Technical Guide

sFlow®

Feature Overview and Configuration Guide

Introduction

sFlow is an industry-standard sampling system that is embedded in Allied Telesis' high-performing Layer 3 switches. sFlow enables you to use network devices to systematically sample and collect network traffic data. From this data you can quickly see:

- what the network is being used for
- trends useful for performance optimisation
- traffic indicating potential security threats
- usage for billing and accounting purposes
- abnormal traffic and indications of its causes

In this guide, we explain how sFlow works and examine the operation of sFlow processing. We also present some details of the AlliedWare Plus™ sFlow implementation.

Content

Which products and software version does it apply to?

This guide applies to the all Allied Telesis devices running AlliedWare Plus version 5.5.1-1.1 or higher that support sFlow. Check your product's datasheet to see if it supports sFlow.

For more information, see the following documents:

You also may find the following sources of information about sFlow useful:

- The product's Command Reference
- The product's Datasheet

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

You also may find the following sources of information about sFlow useful:

- http://www.sflow.org
- http://www.sflow.org/sflow_version_5.txt
- http://www.inmon.com

What sFlow does

sFlow sampling technology is used in high-speed switched networks to provide visibility to network usage. sFlow agent software is embedded in switches and routers, and sends data to a central sFlow collector, enabling network administrators to quickly see:

- the Layer 2 to Layer 7 traffic flows for all ports including Gigabit-speed ports
- what the network is being used for: detailed real-time data including usage related to particular interfaces, protocols, sources and destinations, including thresholds
- problems and abnormal traffic and indications of their causes
- traffic indicating potential security threats
- trends useful for performance optimization
- usage for billing and accounting purposes

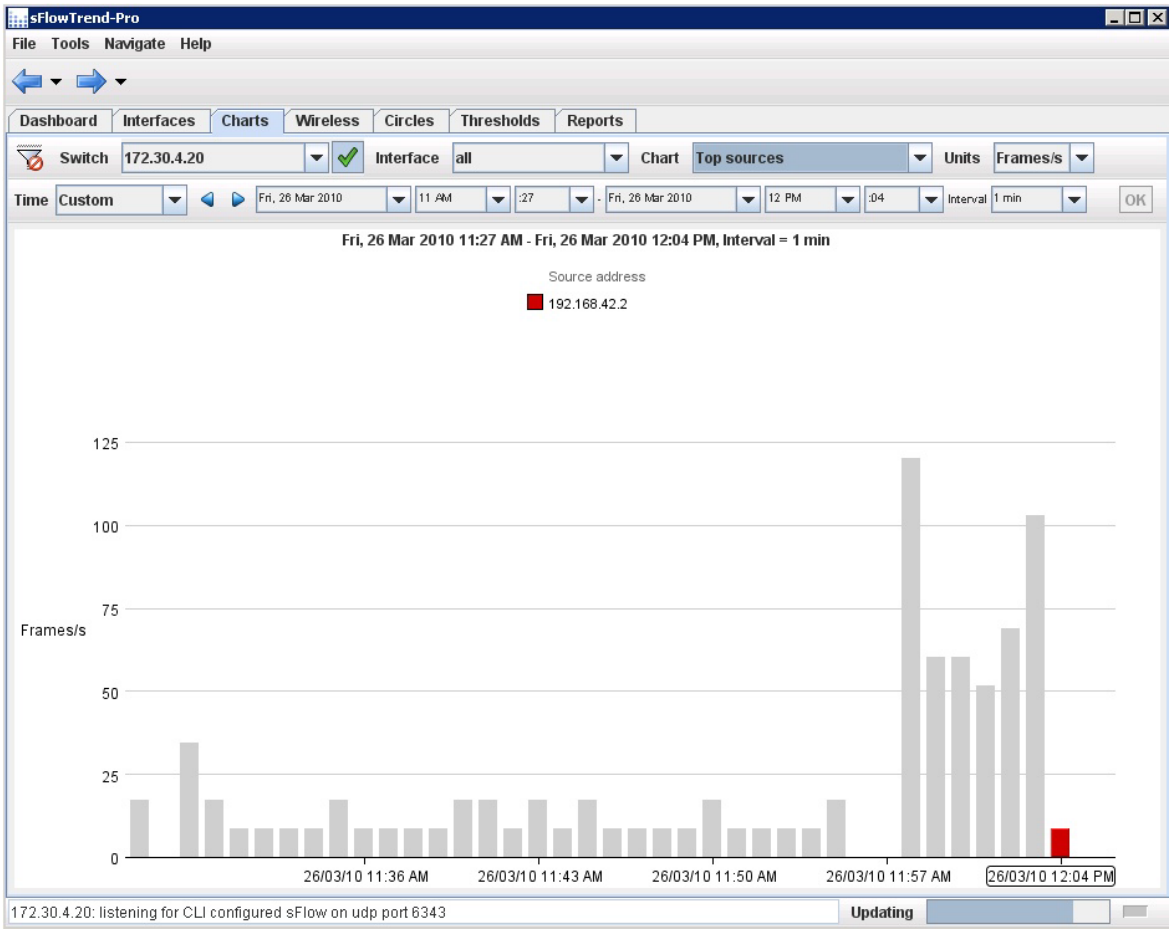
An sFlow system provides continuous monitoring under all network conditions. It can generate management reports on network performance, and can be scaled to add monitoring for more devices as your network expands.

For details of the latest industry standard (as at September 2016), see the sFlow Version 5 specification, July 2004 (http://www.sflow.org/sflow_version_5.txt).

sFlow operates by regularly polling interface counters and sampling traffic on a switch or router. This data is forwarded to a dedicated workstation for analysis. Using sFlow collector software, the information collected from sFlow agents can be analyzed and presented to network administrators in a variety of ways, such as charts, dashboards, and thresholds.

