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, Continuous Computing, GE Fanuc, Raza Microelectronics, WindRiver
Market Approach

Qosmos

Clients

End User Needs

Software

Appliances

Network Equipment Manufacturers

System Integrators

Software/Solution Vendors

Network information extraction is becoming pervasive

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

...
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

Classification
Identify IP Protocols

Network Information Extraction

Classification
Identify IP Protocols

Classified Flows

Filtering
Select traffic of interest

QOSMOS
ix technology
real time analysis

Information eXtraction
metadata & content

Structured Network Intelligence

IP flows

IP Network

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
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 Classification

HTTP   TCP   IP   Ethernet   Base

Application is HTTP

Client IP@

Method
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 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 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 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

Encapsulated
TCP IP Base IP Ethernet HTTP UDP

Attribute
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

QOSMOS

[Diagram showing the flow of information extraction processes and formats.]
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
Session: RTP

Base UDP IP Ethernet RTP

P6 P5 P3 P2 P1

P4?

Loss Jitter MOS
Information Extraction

- **Attribute extraction**
  - Direct extraction
  - Calculated attribute (metric)
  - Inherited extraction
  - Tuple format and export

- **Content extraction**
  - UDP stream
  - Specific application content
  - User content
    - User Transaction
    - File

Diagram:
- SIP
- Base
- TCP
- IP
- Ethernet
- SIP

- RTP
- Base
- UDP
- IP
- Ethernet
- RTP

- Phone IP@
- MOS
- 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

---

Tupple

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>Phone IP@</th>
<th>MOS</th>
<th>Caller</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CSV

- FTP, HTTP, etc...
- Forwarding

LOG

Analyses

PERFORMANCE MANAGEMENT

SECURITY

OPTIMIZATION

BILLING MONETIZING
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
- IP Ethernet
- HTTP

Content extraction
- Content
- P1
- P2
- P3
- P4
- P5
- P6
- P7

UDP Streaming
- Content
- QOSMOS
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 Information eXtraction 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