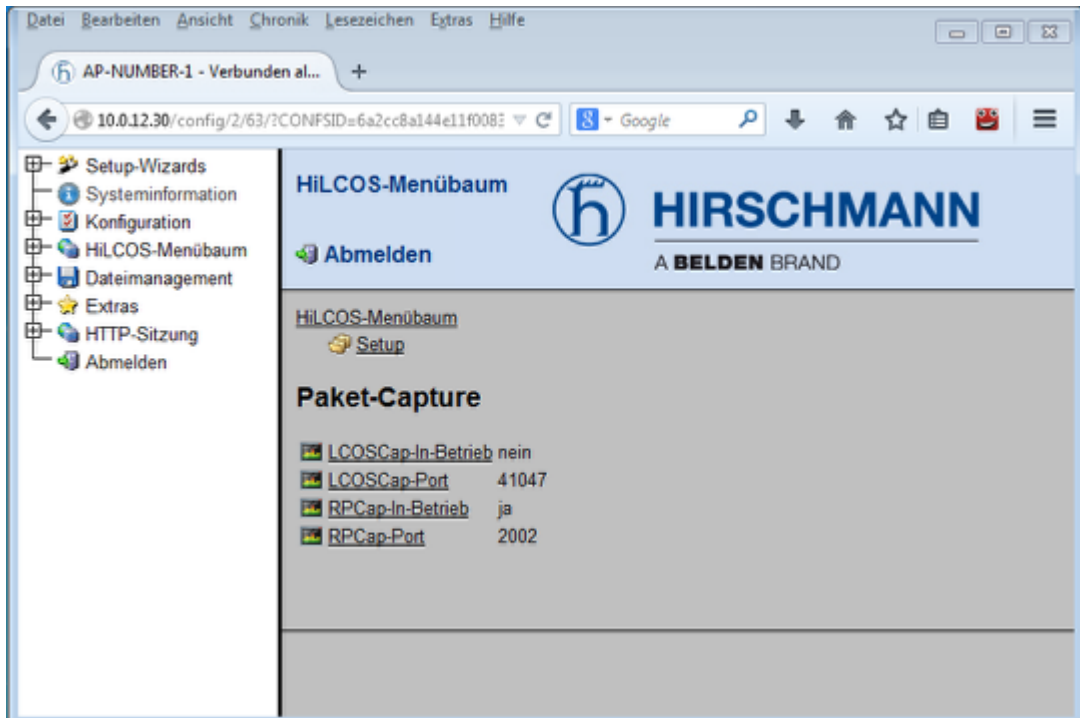


How to remotely capture the traffic of an Open BAT interface with RPCap function and Wireshark

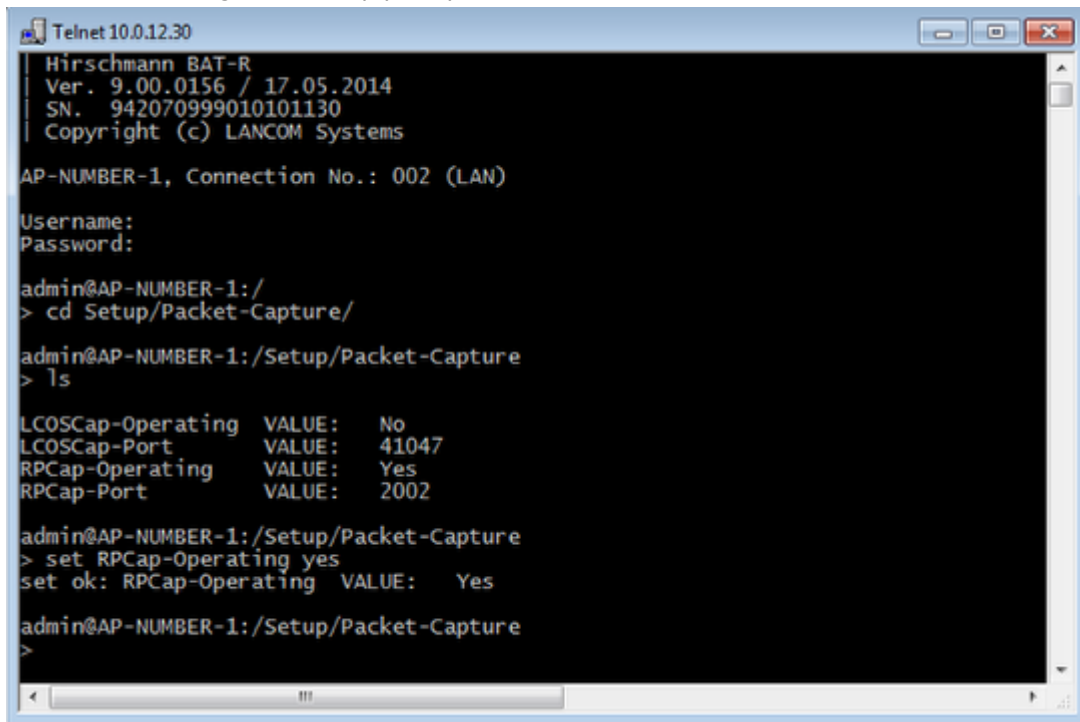
- 2018-02-21 - BAT, WLC (HiLCOS)

