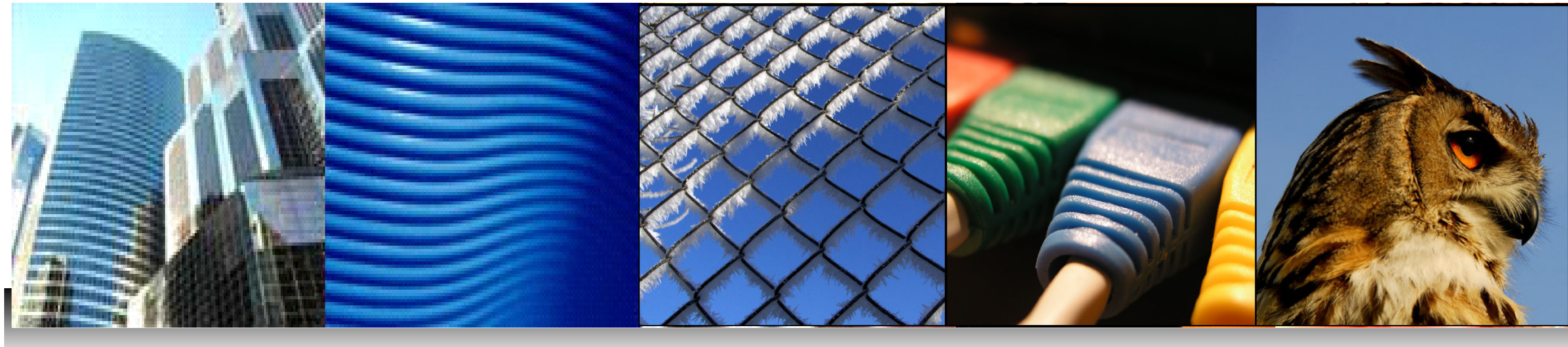
Seamless **FIELD** Traffic Interception



using hand-held / battery-operated appliances

ALBEDO Telecom

the Path to Excellence

About ALBEDO Telecom

TELECOMS EXPLAINED – Unravel Emerging Technologies
Triple Play
Building the converged network for IP, VoIP and IPTV
Francisco J. Hens
José M. Caballero
WILEY
ALBEDO
METRO.ISO
623.5 KΩ +100V
Installation and Maintenance of
SDH/SONET, ATM, xDSL, and Synchronization Networks
Net.Time
GM
B
S
Net.Storm

ALBEDO Telecom offers a full range of telecommunication products and services to the international market.

- **Hand-held Filtering Taps**: battery operated, 1kg. double port
- **Stream-to-disk appliance**: SSD disk, wirespeed capture, wirespeed storage, 2Gb/s
- **Impairment Generator**: Carrier Ethernet and IP
- **Hand-held testers**: E1, SDH, GbE, SyncE, IP, IPTV, VoIP, Datacom, Jitter, Wander
- **Acceptance Labs**: IPTV, VoIP, ISDN, POTS
- **Consultancy / Integration**: IPTV, VoIP

Handy while **Intelligent** Interception

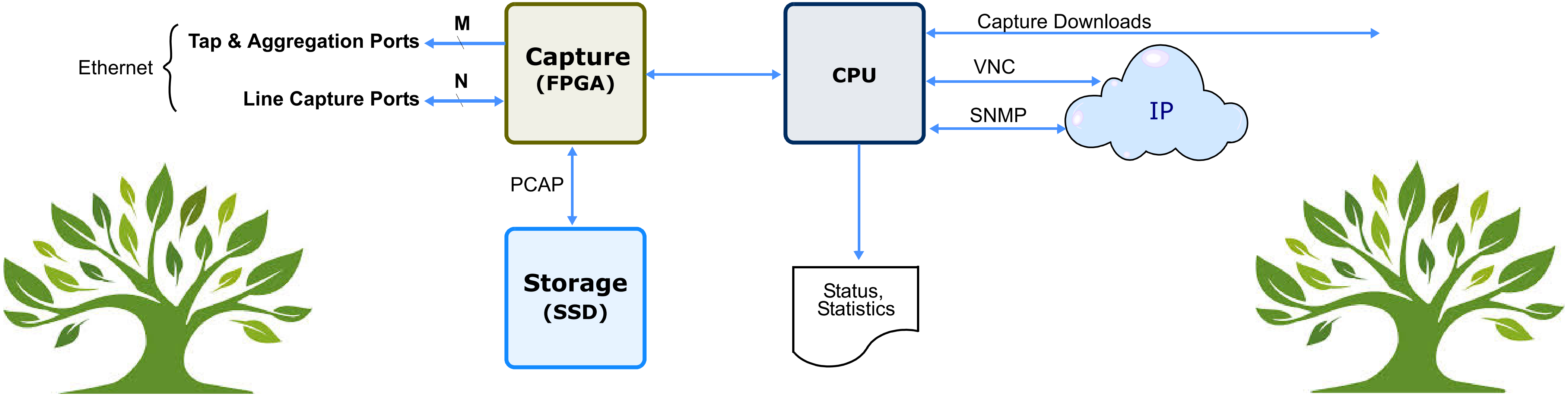
Packet sniffing of live traffic has become a common practice

