WEEK 1.9

NETWORK COMMANDS

The ability to effectively troubleshoot computer and network related problems is an important skill. The process of identifying and solving a problem requires a systematic step-by-step approach. This laboratory introduces the most common related network commands.

🕛 You have one 2-hour supervised laboratory to work on the practical tasks. Outstanding sections of the laboratory must be completed in your own time.

Form **groups of four**

Start a document where you will be recording your answers for each task

To connect to Unix from Windows: Programs menu select > Host Access > Putty (SSH) > ssh student.cms.gre.ac.uk
You will be prompted for your user id and password.

TASK 1

Login to two machines on the CMS_DOMAIN network. On one machine, connect to the UNIX server. For each Windows machine, use the command prompt to enter **ipconfig**, which displays the IP address, Subnet Mask and Default Gateway. A machine may have multiple IP addresses such as wired, wireless and virtual networks. You need the IP address for the Ethernet adapter Local Area Connection

From the UNIX prompt enter **ifconfig –a**
Note, this does not display the default gateway.

The subnet mask is displayed in Hexadecimal, so you will need to convert it to dotted decimal.

Complete the following table.

	Machine A	Machine B	UNIX
IPv4 Address			
Subnet Mask			
Default Gateway			-
Machine's IP Class			
Machine's Network Address			
Machine's Host Address			

Medium Access Control (MAC) Addresses

A MAC address is a 48 bit address represented by 12 hexadecimal digits. The Institute of Electrical and Electronic Engineers (IEEE) controls the allocation of MAC addresses. All NIC manufacturers require IEEE registration - This registration Organisationally Unique Identifier (OUI) is a 24-bit code. The OUI code is the first three Hex pairs in the adapter address, the rest of the MAC address is unique for each of the manufactures' cards. The manufacturer of the Network Interface Card (NIC) can be indentified from the IEEE's Database Search.

TASK 2a

For the windows system use **ipconfig /all** to fill in the following tables:

	Machine A	Machine B
Host Name		
Physical Address		
NIC Manufacturer		
IPv4 Address		
Subnet Mask		
Lease Obtained		
Lease Expires		
Default Gateway Address		
DHCP Server Address		
DNS Servers Addresses		
Primary WINS Server Address		

	Machine A			Machine B		
	Network Class	Network Address	Host Address	Network Class	Network Address	Host Address
IPv4 Address						
Default Gateway Address						
DHCP Server Address						
DNS Servers Addresses						
Primary WINS Server Address						

TASK 2b

From the UNIX system complete the following table:

UNIX COMMAND		Address(es)
netstat -rn	Default Gateway Address	
cat /etc/resolv.conf	DNS Servers Addresses	

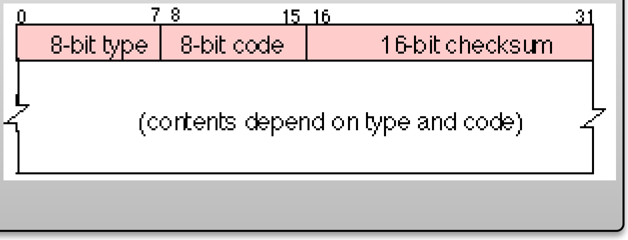
TASK 3

Based on your observations, what can be deduced about the following results taken from three computers connected to one switch? Can the computers communicate to each other? If not why?

	Computer 1	Computer 2	Computer 3
IP Address	192.168.12.113	192.168.12.205	192.168.112.97
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	192.168.12.1	192.168.12.1	192.168.12.1

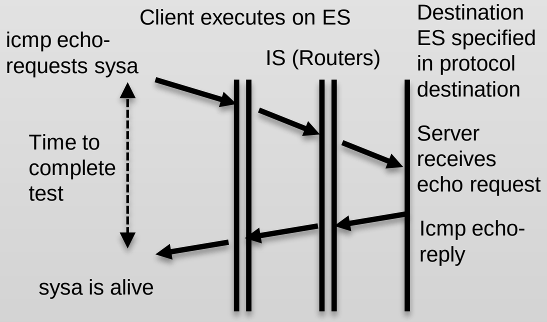
The **Internet Control Message Protocol** (**ICMP**) is one of the protocols of the Internet Protocol (IP) suite**.** It is used to report problems with delivery of IP datagrams within an IP network, such as when a particular End System (ES) is not responding, when a network is not reachable or overloaded, when an error occurs in the IP header information, etc. It is often used by Internet managers to verify correct operation of End Systems and to check that routers are correctly routing packets to the specified destination address. An ICMP message consists of 32 bits of Protocol control Information and an optional message payload:

Type: ICMP type (e.g. type 8 is echo request – ping)
Code: Further qualifies the type; e.g. an ICMP Destination Unreachable might have this field set to 1 through 15, each bearing different meaning.
Checksum - This contains error checking data.
Data - Contains the data specific to the message type indicated by the Type and Code fields.



