



Paul Hoffmann
CEO DATAKOM/GTEN



State of the Art Solutions for Interception

+ Clean Bandwidth = Clean Services

ISS World Dubai 25th – 28th February 2007

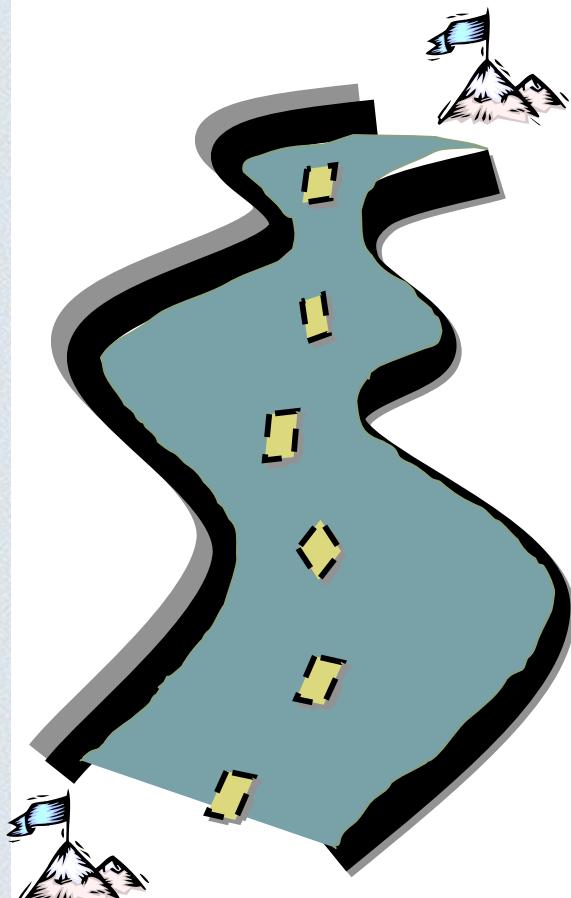


www.datakom.de

DATAKOM

(Mother Company of GTEN)

Innovative Test-, Analyzing and
Performance Management-Systems
for Voice - and Data Networks
+ Training and Consulting Services



**1986 founding of
DATAKOM**

2000/2001 Founding of GTEN AG

- Take over of Technology, Patent, rights and obligation contracts
- Contract with large Carrier in Germany for LI Service



1999

**Contract with Mannesmann
ARCOR, Deutsche Telekom
und o.tel.o**



1997

**Development of the
G10-LI - Technology
Mediation between Carriers,
Ministries, BNetzA and LEAs**



**20 years of experience in the
Protocol- / Performance-
Analysis of Data- / Voice-
Networks**



Life Cycle of Companies inside IT- Industry

- Usually, only some very large Companies do exist for very long Time
- Small and Medium Size Companies Appear and Disappear
- But there are some exceptions.

Why ?



Old Dutch Saying

- During „Stormy“ (Windy) Times
- (and over the last 20 years we had such times inside IT Market)

some are building:



Protection Houses





- And others:
 - Like DATAKOM



Windmills

GTEN





DATAKOM History



- 1986 Founding of DATAKOM GmbH by Paul Hoffmann und Lydia Krowka
- 1988 Start of DATAKOM-Academy
- 2000 Start of GTEN AG with patented Technology for Lawful Interception

Until today



more than 10 000 Installation from **DATAKOM and GTEN**



GTEN - Division History

1986

- Foundation of DATAKOM GmbH
- Extensive experience in the protocol/ performance analysis of data/voice networks

1997

- Basic development of GTEN technology
- Mediation between carriers, ministries, BNetzA and LEAs

1999

- Contract with Mannesmann, ARCOR, Deutsche Telekom and o.tel.o
- Initial certification of LI solution by BMWi

2000

- Foundation of GTEN AG***
- Contract with Viag Interkom (later on BTIgnite)
- Investment backer was obtained in the form of Wellington Partners

2001

- Transfer of technology, patent rights and customer contracts
- Enhancement of existing GTEN solution towards IP applications

