Wireshark tracing for fault finding

237 Darren Wheeler Mon, May 13, 2019 Technical documents 2607

How do I perform a Wireshark trace?

If you have been asked to complete a wireshark trace this is because your reported fault needs further inspection from site, these are typically asked for when the report is call quality or transfer difficulties. It is important that you start the wireshark trace before starting the call, and end the trace after both parties to the call have hung up.

Requirements

- Ethernet Hub or Port mirror capable switch
- Wireshark installed on a decent computer with a large drive capacity that can see the phones

Hub

An unsophisticated device plugged into your existing network, in this case between phone and Internet connection. As a hub does not intelligently switch or manage packets a pc plugged into the same hub can view everything passing through making monitoring 100%

If you do not already have a hub, one can be purchased for around £20 from online stores such as Misco, Dabs, Ebuyer or Maplin.

There has to be an element of downtime as the hub is connected into the network.

Port mirroring

To forward the copy of all in-bound and outbound traffic (packets) from one port (or multiple ports) to another port designated by an administrator, simultaneously without affecting the normal operation of a switch. This is required for monitoring the network traffic, monitoring the performance of a switch and other applications.

There are disadvantages, port mirroring can cause buffer overflow and dropped packets since all the packets go through a buffer in the switch. So, accurate time sensitive measurements like jitter, packet gap analysis or latency measurement can become difficult. Also, there is additional load imposed on the CPU of the switch affecting the operational performance of the switch.

It is known the Mikrotik devices, in partiular RB951 perform this function well.

Wireshark

The application Wireshark is a well known free support utility and available for download at Wireshark Download, you will need to select the most appropriate version for your computer.

When running all seen packets are dumped into a .pcap file which can then be saved and sent to administrators for inspection. As all packets are dumped the saved file can become very large, below are instructions on how to configure for best practices.

Configuring Wireshark

To ensure the file is sent without issue and easily identifiable please follow below steps;

1. Under the Capture Menu, select Options
2. Select the Interface used, more than likely Ethernet
3. Leave promiscuous mode on all interfaces checked
4. Save the file as CustomerName_Date in a memorable location, where CustomerName is your business name and todays date.
5. Tick Use Multiple Files and increase to 2 megabytes
6. Stop capture after 2 hours, just in case forgotten to stop. Removes accidental fill up of your hard disk, previous captures show 1MB per minute.
7. Click Start

Perform test calls to simulate the issue

To stop the capture click the red square in the toolbar of Wireshark.

Submit troubleshooting files

Assuming you have successfully experienced the issue whilst Wireshark was running, you will need to send an email to support@ic.co.uk with the attached files.

In this email you should detail:

- full telephone number (external and internal), and username of both the party making the call (caller), as well as the party receiving the call (callee).
- detailed description of the nature of the problem encountered on the call, and which parties on the wireshark captured call perceive the issue (the caller, callee or both.
- which calls are being affected by this problem (detail particular extension/s, sites or external parties, is the problem specific to times of the day / days of the week)
- the frequency with which the problem occurs (eg infrequently, several times an hour /

day, on all calls)

- the date and time the phone call started (where possible give us this date / time from the details recorded in the wireshark file)
- date and time the problem was first encountered

The wireshark trace should capture the entire phone call from start to finish otherwise troubleshooting is not possible.

Online URL: https://kb2.ic.uk/article.php?id=237