

PRACTICAL-2

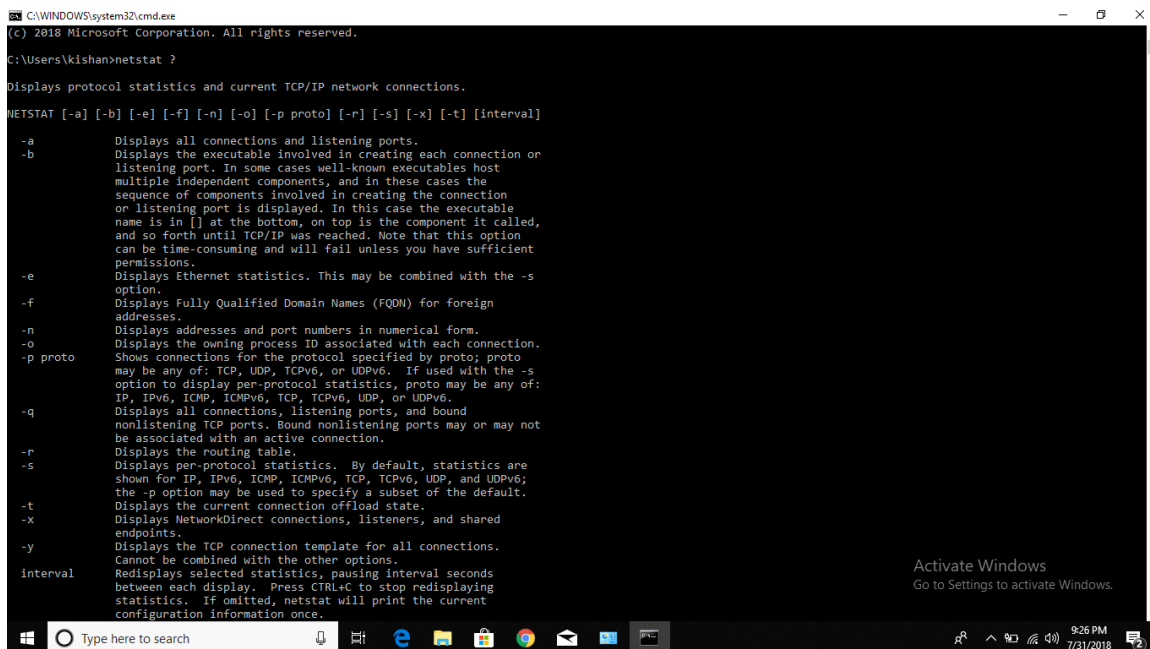
AIM-TCP/UDP connectivity using Netstat

Task 1: Explain common netstat command parameters and outputs.

-Open a terminal window by clicking on Start | Run. Type cmd, and press OK.

-To display help information about the netstat command, use the /? options, as shown:

C:\> netstat /? <ENTER>



```
CA\WINDOWS\system32\cmd.exe
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\kishan>netstat ?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

-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 (FQDN) 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, ICMPv6, or UDPv6. If used with the -s
           option to display per-protocol statistics, proto may be any of:
           IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-q          Displays all connections, listening ports, and bound
           nonlistening TCP ports. Bound nonlistening ports may or may not
           be associated with an active connection.
-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.
-t          Displays the current connection offload state.
-x          Displays NetworkDirect connections, listeners, and shared
           endpoints.
-y          Displays the TCP connection template for all connections.
           Cannot be combined with the other options.
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.
```

Step : Use netstat to view existing connections.

