Lab : Observing TCP and UDP using Netstat and Examing Route

Learning Objectives

- Explain common **netstat** command parameters and outputs.
- Use **netstat** to examine protocol information on a pod host computer.
- Use the **route** command to examine a Windows computer routing table.

Background

netstat is an abbreviation for the network statistics utility, available on both Windows and Unix / Linux computers. Passing optional parameters with the command will change output information. **netstat** displays incoming and outgoing network connections (TCP and UDP), host computer routing table information, and interface statistics.

For packets to travel across a network, a device must know the route to the destination network. This lab will compare how routes are used in Windows computers. Some routes are added to routing tables automatically, based upon configuration information on the network interface. The device considers a network directly connected when it has an IP address and network mask configured, and the network route is automatically entered into the routing table. For networks that are not directly connected, a default gateway IP address is configured that will send traffic to a device that should know about the network.

Scenario

In this lab the student will examine the **netstat** command on a pod host computer, and adjust **netstat** output options to analyze and understand TCP/IP Transport Layer protocol status.

Using a pod host computer, examine the routing table with the **route** command and identify the different routes and gateway IP address for the route. Delete the default gateway route, test the connection, and then add the default gateway route back to the host table.

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>
```

Use the output of the **netstat** /? command as reference to fill in the appropriate option that best matches the description:

Option	Description
	Display all connections and listening ports.
	Display addresses and port numbers in numerical form.
	Redisplay statistics every five seconds. Press CTRL+C to stop redisplaying statistics.
	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.
	Redisplay all connections and listening ports every 30 seconds.
	Display only open connections. This is a tricky problem.

When **netstat** statistics are displayed for TCP connections, the TCP state is displayed. During the life of a TCP connection, the connection passes through a series of states. The following table is a summary of TCP states, compiled from RFC 793, Transmission Control Protocol, September, 1981, as reported by **netstat**:

State	Connection Description
LISTEN	The local connection is waiting for a connection request from any remote device.
ESTABLISHED	The connection is open, and data may be exchanged through the connection. This is the normal state for the data transfer phase of the connection.
TIME-WAIT	The local connection is waiting a default period of time after sending a connection termination request before closing the connection. This is a normal condition, and will normally last between 30 - 120 seconds.
CLOSE-WAIT	The connection is closed, but is waiting for a termination request from the local user.
SYN-SENT	The local connection is waiting for a response after sending a connection request. The connection should transition quickly through this state.
SYN_RECEIVED	The local connection is waiting for a confirming connection request acknowledgment. The connection should transition quickly through this state. Multiple connections in SYN_RECEIVED state may indicate a TCP SYN attack.

IP addresses displayed by **netstat** fall into several categories:

IP Address	Description
127.0.0.1	This address refers to the local host, or this computer.
0.0.0.0	A global address, meaning "ANY".
Remote Address	The address of the remote device that has a connection with this computer.

Task 2: Use `netstat` to Examine Protocol Information on a Pod Host Computer.

Use `netstat` to view existing connections. From the terminal window in Task 1,

above, issue the command **`netstat –a`**:

```
C:\> netstat –a <ENTER>
```

A table will be displayed that lists protocol (TCP and UDP), Local address, Foreign address, and State information. Addresses and protocols that can be translated into names are displayed.

The `–n` option forces netstat to display output in raw format. From the terminal window, issue the command **`netstat –an`**:

```
C:\>netstat–an
```

Use the window vertical scroll bar to go back and forth between the outputs of the two commands. Compare outputs, noting how well-known port numbers are changed to names. Write down three TCP and three UDP connections from the **`netstat –a`** output, and the corresponding translated port numbers from the **`netstat –an`** output. If there are fewer than three connections that translate, note that in your table.

Connection	Proto Local Address	Foreign Address	State

Important information about protocols and ports:

- DNS- domain name server, port 53
- FTP- FTP server, port 21
- SMTP- SMTP mail server, port 25
- TELNET-Telnet server, port 23

Use the `route` Command to Modify a Windows Computer Routing Table.

```
C:\>netstat –r

Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x20005 ...00 16 76 ac a7 6a Intel(R) 82562V 10/100 Network Connection
===========================================================================
===========================================================================

Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0  172.16.255.254    172.16.1.2     1
        127.0.0.0        255.0.0.0        127.0.0.1     127.0.0.1     1
      172.16.0.0      255.255.0.0        172.16.1.2    172.16.1.2    20
      172.16.1.2  255.255.255.255        127.0.0.1     127.0.0.1    20
172.16.255.255  255.255.255.255        172.16.1.2    172.16.1.2    20
255.255.255.255  255.255.255.255        172.16.1.2    172.16.1.2     1
Default Gateway:        172.16.255.254
===========================================================================
Persistent Routes:
None
C:\>
```

Figure 1. Output of the `netstat` Command

Shown in Figure 1, output from the **netstat –r** command is useful to determine route and gateway information.

Examine the active routes on a Windows computer.

A useful command to modify the routing table is the **route** command. Unlike the **netstat –r** command, the **route** command can be used to view, add, delete, or change routing table entries. To view detailed information about the **route command,** use the option **route /?**.

An abbreviated option list for the **route** command is shown below: To view active routes, issue the command **route PRINT**:

route PRINT	Prints active routes
route ADD	Adds a route: route ADD *network* MASK mask *gateway*
route DELETE	Deletes a route: route DELETE *network*
route CHANGE	Modifies an existing route

```
C:\ >route PRINT
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x70003 ...00 16 76 ac a7 6a .Intel(R) 82562V 10/100 Network Connection
===========================================================================
===========================================================================

Active Routes:
      Network Destination  Netmask          Gateway       Interface   Metric
              0.0.0.0            0.0.0.0 172.16.255.254   172.16.1.2       1
            127.0.0.0          255.0.0.0    127.0.0.1      127.0.0.1       1
           172.16.0.0    255.255.0.0      172.16.1.2     172.16.1.2      20
           172.16.1.2  255.255.255.255     127.0.0.1      127.0.0.1      20
       172.16.255.255  255.255.255.255     172.16.1.2     172.16.1.2      20
      255.255.255.255  255.255.255.255     172.16.1.2     172.16.1.2       1
     Default Gateway:    172.16.255.254

===================================
```

Persistent Routes:
None
C:\>

Delete a route from the Windows computer routing table.

How important is the default gateway route? Delete the gateway route, and try to ping www.hh.se. The syntax to remove the default gateway route is:

route DELETE *network*

```
C:/> route DELETE 0.0.0.0
```

Examine the active routing table and verify that the default gateway route has been removed: What is the default gateway IP address?

Examine the active routing table and verify that the default gateway route has been removed: What is the default gateway IP address?

Try to ping www.hh.se. What are the results?

If the default gateway IP address is removed, how can the DNS server be reached to resolve www.hh.se ?

Can other computer on LAN be reached?

Insert a route into the Windows computer routing table.

In the following configuration, use the IP address assigned to your host pod interface. The syntax to add a route to the Windows computer routing table is:

route ADD *network* **MASK** *mask gateway-IP address*

C:/> **route ADD 0.0.0.0 MASK 0.0.0.0 172.16.255.**254

Examine the active routing table, and verify that the default gateway route has been restored:
Has the default gateway route been restored? _____

C:\ >**route PRINT**

Try to ping www.hh.se. What are the results?