2002

- Contract with Telefonica
- GTEN becomes full voting member of ETSI
- GTEN New solution approved according to BNetzA and Dutch TIIT

2003

- Two large IP monitoring systems deployed in North Africa and Middle East
- VoIP LI solution certified by RegTP

2004

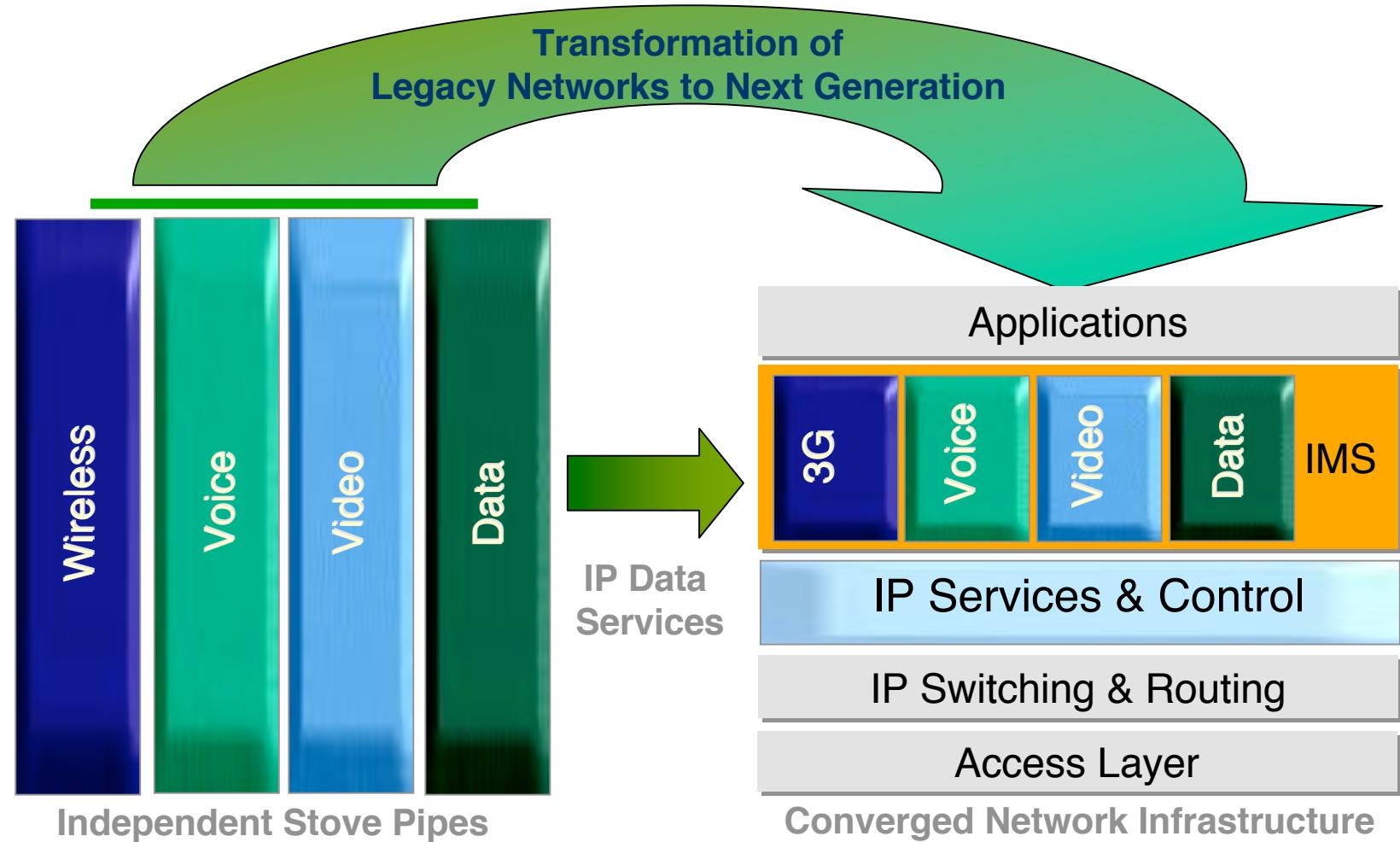
- Introduction of ATM Interceptor
- Start of development of email solution

2005/6

- Email solution certified by RegTP
- Contracts with Easynet, KEVAG and DIG
- Enhancements with existing Customer
- Development new Product Strategy
- Cleaning up Partner Selection
- Clean Bandwidth Concept



What is happening in the market today? *The opportunity lies in the transformation of services.*



Money is being spent to maintain the functionality, usability and security of the customer offerings.



