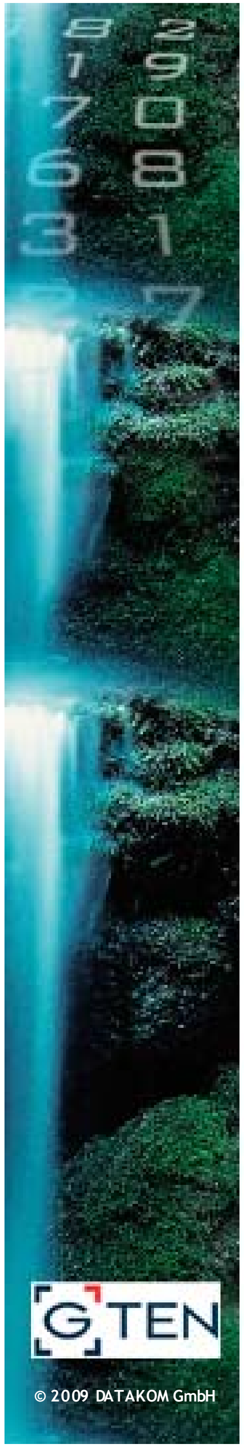
# One is enough ...

... combining

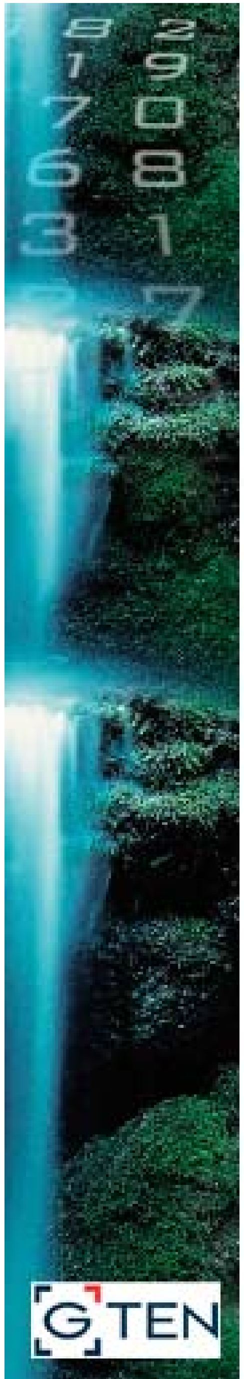
Lawful Interception,
Mediation
&
Data Retention
in IP-networks

ISS Prague June 03. - 05. 2009
Thomas Fischer



# Company

## DATAKOM GmbH
## &
## GTEN Division



## The Company

### Datakom was founded in 1986

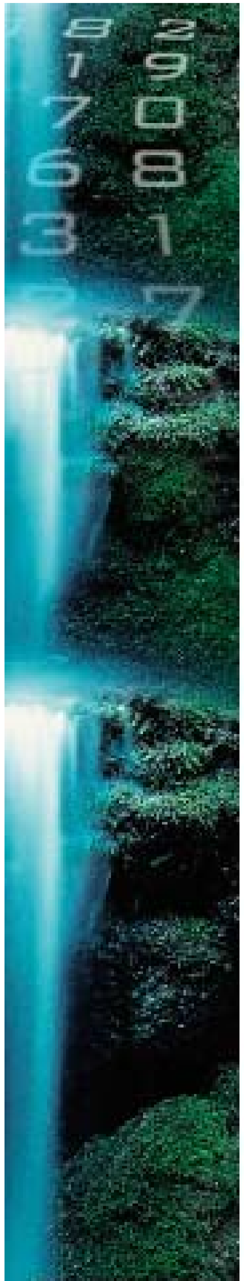
Business:

- Network Monitoring
- Network Analysis, Measurement
- Pre-deployment and appliance testing
- QoS
- SLA

### GTEN Division started in the year 2000

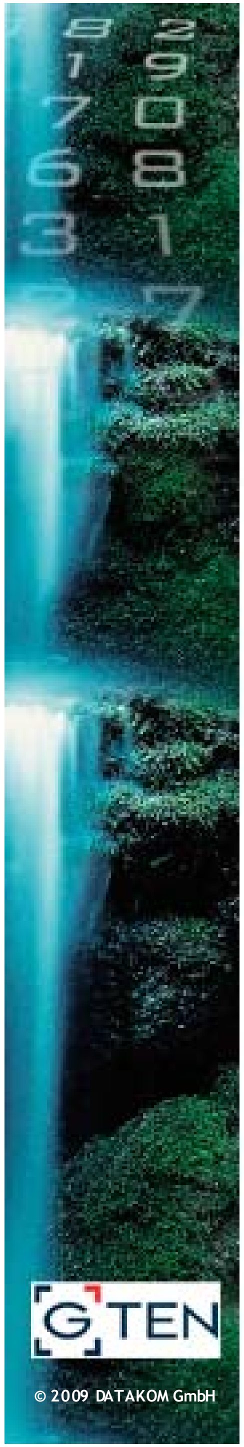
Business:

- Lawful Interception in IP networks
- Lawful Interception in Circuit Switched networks
- Data Retention
- Tactical LI Solutions (GSM, UTMS, WiFi)
- Network Security
- Subscriber / Application based network & traffic management
- Interception Center (ICC) for German Carriers / ISPs, certified by German Federal Network Agency



# Deep Packet Inspection & Processing

## DPP-Probes



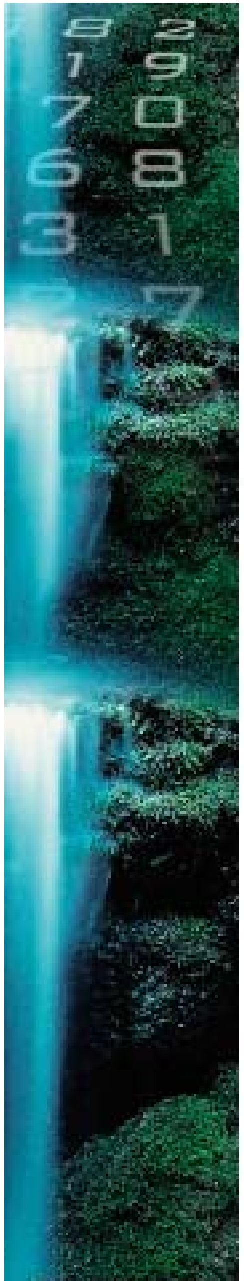
## Lawful Interception (LI)

**The challenges of LI (especially in IP networks) are:**

- increasing bandwidth, amount of data
- increasing number of subscribers
- increasing number of applications
- how to identify a specific subscriber (a target) ?
- how to identify specific applications ?
- non intrusive and not detectable
- data security
- keep the pace with network development / applications
- scalable, modular system
- ....

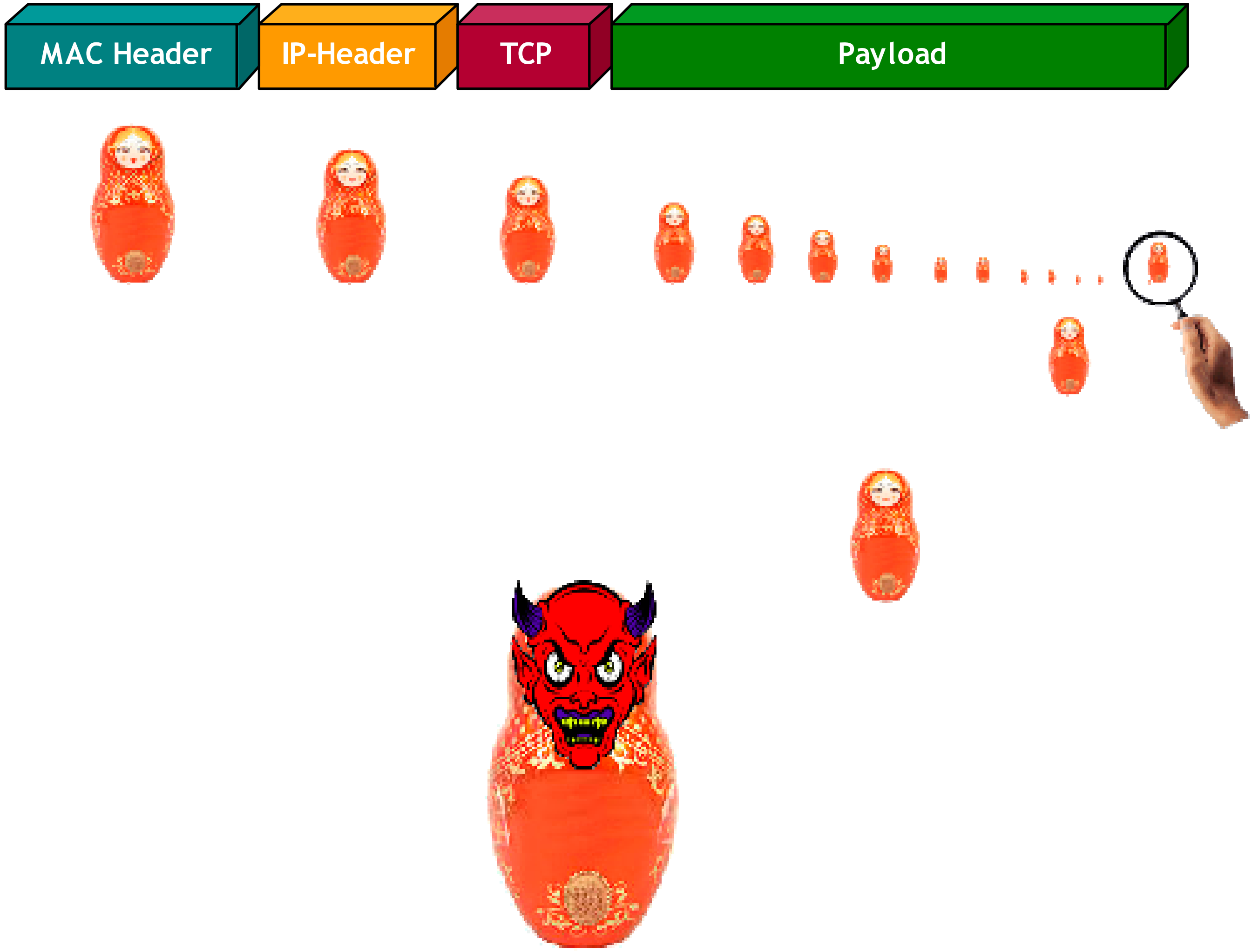
**... every bit and byte has to be analyzed ...**