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

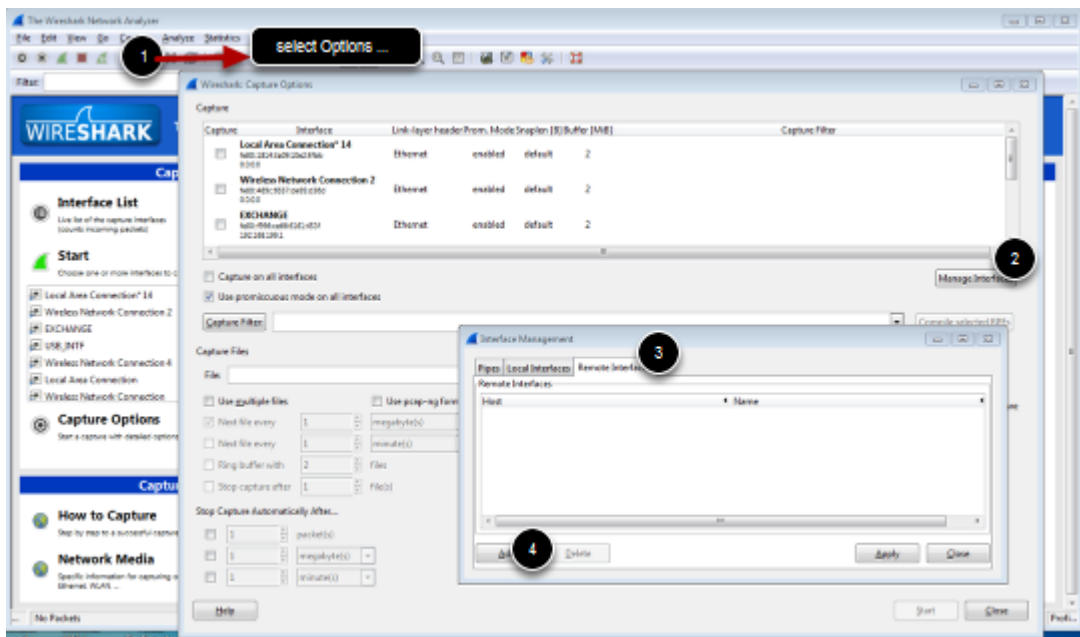
Enable RPCap on the BAT using the web interface or per CLI



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

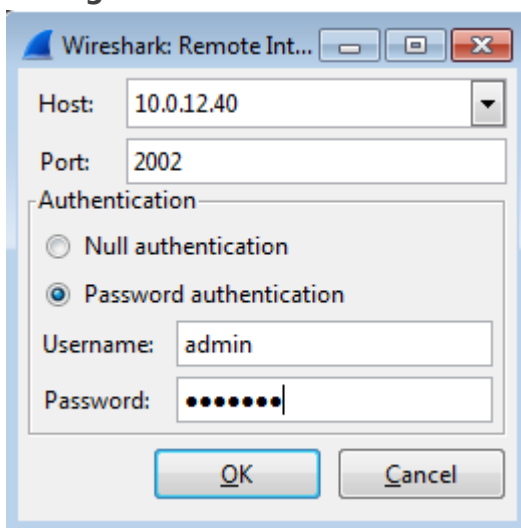


Add remote interfaces in wireshark options



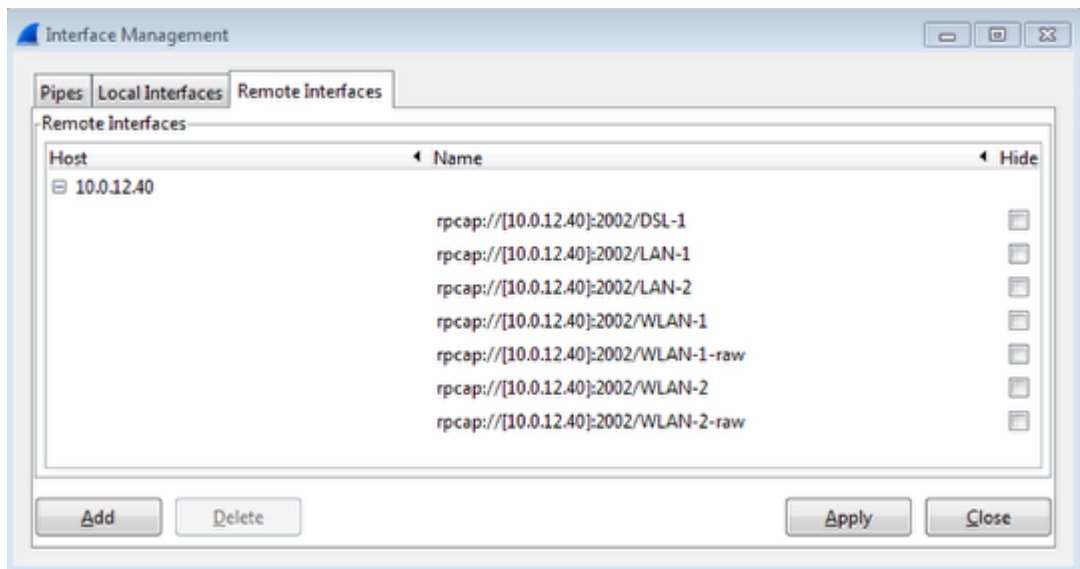
From Wireshark main Windows, open the Capture Options window (Capture/Options...). Click on manage Interface and select the tab Remote Interfaces and click on Add

