QOSMOS
Your Network is Information

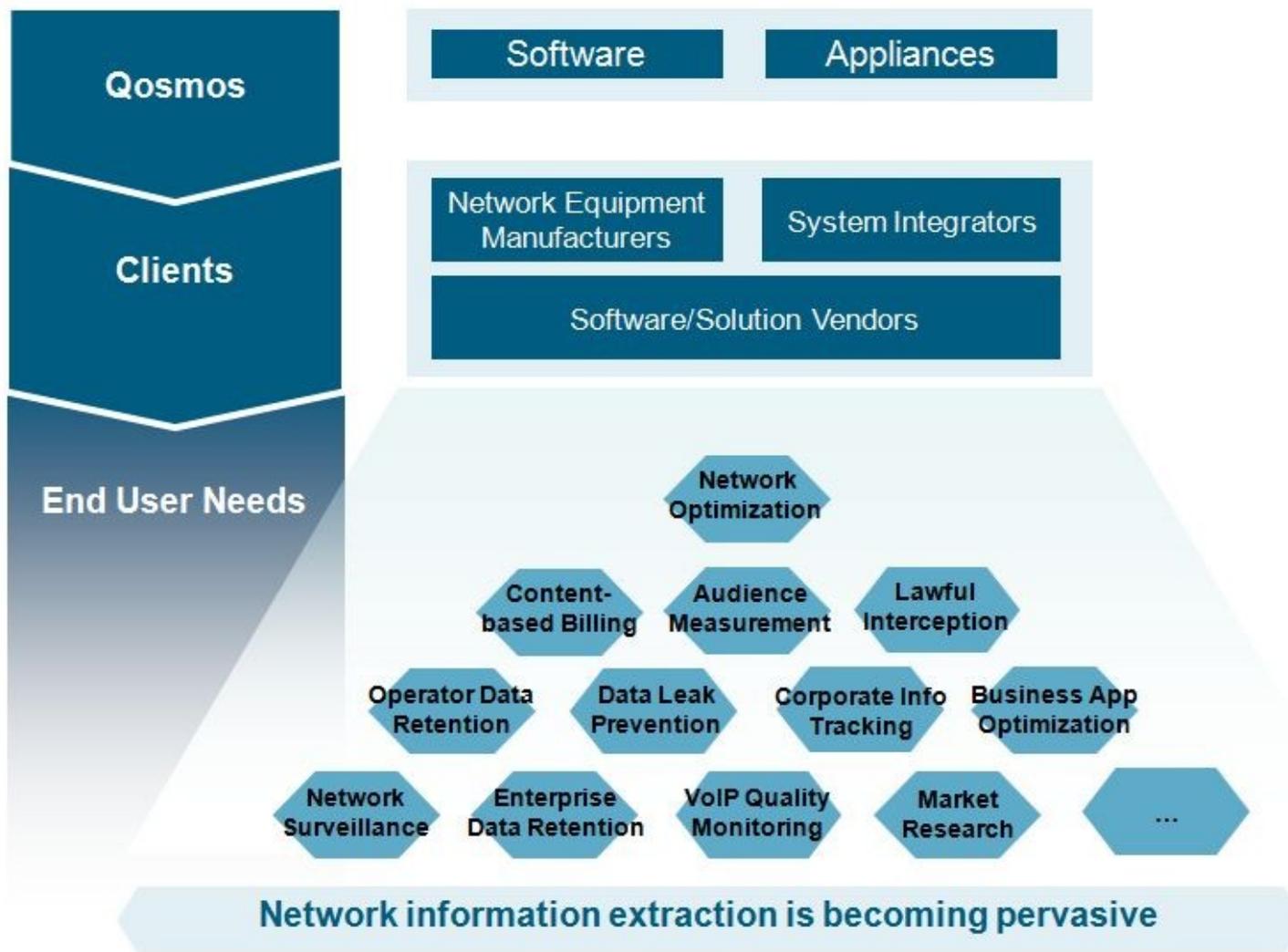# Network Intelligence Technology Introduction

Frederic Rivart, Senior SE
December 12th, 2008

Qosmos : Network Intelligence Vendor

- Founded in 2000 by members of the LIP6 Computer Research Laboratory, Paris
- Backed by leading VCs, Sofinnova Partners & Alven Capital, research organization GfK Group
- Several patents
- International presence in EMEA, US and APAC
- Member of dPacket.org & TM Forum
- Technology Partners
  - Freescale, Cavium Networks, Continious Computing, GE Fanuc, Raza Microelectronics, WindRiver

Market Approach

Qosmos

Software | Appliances

Clients

Network Equipment Manufacturers | System Integrators

Software/Solution Vendors

End User Needs

Network Optimization

Content-based Billing | Audience Measurement | Lawful Interception

Operator Data Retention | Data Leak Prevention | Corporate Info Tracking | Business App Optimization

Network Surveillance | Enterprise Data Retention | VoIP Quality Monitoring | Market Research | ...

Network information extraction is becoming pervasive

QOSMOS
Your Network is Information

Product Portfolio

Qosmos ixEngine
Information eXtraction Engine
(Software Libraries)

Qosmos ixEngine
- Software suite that enables developers to implement powerful Network Intelligence features in their products

Qosmos ixEngine Protocol Plugin Creator
- Specially designed for the creation of new/custom protocol plugins

Product Range
- x86/32bits
- x86/64bits
- RMI XLR
- Cavium Octeon
- Freescale PowerQUICC