From the terminal window in Task 1, above, issue the command netstat -a:

C:\> netstat -a <ENTER>

```
C:\Windows\system32\cmd.exe

C:\>netstat -o

Active Connections
  Proto Local Address           Foreign Address         State       PID
C:\>netstat -n

Active Connections
  Proto Local Address           Foreign Address         State
C:\>netstat -a

Active Connections
  Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              ITME2T3:0              LISTENING
TCP    0.0.0.0:445              ITME2T3:0              LISTENING
TCP    0.0.0.0:1025             ITME2T3:0              LISTENING
TCP    0.0.0.0:1026             ITME2T3:0              LISTENING
TCP    0.0.0.0:1027             ITME2T3:0              LISTENING
TCP    0.0.0.0:1028             ITME2T3:0              LISTENING
TCP    0.0.0.0:1029             ITME2T3:0              LISTENING
TCP    0.0.0.0:1030             ITME2T3:0              LISTENING
TCP    0.0.0.0:3389             ITME2T3:0              LISTENING
TCP    169.254.102.166:139      ITME2T3:0              LISTENING
TCP    [::]:135                 ITME2T3:0              LISTENING
TCP    [::]:445                 ITME2T3:0              LISTENING
TCP    [::]:1025                ITME2T3:0              LISTENING
TCP    [::]:1026                ITME2T3:0              LISTENING
TCP    [::]:1027                ITME2T3:0              LISTENING
TCP    [::]:1028                ITME2T3:0              LISTENING
TCP    [::]:1029                ITME2T3:0              LISTENING
TCP    [::]:1030                ITME2T3:0              LISTENING
TCP    [::]:3389                ITME2T3:0              LISTENING
TCP    [::]:1031                ITME2T3:0              LISTENING
```

```
C:\Windows\system32\cmd.exe

C:\>netstat -a

Active Connections
  Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              ITME2T3:0              LISTENING
TCP    0.0.0.0:445              ITME2T3:0              LISTENING
TCP    0.0.0.0:1025             ITME2T3:0              LISTENING
TCP    0.0.0.0:1026             ITME2T3:0              LISTENING
TCP    0.0.0.0:1027             ITME2T3:0              LISTENING
TCP    0.0.0.0:1028             ITME2T3:0              LISTENING
TCP    0.0.0.0:1029             ITME2T3:0              LISTENING
TCP    0.0.0.0:1030             ITME2T3:0              LISTENING
TCP    0.0.0.0:3389             ITME2T3:0              LISTENING
TCP    169.254.102.166:139      ITME2T3:0              LISTENING
TCP    [::]:135                 ITME2T3:0              LISTENING
TCP    [::]:445                 ITME2T3:0              LISTENING
TCP    [::]:1025                ITME2T3:0              LISTENING
TCP    [::]:1026                ITME2T3:0              LISTENING
TCP    [::]:1027                ITME2T3:0              LISTENING
TCP    [::]:1028                ITME2T3:0              LISTENING
TCP    [::]:1029                ITME2T3:0              LISTENING
TCP    [::]:1030                ITME2T3:0              LISTENING
TCP    [::]:3389                ITME2T3:0              LISTENING
TCP    [::]:1031                ITME2T3:0              LISTENING
UDP    0.0.0.0:500              **
UDP    0.0.0.0:3389             **
UDP    0.0.0.0:4500             **
UDP    0.0.0.0:5355             **
UDP    127.0.0.1:1900           **
UDP    127.0.0.1:61819          **
UDP    169.254.102.166:137      **
UDP    169.254.102.166:138      **
UDP    169.254.102.166:1900     **
UDP    169.254.102.166:61818    **
UDP    [::]:500                  **
UDP    [::]:3389                 **
UDP    [::]:4500                 **
```

C:\> netstat -b <ENTER>

```
C:\Windows\system32\cmd.exe

UDP 0.0.0.0:3389 *:*
UDP 0.0.0.0:4500 *:*
UDP 0.0.0.0:5355 *:*
UDP 127.0.0.1:1900 *:*
UDP 127.0.0.1:61819 *:*
UDP 169.254.102.166:137 *:*
UDP 169.254.102.166:138 *:*
UDP 169.254.102.166:1900 *:*
UDP 169.254.102.166:61818 *:*
UDP [::]:500 *:*
UDP [::]:3389 *:*
UDP [::]:4500 *:*
UDP [::]:5355 *:*
UDP [::]:1900 *:*
UDP [::]:61817 *:*
UDP [fe80::59b:d0df:a065:66a6%7]:1900 *:*
UDP [fe80::59b:d0df:a065:66a6%7]:61816 *:*

C:\>netstat -b
The requested operation requires elevation.

C:\>netstat -e
Interface Statistics

              Received              Sent
Bytes                0                0
Unicast packets      0                0
Non-unicast packets  0                0
Discards             0                0
Errors               0                0
Unknown protocols    0

C:\>
```

