

Understanding Using sFlow Technology for Network Monitoring on an EX-series Switch

sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology randomly samples network packets and sends the samples to a monitoring station. You can configure sFlow technology on an EX-series switch to continuously monitor traffic at wire speed on all interfaces simultaneously.

sFlow technology has the following two sampling mechanisms:

- Packet-based sampling: Samples one packet out of a specified number of packets from an interface enabled for sFlow technology.
- Time-based sampling: Samples interface statistics at a specified interval from an interface enabled for sFlow technology.

The sampling information is used to create a network traffic visibility picture. JUNOS software fully supports the sFlow standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks* (see RFC 3176).



NOTE: sFlow technology on EX-series switches samples only raw packet headers. A raw Ethernet packet is the complete Layer 2 network frame.

An sFlow monitoring system consists of an sFlow agent embedded in the switch and a centralized collector. The sFlow agent's two main activities are random sampling and statistics gathering. It combines interface counters and flow samples and sends them across the network to the sFlow collector.

EX-series switches adopts the distributed sFlow architecture. The sFlow agent has two separate sampling entities that are associated with each packet forwarding engine. These sampling entities are known as subagents. Each subagent has a unique ID that is used by the collector to identify the data source. A subagent has its own independent state and forwards its own sample messages to the sFlow agent. The sFlow agent is responsible for packaging the samples into datagrams and sending them to the sFlow collector. Since sampling is distributed across subagents, the protocol overheads associated with sFlow are significantly reduced at the collector. If the mastership assignment changes in a Virtual Chassis setup, sFlow technology continues to function.



NOTE: JUNOS software on EX-series switches supports sFlow version 5.

The sFlow collector uses the sFlow agent's IP address to determine the source of the sFlow data. The IP address assigned to the agent is based on the following order of priority of interfaces configured on the switch:

1. Loopback interface
2. Virtual Management Ethernet (VME) interface

3. Management Ethernet interface

4. Any other Layer 3 interface

If a particular interface has not been configured, the IP address of the next interface in the priority list is used as the IP address for the agent. For example, if the loopback interface has not been configured, then the IP address of the VME interface is assigned as the agent's IP address. Once an IP address is assigned to the agent and an interface with a higher priority is configured, the agent's IP address is not modified till the sFlow service is restarted. At least one interface has to be configured for an IP address to be assigned to the agent.



NOTE: If a loopback interface has the IP address 127.x.x.x, the agent is not assigned the IP address of that interface. The next interface on the priority list is used as the agent's IP address.

sFlow data can be used to provide network traffic visibility information. Infrequent sampling flows are not reported in the sFlow information, but over time the majority of flows are reported. Based on a defined sampling rate, 1 out of N packets is captured and sent to the collector. This type of sampling does not provide a 100 percent accurate result in the analysis, but it does provide a result with quantifiable accuracy. A polling interval defines how often the sFlow data for a specific interface are sent to the collector, but an sFlow agent is free to schedule polling.

- Related Topics**
- Example: Monitoring Network Traffic Using sFlow Technology on EX-series Switches
 - Configuring sFlow Technology for Network Monitoring (CLI Procedure)
 - Monitoring Interface Status and Traffic