**Application / Content Awareness**

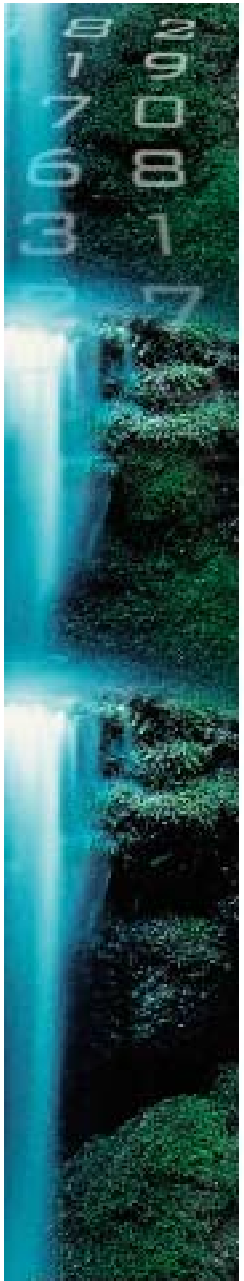


G TEN

# The problem in IP-networks ...

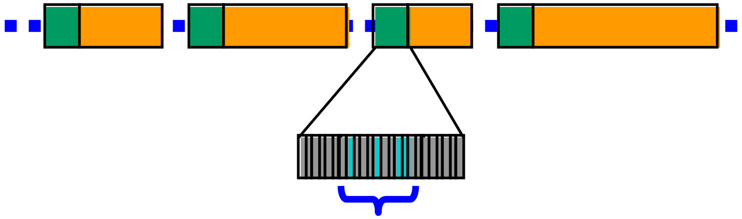


***<u>TOTAL</u> visibility at network speed is a necessity !***

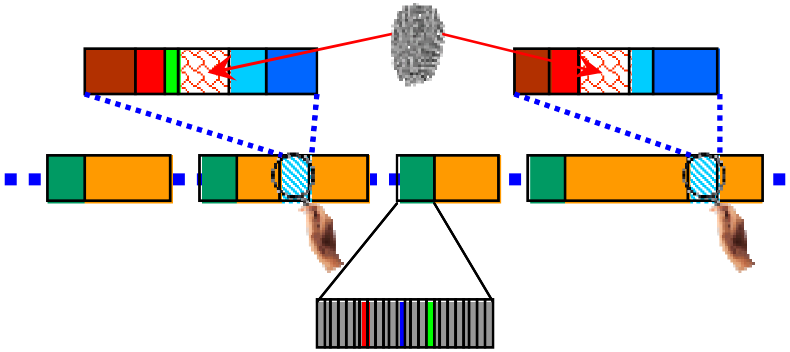


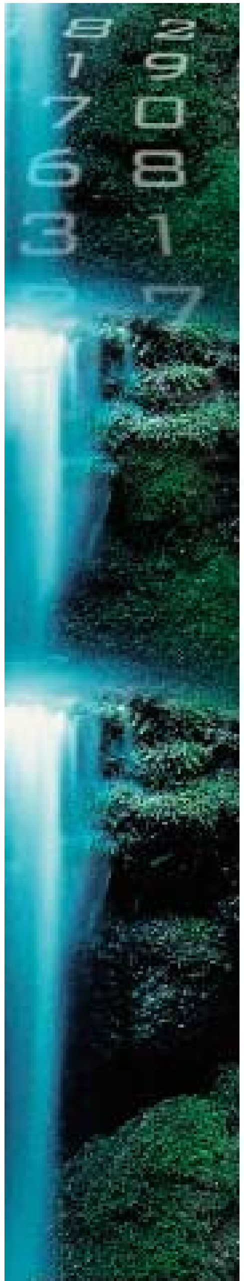
## Total Visibility needs Deep Packet Inspection / Processing

- **Header Analysis**
  - Ports

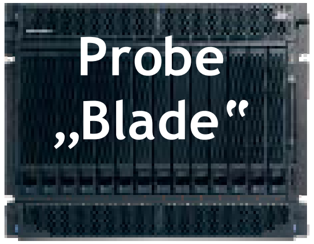


- **Signature Analysis**
  - String Match
  - Numerical
  - Behavior / Heuristic
  - Encryption / Camouflage





# ... the solution DPI/DPP-Probes ...

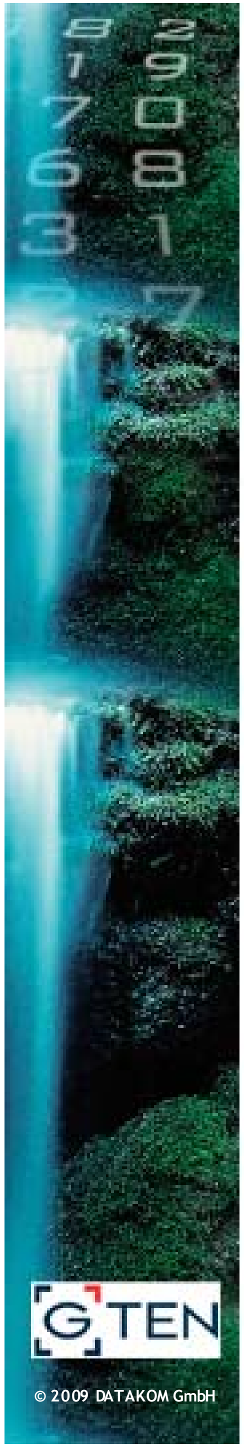


Probe
„Server“

**several Deep Packet Processing Probes (various configurations)**

- 100% packet inspection at full line speed
- full layer 2-7 packet inspection / processing (*inspect, intercept, block, ...)*
- 1 to >10 Gbit/s total bi-directional processing capacity
- scalable architecture
- Interfaces:
  - Gigabit Ethernet (Copper/Fiber)
  - 10GE
  - GE Capturing/Forwarding Ports
- over 100 Protocols / Applications are identified and can be filtered for
- target based capturing

G TEN



# DPP-Probe Filter/Target Criteria

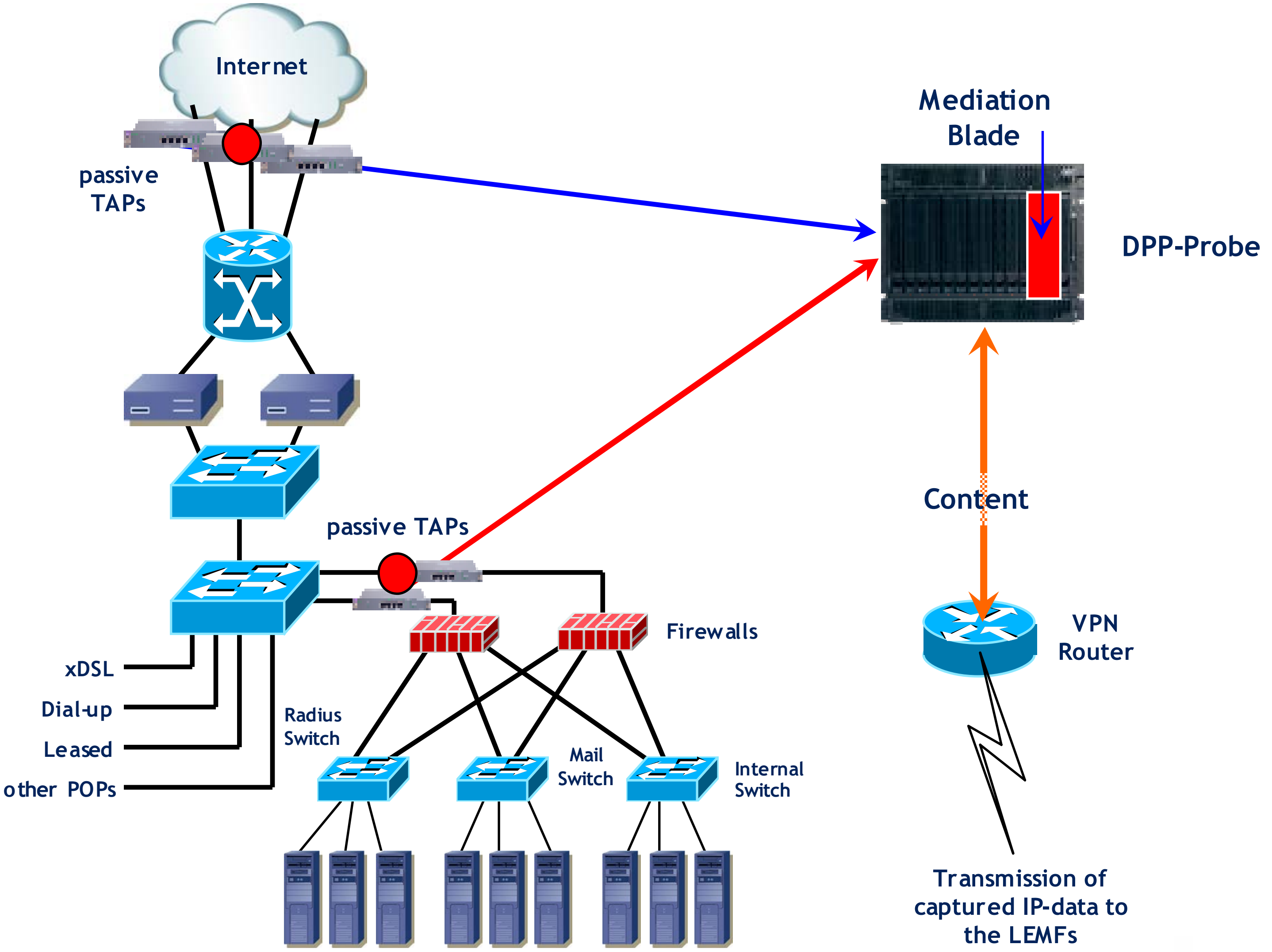
- **Peer-to-Peer Protocols (P2P)**
  - 20 Protocol types (130 variants)
- **VoIP incl. Skype**
  - 6 Protocol types (84 variants)
- **Instant Messaging (IM)**
  - 9 Protocol types (25 variants)
- **Standard Protocols**
  - 27 Protocol types (58 variants)
- **Streaming Protocols**
  - 28 Protocol types (5 variants)
- **Tunneling Protocols**
  - 11 Protocol types (5 variants)

# IP Monitoring System

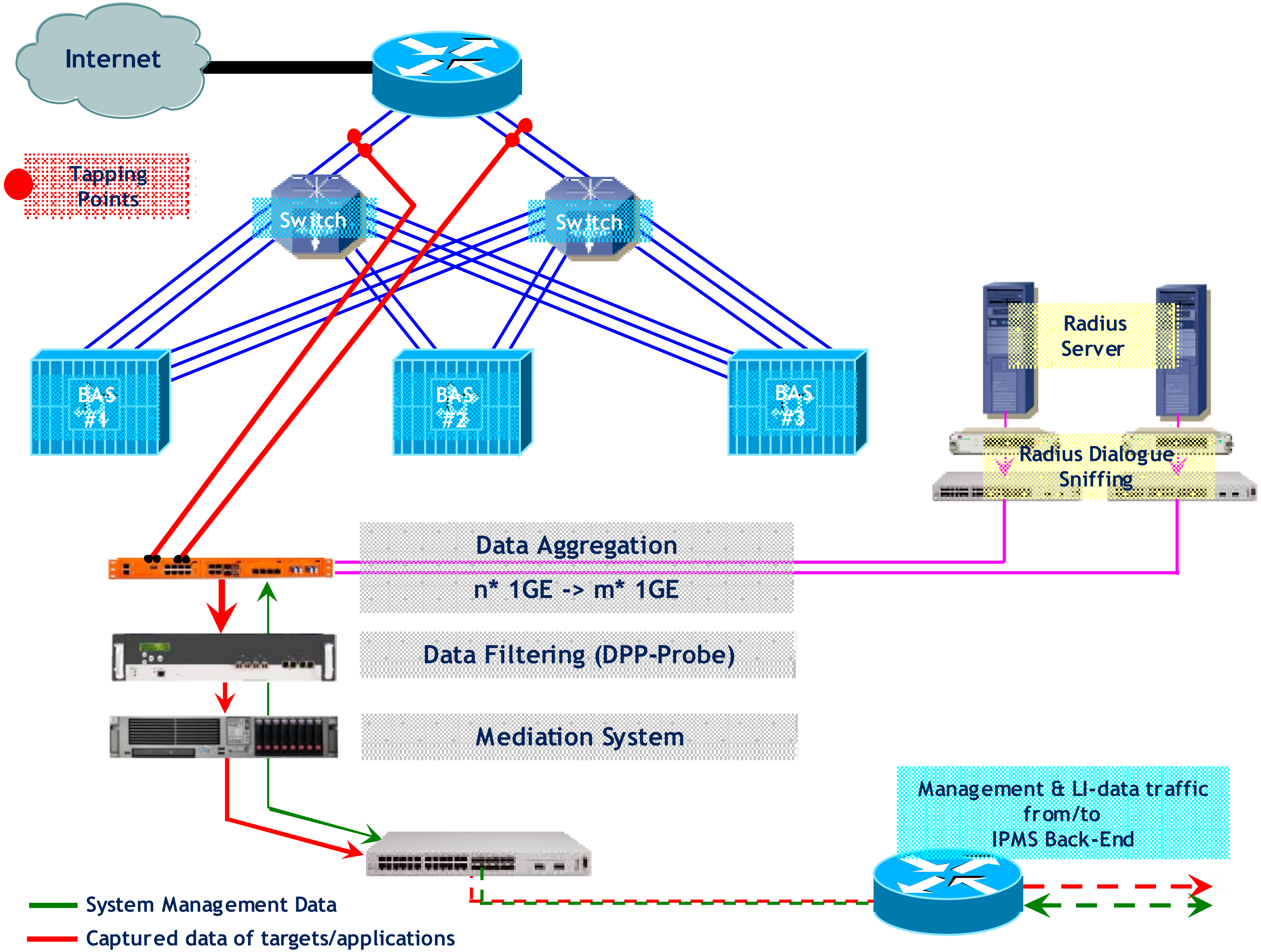
## IPIS
## IP Interception System
## (Front-End)