- Intelligent collection
- Internet TV (IPTV) Multistream captures
- Internet Voice (VoIP) monitoring, capture and surveillance
- Law enforcement and Legal Interception
- 24/365 Access Monitoring and Forensic Analysis
- Cyber-security and Criminal Investigations

Drawbacks in interception appliances

- Lack of performance to process 100% of the traffic
- Low capacity to filter and capture packets in real time
- Not all are undectable
- Not all are transparent
- Bulky to transport and install
- Complex to be used, many devices envolved everywhere at anytime
- The cost is generally High

Field Data Tapping & Storage



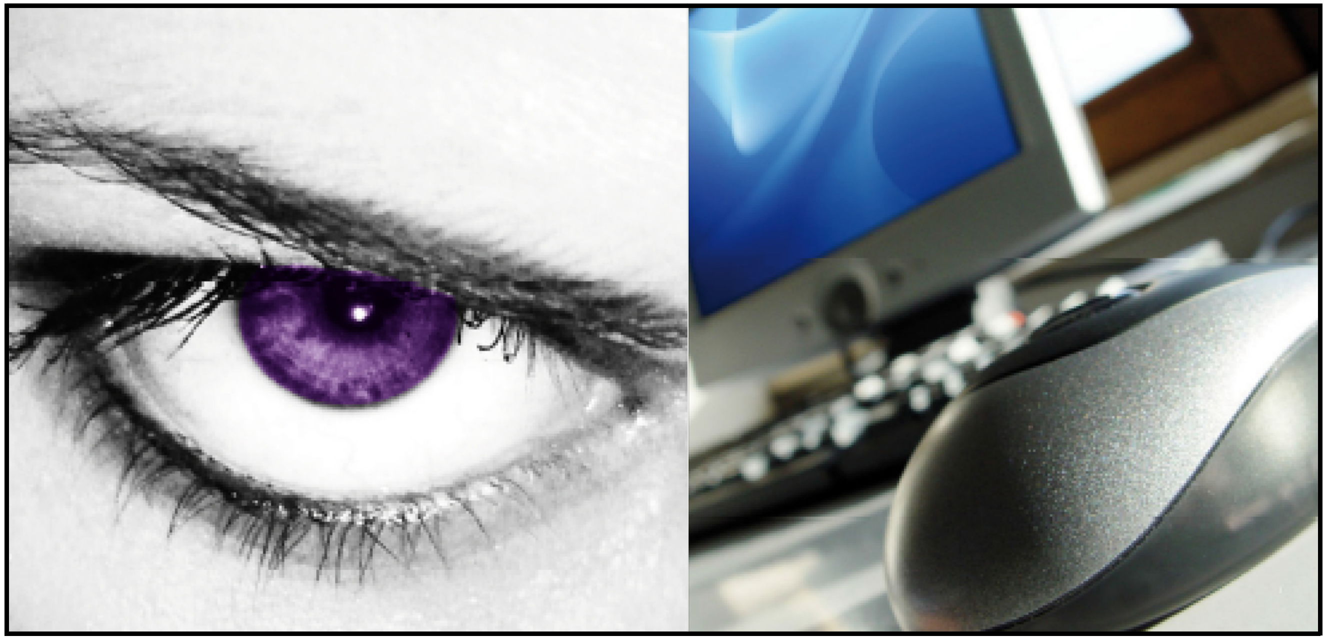
Improvements Solid State Drives (SSD) and continuous optimization of FPGA are bringing new possibilities in data capture and processing applications.

- FPGAs are suited for wire-speed processing
- SSD supply performance, large storage capacity, very fast
- Both are rugged and suitable for portable and hand-held equipment

Data capture is combined with the functionality of a network tap to enable easy access to the traffic stream that has to be analyzed.

Interception & Analysis

1 - CAPTURE



2 - ANALYSIS

Data capture and protocol analysis are related but are totally different functions.

1. **Capture** has to be fast (wirespeed) and effective (no loss, no delay)
2. **Analysis** has no real-time processing requirements

Often 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.

