sFlow Introduction

This guide describes the sFlow® feature, and how to configure it on your AlliedWare Plus™ switch. Figure 1 shows a basic sFlow network structure. The three network switches also function as sFlow agents. Each agent switch captures samples of the traffic passing through its monitored ports, and sends these samples together with counter information back to the sFlow collector. The agents sample data from a number of switch ports, each acting as an sFlow data source.

Figure 1: Basic sFlow network

*sFlow® is a registered trademark belonging to InMon Corp, San Francisco, CA.
Products and software version that apply to this guide

This guide applies to AlliedWare Plus products that support sFlow, running version 5.4.4 or later.

To see whether your product supports sFlow, see the following documents:

- The product’s Datasheet
- The AlliedWare Plus Datasheet
- The product’s Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Feature support may change in later software versions. For the latest information, see the above documents.

Content

sFlow Introduction...............................................................................................................................................................1
  Products and software version that apply to this guide...............................................................2
  Sampling methods......................................................................................................................................................4
The sFlow Collector...........................................................................................................................................................5
Configuring sFlow on your Switch...........................................................................................................................5
  Configuration procedure........................................................................................................................................6
Configuration example......................................................................................................................................................7
sFlow Datagrams...............................................................................................................................................................12
The sFlow MIB...............................................................................................................................................................15
The sFlow Agent

Your switch can act as an sFlow agent. The key capabilities of the agent are to:

- sample frames as they pass through selected ports on the switch, and provide sampled extracts of the network traffic.
- periodically capture interface counter data.
- package together the sampled frame and counter information that can be sent to the collector for analysis and display.
- be configurable via SNMP MIB objects.
- communicate to heterogeneous collector devices by means of standard protocols.

Agent components and functionality

sFlow functionality on your switch is based on the requirements defined in of RFC 3176 and its updates defined in the sFlow version 5 memo dated July 2004. This memo can be found at the web site, www.sflow.org/sflow_version_5.txt.

The terms defined in Table 1 are used to describe the agent and its functionality on your switch:

<table>
<thead>
<tr>
<th>sFLOW® COMPONENT</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Device</td>
<td>Typically either a network switch or router that has the ability to forward frames across an Ethernet network; or between Ethernet networks, in the case of a router.</td>
</tr>
<tr>
<td>Data Source (sFlow Source Port)</td>
<td>The location of a sampling point within the switch. This is typically a switch port.</td>
</tr>
<tr>
<td>Packet Flow</td>
<td>A series of data frames that belong to a single conversation, which are traversing the network device.</td>
</tr>
<tr>
<td>Sampling Rate</td>
<td>The ratio of frames passing through the data source, to those captured and forwarded as sFlow data.</td>
</tr>
<tr>
<td>Counter Sampling</td>
<td>The periodic polling of counters taken at the data source.</td>
</tr>
<tr>
<td>sFlow Datagram</td>
<td>A UDP datagram that contains details of sFlow captured data, and counters sent by the sFlow Agent to its Collector.</td>
</tr>
<tr>
<td>sFlow Instance</td>
<td>A measurement process that is associated with a particular port, although a port can have more than one instance associated with it. Each instance operates independently of other instances. For example, a packet flow instance from a particular port will operate at its configured sampling rate, whilst the counter instance will operate at its sampling interval.</td>
</tr>
</tbody>
</table>

The sFlow agent (switch) uses sampling technology to derive traffic statistics from its monitored ports. Samples are taken at the sFlow source ports. After collecting its information, the switch then packetizes its samples and statistical data, and sends both to a remote sFlow collector.
Sampling methods

Two sampling methods are employed within the sFlow agent: frame sampling, and counter sampling. Both sample types are combined within the datagrams sent to the collector. The frame sample data will result in a relatively constant traffic stream, but the counter information is sent where it can fill available space within each datagram. Datagrams are normally sent to the collector at the rate of one each second. However, several datagrams can be sent in rapid succession, where more information exists than can be sent in a single datagram.

Frame sampling

As frames enter or leave an sFlow source port, they are sampled at a rate determined by the sflow sampling-rate command for that particular port.

