ALBEDO Telecom
Joan d'Austria, 112 - Barcelona - SP - 08018
Chalfont St Peter - Bucks - UK - SL9 9TR
www.albedotelecom.com

Packet tapping for traffic analyzers

Traffic analysis is a key activity of network management departments and engineers have often to face the challenge to capture and tap IP packets in real time to investigate a wide number of scenarios:

- protocol analysis and service troubleshooting,
- loss of performance investigation,
- denial of service and cyber attacks,
- security and lawful studies,
- traffic statistics, network mining,
- backhaul and application rollout.

To achieve the targets it is necessary to identify the streams and types of traffic traversing the network that are going to be decoded and correlated. Proper analysis begins with accurate packet captures, which is generally requires a function of hardware because software are unable to work at wirespeed without losing packets and generating delay to absolutely all traffic.

The sequence of the process could be detect, filter, analyze and map traffic, identifying threats to the network to limit their impact. To achieve these objective network administrators and technicians generally use branded traffic analyzers and also some popular open source tools, such as Wireshark.

Figure 1 *Net.Hunter is a stream-to-disk appliance capable of monitoring live traffic to capture and record selected TCP/IP flows at wirespeed. It includes an embedded tap with triggers and programmable filter conditions.*

1. CAPTURE AND ANALYSIS

Data capture and protocol analysis are related but are totally different functions. Capture has to be fast and effective but protocol analysis has no real-time processing requirements. A portable capture device may or may not include protocol analysis.

Sometimes it is enough to supply the means to enable the user to identify and download the interesting data within the captured stream and leave protocol analysis to dedicated, usually software-based equipment. In order to solve the problem lets try to study how we can do it as there are a number of alternatives will be provided with usage techniques that enable you to capture traffic

Considerations on traffic capture

The first and simplest approach is to use the PC running the analysis software to capture packets (See Figure 5). Unfortunately this approach only works under below low traffic conditions, but this is not only the unique reason there are more related with performance, packet lost, timestamping, etc.

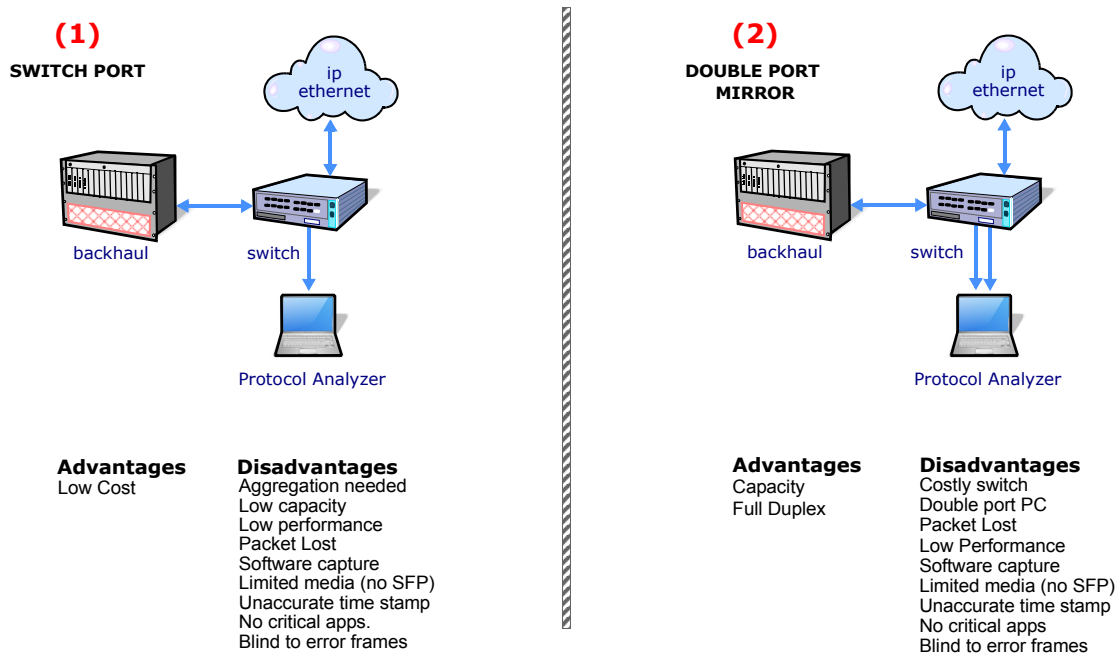

Figure 5 *None of these methodologies are appropriate for critical analysis because software captures can never ever reach wirespeed then it could be only accepted in case of low speed and non-critical data applications.*