# IPIS Concept [ETSI]

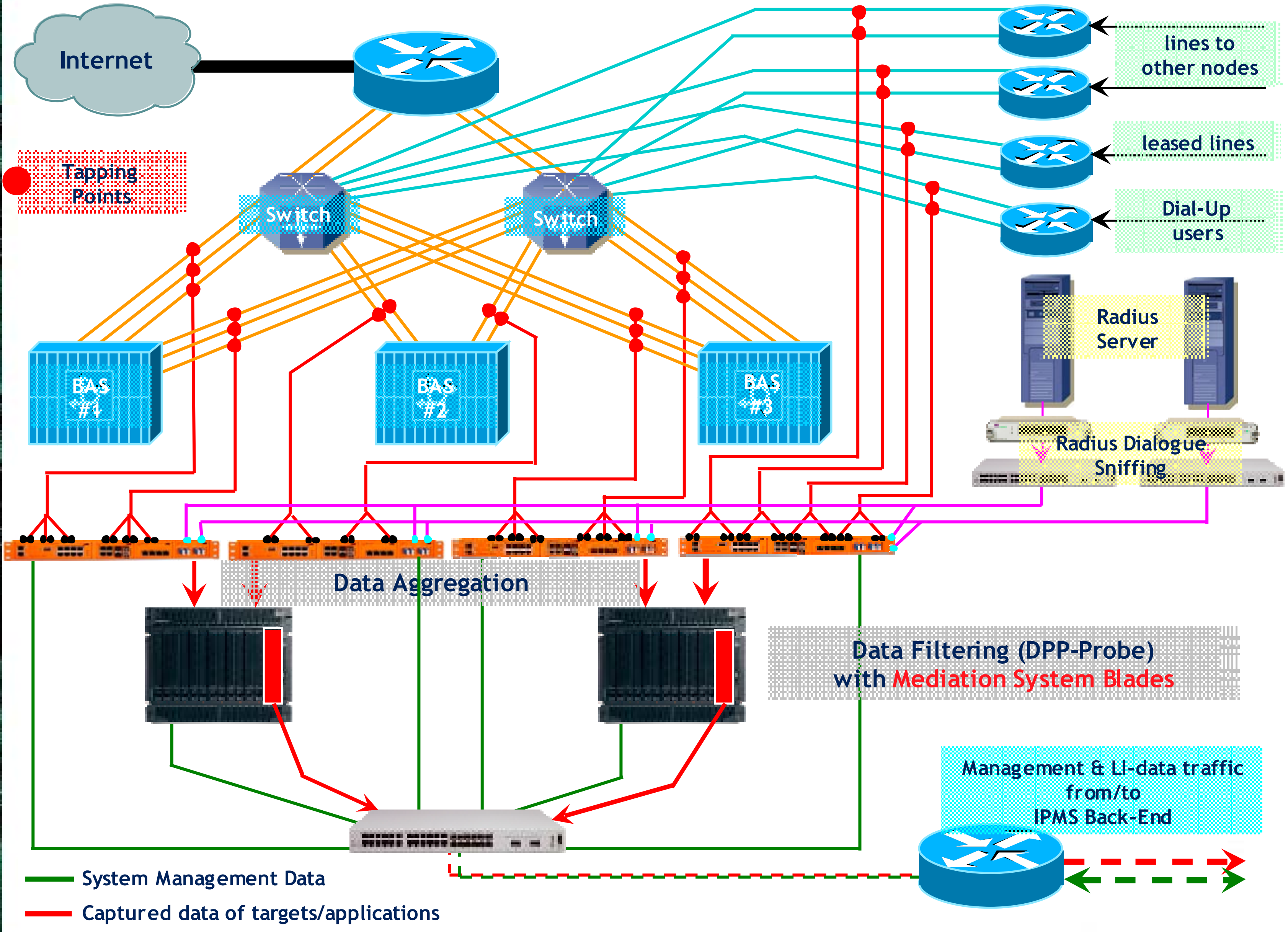
The Mediation System „converts" the captured IP-data according to ETSI-Standards and delivers it to one or more LEMFs (Monitoring Center, Back-End).

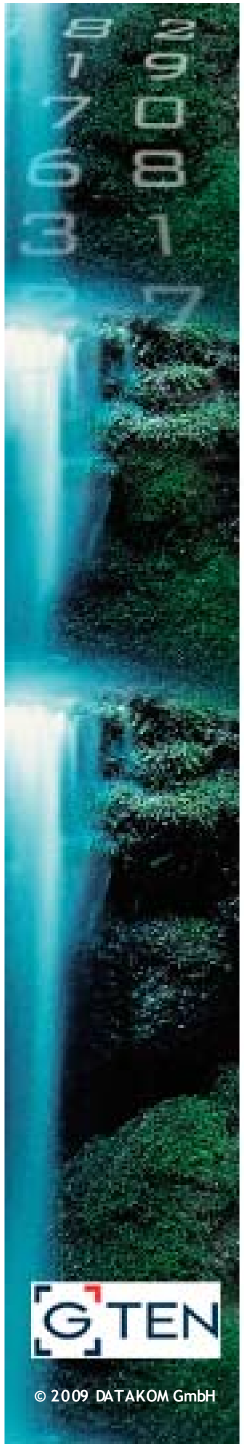


# Example 1: Simple IPIS Front-End



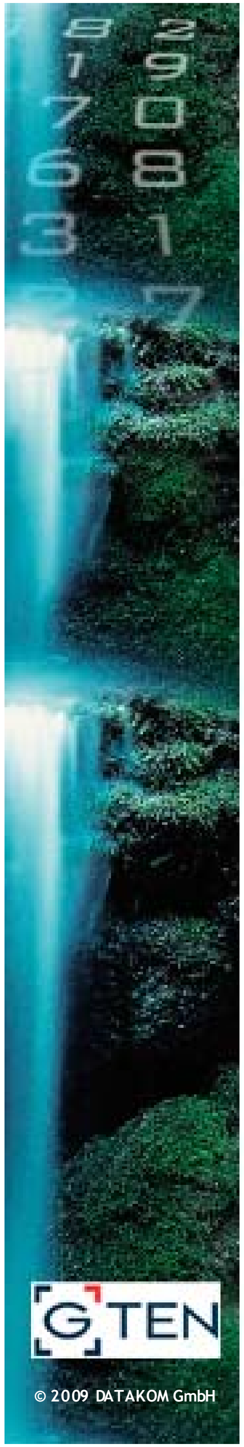
# Example 2: Complex IPIS Front-End





# IP Monitoring System

## Mediation System

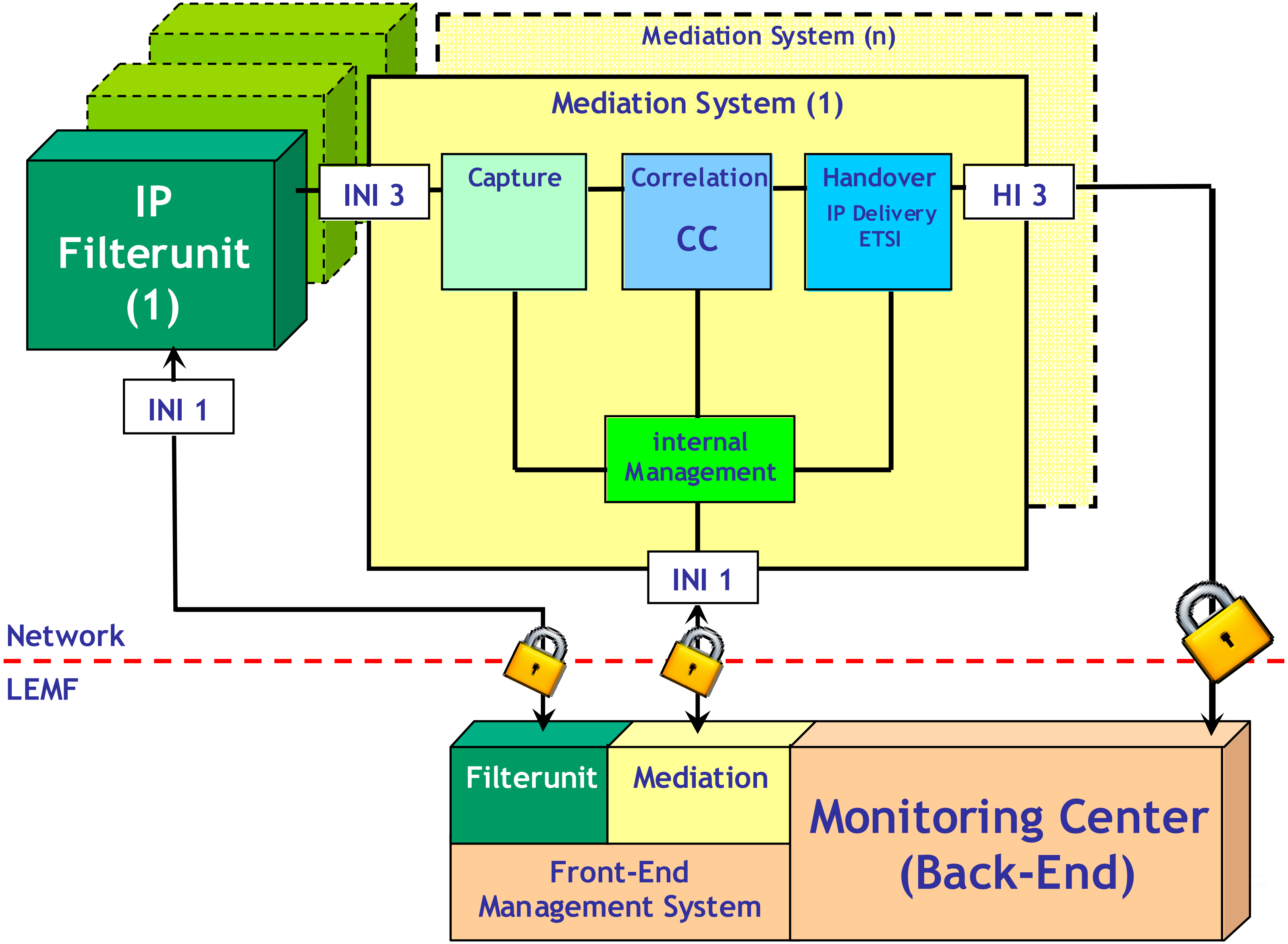


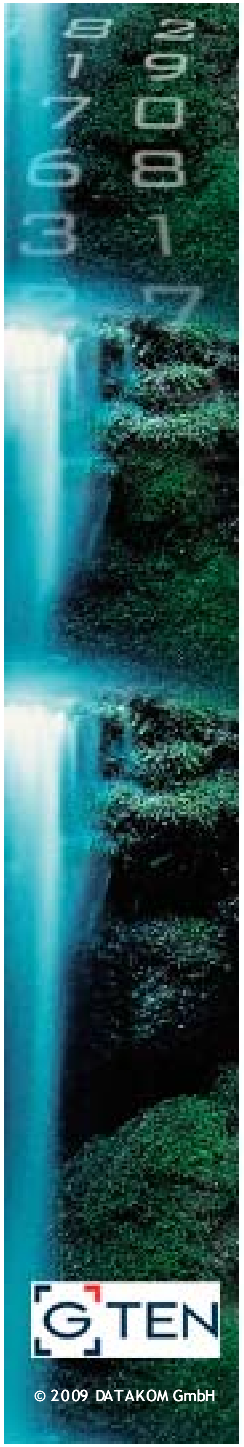
# IPMS Mediation System – General

## The Mediation System has to

- receive the captured IP-data from the DPP-Probe(s)
- correlate the data according to the warrants in the MC(s)
- convert the data into required formats (ETSI)
- distribute the data to one or more Monitoring Centers
- provide warnings about the transmission links to the MCs
- be administered together with the Probe(s)