Field Portable Capture & Storage

Portable capture devices are ideal for organizations willing to capture datas and looking to ensure that their networks are robust, scalable and safe

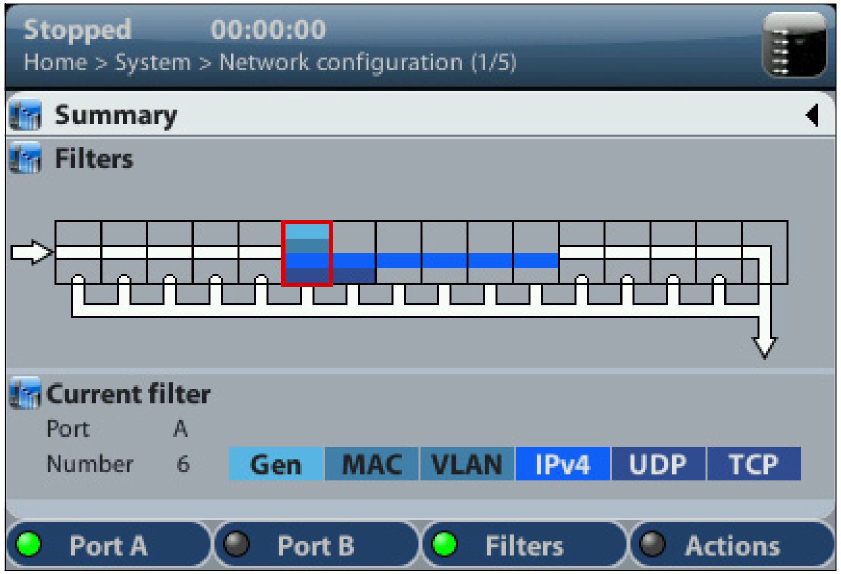
- All you need is a hand-held device: Easy to hide
- Self-contained: no need for a PC, a server, or a switch
- Battery Operated: means fault tolerant
- Direct or remote Operation by VNC or SNMP
- Ideal to be transported: small and protected
- Captures should be time-stamped (ie PCAP)

Portable Capture Applications

- Fighting attacks like phishing linked to malware and other security threats.
- Event based pre-filtering could be used to detect intrusions
- Reconstruction of web sessions, e-mails and 'chat line' conversations
- Temporal Lawful Interception using filtering on fixed patterns or event based
- Fight against Criminal and Terrorist plans

Law Enforcement and Intelligent analysis will be done in the laboratory using the software and the tools to decode the captured information.

Wire-speed Filtering



Stopped 00:00:00
Home > System > Network configuration (1/5)

Summary

Filters

Current filter
Port A
Number 6

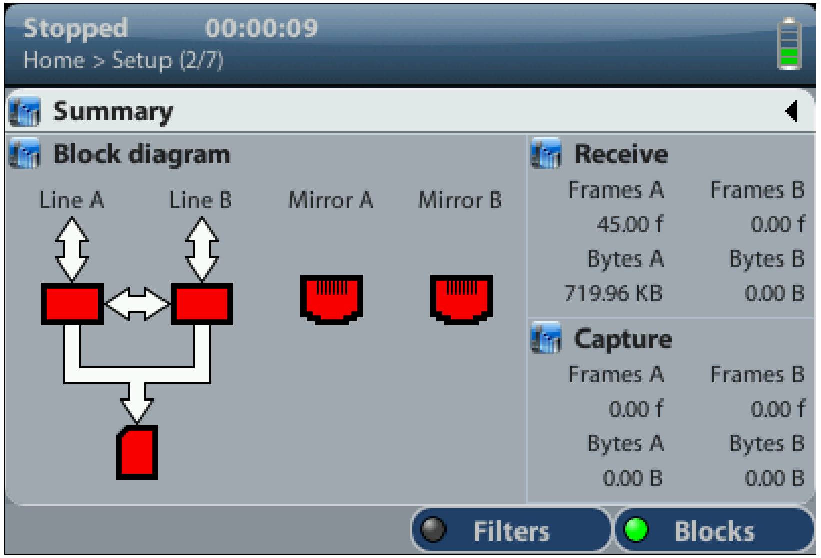
With filters investigators make sure that only important data will be stored.

- i.e. if Internet telephony is the target all other data is ignored
  <u>The effect is a much better usage of the storage capacity</u>.
- Packets can be marked depending on the rule applied to match each of them. This classification can be used later for post-filtering and protocol analysis.
- 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.

Intelligence and Filtering Criteria

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

Configuration & Control



Stopped 00:00:09

Home > Setup (2/7)

Summary

Block diagram

Receive

Frames A	Frames B
45.00 f	0.00 f
Bytes A	Bytes B
719.96 KB	0.00 B

Capture

Frames A	Frames B
0.00 f	0.00 f
Bytes A	Bytes B
0.00 B	0.00 B

A dedicated screen and keyboard makes unnecessary external devices like controlling PC with special management software.