2. ACCESS TO THE NETWORK TRAFFIC

There are two modes to get access to the live traffic in mirror mode and in pass through mode, while it can be directly with software or hardware assisted using taps. These are some of the resulting scenarios

Switch Port

The switch copies the aggregated Tx and Rx data traffic and sends a copy to a third port. However it can only support a maximum of 1000 Mbps despite a full-duplex data stream can reach 2000 Mbps then packets could be dropped (See Figure 5).

Double Mirror Port

This technique is based on a special node capable to traffic routing of both Tx and Rx. It has wider capacity but there is a limitation of the internal buffers of the switch and the PC that may overflow in case of long burst of packets. and traffic could be lost (See Figure 5).

Software Monitor Mode

It requires a PC with two Ethernet ports and software to capture in both directions. Packets to be analyzed shall be captured and saved while the complete stream shall be forwarded in both Tx + Rx directions. However, NEVER TRY THIS CONFIGURATION, except in your laboratory, then you will observe that only works for a links with little traffic -no more than a few Mbit/s- because the CPU can't cope and delays absolutely all traffic. When the bit rate is higher than 15 or 20Mbit/s the situation is even worse as not only delays but also begins to lose packets. At 100Mbit/s will probably collapse and the link will go down (See Figure 6).

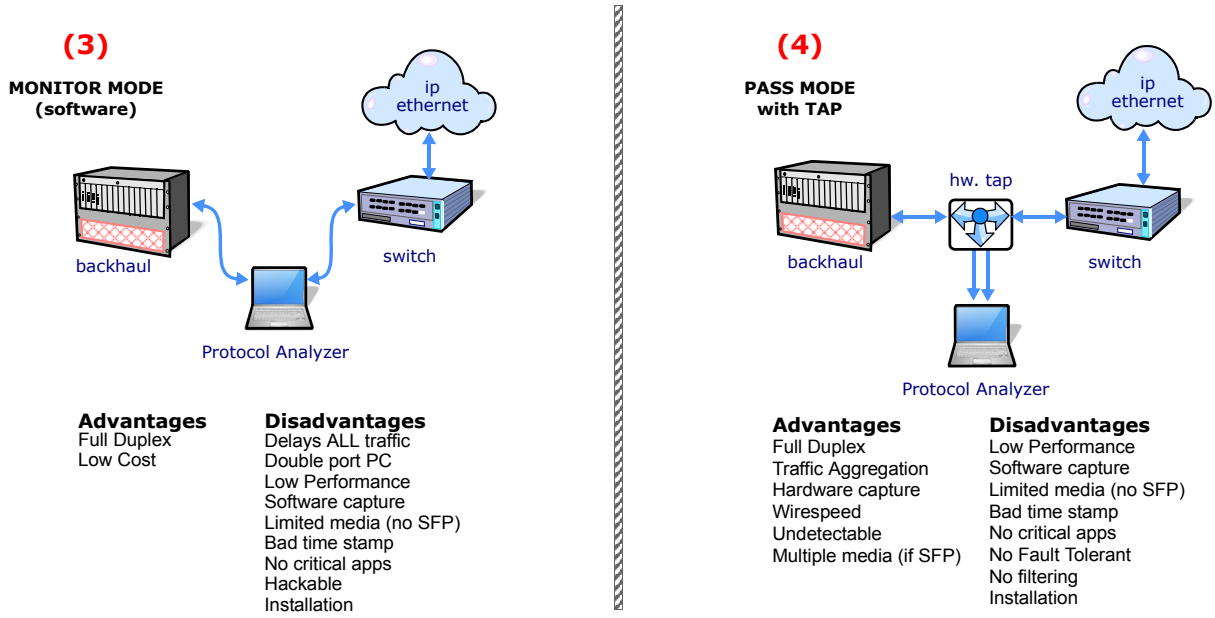

Figure 6 *The use of hardware tap is a big step forward but still not enough for professional applications.*