Bandwidth Pressure from Next Generation Applications

<u>Application</u>	<u>Downstream</u>	<u>Upstream</u>
Streaming Audio	128K - 384K	64K
Internet Access	256K - 1.5M	64K - 640K
Web Hosting	400K - 1.5M	400K - 1.5M
Video Conferencing	384K - 1.5M	384K - 1.5M
Distance Learning	384K - 1.5M	384K - 1.5M
Telecommuting	1.5M - 3M	1.5M - 3M
Interactive Video	1.5M - 6M	128K - 6M
VoD	1M - 18M	64K - 640K
Multiple Digital TV	2M - 8M	64K - 640K
Multiple VoD	6M	64K - 640K
HDTV	6-18M	64K
Gaming	2-20M	64K - 20M

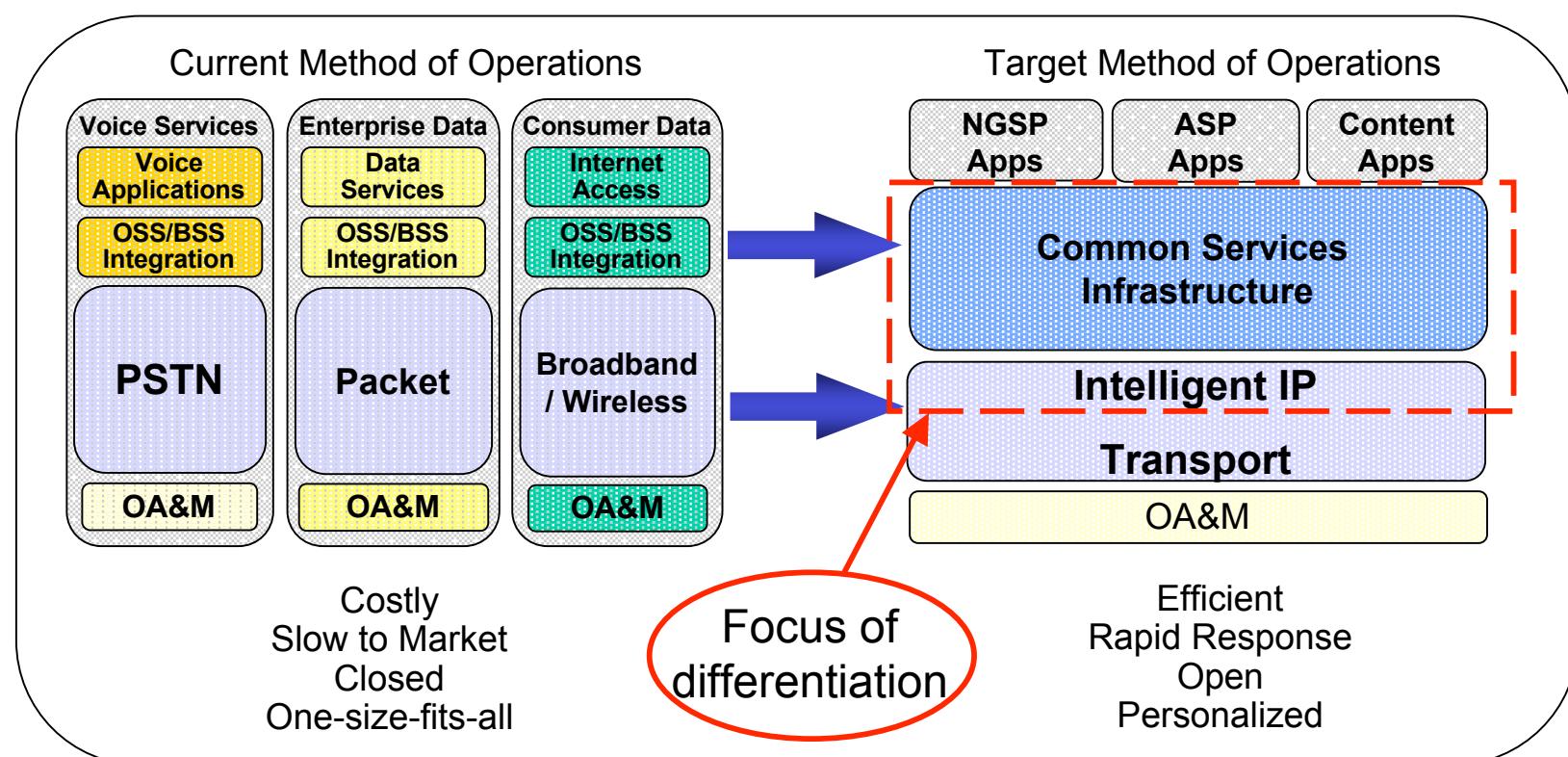
Source: Cisco 2005



Migration to IP is Critical for Participation in the IP Economy, but also Transparency

The pace of convergence to a common IP infrastructure is accelerating

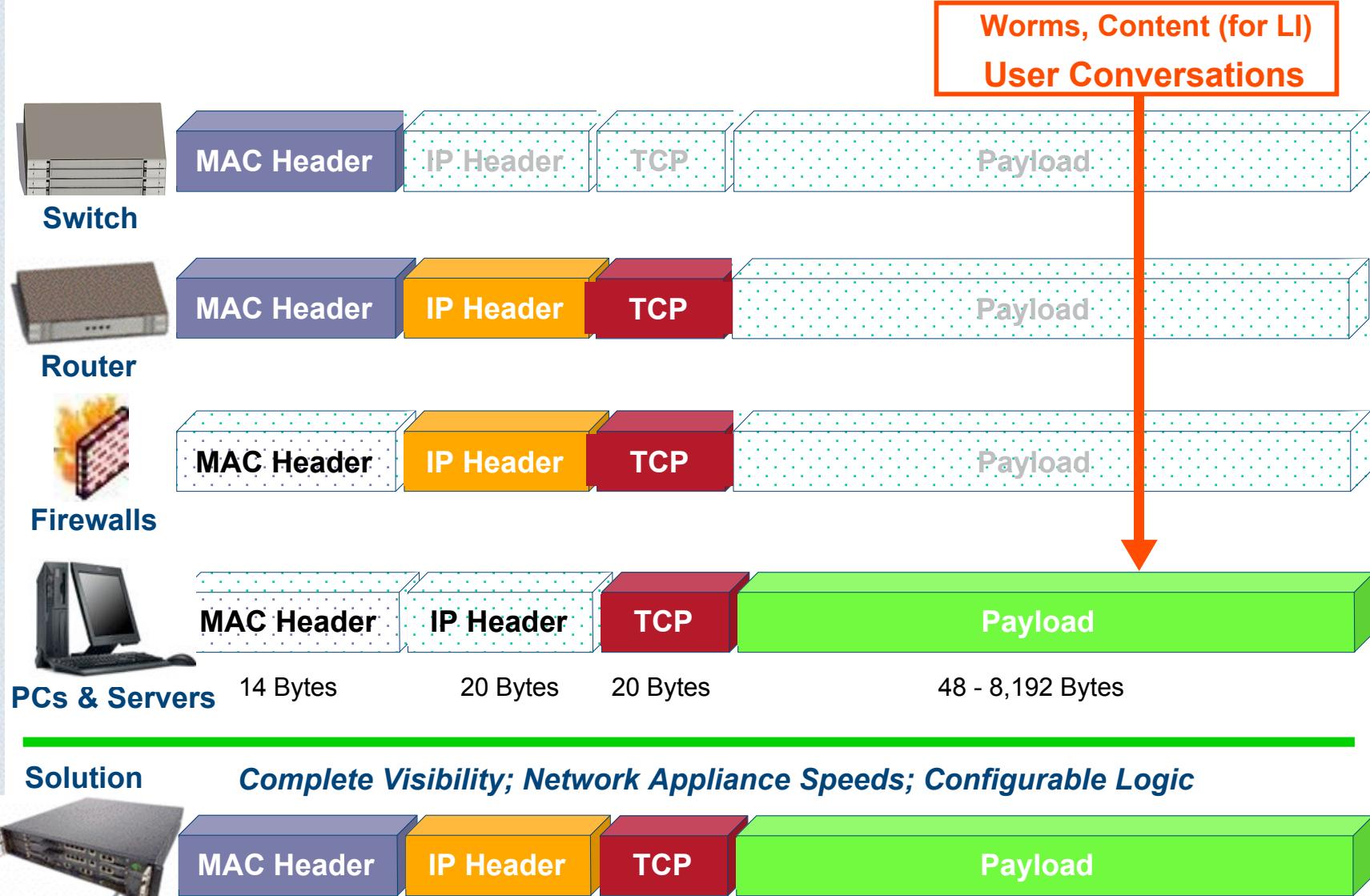
- New-age IP service providers have distinct advantages over incumbents
 - ♣ e.g. personalized services
 - ♣ faster service development cycles
 - ♣ More granular, bounded service levels