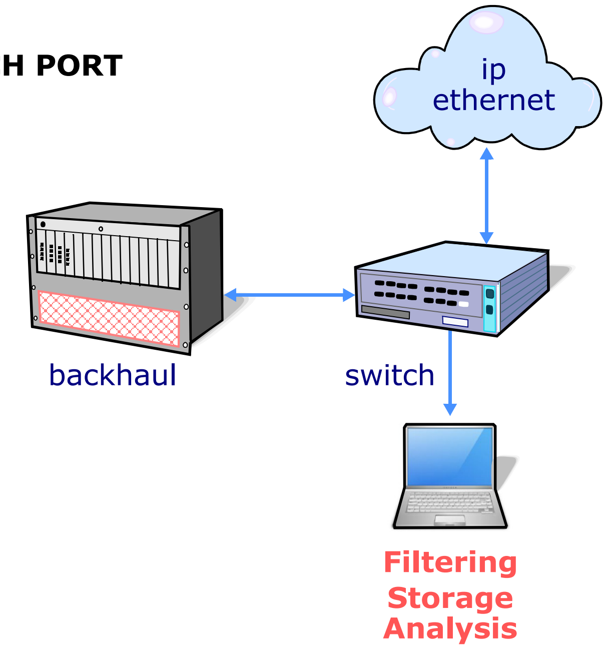
- Configuration commands: to configure and start / stop captures, configure filter.
- Result retrieval commands

The use of remote control such as VNC or SNMP allow the management and full control of the unit.

Considerations on traffic Interception (I): **Data Servers**

(1)

SWITCH PORT



Advantages

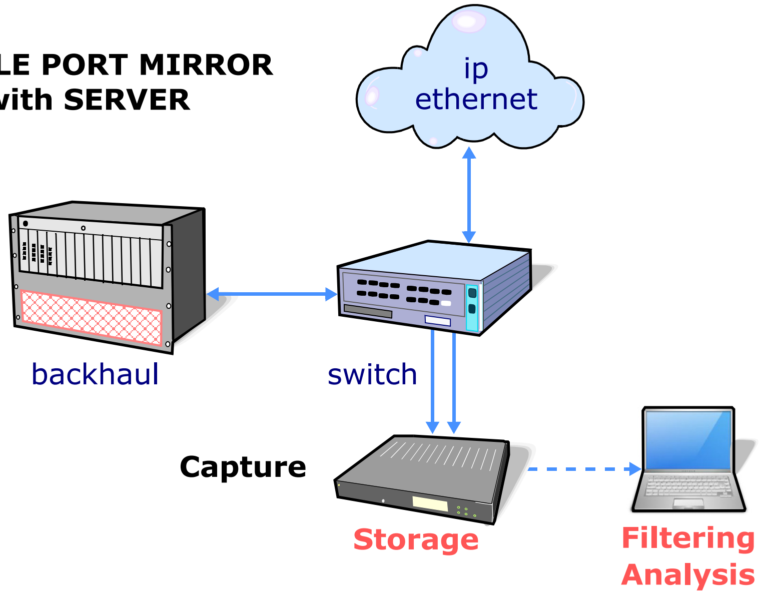
Low Cost

Disadvantages

Aggregation needed
Low capacity
Low performance
Packet Lost
Software capture
Limited media (no SFP)
Unaccurate time stamp
No critical apps.
Blind to error frames

(2)