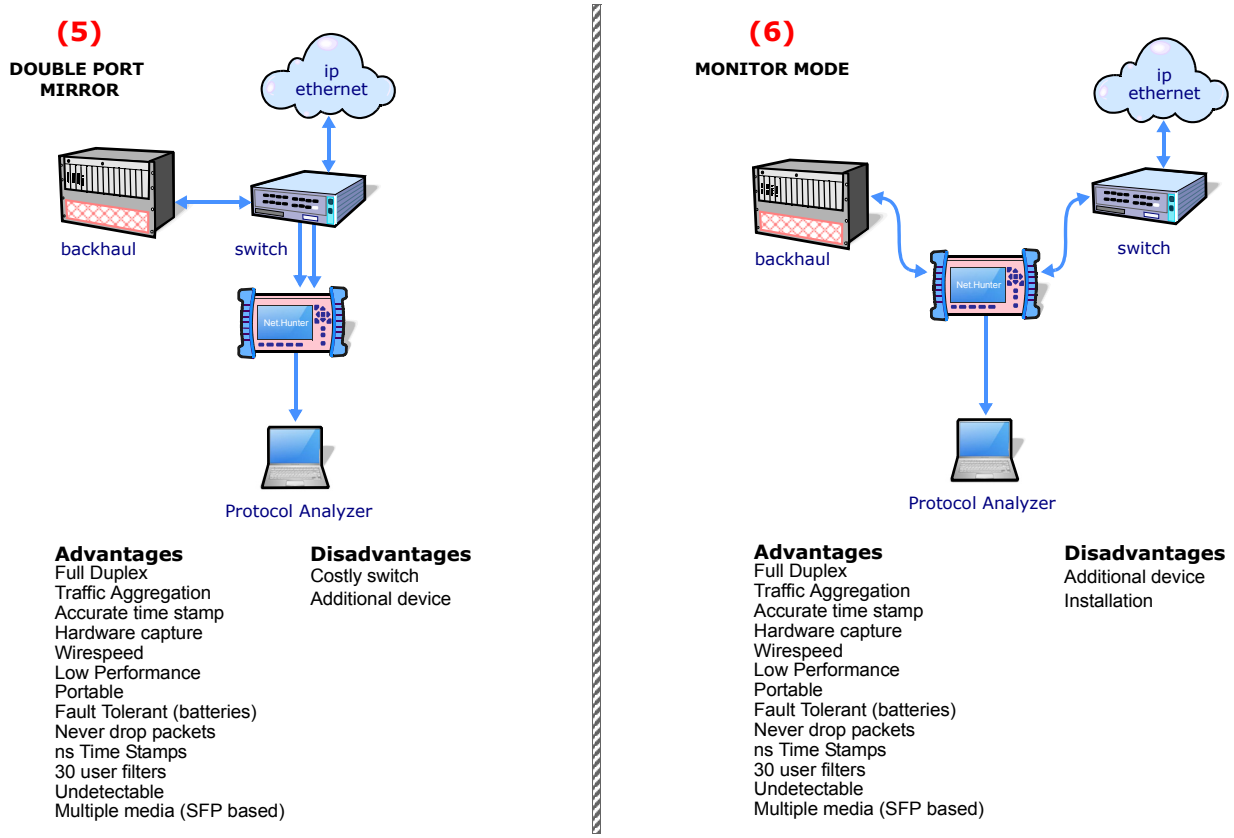

Figure 7 *ALBEDO handy taps unique solution for critical data high performance applications.*

Hardware tap

This is a passive splitting mechanism installed in pass through to forward at wirespeed both Tx + Rx to a dedicated channel. Taps are equipped with a dual-receive capture, and dual-transmit features capable of aggregating both data streams. A tap never drop packets, regardless of speed or bandwidth and unlike other alternatives, good taps may also forward physical layer errors (important for troubleshooting) to the monitoring device. A tap is completely passive; it cannot interfere in any way with the full-duplex network, but it may saturate de PC that can't save a bit rates higher that a few Mbit/s (generally less 100Mbit/s) because of the limitations of the operating system. Moreover these limitations also affect to the Time Stamping because the PC generates itself time unaccuracies depending on the line volume of traffic and PC model (See Figure 6).

