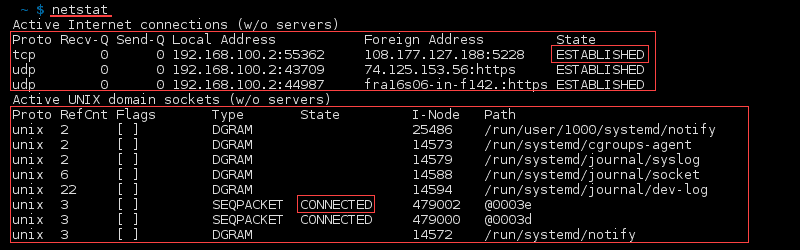
The **netstat** command is a CLI tool for **net**work **stat**istics. It gives an overview of network activities and displays which ports are open or have established connections. The netstat tool is essential for discovering network problems.

The primary usage of **netstat** is without any parameters:

netstat



The first list in the output displays active established internet connections on the computer. The following details are in the columns:

* **Proto**– Protocol of the connection (*TCP*, *UDP*).
* **Recv-Q** – Receive queue  of bytes received or ready to be received.
* **Send-Q** – Send queue of bytes ready to be sent.
* **Local address***–*Address details and port of the local connection. An asterisk (\*) in the host indicates that the server is listening and if a port is not yet established.
* **Foreign address**– Address details and port of the remote end of the connection. An asterisk (\*) appears if a port is not yet established.
* **State***–*State of the local socket, most commonly *ESTABLISHED,* *LISTENING, CLOSED*or blank*.*

The second list shows all the active “*Unix Domain*” open sockets with the following details:

* **Proto**– Protocol used by the socket (always *unix*).
* **RefCnt**– Reference count of the number of attached processes to this socket.
* **Flags** – Usually *ACC* or blank.
* **Type** – The socket type.
* **State** – State of the socket, most often *CONNECTED, LISTENING* or blank.
* **I-Node** – File system inode (index node) associated with this socket.
* **Path**– System path to the socket.

**Different States**

*Due to the way TCP/IP works, connections can not be closed immediately. Packets may arrive out of order or be retransmitted after the connection has been closed.*

***CLOSE\_WAIT****indicates that the remote endpoint (other side of the connection) has closed the connection.*

***TIME\_WAIT****indicates that local endpoint (this side) has closed the connection. The connection is being kept around so that any delayed packets can be matched to the connection and handled appropriately. The connections will be removed when they time out within four minutes.*

|  |  |
| --- | --- |
| **ESTABLISHED** | The socket has an established connection. |
| **SYN\_SENT** | The socket is actively attempting to establish a connection. |
| **SYN\_RECV** | A connection request has been received from the network. |
| **FIN\_WAIT1** | The socket is closed, and the connection is shutting down. |
| **FIN\_WAIT2** | Connection is closed, and the socket is waiting for a shutdown from the remote end. |
| **TIME\_WAIT** | The socket is waiting after close to handle packets still in the network. |
| **CLOSE** | The socket is not being used. |
| **CLOSE\_WAIT** | The remote end has shut down, waiting for the socket to close. |
| **LAST\_ACK** | The remote end has shut down, and the socket is closed. Waiting  for acknowledgement |
| **LISTEN** | The socket is listening for incoming connections. Such sockets are not included in the output unless you specify the  --listening (-l) or --all (-a) option. |
| **CLOSING** | Both sockets are shut down but we still don't have all our data sent. |
| **UNKNOWN** | The state of the socket is unknown. |

[1] Linux Commands Refernce: <https://www.tecmint.com/find-out-which-process-listening-on-a-particular-port/>