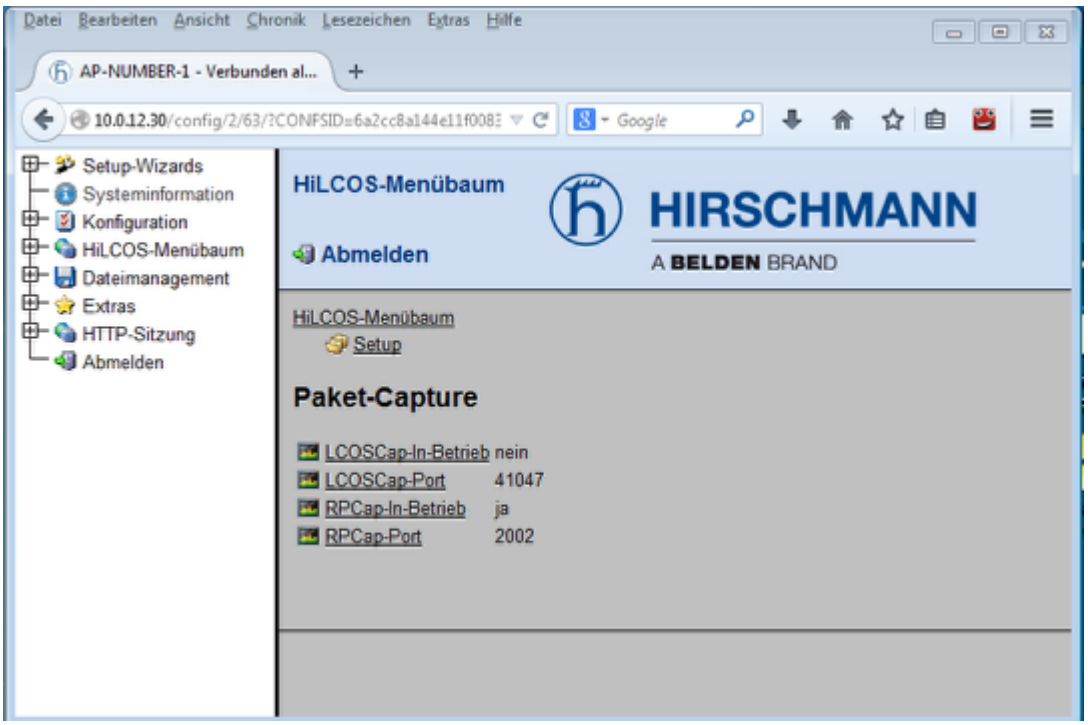
How to remotely capture the trafic of an Open BAT interface with RPCap function and Wireshark

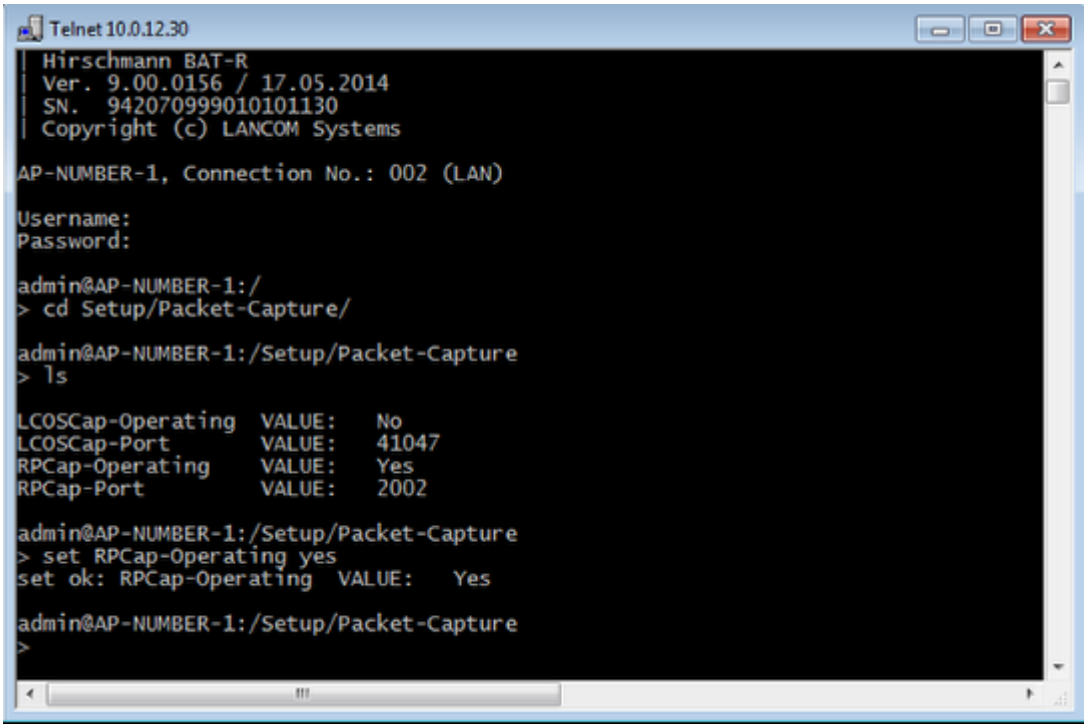
- 2018-02-21 - BAT, WLC (HiLCOS)