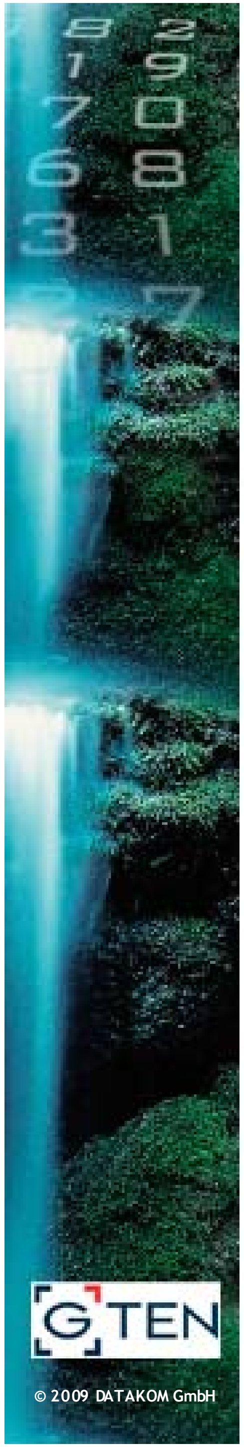
# IPMS Mediation System – Functions





# IP Monitoring System

## Data Retention

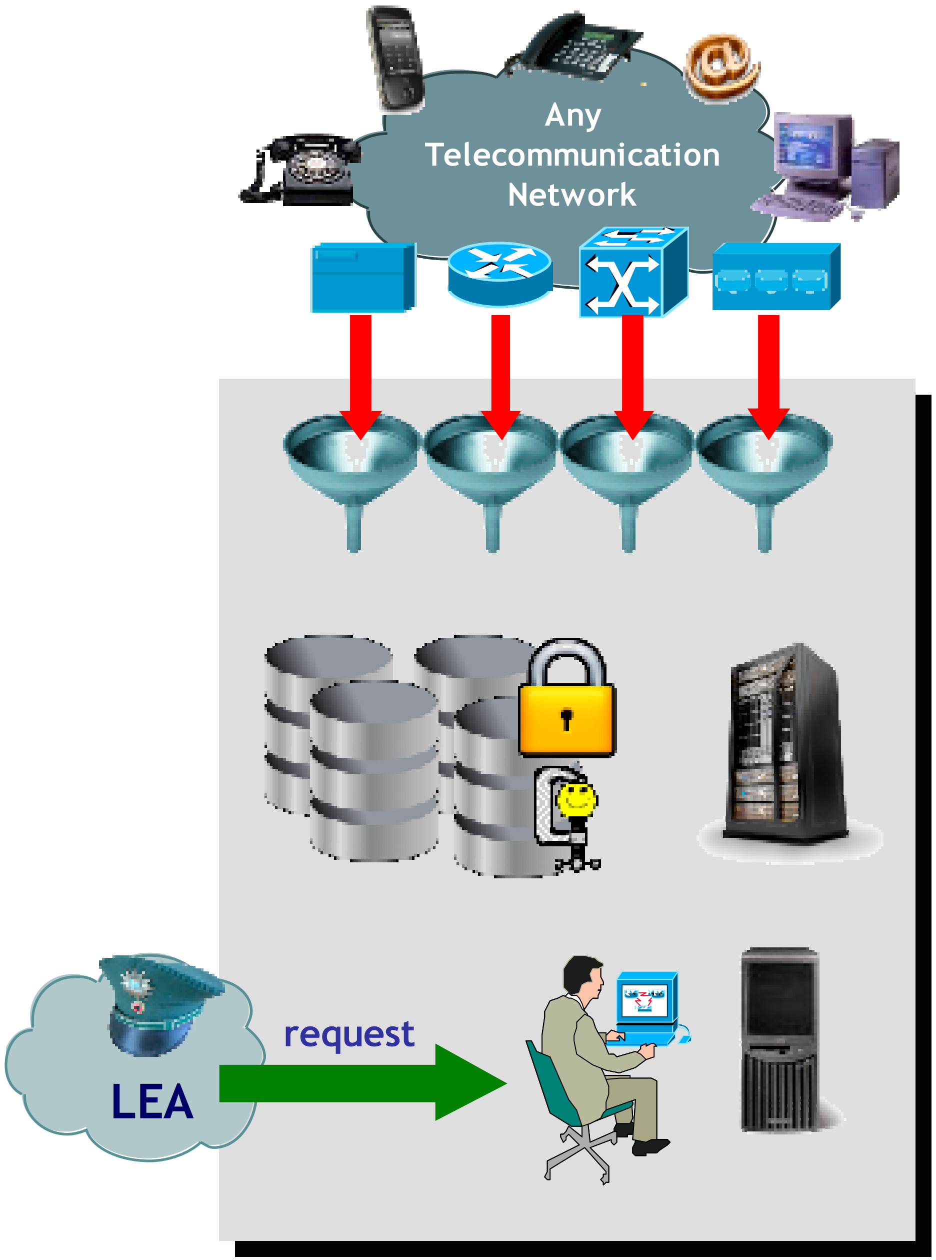


# Data Retention challenges

## The Challenges for a (IP) Data Retention ...

- International / national Technical, Privacy & Security regulations
- Increase in traffic + storage period = pushing data size to the sky
- IP-Data Retention is even more challenging (IPData Records = IPDRs)
- Huge amount of data compared to traditional telephone CDRs
- Telephony CDRs are standard and well defined; from their correctness depends the phone bill
- IPDRs may range from IP-Packets to System Logs from different hardware

# Data Retention System - Functional Groups



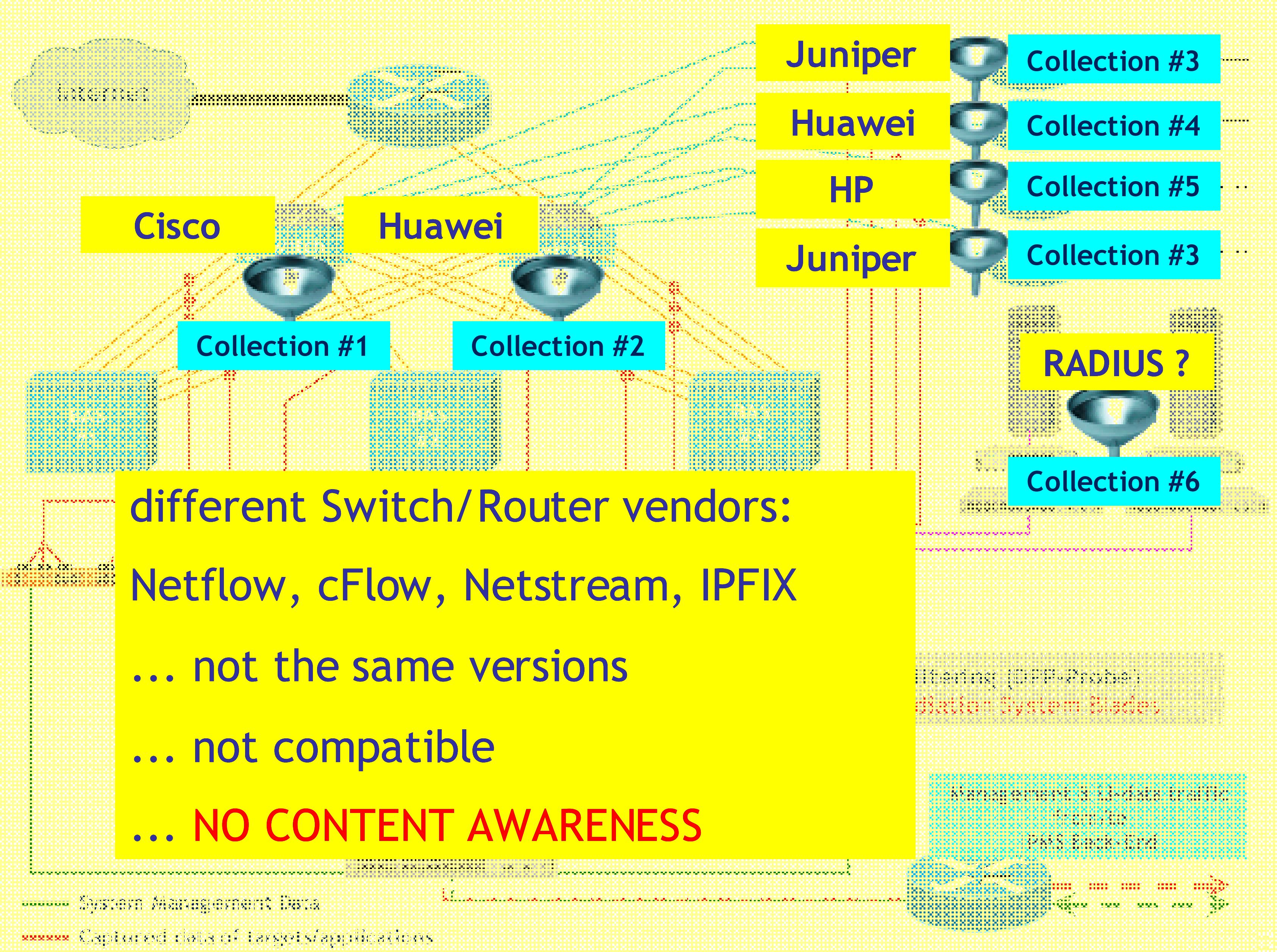
**Telco Network:**
Switches
Routers
Subscriber DB
...

Data Collection #1 - #n

Database Server
Data Warehouse

Management &
Administration

# LI in an IP-network + Data Retention on top ...



different Switch/Router vendors:

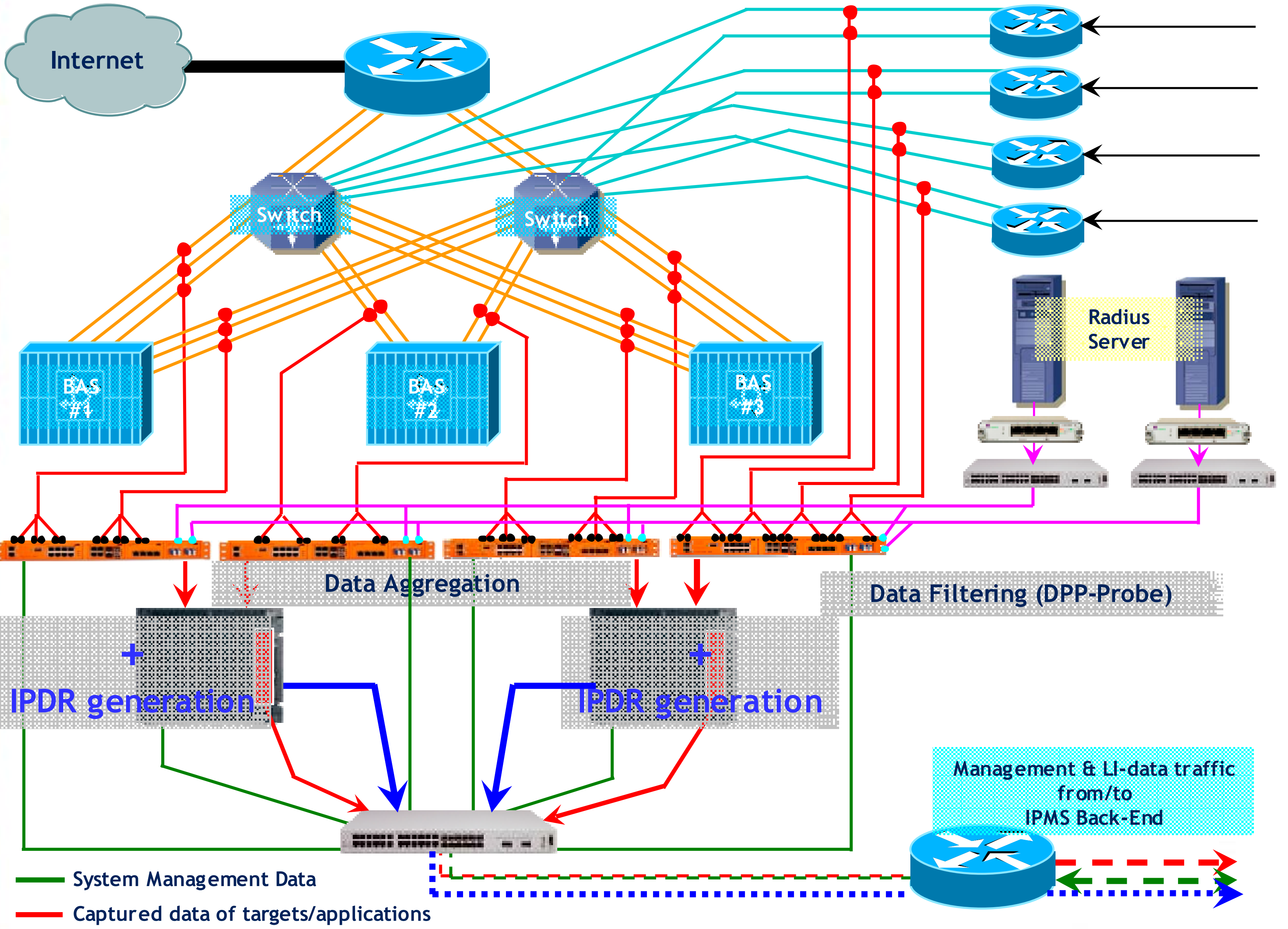
Netflow, cFlow, Netstream, IPFIX

... not the same versions

... not compatible

... NO CONTENT AWARENESS

# LI in an IP-network + INTEGRATED Data Retention ...

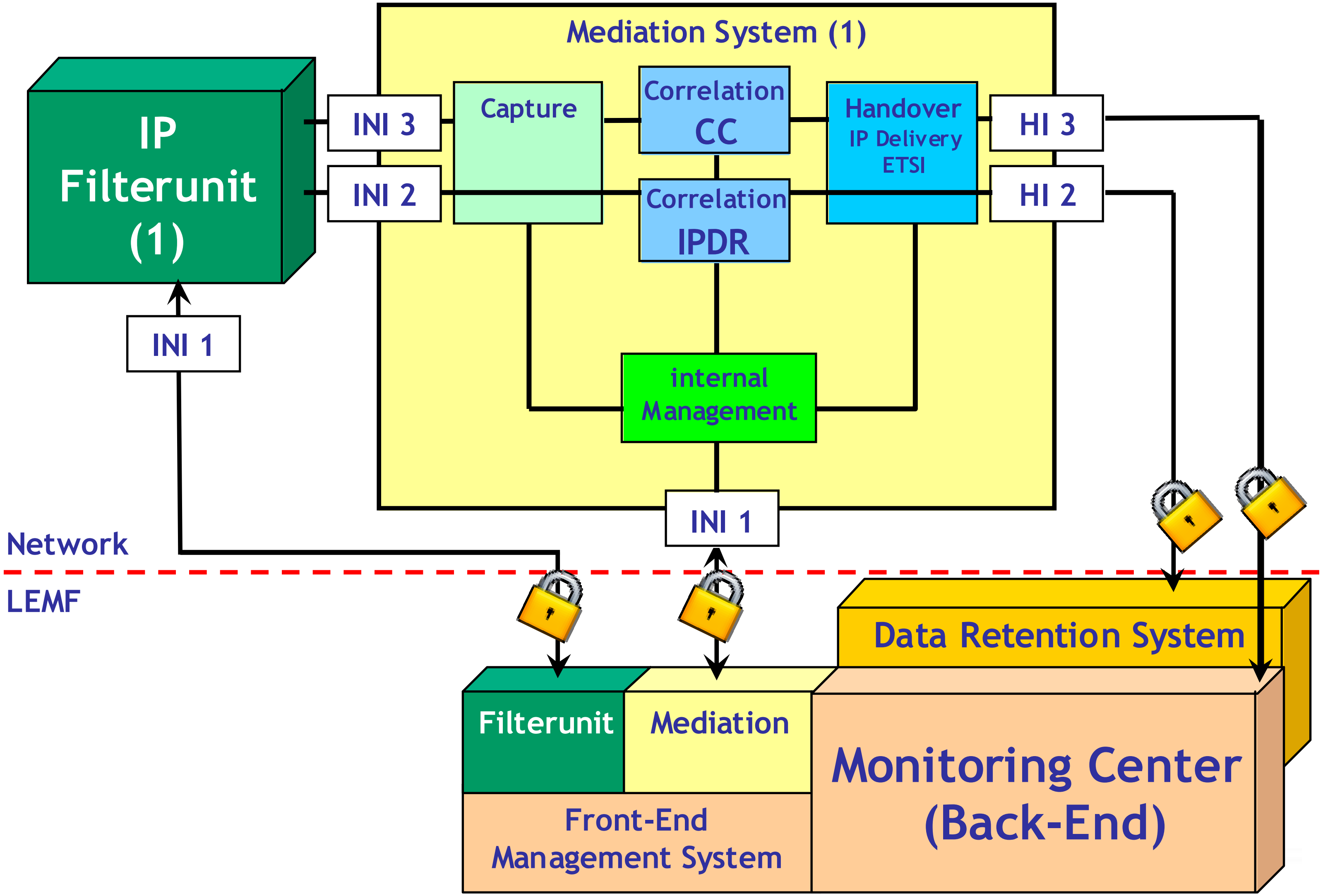


🟩 System Management Data

🟥 Captured data of targets/applications

GTEN

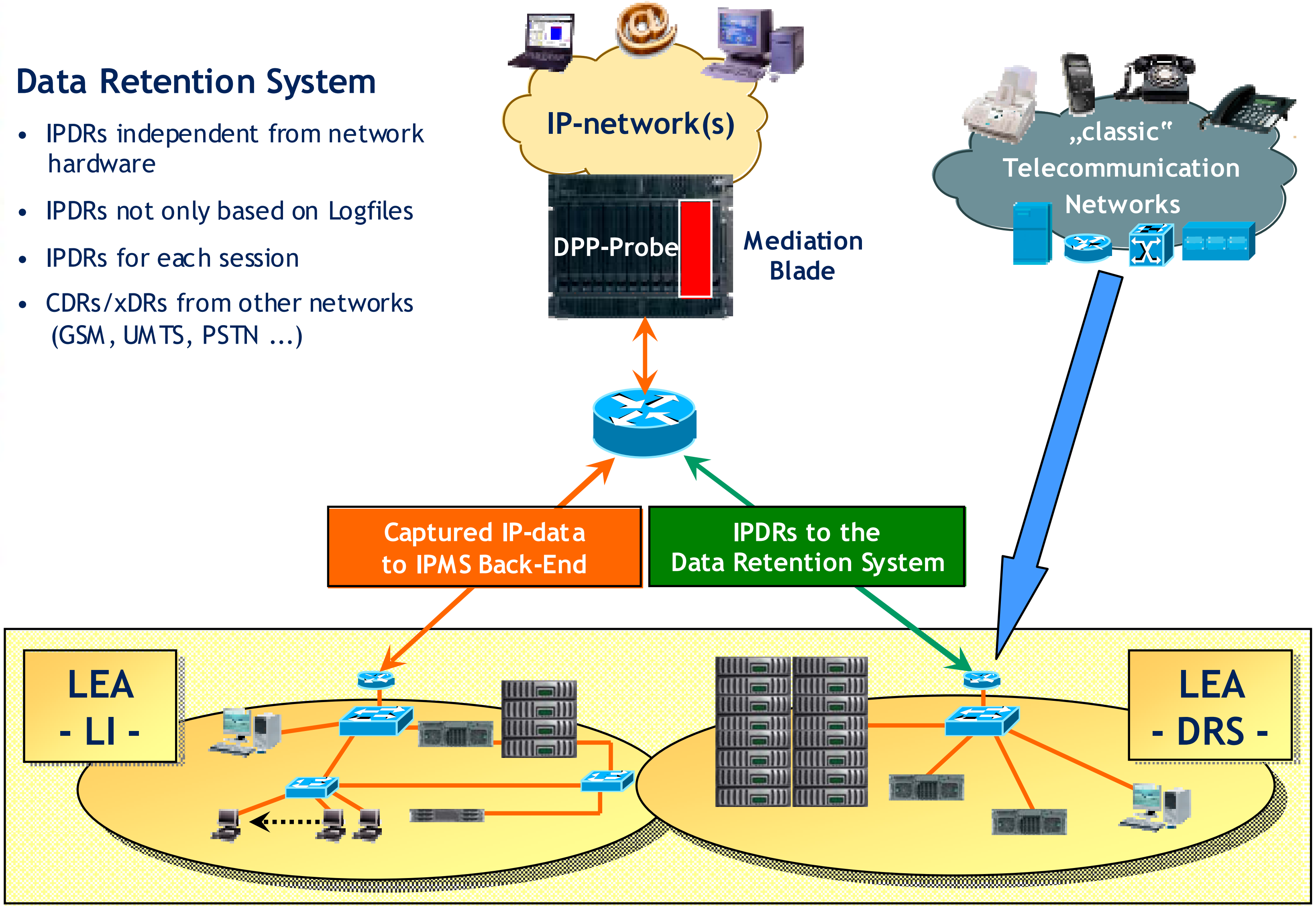
# Mediation System – Functions for IPDRs

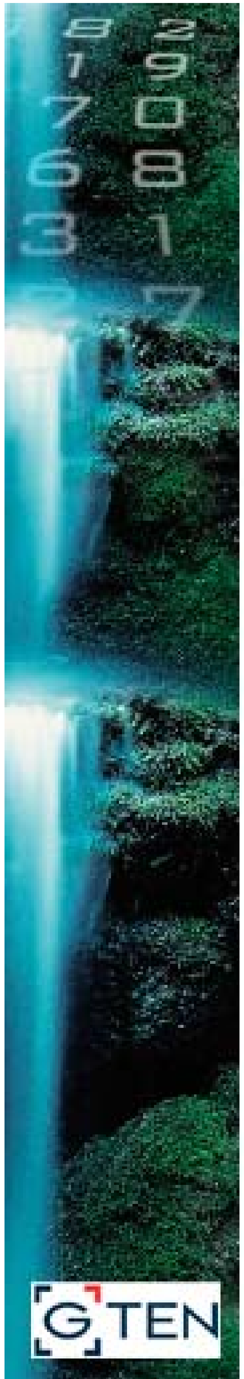


# Combined IPMS & Data Retention System

## Data Retention System

- IPDRs independent from network hardware
- IPDRs not only based on Logfiles
- IPDRs for each session
- CDRs/xDRs from other networks (GSM, UMTS, PSTN ...)


