**Class: SY B.Tech Sem VI**

**AY: 2023-2024**

**Course: Information Theory for Cyber Security (Laboratory)**

**Couse Code: 1ICPC210**

**Experiment No. 1 (Part A)**

**Title: Perform Basic commands of Network and Operating system**

* Ipconfig, Tracert, Ping, ARP, Netstat, Nslookup, Hostname, Nbtstat, Getmac, Systeminfo

**Objectives:**

1. **Evaluate Command Execution Efficiency**: Measure the time taken by various networking commands (e.g., ping, traceroute, nslookup) to execute on different network configurations or devices.
2. **Assess Command Accuracy:** Determine the accuracy and reliability of networking commands in providing expected results under various network conditions (e.g., latency, packet loss, network congestion).
3. **Compare Command Performance Across Platforms:** Compare the performance of networking commands across different operating systems (e.g., Windows, Linux, macOS) or network devices (e.g., routers, switches, firewalls).
4. **Optimize Command Parameters**: Experiment with different parameters (e.g., packet size, timeout values) of networking commands to optimize their performance under specific network conditions.

**Ipconfig/Ifconfig:**

Ipconfig is used to view and configure the network settings on a Windows computer. It’s often used to troubleshoot network issues, like connectivity problems or incorrect IP addresses. It also works to view the current IP configuration of a computer, as the command displays the IP addresses assigned to their network adapters as well as the default gateway and DNS servers.

Options:

IPCONFIG /all Display full configuration information.

IPCONFIG /release [adapter] Release the IPv4 address for the specified adapter.

IPCONFIG /release6 [adapter] Release the IPv6 address for the specified adapter.

IPCONFIG /renew [adapter] Renew the IPv4 address for the specified adapter.

IPCONFIG /renew6 [adapter] Renew the IPv6 address for the specified adapter.

IPCONFIG /flushdns Purge the DNS Resolver cache.

IPCONFIG /registerdns Refresh all DHCP leases and re-register DNS names.

IPCONFIG /displaydns Display the contents of the DNS Resolver Cache.

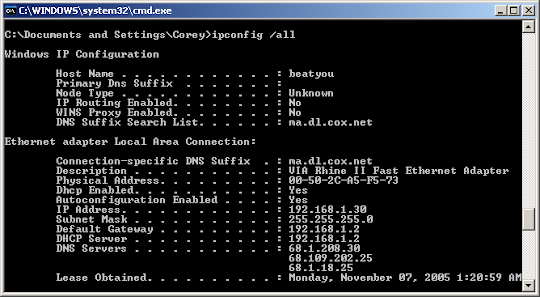
IPCONFIG /showclassid adapter Display all the DHCP class IDs allowed for adapter.

IPCONFIG /showclassid6 adapter Display all the IPv6 DHCP class IDs allowed for adapter.

IPCONFIG /setclassid adapter [classid] Modify the DHCP class id.

IPCONFIG /setclassid6 adapter [classid] Modify the IPv6 DHCP class id.

IPCONFIG /? Display help.



**Ping:**

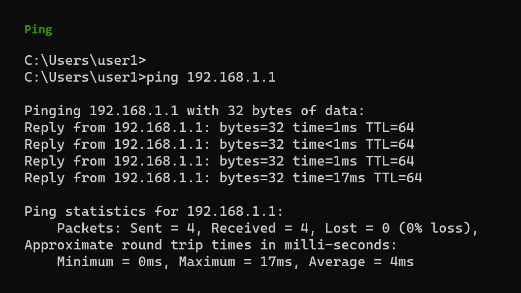
Ping (Packet InterNet Groper) is a utility that sends a signal to another computer over a network and then receives a reply from the computer that was pinged and sends it back to the first computer.