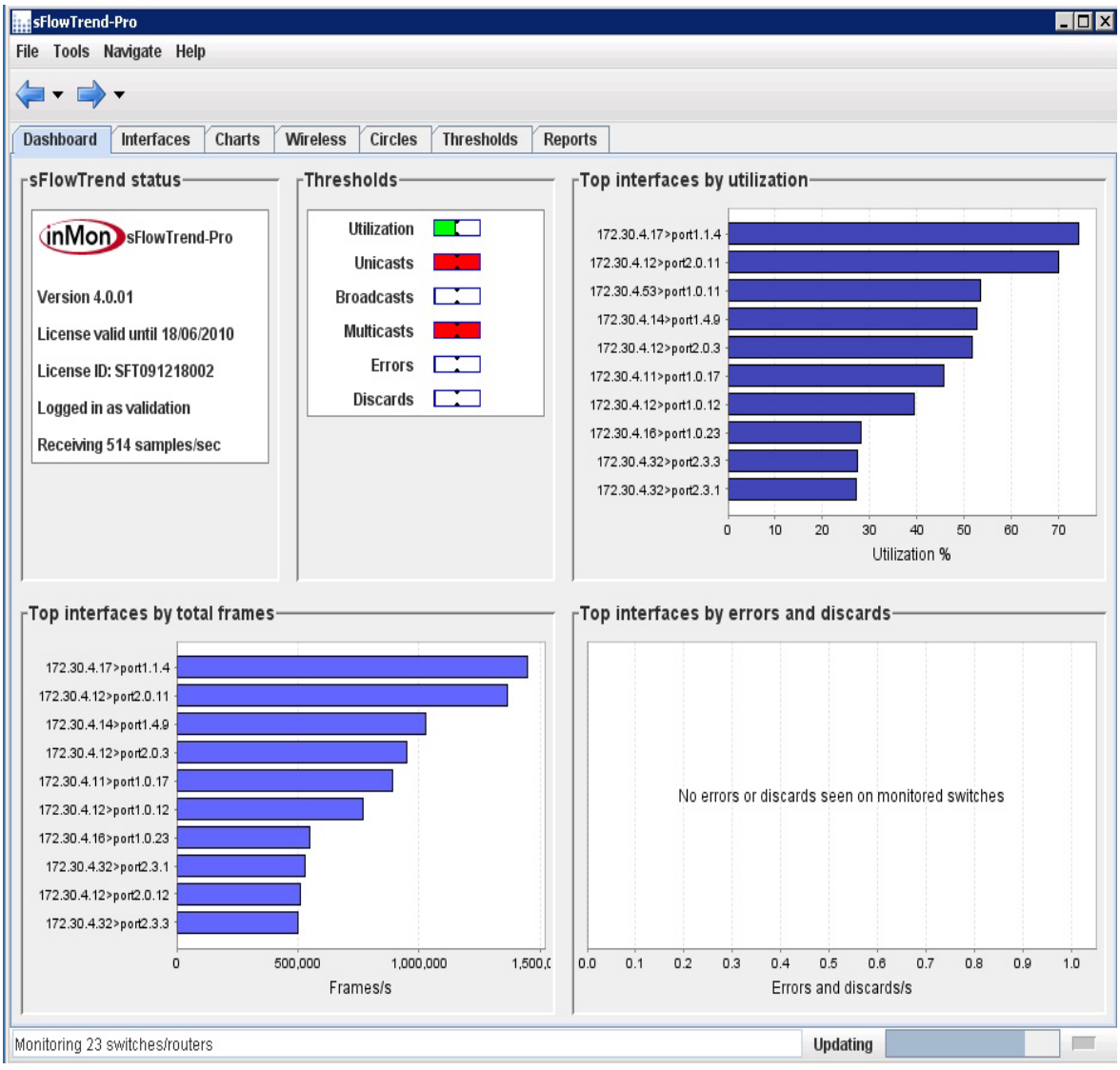
The figures below show windows from sFlow collector software, sFlowTrend-Pro from InMon Corp., displaying information it has collected and analyzed from AlliedWare Plus sFlow agents.

Charts Charts can be based on a variety of parameters, for example, to show which interfaces, which VLANs, and which protocols send and receive the largest amount of traffic.