The "**ping**" program contains a client interface to ICMP. It may be **used by a user to verify that an end-to-end Internet Path is operational** and to collect performance statistics (the measured round trip time and the number of times the remote server fails to reply). Each time an ICMP echo reply message is received, the ping program displays a single line of text with the received sequence number and the measured round trip time (in ms). Each ICMP Echo message contains a sequence number (starting at 0) that is incremented after each transmission, and a timestamp value indicating the transmission time.

The operation of ICMP is illustrated in this frame transition diagram for the case of one Intermediate System (i.e. IP router). In this case two types of message are involved the ECHO request (sent by the client) and the ECHO reply (the server's response). Each message may contain optional data. When data are sent by a server, the server returns the data in the generated reply. ICMP packets are encapsulated in IP for transmission across the internet.



Examples (More ping options on pages 7 and 8):

Windows	ping www.gre.ac.uk	send 4 datagrams of 32 bytes to host www.gre.ac.uk and collect statistics
	ping -n 10 -l 64 www.gre.ac.uk	send 10 datagrams at one per second, each of 64 bytes, to the host www.gre.ac.uk and collect statistics
	ping -t www.gre.ac.uk	send continuous datagrams at one per second, each of 32 bytes, to the host www.gre.ac.uk and collect statistics
UNIX	ping www.gre.ac.uk	send 1 datagram of 56 bytes to host www.gre.ac.uk
	ping -s www.gre.ac.uk 64 10	send 10 datagrams at one per second, each of 64 bytes and collect statistics
	ping -s www.gre.ac.uk	send continuous datagrams at one per second, each of 56 bytes and collect statistics

TASK 4

a) From the Windows and UNIX environments

	Ping from Windows Successful?	Ping from UNIX Successful?
ping the IP address of a Windows computer (IP: ______________________)		
ping the IP address of a UNIX machine (IP: ______________________)		
ping the IP address of the default gateway (IP: ______________________)		
ping the IP addresses of a DNS server (IP: ____)		
ping the Loopback IP address (IP: 127.0.0.1)		
ping the hostname of another computer (hostname: ______________________)		
ping www.cisco.com		
ping www.microsoft.com		

If the Loopback IP ping is successful, then TCP/IP is properly installed and functioning on the PC.

The UNIX hostname of a computer can be found with the **hostname** command

Notice that when pinging microsoft, the DNS server is able to resolve the name to an IP address, but there is no response. Some Microsoft routers are configured to ignore ping requests. This is a frequently implemented security measure.

b) From both Windows and UNIX environments. - send 5 datagrams at one per second, each of 128 bytes to the host www.cisco.com. Fill in the table *(*do not forget the unit of measurement)*:

	Command	Average Delay
Windows		
UNIX		

c) From the UNIX environment, use any suitable host name and send a fixed number of pings, i.e.10 and then double the packet size each time e.g. 250, 500, 1000, 2000, 4000, 8000, 16,000 etc. Use a table to record the time taken and plot a graph (time on the vertical axis, datagram size in Bytes on the horizontal axis) to show the trends.

What is the largest packet size you were able to send? Comment on the results - what you expected, and what actually happened. Comment on how the increase in packet size impacts on the network's performance.

The “**traceroute**" program contains a client interface to ICMP. Like the ping program, it may be used by a user to verify an end-to-end Internet Path is operational, but also provides information on each of the Intermediate Systems (i.e. IP routers) to be found along the IP Path from the sender to the receiver. Traceroute uses ICMP echo messages. These are addressed to the target IP address. The sender manipulates the Time-to-Live (TTL) value at the IP layer to force each hop in turn to return an error message.

