Solution Brief

Using sFlow® to Manage Your Wireless Network

Stuart Johnston, InMon Corp., April 18, 2008

1 Introduction

sFlow® (www.sflow.org) is the industry standard for monitoring network traffic. You have probably come across sFlow already, as it is implemented in many ProCurve switches. You might have tried it out, using the Traffic component in ProCurve Manager Plus, or using a specialized product such as sFlowTrend from InMon Corp. Perhaps your business has now come to reply on the detail and quality of information that sFlow is able to provide on the traffic flowing through your network.

The latest enhancement to sFlow adds more information to help manage a wireless network. If you are responsible for running a wireless network, you will appreciate how difficult it is to maintain security, manage channel and access point location, and utilize the available bandwidth as efficiently as possible in a wireless network. However, it can also be very challenging to understand how a wireless LAN is being used.

sFlow for wireless is designed to help address this problem. As well as the usual detail of traffic that you get with sFlow on a wired network, the wireless extensions allow visibility into the wireless specific attributes of the traffic, for example the channel used for transmission and reception, the SSID in use, and the encryption algorithm used. Also, if the traffic was encrypted, the sFlow data can contain the unencrypted payload to allow deeper visibility.

The first implementations of sFlow for wireless are, on the access point side, in the ProCurve Wireless Edge Services xl Module and WESM zl module, and on the software side, InMon's sFlowTrend (www.sflowtrend.com). A previous article from ProCurve, available at http://www.hp.com/rnd/itmgrnews/going_with_sflow.htm, gives some more information on sFlow for wireless, and the announcement of the products supporting it is at http://procurve.com/news/wireless_monitoring_standard.htm.

The remainder of this article will explain how sFlow for wireless can be used, and give some examples.

2 Getting Started

As with all ProCurve switches that support sFlow, the wireless access points (we'll call the Wireless Edge Services Module an 'access point' for simplicity here) support the sFlow MIB. This makes it easy to get going with sFlow. The software that you are using to analyze sFlow, e.g. ProCurve Manager Plus or sFlowTrend, will use the sFlow MIB to configure the access point with its IP address, and other relevant information.

To allow it to do this, the software must be told that you want to monitor the access point and configured with the correct SNMP *write* community for the access point.

In sFlowTrend, Use *Tools→Configure switches*, then *Add* a switch. Enter the IP address of the access point, and ensure that the write community is correct. Make sure that the *Configure sFlow via SNMP* checkbox is selected, and press *OK*.

Once you have configured all the access points that you wish to monitor, they will start sending data to the software. Wait a few minutes for enough data to be received, then you can start monitoring the traffic on your wireless network.

3 Monitoring Your Traffic

After you have been collecting data for a few minutes, take a look at the network traffic on the access point, to make sure everything is working. If you are using sFlowTrend, select the

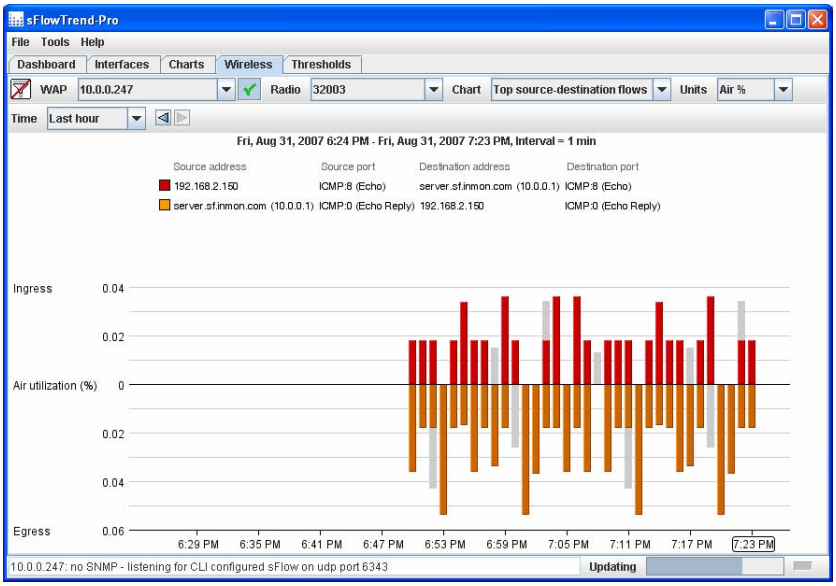
Wireless tab, and then select the access point in the *WAP* selector. You can then view the traffic on the access point in different ways – for example, to see the top sources of traffic on the access point, select *Top sources* in the *Chart* selector. This will show the top 5 sources of traffic, minute by minute. Even if the traffic is encrypted on the wireless LAN, sFlow for wireless allows the traffic to be examined by source, destination, protocol, connection, etc. Traffic that is not from one of the top 5 sources will be colored grey. If the bulk of a minute is taken up by one source, then you might consider investigating that host further. We'll look at different ways to find out how or what is using the bandwidth on the network.

3.1 Understanding Network Utilization

Often, the first place to start in viewing the health of the network is with interface counters. The counters provided through sFlow are similar to those that you may access through SNMP, however the way that sFlow exports the counters is much more efficient. This means that the counters can be continually provided from many switches to a management station, without impacting the network or switch performance.

Because counters are defined per radio in a wireless network, just as they are per port for a wired network, before you can view the counters in sFlowTrend, you must first select the radio that you are interested in. Let's assume that your users are complaining about poor performance when they are connected to one specific access point. Select the access point in the *WAP* selector, then select a radio using the *Radio* selector You can then select the *Utilization* chart and quickly look at each radio on the access point, to determine if it is heavily used.