IP-network(s)
DPP-Probe
Mediation Blade
„classic“ Telecommunication Networks
Captured IP-data to IPMS Back-End
IPDRs to the Data Retention System
LEA - LI -
LEA - DRS -



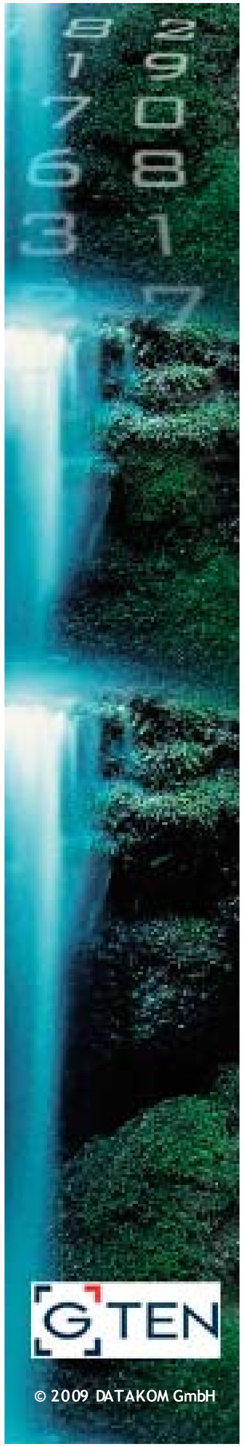
# Data Retention integrated into IP Lawful Interception

**<u>combining</u> the Data Retention with the IP Monitoring System using the same IPIS Front-End to generate and transmit the IPDRs has significant advantages:**

- **ONE** DPP-Probe for both LI & DR
- **ONE** Mediation System "
- **ONE** Management "
- **ONE** Partner "
- DPP-Probes used to capture LI-targets AND generate IPDRs for Data Retention simultaneously
- LI-Filtering PLUS <u>independent</u> IPDR-Filtering

**Saving Time, Equipment & Money**

**... ONE is enough ...**



# Summary ...

**Datakom / GTEN Division provides Turn-Key LI-Solutions**

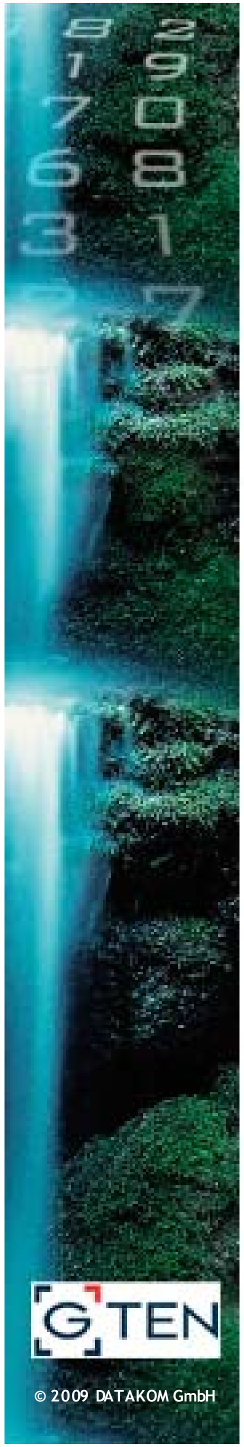
- Deep Packet Processing Probes (DPP-Probes)
- providing a subscriber based Lawful Interception
- providing Protocols & Applications based LI (WebMail, Email, FTP, ...)
- creating IPDRs for Data Retention with the same LI-Probes
- creating IPDRs for all traffic or selected by Protocols / Applications
- Network / countrywide IP Front-Ends
- Monitoring Center (for all telecommunication traffic)
- Data Retention System (for all telecommunication CDRs, IPDRs)

**... and beyond that the DPP-Probes can provide additional benefits**

- Identifying & Blocking of unwanted traffic with active DPP-Probes (Skype, URLs, VoIP ...)
- generate Traffic Statistics for all Protocols / Applications (what's going on in the network)

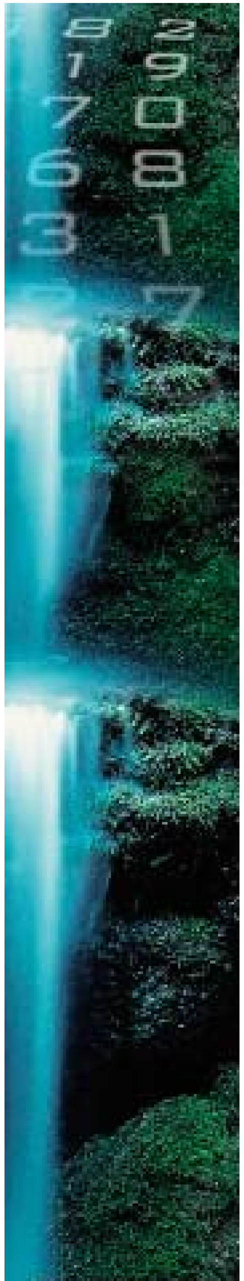
Thank you very much for your
interest in our solutions and services

Have a save trip home ...



# Some extra Slides ... (1)

## Protocols & Application DDP-Probes are able to filter/capture

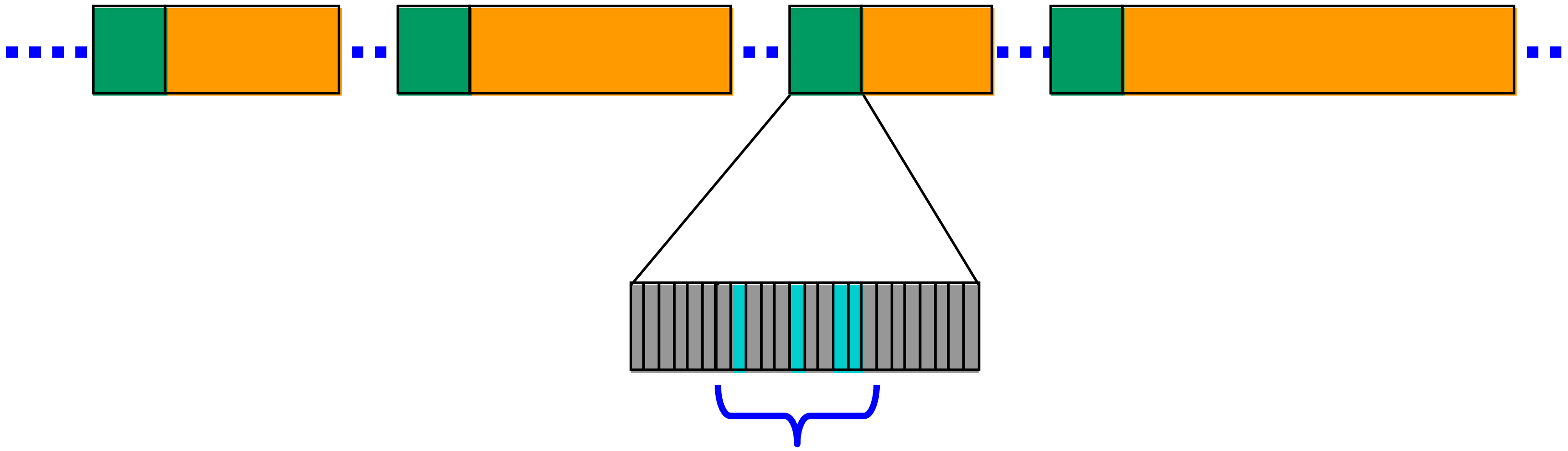


# Total Visibility needs Deep Packet Inspection / Processing

## Example: P2P-Applications

- Becoming more and more popular (BitTorrent, eDonkey, ...)
- Tremendous amount of data
  - 40% - 90% of the net traffic
  - negative impact on the net traffic
  - bandwidth consuming = decreasing performance
  - increasing communication costs
- Content is very often "dubious"
  - copyright infringement
  - illegal content
- Security risks (spyware, viruses, ...)
- Productivity decreases
- Identification difficult and control even more

# Basics – Headers only

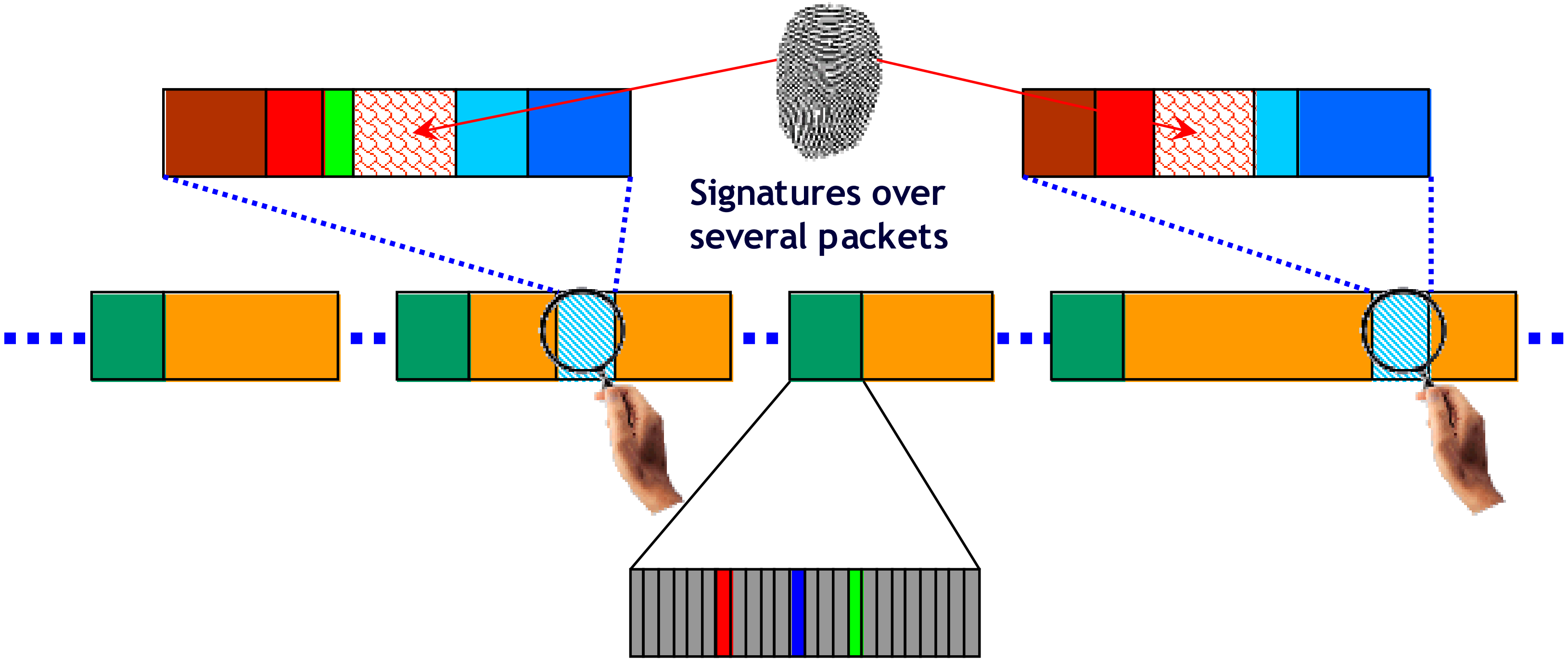


The Header is sufficient to identify the „communication intent“ but it contains no information about the Application used

In case an Application initiates additional connections for the communication, Source & Destination Addresses are not sufficient any more to identify this behavior

In addition this information is spread over several packets ...

## Sophisticated – Signatures



Signatures over several packets

Signature = recipe for identification

Signature Library to identify Applications / Protocols

Implementation of a systematical identification process for Applications / Protocols

Problem of False Positives / Negatives = Misinterpretation

Application behaves different behind a Proxy / Firewall

Challenge: „0" False Positives / False Negatives

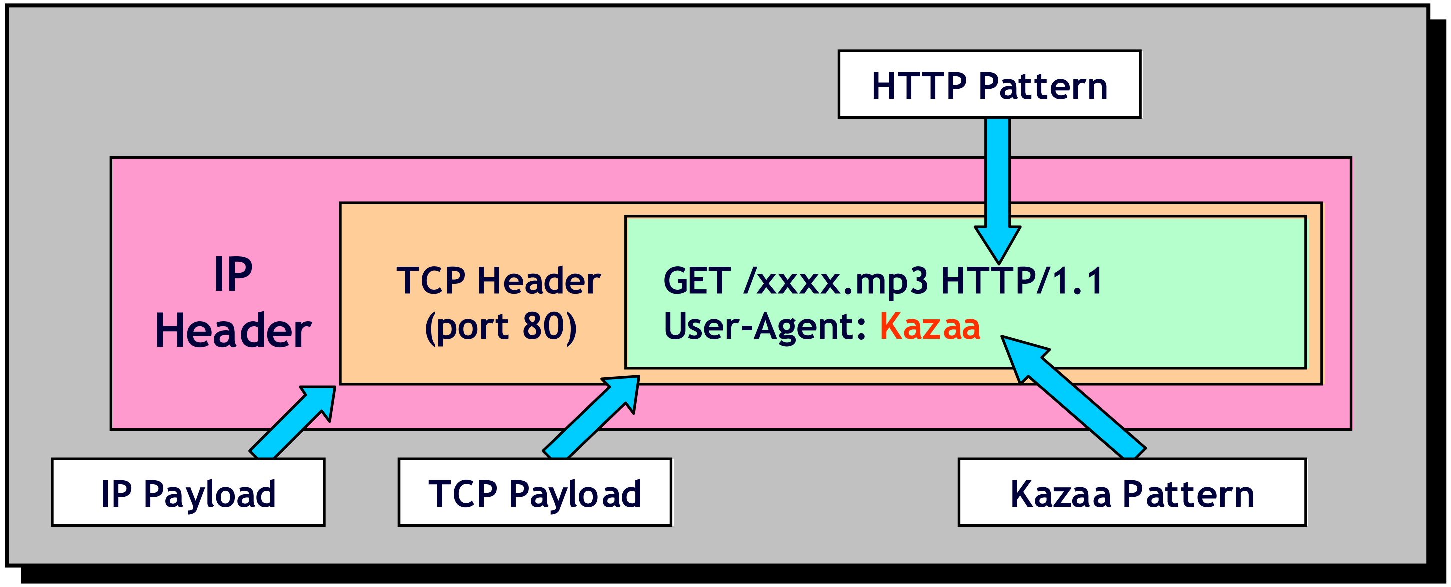
# Methods of Signature Analysis 1

- **Port-Analysis**

  only works when applications follow the rules (e.g. POP3 = 110)