It starts by sending an ICMP Echo request message with the IP destination address of the system to be tested and with a TTL value set to 1. The first system that receives this packet decrements the TTL and discards the message, since this now has a value of zero. Before it deletes the message, the system constructs an ICMP error message (with an ICMP message type of "TTL exceeded") and returns this back to the sender. Receipt of this message allows the sender to identify which system is one link away along the path to the destination. The sender repeats this twice more, each time reporting the system that received the packet. If all packets travel along the same path, each ICMP error message will be received from the same system. Where two or more alternate paths are being used, results may vary. If the system that responded was not the intended destination, the sender repeats the process by sending a set of three identical messages, using a TTL value that is one larger than the previous attempt. The first system forwards the packet (decrementing the TTL value in the IP header), but a subsequent system that reduces the TTL value to zero, generates an ICMP error message with its own source address. In this way, the sender learns the identity of another system along the IP path to the destination. This process repeats until the sender receives a response from the intended destination (or the maximum TTL value is reached).

Some Routers are configured to discard ICMP messages, while others process them but do not return ICMP Error Messages. Such routers hide the "topology" of the network but can impact correct operation of protocols. When "traceroute" encounters a router that does not respond, it prints a "*" character.

TASK 5

a) Complete the following table using: (more options on pages 7 and 9)

In Windows: **tracert** *hostname* (or *IP address*)

In Unix: **traceroute -I** *hostname* (or *IP address*)

Domain Name	IP addresses	Host Name	Network Address	Number of Hops - Windows	Number of Hops - UNIX
www.cms.gre.ac.uk					
staffweb.cms.gre.ac.uk					
www.gre.ac.uk					

b) Choose three suitable domains, one from the United States, one from Australia and one from from the far East and complete the following table

Domain Name	IP addresses	Host Name	Network Address	Number of Hops - Windows	Number of Hops - UNIX

The **netstat** command is used to display network protocol statistics and information.

TASK 6

Use netstat with the appropriate parameters. Complete the following table (details on pages 10-11):

Task	Windows Command	UNIX command	Windows	UNIX
Show all active connections			-	-
Show all active TCP connections in numerical form			-	-
Show all active TCP connections with Fully Qualified Domain Names for foreign addresses			-	-
What are the number of IP packets received and sent since boot-up? How many were in error?				
What are the numbers of IP packets sent and received in a typical 10 second interval?				
What are the numbers of TCP segments transmitted and received in a typical 20 second interval? How many retransmissions were there?				
UDP datagrams - what are the numbers transmitted and received in a typical 20 second interval?				
How many ICMP messages were sent and received in a typical 20 second interval?				
List the routing table entries				

*Attach the marking scheme on the front of your document, print it and hand it in at the beginning of the next laboratory. ONE printout to be handed in per team. In addition, **ALL** team members need to individually upload their documents into **week 1.9 (in PDF format)** by midnight the day before their next laboratory. Even for your individual uploads, make sure that the marking scheme has the names of all the members of your team.*

Windows ping options

ping	[-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
-t	Ping 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 (IPv4-only).
-i TTL	Time To Live.
-v TOS	Type Of Service (IPv4-only).
-r count	Record route for count hops (IPv4-only).
-s count	Timestamp for count hops (IPv4-only).
-j host-list	Loose source route along host-list (IPv4-only).
-k host-list	Strict source route along host-list (IPv4-only).
-w timeout	Timeout in milliseconds to wait for each reply.
-R	Use routing header to test reverse route also (IPv6-only).
-S srcaddr	Source address to use.
-4	Force using IPv4.
-6	Force using IPv6.

Windows tracert options

tracert	[-d] [-h maximum_hops] [-j host-list] [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
-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 (IPv4-only).
-w timeout	Wait timeout milliseconds for each reply.
-R	Trace round-trip path (IPv6-only).
-S srcaddr	Source address to use (IPv6-only).
-4	Force using IPv4.
-6	Force using IPv6.

