cpacket NETWORKS

Use Case: Using De-duplication counters to identify architecture flaws and faulty network equipment

Business Goals

- Early problem identification and proactive maintenance to reduce total costs
- Reduce troubleshooting time and costs with more network visibility
- Efficiently manage the network while

cPacket's Benefits

- Complete visibility at all speeds and feeds
- Accurate Packet broker counters such as de-duplication counters on every port
- 'Single pane of glass' access to all cPacket sensors
- Integrate with external devices using RESTful APIs for integration and automation

> "ACCORDING TO IHS, **DOWNTIME** IS COSTING NORTH AMERICAN ORGANIZATIONS **$700 BILLION PER YEAR.** THIS DOWNTIME RANGES FROM **$1 MILLION** A YEAR FOR A TYPICAL MID-SIZE COMPANY TO **$60 MILLION** A YEAR FOR A LARGE ENTERPRISE."

A fully functional packet broker with capabilities to run all features simultaneously at all speeds and feeds is an absolute necessity for network visibility, monitoring and troubleshooting. According to IHS, downtime is costing North American organizations $700 billion per year. This downtime ranges from $1 million a year for a typical mid-size company to $60 million a year for a large enterprise. NetOps/SecOps engineers require advanced monitoring tools to help them proactively identify issues that may cause downtime. One significant broker feature is de-duplication. It is valuable for troubleshooting as well as identifying failing or misconfigured equipment.

De-duplication is the ability to detect and eliminate duplicates of a packet to reduce the amount of network traffic sent to downstream tools. This allows for a more efficient method of managing the network, so tools can operate at their peak performance.

This use case will explain how to use de-duplication for troubleshooting and network monitoring.

Visibility is key to efficient maintenance and troubleshooting. Having a complete visible monitoring architecture allows NetOps to quickly access any part of the network for efficient troubleshooting. Among the many packet broker features available, de-duplication is one feature that can be leveraged for troubleshooting. The following describes how this can be accomplished.