DOUBLE PORT MIRROR with SERVER



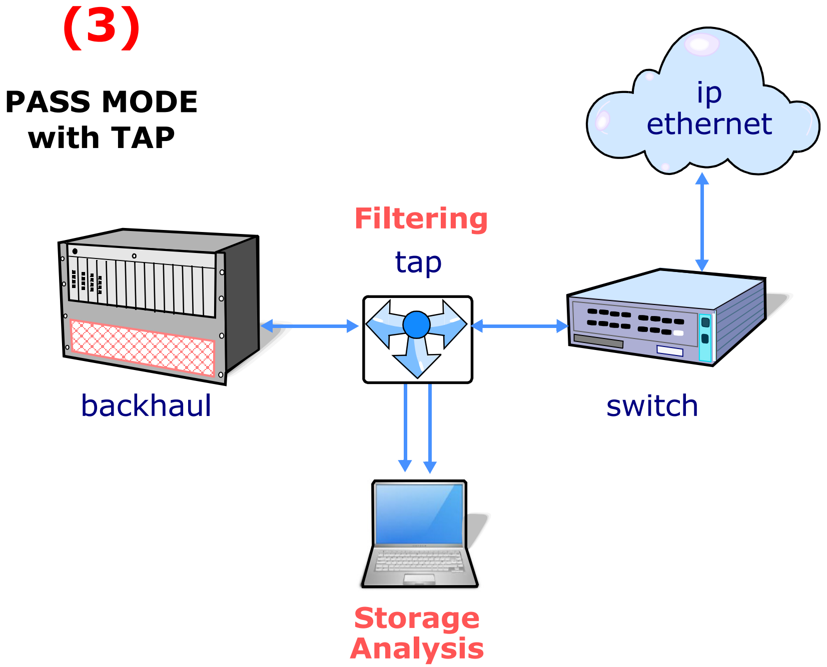
Advantages

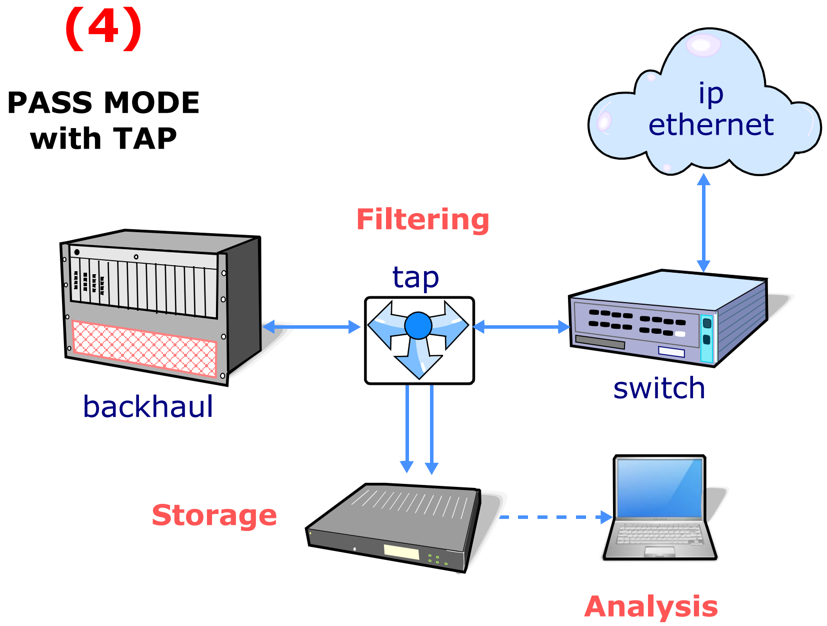
Capacity
Full Duplex

Disadvantages

Costly switch
Double port PC
Packet Lost
Mid Performance
Software capture
Limited media (no SFP)
Unaccurate time stamp
No critical apps
Blind to error frames
Transport

Considerations on traffic Interception (II): **taps**





Advantages
Full Duplex
Traffic Aggregation
Hardware capture
Wirespeed
Undetectable
Multiple media (if SFP)

Disadvantages
Low Performance
Software capture
Limited media (no SFP)
Bad time stamp
No critical apps
No Fault Tolerant
Installation

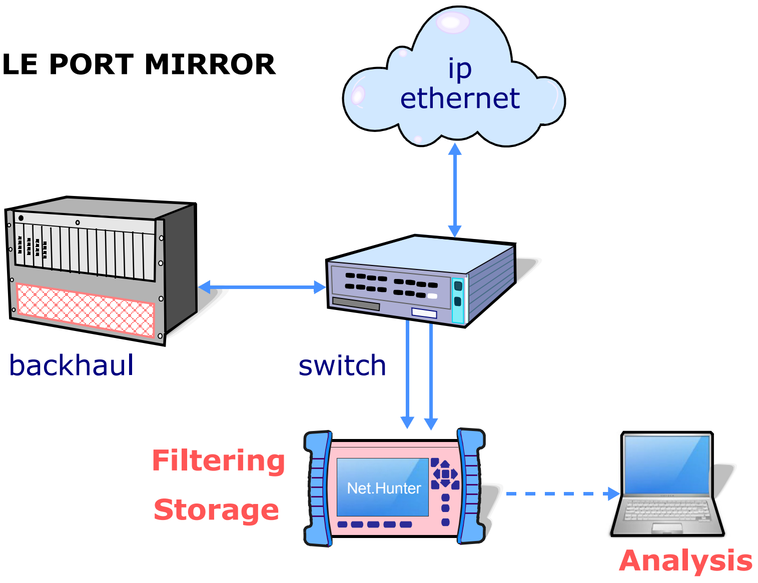
Advantages
Full Duplex
Traffic Aggregation
Hardware capture
Wirespeed
Undetectable
Multiple media (if SFP)

Disadvantages
Bulky
Expensive
Bad time stamp
No Fault Tolerant
Complex Installation