With the ping command, you can quickly determine whether a machine has internet access and can communicate with other computers or network devices. Ping also has additional features such as:

1. Network connectivity testing
2. Network interface card troubleshooting
3. Putting DNS name resolution issues to the test

Options:

|  |  |
| --- | --- |
| -4 | Force IPv4 |
| -6 | Force IPv6 |
| -d | Forbid fragmentation |
| -f | flood ping: Sends a large number of pings in a short time. Can be used to test network bandwidth, for example.  Important: It is easy for flood ping to be misinterpreted as a denial-of-service (DoS) attack. |
| -n | Returns the computer name of a specified IP address. |
| -o | Immediately sends another request after a response. |
| -q | Ping command returns no output to the CLI (quiet). |
| -r | Switches to the traceroute mode. The path taken by the data packets to the target computer is displayed with all intermediate stations. |
| -b | Do not stop pinging after receiving a PacketTooBig (DF), in order to achieve "Path MTU Discovery". |
| -s n | Sets the packet size to n bytes (max. 65500). |
| -i n | Time between packets in seconds. |
| -c n | Send n pings. |
| [-x x] | Atomic fragments: (n)ever, (f)orce, (a)utomatic |
| [-p <dscp>] | Use a specific DSCP value for this ping. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service). Possible DSCP values: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF |
| -a a.b.c.d | Sets the ping's sender address (default: IP address of the device. |
| -a <name> | Uses a named network, interface, or loopback address as the sender address |

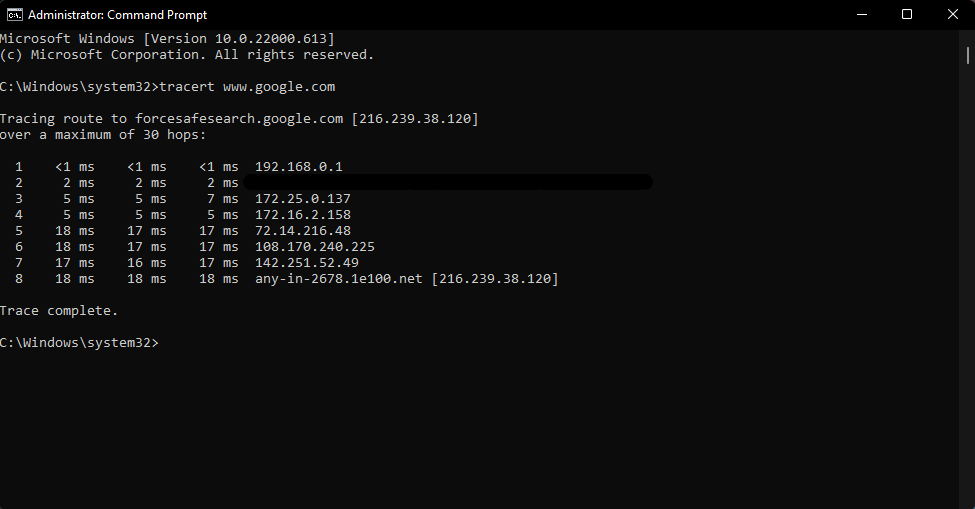


**Tracert:**

Traceroute is a utility that records the Internet route (gateway computers at each hop) between your computer and a specified destination computer. It also calculates and displays the amount of time for each hop. This utility helps you find where high transfer times are occurring in your internal network and the Internet.

Options:

|  |  |
| --- | --- |
| -d | This option prevents tracert from resolving [IP addresses](https://www.lifewire.com/what-is-an-ip-address-2625920) to [hostnames](https://www.lifewire.com/what-is-a-hostname-2625906), often resulting in much faster results. |
| -h MaxHops | This tracert option specifies the maximum number of [hops](https://www.lifewire.com/what-are-hops-hop-counts-2625905) in the search for the target. If you do not specify MaxHops, and a target has not been found by 30 hops, tracert will stop looking. |
| -w TimeOut | You can specify the time, in milliseconds, to allow each reply before timeout using this tracert option. |
| -4 | This option forces tracert to use IPv4 only. |
| -6 | This option forces tracert to use IPv6 only. |
| target | This is the destination, either an IP address or hostname. |
| /? | Use the [help switch](https://www.lifewire.com/help-switch-2625896) with the tracert command to show detailed help about the command's several options. |



