OM10K Port Monitor Setup

With port speeds up to 10Gbps, the OM10K is a powerful tool for network monitoring.

This document covers the following:

- Configuring the Aggregator - output port which carries the data from the monitored ports
- Configuring the Monitored – input ports which are being monitored
- Ensuring no data can leak from the Aggregator port into a Monitored port.

Relevant Application Notes:

These following application notes are available in the *DOWNLOADS* sections of:
www.luxcom.com/product/om10k-8/ and www.luxcom.com/product/om10k-24/

App.1 OM10K Management Interface Access.pdf gives instructions on accessing the OM10K management interface.

App.2 OM10K LUA CLI Overview.pdf gives an overview of the CLI (Command Line Interface) command structure, and *how to modify the configuration files so the desired CLI commands are executed at startup*.

App.4 OM10K VLAN Setup.pdf gives examples of setting up Port and Tag based VLANs using CLI commands.

Relevant CLI Commands:

interface ethernet device/port defines the port which is being configured.

switchport isolate command defines a list of ports which will be isolated from ingress traffic on the given port. It must be used with a single port, not a range of ports. All traffic received on a port is dropped if the port is isolated from all destination ports. This is useful for blocking packets received on a port being used for monitoring (span port).

switchport protected command overrides the filtering database (FDB). This sends all traffic received on a port to an uplink port. Note that packets sent to other ports are still subject to the FDB.

port monitor command mirrors a ports ingress or egress data to another port. “rx” mirrors ingress packets, “tx” mirrors egress packets, and “both” mirrors both ingress and egress packets. Up to 7 analyzer ports can be configured. Any port can be monitored.

Aggregate a group of monitor ports into one data stream.

- .
- Do not allow any data from any other OM10K ports to egress Port 0-2 and Port 8.

```
configure
// Configure Aggregated monitor output Port8
interface ethernet 0/8             -- Note[1]
switchport isolate all             -- Note[2]
exit
// Configure Monitored Port 0 to forward all packets to port 8
interface ethernet 0/0             -- Ingress port 0
switchport isolate 0/0-7,0/9-27   -- Note [3]
switchport protected ethernet 0/8 -- Note [4]
exit
// Configure Monitored Port 1 to forward all packets to port 8
interface ethernet 0/1             -- Ingress port 1
switchport isolate 0/0-7,0/9-27
switchport protected ethernet 0/8
exit
// Configure Monitored Port 2 to forward all packets to port 8
interface ethernet 0/2             -- Ingress port 2
switchport isolate 0/0-7,0/9-27
switchport protected ethernet 0/8
exit
// Isolate other ports on the switch from communicating with Ports 0,1,2,8
// This will allow the other ports to act as a normal switch.
interface ethernet 0/3             -- Port 3
switchport isolate 0/0-2,0/8
exit
interface ethernet 0/4             -- Port 4
switchport isolate 0/0-2,0/8
exit
// Repeat these above three lines for all other ports. Note [5]
end
```

The port isolation status can be displayed using the “show interfaces switchport isolate” command:

```
Console# show interfaces switchport isolate
Dev  Port   LocalPorts(isolated)    CpuPort(isolated)
---  -----  --------------------    -----------------
0    0      0-7,9-27                   false
0    1      0-7,9-27                   false
0    2      0-7,9-27                   false
0    8      0-27                       false
0    3      0-2,8                      false
0    4      0-2,8                      false
```

As can be seen, all ports except port 8 are isolated on the ports being aggregated.

Any port can be used for the uplink and multiple uplink ports could be configured.

Set up a monitor port to listen to ingress or egress data on specific ports.

Example:

- This setup allows the OM10K to switch packets normally to their destination and at the same time to monitor the throughput.
- Set up SFP Port 8 to monitor output.
- Do not allow any ingress data to Port 8 to leak into Ports 0-2.
- Set up Port 0 to monitor the ingress data
- Set up Port 1 to monitor the egress data
- Set up Port 2 to monitor the ingress and egress data

```
configure
interface ethernet 0/8                    -- Note[1]
switchport isolate all                    -- Note[2]
// Mirror received packets on port 0
port monitor 0/0 rx
// Mirror transmitted packets on port 1
port monitor 0/1 tx
// Mirror both transmitted and received packets on port 2
port monitor 0/2 both
end
```

Notes:

[1] 0/8 = *device/port* The *device* is always 0. *Port* numbers are labeled beside the RJ45 or SFP.

[2] Prevents packets which ingress port 8 from egressing any other port.

[3] Prevent packets which ingress port 0 from egressing any other port except 8.

[4] Send *all* packets (disables MAC table filtering) which enter port 0 to port 8.

[5] If these ports are not isolated, received broadcast packets will egress ports 0,1,2,8.