ALBEDO Telecom
the Path to Excellence

ALBEDO Net.Shark is an FPGA-based tap that improves Wireshark performance by means of hardware programmable filters. It can capture packets at wire-speed (2 x GbE) something that Wireshark CPUs can't do.

Datasheet

ALBEDO Net.Shark

Wireshark is a network packet analyser to examine communication networks.

Important features are: live packet data capture, display packets with very detailed protocol information, open/save data, import/export from/to other programs. It can search/filter data on many criteria. Wireshark is open source and probably the best packet analyser available.

Net.Shark is a FPGA based tap with filtering capabilities, that connected in pass-through mode, is able to capture traffic at wire-speed. Packets are transmitted through two ports and traffic compliant with one of the filters is sent to Wireshark.

1. CONFIGURATION

1.1 Ports and Interfaces

- SPAN Ports: SFPs based 1 Gb/s
- SFP interfaces including: 10BASE-T, 100BASE-TX, 100BASE-FX, 1000BASE-T, 1000BASE-SX, 1000BASE-LX
- DROP Ports: Dual RJ-45 port for electrical connection 10/100/1000BASE-T
- Local Storage: SD storage in PCAP format
- Jitter less time-stamp

1.2 Formats and Protocols

- Ethernet frame: IEEE 802.3, IEEE 802.1Q
- IP packet: IPv4 (IETF RFC 791)
- Jumbo frames: up to 10 kB MTU (Maximum Transmission Unit)
- Throughput between measurement SPAN ports: 2x1 Gbit/s or 2x1,500,000 frames/s
- Autonegotiation parameters including bit rate (10, 100, and 1000 Mbit/s) and duplex mode
- Configurable MTU size

2. OPERATION

- SPAN ports: GbE SFP interfaces are used to connect -in pass thought- to the network Host A and Host B
- DROP Ports: GbE RJ45 interfaces to forward captured packets to the protocol analyzer device (i.e. Wireshark)
- STORAGE: captured frames saved in SD card
- All frames coming to Net.Shark are forwarded to destination without delay or lost
- Frames compliant with filtering conditions and copied to Wireshark device
- Operation is based on 16 filters per SFP port
- Filtered frames can be aggregated in one drop port

3. FILTERS

- 16 simultaneous filters can be applied to the traffic
- The Filtering process is executed sequentially
- When a packet satisfies a filter is sent to the Drop Port and immediately forwarded to the output. No more filters are processed
- Each packet may modify only the statistics of one filter
- Customizable filters defined by field contents on Ethernet, IP, UDP and TCP headers
- Agnostics filters defined by 16 bits masks and user defined offset
- Lawful filter: 64 byte pattern match at any place in the frame payload