**ARP:**

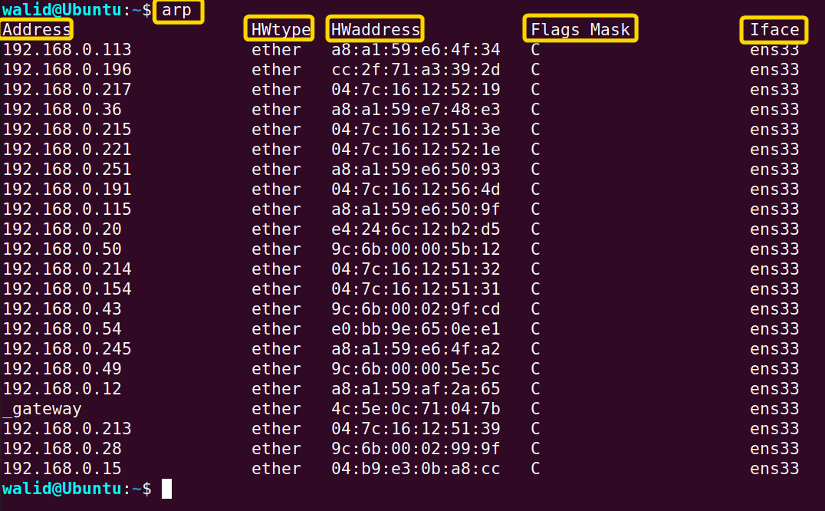
The ARP commands to view, display, or modify the details/information in an ARP table/cache.

The ARP cache or table has the dynamic list of IP and MAC addresses of those devices to which your computer has communicated recently in a local network. The purpose of maintaining an [ARP table](https://www.javatpoint.com/arp-table) is that when you want to communicate with another device, your device does not need to send the [ARP request](https://www.javatpoint.com/arp-request) for the MAC address of that device.

The [ARP](https://www.javatpoint.com/address-resolution-protocol) commands also helps to find out the duplicate [IP](https://www.javatpoint.com/ip-full-form) address and invalid entries in an ARP table/cache.

Options:

* arp -a: This command is used to display the ARP table for a particular IP address. It also shows all the entries of the ARP cache or table.
* arp -g: This command works the same as the arp -a command.
* arp -d: This command is used when you want to delete an entry from the ARP table for a particular interface. To delete an entry, write arp -d command along with the IP address in a command prompt you want to delete.
* arp -d \*: You can also delete all the entries from the ARP table. This command will remove or flush all the entries from the table.
* arp -s: This command is used to add the static entry in the ARP table, which resolves the InetAddr (IP address) to the EtherAddr (physical address). To add a static entry in an ARP table, write arp -s command along with the IP address and MAC address of the device in a command prompt.
* /?: This command is used to show the help at the command prompt.
* arp purge-delay: The arp purge-delay command delays the purging in the ARP entries in an ARP table/cache when the interface goes down or slows down. When the interface comes up within the delay time, the ARP entries are restored, and packet loss with ECMP (Equal Cost Multipath) is restricted.
* no arp purge-delay: This command is used to turn off the purge delay.
* arp timeout: This command is used to determine how long the dynamic entries learned on the interface resides in the ARP cache. This command is also used in the interface configuration mode. When the timeout of an interface changes, this change only applies to that particular interface.
* show interface: This command is used to show the ARP timeout value. The format of the timeout value is hours: minutes: seconds.
* clear arp cache: This command deletes/removes all the dynamic entries from the ARP table.
* proxy-arp: This command is used to enable the proxy ARP on an interface. The network devices are able to respond to ARP requests only when the proxy ARP is enabled.
* no proxy-arp: This command is used to disable the proxy-arp on the interface.
* show arp: This command is used to indicate the Address Resolution Protocol. ARP creates a correspondence between network addresses and hardware addresses of Ethernet. The record of each correspondence is stored in an ARP table for a fixed amount of time.
* show arp traffic: This command is used to display the static traffic on the Address Resolution Protocol (ARP).