Considerations on traffic Interception: **stream-to-disk**

(5)

DOUBLE PORT MIRROR

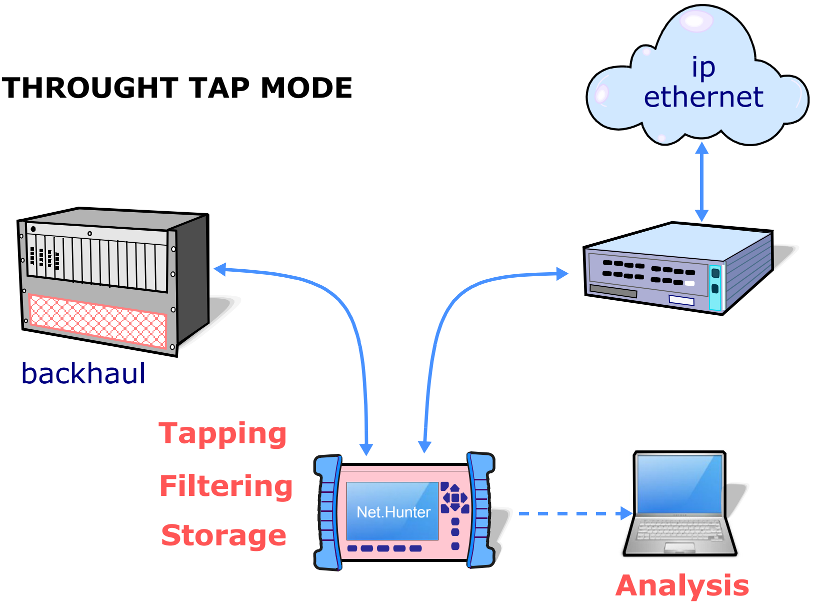


Advantages
Full Duplex
Traffic Aggregation
Accurate time stamp
Hardware capture
Wirespeed
Low Performance
Portable
Fault Tolerant (batteries)
Never drop packets
ns Time Stamps
30 user filters
Undetectable
Multiple media (SFP based)

Disadvantages
Costly switch

(6)