C:\> netstat -e <ENTER>

C:\> netstat -f<ENTER>

```
C:\Windows\system32\cmd.exe

C:\>netstat -b
The requested operation requires elevation.

C:\>netstat -e
Interface Statistics

              Received              Sent
Bytes                0                0
Unicast packets      0                0
Non-unicast packets  0                0
Discards             0                0
Errors               0                0
Unknown protocols    0

C:\>netstat -f
Active Connections

Proto Local Address          Foreign Address         State
C:\>
```

```
C:\Windows\system32\cmd.exe

C:\>netstat -s

IPv4 Statistics

Packets Received                = 0
Received Header Errors          = 0
Received Address Errors         = 0
Datagrams Forwarded             = 0
Unknown Protocols Received      = 0
Received Packets Discarded      = 194
Received Packets Delivered      = 2903
Output Requests                 = 1501
Routing Discards                = 0
Discarded Output Packets        = 0
Output Packet No Route          = 11
Reassembly Required             = 0
Reassembly Successful           = 0
Reassembly Failures             = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created               = 0

IPv6 Statistics

Packets Received                = 0
Received Header Errors          = 0
Received Address Errors         = 0
Datagrams Forwarded             = 0
Unknown Protocols Received      = 0
Received Packets Discarded      = 304
Received Packets Delivered      = 124
Output Requests                 = 2098
Routing Discards                = 0
Discarded Output Packets        = 0
Output Packet No Route          = 19
Reassembly Required             = 0
Reassembly Successful           = 0
```

```
C:\Windows\system32\cmd.exe

C:\>netstat -r

=====
Interface List
7...02 00 4c 4f 50 .....Ncap Loopback Adapter
1...00 00 00 00 00 00 .....Software Loopback Interface 1
4...00 00 00 00 00 00 .....Microsoft ISATAP Adapter
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        306
127.255.255.255           255.255.255.255 On-link         127.0.0.1        306
169.254.0.0                255.255.0.0      On-link         169.254.102.166  266
169.254.102.166           255.255.255.255 On-link         169.254.102.166  266
169.254.255.255           255.255.255.255 On-link         169.254.102.166  266
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link         169.254.102.166  266
255.255.255.255           255.255.255.255 On-link         127.0.0.1        306
255.255.255.255           255.255.255.255 On-link         169.254.102.166  266
=====
Persistent Routes:
Network Address            Netmask          Gateway Address  Metric
0.0.0.0                    0.0.0.0          100.81.81.3      Default
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination Gateway
1 306 ::1/128 On-link
7 266 fe80::/64 On-link
7 266 fe80::59b:d0df:a065:66a6/128 On-link
1 306 ff00::/8 On-link
7 266 ff00::/8 On-link
```

```
C:\Windows\system32\cmd.exe

Fragments Created          = 0

IPv6 Statistics
Packets Received           = 0
Received Header Errors     = 0
Received Address Errors    = 0
Datagrams Forwarded        = 0
Unknown Protocols Received = 0
Received Packets Discarded = 304
Received Packets Delivered = 124
Output Requests            = 2098
Routing Discards           = 0
Discarded Output Packets   = 0
Output Packet No Route     = 19
Reassembly Required        = 0
Reassembly Successful      = 0
Reassembly Failures        = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created          = 0

ICMPv4 Statistics
Received Sent
Messages      0      0
Errors        0      0
Destination Unreachable 0      0
Time Exceeded 0      0
Parameter Problems 0      0
Source Quenches 0      0
Redirects      0      0
Echo Replies   0      0
Echos         0      0
Timestamps     0      0
Timestamp Replies 0      0
Address Masks  0      0
Address Mask Replies 0      0
```

```
C:\Windows\system32\cmd.exe

Received Sent
Messages      0      25
Errors        0      0
Destination Unreachable 0      0
Packet Too Big 0      0
Time Exceeded 0      0