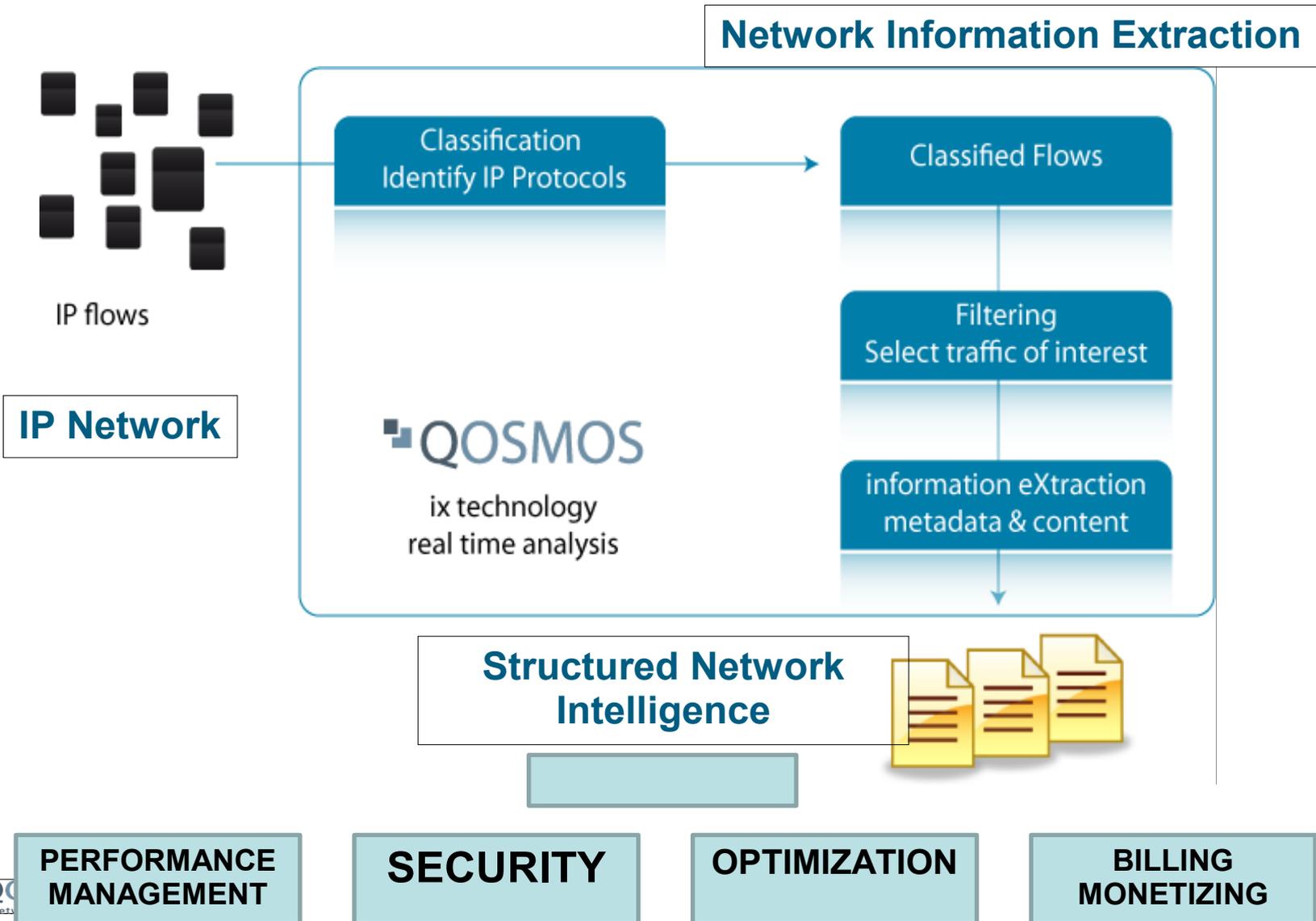## Qosmos ixMachine
Information eXtraction Machines

Qosmos ixMachine
- Hardware appliances that extract extremely fine-grained information from the network to feed third-party systems

Product Range
- ixM 10 Series: CPE (~ 10s Mbps)
- ixM 100 Series: Access (~ 100s Mbps)
- ixM 1 000 Series: Edge (~ Gbps)
- ixM 10 000 Series: Core (~ tens of Gbps)