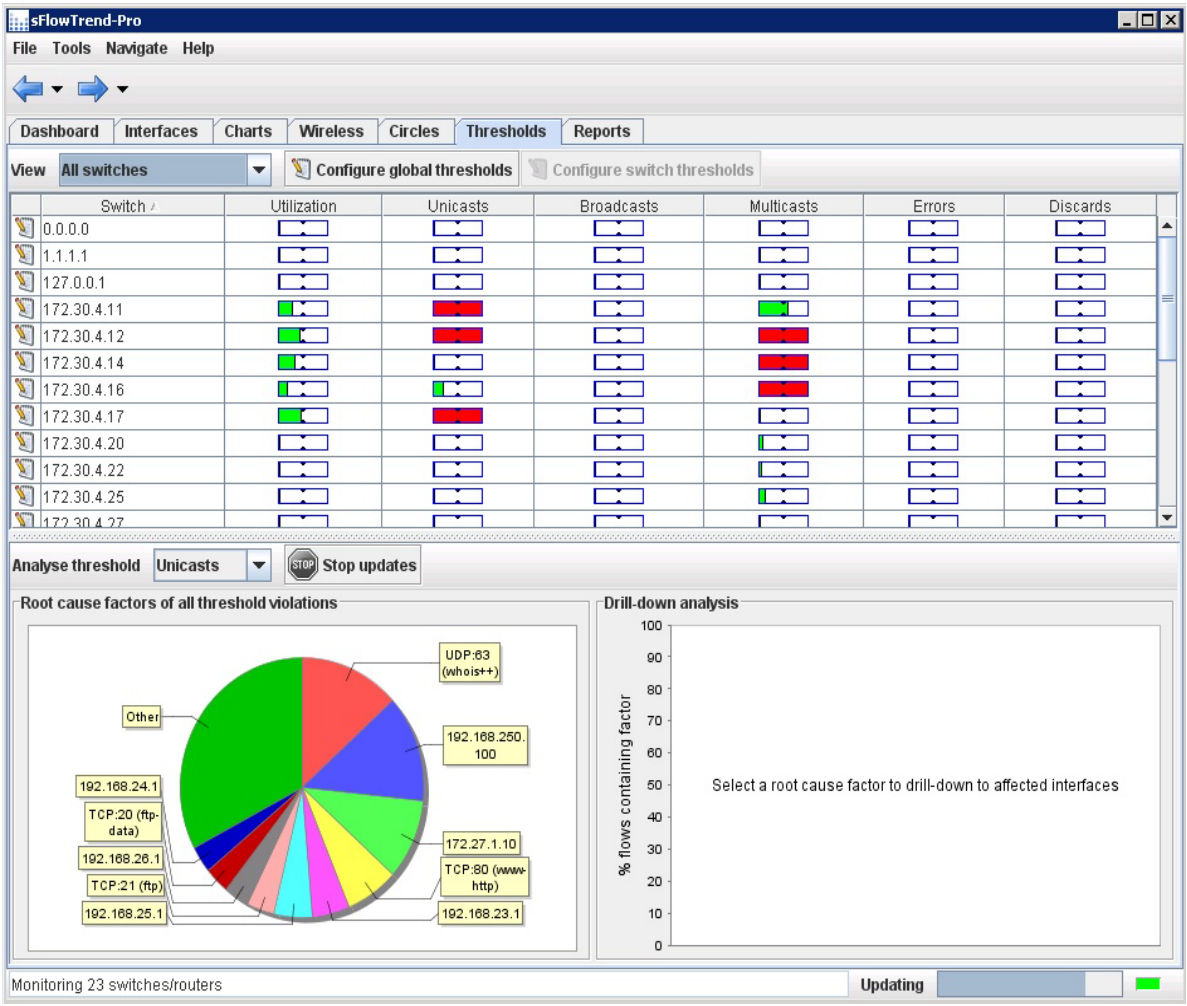


Dashboard This is the initial window that sFlowTrend-Pro collector software displays when it starts up. This window displays summary information about utilization and thresholds. This provides a quick snapshot of network health, such as:

- Are there any bottlenecks (over-utilised ports)?
- Are there cabling or switch faults that are corrupting data?
- Is the overall level of broadcast traffic within acceptable bounds?



Thresholds Thresholds can be configured for agents and interfaces, and threshold violations can be displayed. The table in the window below shows that unicast and multicast thresholds have been exceeded on particular switches in the network, while the pie graph shows an overview of threshold violations across the monitored network.



sFlow solution components

The key components of an sFlow monitoring system are sFlow agents and sFlow collectors.

sFlow agent

An sFlow **agent** is a switch or router through which the traffic to be monitored is flowing. This is the device that performs the sampling, and sends the sampled data to one or more sFlow collectors. Many agents can send data to the same collector.

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.

sFlow collector

The sFlow **collector** is a software application, running on a workstation or server, that collects the traffic data from a number of sFlow agents, stores the data, analyses it, and presents the analysis to the network administrator. Some sFlow collectors can use SNMP to configure agents. The sFlow collector should also be able to use SNMP to resolve the interface index numbers sent to it, so that it can present information related to the interface names of the associated physical interfaces. Other than such SNMP messages, the collector does not send any information back to the agents.

sFlow sampling

The sFlow agent can perform either or both of these two types of sampling:

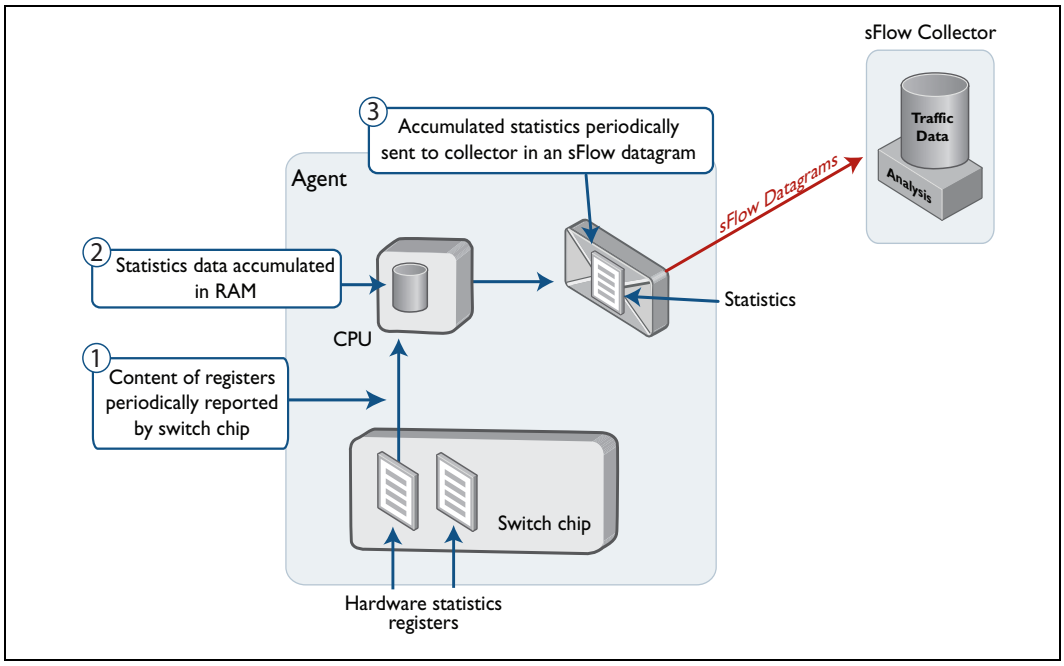
- counter sampling (also called counter polling)
- packet sampling—also referred to as flow sampling or frame sampling.

Counter sampling

For counter sampling (polling), the sFlow agent (the switch) periodically polls the hardware interface statistics registers (counters) in the switch chip for per-port statistics, and stores these in RAM until it is time to send the next message to the sFlow collector. It gathers overall port statistics, such as the number of broadcasts, errors, and so on.

The agent includes these statistics in the sFlow datagrams it sends to the collector, together with the packet sampling information if packet sampling is also configured on the agent. From these statistics, the sFlow collector gets information about the actual utilization of each port, for instance, broadcast to multicast to unicast ratios. If the agent is configured for counter sampling, it sends an sFlow datagram at intervals of at most one second, containing a snapshot of the counters cached in RAM from the most recent polling of interface counters.