- **String Match Analysis**

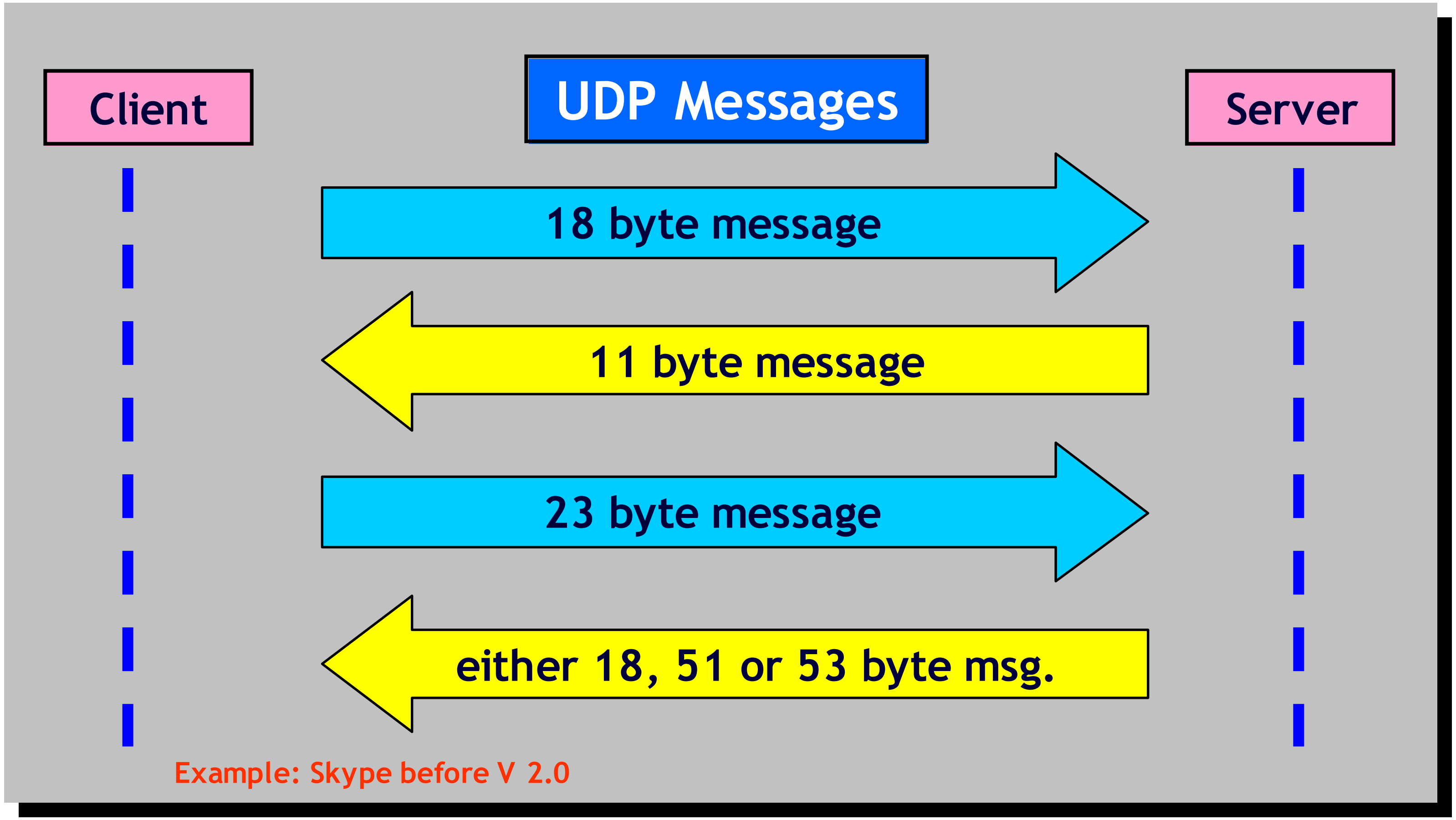
  Search for combinations of characters and/or numerical values within the data packets - across packet boarders



## Methods of Signature Analysis 2

- **Numerical Analysis**

  arithmetical / numerical characteristics within packets or session flows



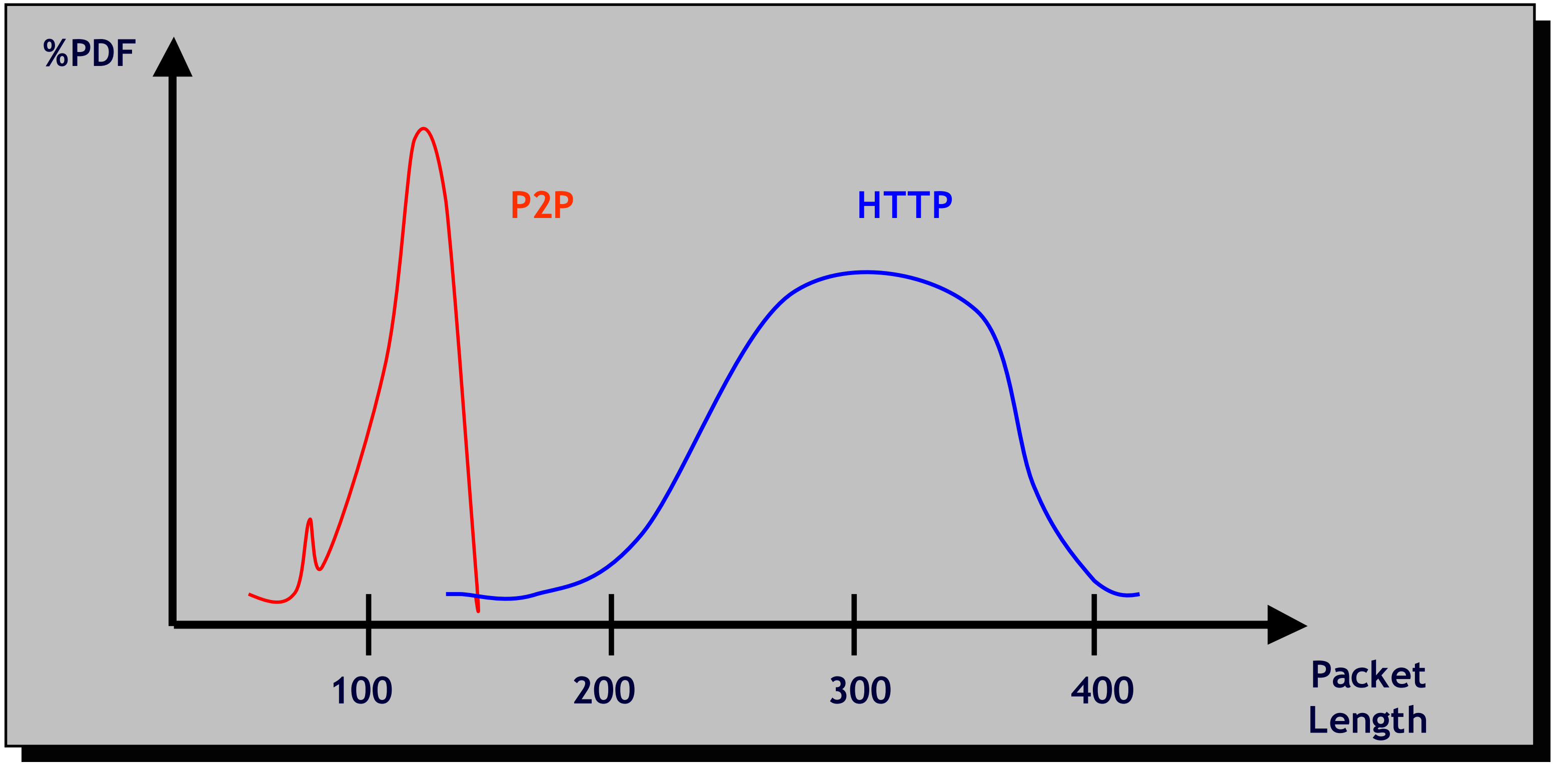
Example: Skype before V 2.0

# Methods of Signature Analysis 3

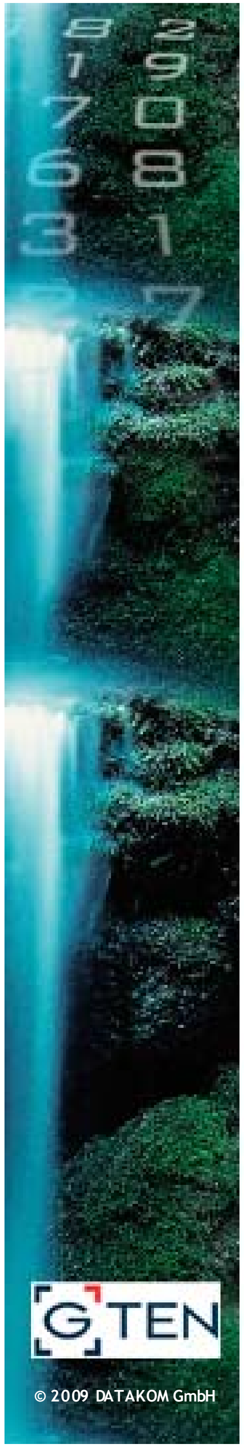
## ➢ Behavior / heuristic Analysis

Analysis using statistical data and typical patterns

(Packet Length, Packet Timing, Flow Behavior)



*Heuristic is a method to handle complex problems, which can't be solved completely by using simple rules and with the help of only few information and details.*



