TCP Dumps

About TCP Dumps

CPS administrators can use the **tcpdump** Linux command in the command line to intercept and display TCP/IP packets, as well as others, as they are being transmitted or received.

With the **tcpdump** command, you can analyze network behavior, performance, and applications that generate or receive network traffic.

While not specific to CPS, the following examples of **tcpdump** are frequently helpful for troubleshooting CPS network packets.

Note Starting the heapdump on policy director (LB) will have an impact on performance.

TCPDUMP Command

```
tcpdump -i any -s 0 port XXXX
```

where, XXXX is the port number you are interested in.

Options

To Specify Multiple Ports

To capture more than one port:

```
tcpdump -i any -s 0 port 1812 or 1813
```

To capture a port range:

```
tcpdump -i any -s 0 portrange 1812-1817
```

Combining both techniques:

```
tcpdump -i any -s 0 portrange 1812-1817 or port 1700
```

Verbose Mode

```
tcpdump -i any -s 0 -v port XXXX
```

Even more Verbose Mode

```
tcpdump -i any -s 0 -vv port XXXX
```

Restrict to a Specific Interface, such as eth0

```
tcpdump -i eth0 -s 0 port XXXX
```

Redirect Output of the Command to a File

```
tcpdump -i any -s 0 port 1812 -w output.pcap
```

The resulting `output.pcap` file can be opened and utilized using such tools as WireShark.

More options

From a UNIX/Linux prompt, type **man tcpdump**.

Specific Traffic Types

Note These examples assume that the default ports have not been changed or have been specified in Cisco Policy Builder. One must modify these examples to use the appropriate ports that have been specified in Cisco Policy Builder if the default/typical values have been changed.

Capture SNMP Traffic

```
tcpdump -i any -s 0 port 1161 or 1162 or 161 or 162
```

Note This command works for both the sending and receiving machine; the port just needs to match the source or destination port.

Other Ports

The following information is the information format:

Host/VM name Port "Service/traffic type"

where XX is the numeric value of the given host, i.e. pcrfclient01.

pcrfclientXX 80 "Subversion"

pcrfclientXX 7070 "Policy Builder"

sessionmgrXX 27717 "Session Database"

sessionmgrXX 27718 "Quota/Balance Database"

sessionmgrXX 27719 "Reporting Database"

sessionmgrXX 27720 "USuM Database"

lbvipXX 80 "Subversion vip external"

lbvipXX 8080 "QNS/Unified API VIP"

lbvipXX 11211 "Memcache vip internal"

lbvipXX 7070 "Policy Builder VIP"

qnsXX 9091 "QNS admin port"