Network Troubleshooting CLI Commands

Windows macOS/*nix Description & Options

ping ping Test the network

Test the network connection with a remote IP address

ping-t [IP or host] ping-l 1024 [IP or host]

The -t option to ping continuously until Ctrl-C is pressed.

If you specify the -t option you can always get statistics without interrupting pings by pressing Ctrl + Break

tracert traceroute

Displays all intermediate IP addresses through which a packet passes through, between the local machine and the specified IP address.

tracert [@IP or host] tracert -d [@IP or host]

This command is useful if the ping command does return any data, to determine at what level the connection failed.

- -T Use TCP SYN for probes
- -I Use ICMP ECHO for probes
- -F Do not fragment probe packets.
- -n Do not try to map IP addresses to host names when displaying
- -p n For UDP tracing, specifies the destination port base traceroute will use (the destination port number will be incremented by each probe). For ICMP tracing, specifies the initial icmp sequence value (incremented by each probe too). For TCP specifies just the (constant) destination port to connect.
- **-t** tos For IPv4, set the Type of Service (TOS) and Precedence value. Useful values are 16 (low delay) and 8 (high throughput). Note that in order to use some TOS precendence values, you have to be super user. For IPv6, set the Traffic Control value.
- -w waittime Set the time (in seconds) to wait for a response to a probe (default 5.0 sec).
- -q nqueries Sets the number of probe packets per hop. Default is 3
- -A Perform AS path lookups in routing registries and print results directly after the corresponding addresses.
- -M method Use specified method for traceroute operations. Default traditional udp method has name default, icmp (-I) and tcp (-T) have names icmp and tcp respectively. Method-specific options can be passed by -O . Most methods have their simple shortcuts, (-I means -M icmp, etc).
- --mtu Discover MTU along the path being traced. Implies -F -N 1. New mtu is printed once in a form of F=NUM at the first probe of a hop which requires such mtu to be reached.

dig dig

Get DNS information

dig domain

- -p n Where n is the port number that dig will send its queries instead of the standard DNS port number 53. This option would be used to test a name server that has been configured to listen for queries on a non-standard port number.
 - -x Perform a reverse lookup.
- **-t type** Sets the query type to *type*. The default query type is "A", unless the **-x** option is supplied to indicate a reverse lookup.

@IP/name Specify the name or IP address of the name server to query. This can be an IPv4 address in dotted-decimal notation or an IPv6 address in colon-delimited notation.

ipconfig ifconfig

Displays or refresh the TCP/IP configuration

ipconfig /all [/release [adapter]] [/renew [adapter]]
/flushdns /displaydns /registerdns [-a] [-a] [-a]

/all: Displays all network configuration, including DNS, WINS, DHCP servers, etc ...

/renew [adapter]: Renews DHCP configuration for all adapters or a specific adapter indicated by the [adapter] parameter.

/release [adapter]: Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and cancel the IP address configuration for all adapters (if adapter is not specified) or a specific adapter indicated by the [adapter] parameter. This parameter disables TCP/IP for network cards configured to automatically obtain an IP address.

/flushdns: Empty and reset DNS client resolver cache. Option is useful to exclude negative entries & all other entries added dynamically to cache /displaydns: Displays the DNS client resolver cache, which includes entries preloaded from the local host file and any recently obtained records for name queries resolved by the host computer. The DNS Client service uses this information to quickly resolve frequently queried names, before querying the configured DNS servers.

/registerdns: Refreshes all DHCP leases and re-registers DNS names.

telnet telnet

TELNET

telnet <IP or host> telnet <IP or host> <port TCP>

The telnet command to access to a remote host in Terminal mode (passive screen). It also allows you to check if any TCP service is running on a remote server by specifying the IP address after the TCP port number. The most common ports are:

ftp (21), telnet (23), smtp (25), www (80), pop3 (110), nntp (119), nbt (137-

netstat netstat

Displays the status of the TCP/IP stack on the local machine netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

- -a Displays all connections and listening ports (server-side connections are normally inhibited).
- -e Displays Ethernet statistics. Can 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. Used with the -s option to display per-protocol statistics, proto may be TCP, UDP or IP.
- -r Displays the contents of the routing table.
- -s Displays statistics by protocol. By default, statistics on TCP, UDP and IP are displayed, the -p option can be used to specify a subset. interval: Re-display the selected statistics, pausing after a specific "interval" (in seconds) between each display. Press Ctrl + C to stop displaying statistics.
- -abnov Displays processes using the internet connection (local IP address, port, remote IP adress and the PID of the process that uses the connection as well as its name).

Arp Arp

ARP: Resolving IP addresses to MAC addresses. Displays and modifies the translation tables of IP addresses to physical addresses used by the ARP address resolution protocol.

ARP -s adr_inet adr_eth [adr_if] ARP -d adr_inet [adr_if] ARP -a [adr_inet] [-N adr_if]

- -a Displays active ARP entries by interrogating the current data protocol. If adr_inet is specified, only the physical and IP addresses of the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
- -g is the same as -a

adr_inet Specifies an internet address.

- -N adr_if Displays ARP entries for network interface specified by adr_if.
- -d Deletes the host specified by adr_inet.
- -s Adds the host and associates the adr_inet internet address with the adr_eth physical address. The physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

adr_eth Specifies a physical address.

adr_if Specifies the internet interface whose address translation table should be modified. When not specified, the first applicable interface will be used.

hostname

Displays the name of the machine

nslookup nslookup

nslookup sends DNS requests to a DNS server

nslookup [domain] [dns server]

The nslookup command to send DNS requests to a server. By default, if you do not specify the DNS server, the command will use the one that is configured for your network interface

netsh

netsh: command-line scripting utility

netsh [-a AliasFile] [-c Context] [-r RemoteComputer]
[{NetshCommand -f Scriptile}]

- -a Returns you to the **netsh** prompt after running AliasFile.
- -c Changes to the specifed netsh context.
- -r Configures a remote computer
- -f Exits netsh.exe after running the script
- /? Displays help at the command prompt

Some Wireless LAN netsh Commands to try

netsh wlan show interfaces

netsh wlan show wlanreport

netsh wlan show wirelesscapabilities

netsh wlan show profiles

netsh wlan show networks

netsh wlan show interface name="Interface_Name"

netsh wlan show drivers

netsh wlan export profile name="ProfileName"

netsh trace show wlans

netsh trace show scenarios

netsh trace show NetConnections