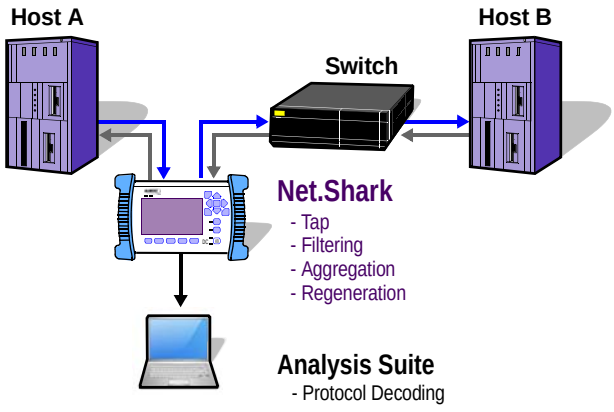


Figure 1. *Net.Shark and Wireshark in operation.*

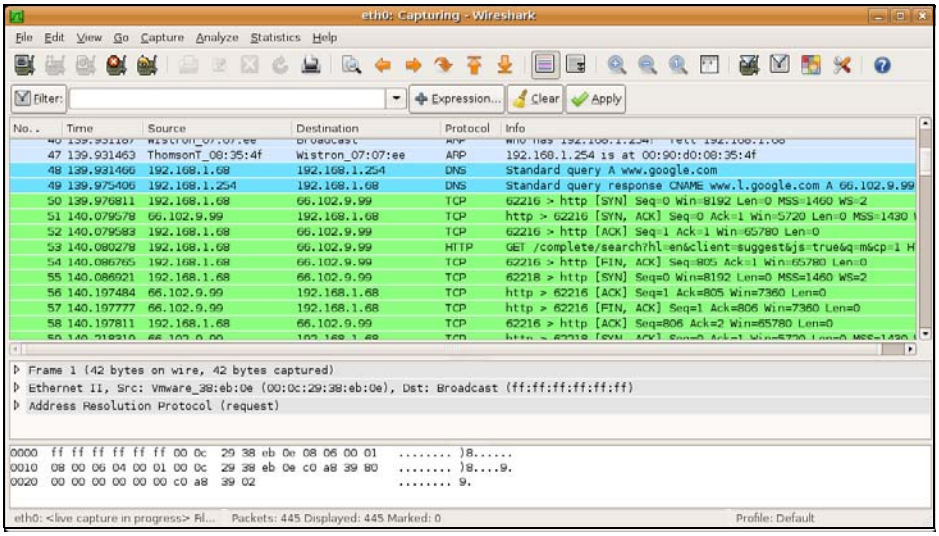
CONFIDENTIAL

3.1 Ethernet filters

- Ethernet Selection
- By source and destination MAC addresses. Selection of MAC address sets with masks
- By Ethertype value with selection mask.
- By VLAN-VID with selection mask
- By VLAN-CoS value with selection mask

3.2 IP filters

- IPv4 address: source, destination, and source-and-destination
- IP address group: subset of addresses filtered by masks
- Protocol encapsulated in the IP packet (TCP, UDP, Telnet, FTP, etc.)
- DSCP field, single value and range
- TCP/UDP port, single value and range



4. RESULTS

- Autonegotiation results including current bit rate, duplex mode, Ethernet interface
- SFP presence, vendor, and part number
- Traffic statistics per each of the Four Ports
- Statistics for both transmit and receive directions
- Frame counts: Ethernet, and IEEE 802.1Q
- Frame counts: unicast, multicast and broadcast
- Basic error analysis: FCS errors, undersized frames, oversized frames, fragments, jabbers, collisions
- Frame size counts: 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 bytes
- Four byte counts: Port A (Tx / Rx) and Port B (Tx / Rx)
- All traffic counters follow RFC 2819
- Counters and statistics per filter (up to 16)

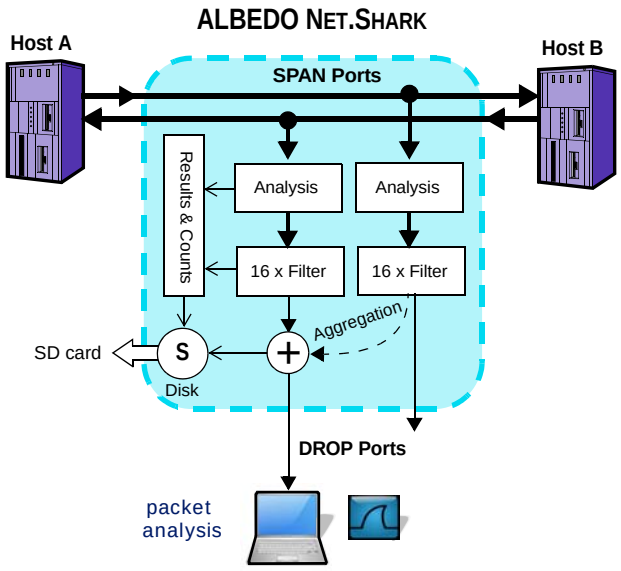


Figure 2. *Logical block*

5. USER INTERFACE

- Direct configuration and management in graphical mode using the keyboard and display of the instrument
- Remote access for configuration and management in graphical mode from remote IP site thought the Ethernet interface of the control panel
- Remote access with command line (CLI) using of either Telnet or SSH offering for configuration, management and task automation
- Remote access via SNMP for configuration, management and integration

6. GENERAL

- Operation time with batteries: 3.5 hours (minimum, two battery packs)
- Configuration files available
- Capture local storage in CAP format
- Export through attached USB port
- TFT color screen (480 x 272 pixels)
- Dimensions: 223 mm x 144 mm x 65 mm
- Weight: 1.1 kg (with rubber boot, one battery pack)