

Best Practices Guide



Monitoring access devices such as the Net Optics Director Data Monitoring Switch provide the capability to intelligently filter traffic to prevent tools from becoming oversubscribed and enable them to focus only on traffic of interest. This guide has recommendations of best practices for using intelligent filtering.

Examples are given in Director CLI syntax.

Share Tools Across Many Links

- Let any attached tool monitor any network link by copying all of the traffic from a network port to a monitor port; do this by creating a filter with no filter elements.

This filter copies all traffic from Network Port 1 to Monitor Port 7:

```
filter add in_ports=n1.1 action=redir redir_ports=m.7
```

Operate More Efficiently

- Use tools more efficiently by aggregating traffic from multiple low-utilization network links; do this by specifying multiple network ports in the in_ports portlist.

This filter aggregates traffic from four network ports.

```
filter add in_ports=n1.1-n1.3,n2.6 action=redir redir_ports=m.4
```

- Enable multiple tools or groups to monitor the same information simultaneously, without conflict, by regenerating traffic to multiple monitoring tools; do this by specifying multiple monitor ports in the redir_ports portlist.

This filter regenerates traffic to three monitor ports.

```
filter add in_ports=n1.3 action=redir redir_ports=m.4-m.6
```

Prevent Tool Overload

- Prevent monitoring tools from becoming oversubscribed and enable them to focus only on traffic of interest by pre-filtering the traffic sent to the tools. Filter by the following packet header information:
 - o Layer 4 IP protocol (ip_protocol)
 - o IPv4 source and destination IP addresses (ip4_src, ip4_dst)
 - o IPv6 source and destination IP addresses (ip6_src, ip6_dst)
 - o Layer 4 source and destination port addresses (l4_src_port, l4_dst_port)
 - o Source and destination MAC addresses (mac_src, mac_dst)
 - o VLAN number (vlan)

Best Practices Guide

Masks are supported (by appending “_mask” to the parameter name) to create ranges for all parameters except ip_protocol.

- Create complex filters that logically AND filter criteria by including multiple criteria in the filter.

This filter selects packets that have a particular protocol (HTTP) AND IP address:

```
filter add ip_protocol=80 ip4_src=10.10.1.0
```

- Create complex filters that logically OR filter criteria by specifying multiple filters with the same in_ports and redir_ports portlists.

This set of filters selects packets that have protocols of TCP OR UDP:

```
filter add in_ports=n1.8 action=redir redir_ports=m.2 ip_protocol=6  
filter add in_ports=n1.8 action=redir redir_ports=m.2 ip_protocol=17
```

- Create contiguous ranges of IP addresses, MAC addresses, and ports by using masks.

This filter covers the address range 10.10.1.0 to 10.10.1.15:

```
filter add ip4_src=10.10.1.0 ip4_src_mask=255.255.255.240
```

- Select non-contiguous sets of IP addresses, MAC addresses, and ports by creating parallel filters.

This set of filters redirects traffic from three non-contiguous IP addresses:

```
filter add in_ports=n1.1 action=redir redir_ports=m.5 ip4_src=10.10.1.0  
filter add in_ports=n1.1 action=redir redir_ports=m.5 ip4_src=10.10.1.5  
filter add in_ports=n1.1 action=redir redir_ports=m.5 ip4_src=10.10.1.120
```

Exclude Unwanted Traffic

- Monitor all traffic except for packets meeting the filter criteria by creating exclusive filters; do this by dropping unwanted traffic.

This set of filters copies all of the traffic that is NOT UDP protocol:

```
filter in_ports=n1.11 action=drop add ip_protocol=17  
filter in_ports=n1.11 action=redir redir_ports=m.6
```

Mix 1 Gigabit and 10 Gigabit Equipment

- Use 1 Gigabit monitoring tools on 10 Gigabit network links by filtering the traffic from a 10 Gigabit network port to multiple 1 Gigabit monitor ports.

This set of filters distributes all of the traffic from a 10 Gigabit port to four 1 Gigabit monitor ports by filtering on protocol:

```
filter add in_ports=t1.1 action=redir redir_ports=m.1 ip_protocol=6  
filter add in_ports=t1.1 action=redir redir_ports=m.2 ip_protocol=17  
filter add in_ports=t1.1 action=redir redir_ports=m.3 ip_protocol=1  
filter add in_ports=t1.1 action=redir redir_ports=m.4
```

Best Practices Guide

This set of filters distributes all of the traffic from a 10 Gigabit port to five 1 Gigabit monitor ports based on IP addresses of subnets that are known to be active on the 10 Gigabit link:

```
filter add in_ports=t1.2 ip4_src=10.10.1.0 ip4_src_mask=255.255.255.0 action=redir  
redir_ports=m.6
```

```
filter add in_ports=t1.2 ip4_dst=10.10.1.0 ip4_dst_mask=255.255.255.0 action=redir  
redir_ports=m.6
```

```
filter add in_ports=t1.2 ip4_src=10.10.2.0 ip4_src_mask=255.255.255.0 action=redir  
redir_ports=m.7
```

```
filter add in_ports=t1.2 ip4_dst=10.10.2.0 ip4_dst_mask=255.255.255.0 action=redir  
redir_ports=m.7
```

```
filter add in_ports=t1.2 ip4_src=10.10.3.0 ip4_src_mask=255.255.255.0 action=redir  
redir_ports=m.8
```

```
filter add in_ports=t1.2 ip4_dst=10.10.3.0 ip4_dst_mask=255.255.255.0 action=redir  
redir_ports=m.8
```

```
filter add in_ports=t1.2 ip4_src=10.10.4.0 ip4_src_mask=255.255.255.0 action=redir  
redir_ports=m.9
```

```
filter add in_ports=t1.2 ip4_dst=10.10.4.0 ip4_dst_mask=255.255.255.0 action=redir  
redir_ports=m.9
```

```
filter add in_ports=t1.2 action=redir redir_ports=m.10
```

- Use 10 Gigabit monitoring tools to efficiently monitor multiple 1 Gigabit links by aggregation.

This filter aggregates ten 1 Gigabit ports to a single 10 Gigabit monitoring tool:

```
filter add in_ports=n2.1-n2.10 action=redir redir_ports=t2.2
```

Intelligent filtering within access devices presents many opportunities to operate more efficiently, prevent tool overload, and increase the ROI of investments in expensive monitoring tools. This new technology is rapidly becoming a required feature of the Monitoring Access Platform (MAP) as its value becomes more and more apparent in real-world applications. Apply the best practices presented here and start reaping the benefits of intelligent filtering in your monitoring environment today.

For further information:

<http://www.netoptics.com>

Net Optics, Inc.

5303 Betsy Ross Drive

Santa Clara, CA 95054

(408) 737-7777

info@netoptics.com

Customer First!