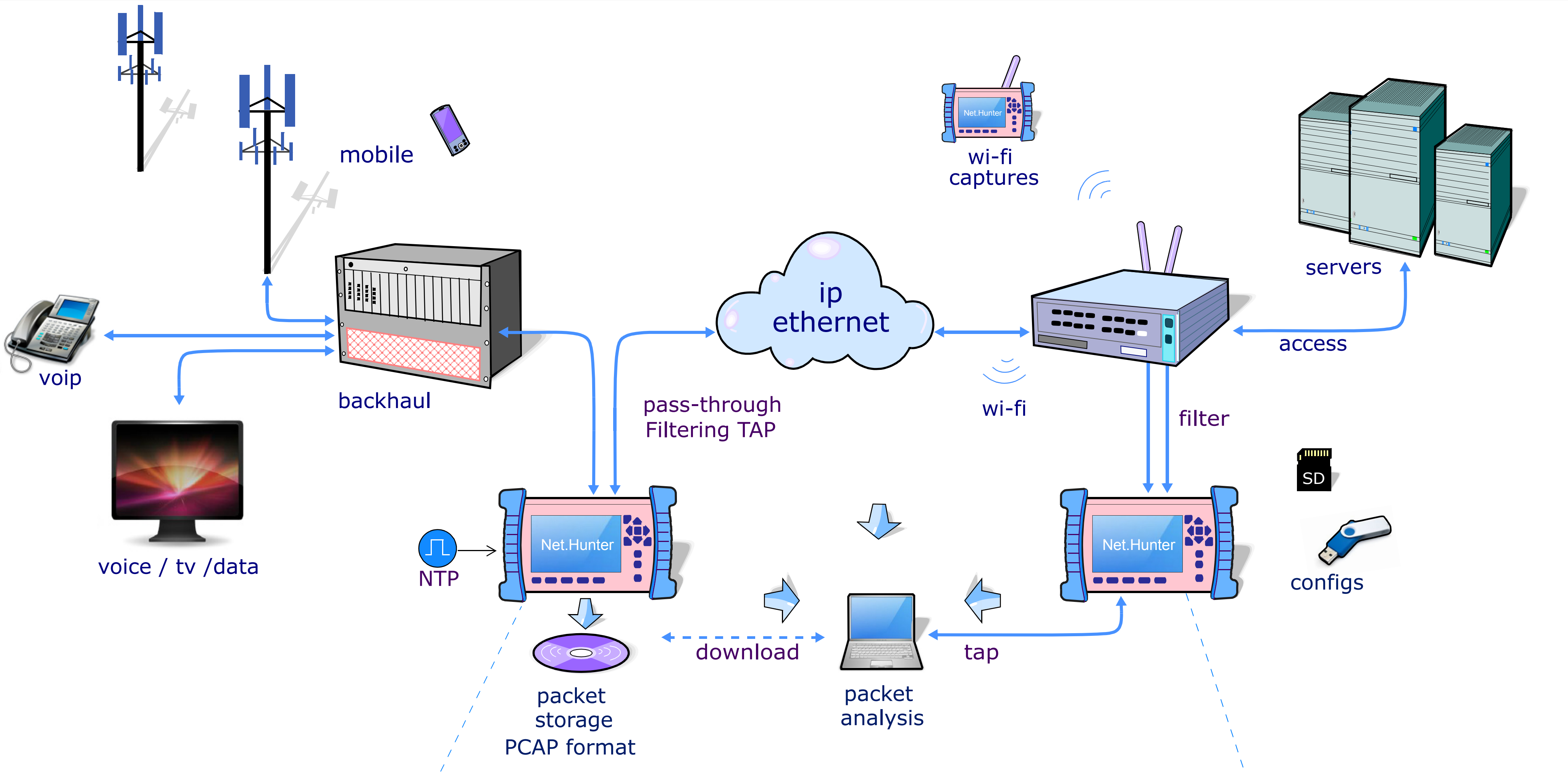
PASS-THROUGHT TAP MODE



Advantages
Full Duplex
Traffic Aggregation
Accurate time stamp
Hardware capture
Wirespeed
Low Performance
Portable
Fault Tolerant (batteries)
Never drop packets
ns Time Stamps
30 user filters
Undetectable
Multiple media (SFP based)

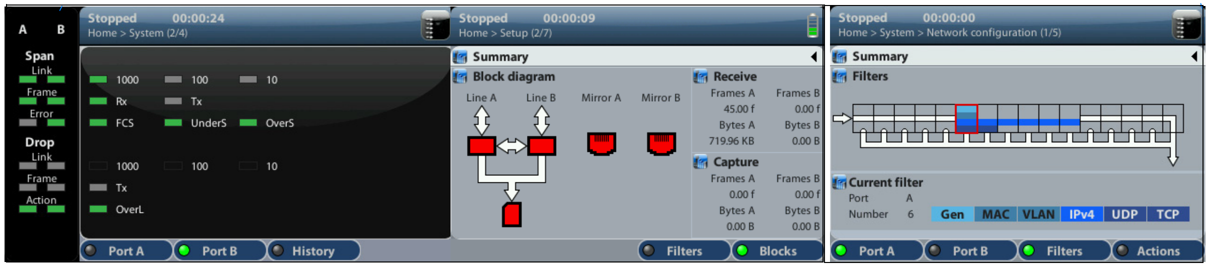
Disadvantages
Installation
Cabling

Field Captures with **hand-held** appliance



VNC Remote Control

GUI



A B

Span: Link, Frame, Error

Drop: Link, Frame, Action

Stopped 00:00:24
Home > System (2/4)

1000 100 10
Rx Tx
FCS UnderS OverS

1000 100 10
Tx
OverL

Stopped 00:00:09
Home > Setup (2/7)

Summary

Block diagram: Line A, Line B, Mirror A, Mirror B

Receive

Frames A	Frames B
45.00 f	0.00 f
Bytes A	Bytes B
719.96 KB	0.00 B

Capture

Frames A	Frames B
0.00 f	0.00 f
Bytes A	Bytes B
0.00 B	0.00 B

Stopped 00:00:00
Home > System > Network configuration (1/5)