Configure the BAT as remote device



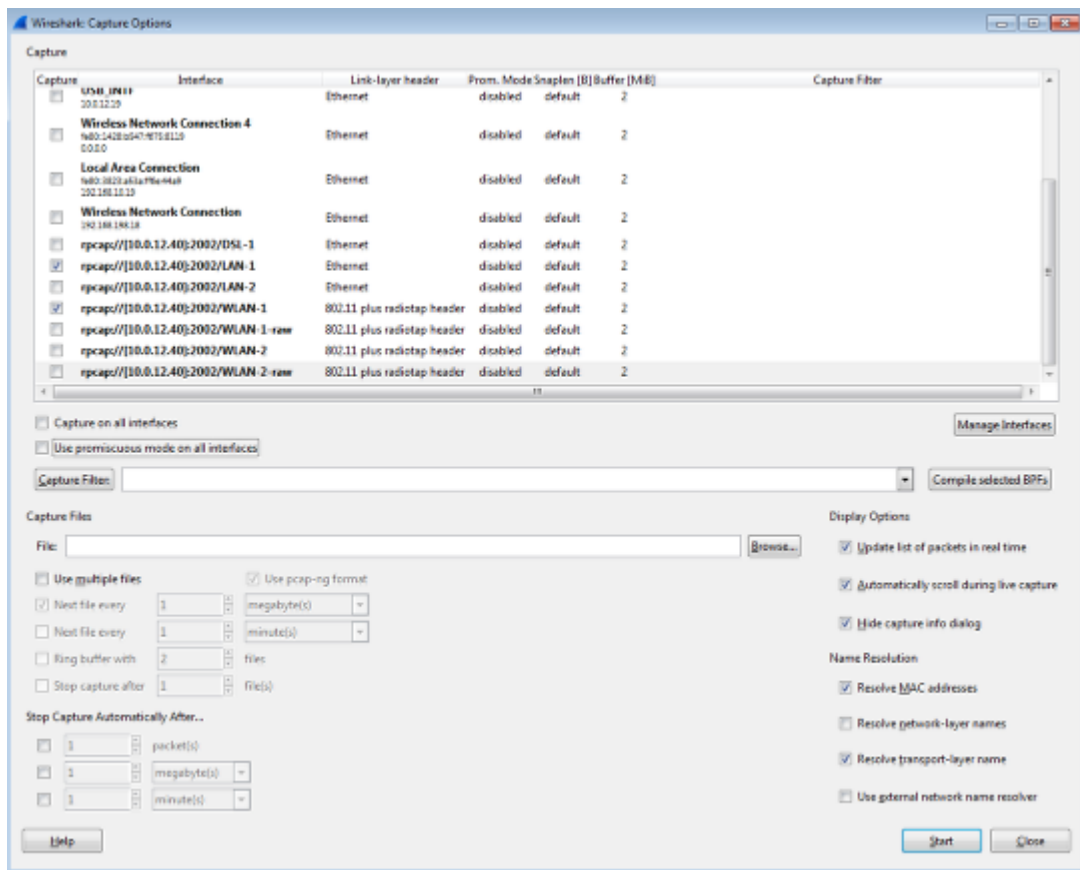
Give the IP address of the BAT, the RCap port relevant username and password to access the device then click ok

RCap gives all the available interfaces on the remote device



click on Apply and Close

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



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

Result view

The screenshot shows the Wireshark interface with a packet capture list and details pane. The packet list shows various TCP and RRCAP packets. The details pane for packet 6 shows a Radiotap header with the following fields:

- Header revision: 0
- Header pad: 0
- Header length: 36
- Present flags
- MAC timestamp: 383151112
- Flags: 0x00
- Data rate: 2.0 Mb/s
- Channel frequency: 2462 (86.11)
- Channel type: 802.11g (pure-g) (0x00c0)
- SSI signal: -57 dbm
- SSI noise: -87 dbm
- Antenna: 0
- Channel number: 11
- Channel frequency: 2462
- Channel type: unknown (0x000400c0)
- IEEE 802.11 Beacon frame, Flags:
- IEEE 802.11 Wireless LAN management frame

The packet bytes pane shows the raw data of the captured packet, with a hex and ASCII view.

RPCap tunnels the traffic 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.