ALBEDO capture technology

It has all the advantage of hardware tap and overcomes those issues caused by the PC. Albedo handheld taps do filter at wirespeed before capturing it, allowing the rest of the flows to pass with no delay no lost. Those packets that are compliant with any of the 30 user programmable filters (based on MAC, IP, TCP, Port, etc.) are copied and forwarded to the PC equipped with the analyzer that shall only receive those packets that is interested on. Albe-

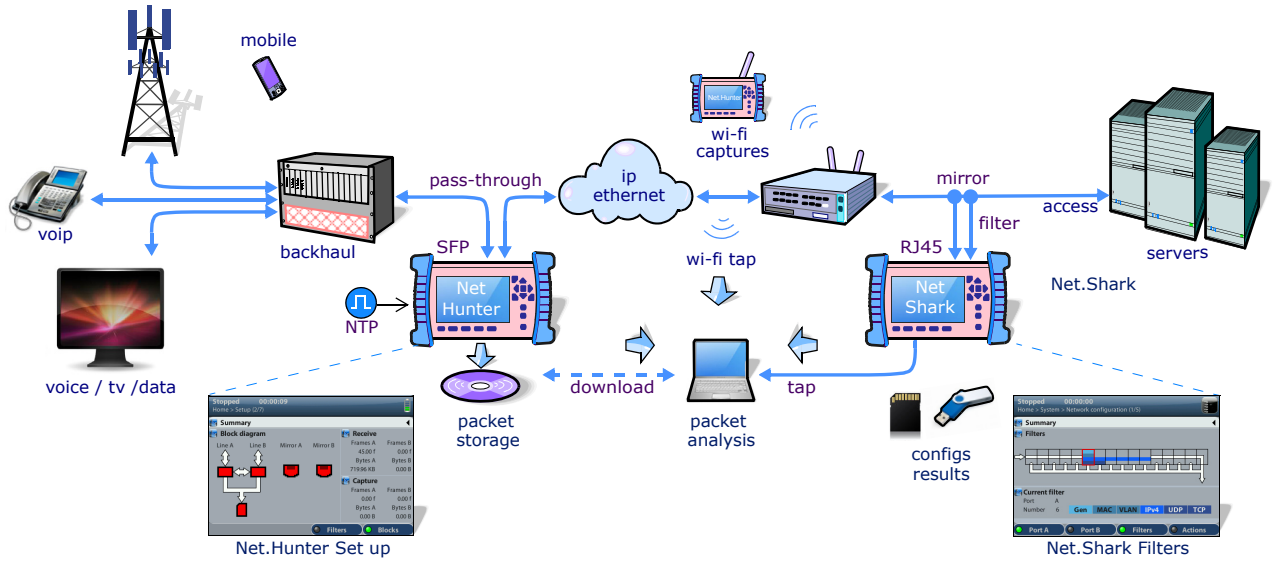

Figure 8 *Net.Hunter is a compact solution to manage quality, troubleshooting threats, incidents and malware.*

do handy Taps have an embedded splitting mechanism installed, also have user programmable filters, aggregation features, wirespeed storage[1], and two forwarding ports to tap the captured packet.

Albedo taps are equipped with a dual SFP capture interfaces and two 1000BASE-T ports to tap the filtered traffic to the PC. Albedo taps never drop packets, working at full wirespeed in full duplex and unlike the above mentioned alternatives just taps may capture physical layer errors, FCS errored frames, and non-standard frames as jabbers. Albedo taps are totally transparent to the network as a strip of fiber because they do not have a network IP or MAC address therefore are very secure and cannot be hacked. Regarding the intrinsic delay is better that 250ns which means nothing as all the filtering and tap process is executed by means of programmable hardware (FPGA) network (See Figure 7).

3. KEY FEATURES FOR EXCELLENCE IN CAPTURING

For a well done work it is important to bear in mind a number of factors that play a critical role in IP packet capture including: how data is transferred off the wire, timestamping, formatting, capacity, physical media, mobility and, of course the cost.