Network Intelligence: How to Make Sense out of Network Traffic

Network Information Extraction

IP Network

IP flows

Classification
Identify IP Protocols

Classified Flows

Filtering
Select traffic of interest

QOSMOS
ix technology
real time analysis

information eXtraction
metadata & content

Structured Network Intelligence

PERFORMANCE MANAGEMENT	SECURITY	OPTIMIZATION	BILLING MONETIZING

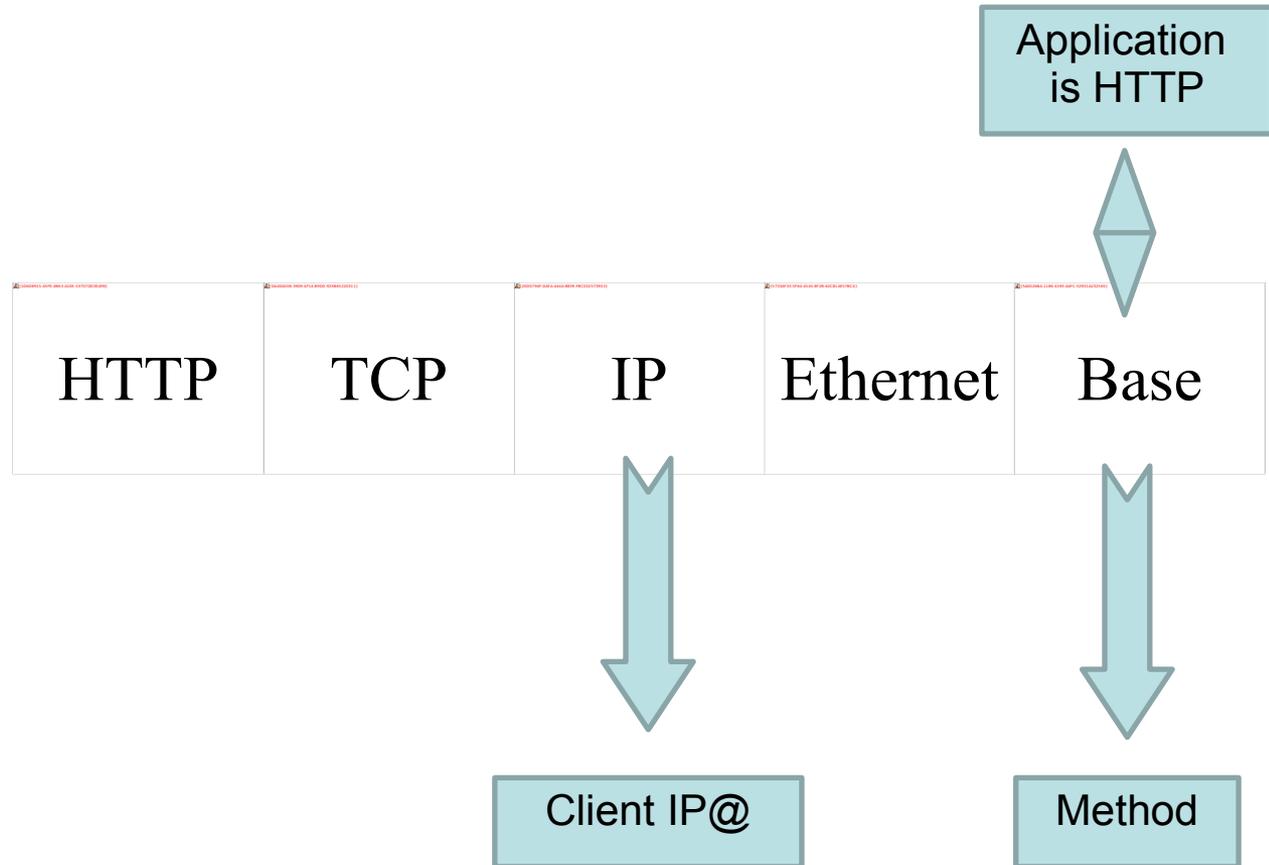# Application Classification

- Classification need:
  - Attributes and Content extraction is application dependant.
  - Reliable and easy to use filter.
- Classification technologies
  - Packet based analyses
    - TCP Port mapping
    - Packet signature (Pattern matching)
  - Session based Analyses
    - Session Grammar Analyses
    - Session Inheritance Analyses
- Classification Path
- Classification Attribute

Application Classification

- Classification need:
  - Attributes and Content extraction is application dependant.
  - Reliable and easy to use filter.
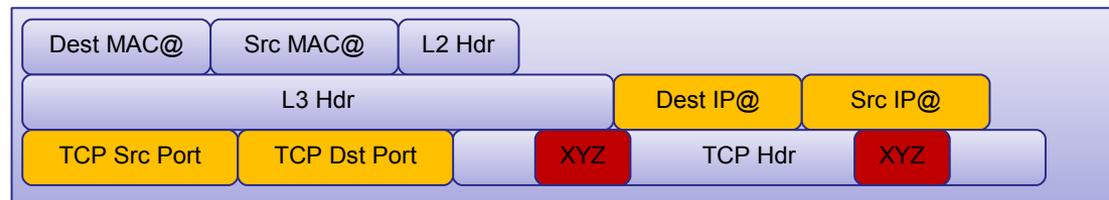- Classification technologies
  - Packet based analyses
    - TCP Port mapping
    - Packet signature (Pattern matching)
  - Session based Analyses
    - Session Grammar
    - Session Correlation
- Classification Path
- Classification Attribute

Application is HTTP

HTTP	TCP	IP	Ethernet	Base

Client IP@

Method

Application Classification

Classification need:
- Attributes and Content extraction is application dependant.
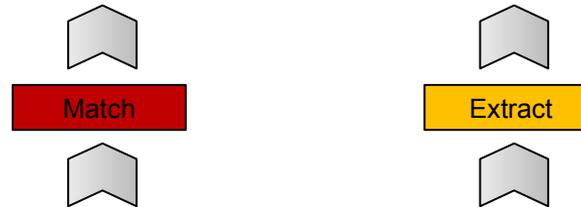- Reliable and easy to use filter.

Classification technologies
- Packet based analyses
  - TCP Port mapping
  - Packet signature (Pattern matching)
- Session based Analyses
  - Session Grammar
  - Session Correlation

Classification Path

Classification Attribute

Classification		
Match		Extract

Dest MAC@	Src MAC@	L2 Hdr		
L3 Hdr			Dest IP@	Src IP@
TCP Src Port	TCP Dst Port	XYZ	TCP Hdr	XYZ

Dest MAC@	Src MAC@	L2 Hdr	
L3 Hdr		Dest IP@	Src IP@
TCP Src Port	TCP Dst Port	TCP Hdr	