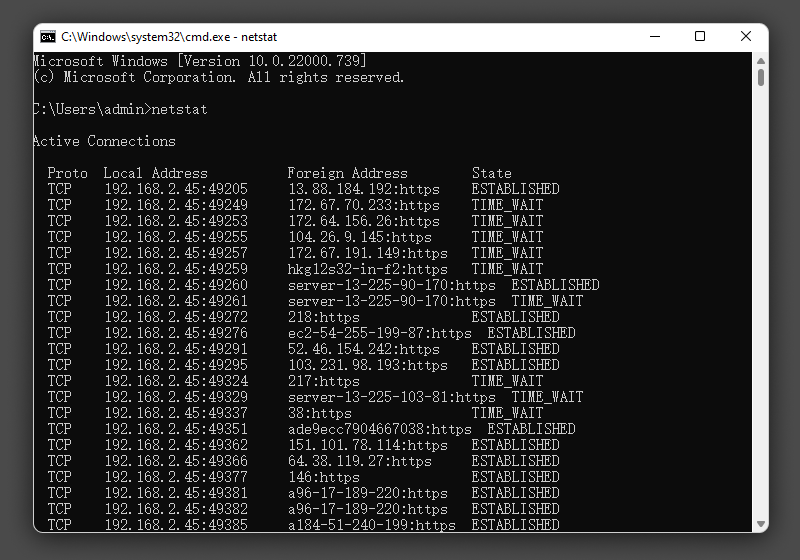


**Netstat:**

The netstat command is like a special tool in [Linux](https://www.geeksforgeeks.org/introduction-to-linux-operating-system/) that helps you understand and check things about how your computer connects to the internet. It can tell you about the connections your computer is making, the paths it uses to send information, and even some technical details like how many packets of data are being sent or received.

Options:

|  |  |
| --- | --- |
| netstat | Execute the netstat command alone to show a relatively simple list of all active [TCP](https://www.lifewire.com/transmission-control-protocol-and-internet-protocol-816255) connections which, for each one, will show the local [IP address](https://www.lifewire.com/what-is-an-ip-address-2625920) (your computer), the foreign IP address (the other computer or network device), along with their respective port numbers, as well as the TCP state. |
| -a | This switch displays active TCP connections, TCP connections with the listening state, as well as UDP ports that are being listened to. |
| -b | This netstat switch is very similar to the -o switch listed below, but instead of displaying the PID, will display the process's actual file name. Using -b over -o might seem like it's saving you a step or two but using it can sometimes greatly extend the time it takes netstat to fully execute. |
| -e | Use this switch with the netstat command to show statistics about your network connection. This data includes bytes, unicast packets, non-unicast packets, discards, errors, and unknown protocols received and sent since the connection was established. |
| -f | The -f switch will force the netstat command to display the [Fully Qualified Domain Name](https://www.lifewire.com/what-does-fqdn-mean-2625883) (FQDN) for each foreign IP addresses when possible. |
| -n | Use the -n switch to prevent netstat from attempting to determine [host names](https://www.lifewire.com/what-is-a-hostname-2625906) for foreign IP addresses. Depending on your current network connections, using this switch could considerably reduce the time it takes for netstat to fully execute. |
| -o | A handy option for many troubleshooting tasks, the -o switch displays the process identifier (PID) associated with each displayed connection. See the example below for more about using netstat -o. |
| -p | Use the -p switch to show connections or statistics only for a particular protocol. You can not define more than one protocol at once, nor can you execute netstat with -p without defining a protocol. |
| protocol | When specifying a protocol with the -p option, you can use tcp, udp, tcpv6, or udpv6. If you use -s with -p to view statistics by protocol, you can use icmp, ip, icmpv6, or ipv6 in addition to the first four I mentioned. |
| -r | Execute netstat with -r to show the IP routing table. This is the same as using the route command to execute route print. |
| -s | The -s option can be used with the netstat command to show detailed statistics by protocol. You can limit the statistics shown to a particular protocol by using the -soption and specifying that protocol, but be sure to use -s before -p protocol when using the switches together. |
| -t | Use the -t switch to show the current TCP chimney offload state in place of the typically displayed TCP state. |
| -x | Use the -x option to show all NetworkDirect listeners, connections, and shared endpoints. |
| -y | The -y switch can be used to show the TCP connection template for all connection. You cannot use -y with any other netstat option. |
| time\_interval | This is the time, in seconds, that you'd like the netstat command to re-execute automatically, stopping only when you use [Ctrl-C](https://www.lifewire.com/what-is-ctrl-c-used-for-2625834) to end the loop. |
| /? | Use the [help switch](https://www.lifewire.com/help-switch-2625896) to show details about the netstat command's several options. |