UNIX ping options

ping	[-s] [-l | U] [adLnRrv] [-A addr_family] [-c traffic_class] [-g gateway [-g gateway ...]] [-F flow_label] [-I interval] [-i interface] [-P tos] [-p port] [-t ttl] host [data_size] [npackets][
-A addr_family	Specify the address family of the target host. addr_family can be either inet or inet6. Address family determines which protocol to use. For an argument of inet, IPv4 is used. For inet6, IPv6 is used.
-a	ping all of the addresses, both IPv4 and IPv6, of the multi-homed destination. The output will appear like ping has been run once for each IP address of the destination. If this option is used together with -A, ping probes only the addresses that are of the specified address family. When used with the -s option and count is not specified, ping continuously probes the destination addresses in a round robin fashion. if count is specified, ping will send count number of probes to each IP address of the destination and then exit.
-c traffic_class	Specify the traffic class of probe packets. The value must be an integer in the range from 0 to 255. Gateways along the path may route the probe packet differently depending upon the value of traffic_class set in the probe packet. This option is valid only on IPv6.
-d	Set the SO_DEBUG socket option.
-F flow_label	Specify the flow label of probe packets. The value must be an integer in the range from 0 to 1048575. This option is valid only on IPv6.
-g gateway	Specify a loose source route gateway so that the probe packet goes through the specified host along the path to the target host. The maximum number of gateways is 8 for IPv4 and 127 for IPv6. Note that some factors such as the link MTU can further limit the number of gateways for IPv6.
-i interface_address	Specify the outgoing interface address to use for multicast packets for IPv4 and both multicast and unicast packets for IPv6. The default interface address for multicast packets is determined from the (unicast) routing tables. interface_address can be a literal IP address, for example, 10.123.100.99, or an interface name, for example, le0, or an interface index, for example 2.
-I interval	Turn on the statistics mode and specify the interval between successive transmissions. The default is one second. See the discussion of the -s option.
-l	Use to send the probe packet to the given host and back again using loose source routing. Usually specified with the -R option. If any gate- ways are specified using -g, they are visited twice, both to and from the destination. This option is ignored if the -U option is used.
-L	Turn off loopback of multicast packets. Normally, if there are members in the host group on the outgoing interface, a copy of the multicast pack- ets will be delivered to the local machine.
-n	Show network addresses as numbers. ping normally displays addresses as host names.
-P tos	Set the type of service (tos) in probe packets to the specified value. The default is zero. The value must be an integer in the range from 0 to 255. Gateways also in the path may route the probe packet differently depending upon the value of tos that is set in the probe packet. This option is valid only on IPv4.
-p port	Set the base UDP port number used in probes. This option is used with the -U option. The default base port number is 33434. The ping utility starts setting the destination port number of UDP packets to this base and increments it by one at each probe.
-r	Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has been dropped by the router daemon. See in. routed(1M).
-R	Record route. Sets the IPv4 record route option, which will store the route of the packet inside the IPv4 header. The contents of the record route will only be printed if the -v and -s options are given. They will only be set on return packets if the target host preserves the record route option across echoes, or the -l option is given. This option is valid only on IPv4.
-s	Send one datagram per second and collect statistics
-t ttl	Specify the IPv4 time to live, or IPv6 hop limit, for unicast and multicast packets. The default time to live (hop limit) for unicast packets is set with ndd(1M) using the icmp_def_ttl vari- able. The default time to live (hop limit) for multicast is one hop.
host data_size npackets	host or its IP address. data_size - packet size in bytes (default 56 bytes - i.e. leave blank). npackets - number of times to send the ping request (default will continue indefinitely – Ctrl C to kill).
-U	Send UDP packets instead of ICMP (ICMP6) packets. ping sends UDP pa64 10 ckets to consecutive ports expecting to receive back ICMP (ICMP6) PORT_UNREACHABLE from the target host.
-v	Verbose output. List any ICMP (ICMP6) packets, other than replies from the target host.

