Multi Stage Filtering

With the increasing traffic volume in modern data centers, largely driven by e-Business and mobile devices, network and application performance monitoring has become more and more challenging. All indications point to a continually increasing data load for the foreseeable future, making “Big Data” a key challenge for every network.

In addition, security monitoring with tools such as IDS, IPS and Malware Detection is now a critical function within every company, whether that company does business online or not. Security concerns add to the complexity of providing a scalable network monitoring architecture because it’s no longer enough to monitor for performance – now you’re monitoring Big Data for critical content.

As data volumes increase beyond the ability of tools to examine every packet, effective packet filtering at the network monitoring switch becomes a bottleneck – you can’t look at everything, and you can’t afford to drop crucial packets. In this environment, traditional ingress and egress packet filtering may fall short in certain aspects. A more intelligent filtering system is needed to address Big Data and the increasing number and variety of monitoring tools.

Challenges from Traditional Filtering
A short review of traditional packet filtering allows a better understanding of the rationale for Multi Stage Filtering. Each mode of filtering provides certain features and bears certain shortcomings that are solved through APCON’s Multi Stage Filtering environment.

Ingress Filters
Ingress filters either allow (pass) or deny (drop) traffic on ingress ports. If a pass filter is applied to an ingress port, all traffic specified in the filter is sent to the egress on all configured connections. This type of filter is adequate when all the tools need to receive the same type of traffic. However, if tools are expecting different types of traffic, an ingress filter will not be flexible enough to support those different needs. In general, only one filter can be tied to an ingress port. If the data flowing into an ingress port is multicast to several ports for use by different tools, the same ingress filter is applied to all these different connections.
On the other hand, if a drop filter is applied to an ingress port, the various tools sharing this ingress port will not receive dropped traffic even if some of these tools need to see that traffic.

For these reasons, ingress filters are suitable only for monitoring scenarios of limited variation and well-defined scope. In reality, ingress filtering is rarely used, especially with the increasing number of tools that monitor different types of network traffic flowing from the same data source.

**Egress Filters**

Egress filters allow only specific traffic to be sent to the tool connected to the egress port. Egress filtering is more granular and flexible than ingress filtering. However, oversubscription and dropped packets can occur in some of the following scenarios:

- Traffic aggregated from multiple ingress ports causing oversubscription and wholesale packet drops before packets can be filtered
- Traffic from high bandwidth 10G or 40G ingress ports being sent to low bandwidth 1G ports, exhausting the buffer and dropping packets
- Ingress traffic being replicated and multicast to all egress ports before filtering, which can overload the switching capacity, resulting in potential packet drops

To be used effectively, monitoring tools require pinpoint accuracy, and each tool needs to receive a complete set of accurate traffic; nothing more and definitely nothing less. To achieve this granular division of traffic, a new and more sophisticated way of filtering is needed. The goal is to ensure that all monitoring tools receive the data they are expecting in an environment of ever-increasing data volume and monitoring complexity.

**Multi Stage Filtering**

APCON Multi Stage Filtering (MSF) provides a more adaptable and precise method of specifying exactly which packets from an ingress stream should be transmitted to each egress port. This allows exact processing of aggregated or high capacity 10G and 40G streams for use with 1G monitoring tools.

APCON’s Multi Stage Filtering solution supports up to 3 stages of filtering through a Filter Stack. The Filter Stack makes use of your existing filter library and links selected filters together to provide more configurable filter programming. The “building block” filters that engineers have previously created and stored in their filter library are based on a Boolean logic combination of different rules. Each rule provides the ability to filter on over 35 predefined Layer 2, Layer 3 and Layer 4 parameters including IPv4/IPv6 addresses, application TCP or UDP port numbers, VLAN IDs, MAC addresses, and more.

In addition, users can filter on the actual physical ingress port of the APCON switch as well as by custom offset in the packet header and payload for DPI.

The Filter Stack allows you to prioritize filtering on the ingress port. Filters in the Filter Stack are processed from top to bottom in the order defined. The first filter in the stack examines all the traffic. The next filter in the stack sees only what is passed by the first filter, and so on.