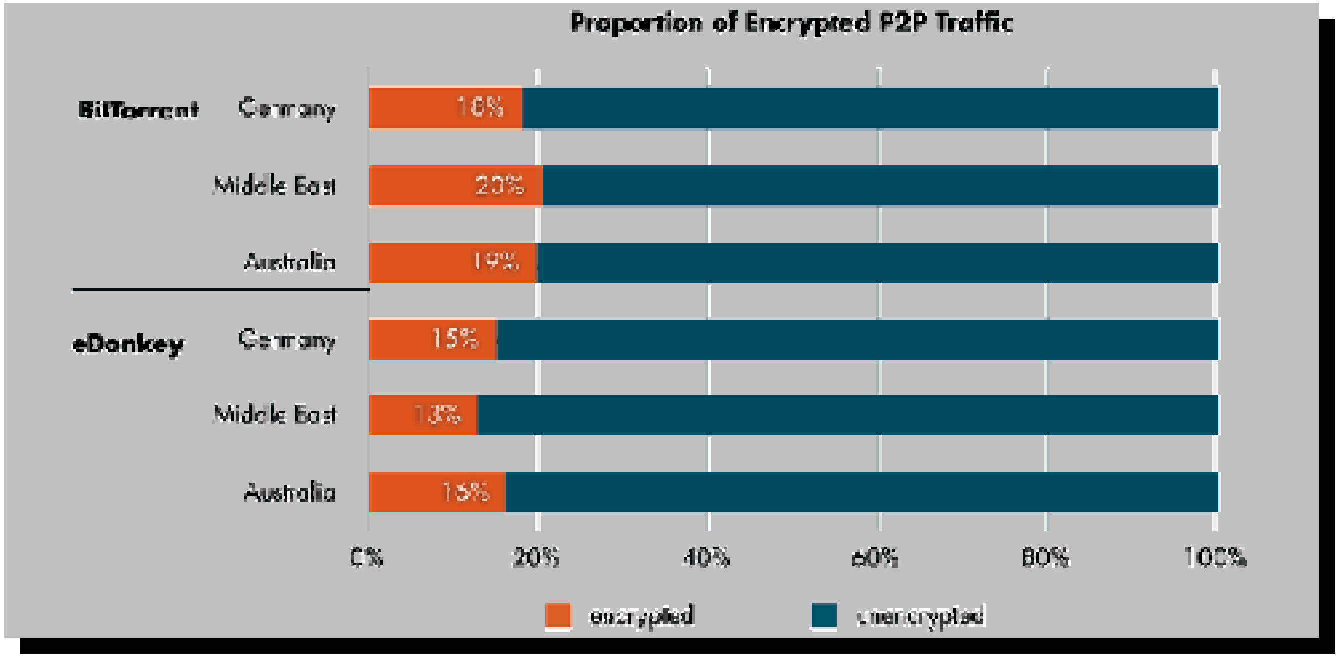
# Methods of Signature Analysis 4

## ➢ Encryption / Camouflage

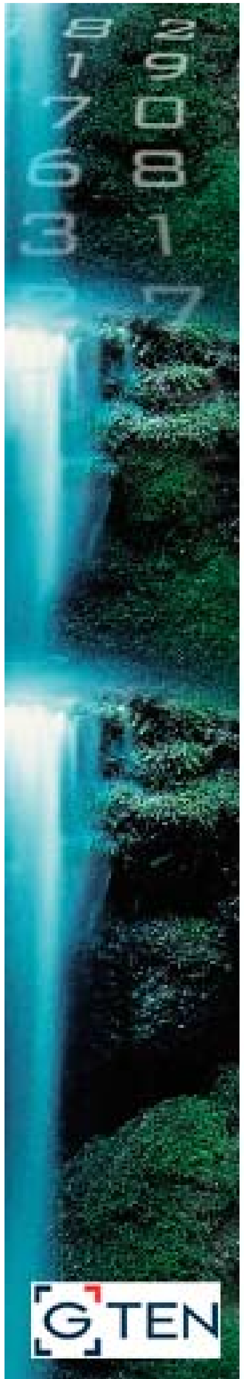
**Encryption:** protect the application and the content

**Camouflage:** hide the intent by unnecessary increase of complexity

**Encryption makes the content of communication unusable for DPI/DPP. However - the different methods of analysis still work pretty well to identify the different Applications and Protocols.**

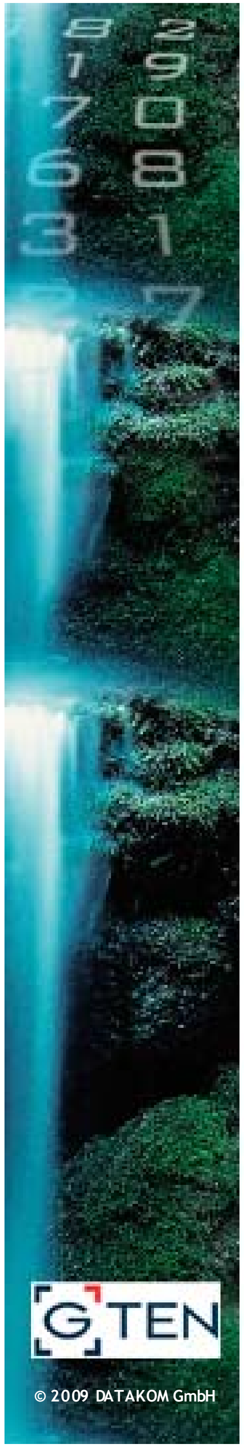


Source: ipoque Internet Study 2007



# Some extra Slides ... (2)

Protocols & Application DDP-Probes
are able to filter/capture



# IPIS Filter/Target Criteria (1)

## Peer-to-Peer (P2P)

| | | | | |
|---|---|---|---|---|
| AppleJuice | eDonkey (12) | iMesh (3) | OpenFT | Thunder / Webthunder |
| Ares (2) | Filetopia | KaZaa / Fasttrack (6) | OFF | WinMX |
| BitTorrent (51) | Freenet | Manolito (3) | Pando | Winny |
| DirectConnect (21) | Gnutella (26) | Mute | SoukSeek (2) | XDCC (3) |

## Voice over IP (VoIP) / Skype

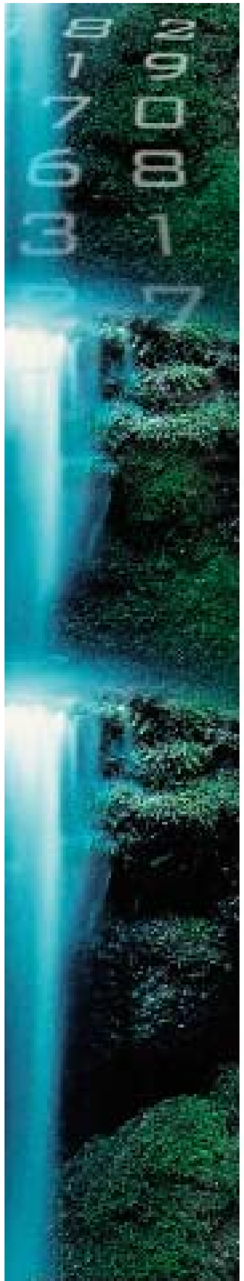
| | |
|---|---|
| H.323 (4) | SIP (7) |
| IAX (10) | Skinny |
| MGCP | Skype (73) |

## Instant Messaging (IM)

| | | | | |
|---|---|---|---|---|
| Gadu-Gadu | QQ | Oscar (7) | Paltalk | PoPo |
| IRC | Jabber/Google Talk (6) | MSN (6) | Yahoo (6) | |

## Standard Protocols

| | | | | |
|---|---|---|---|---|
| Citrix | HTTP | NFS | PostgreSQL | SSDP |
| BGP | ICMP | NTP | RDP | Telnet |
| DHCP | IGMP | OSPF | SMB/CIFS | Usenet |
| DNS | IMAP | pcAnywhere | SMTP | VNC |
| EGP | MySQL | POP3 | SNMP | Direct Download Link (58) |
| FTP | RADIUS | | | |



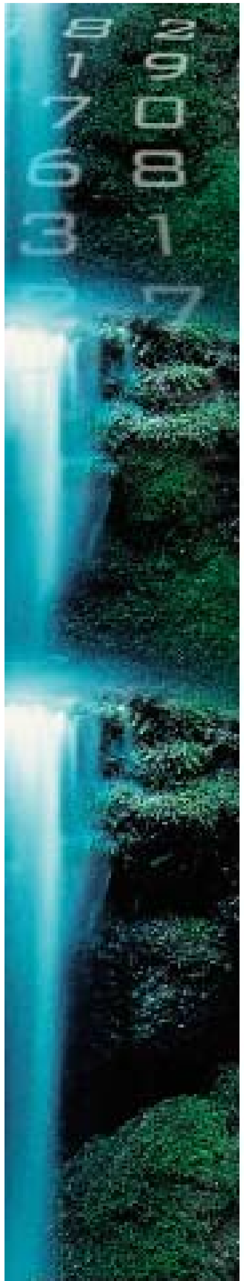
# IPIS Filter/Target Criteria  (2)

| Streaming Protocols | | | |
|---|---|---|---|
| AVI | Move | Real Media Stream | TVAnts |
| Feidian | MPEG | RTP | TVUPlayer |
| Flash (5+) | OGG | RTSP | UUSee |
| Icecast | PPStream | SCTP | V CAST |
| Joost | QQLiveMedia | SHOUTcast | VeohTV |
| Kontiki | QQLivePlayer | Slingbox | Windows Media Stream |
| MMS | QuickTime | SopCast | Zattoo |

| Tunnel Protocols | | | |
|---|---|---|---|
| SSL (5) | IPsec | SSH | VPN-X |
| GRE | OpenVPN | Tor | VTun |
| HamachiVPN | SoftEthernet | VPN | |

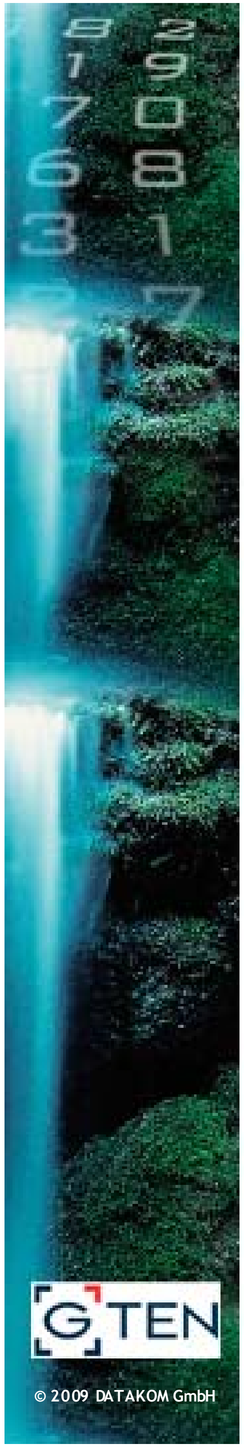
## over 120 protocols / applications are

- detected
- analyzed
- filtered

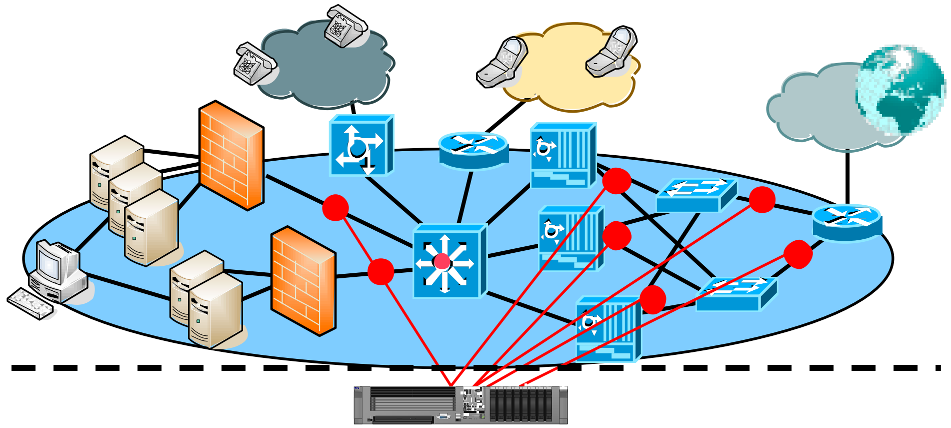


# Some extra Slides ... (3)

## Functional Parts of an
## IP Monitoring System
## (IPMS)



# The 3 (4) functional parts of an IPMS



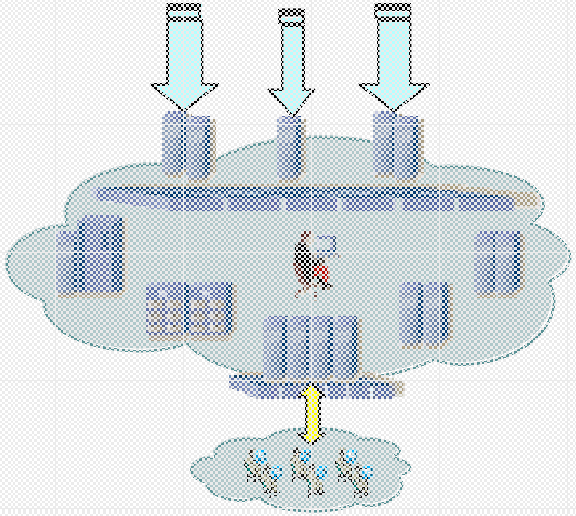
## IP Interception System (IPIS - Front-End)

IP-data filtering:
- Targets
- Applications

## Mediation System(s)

● = Tapping Points (Monitoring Sites) in the IP-Networks

Secured Data Transmission
& Management
FE -> BE



## Any Monitoring Center (MC - Back-End)

- recording
- storing
- archiving
- decoding
- evaluation