Market Conditions

Networking Focused Increasingly on the Content



- There is no good solution available to enable real-time network services & content control incl. Interception
 - ♣ Routers/switches are content-blind, closed systems
 - Header, not payload
 - Pass traffic, don't analyze
 - functionality is fixed
 - ♣ Appliances are point solutions, often ASIC-based and not extensible
 - ♣ Servers (Sun, Dell, ...) are low speed and add latency
- The rate of increase for network transmission speeds and volumes is compounding the problem





Market Conditions Driving 10GbE Deployments

- Broadband data is exploding
 - ♣ “At the end of March 2006, 42 percent of Americans had high-speed at home, up from 30 percent in March 2005, or a 40 percent increase.” *Pew Internet Survey, May 29, 2006*
 -
- Next generation of IP services are bandwidth hogs!
 - ♣ VoD estimated at 1-18Mbps downstream (HDTV 6-18Mbps)
 - ♣ Gaming: 2-20Mbps downstream (64Kbps-20Mbps upstream)
- 10GbE switch port pricing dropped to below \$1,000 per port
- Dell’Oro predicts that over the next five years 23 million 10GbE ports will ship, worth \$14bn



Situation regarding Lawful Interception

- Technology today based on old Network Design
- Handshake Interfaces between Network Provider and Law Enforcement Agencies are designed for old Telephone Networks where Content and Signaling where using different Routes
- Transport of Terrabytes Data towards LEAs very often useless and expensive
- New Generation Networks „Crying“ for new LI - Technology

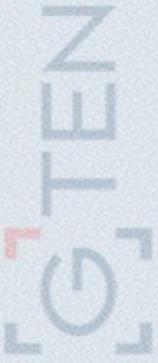


Many (to many) standards don't make things better

- *
- TC LI (Technical Committee LI)
 - * DTR/LI-00014 Lawful Interception of WLAN Internet Access
 - Beschreibt die Interception Domain und die Ausleitung von Wireless Internet. Wird voraussichtlich in 2006 herausgebracht.
 - *
- DTR/LI-00020 Data Handover Architecture
 - Beschreibt die Architektur für die Ausleitung von Daten (EU Data Retention Act). Wird voraussichtlich in 2006 herausgebracht.
 - *
- DTS/LI-00024 Lawful Interception;
 - Service specific details for IP Multimedia Services Spezifikation für das Handover von Voice und sonstigen multimedialen Diensten in paketvermittelten Netzen (mit und ohne IMS). Wird voraussichtlich in 2006 herausgebracht.
 - *
- DTR/LI-00025 Lawful Interception;
 - Architecture for IP Networks within a Communication Service Provider's domain Beschreibt die Architektur für LI in paketvermittelten Netzen. Wird voraussichtlich in 2006 herausgebracht.
 - *
- DTS/LI-00030 Lawful Interception;
 - Service specific details for PSTN Emulation Services (PES) Spezifiziert die Ausleitung von Daten aus multimedialen Netzen, die PSTN Emulation System Eigenschaften besitzen (legacy TDM). Wird voraussichtlich in 2006 herausgebracht.
 - *
- TISPAN LI
 - (Technical Committee - The harmonisation of IP Network Architectures)
 - *
- DTS/07013
 - Telecoms & Internet converged Services & Protocols
 - for Advanced Networks (TISPAN);
- NGN Lawful Interception;
 - Lawful Interception functional entities, information flow
 - and reference points
- Spezifiziert wird der sog. Point of Interception für NGN Netze. Für das Handover wird auf die Dokumente TS 102 232 und 133.108 verwiesen. Wird voraussichtlich Ende 2006 herausgebracht.
- * Bereits veröffentlichte Standards, die erweitert werden (Work Items)
- Standards, die bereits herausgebracht und von europäischen Staaten adaptiert sind.
 - * TS 101 671