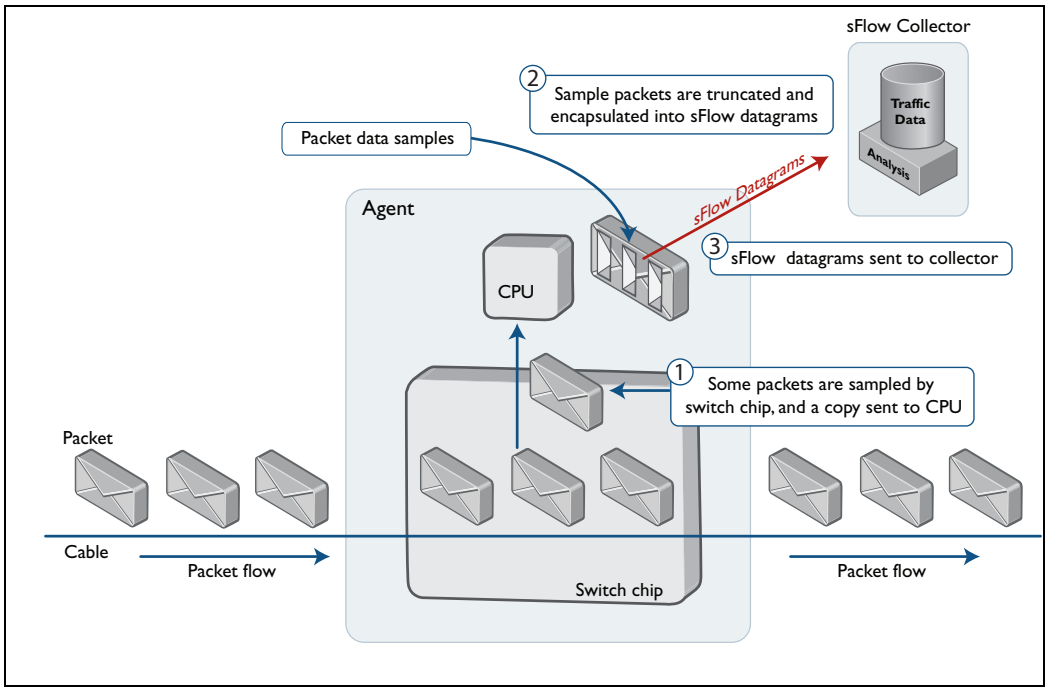
For more information about the statistics collected, see "Agent to collector datagrams" on page 11.



Packet sampling

Packet sampling schemes are widely used to characterize network traffic. If the sFlow agent (switch) is configured for packet sampling, it takes copies of random samples of the packets that are being forwarded within the switch (leaving the original alone) and sends them to the switch CPU to be processed. The CPU sends a configured portion of the sampled packet, containing a number of protocol headers and possibly some of the payload data, to the sFlow collector.

The random sampling process prevents synchronization with any periodic patterns in the traffic. On average, 1 in every N packets is captured and analyzed. This sampling can be applied to ingress and egress frames independently. The rate at which the agent sends datagrams depends on the sampling rate, the traffic rate, and the configured maximum datagram size; it typically includes several samples in one datagram.



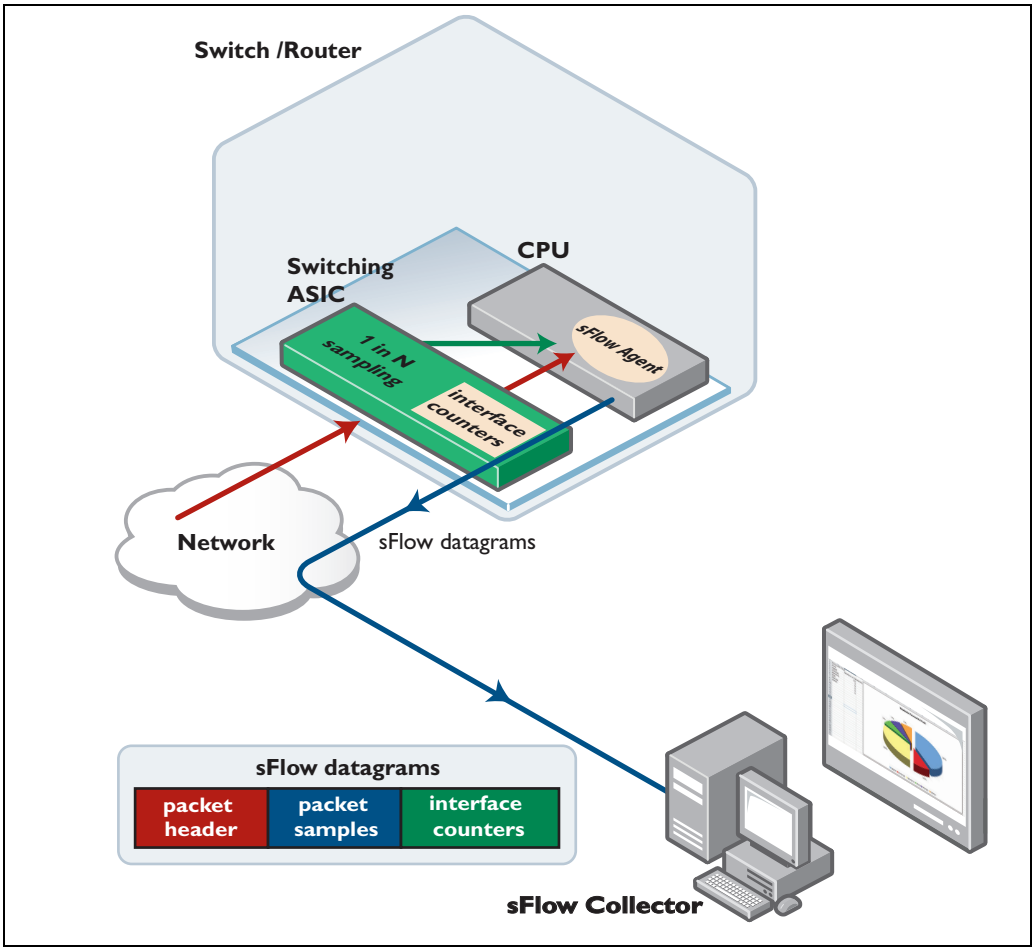
Data confidentiality

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.

Agent to collector datagrams

After it has gathered packet and counter samples, each sFlow agent packetizes the data and sends it to an sFlow collector in UDP datagrams. These datagrams bear the IP address of the collector and the standardized UDP destination port number 6343. Using a standardized port helps to avoid configuration problems between the sFlow agents and collectors. Depending on whether the agent is configured for counter sampling, packet sampling, or both, an sFlow datagram can contain either interface counters, packet samples, or a mixture of both.

The following figure illustrates the flow of data related to sFlow datagrams in the case that both counter and packet sampling is being performed. For a detailed specification of the sFlow protocol, see www.sflow.org/sflow_version_5.txt.



The following table provides information about the contents of sFlow datagrams.