Parameter Problems 0      0
Echos         0      0
Echo Replies   0      0
MLD Queries    0      0
MLD Reports    0      0
MLD Dones     0      0
Router Solicitations 0      15
Router Advertisements 0      0
Neighbor Solicitations 0      5
Neighbor Advertisements 0      5
Redirects      0      0
Router Renumberings 0      0

ICMPv6 Statistics
Received Sent
Messages      0      25
Errors        0      0
Destination Unreachable 0      0
Packet Too Big 0      0
Time Exceeded 0      0
Parameter Problems 0      0
Echos         0      0
Echo Replies   0      0
MLD Queries    0      0
MLD Reports    0      0
MLD Dones     0      0
Router Solicitations 0      15
Router Advertisements 0      0
Neighbor Solicitations 0      5
Neighbor Advertisements 0      5
Redirects      0      0
Router Renumberings 0      0
```

```
C:\Windows\system32\cmd.exe

Router Renumberings      0      0

TCP Statistics for IPv4
    Active Opens          = 0
    Passive Opens         = 0
    Failed Connection Attempts = 20
    Reset Connections     = 0
    Current Connections    = 0
    Segments Received     = 0
    Segments Sent         = 0
    Segments Retransmitted = 0

TCP Statistics for IPv6
    Active Opens          = 1
    Passive Opens         = 1
    Failed Connection Attempts = 0
    Reset Connections     = 2
    Current Connections    = 0
    Segments Received     = 33770
    Segments Sent         = 33716
    Segments Retransmitted = 56

UDP Statistics for IPv4
    Datagrams Received    = 777
    No Ports              = 673
    Receive Errors        = 0
    Datagrams Sent        = 1263

UDP Statistics for IPv6
    Datagrams Received    = 124
    No Ports              = 304
    Receive Errors        = 0
    Datagrams Sent        = 586
```

```
C:\Windows\system32\cmd.exe

Current Connections      = 0
Segments Received        = 0
Segments Sent            = 0
Segments Retransmitted   = 0

TCP Statistics for IPv6
    Active Opens          = 1
    Passive Opens         = 1
    Failed Connection Attempts = 0
    Reset Connections     = 2
    Current Connections    = 0
    Segments Received     = 33770
    Segments Sent         = 33716
    Segments Retransmitted = 56

UDP Statistics for IPv4
    Datagrams Received    = 777
    No Ports              = 673
    Receive Errors        = 0
    Datagrams Sent        = 1263

UDP Statistics for IPv6
    Datagrams Received    = 124
    No Ports              = 304
    Receive Errors        = 0
    Datagrams Sent        = 586

C:\>netstat -t

Active Connections

Proto Local Address          Foreign Address         State       Offload State
-----
C:\>
```

```
C:\Windows\system32\cmd.exe

Failed Connection Attempts      = 0
Reset Connections              = 2
Current Connections            = 0
Segments Received              = 33770
Segments Sent                  = 33716
Segments Retransmitted         = 56

UDP Statistics for IPv4

Datagrams Received            = 777
No Ports                     = 673
Receive Errors                = 0
Datagrams Sent                = 1263

UDP Statistics for IPv6

Datagrams Received            = 124
No Ports                     = 304
Receive Errors                = 0
Datagrams Sent                = 586

C:\>netstat -t

Active Connections

Proto Local Address          Foreign Address         State       Offload State

C:\>netstat -x

C:\>netstat -y

Active Connections

Proto Local Address          Foreign Address         State       Template

C:\>
```

```
C:\Windows\system32\cmd.exe

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

-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 (FQDN) 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, proto 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.
-t      Displays the current connection offload state.
-x      Displays NetworkDirect connections, listeners, and shared
        endpoints.
-y      Displays the TCP connection template for all connections.
        Cannot be combined with the other options.
interval Redispays 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.
```