Regional Financial Services Firm Switches to APCON for Packet Deduplication Technology

Case Study

A $59 billion regional bank holding company in the U.S. Midwest needed to provide increased visibility of production traffic flows to a variety of monitoring and security systems at two separate data centers. Network monitoring functions in place include Application Performance Monitoring, Network Performance Monitoring, Intrusion Detection and Intrusion Prevention appliances. Specific tools in use include Vantage Real User Monitoring, NetScout, Data Loss Prevention, Intrusion Detection, NetWitness, FireEye and others. The bank chose APCON to meet its needs for a scalable system that could effectively deduplicate its traffic.

- **Scalability**
  This bank's existing solution was not scalable to meet new growth requirements.
- **Deduplication**
  Duplicate packets challenged total visibility by wasting resources and hindering session-based analysis.
- **APCON Solution**
  APCON IntellaFlex technology provided the scalability and line-rate deduplication required to meet this bank's needs.

The company's existing network monitoring system consisted of a limited number of network taps feeding a network monitoring switch manufactured by an APCON competitor. This system provided limited visibility and was not scalable, and thus could not address regular microbursts in network traffic. The system also generated substantial duplicate packets that the competing switch could not eliminate, thus creating challenges in monitoring and adding to overall tool costs.

When the company was faced with a network expansion, their existing network monitoring switch simply couldn't keep up. The project required installation of 64 new network taps and 16 new port SPANs adding a tremendous amount of data to the flows going to the monitoring systems. The old switch lacked the capacity to expand.

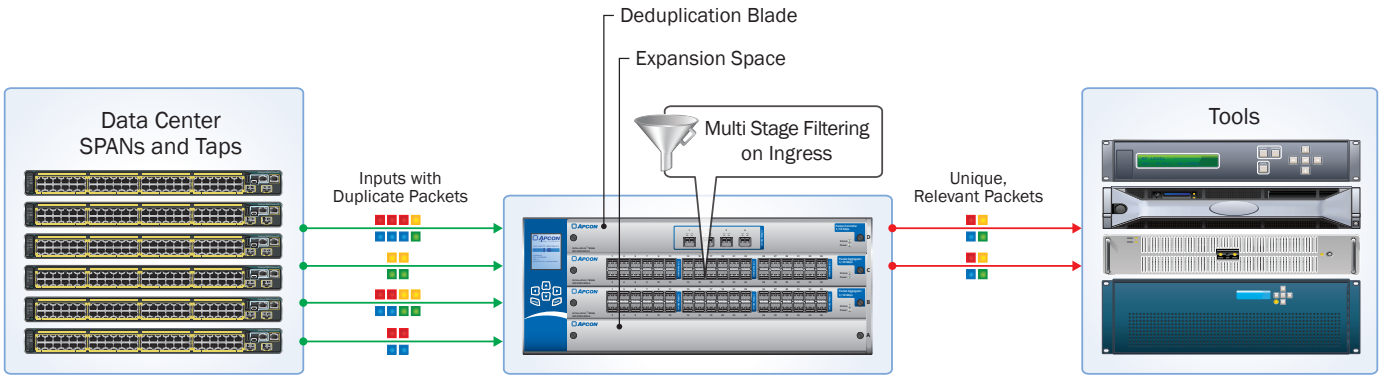
The company began a search for a chassis-based solution that offered greater port density, high availability, system scalability, and the technology to deduplicate traffic, all with an easy-to-use graphical interface.

The Technical Challenge of Deduplication

Any network monitoring system that approaches total network visibility must deal with duplicate packets. Simply put, if your network is tapped in multiple locations and uses SPAN or Mirror ports to retransmit some or all production traffic to the monitoring system, your network monitoring switch will receive multiple copies of the same packet as it traverses your network. In some cases, up to 55% of traffic received at the network monitoring switch may be duplicate packets.

Duplicate packets cause several problems if the network monitoring switch is not able to eliminate the copies. The first and most pervasive issue is that tools such as network data recorders become loaded with duplicates, reducing their effective lookback time window. Over time, this load of duplicate packets results in unnecessary purchases of expensive redundant tools.

Also, session-based appliances such as the Application and Network Performance Monitoring tools in use at this company cannot reconstruct sessions accurately when presented with duplicate packets. The errors are introduced because the tools can no longer recreate and review the user's interaction reliably if multiple copies of the same interaction are arriving at the tool.



To adequately serve APM/NPM tools and to maximize the efficiency of network data recorders and other time-based tools, duplicate packets must be identified and eliminated from the data stream. In a modern financial data center, this must happen in real time at the full line rate of the network. An ultrafast low-latency network monitoring switch with advanced intelligent network monitoring technology is required.

APCON's IntellaFlex Packet Controller meets these needs, with the widest time window available on the market. When duplicate packets are generated, they typically arrive at about the same moment at the network monitoring switch. With the IntellaFlex Packet Controller, network engineers can examine each packet as it traverses the switch, and any packet deemed identical (based on a configurable set of tests) that arrives within a configurable time window up to ½-second will be discarded. Half a second is a very long time in the working life of a production data center network, and this feature will effectively deduplicate almost any network traffic.

APCON Delivers Results

This bank looked at every competing switch on the market, and chose the APCON IntellaFlex solution for its capacity, scalability and new technology in the realm of filtering and packet deduplication. They purchased several APCON IntellaPatch XE four-blade switches, and then populated each switch with one APCON IntellaFlex Packet Controller blade for deduplication services, and two 36-port configurable IntellaFlex 1G/10G port blades.

A single blade slot in each switch was left available for future growth, but even if the bank grows beyond these chassis, APCON IntellaFlex blades are transferable into the larger eight-blade chassis, preserving the bank's investment in blades. APCON offers true scalability, protecting existing installations from the need for forklift replacements.

The APCON solution provided the port density to accommodate all of the tap and SPAN/Mirror data inputs currently required for total network visibility, with the technology to examine each packet and eliminate duplicates at full 10G line rate. Data streams that arrive on any port may be directed through the deduplication engines on the Packet Controller blade and then out to the monitoring tools.

Additionally, all APCON switches offer a convenient web-accessible graphical user interface that includes the ability to perform complex Multi Stage Filtering in real time. Multi Stage Filtering is a new development, and represents a major technological advancement in Ethernet packet filtering by creating the ability to program the monitoring system, where only simple pass/drop filters were available before. This unique capability makes the intelligent network monitoring switch more efficient, and reduces oversubscription and wasted tool resources.

As each packet enters the switch, it is subject to a cascading "stack" of filters. Each filter may pass matching traffic to additional filters, to an output port, or both. In this way, traffic from a variety of sources can be sorted and directed to the correct tools, maximizing efficiency and eliminating dropped packets from the monitoring system. Multi Stage Filtering allows efficient distribution of packets in real time to a variety of tools, even when using a legacy 1G tool to monitor a 10G link or an aggregation of several 1G links.

APCON delivered the new switches in early 2014, allowing this bank to stay on top of its network monitoring needs with full network visibility, a clean stream of data to its tools, and scalability to grow into the future.

APCON, Inc. ▪ apcon.com ▪ +1 503-682-4050 ▪ 800-624-6808