line length must be less than 256 characters.
- **Nslookup** has two modes: interactive and noninteractive.

  If you need to look up only a single piece of data, use noninteractive mode. For the first parameter, type the name or IP address of the computer that you want to look up. For the second parameter, type the name or IP address of a DNS name server. If you omit the second argument, **nslookup** uses the default DNS name server.

  If you need to look up more than one piece of data, you can use interactive mode. Type a hyphen (-) for the first parameter and the name or IP address of a DNS name server for the second parameter. Or, omit both parameters and **nslookup** uses the default DNS name server. Following are some tips about working in interactive mode:

  - To interrupt interactive commands at any time, press CTRL+B.
  - To exit, type **exit**.
  - To treat a built-in command as a computer name, precede it with the escape character (\).
  - An unrecognized command is interpreted as a computer name.
- If the lookup request fails, **nslookup** prints an error message. The following table lists possible error messages.

Error message	Description
Timed out	The server did not respond to a request after a certain amount of time and a certain number of retries. You can set the time-out period with the **set timeout** subcommand. You can set the number of retries with the **set retry** subcommand.
No response from server	No DNS name server is running on the server computer.
No records	The DNS name server does not have resource records of the current query type for the computer, although the computer name is valid. The query type is specified with the **set querytype** command.
Nonexistent domain	The computer or DNS domain name does not exist.
Connection	The connection to the DNS name server or finger server could not be made.

refused -or- Network is unreachable	This error commonly occurs with **ls** and **finger** requests.
Server failure	The DNS name server found an internal inconsistency in its database and could not return a valid answer.
Refused	The DNS name server refused to service the request.
Format error	The DNS name server found that the request packet was not in the proper format. It may indicate an error in **nslookup**.

***-SubCommand* ... :** Specifies one or more **nslookup** subcommands as a command-line option. For a list of subcommands, see Related Topics.

***ComputerToFind* :** Looks up information for *ComputerToFind* using the current default DNS name server, if no other server is specified. To look up a computer not in the current DNS domain, append a period to the name.

***-Server* :** Specifies to use this server as the DNS name server. If you omit *-Server*, the default DNS name server is used.

{help|?} : Displays a short summary of **nslookup** subcommands.

Remarks

- If *ComputerToFind* is an IP address and the query is for an A or PTR resource record type, the name of the computer is returned. If *ComputerToFind* is a name and does not have a trailing period, the default DNS domain name is appended to the name. This behavior depends on the state of the following **set** subcommands: **domain**, **srchlist**, **defname**, and **search**.
- If you type a hyphen (-) instead of *ComputerToFind*, the command prompt changes to **nslookup** interactive mode.
- The command-line length must be less than 256 characters.
- **Nslookup** has two modes: interactive and noninteractive.

  If you need to look up only a single piece of data, use noninteractive mode. For the first parameter, type the name or IP address of the computer that you want to look up. For the second parameter, type the name or IP address of a DNS name server. If you omit the second argument, **nslookup** uses the default DNS name server.

  If you need to look up more than one piece of data, you can use interactive mode. Type a hyphen (-) for the first parameter and the name or IP address of a DNS name server for the second parameter. Or, omit both parameters and **nslookup** uses the default DNS name server. Following are some tips about working in interactive mode:

  - To interrupt interactive commands at any time, press CTRL+B.
  - To exit, type **exit**.
  - To treat a built-in command as a computer name, precede it with the escape character (\).
  - An unrecognized command is interpreted as a computer name.
- If the lookup request fails, **nslookup** prints an error message. The following table lists

possible error messages.

Error message	Description
Timed out	The server did not respond to a request after a certain amount of time and a certain number of retries. You can set the time-out period with the **set timeout** subcommand. You can set the number of retries with the **set retry** subcommand.
No response from server	No DNS name server is running on the server computer.
No records	The DNS name server does not have resource records of the current query type for the computer, although the computer name is valid. The query type is specified with the **set querytype** command.
Nonexistent domain	The computer or DNS domain name does not exist.
Connection refused -or- Network is unreachable	The connection to the DNS name server or finger server could not be made. This error commonly occurs with **ls** and **finger** requests.
Server failure	The DNS name server found an internal inconsistency in its database and could not return a valid answer.
Refused	The DNS name server refused to service the request.
Format error	The DNS name server found that the request packet was not in the proper format. It may indicate an error in **nslookup**.

Sources

1. Microsoft TCP/IP Utilities
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ipconfig.mspx?mfr=true
2. Wikipedia http://en.wikipedia.org