The Risk of using a Laptop for Packet Capture

Full Control Networks Whitepaper

The most popular packet capture solution in the world is WireShark. It's no coincidence that it's free, but it is also quite capable. Even the more expensive analysers with extended problem databases and issue recognition features all support the WireShark file formats, which have become a "defacto" file standard these days. However, whether the software is free or paid for, it can only be as good as the information that gets passed up to it. This is where we need to be careful.

The vast majority of us will be using Wireshark on our laptops, a few people use dedicated PCs or servers but there is an increasing trend in using some sort of specialist capture engines, why is this?

There is a traditional argument about the performance of laptops and their ability to capture accurately. Laptop performance keeps improving, but the amount of data in our networks keeps increasing too. Diehard packet engineers will always look to their laptop in these situations but the one area that seems to be defeating them is the sheer volume of packets that a simple 5 minute capture can generate.

So, the questions are, is my laptop still a reliable way to troubleshoot these issues and how can I over-come the problem of having several million packets to sort through?

Here is our advice.

Real-time vs Historical Analysis

We need to start with the approach you're trying to take. If you're troubleshooting in real time and you know the device that's having issues, then the using a laptop can be of value.

Firstly, you know where to plug it in, so you can limit the amount of data it is going to see. Even if you are forced to connect your laptop near the router, you can quickly put an address filter in and keep the traffic focused on your target device.

Secondly, assuming the issues are on-going then the real time capture will contain information related to this issue, so you have relevant information to process and try and get to the root of the issue.

However, that is a best-case situation. A more typical state of affairs will involve you chasing around the network trying to pin down some issue that comes and goes. Here you can try and pick some central point to gather the packets from, but are faced with a mountain of packets from lots of devices whilst you wait for the situation to re-occur.

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

FULLCONTROL NETWORKS

Worse still the problem does re-appear but you have 10 million packets to post filter to get to the bit you want. Been there, done that! 10 million packets does not take long in a modern network, but even with some i7 processor laptops, loading these files can be 5-10mins at a time, it's not easy.

It's this historical analysis that's the difficult one, when you think about it, the phone never rings before the problem occurs!

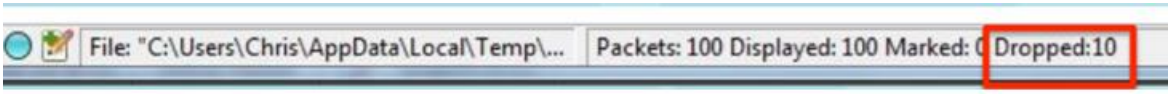
The Issues with Accuracy

The first thing to note is your laptop was never designed to capture packets, neither your server to a lesser extent. Although most laptops are getting better at operating somewhere near the 1Gig interface, it's pretty easy to make them to drop packets by sending fast bursts of data at them. This is exactly what will happen when you have data from a faster device (say a 10Gig attached server) sending data to a slow device, like a 1Gig PC or a 100Mbs router.

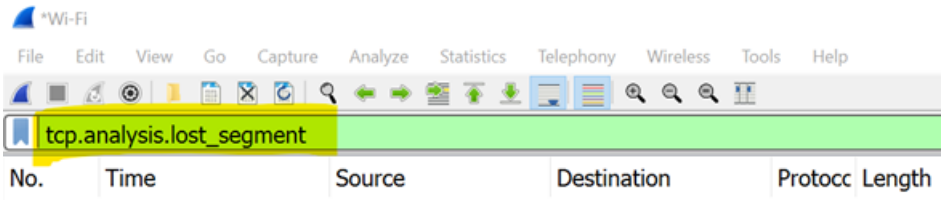
NIC cards these days are getting towards 80-90% of the stated interface speeds, however it's pretty easy at these speeds to overrun the buffers and drivers that copy the data to disk, and hence you lose frames.

With a TCP based application, this is not a huge issue as the TCP protocol will send corrections for lost packets, however if the data did get to the target device but your laptop did not manage to copy it, then you have an issue. You can think the packet was lost, when actually it got through, complicated stuff!

At the bottom of the Wireshark capture is the first clue, a counter that is part of the NIC card drivers, which notes that there was a frame to be read, but the buffer had not been emptied yet, hence its discarded or dropped, see below.



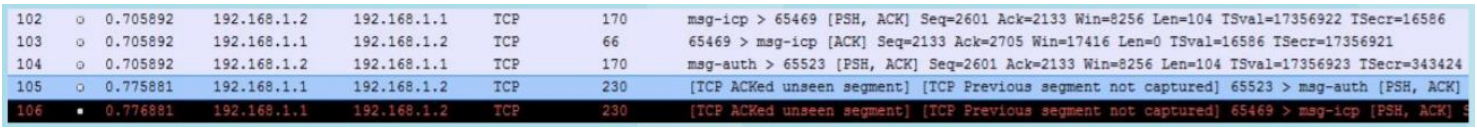
There are better clues to the situation if you can use the Wireshark filters. This is where the Wireshark community are very helpful in posting tips on how to get the best from the tools. Applying the following filter before you analyse the capture will highlight the missing parts of the TCP threads in your capture.