If you find a radio that has very high utilization, then the next obvious question is, "Why?" The counters are an excellent way of viewing the overall summary of part of the network, but the real power of sFlow is the ability to drill down into the detail of a radio (or wired port), and see what is actually using up the bandwidth. To do this, select one of the other charts in sFlowTrend – for example, *Top sources*. This shows the sources of all the traffic on this radio. Select *Air utilization* in the *Units* selector to show each source's traffic by the percent of available bandwidth.



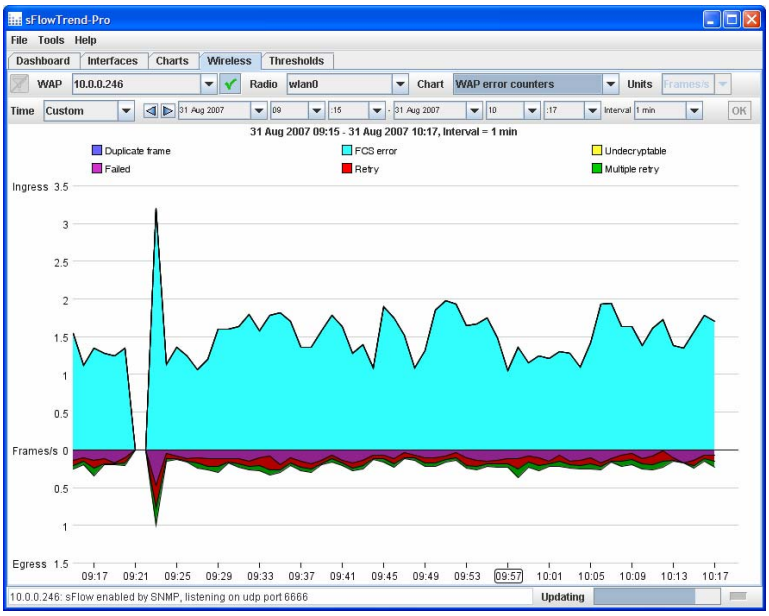
If you see one or two hosts taking up most of the bandwidth, then they are likely to be the culprits. Of course, the traffic they are sending could be legitimate, but if they are using up

most of the bandwidth on the wireless link, and are making it difficult for other users to be productive, then perhaps it would be more appropriate for them to use a wired connection. Or maybe they are engaged in an inappropriate activity, downloading streaming video for example. You can drill down further to try to understand what people are actually doing by selecting *Top connections*. This will show the source and destination IP address, and also the TCP or UDP ports that are being used. Again, you can look for the biggest contributors to the overall utilization, and address the problem as appropriate.

Perhaps you see overall high bandwidth utilization, but each of the sources themselves is very small. This can happen just because your wireless network is very heavily used – lots of people are connected, and although none are using significant bandwidth, when they add up the network is heavily utilized. If you see this, then perhaps you need to add an additional radio or access to the network to increase capacity.

3.2 Specific Wireless Charts

With sFlow for wireless, additional wireless counters are available. These include wireless errors, and specific wireless control frames. Of particular interest are the wireless error counters. If you see a high count of one particular error, then it may be worth investigating further. Often, the retry count will be quite high, as other wireless devices connected to the network, or from adjacent networks, can cause interference which results in retransmissions. If it is very high, though, it might mean that you should reconsider the channel allocation of your radios to avoid conflicts.



The radio ports available for the ProCurve Wireless Edge Services Module, and the Access Point 530, each support multiple different wireless networks standards at the same time – for example 802.11a and 802.11g. It is useful to understand how much traffic is being sent over each protocol, especially in the case of 802.11b and 802.11g. Using the *Top wireless versions* chart you can see the traffic categorized by which protocol it was sent on. If the bandwidth is heavily utilized and you see that a substantial proportion of traffic was sent on 802.11b, then that could be cause for concern since 802.11b makes less efficient use of the bandwidth than 802.11g. Maybe one or two users are still using 802.11b, and upgrading them to 802.11g would be a cost effective solution.

sFlow for wireless includes a count of the number of stations associated with each radio, which means that your analysis software can keep track of a history of associations. For example, using the *WAP associated stations* chart in sFlowTrend, you can look back in time at how many stations were connected to this radio at any point. This can be useful when you are trying to diagnose a problem, for example to see if the number of connections was abnormally high.

3.3 Security

As well as the normal security analysis that is possible with sFlow, sFlow for wireless also allows you to examine the encryption in use on each link. This is very helpful information if you are trying to ensure that all of your clients are using an appropriate secure algorithm. By selecting the *Top cipher suites* chart you will see the traffic broken out by the encryption algorithm used. One word of caution here – traffic coming from the wired interface on an access point is not encrypted using an 802.11 encryption scheme, so you may see some traffic that is marked as *None/unknown*.

4 Exploring Further

There are many new features that are specific to wireless networks, that can help you get a handle on what's really happening. Also, of course, you are not just limited to using the new features; all of the traditional monitoring that is possible with sFlow is now available for wireless devices. More sophisticated queries are also possible using the wireless fields – for example, you could view *Top connections* filtered by the wireless protocol used (an example would be if you wanted to migrate users from 802.11a to 802.11g, then you might want to filter by 802.11a to determine which systems are using it).

Give sFlow a try for your wireless devices – it is often an eye-opening experience to see what traffic is flowing on your network.