This lesson explains via a few steps how to use the RPCap function to capture trafic remotely on specific interface(s) of the BAT devices (rel 8.90)

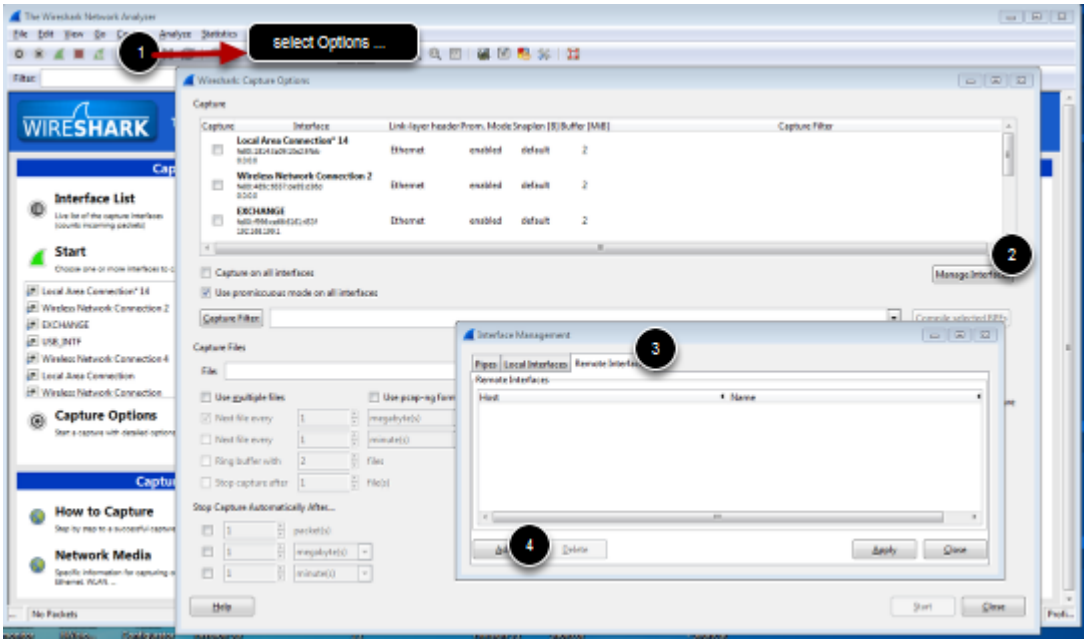
Enable RPCap on the BAT using the web interface or per CLI