P7 P6 P5 P4 P3 P2 P1

Application Classification
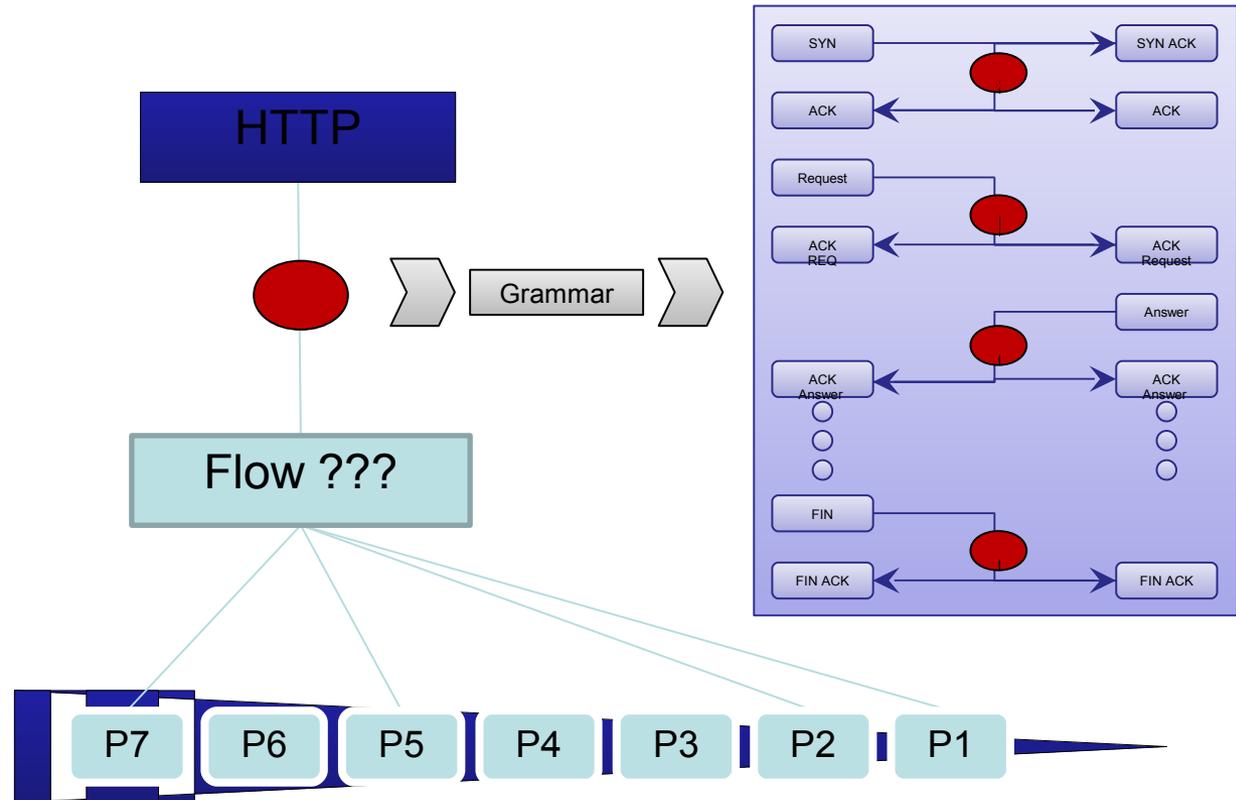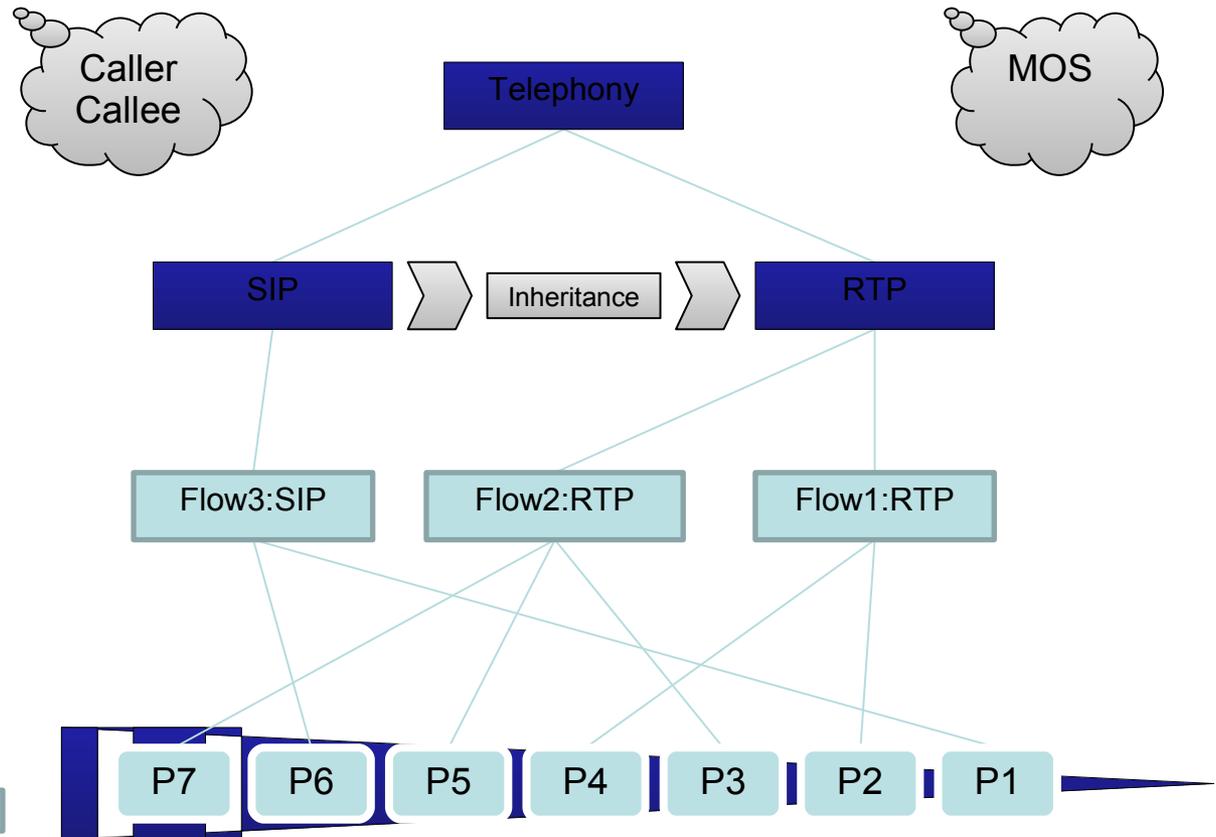
- Classification need:
  - Attributes and Content extraction is application dependant.
  - Reliable and easy to use filter.
- Classification technologies
  - Packet based analyses
    - TCP Port mapping
    - Packet signature (Pattern matching)
  - Session based Analyses
    - Session Grammar
    - Session Correlation
- Classification Path
- Classification Attribute

HTTP

Grammar

Flow ???

P7　P6　P5　P4　P3　P2　P1

SYN — SYN ACK
ACK — ACK
Request
ACK REQ — ACK Request
Answer
ACK Answer — ACK Answer
FIN
FIN ACK — FIN ACK

QOSMOS
Your Network is Information

Application Classification
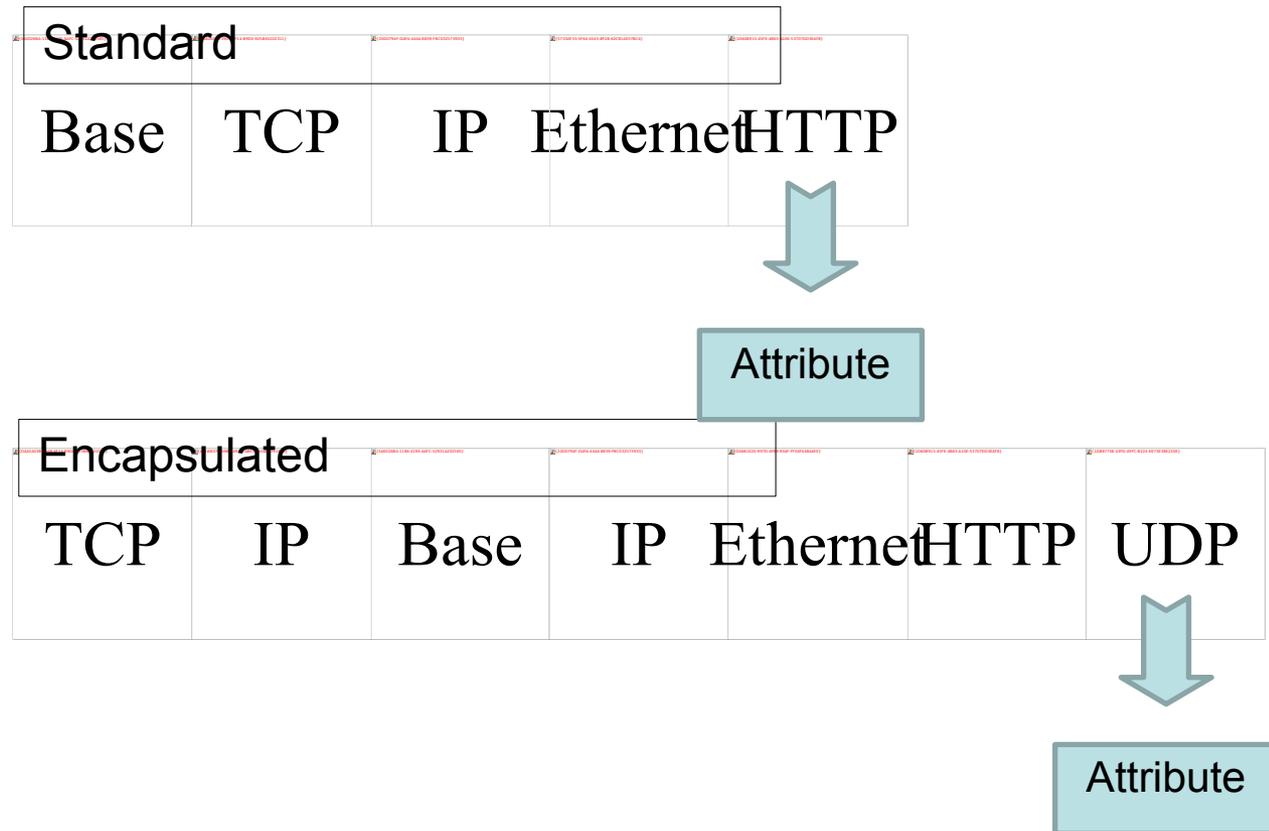
- Classification need:
  - Attributes and Content extraction is application dependant.
  - Reliable and easy to use filter.
- Classification technologies
  - Packet based analyses
    - TCP Port mapping
    - Packet signature (Pattern matching)
  - Session based Analyses
    - Session Grammar
    - Session Correlation
- Classification Path
- Classification Attribute