Table 1: Contents of sFlow datagrams

PACKET HEADER	DESCRIPTION
Version	The sFlow version being used.
IP Address Type	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	How long the system has been operational for.
Sample count	The number of samples in the datagram.
Ingress interfaces	The ifindex of the switch port via which the packets entered the agent (if known).
Egress interfaces	The ifindex of the switch port via which the packets exited the agent (if known).
Sample dataset	sFlow specific parameters: • sequence numbers • sampling rate • total packets that could have been sampled • number of sampled packets dropped for lack of processing resource
PACKET SAMPLES	Packet sample information—may contain several samples.
Packet data	In AlliedWare Plus, packet samples consists of up to the first 200 bytes of the sampled packet, called a **header sample**. Even though it is called a header sample, the sampled data may include part of the packet payload data as well, depending on the length of the sample (up to 200 bytes), and the number and length of the protocol headers.
COUNTER SAMPLE	Counter statistical information—fitted in where space permits.
If index	The ifindex of the interface that the counters relate to.
Physical interface parameters	• speed • duplex mode • admin status • operational status of the interface
In counters	• ifInOctets • ifInUcastPkts • ifInMultiPkts • ifInBroadcastPkts • ifInDiscards • ifInErrors • ifInUnknownProbs
Out counters	• ifOutOctets • ifOutUcast Pkts • ifOutDiscards • ifOutErrors

Table 1: Contents of sFlow datagrams

Promiscuous mode	The private VLAN promiscuous mode of the interface.
Ethernet statistics	• alignment errors • FCS errors • collisions • SQE errors • deferred transmission • internal MAC errors • carrier sense errors • overlength frame errors • symbol errors

sFlow on Allied Telesis products

Support for sFlow in AlliedWare Plus

Allied Telesis switches running AlliedWare Plus 5.5.1-1.1 or higher can be configured as sFlow agents based on the sFlow Version 5 specification 2004 (http://www.sflow.org/sflow_version_5.txt), including support for:

- counter and packet sampling on physical switch ports
- sampling of unicast, multicast, and broadcast traffic on ingress ports; sampling of unicast traffic on egress ports
- standard packet header samples up to 200 bytes in length
- sending sFlow datagrams to multiple collectors.

Table 1: sFlow components

SFLOW® COMPONENT	DEFINITION
Network Device	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.
Data Source (sFlow Source Port)	The location of a sampling point within the switch. This is typically a switch port.
Packet Flow	A series of data frames that belong to a single conversation, which are traversing the network device.
Sampling Rate	The ratio of frames passing through the data source, to those captured and forwarded as sFlow data.
Counter Sampling	The periodic polling of counters taken at the data source.
sFlow Datagram	A UDP datagram that contains details of sFlow captured data, and counters sent by the sFlow Agent to its Collector.
sFlow Instance	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.

Interoperability

Allied Telesis interoperates with sFlow collector software that supports the sFlow Version 5 specification, including:

- sFlowTrend—sFlowTrend can be downloaded free from http://www.inmon.com
- sFlowTrend-Pro—A free trial of sFlowTrend-Pro can be downloaded from http://www.inmon.com

Limitations of sFlow in AlliedWare Plus

Hardware design and resource constraints apply some limitations to the sFlow implementation on AlliedWare Plus switches.

Limitations that apply to all switches running AlliedWare Plus:

- Sampling of multicast and broadcast traffic on egress ports is not supported.
- High frequency packet sampling of ports with high traffic loading that are transmitting jumbo frames larger than 8000 bytes may result in occasional packet loss and inconsistent results. In these circumstances, we recommend setting the sampling rate to 1000 or higher (that is, on average 1 in 1000 or more packets are sampled).
- While you can configure multiple collectors, all the collectors will be receiving the exact same samples and counters. You can't have independent counter sampling and packet sampling settings for different collectors (this is a hardware limitation).
- If the destination MAC address of a sampled egress packet is not in the switch's forwarding database, the sample is not included in a datagram to the sFlow collector.

Limitations that are specific to x220, x530, x900, and SwitchBlade x8100 Series switches only:

- sFlow and mirroring must not be enabled on the same switch.
- Egress packets are sampled before header manipulation for tunnel encapsulation/decapsulation, User Priority (CoS) and DSCP remarking, so the sampled packets do not have these adjustments.

Limitations that are specific to GS970M, IE300, IE510, IX5, x210, x230, x310, x550, x600, x610 x930, x950, SwitchBlade x908, and SwitchBlade x908 GEN2 Series switches only:

- sFlow and mirroring must not be enabled on the same switch.
- If the packet is IPv4 or IPv6 routed, and the egress port is sFlow sampling, and the ingress and egress ports are on the same switch instance then the packet that is egressed will be sampled as ingressed, i.e. the egress sample does not have the source and destination MACs adjusted.

From software version 5.5.1-2.1 onwards, sFlow is supported on the AR4050S UTM Firewall. Limitations are as follows:

sFlow commands on the AR4050S UTM Firewall:

- match those on switches, but are available on Layer 3 interfaces rather than switch ports.
- support Layer 3 interfaces (Ethernet, VLANs, PPP, tunnels, 802.1q).
- do not support switch ports on routers.

Configuring sFlow in AlliedWare Plus

You can configure the switch to be an sFlow agent in one of these ways:

- "Using the CLI to configure the switch as an sFlow agent" on page 18
- "Using the collector to configure the switch as an agent" on page 21—some collector software applications, including sFlowTrend-Pro, support this.
- "Using an SNMP manager to configure the switch as an agent" on page 22

Before configuring sFlow

Configuring sFlow is not complicated, but every customer's network and requirements are different, so consider the following matters before configuring sFlow on your LAN.

- How many ports on the sFlow agent are going to be sampled?
- Which sampling rate will be used?

  sFlow operates in both software and hardware. The switch chip periodically copies a packet (leaving the original alone) and sends it to the CPU for processing. The period is configured via the sampling rate. Over time, the total number of packets monitored divided by the total number of packets sampled approximates to the sampling rate.

  Setting the packet sampling rate to a high sampling frequency can place a heavy load on the switch's CPU. The severity of this loading increases with the number of ports configured, the port speeds, and their packet sampling rates.

- Which value will be configured for sFlow's max-datagram size? This is the size of the packet to be sent from the sFlow agent to the sFlow collector.

  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 a the minimum number of datagrams.That is, to fragment datagrams when necessary, but do it as little as possible.

  The max-datagram size should be less than the MTU (Maximum Transmission Unit) size for the network over which the sFlow packets are being sent to the collector. If the packets are bigger than the MTU size then the sFlow agent will need to fragment them, and this should be done as little as possible in order to reduce processing load on the sFlow agent.