You can also change the RPCap port, per default it's 2002

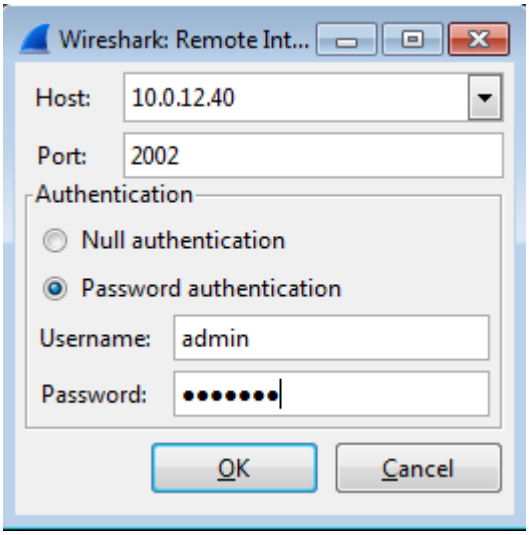


Add remote interfaces in wireshark options



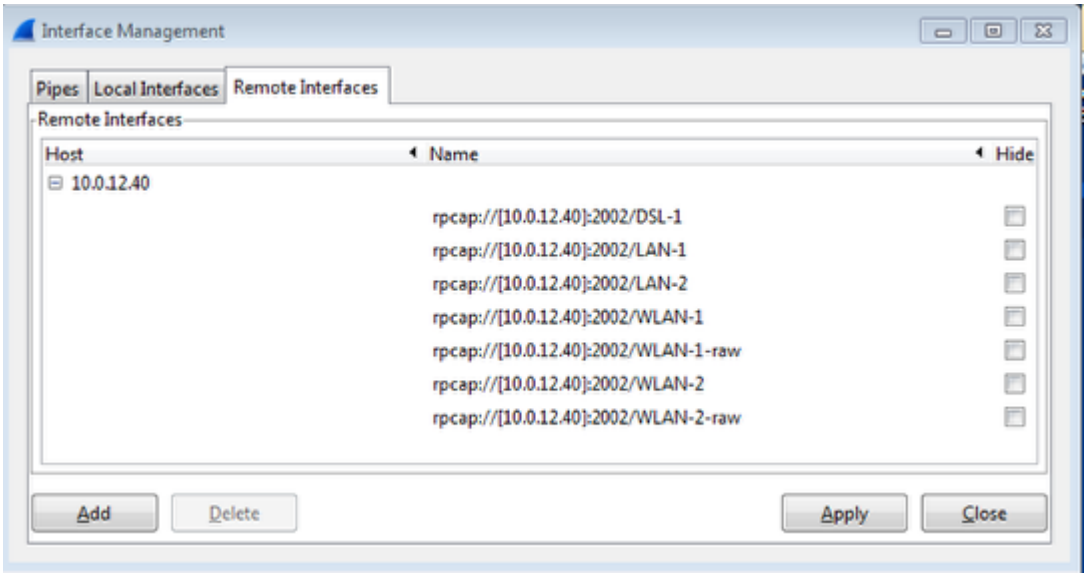
From Wireshark main Windows, open the Capture Options window (Capture/Options...). Clic on manage Interface and select the tab Remote Interfaces and clic on Add

Configure the BAT as remote device



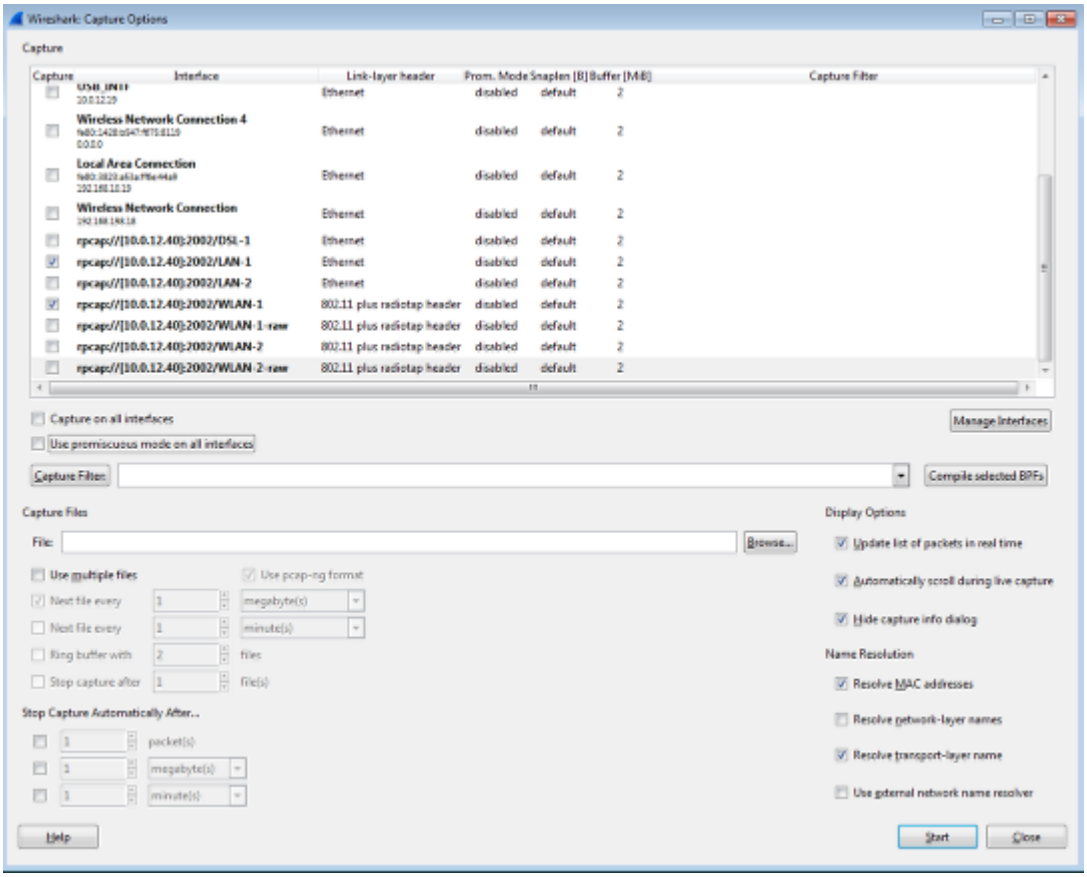
Give the IP address of the BAT, the RPCap port relevant username and password to access the device then clic ok