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

FULLCONTROL NETWORKS

Even more information can be seen in the capture itself. The screen shot below shows that Wireshark has seen an ACK for a frame it never registered, so the end device is OK but your capture is not, confusing! This is something we see a lot when peoples send us their captures to look at.



Another area to be aware of is the accuracy of the time stamping. Wireshark can show you to 6 decimal places in each second when the packets turned up, but this is only as accurate as the NIC and its driver. This is where laptops are acceptable to closer to 2 decimal places and the rest is pretty meaningless. If you need greater accuracy than this, you need a dedicated hardware capture solution, period.

How you can improve the performance of your laptop to capture packets

If you really are suffering from dropped packets and missing segments, there are a few things you can do to help.

- You do need a decent laptop for this work; 64 bit architecture, fast processor, memory and disk all come into play.
- Don't have any other windows open, each one reserves memory and takes up CPU cycles so best they are not there at all.
- Don't use the update packets in the live view – this is very processor intensive and will compromise the resources in your laptop to capture and store packets in the first place.
- Don't use live capture filters – again this suck resources away from the core ability to just capture as much as you can. Leave all filtering to post capture.
- Increase the size of the of the capture buffer – at the time of writing the standard install of Wireshark allocated a buffer of 2MB per interface on my machine, or to put this another way about 2000 packets before it starts to over write the data. That's not a very long time-window if you are trying to solve an intermittent problem.

These tips will squeeze out a bit more from your laptop, the clues above around dropped packets and missing segments will give you a better idea of how well your device is doing. As a general rule you want errors to be no more than 1-2% to trust the quality of the information you have.

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

So, can I use my Laptop, or not?

Sort of. It's really a question of how you use your laptop in these situations. If you're just looking at specific machines (1Gig connected but not too busy) then you will be OK to continue like this. However, what we've noticed other people doing, and now doing ourselves, is capturing the packets with something more substantial, finding the bit of the capture we are interested in and then using our laptops to see what's going on. Trying to do this with a laptop is generally too difficult, too slow and not accurate enough.

There is a historical point here, which is that dedicated capture solutions have been around for many years, but they have been very expensive, usually for two reasons:

- They come wrapped with Application Performance software which has a high-ticket price
- They guarantee 100% captures to micro second accuracy, which 99% of us don't need

There are a few offerings in the market place now which offer a dedicated capture engine, that's not too expensive, that lets you use the laptop and Wireshark format that you know and love to sort the rest out. Some of these offer a quick summary of what you've captured - allowing you to cut down the section you need to load into your laptop for that more detailed view. The days of seeing packets come through live are really gone. They come through too fast and they take up too much of the device resources to be anything like accurate or useable.

An example could be a 1Gig device ticking over at 100Mbs, with you trying to capture an intermittent issue and trying to look at 5-minute blocks of data. If we use an average packet size of 1000bytes this equates to over 3 million packets, which is just too many to process and probably won't load onto your laptop anyway.

A more realistic approach is to find the 10-minute window you are interested in, filter it down to maybe 1 minute when your problem occurs or a particular conversation with issues, then load that into your laptop. Now you are probably down to 100K packets which your laptop and Wireshark can process in reasonable time as you work through various threads investigating your issue.

What about SPAN/Mirror Ports?

Let's be clear from the start, these have been a life saver for many a network engineer trying to find out what's going on. However, this approach is not without its issues.

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

Switches do not have unlimited amounts of SPAN ports and the more this goes on the more times I've had to ask to "borrow" the SPAN port which is being used for something else, usually VoIP call monitoring solutions or some sort of IDS.

This is poor in many ways. Poor design as permanent monitoring solutions should be tapped to make them permanent. And no-one wants gaps in their IDS/VoIP records every time you need to troubleshoot an issue.

Either way, the issue SPAN can't help you with is the volume of data you still end up having to sort through. You might have isolated the issues to a specific interface or VLAN, but you are still faced with huge amounts of data to sort through before your laptop will even load the file into Wireshark.

Getting the packets into some sort of capture engine and then a basic sort through before Wireshark is still a much easier approach.

Summary

If you know the issue and the device and the link it not too busy, using your laptop to capture data is probably going to be fine. However, is that the most common scenario?

Even if you do have a pretty good idea of the IP address of the affected devices, it's the window in time to capture your issues that's the more common problem. As suggested here you can rack up millions of packets just waiting for something to happen and then what do you do? In theory you have good data to investigate, but in practise you have too much "noise" surrounding it.

You don't have to invest in one of the 6 figure APM solutions for these one-off issues. But you might need some sort of high-speed capture and quick filter solutions available on the market, that can send a subset of your data (in reality 1000s of packets still) for you to push through Wireshark.

There are now intelligent taps and packet brokers which can provide a moderated feed for your laptop. Some allow filters, most have buffers, but basically all of them will be better at the job of capturing packets than the NIC card in your laptop. At Full Control Network we use Datacom products.

If you want to go that bit further, some of these capture engines have simple high performing DBs which allow the data to be stored and summarised (usually as web pages). Then you can be even more selective about which bits you load onto your laptop for analysis. At Full Control Networks we use the Allegro Packets solutions, some of which are just the size of a paperback book!

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