Sampling occurs every N frames (on average), where N is the rate value set via sflow sampling-rate command. The sampling rate applies to ingress and egress frames independently. For example, a value of 1000 will sample one frame in every 1000 frames received and one in every 1000 frames sent from the specified port.

Caution

Setting the sFlow sampling rate to a very low value (frequent sampling) can place a heavy load on the switch’s CPU. The severity of this loading will increase with the number of ports configured for sampling, the port speeds, and their data sampling rates.

Data confidentiality

Sampling operates by capturing the initial portion of the frames (statistically) selected. The portion sampled is set by the sflow max-header-size command, or SNMP. If the maximum header size is greater than the actual headers in the sampled frames, then portions of the user data (payload) will also be captured and encapsulated in the datagrams sent to the collector. The amount of user data captured can be minimized by careful selection of the maximum header size.

Counter polling

The function of counter polling is to provide snapshots of various system counters. This produces a series of data counter sets for each port, which can be independently polled at user defined rates, and sent (once a second or less) to the collector.

Allied Telesis switches running AlliedWare Plus software support generic interface counters only. For more information on the data types included in the sampling count, see "sFlow Datagrams" on page 12.
The sFlow Collector

The sFlow collector receives traffic samples and counter information from a number of sFlow agents. These samples are received as a series of UDP datagrams. From the data contained within these datagrams, the collector is able to provide statistical and/or graphical information about network traffic.

The sFlow agent application on your switch supports only a single collector configuration.

sFlow collectors are proprietary third party products. Your switch, running as an sFlow agent, has been designed for interoperability with any sFlow collector that supports the sFlow Version 5 specification, including the inMon sFlow collector.

The sFlow Collector may also contain an SNMP Manager that is able to configure sFlow on its agent switches.

Configuring sFlow on your Switch

This section provides some guidelines for setting up the sFlow® agent on your switch. sFlow can be configured directly on your switch – using the CLI, or it can be configured via an SNMP manager. The SNMP management function can be carried out either by a the sFlow collector, or a separate SNMP manager. The configuration examples in this section are shown using the CLI.

sFlow configuration can vary greatly with your overall configuration, data profile, and monitoring intensity. Also, many interdependencies exist between parameter settings. For this reason, few firm configuration settings are recommended in this overview guide, but instead these parameter relationships are explained and some typical configuration examples are shown.

---

**Caution**

On an SBx908 with a XEM-2XP module fitted, sFlow sampling does not operate for this XEM when the XEM-2XP is installed in the lowest numbered SBx908 bay. Ensure that any XEM-2XP modules are not fitted in the lowest bay in an SBx908.

If a XEM module that is installed in a lower numbered SBx908 bay is hot swapped then a XEM-2XP module installed in a higher numbered SBx908 bay may become the XEM in the lowest numbered bay, resulting in sFlow sampling not operating. Ensure that any XEM-2XP modules will not become the XEM in the lowest numbered bay in an SBx908 by fitting the XEM-2XP in the highest numbered bay.

---

**Caution**

The sFlow configurations are set either by the switch’s CLI, or the sFlow collector via SNMP. Sometimes the collector will override the sFlow settings that were initially configured by the CLI, in order to apply its own default settings.

If you want to apply the sFlow settings set by the CLI, or by an external network management system, then turn off network management at the collector.

We also advise that as part of your sFlow commissioning process, you review your security access procedures relating to sFlow access and its data traffic management.
The default settings on your switch have sFlow turned off for all ports.

The following commands are used to setup and configure sFlow on your switch. These are introduced in the order in which you would logically need to use them.

### SFLOW COMMAND | FUNCTIONALITY
--- | ---
`sflow enable` | enables sFlow on your switch (or stack).
`sflow max-header-size` | sets the maximum sFlow data capture size.
`sflow collector max-datagram-size` | sets the maximum size for the agent to collector datagrams.
`sflow agent (address)` | sets the sFlow agent IP address on the switch.
`sflow polling-interval` | sets the counter polling interval for specified ports.
`sflow sampling-rate` | sets the mean sampling rate for specified ports.
`sflow collector (address)` | the sFlow agent’s collector IP address and/or UDP port.