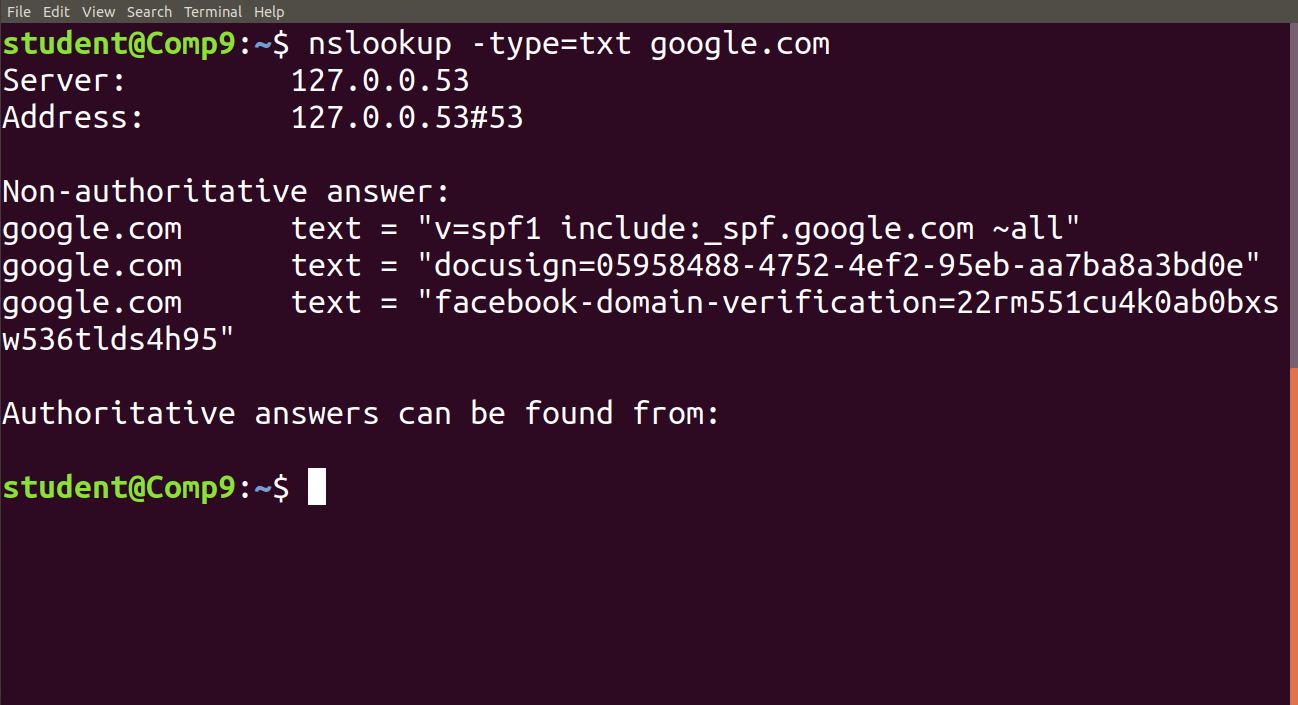


**Nslookup:**

Network administrators use nslookup to [troubleshoot server connections](https://www.techtarget.com/searchnetworking/tip/Troubleshoot-name-resolution-on-Windows-Linux-and-macOS) or for security reasons. For example, network pros might use nslookup to guard against [phishing](https://www.techtarget.com/searchsecurity/definition/phishing) attacks, in which attackers alter domain names. An attacker might substitute the numeral 1 for a lowercase l to make an unfriendly site look friendly and familiar, e.g., *joes1owerprices.com* vs. *joeslowerprices.com*. Network admins use nslookup to troubleshoot such attacks. DNS, or nslookup, also helps deter [cache poisoning](https://www.techtarget.com/searchsecurity/definition/cache-poisoning), in which attackers distribute data to caching resolvers that pose as authoritative origin servers.

Options:

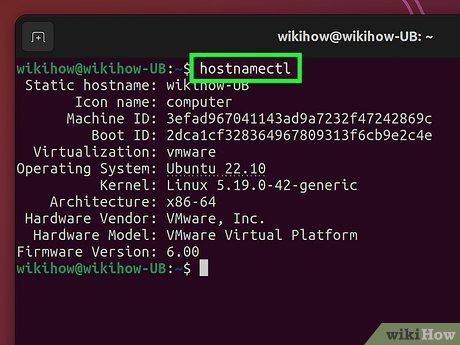
* /name -- queries the current name server for the specified name.
* /server name -- sets the current name server to the server the user specifies.
* /root -- sets the root server as the current server.
* /set type=x -- specifies the type of records to be displayed, such as A, [CNAME](https://www.techtarget.com/searchwindowsserver/definition/canonical-name), MX, NS, PTR or SOA. Specify ANY to display all records.
* /set debug -- turns on debug mode, which displays detailed information about each query.
* /set recurse -- tells the DNS name server to query other servers if it does not have the information.
* /exit -- exits nslookup and returns the user to a command prompt.