Wire-speed Pre-Filtering

Pre-filtering is an important feature even for devices prepared for wire-speed capture. Do exit an important number of advantages:

1. Net.Hunter: 120GB disk to record packets at wirespeed.
   Net.Shark: SD card for low speed capture and recording up to 1 + 1 Mb/s.

- With the help of filters, users make sure that only important data is going to be stored. For example, if only IP telephony signalling is going to be analyzed, all other data can be ignored. The effect is a much better usage of the storage capacity. With the help of pre-filtering, it is possible to extend the maximum capture time from a few hours or minutes to days or weeks by constraining the raw volume of data.
- The second advantage of pre-filtering is that it can be used to mark packets depending on the filtering rule applied to match each of them. This classification can be used later for post-filtering and protocol analysis. Hardware processing is well suited to filter data based on fixed-length packet fields like IP / MAC addresses or class of service (CoS) marks (see Table 1). As a result it is possible to match any packet directed to an specific IP address, or directed to a network specified by its network prefix, or packets between two hosts specified by their source and destination addresses.
- Port based filtering can be used to match traffic from single applications like web traffic (port 80), e-mail (port 25), VoIP signalling (port 5060) and many others. Filtering based on CoS marks can be used to filter traffic classes subject to controlled performance defined by the Service Level Agreement (SLA). More advanced filtering is based on fixed alphanumeric patterns. Fixed pattern filters can be used to find any word or sentence within the data stream. There are many applications of this kind of filters. For example, an IP telephony trunk link based on SIP signalling use SIP INVITE messages to establish calls. Filtering the “INVITE” word may be used to get information about IP calls occurring in the link.

Table 1

User defined filters to capture selected traffic

Filter Type	*Details*
Ethernet Selection	Selection by source and destination MAC addresses or Ethertype field
VLAN selection	Selection by VLAN-ID or CoS marks. Matching of C-VLAN or S-VLAN fields in frames with multiple VLAN tags
IP selection	Matching of source and destination IPv4 / IPv6 addresses, DSCP and protocol (UDP, TCP, ICMP...)
TCP / UDP selection	Filtering of source and destination TCP / UDP ports. Selection of port ranges
Fixed offset selection	This filter matches an specific bit pattern in a user configurable position within the packet.
Fixed pattern selection	Matches a fixed pattern in a variable position within the frame. The pattern is specified as an alphanumeric string
Length selection	Matches packets with an specific length or frames within a custom length range

An essential feature of filtering blocks is that they can be combined to give more complex filters. For example, users can configure various filters within the same block to get the combined effects of an “AND” filter. In the same way, several filtering rules are combined in different blocks to get the aggregated effect of an “OR” filter.

Accurate Time Stamps

A very accurate timestamping is key for troubleshooting, in particular for VoIP and IPTV packets a bad PCAP could indicate that there is jitter to in the line despite such a problem does. When packet get time marks with

Figure 9 *Net.Shark is the world' first portable tap. It includes 2x16 programmable filters to identify flows is able to worl at wirespeed and timestamping packets without generating any perturbance on live traffic.*

Net.Shark or Net.Hunter the accuracy is always better than 1ns. avoiding a lot of headaches looking for non existing faults. Moreover ALBEDO unit could be externally synchronized by means of NTP sources to manage a common clock source.

Electrical and SFP ports

Different media types is absolutely common in telecoms this is the reason why ALBEDO taps are equipped with a double SFP Port to capture in any type of cable. With SFPs you can access different media types (Optical SX, LX, ZX, and Copper TX) and support varying data rates up to Gb/s.

4. FILTER & TAP APPLICATIONS

Scenarios using Albedo portable taps are considerably wide due to the ability to be connected and start operation in minutes without any special requirement. Portable capture devices are very well suited to temporary network connections in cases where analysis is required only for a limited period of time a few hours or days. A good example would be analysis carried out in a cellular network through connection to one or several mobile base stations. Applications can be distributed in two large families, (a) *troubleshooting* of communication networks and (b) *security*, including forensic analysis and lawful interception.