Caller Callee

Telephony

MOS

| SIP | Inheritance | RTP |

Flow3:SIP   Flow2:RTP   Flow1:RTP

P7   P6   P5   P4   P3   P2   P1

Application Classification

Classification need:
- Attributes and Content extraction is application dependant.
- Reliable and easy to use filter.

Classification technologies
- Packet based analyses
  - TCP Port mapping
  - Packet signature (Pattern matching)
- Session based Analyses
  - Session Grammar
  - Session Correlation

Classification Path

Classification Attribute

Standard				
Base	TCP	IP	Ethernet	HTTP

Attribute

Encapsulated						
TCP	IP	Base	IP	Ethernet	HTTP	UDP

Attribute

QOSMOS
Your Network is Information

Information Extraction

- Attribute extraction
  - Direct extraction
  - Calculated attribute (metric)
  - Inherited extraction
  - IX format and export
- Content extraction
  - UDP stream
  - Specific application content
  - User content
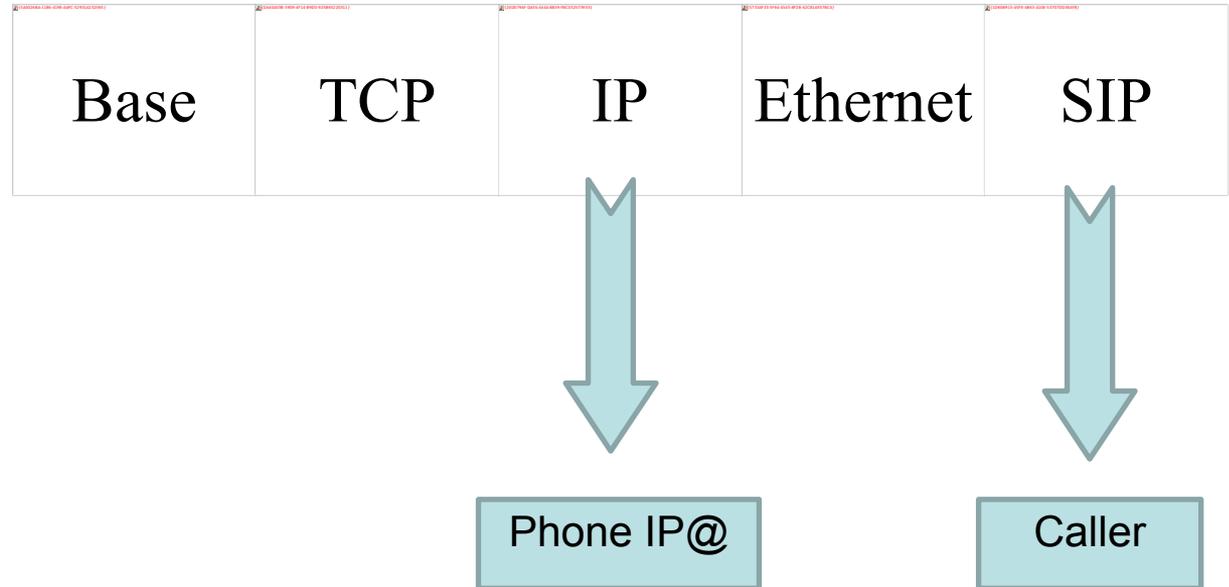   - User Transaction
    - File