**Hostname:** Hostname command in Linux is used to obtain the[DNS (Domain Name System)](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/) name and set the system’s hostname or[NIS (Network Information System)](https://www.geeksforgeeks.org/linux-network-information-service/) domain name. A hostname is a name given to a computer and attached to the network. Its main purpose is to uniquely identify over a network.

Options:

|  |  |
| --- | --- |
| -a | This option is used to get the alias name of the host system (if any). It will return an empty line if no alias name is set. This option enumerates all configured addresses on all network interfaces. |
| -A | This option is used to get all FQDNs (Fully Qualified Domain Name) of the host system. It enumerates all configured addresses on all network interfaces. An output may display the same entries repetitively. |
| -b | Used to always set a hostname. Default name is used if none specified. |
| -d | This option is used to get the Domain if local domains are set. It will not return anything (not even a blank line) if no local domain is set. |
| -f | This option is used to get the Fully Qualified Domain Name (FQDN). It contains short hostname and DNS domain name. |
| -F | This option is used to set the hostname specified in a file. Can be performed by the superuser(root) only. |
| -i | This option is used to get the IP (network) addresses. This option works only if the hostname is resolvable. |
| -I | This option is used to get all IP(network) addresses. The option doesn’t depend on resolvability of hostname. |
| -s | This option is used to get the hostname in short. The short hostname is the section of hostname before the first period/dot(.). If the hostname has no period, the full hostname is displayed. |
| -V | Gives version number as output. |

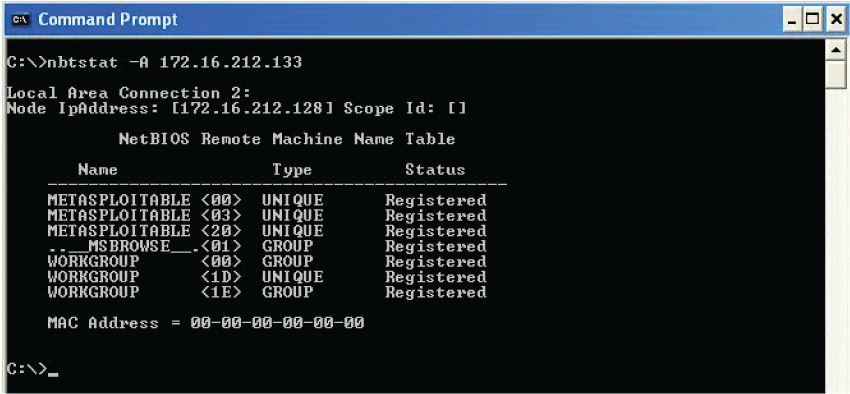


**Nbtstat:**

The nbtstat command displays information about the NetBIOS over TCP (NBT) connection for the Node. It displays the IP address associated with the interfaces, the broadcast IP mask, the IP addresses of the WINS servers in use, and information about the registered NetBIOS names for the node.

Options:

|  |  |
| --- | --- |
| -a RemoteName | Adapter status by name. Lists the name table of the remote machine identified by  machine name RemoteName. |
| -A IpAddress | Adapter status by address. Lists the name table of the remote machine  identified by [IP address](https://www.computerhope.com/jargon/i/ip.htm) IpAddress. |
| -c | Show cached name table. Lists NBT's cache of remote machine names  and their IP addresses. |
| -n | Shows local names. Lists local NetBIOS names. |
| -r | Shows resolved names. Lists names resolved by broadcast or WINS. |
| -R | Reload name table. Purges and reloads the cached name table. |
| -S | Shows sessions by IP address. Lists sessions table with the destination IP addresses. |
| -s | Shows sessions by name. Lists sessions table, converting destination IP addresses  to their NETBIOS names. |
| -RR | Release and refresh. Sends "release name" [packets](https://www.computerhope.com/jargon/p/packet.htm) to WINS, then refreshes  the list of names. |
| interval | If a numeric interval is specified, the program will continuously redisplay  the information specified by other options, pausing interval seconds between each display.  Press [Ctrl+C](https://www.computerhope.com/jargon/c/ctrlc.htm) to stop redisplaying statistics. |