### Configuration procedure

The following process sets out a systematic procedure to configure sFlow on your switch:

#### Information gathering

sFlow configuration is dependent on your network structure and its data. Start by gathering together the following information.

- Obtain (or determine) the sFlow collector IP address.
- Select an appropriate UDP port for your sFlow datagrams. The recommended value is 6343, and is the default value preconfigured on your switch.
- Select an appropriate IP address for your sFlow agent. We recommend that you use the local IP address of your switch. For more information on local addresses and how to set them up, see the `interface (to configure)` command.
- Assess the sensitivity of the data that your sFlow agent will be sampling.
- Obtain details of the protocols that your sFlow agent will be sampling. If you intend sampling unusual or proprietary protocols, obtain details of their header lengths.
- Calculate the most appropriate max-header-size for your sFlow sampling.
- Select the ports that you want to sample, and their sample rate.

These two factors vary (not quite) proportionally; so if you double the number of ports and double your sampling rate (i.e. sample half as many frames) then you will “almost” return to your earlier situation. Also note the speeds of the ports you have selected, because - for the same port utilization - the faster the port speed, the greater the load on the CPU.

- Review the speed of the port used to transport the sFlow datagrams to the collector. Unless configured to a specific port, the collector traffic will share the same network port with other traffic.

The capacity of the collector port should be sufficient to carry the volume of sFlow traffic. This topic is expanded on in the “Configuration example” on page 7.
Managing the sFlow processing overhead

The sFlow data sampled on the ports converges into the CPU for processing and UDP packetizing. Therefore one of the major factors when configuring sFlow is to prevent the sFlow data volumes from placing a significant overhead on the CPU processing. The two most significant factors here are, the number of ports sampled, and the sampling rate. The other (and lessor) factors in this equation are the frame size distribution and the maximum header size. The shorter the frames are on the network, the heavier the sFlow processing load will be (for the same number of frames per second). Conversely the shorter the maximum header size selected, the lighter the sFlow processing load will be (because less data per frame is sent to the CPU).

Configuration example

This section provides a configuration example based on the network shown below:

**Figure 2: sFlow configuration example**

---

**Step 1:** Determine the IP addresses and UDP ports.
- Collector IP address is 192.0.2.65
- sFlow UDP port uses the default of 6343
- Agent (local) IP address 192.0.2.33. This is the address that the collector may use to configure the agent via SNMP.
Step 2: Determine the maximum sFlow datagram size.

Datagrams will be sent at one second intervals regardless of the amount of data they contain. If the amount of data to be sent is greater than the maximum datagram size, then several datagrams will be sent in quick succession - within the 1 second interval. The objective is to contain the sFlow information in the minimum number of datagrams. That is, to fragment datagrams when necessary, but do it as little as possible.

Find the maximum datagram size that will pass through all network components without fragmenting. Then set the sFlow datagram size a little less than this value.

- The maximum datagram size should be less than the MTU size.

For this example, the MTU is assumed to be set to its default of 1500 bytes. In this situation we could leave the maximum datagram size at its default of 1400 bytes; but in order to show this as a configuration step, we will change it to 1200 bytes.

Note: sFlow datagrams are generally transmitted at 1 second intervals. However, where there is more information than can fit into one datagram, several datagrams are sent sequentially, within the 1 second time frame.

Step 3: Determine the max-header-size for the sampled data.

The maximum header size for the sampled data is set by the sflow max-header-size command. The optimum setting is to capture only the header portion of the frame and discard the user-data portion. This is especially important where the user data contains sensitive information.

Keeping the max-header-size as small as possible has the additional benefit of lightening the CPU load. First, inspect the nature of the data to be sampled and the protocols used to carry it.

For this example we will assume that the network contains Ethernet II frames with the 4 byte 802.1Q header component, IP, TCP protocols. In this situation the following rules can be applied:

For an environment using standard TCP/IPv4 over Ethernet frames, consider the following protocol basics.

- Ethernet header (including the 4 byte 802.1Q header component) = 18 bytes
- IPv4 header = 24 bytes
- TCP header = 24 bytes
- Total = 66 bytes

A similar calculation can be made for an environment using IPv6 over Ethernet.