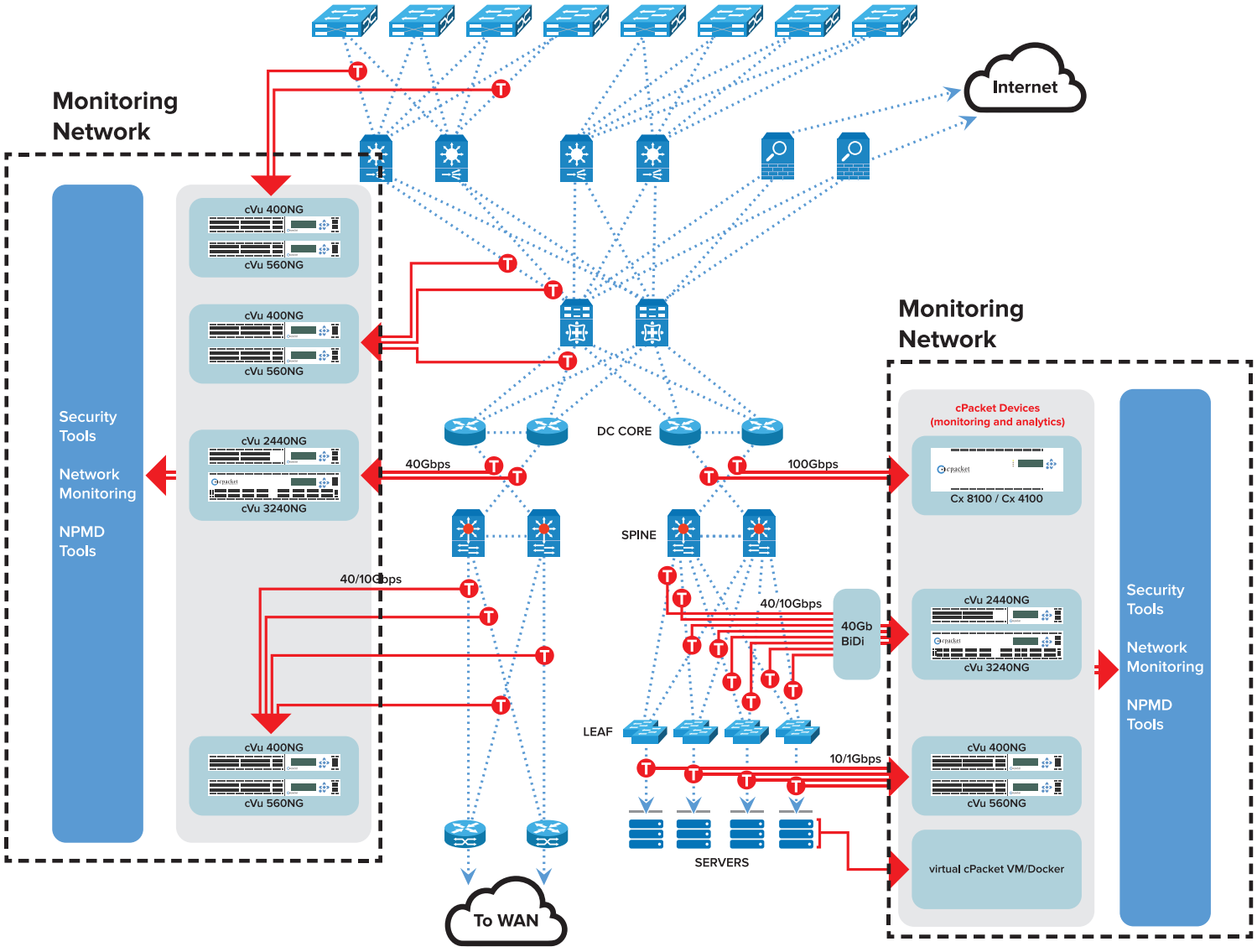

Figure 1: Network topology with a packet broker architecture

Figure 1 above shows the two different networks that exist in an organization. The production network runs the business. It consists of routers, switches, and firewalls that are actively moving packets in and out of the network. Production network traffic is fed to a monitoring network via SPANs and TAPs to packet brokers, which then feed the network traffic to specialty tools for monitoring and security. The purpose of a monitoring network is to observe the production network for performance, SLA, security and troubleshoot issues in the production network.

In the figure above, the cVu network sensors (1G-100G speed per port) are the gateways to the monitoring network. They are the packet brokers that support many critical network performance monitoring (NPM) features such as TCP health metrics, predictive analytics and protocol identification, in addition to packet broker functions such as slicing, header stripping and dynamic truncation.

De-duplication is the ability to detect and eliminate duplicates of a packet and allowing only a single packet (generally, the first packet) to proceed through the monitoring network.

Network infrastructure devices, such as switches and routers that are operating normally do not generate many duplicate packets. However, in certain situation, duplicate packets can be seen in some segments of the network due to poor network design or a flaw in the network-topology. Also, misconfigured or potentially failing equipment can generate bursts of duplicate packets or malformed packets. To identify and rectify these situations, de-duplication can be very useful.

On cPacket's cVu devices, de-duplication counters are available per port. These counters are very useful in identifying the above situations. Whenever there is a burst of duplicate packets or malformed packets, the cVu's de-duplication and CRC counters identify these errors and automatically generate system alerts that are sent to cClear. Figure 2 below shows the de-duplication counters for Port 01 on a cVu 3240. Counter value of 0 implies there were no duplicate packets identified on that port.

cpacket: Port 1: Port_01 - current

Name	Current: (bps)	(pps)	CRC Errors	Framing Errors	
Receive	772,729,696	1,420,459	0	0	
Transmit	---	---	---	---	
Dropped	0	0	---	---	
Lost/Over-subscribed	---	0	---	---	
Deduplicated	0	0	---	---	
inputBuffering Dropped	---	0	---	---	

Figure 2: De-duplication counters help identify faulty equipment and network topology issues

In addition to looking at the de-duplication counters, the 'CRC Errors' column in the Figure 2 shows the count of packets with CRC errors. If a port (and hence that segment in the network) received malformed packets, they would be flagged for CRC errors and the counter would increment.

To effectively troubleshoot a network, NetOps/SecOps have several options. First, engineers can capture packets on the port using the quick capture capability on the cVu device itself for analysis in tools such as Wireshark. Second, for long-term packet capture and analysis, cStor devices can be added which enable long term storage and analysis. A third option is to use cSearch, which can be used to search the network for specific patterns as well as testing and verifying network level configurations.

Benefits

Choosing the right network architecture with a focus on monitoring and troubleshooting provides rich dividends strategically and tactically in terms of reduced troubleshooting costs. SecOps and NetOps can leverage the many features and functionalities to increase network transparency and visibility. In addition to packet broker features such as de-duplication and packet slicing, cPacket's solution provides comprehensive network and NPM related metrics that the downstream tools can use to provide more intelligent insights. This will lead to better decision making, verifying network configurations more efficiently and improved network operations resulting in reduced MTTR and greater uptime.

Unlock the Advantages with cPacket

cPacket's solutions offer unprecedented performance, deeper levels of insight, and real-time analytics to solve the most complex network challenges faced in today's enterprises. cPacket's advanced distributed intelligence enables network operators to proactively detect problems before they negatively impact end-users using predictive analytics. cPacket provides a unique algorithmic chip that delivers complete packet inspection immediately at the wire for accurate results.

cPacket Networks is committed to achieving quality standards in network performance monitoring and is trusted by network operators worldwide.