RPCap gives all the available interfaces on the remote device



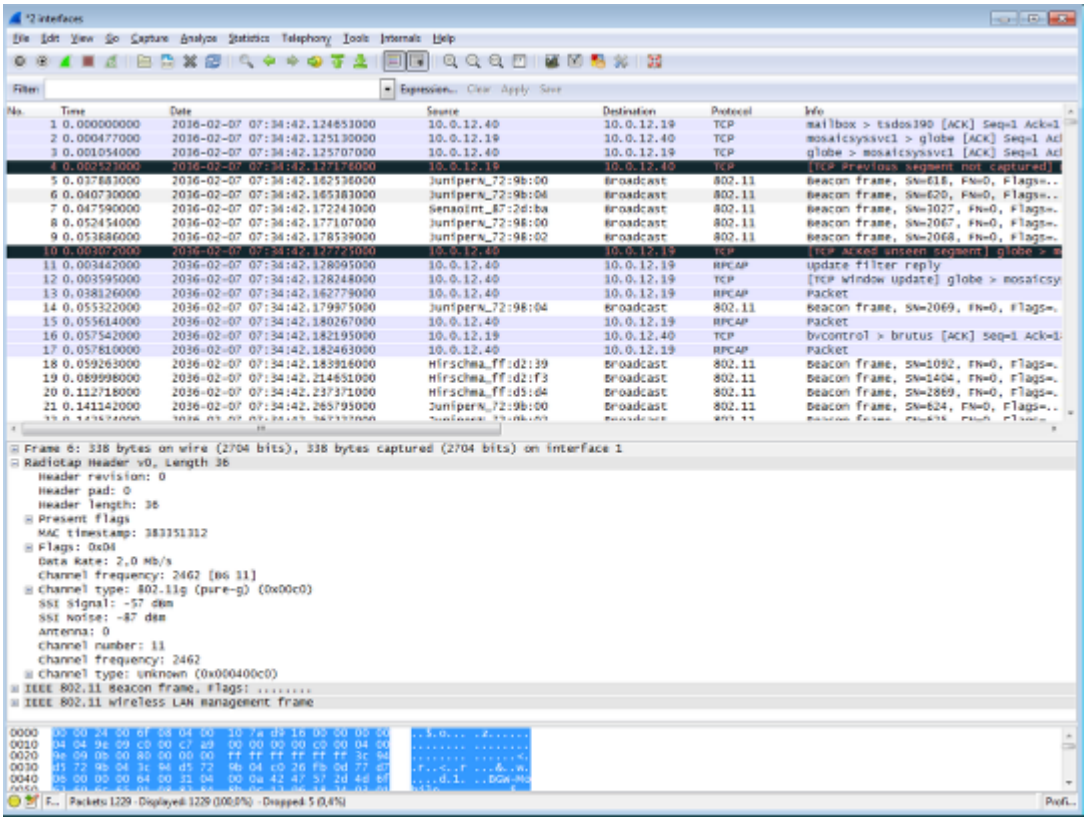
clic on Apply and Close

From the Capture option Window, the remote interfaces are now available, select the one(s) you want to capture the trafic on.



In this example trafic going through LAN-1 and WLAN-1 will be captured. Then just clic on start

Result view



RPCap tunnels the trafic between the BAT and the capturing station. Packets from WLAN-1 with radio header and packets from LAN-1 are in the same capture but can be read separately filtering the interface id.