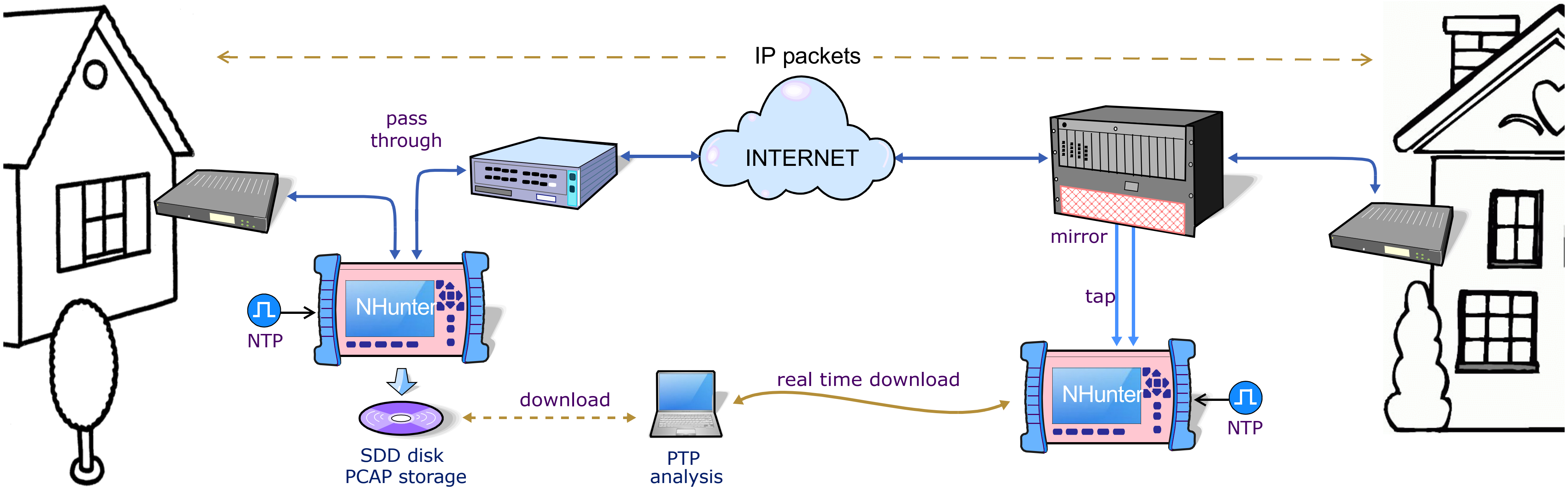
Summary

Filters

Current filter
Port A
Number 6

SNMP management

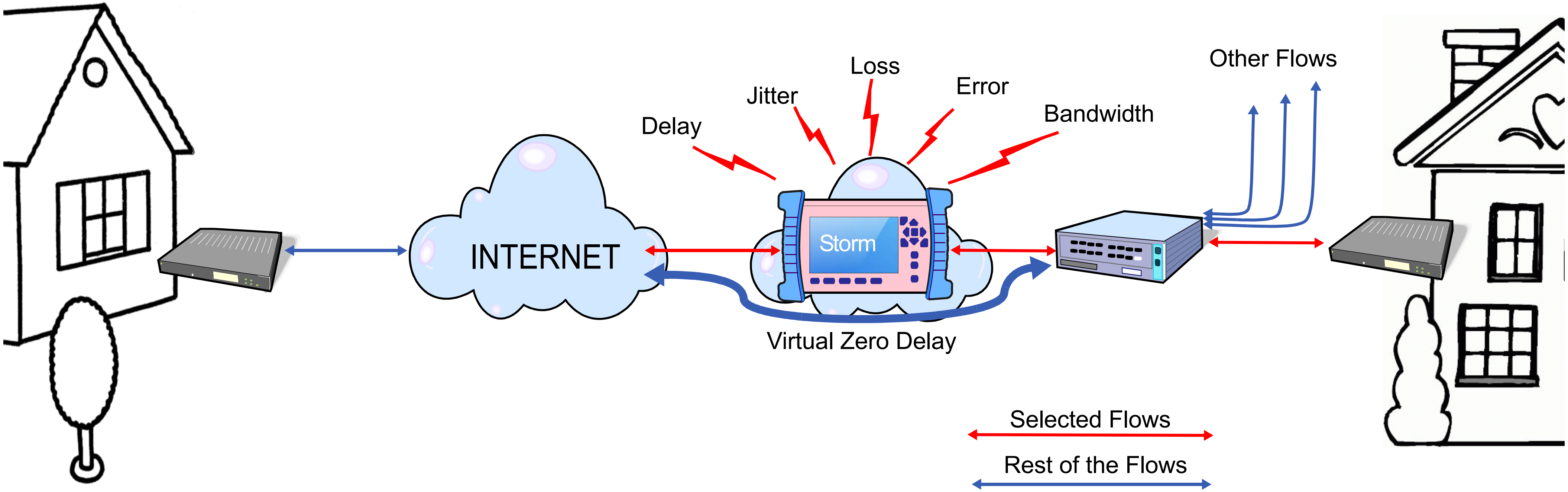
Seamless **packet captures**



Net.Hunter captures flows in both directions at wirespeed no delay & zero lost

- Captured packets are saved on SSD disk in real time and PCAP format
- 30 user programmable filters to identify, copy and paste each flow
- No limitation in captures: IP address, TCP ports, VoIP, emails, chats, arbitrary characters, etc. even non standard packets

Network **Impairments** Generation



With Net.Storm expert can simulate real WAN scenarios

- Generation -in a 100% controlled way- packets impairments
- Check how boundary clock manage vs. Packet Lost, Delay, Jitter, Error...
- Net.Storm can also be used to disturb selected traffic flows

That's all

ALBEDO Telecom

the Path to Excellence