Network troubleshooting

Include tracing of difficult to assess, temporary, intermittent problems. Traditional monitoring tools provide permanent information about the network in terms of various Key Performance Indicators (KPIs) but they are unable to deal with issues related with unexpected protocol interactions. Full protocol captures arise as the only way to deal with these problems.

Security

Fighting against attacks like phishing linked to malware and other security threats. Event based pre-filtering could be used to detect intrusions. With the help of these tools, investigators will have the capability to reconstruct web sessions, e-mails and 'chat line' conversations in a chronological order to investigate security incidents. Lawful Interception applications. In case of portable devices the focus is again in non-permanent interception. Both filtering based on fixed patterns and event based filters could be used to built efficient LI based on wire-speed captures.

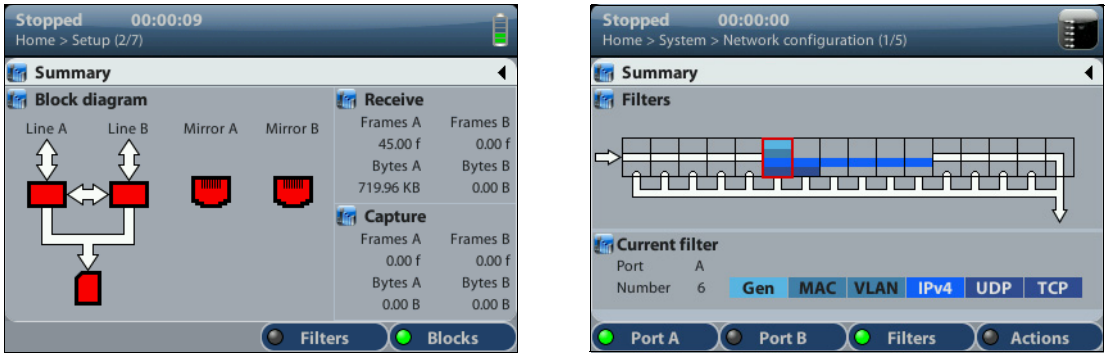

Figure 10 *Graphical user interface based on colour screen specifically designed for local management.*

5. CONCLUSIONS

Portable capture devices are ideal for enterprises looking to ensure that their networks are robust, scalable and secure. Portable capture and recording taps make easier the capture process of full-duplex data in Ethernet interfaces operating at 1 Gb/s using small, highly portable devices weighting no more than 1 kg and operated by batteries.

These unique tools find applications in fighting against security threats, troubleshooting of data, multiplay networks and lawful interception. All these are also applications of traditional appliances but portable devices are cheaper and more versatile. Portable devices are configured locally with the help of a graphical user interface but they may also include interfaces to allow remote management.

ALBEDO Telecom

ALBEDO Telecom designs, manufactures, and delivers solutions that enable Telecom organizations of all sizes to test, measure, troubleshoot, monitor, and migrate mission critical networks and multiplay applications.

On local segments and across distributed networks, ALBEDO enable Organizations, Installers, Operators, Service Providers and Suppliers to quickly check the health of Network Architectures, Service Agreements (SLA), IP Quality (QoS), or fix any issue.

Your Business Partner

Results. ALBEDO Telecom helps the industry to make the most of the investment on infrastructure.

Expertise. ALBEDO Telecom engineers and consultants provide industry leading knowledge in hand-held TAPs and WAN emulators, IPTV, VoIP, Carrier-Ethernet, Synchronization, Jitter, Wander, SyncE, PTP, E1, and Datacom to address customers unique needs.

Integration. ALBEDO Telecom integrates disparate telecom technologies and applications, facilitating new business efficiencies.

Agility. ALBEDO Telecom increases the ability of customers to respond quickly to new market opportunities and requirements.

Coverage. ALBEDO Telecom offers solutions that facilitates the migration and the roll-out to new architectures.

ALBEDO Telecom

the Path to Excellence

Joan d'Austria, 112 - Barcelona - 08018 - SP
Chalfont St Peter - Bucks - SL9 9TR - UK
www.albedotelecom.com

aims

+ UNDERSTAND causes of telecom interoperability issues
+ EXPERIENCE the best quality in unified networking
+ ASSESS different hardware, firmware, and software solutions
+ LEARN from experts by means of professional services and consultancy