- Ethernet header (including the 4 byte 802.1Q component) = 18 bytes
- IPv6 header = 40 bytes
- TCP header = 24 bytes
- Total = 82 bytes
In the above network scenarios:

- For IPv4 - any data existing between 66 bytes and the value set by this command will be included in the sFlow packet samples. For example, with the default of 128 applied, up to 128-66=62 bytes of user data could be included in the sFlow datagram samples sent between the Agent and the Collector.

- For IPv6 - any data existing between 82 bytes and the value set by this command will be included in the sFlow packet samples. For example, with the default of 128 applied, up to 128-82=46 bytes of user data could be included in the sFlow datagram samples sent between the Agent and the Collector.

Note that the agent-to-collector datagrams contain their own UDP headers, which are outside this calculation.

For this example the **sflow max-header-size** will be set to 68 bytes (assuming an Ethernet - IPv4 - TCP environment).

**Step 4: Select ports to sample.**

- Each sampled sFlow port speed is 1 Gbps
- 12 ports have been selected for sampling
- Check that none of the ports selected have mirroring configured. sFlow will not operate if any port on the switch is configured for mirroring.

**Step 5: Determine the sampling rate.**

Selecting the sampling rate involves a trade-off between sFlow requirements, and system loading. The lower the sampling rate, the more samples will be taken, and the more accurate their results will be. Unfortunately, taking more samples increases the load on the switch CPU and on the network connection to the collector.

For this particular configuration, the value of the sampling rate was set to 2750 to present a light load on the CPU.

**Step 6: Review and adjust settings.**

Because sFlow traffic loading will vary with the traffic profile, the following general assumptions are made. The following traffic profile is assumed.

- 50% of frames are <200 bytes long
- 40% of frames are >1400 bytes long

The following settings are:

- 12 x 1 Gbps ports are being sampled
- sFlow max-header size = 68 bytes
- sampling rate (N = 2750)
- average port utilization is assumed to be approximately 60%
- average data rate to the collector is assumed to be approximately 250 kbps

When setting the sampling rate, consider the following factors that will affect the CPU load. This load will increase (not necessarily linearly) as you:
- increase the number of ports configured
- increase the port speeds
- decrease the sampling rate
- increase the max-header-size

For this configuration the average sFlow collector traffic is expected to be approximately 250 kbps. In this example the agent-to-collector traffic will be shared with non-sFlow traffic. Although not described in this example, you can specifically configure the collector port to route only sFlow traffic.

To do this you would need to assign a separate VLAN (and IP address) to the agent-to-collector interface and direct your sFlow traffic to this interface.

We advise that you ensure adequate bandwidth is provided for both the sFlow and general traffic that could share its network connection.

We will now use these settings to configure the network.
Configuration procedure

The following steps apply the settings obtained in the previous section.

**Step 1: Enable sFlow switch-wide (globally).**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter Global Configuration Mode.</td>
</tr>
<tr>
<td><code>sflow enable</code></td>
<td>Enable the sFlow agent globally on the switch.</td>
</tr>
</tbody>
</table>

**Step 2: Configure the sFlow collector settings.**

**Step a. Set the sFlow collector max-datagram size**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sflow collector max-datagram-size 1200</code></td>
<td>Set the maximum size of the sFlow datagrams to 1200 bytes.</td>
</tr>
</tbody>
</table>

**Step b. Set the sFlow collector (address)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sflow collector ip 192.0.2.65</code></td>
<td>Set the sFlow collector address to 192.0.2.65.</td>
</tr>
</tbody>
</table>

**Step 3: Configure the sFlow agent settings.**

**Step a. Set the sFlow agent (address)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sflow agent ip 192.0.2.33</code></td>
<td>Set the sFlow agent address to 192.0.2.33.</td>
</tr>
</tbody>
</table>

**Step b. Set the sFlow sampling rate on sFlow Source Ports**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface port1.0.11-port1.0.22</code></td>
<td>Select the port range to configure (ports 1.0.11 to 1.0.22).</td>
</tr>
<tr>
<td><code>sflow sampling-rate 2750</code></td>
<td>Set the sampling rate on the selected ports.</td>
</tr>
</tbody>
</table>

**Step 4: Check the configuration.**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>do sh running-config sflow</code></td>
<td>Validate that sFlow is enabled. Note that the prefix “do” enables you to run an Exec Mode command from an Interface Mode prompt.</td>
</tr>
</tbody>
</table>
sFlow Datagrams

After data sampling and counter information has been gathered, each sFlow agent packetizes the data and sends it to an sFlow collector where it can be analyzed and displayed in charts and tables.