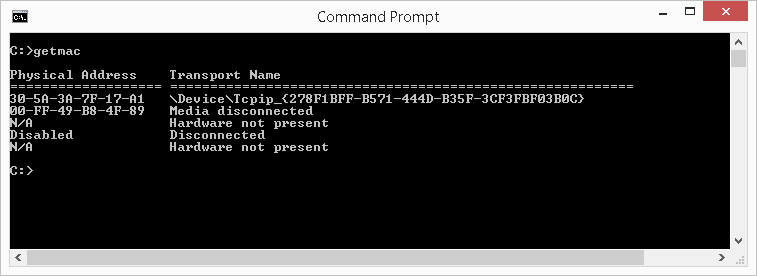


**Getmac:**

Returns the media access control (MAC) address and list of network protocols associated with each address for all network cards in each computer, either locally or across a network. This command is particularly useful either when you want to enter the MAC address into a network analyzer, or when you need to know what protocols are currently in use on each network adapter on a computer.

Options:

|  |  |
| --- | --- |
| /s <computer> | Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer. |
| /u <domain>\<user> | Runs the command with the account permissions of the user specified by user or domain\user. The default is the permissions of the current logged on user on the computer issuing the command. |
| /p <password> | Specifies the password of the user account that is specified in the /u parameter. |
| /fo {table | list | csv} | Specifies the format to use for the query output. Valid values are table, list, and csv. The default format for output is table. |
| /nh | Suppresses column header in output. Valid when the /fo parameter is set to table or csv. |
| /v | Specifies that the output display verbose information. |
| /? | Displays help at the command prompt. |

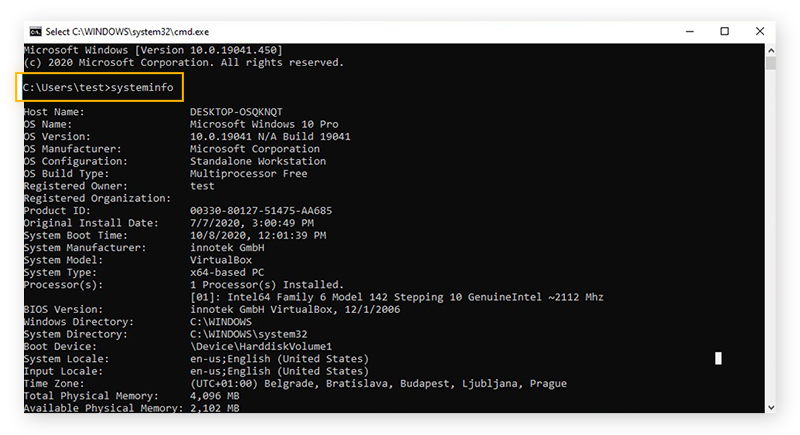


**Systeminfo:**

The systeminfo command is a built-in tool of the Windows operating system that displays detailed information about the computer’s hardware and software configuration. This command is used in the Command Prompt.

Options:

|  |  |
| --- | --- |
| /s system | Specifies the name or [IP address](https://www.computerhope.com/jargon/i/ip.htm) of a remote computer (do not use [backslashes](https://www.computerhope.com/jargon/b/backslash.htm)).  The default is the local computer. |
| /u [domain\]user | Runs the command with the account permissions specified by username or  domain\username. The default settings are those of the user who is currently logged in. |
| /p password | Specifies the password of the user account that is in the /u parameter. |
| /fo format | Specifies the format to use for the output. Valid format values are TABLE,  LIST, and [CSV](https://www.computerhope.com/jargon/c/csv.htm) (comma-separated values). The default format for output is LIST. |
| /nh | Suppresses column headers in the output. Valid only when the /fo parameter is set  to TABLE or CSV. |



**21st Century Skills:**

1. **Technical Proficiency**: Understanding networking commands requires technical proficiency in computer networking concepts, protocols, and infrastructure, which are fundamental skills in today's digital age.
2. **Problem-Solving:** Networking commands often involve troubleshooting network issues, diagnosing connectivity problems, and optimizing network performance, fostering problem-solving skills essential in various professional contexts.
3. **Attention to Detail:** Working with networking commands often involves dealing with intricate network configurations, protocols, and parameters, emphasizing the importance of attention to detail to ensure accurate and reliable results.
4. **Continuous Learning**: Networking is a vast and evolving field, requiring continuous learning and skill development to stay updated with the latest technologies, trends, and best practices, promoting a growth mindset and a commitment to lifelong learning.