Determine the Monitoring Protocol for Your Network

This section will help you understand the key distinctions between NetFlow and sFlow, equipping you with the necessary insights and knowledge to make an informed decision when it comes to selecting the most suitable monitoring protocol for your network.

Key Differences between sFlow and Netflow

This section helps you understand the difference between Netflow and sFlow based on the following factors:

Table 1: Differences between sFlow and Netflow

Factor	Netflow	sFlow
Functionality	Stores the exported metadata aggregated related to IP traffic in the form of a Netflow Record Template. This Netflow Record is saved until the active timer expires, at which point it's exported to the collector.	sFlow is transient and therefore the data is not stored, instead, it's promptly transferred to the collector.
Monitored Flows	Monitors the following traffic: • Layer 2 • Layer 3: MPLS, IPv4, IPv6, SRv6	Monitors the following traffic: • Layer 2 • Layer 3: MPLS, IPv4, IPv6, SRv6 • VLANs **Note** VLAN is not supported in netflow for Cisco 8010 Series Routers.
Flow Data Processing	Processes flow data and stores it as flow records.	The flow data is sent to the collector for analysis. Unlike NetFlow, sFlow is not cached and contains fewer flow data fields.

Factor	Netflow	sFlow
Scalability	Scalability is determined by the number of packets sampled as per the NetFlow sampler map.	Scalability is determined by the number of sFlow packets.
Mechanism	Packet aggregation into flows. Netflow is stateful as it stores the Flow record until the active timer expires.	Packets are sampled randomly, while counters are sampled based on time intervals. sFlow is not stateful since the data is not stored; it's directly forwarded to the collector.
Resource usage	Elevated, due to more information provided, resulting in a significant burden on the router.	Typically places lower load on the router.

Summary

Before you identify the best protocol to monitor traffic, you must consider the type of devices that make up your network and the factors that influence the network performance such as latency, scalability and so on.

- Opt for NetFlow when you want to gather extensive data and enhance visibility, though it might introduce a slightly higher latency compared to sFlow. NetFlow offers comprehensive insights into traffic flows. With this information, you can effectively address network issues, identify security risks, strategize network upgrades, and optimize bandwidth utilization.

- Opt for sFlow if you're aiming to oversee traffic in networks with limited bandwidth. sFlow imposes lesser load on network and computing resources compared to NetFlow. Consequently, for small and medium-sized businesses (SMBs) and smaller networks that use less powerful devices, sFlow is more suitable. It can effectively mitigate any performance concerns. sFlow operates with lower resource demands and because of it's sampling approach to collect data from a subset of packets. By utilizing this sampled data, you can analyze traffic patterns, enabling the identification of irregularities and the optimization of network performance.

If your network setup accommodates both NetFlow and sFlow, you have the option to leverage both technologies and take advantage of their respective strengths. By identifying specific use cases, you can make a well-informed choice regarding the protocol that meets your network's traffic monitoring needs.