UNIX traceroute options

traceroute	[-adFIlnSvx] [-A addr_family] [-c traffic_class] [-f first_hop] [-g gateway [-g gateway ...] | -r] [-i iface] [-L flow_label] [-m max_hop] [-P pause_sec] [-p port] [-Q max_timeout] [-q nqueries] [-s src_addr] [-t tos] [-w wait_time] host [packetlen]
-A addr_family	Specify the address family of the target host. addr_family can be either inet or inet6. Address family determines which protocol to use. For an argument of inet, IPv4 is used. For inet6, IPv6 is used …
-a	Probe all of the addresses of a multi-homed destination. The output looks like traceroute has been run once for each IP address of the destination. If this option is used together with -A, traceroute probes only the addresses that are of the specified address family.
-c traffic_class	Specify the traffic class of probe packets. The value must be an integer in the range from 0 to 255. Gateways along the path may route the probe packet differently depending upon the value of traffic_class set in the probe packet. This option is valid only on IPv6.
-d	Set the SO_DEBUG socket option.
-F	Set the "don't fragment" bit. This option is valid only on IPv4.
-f first_hop	Set the starting ttl (hop limit) value to first_hop, to override the default value 1. traceroute skips processing for those intermediate gateways which are less than first_hop hops away.
-g gateway	Specify a loose source route gateway. The user can specify more than one gateway by using -g for each gateway. The maximum number of gateways is 8 for IPv4 and 127 for IPv6. Note that some factors such as the link MTU can further limit the number of gateways for IPv6. It cannot be used with the -r option.
-I	Use ICMP (ICMP6) ECHO instead of UDP datagrams.
-i iface	For IPv4, this option specifies a network inter- face to obtain the source IP address. This is normally only useful on a multi-homed host. The -s option is also another way to do this. For IPv6, it specifies the network interface on which probe packets are transmitted. The argument can be either an interface index, for example, 1, 2, or an interface name, for example, le0, hme0.
-L flow_label	Specify the flow label of probe packets. Integer from 0 to 1048575. This option is valid only on IPv6.
-l	Print the value of the ttl (hop limit) field in each packet received.
-m max_hop	Set the maximum ttl (hop limit) used in outgoing probe packets. The default is 30 hops, which is the same default used for TCP connections.
-n	Print hop addresses numerically rather than sym- bolically and numerically. This saves a nameserver address-to-name lookup for each gate- way found on the path.
-P pause_sec	Specify a delay, in seconds, to pause between probe packets. This may be necessary if the final destination does not accept undeliverable packets in bursts. By default, traceroute sends the next probe as soon as it has received a reply. Note that pause_sec is a real number.
-p port	Set the base UDP port number used in probes (default is 33434). traceroute hopes that nothing is listening on UDP ports (base+(nhops- 1)*nqueries) to (base+(nhops*nqueries)-1)at the destination host, so that an ICMP (ICMP6) PORT_UNREACHABLE message will be returned to terminate the route tracing. If something is listening on a port in the default range, this option can be used to select an unused port range. nhops is defined as the number of hops between source and destination.
-Q max_timeout	Stop probing this hop after max_timeout consecu- tive timeouts are detected. The default value is 5. Useful in combination with the -q option if you have specified a large nqueries probe count.
-q nqueries	Set the desired number of probe queries. The default is 3.
-r	Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to send probes to a local host through an inter- face that has been dropped by the router deamon. You cannot use –r if -g is used.
-s src_addr	Use the following address, usuallly given as a literal IP address, not a hostname, as the source address in outgoing probe packets. … If it is not one of this machine's interface addresses, an error is returned. For IPv4, when used together with -i, the given address should be configured on the specified interface or an error will be returned. For IPv6, the interface name and the source address do not have to match.
-t tos	Set the tos(type-of-service) in probe packets to the specified value. The default is zero. The value must be an integer in the range from 0 to 255. Gateways along the path may route the probe packet differently depending upon the tos value set in the probe packet. This option is valid only on IPv4.
-v	Verbose output. For each hop, the size and the destination of the response packets is displayed. Also ICMP (ICMP6) packets received other than TIME_EXCEEDED and UNREACHABLE are listed as well.
-w waittime	Set the time, in seconds, to wait for a response to a probe. The default is 5 seconds.
-x	Prevent traceroute from calculating checksums…

Windows netstat options

netstat with no arguments displays the following statistics for active TCP/UDP connections:

-Proto: - The name of the protocol (TCP or UDP).

-Local Address: - The IP address of the local computer and the port number being used. If the port is not yet established, the port number is shown as an asterisk (*).

-Foreign Address: - The names and port number of the remote computer to which the socket is connected. If the port is not yet established, the port number is shown as an asterisk (*).

