**Indication:** Traffic/communication issue on a specific port.

**Problem:** Firewall could be blocking port.

First step is to verify the port information is shown (using CLI or GUI) and that its status is correct. Information about IPTables (firewall) could be obtained through following ways:-

*GUI*

```
Cisco Unified OS Administration
 Show->IP Preferences
```

*CLI*

```
show network ipprefs
 show network ipprefs all
 show network ipprefs enabled
 show network ipprefs public
```

Next, verify the port is shown in the firewall rules. Use the CLI command ?utils firewall list?. Note, if the port is not shown in the list it is being blocked. You can verify ports are being blocked by the firewall by turning on the debug mode in the firewall. Use the CLI command ?utils firewall debug?. This will cause iptables to log every packet it blocks.

There are logs that detail when changes to the firewall or changes to the port information occur:

syslog/messages ? iptables log

syslog/secure ? will show changes to port information (such as when a port is enabled/disabled).

Note, the syslog logs are available via RTMT. Same can also be obtained via CLI, following are the commands:-

```
file get activelog syslog/messages
file get activelog syslog/secure
```

Note, we throttle the log messages going into the log. So, if there are lots of packets getting blocked, we might not log all instances. Example from syslog messages log:

```
Aug  4 10:32:23 bldr-ccm23 kern 4 kernel: dropped packet IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:0f:
Aug  4 10:32:25 bldr-ccm23 kern 4 kernel: dropped packet IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:0e:
```

As a last resort you can temporarily disable the firewall by using the CLI command ?utils firewall disable?. Note, both the disable and debug mode of the firewall will automatically revert back after a default of 5 minutes. This time can be extended to a maximum of 24 hours.