  If you get an sFlow message indicating that a packet or counter sample is too big for the datagram, this probably means the max-datagram-size is too small to fit the sample into, and it should be increased, for instance, to the default value (1400 bytes).

- What will the max-header-size be? This is the maximum number of bytes extracted from packets by the sFlow agent to form the packet samples.

  Keeping the max-header-size as small as possible lightens the CPU load, and minimises the forwarding of sensitive payload data. However, the samples need to be large enough to hold all the information you need to collect.

When calculating the number of bytes to include in the header sample, consider the following allocated sizes for fields in standard TCP/IPv4 over Ethernet frames:

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

An environment using IPv6 over Ethernet:

- Ethernet header (including the 4 byte 802.1Q tag) = 18 bytes
- IPv6 header = 40 bytes
- TCP header = 24 bytes
- Total = **82** bytes

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

- Before enabling sFlow, ensure that port mirroring is not configured on any ports on the switch.
- 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.
- 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

Performance considerations

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).

When configuring sFlow, 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

Using the CLI to configure the switch as an sFlow agent

To configure the AlliedWare Plus switch as an sFlow agent, follow the procedure below. For more detailed information, see the ***sFlow Introduction*** and ***sFlow Commands*** chapters in the ***Software Reference*** for your switch. If you do not wish the sFlow collector software to modify the sFlow configuration on the switch, turn this feature off at the collector.

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

Table 2: sFlow command functionality

SFLOW COMMAND	FUNCTIONALITY
sflow enable	Enables sFlow on your switch (or stack).
sflow max-header-size	Sets the maximum sFlow data capture size.
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 id	The sFlow agent's collector IP address and optionally, the collectors port and/or max-datagram-size.

Configuring the switch as an sFlow Agent

1. **Configure global sFlow settings for the switch.**

Enable sFlow.

```
awplus(config)# sflow enable
```

Set the agent IP address. This will identify the switch as an agent to the collector, and provide an IP address for the collector to send SNMP messages to if required. You can set the agent IP address to any valid IP address, including:

- the local (loopback) IP address of the switch (IP address of interface lo—recommended). If there is more than one path from the collector to the agent, this may make SNMP communication from the sFlow collector to the agent (such as for configuring the agent or resolving names) more resilient to individual link failures.
- an IP address for a particular switch interface. In this case, the interface IP address and the sFlow agent IP address should both be manually set to the same fixed IP address.

```
awplus(config)# sflow agent ip <agent-ip-address>
```

Set the IP address of the collector that the switch will send sFlow data to.

- By default, the maximum size of the sFlow datagrams that the switch will send to the collector is 1500 bytes. If necessary, modify this setting. Use the optional VRF parameter to send samples to collectors that reside within a non-global VRF.

```
awplus(config)# sflow collector id <1-5> ip <ip-address> [vrf <vrf-
name>] [port <1-65535>|max-datagram-size <200-1500>]
```

2. **Configure VRF to send samples to collectors.**

Configure sending samples to a collector residing within VRF 'red':

```
awplus(config)# sflow collector id 1 ip 10.0.0.1 vrf red
```

Output of the **show sflow** command showing multiple collectors configured, some in non-global VRFs:

```
awplus#show sflow

sFlow Agent Configuration:                    Default Values
  sFlow Admin Status ........ Enabled         [Disabled]
  sFlow Agent Address ....... 192.168.1.117   [not set]

sFlow Collector Configuration:
------------------------------------------------------------------------
  ID  IP Address                                UDP Port  Max Datagram Size
      VRF
------------------------------------------------------------------------
   1  192.168.1.1                                   9000               1400
      red
   2  10.0.0.1                                      6343               1400
      -
   3  10.0.0.2                                      9000               1400
      blue

sFlow Agent Status:
  Polling/sampling/Tx ....... Active
```

3. **Configure packet sampling.**

Select the ports to configure for packet sampling. You can configure different settings on different sets of ports.

```
awplus(config)# interface <port-list>
```

Enable packet sampling, and set the sampling rate. The rate is a number X, meaning on average sample 1 in every X ingress packets, and 1 in every X egress packets. By default, packet sampling is disabled (**sampling-rate**=0).

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.

```
awplus(config-if)# sflow sampling-rate {0|<50-16777215>}
```

Some switches have a minimum sampling rate of 256. Please check for product's Command Reference for the range of permissible values.

Configure the maximum number of bytes captured by the sFlow agent to send in the header sample portion of the packet samples. Range: 14 to 200 bytes; default: 128 bytes.

```
awplus(config-if)# sflow max-header-size <size>
```

4. **Configure counter sampling.**

Select the switch ports to configure for counter sampling. You can configure different settings on different sets of switch ports.

```
awplus(config)# interface <port-list>
```

Configure the polling interval (in seconds) for counter sampling. By default, counter sampling is disabled (**polling-interval**=0).

```
awplus(config-if)# sflow polling-interval {0|<1-16777215>}
```

5. **Confirm the sFlow configuration on the switch.**

Display and check the sFlow configuration on the switch.

```
awplus(config-if)# exit
awplus(config)# exit
awplus# show sflow
awplus# show sflow interface [<port-list>]
awplus# show running-config sflow
```

6. **Configure SNMP on the switch.**

To allow the sFlow collector to use SNMP communication with the switch to resolve data such as interface indexes, enable the SNMP server (enabled by default).

```
awplus(config)# snmp-server
```

For SNMP v2c, create an SNMP community with read-write access for sFlow configuration (called **sflow** in this example).

```
awplus(config)# snmp-server community sflow rw
```

For more information about configuring SNMP on the switch, see the ***SNMP Introduction*** and ***SNMP Commands*** chapters in the ***Software Reference*** for your switch. The switch supports the SFLOW-MIB, as defined in http://www.sflow.org/SFLOW-MIB5.txt.

Using the collector to configure the switch as an agent

Some sFlow collectors can use SNMP to configure agents. Note that this may not allow precise control of the sFlow configuration on the switch. For instance, the collector may configure packet and counter sampling on all switch ports, and determine the sampling and polling rates.

To allow an sFlow collector to configure the switch as an agent, the collector must:

- be set to configure the agent
- have the agent IP address
- be configured to allow SNMP communication with the agent

The switch (agent) must:

- be configured to allow SNMP read-write access to the collector
- have sFlow enabled, and an agent IP address configured. The sFlow collector can configure all other settings.

