

Flexible NetFlow:

Building on NetFlow Version 9

Prosperon Networks - Tel: 08458331185 - www.prosperon.co.uk - sales@prosperon.co.uk

NetFlow, a technology invented by Cisco, has become the simplest way learn who, what, when and where traffic was created on the network. Prior to NetFlow, SNMP was used to learn what connections were congested and packet analyzers were deployed to investigate the source of the volume. NetFlow has not replaced these technologies; rather, it is doing to network management what television did to radio. Although NetFlow still doesn't look beyond summarized IP traffic, with Flexible NetFlow the lines may become a bit more blurry between NetFlow analyzers and packet analyzers, or even Intrusion Detection Systems.

Flexible NetFlow relies on NetFlow version 9

Flexible NetFlow wouldn't be possible without version 9 of NetFlow. Flexible NetFlow allows the creation of multiple separate Flow Monitors to run simultaneously for security or traffic analysis. Specifically, it allows administrators to create Flow Monitors which focus on collecting traffic formats from layer 2 to layer 7 with deep packet inspection for application monitoring. In short, it has the ability to launch a separate, deeper flow monitor while a traditional flow monitor is transmitting to a collector. Although it supports version 5 and IPFIX, Flexible NetFlow must leverage NetFlow version 9, if the administrator wants to track up to the first 1200 bytes of the IP packet, which in many cases is the entire packet. The maximum frame size in Ethernet is 1500 bytes.

In most cases, it wouldn't make sense to capture the first 1200 bytes of all packets, as this would defeat the purpose of NetFlow's inherently clever summarization architecture. However, it may make sense to set a threshold that triggers a brief Flow Monitor. The Flow Monitor could, in turn, create an "Immediate" NetFlow cache on the router to capture and export the first 1200 bytes of each of the culprit's packets for several seconds. These captures are called Flow Records. A feature like this would allow administrators to gather information deeper into packets for security analysis without interrupting the archiving of summarized data for historical baselines. Loaded with the actual packets, problems such as Denial of Service (DoS) and worm attacks can be thoroughly investigated and more accurately diagnosed.

Three Types of NetFlow Caches

Normal Cache is used in traditional NetFlow, and generally for basic traffic analysis and base lining.

Permanent Cache is a fixed size, chosen by the administrator. Once the cache is full, the overflow is dropped. Exports can be configured to periodically send records to a collector. Typically, it is used to track traffic between specific end points.

Immediate Cache is used when every individual packet needs to create a new flow. Generally, it is used when capturing large portions of the original packet is necessary.

More on Exporting

Flow Records are exported from the Flow Cache when they reach the default inactive state of 15 seconds.

As long as the Flow Record is updated with new data within 15 seconds, it will last up to 30 minutes before the active flow timer expires and the record is sent off to a collector. Flexible NetFlow prefers to send records off in a NetFlow v9 packet, which can contain up to 24 other unique Flow Records.

A NetFlow version 5 packet could contain up to 30 Flow Records. Nevertheless, both the inactive and active timers are configurable. By and large, for NetFlow traffic analysis, the active timer is changed from 30 minutes to 1 minute. If the active timer isn't changed to 1 minute, the collector will likely report spikes well over 100% utilization in the 1 minute interval trends.

Flow Exporters

A Flow Exporter is actually responsible for sending the Flow Records off to the collector in a NetFlow version 9 frame (RFC 3954). The number of Flow Exporters is only dependent on the resources available on the switch or router. From a single router, NetFlow can now be sent to more than two unique destinations.

The Flow Exporter can also send optional data, such as tables of interface ifIndex to interface name mappings. This can potentially reduce or eliminate the need for SNMP polling.

Get Ready to Sample

In Flexible NetFlow, the Flow Cache can be configured for packet sampling where a subset of random packets is sampled from the stream. Most routers participating in NetFlow are only generating between .5 to 20 flow packets per second therefore, it is reasonable to accomplish a 100% representation of the traffic actually seen by the router.

Although they are not the norm, some routers participating in NetFlow have been known to transmit upwards of 1,500 NetFlow packets per second, resulting in tens of thousands of flows per second, all from a single router. This volume can lead to extremely large database tables and unacceptably long queries when reports need to be generated. Flexible Netflow like sFlow, from InMon Corporation, has the ability to sample traffic.

Why Sample?

Flexible NetFlow needed to address this volume issue, as there is such a thing as too much. For example, traffic on an OC 192 would require more NetFlow packets than most routers today could generate. Even if the router can generate tens of thousands of NetFlow packets per second, the NetFlow collector/analyzer needs to be able to store and report on that information. With today's technologies, this usually isn't feasible. Sampling is the way to go with high volume NetFlow routers. In this case, SNMP would be a great way to get accurate utilization reports.

Summary

Flexible NetFlow is leveraging the power of NetFlow version 9. Many will argue that it should have been named "Flexible NetFlow version 9." It will work with existing collection tools, and is ready for vendors to create utilities which capitalize on its flexibility.

For More Information

For more details on Cisco's Flexible NetFlow, visit www.Plixer.com and www.Cisco.com. Much of the above information can be found in the "Introduction to Cisco IOS® Flexible NetFlow" whitepaper.