Managing LAN & WAN Bandwidth

Full Control Networks Whitepaper

One of the most popular questions people ask the network team is "Are we running out of bandwidth?" closely followed by "Is there a bottleneck?". This is more likely with regards to the WAN than in a modern switched LAN network, but traffic loading can be an issue. The question is how do you look into these problems?

There are two main technologies out there for monitoring bandwidth; SNMP and NetFlow. In theory they compete but in reality, they are quite different and a lot of people have both. Here we try to position these solutions and give you reasons for one vs the other or if you need both.

SNMP Tools

The most popular tool for monitoring bandwidth. In fact, SNMP based tools are probably the most common network tools in the world and range from "free" download versions to sophisticated Data Centre management tools that may claim to be the only tool you need.

SNMP tools gather their statistics from counters held inside your network hardware, known as MIBs. They poll specified key devices, such as switches and routers, for their counters, get a number, then poll again a couple of minutes later and plot the results. These solutions are great for up/down availability and trends, but remember, due to the sampling rate they use, they will tend to understate the situation. Hence, any interface that says its 50% busy is definitely worth investigating.

This is fairly simple technology and as such it is very widely supported by almost all networking hardware. There are a lot of solutions on the market, which also keeps the price low, in fact even the freeware tools can provide good basic data.

The downside is that all the data gathered is sourced "second hand", the packets themselves are never read directly. So, although ideal for providing baselines and generic statistics, SNMP tools can't tell you who or what is the cause of a traffic spike.

Flow Based Solutions

The first thing to mention is that there are several different types of Flow out there; NetFlow, sFlow, J-Flow, IPFIX etc and for the purposes of this article we treat them all the same.

Flow information comes from the Routing cache of Layer 3 networking devices, typically Routers, Firewalls, some layer 3 switches, Load Balancers etc. Some VM switches are now also reporting Flow information from your virtual environment too.

As these devices receive data frames, they read the IP information in the frame and make decisions about what to do with it based on the policies they have. If the device supports Flow exporting, you can set it to send this routing cache out once a minute to a collector (server with a database on it) which can turn the data into pictures, tables and graphs.

01677 428700
info@fullcontrolnetworks.co.uk
www.fullcontrolnetworks.co.uk

FULLCONTROL NETWORKS

At this stage there are a few key points to note. Firstly, as NetFlow contains IP layer information these solutions can tell you who is talking to who (something SNMP tools can't). Secondly, Flow data contains information such as application port numbers, so you can also report on what applications are using the bandwidth, again SNMP tools can't. So, at this stage NetFlow seems to contain some of the killer information about what's exactly using up all your bandwidth.

However, there are some drawbacks. Only a limited number of devices in most networks will actually support Flow exports compared to SNMP. In a WAN network this is less likely to be an issue, but in a layer 3 switched network support for Flow can be patchy at best.

The next issue is that Flow data is also effectively second hand. It is also relying on the network hardware to pass the data along, rather than reading the data directly. The polling intervals are also very rigid at 1 minute, whereas in SNMP you can get options to wind them up or down depending on what requirements you have.

The last point is that there tends to be more data to handle, more fields to process with Flow exports than SNMP, so the databases involved are more cumbersome. Generally, the more you pay, more of the Flow records get processed and reported on. Cheaper solutions tend to focus on the top 5 fields around users and applications and put the rest of the Flow data into the database unprocessed. Which can be confusing as your dashboard is only seeing part of the picture, and next to useless if you are using Flow records as part of some security or compliance solution.

SD-WAN

What is interesting is that NetFlow tools have quickly embraced the concepts in SD-WAN. Effectively they see SD-WANs as just another interface on the router (even if its virtual) and can report on the IP traffic on that virtual interface in the same way as a physical one. This means if you start running a hybrid WAN environment, there is no real impact on NetFlow monitoring, it just still works.

SNMP tools can report on an SD-WAN interface, but it's the limited up/down and packet count based utilization stats only. If you have gone to the trouble of using SD-WAN then you are probably going to want to know who and what is using those links, hence NetFlow offers that level of detail.

Network Planning and Sec Ops

Flow solutions effectively see all the conversations in the network, IP address to IP address. This means the better solutions (which process all the data on receipt) can deliver more forensic style roles as well.

Planning and designing changes to your network are often hampered by a lack of information as to which devices actually talk to specific sites and servers. Here NetFlow solutions (such as

01677 428700
info@fullcontrolnetworks.co.uk
www.fullcontrolnetworks.co.uk

Scrutinizer by Plixer) allow you to generate reports showing the activity of specific devices or sites (by subnet) so you can see all the IP connection information you need to manage as the router network is changed.

Security solutions are increasingly using NetFlow as a key source of information now too. As the Flow records see all the IP connections being made (again you need a better NetFlow tool for this) they can pick up patterns of connections across the network and see PCs acting like servers or devices making thousands of calls to outside IP addresses, which raise concerns.

Most of the better NetFlow tools will now offer security-based features based on this Flow information and will have some way to highlight unusual traffic patterns and misbehaving devices, Plixer's NTA (network traffic analytics) is a good example of this.

So, which one for me?

In reality most people are happy with SNMP solutions for the reason that a greater percentage of their network hardware is providing data in some fashion, it's the one that has the widest reach across the network. The limited accuracy tends to be over looked and in most cases that's ok, just don't be surprised when occasionally your SNMP solution is reporting all green lights but people are still throwing stuff at the network team across the office. Just understand that SNMP tools have their limits and you might need to move onto a more detailed solution at times.

NetFlow comes through when you have a lot of remote offices or a large WAN budget and you really need to manage the capacity tightly. The extra detail it provides on the IP addresses, applications, interfaces etc is vital in working out whether you need to spend more budget or change the routing polices. Then the cost of these solutions becomes manageable against your budget and how it can help you spend more wisely.

Network migrations are also a good reason for NetFlow data, whether its cloud migrations or managing physical changes to your design, the IP level connection information can be key here. This extends to any thoughts about using SD-WAN, if you are going to that trouble then again, the NetFlow information is going to be key to manage this, SNMP just won't tell you what you want to know.

If the network team has a growing Sec-Ops responsibility, again NetFlow is a great source of information for you. Most of the established Network security solutions have been using it for years and your network team will be pretty comfortable with the IP based information its going to throw at you.

01677 428700
info@fullcontrolnetworks.co.uk
www.fullcontrolnetworks.co.uk