1. **Configure SNMP on the switch.**

Enable the SNMP server (enabled by default).

```
awplus(config)# snmp-server
```

For SNMP v2c, create an SNMP community with read-write access for sFlow configuration (called **sflow** in this example).

```
awplus(config)# snmp-server community sflow rw
```

For more information about configuring SNMP on the switch, see the ***SNMP Introduction*** and ***SNMP Commands*** chapters in the ***Software Reference*** for your switch.

2. **Enable the sFlow agent to be configured by a collector.**

Enable sFlow.

```
awplus(config)# sflow enable
```

Set the agent IP address. This will identify the switch as an agent to the collector, and provide an IP address for the collector to send SNMP messages to. You can set the agent IP address to any valid IP address, including:

- the local (loopback) IP address of the switch (IP address of interface lo—recommended). If there is more than one path from the collector to the agent, this may make SNMP communication from the sFlow collector to the agent (such as for configuring the agent or resolving names) more resilient to individual link failures.

- an IP address for a particular switch interface. In this case, the interface IP address and the sFlow agent IP address should both be manually set to the same fixed IP address.

```
awplus(config)# sflow agent ip <agent-ip-address>
```

Check the sFlow configuration.

```
awplus(config)# exit
awplus# show sflow
awplus# show sflow interface [<port-list>]
```

Using an SNMP manager to configure the switch as an agent

The switch (agent) must be configured to allow SNMP communication with read-write access for the SNMP management workstation.

The switch supports the SFLOW-MIB, as defined in http://www.sflow.org/SFLOW-MIB5.txt.

1. **Configure SNMP on the switch.**

Enable the SNMP server (enabled by default).

```
awplus(config)# snmp-server
```

2. **Configure SNMP v2c.**

For SNMP v2c, create an SNMP community with read-write access for sFlow configuration (called **sflow** in this example).

```
awplus(config)# snmp-server community sflow rw
```

For more information about configuring SNMP on the switch, see the SNMP Feature Overview and Configuration Guide and ***SNMP Commands*** chapters in the ***Software Reference*** for your switch.

Debugging sFlow

If sFlow is not operating as you expect it to in your network, first check the configuration, by using the **show** commands in step 4 on page 20. AlliedWare Plus also provides more detailed debugging information on the switch's internal sFlow processing, which you can configure using the commands shown below. Following these commands are some examples of debug output. If you contact your authorized Allied Telesis support personnel for support, include output from the **show** commands above (step 4 on page 20) and the **debug** commands below.

Configuring sFlow debugging

1. Enable debug messages to be displayed on the console.

```
awplus# terminal monitor [<1-60>]
```

2. Display debug messages for sFlow events that are not switch-port-specific.

```
awplus# debug sflow agent
```

3. Display debug messages for sFlow interface counter polling and/or sampling events for particular switch ports or all switch ports.

```
awplus# debug sflow [interface [<port-list>]] [sampling] [polling]
```

4. Display and check sFlow debug configuration.

```
awplus# show debugging sflow [interface [<port-list>]]
```

5. When you have gathered sufficient debug messages, disable sFlow debugging.

```
awplus# no debug sflow agent
awplus# no debug sflow [interface [<port-list>]] [sampling] [polling]
```

6. Stop sending debug messages to the console.

```
awplus# terminal no monitor
```

Debug output

The sample debug output below comes from a Virtual Chassis Stack (VCStack) of x600 series switches configured as an sFlow agent to monitor traffic on selected switch ports in the stack.

sFlow agent debug

With sFlow agent debugging enabled, we can see from the following output that packets are sampled on ingress and that the packet samples are sent in sFlow datagrams to the sFlow collector at IP address 10.33.13.12.

```
awplus#debug sflow agent
awplus#term mon 10
awplus#
21:40:00 awplus SFLOWD[1030]: sFlow datagram sent to 10.33.13.12, seq 157247, samples 9
21:40:00 awplus SFLOWD[1030]: sFlow datagram sent to 10.33.13.12, seq 157248, samples 11
21:40:01 awplus SFLOWD[1030]: sFlow datagram sent to 10.33.13.12, seq 157249, samples 10
21:40:02 awplus SFLOWD[1030]: sFlow datagram sent to 10.33.13.12, seq 157250, samples 9
21:40:03 awplus SFLOWD[1030]: sFlow datagram sent to 10.33.13.12, seq 157251, samples 8
```

Polling debug

With sFlow polling debug enabled for all switch ports, the following examples of debug output show the switch ports that have been configured for counter sampling, each time the counters for that port are polled. The polling adds these counters to an internal cache of counter data in RAM. When it is time for the switch to send the next datagram to the sFlow collector, it includes a snapshot of the counters in this cache in the datagram.

```
awplus#debug sflow polling
awplus#term mon 3
awplus#21:43:08 awplus SFLOWD[1030]: port3.0.12: Counters polled
21:43:08 awplus SFLOWD[1030]: port3.0.5: Counters polled
21:43:09 awplus SFLOWD[1030]: port2.0.3: Counters polled
21:43:09 awplus SFLOWD[1030]: port2.0.1: Counters polled
21:43:09 awplus SFLOWD[1030]: port1.0.11: Counters polled
21:43:10 awplus SFLOWD[1030]: port3.0.9: Counters polled
21:43:10 awplus SFLOWD[1030]: port2.0.18: Counters polled
21:43:11 awplus SFLOWD[1030]: port4.0.13: Counters polled
21:43:11 awplus SFLOWD[1030]: port4.0.5: Counters polled
21:43:11 awplus SFLOWD[1030]: port3.0.8: Counters polled
```

