robustOS

Sniffer App Datasheet

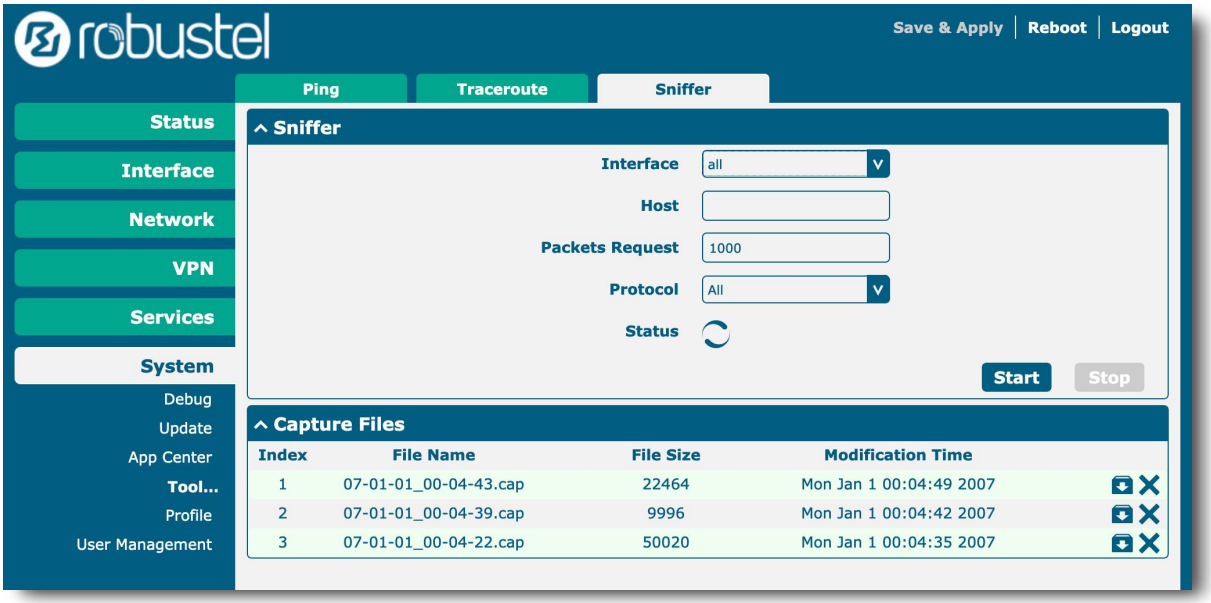
Sniffer is a critical diagnostic tool for your IoT application available in every Robustel router as standard

The 'Sniffer' Application included in all Robustel routers, allows the user to capture the actual data travelling over the 3G/4G network for subsequent analysis in the amazing "Wireshark" application software. The combination of these free capture & analysis tools can help sanity check that only the data that is meant to be transmitted / received is being sent and sources of erroneous communications can be prevented.

This capability can save thousands of dollars in airtime bills, and help to find bugs in client /server communications prior to a mass deployment of 3G/4G routers.

Introduction to the Sniffer App

In the "Tools" section of the "System" menu in the User Interface of all Robustel routers is a service called "Sniffer". By selecting the WWAN interface in the dropdown menu and entering the number of packets required to be captured, it is possible to start to capture the cellular data traversing the cellular interface of the router – independent of source or destination IP addresses. Everything that costs you money in data bills can be captured.



Filtering can be applied by selecting a specific Protocol to be captured although in most instances, capturing all protocols is the best starting position.

Once the trace is complete, the file (*.cap) can be downloaded to your PC for further analysis using a tool like Wireshark.

Robustel's technical team can help you interprate your Sniffer results
For more information on Sniffer please contact your Robustel Sales Respresentative or Distributor

robustel
Email: info@robustel.com
Website: www.robustel.com

robustOS

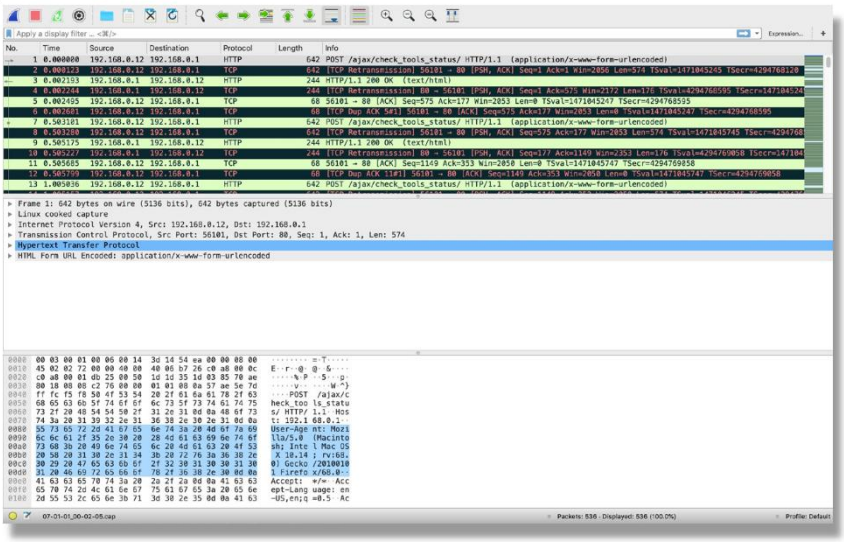
Sniffer App Datasheet

Analysing RobustOS Sniffer results with Wireshark

The ultimate 'free' network Analyser

Once Wireshark is installed on your PC, you can open the *.cap file downloaded from your Robustel router to see the raw data as transmitted over the cellular connection packet by packet. Whilst a full description of the capabilities of the Wireshark analyser is way beyond the scope of this document.
Below are some of the key tools that can quickly help you to solve problems in your IoT application:

- Conversations
- IO Graph
- Follow TCP Stream
- Detailed Analysis



Conversations

The Conversations view in Wireshark allows the statistics of every individual UDP and TCP conversation that is taking place to be viewed individually. Sorting conversations by data usage will instantly highlight which pairs of IP addresses are responsible for the most data usage and can subsequently be targeted to see if a reduction in verbosity hence data costs can be achieved.

IO Graph

Viewing the IO Graph of a capture file with "absolute time" switched on allows a very quick visual indication of when data consumption is at its peak – this can provide some clues as to when and where data consumption issues may exist. Conversely, periods of zero data transfer can be identified to help diagnose communications problems and their root cause.

Follow TCP Stream

Any over the air communications exchange that uses TCP as its bearer can be easily analysed by applying the "Follow TCP Stream" filter (encryption could make this more difficult). This powerful tool allows conversations to be viewed in one direction at a time with the actual data payload (including HTTP) able to be read and understood in plain English on the screen. This is especially useful when proprietary serial protocols are being sent over the air and there is a problem with checksums or turnaround time of RS232/RS485 based ASCII protocols.

Detailed Analysis

Robustel's tech team can assist with Wireshark analysis & suggestions on how to resolve established communications problems as required. A brief investigation can typically be provided free of charge as a gesture of goodwill. More extensive fault-finding is available as a chargeable service.

Email: info@robustel.com
Website: www.robustel.com