Filter Stack results may be mapped directly to destination egress ports, or to egress filters and then to the destination egress ports, or to a different Filter Stack at the next stage of the Multi Stage Filter. There is a new built-in filter called the Default Channel, and this catches all the remaining packets at the bottom of a Filter Stack. If the Default Channel is not defined, all remaining packets in the stack will be discarded.
Example of using Filter Stack on Stage 1 only

Example of using multiple Filter Stacks on all 3 Stages
Benefits of Multi Stage Filtering
APCON’s Multi Stage Filtering solution provides diverse benefits, depending on how the filter stacks are used. Many of the benefits fall into the following categories:

Intelligent Traffic Distribution
APCON Multi Stage Filtering can filter incoming packets on aggregated connections, customizing the output sent to each egress port. This can optimize the tool performance as each tool now sees only the traffic that it is expecting and nothing else. Multi Stage Filtering greatly enhances tool performance and also maximizes effective throughput.

Performance Enhancement
Multi Stage Filtering is efficient because it saves packet replication overhead compared to simple egress filtering. This reduces data throughput requirements across the switch backplane and at the egress ports. If multiple tools need to see the same data, Multi Stage Filtering can replicate any needed traffic to any number of tools. The result is that switch backplane resources will be much more efficiently utilized and dropped packets minimized or eliminated.

Bandwidth Control
Because Multi Stage Filtering forwards only required traffic to each egress port, oversubscription resulting in dropped packets at egress ports can be managed. With effective filtering, even a connection from a high bandwidth 10G or 40G ingress port to a low bandwidth 1G egress port can be managed effectively. Similarly, an aggregated connection from multiple ingress ports, or a combination of aggregation and high bandwidth ingress ports can be managed. As long as the actual required traffic is less than the egress port rate, full data flow can be guaranteed.

Ease of Use
APCON’s Multi Stage Filters are configured and viewed using APCON’s fourth-generation graphical interface, making filter construction and implementation easy and accurate. Existing APCON filter libraries may be repurposed for Multi Stage use from the switch management software.

Feature Integration
In addition to the intelligent traffic distribution capabilities, Multi Stage Filtering can be used with the native Port Tagging and Load Balancing features that are included with every INTELLAFLEX blade. This can further enhance the analysis function and the traffic load management capabilities of APCON INTELLAFLEX technology. Additionally, Multi Stage Filtering may be combined with APCON’s advanced services blades such as Time Stamping, Packet Slicing, Packet Deduplication and INTELLASTORE®.
Multi Stage Filtering Usage Examples
Here are several specific use cases in which Multi Stage Filtering helps with intelligent traffic distribution and eliminating dropped packets.

- Aggregate total inputs of 16G traffic. 600M are SIP traffic and 15.4G are non-SIP traffic.
- Multi Stage Filter of SIP traffic forwards the 600M of SIP to the 1G voice monitoring tool on Output Port1 with no drops.
- Multi Stage Filter for Output 2 selects 8 Gbps of non-SIP traffic of interest to be analyzed by the 10G data monitoring tools.

- Total input of 3 Gbps traffic.
- Applying egress filters on individual output ports might experience packet drops as oversubscription might occur before the egress filters.
- Multi Stage Filtering will pass all appropriate traffic to the output ports accordingly without any drops.
Conclusion

With the increasing “big data” traffic volume stressing networks of all sizes, network and application performance monitoring have become more and more challenging. In addition, security monitoring such as IDS, IPS and Malware Detection has become a critical path item for every company.

Traditional ingress and egress filtering falls short of modern efficiency requirements. However, APCON’s industry-first Multi Stage Filtering provides 100% network visibility by delivering the right data to the right monitoring tools without packet loss. With all three stages of the Multi Stage Filtering configured, this technology meets your most complex and rigorous monitoring requirements and delivers the next generation of intelligent network monitoring.

Multi Stage Filtering is just one of APCON’s answers to the growing challenge of providing scalable, highly available, and state-of-the-art network monitoring architecture at an affordable price. By eliminating waste in switch, port, and tool bandwidth, your existing investment in monitoring tools can last longer and serve you more effectively.