Sampling debug

With sFlow sampling debug enabled for all switch ports, the following examples of output show all the ports that have been configured for sFlow packet sampling, each time a packet has been sampled on those ports.

```
awplus#debug sflow sampling
awplus#term mon 3
awplus#21:43:48 awplus SFLOWD[1030]: port3.0.10: Ingress packet sample taken from port
port3.0.10
21:43:48 awplus SFLOWD[1030]: port3.0.3:  Ingress packet sample taken from port port3.0.3
21:43:48 awplus SFLOWD[1030]: port3.0.1:  Ingress packet sample taken from port port3.0.1
21:43:48 awplus SFLOWD[1030]: port3.0.24: Ingress packet sample taken from port port3.0.24
21:43:48 awplus SFLOWD[1030]: port3.0.7:  Ingress packet sample taken from port port3.0.7
21:43:48 awplus SFLOWD[1030]: port3.0.7:  Ingress packet sample taken from port port3.0.7
21:43:48 awplus SFLOWD[1030]: port3.0.2:  Ingress packet sample taken from port port3.0.2
21:43:48 awplus SFLOWD[1030]: port3.0.7:  Ingress packet sample taken from port port3.0.7
21:43:48 awplus SFLOWD[1030]: port3.0.16: Ingress packet sample taken from port port3.0.16
21:43:48 awplus SFLOWD[1030]: port3.0.14: Ingress packet sample taken from port port3.0.14
21:43:48 awplus SFLOWD[1030]: port3.0.6:  Ingress packet sample taken from port port3.0.6
21:43:48 awplus SFLOWD[1030]: port3.0.11: Ingress packet sample taken from port port3.0.11
21:43:49 awplus SFLOWD[1030]: port3.0.13: Ingress packet sample taken from port port3.0.13
21:43:49 awplus SFLOWD[1030]: port3.0.24: Ingress packet sample taken from port port3.0.24
21:43:49 awplus SFLOWD[1030]: port3.0.6:  Ingress packet sample taken from port port3.0.6
21:43:49 awplus SFLOWD[1030]: port3.0.12: Ingress packet sample taken from port port3.0.12
21:43:49 awplus SFLOWD[1030]: port3.0.1:  Ingress packet sample taken from port port3.0.1
21:43:49 awplus SFLOWD[1030]: port3.0.3:  Ingress packet sample taken from port port3.0.3
21:43:49 awplus SFLOWD[1030]: port3.0.18: Ingress packet sample taken from port port3.0.18
21:43:49 awplus SFLOWD[1030]: port3.0.13: Ingress packet sample taken from port port3.0.13
21:43:49 awplus SFLOWD[1030]: port3.0.11: Ingress packet sample taken from port port3.0.11
21:43:49 awplus SFLOWD[1030]: port3.0.1:  Ingress packet sample taken from port port3.0.1
21:43:49 awplus SFLOWD[1030]: port3.0.24: Ingress packet sample taken from port port3.0.24
21:43:49 awplus SFLOWD[1030]: port3.0.3:  Ingress packet sample taken from port port3.0.3
21:43:49 awplus SFLOWD[1030]: port3.0.14: Ingress packet sample taken from port port3.0.14
21:43:49 awplus SFLOWD[1030]: port3.0.17: Ingress packet sample taken from port port3.0.17
21:43:49 awplus SFLOWD[1030]: port3.0.15: Ingress packet sample taken from port port3.0.15
21:43:49 awplus SFLOWD[1030]: port3.0.1:  Ingress packet sample taken from port port3.0.1
21:43:49 awplus SFLOWD[1030]: port3.0.1:  Ingress packet sample taken from port port3.0.1
21:43:49 awplus SFLOWD[1030]: port3.0.7:  Ingress packet sample taken from port port3.0.7
21:43:49 awplus SFLOWD[1030]: port3.0.13: Ingress packet sample taken from port port3.0.13
21:43:49 awplus SFLOWD[1030]: port3.0.10: Ingress packet sample taken from port port3.0.10
21:43:49 awplus SFLOWD[1030]: port3.0.14: Ingress packet sample taken from port port3.0.14
21:43:49 awplus SFLOWD[1030]: port3.0.13: Ingress packet sample taken from port port3.0.13
21:43:49 awplus SFLOWD[1030]: port3.0.7:  Ingress packet sample taken from port port3.0.7
21:43:50 awplus SFLOWD[1030]: port3.0.16: Ingress packet sample taken from port port3.0.16
21:43:50 awplus SFLOWD[1030]: port3.0.8:  Ingress packet sample taken from port port3.0.8
21:43:50 awplus SFLOWD[1030]: port3.0.11: Ingress packet sample taken from port port3.0.11
21:43:50 awplus SFLOWD[1030]: port3.0.21: Ingress packet sample taken from port port3.0.21
21:43:50 awplus SFLOWD[1030]: port3.0.8:  Ingress packet sample taken from port port3.0.8
21:43:50 awplus SFLOWD[1030]: port3.0.11: Ingress packet sample taken from port port3.0.11
21:43:50 awplus SFLOWD[1030]: port3.0.11: Ingress packet sample taken from port port3.0.11
21:43:50 awplus SFLOWD[1030]: port3.0.15: Ingress packet sample taken from port port3.0.15
21:43:50 awplus SFLOWD[1030]: port3.0.14: Ingress packet sample taken from port port3.0.14
21:43:50 awplus SFLOWD[1030]: port3.0.11: Ingress packet sample taken from port port3.0.11
21:43:50 awplus SFLOWD[1030]: port3.0.10: Ingress packet sample taken from port port3.0.10
21:43:50 awplus SFLOWD[1030]: port3.0.12: Ingress packet sample taken from port port3.0.12
```

Configuration script

This section provides the commands described in "Configuring sFlow in AlliedWare Plus" on page 16, with brief comments included, in a format that can be copied and modified to create parts of a configuration script file.

```
enable
! Configure the switch as an sFlow agent.
! Enable sFlow.
configure terminal
 sflow enable
! Set the agent IP address.
 sflow agent ip <agent-ip-address>
! Set the collector IP address.
 sflow collector id <collector-ip-address>
! Modify the max datagram size if necessary. Default: 1400 bytes.
!
! Configure packet sampling per port.
! Select the switch ports.
 interface <port-list>
! Enable packet sampling and set the sampling rate. Default: 0=disabled.
!  sflow sampling-rate {0|<256-16777215>}
! Configure the max header sample size (in bytes). Default: 128 bytes.
  sflow max-header-size <14-200>
!
! Configure counter sampling per port.
! Select the switch ports
 interface <port-list>
! Configure the polling interval in seconds. Default: 0=disabled.
  sflow polling-interval {0|<1-16777215>}
!
! Configure SNMP.
! Enable the SNMP IPv4 server (enabled by default).
 snmp-server ip
! For SNMP v2c, create an SNMP community with read-write access.
 snmp-server community sflow rw
```

Using the configuration script file

1. Create a script file (called sflow.scp in this example) and place it in a TFTP directory accessible to the switch. Include the commands above, comment out (with an "!") or delete lines you do not need, and replace values with ones appropriate to your network.
2. Load the script file from the TFTP server to Flash memory on the switch:

   ```
   awplus# copy tftp://<tftp-server-ipaddr>/sflow.scp sflow.scp
   ```

3. Activate the script:

   ```
   awplus# activate sflow.scp
   ```

C613-22053-00 REV E

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com