Information Extraction

- Attribute extraction
  - Direct extraction
  - Calculated attribute (metric)
  - Inherited extraction
  - IX format and export
- Content extraction
  - UDP stream
  - Specific application content
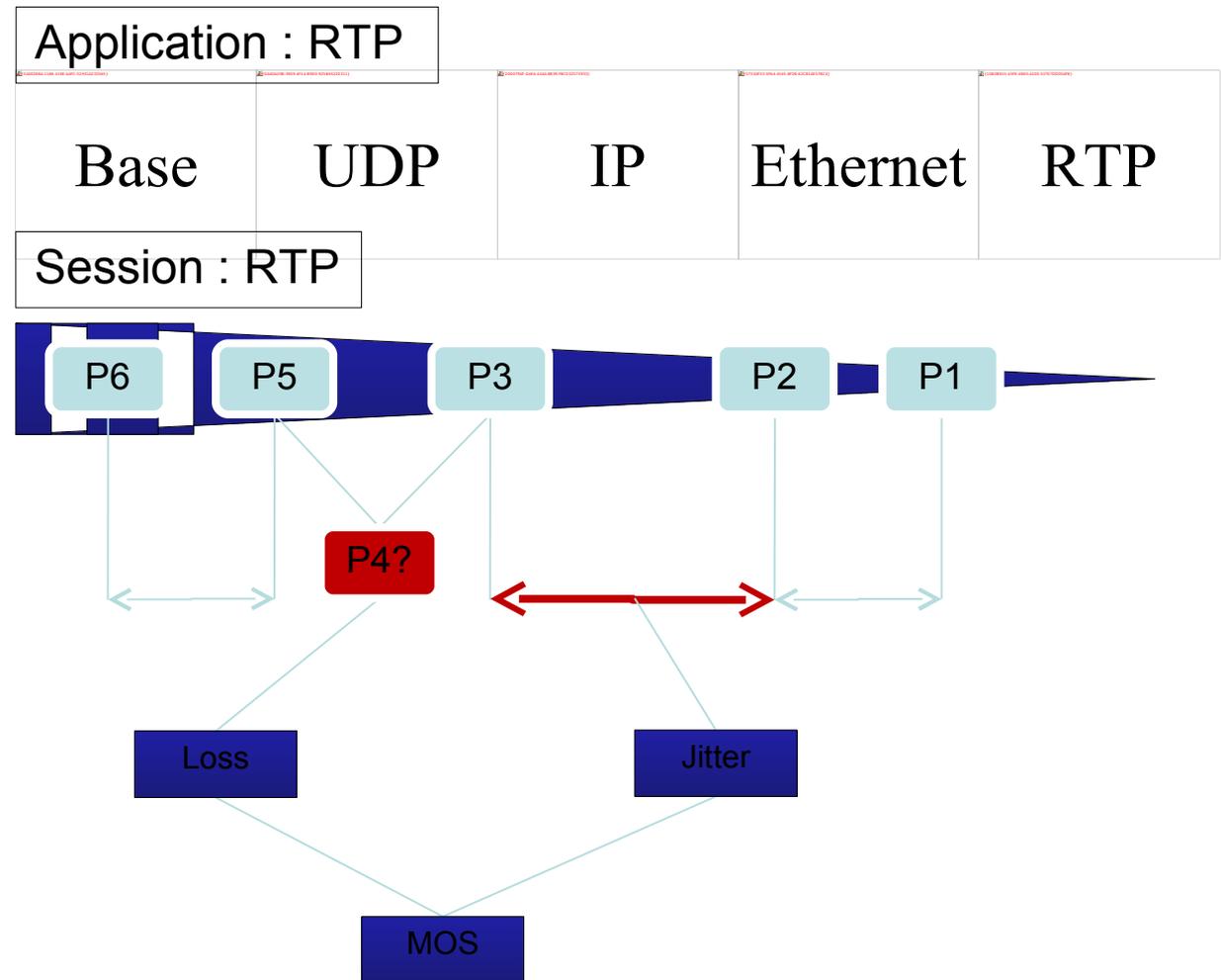 - User content
    - User Transaction
    - File

Base	TCP	IP	Ethernet	SIP

Phone IP@

Caller

Information Extraction

- Attribute extraction
  - Direct extraction
  - Calculated attribute (metric)
  - Inherited extraction
  - IX format and export
- Content extraction
  - UDP stream
  - Specific application content
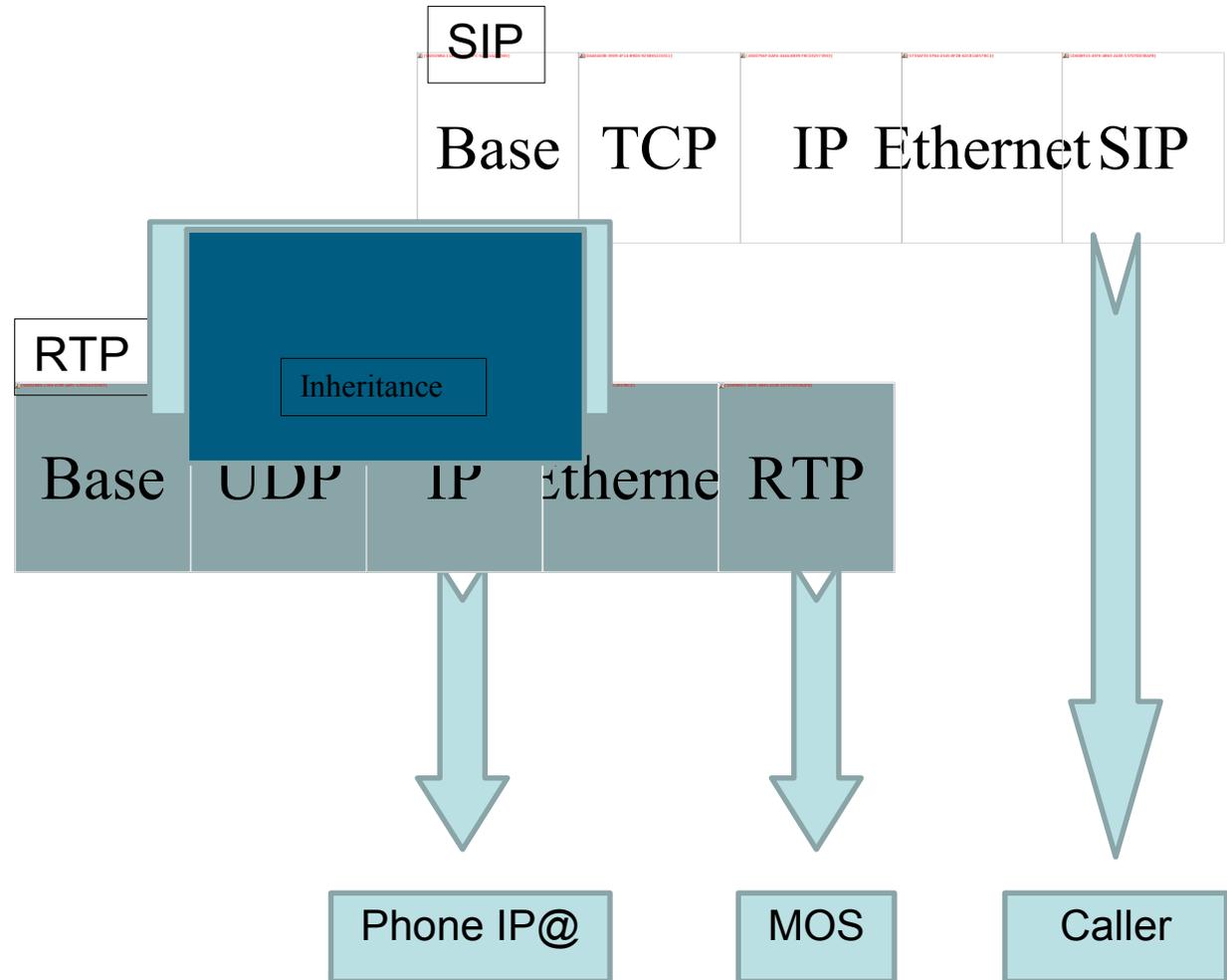 - User content
    - User Transaction
    - File

Application : RTP

| Base | UDP | IP | Ethernet | RTP |

Session : RTP

P6   P5   P3   P2   P1

P4?