-State: - Indicates the state of a TCP connection – for info about the states of a TCP connection, see RFC 793

- LISTEN - represents waiting for a connection request from any remote TCP and port.
- SYN-SENT - represents waiting for a matching connection request after having sent a connection request.
- SYN-RECEIVED - represents waiting for a confirming connection request acknowledgment after having both received and sent a connection request.
- ESTABLISHED - represents an open connection, data received can be delivered to the user. The normal state for the data transfer phase of the connection.
- FIN-WAIT-1 - represents waiting for a connection termination request from the remote TCP, or an acknowledgment of the connection termination request previously sent.
- FIN-WAIT-2 - represents waiting for a connection termination request from the remote TCP.
- CLOSE-WAIT - represents waiting for a connection termination request from the local user.
- CLOSING - represents waiting for a connection termination request acknowledgment from the remote TCP.
- LAST-ACK - represents waiting for an acknowledgment of the connection termination request previously sent to the remote TCP (which includes an acknowledgment of its connection termination request).
- TIME-WAIT - represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request.
- CLOSED - represents no connection state at all.

netstat	[-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]
	Description
/?	Displays help on netstat
-a	Displays all connections and listening ports
-b	Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.
-e	Displays Ethernet statistics. This may be combined with the -s option.
-f	Displays Fully Qualified Domain Names for foreign addresses
-n	Displays addresses and port numbers in numerical form
-o	Displays the owning process ID associated with each connection
-p proto	Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, protocol may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-r	Displays the routing table
-s	Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
-v	When used in conjunction with -b, will display sequence of components involved in creating the connection or listening port for all executables
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

UNIX netstat options

netstat with no arguments displays a list of active sockets for the protocols IPv4, IPv6, UNIX Domain Sockets

netstat	netstat [-anv] [-f address_family] netstat [-n] [-f address_family] [-P protocol] [-g | -m | -p | -s [interval [count]]] netstat -m [-v] [interval [count]] netstat -i [-I interface] [-an] [-f address_family] [interval [count]] netstat -r [-anv] [-f address_family|filter] netstat -M [-ns] [-f address_family] netstat -D [-I interface] [-f address_family]
-a	Show the state of all sockets, all routing table entries, or all interfaces, both physical and logical. Normally, listener sockets used by server processes are not shown. Under most conditions, only interface, host, network, and default routes are shown and only the status of physical interfaces is shown.
-f address _family	Limit all displays to those of the specified address_family. The value of address_family can be one of the following: inet For the AF_INET address family showing IPv4 information. inet6 For the AF_INET6 address family showing IPv6 information. unix For the AF_UNIX address family.
-g	Show the multicast group memberships for all interfaces. If the -v option is included, source-specific membership information is also displayed.
-i	Show the state of the interfaces that are used for IP traffic. Normally this shows statistics for the physical interfaces. When combined with the -a option, this will also report information for the logical interfaces.
-m	Show the STREAMS memory statistics.
-n	Show network addresses as numbers. netstat normally displays addresses as symbols. This option may be used with any of the display formats.
-p	Show the address resolution (ARP) tables.
-r	Show the routing tables. Normally, only interface, host, network, and default routes are shown, but when this option is combined with -a, all routes will be displayed, including cache.
-s	Show per-protocol statistics. When used with the -M option, show multicast routing statistics instead. When used with the -a option, per-interface statistics will be displayed, when available, in addition to statistics global to the system.
-v	Verbose. Show additional information for the sockets, STREAMS memory statistics, routing table, and multicast group memberships.
-I	Show the state of a particular interface. interface can be any valid interface such as hme0 or eri0. Normally, the status and statistics for physical interfaces are displayed. When this option is combined with the -a option, information for the logical interfaces is also reported.
-M	Show the multicast routing tables. When used with the -s option, show multicast routing statistics instead.
-P	Limit display of statistics or state of all sockets to those applicable to protocol. The protocol can be one of ip, ipv6, icmp, icmpv6, icmp, icmpv6, igmp, udp, tcp, rawip. rawip can also be specified as raw. The command accepts protocol options only as all lowercase.
-D	Show the status of Dynamic Host Configuration Protocol (DHCP) configured interfaces.
-R	This modifier displays extended security attributes for sockets and routing table entries. With -r only, this option displays the routing entries' gateway security attributes.
interval	Display statistics accumulated since last display every interval seconds, repeating forever, unless count is specified. When invoked with interval, the first row of netstat output shows statistics accumulated since last reboot. The following options support interval: -i, -m, -s and -Ms. Some values are configuration parameters and are just redisplayed at each interval.
count	Display interface statistics the number of times specified by count at the interval specified by interval