This packetized data is sent to the collector in UDP datagrams. These datagrams bear the IP address of the collector and the port number 6343. Using a standardized port helps to avoid configuration problems between the sFlow agents and collectors.

Although an analysis of the sFlow datagrams is outside the scope of this document, some basic information is provided here for those interested in knowing the basic components of the sFlow datagrams. The full specification of the sFlow protocol can be found at www.sflow.org/sflow_version_5.txt.

sFlow datagrams comprise three basic components:

- Datagram header information
- Flow sample information - may contain several samples
- Counter statistical information - fitted in where space permits

The content of these datagram components is listed below:
sFlow Datagrams

**sFlow header fields**
- Version (the sFlow version being used)
- IP Address Type (can be either an IPv4 or IPv6 address type)
- Source IP Address (the IP address of the sFlow agent)
- Sequence Number (the datagram sequence number)
- System Up-time
- Sample Count (the number of samples in the datagram)
- Sample Dataset

**sFlow flow sample fields**
- Flow Sample 1 (the first sample)
- Sample Type (flow Sample, 0x0001)
- Sample Sequence Number (of flow samples)
- Sampler ID
- Sampling Rate (as set by the “sflow sampling-rate” on page 119.14 or SNMP)
- Sample Pool (the total number of packets that could have been sampled)
- Packets Dropped (the number of packets dropped, due to a lack of resources)
- Input (the interface that the packet was received on - not supported)
- Output (the index number of the interface that the packet was sent from)

Note that your collector should have the ability via SNMP to resolve index numbers to physical port numbers.

- Packet Type
- Header Protocol - Ethernet ISO 88023(1)
- Packet Size (frame Length including the FCS)
- Header Length - The sampled portion of the frame as set by the sflow max-header-size command. May be shorter for small frames.
- Header Bytes
- Extended Elements Number
- Extended Elements

Note that in practice the Ethernet header is usually followed by components for the IP, TCP, and user data.

**sFlow flow sample fields**
- Counter Sample
- Sample Type (Counter Sample, 0x0002)
- Sample Sequence Number
- Sample ID (source ID index value)
- Sample Interval (as set by the command sflow polling-interval)
- Counter Type (1=generic, 2=Ethernet)
Generic interface counters
- ifIndex
- ifType
- ifSpeed
- ifDirection (0=unknown, 1=full-duplex, 2=half-duplex, 3=in, 4=out)
- ifStatus
- InOctets
- InUcastpackets
- InMulticast packets
- InBroadcast packets
- InDiscarded packets (= 0)
- InPackets containing errors
- InPackets containing unknown protocols (= 0)
- OutOctets
- OutUcast packets
- OutMulticast packets
- OutBroadcast packets
- OutDiscarded packets
- OutPackets containing errors
- ifPromiscuous Mode

Ethernet interface counters
- dot3Stats Alignment Errors (= 0)
- dot3Stats FCS Errors
- dot3Stats Single Collision Frames (= 0)
- dot3Stats Multiple Collision Frames
- dot3Stats SQE Test Errors
- dot3Stats Deferred Transmissions (= 0)
- dot3Stats Late Collisions
- dot3Stats Excessive Collisions
- dot3Stats Internal Mac Transmit Errors
- dot3Stats Carrier Sense Errors (= 0)
- dot3Stats Frame Too Longs
- dot3Stats Internal Mac Receive Errors
- dot3Stats Symbol Errors (= 0)
The sFlow MIB

Your switch fully supports inMon's sFlow MIB. For more information, see the website www.sflow.org/SFLOW-MIB5.txt.