Loss

Jitter

MOS

Information Extraction

- Attribute extraction
  - Direct extraction
  - Calculated attribute (metric)
  - Inherited extraction
  - Tupple format and export
- Content extraction
  - UDP stream
  - Specific application content
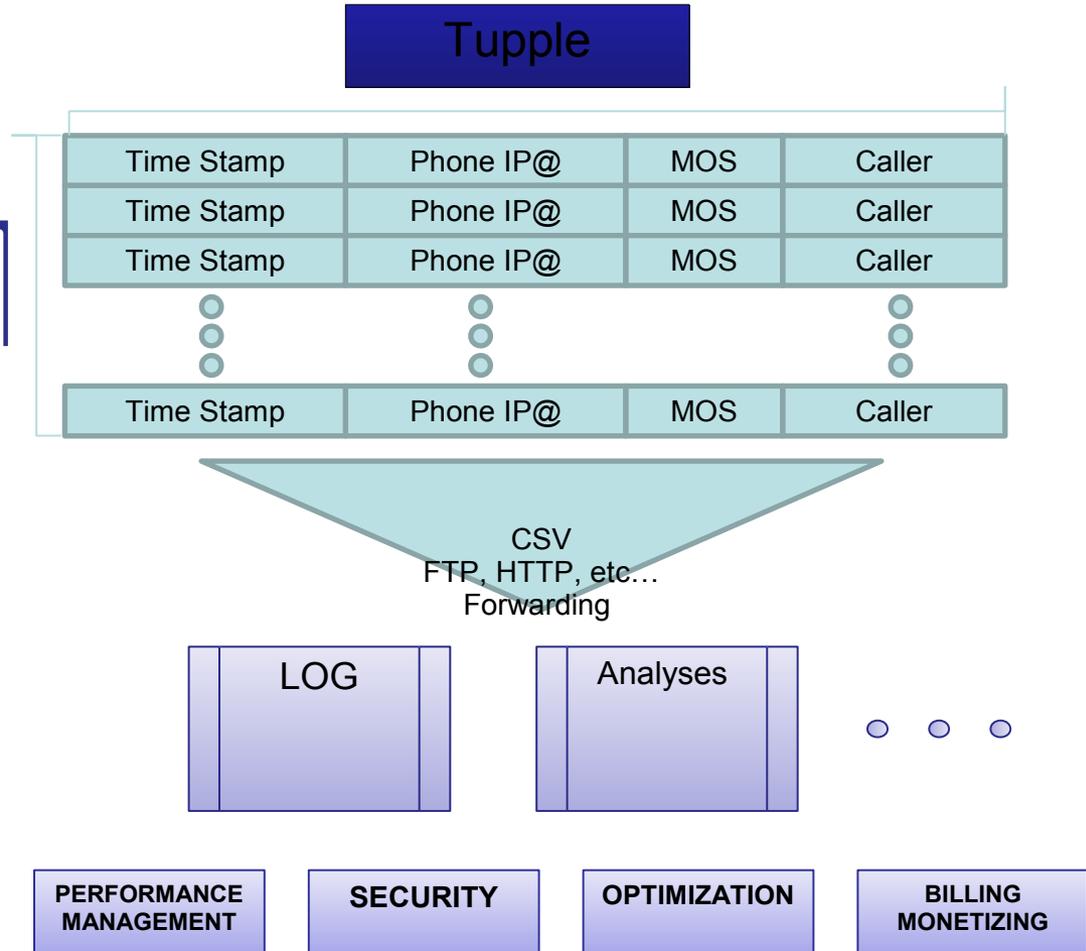 - User content
    - User Transaction
    - File

SIP

Base TCP   IP Ethernet SIP

RTP

Inheritance

Base UDP   IP Etherne RTP

Phone IP@   MOS   Caller

QOSMOS
Your Network is Information

Information Extraction

- **Attribute extraction**
  - Direct extraction
  - Calculated attribute (metric)
  - Inherited extraction
  - IX format and export
- **Content extraction**
  - UDP stream
  - Specific application content
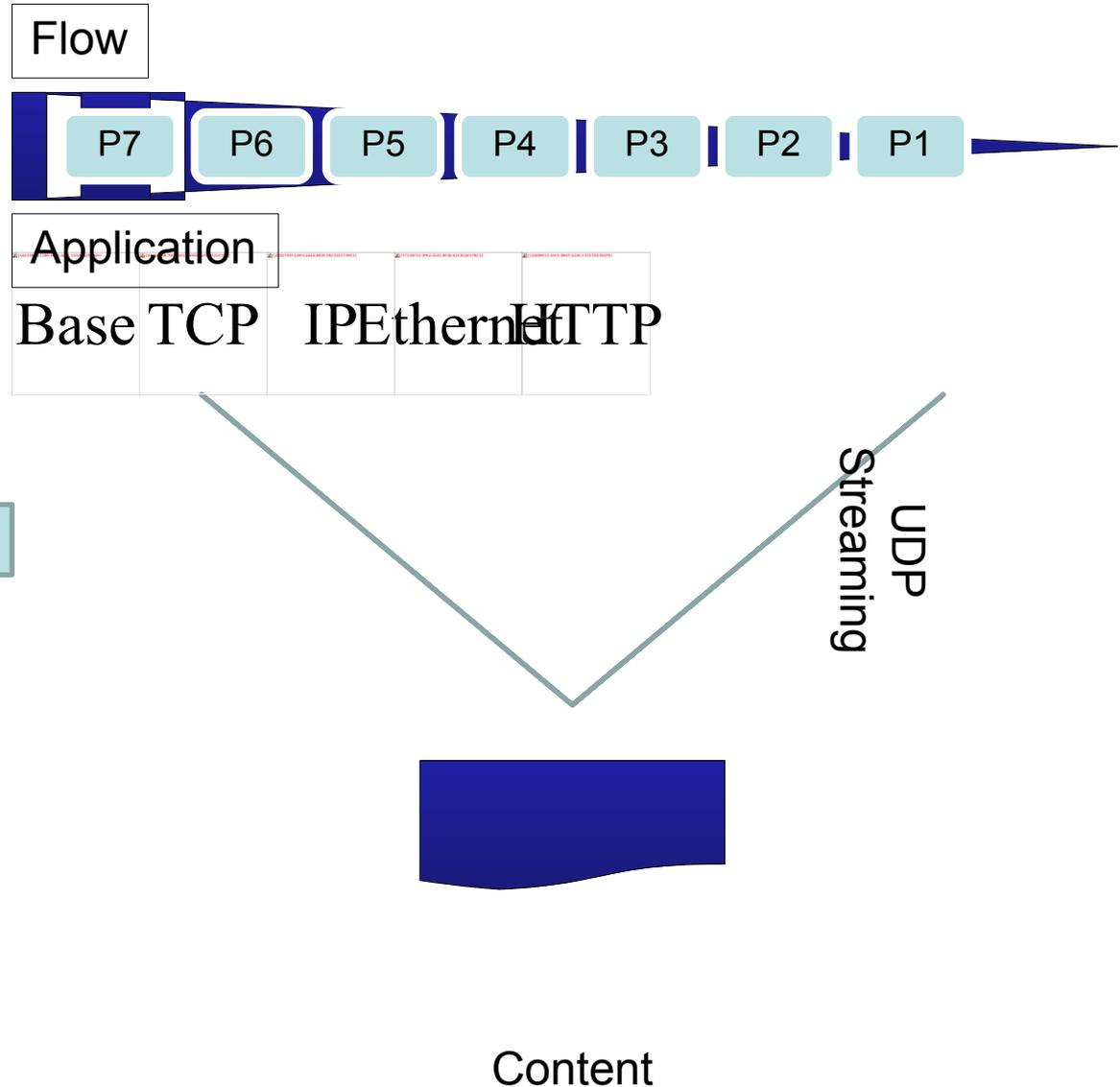 - User content
    - User Transaction
    - File

Tuple

CSV

Time Stamp	Phone IP@	MOS	Caller
Time Stamp	Phone IP@	MOS	Caller
Time Stamp	Phone IP@	MOS	Caller
Time Stamp	Phone IP@	MOS	Caller

CSV
FTP, HTTP, etc...
Forwarding

LOG

Analyses

PERFORMANCE MANAGEMENT	SECURITY	OPTIMIZATION	BILLING MONETIZING

QOSMOS
Your Network is Information

Information Extraction

- **Attribute extraction**
  - Direct extraction
  - Calculated attribute (metric)
  - Inherited extraction
  - IX format and export
- **Content extraction**
  - UDP stream
  - Specific application content
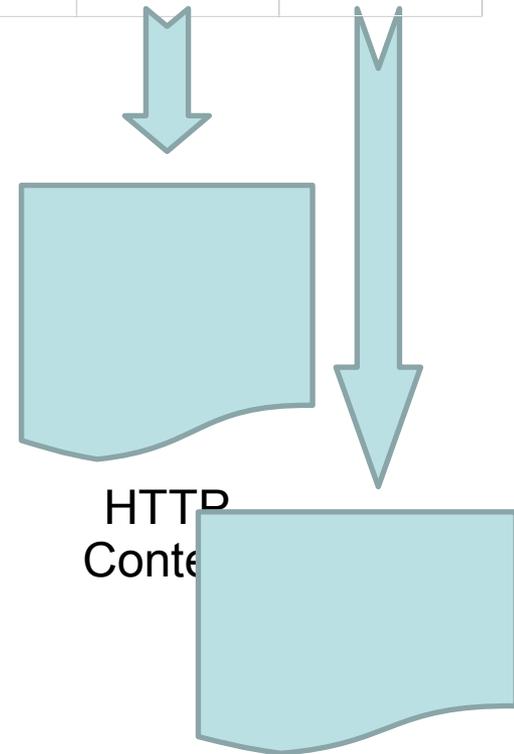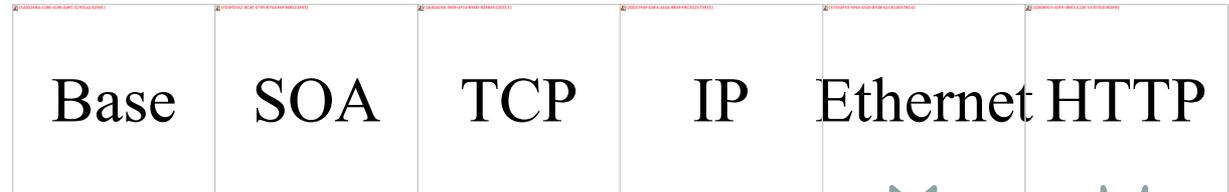 - User content
    - User Transaction
    - File

Flow

| P7 | P6 | P5 | P4 | P3 | P2 | P1 |

Application

Base TCP IPEthernetHTTP

UDP Streaming

Content

Information Extraction

- **Attribute extraction**
  - Direct extraction
  - Calculated attribute (metric)
 - Inherited extraction
  - IX format and export
- **Content extraction**
  - UDP stream
  - Specific application content
  - User content
    - User Transaction
    - File

Base	SOA	TCP	IP	Ethernet	HTTP

HTTP Content

XML File

Demos

- Live **I**nformation e**X**traction Process
    - Real Time Traffic Monitoring
    - Traffic Classification
    - Attribute extraction
- Tuple post processing examples
    - CSV Analyses & Presentation
    - Calculated Attributes : ToIP Quality Monitoring
    - Calculated Attributes : Server Performance Monitoring
    - Extracted Attributes : Advanced Web URI extraction

QOSMOS
Your Network is Information

Your Network is Information

th
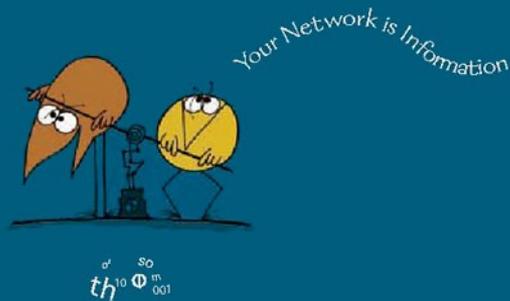
Headquarters
Immeuble Le Cardinet
5, impasse Chalabre
75017 Paris - France
Phone: +33 1 78 09 14 40
Fax: +33 1 40 37 00 02
Email: contact@qosmos.com
Website: www.qosmos.com

w w w . q o s m o s . c o m