List continued

- Handover interface for the lawful interception of telecommunications traffic Erweiterungen für PES und PSS sind in Arbeit. Wird verraussichtlich in 2006 fertig. Diese Spezifikation wird schon europaweit von Regulierungsbehörden adaptiert.
 - * TS 102 232
- Lawful Interception; Handover specification for IP delivery
- Das Handover Interface für IP. Wird in Verbindung mit TS 102 233, 102 234, 102 815 und LI-00024 verwendet. Wegen der unterschiedlichen Einsatzgebiete gibt es noch Anpassungsbedarf. Diese Spezifikation wird schon europaweit von Regulierungsbehörden adaptiert.
 - *
- TS 102 234 Lawful Interception;
- service specific details for internet access services
 - * Wird u.a. für xDSL Layer 3 Ausleitung in Verbindung mit TS 102 232 verwendet. Erweiterungen und Verbesserungen sind geplant. Diese Spezifikation wird schon europaweit von Regulierungsbehörden adaptiert.
 - *
- TS 101 909-20 Part I
- Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services
 - *
- TS 101 909-20 Part II
- Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services
- LI in Breitband Kabelfernsehen Hybrid Fibre/Coaxial (HFC) Datennetzen. Die Spezifikationen beschreiben die Ausleitung von Telefonie und Daten. Diese Spezifikation wird schon europaweit von Regulierungsbehörden adaptiert.
 - *
- TS 101 331 Telecommunications security;
- Lawful Interception; Requirements of Law Enforcement Agencies Die Anforderungen für die Behörden. Das Dokument wird regelmäßig an die zu berücksichtigenden Gegebenheiten angepaßt. Diese Spezifikation wird schon europaweit von Regulierungsbehörden adaptiert.
 - * 3GPP
 - * 133.108 UMTS 3G Security;
- Handover Interface for Lawful Interception
- Spezifiziert wird das Handover Interface für UMTS mit IP Multimedia Subsystemen. Diese Spezifikation wird schon europaweit von Regulierungsbehörden adaptiert.
 - *
- 133.107 UMTS 3G Security;
- Architecture for Lawful Interception
- Spezifiziert wird das Intercept Domain.
- Diese Spezifikation wird schon europaweit von Regulierungsbehörden adaptiert.
- *



Old LI – Technical Design

- GTEN has, like other LI – Vendors, developed many LI- Solutions “dictated” by National Standards
- Result of many existing Standards for Network Provider:

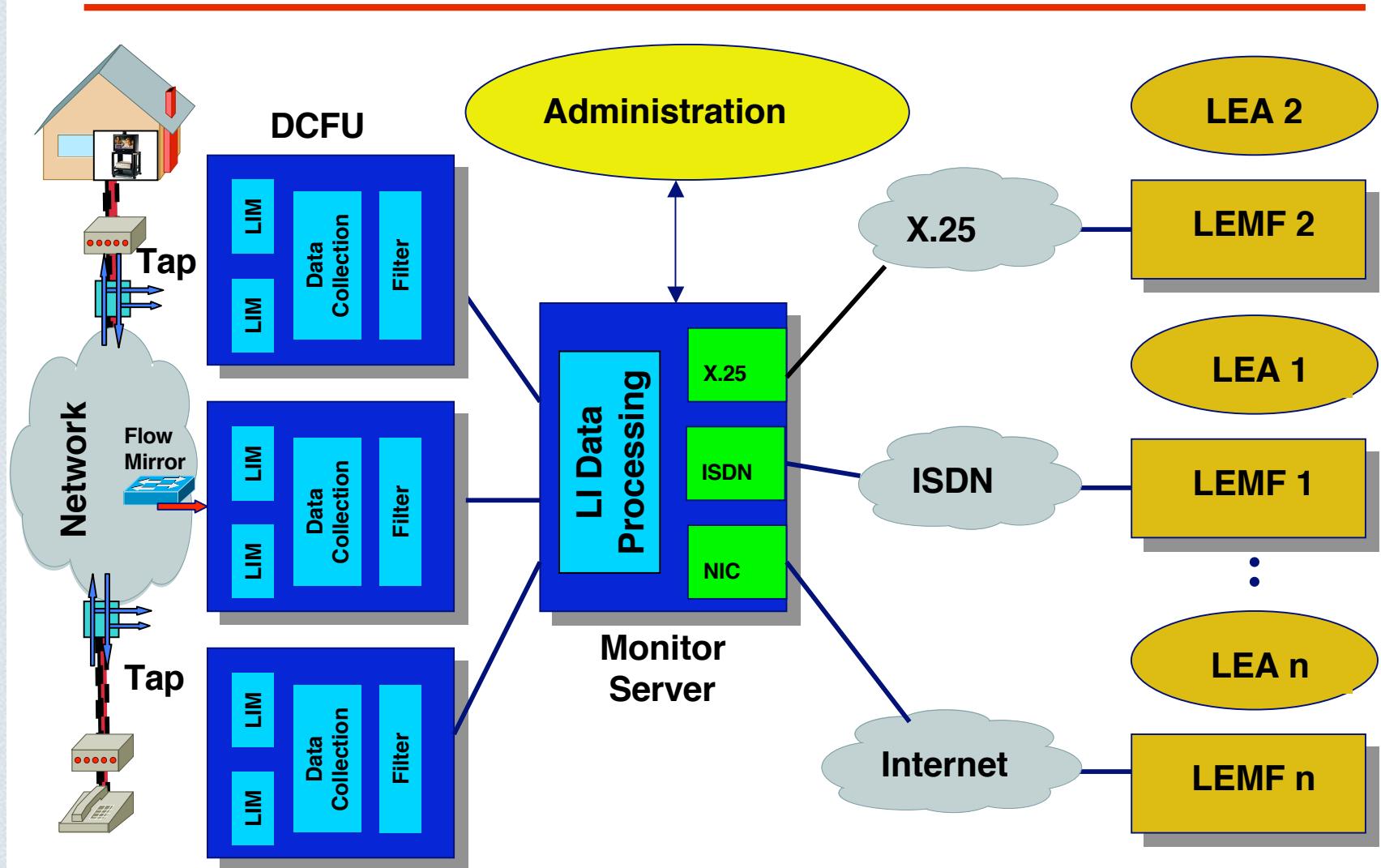
Buying LI- Only – Products very often means creating Cost only and no ROI (Return on Investment)

- Now we/you have the big chance to change this to:
- Network Provider buying the right Technology will see better Performance plus good Portion of ROI and will get

Lawful Interception Solution for very low Cost or no Cost

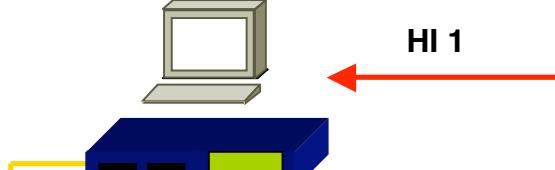
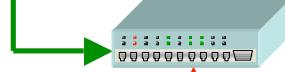
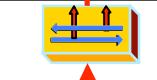
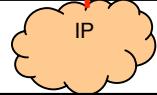


Modular Concept = Excellent Solution but based on old “Legacy Network” Design



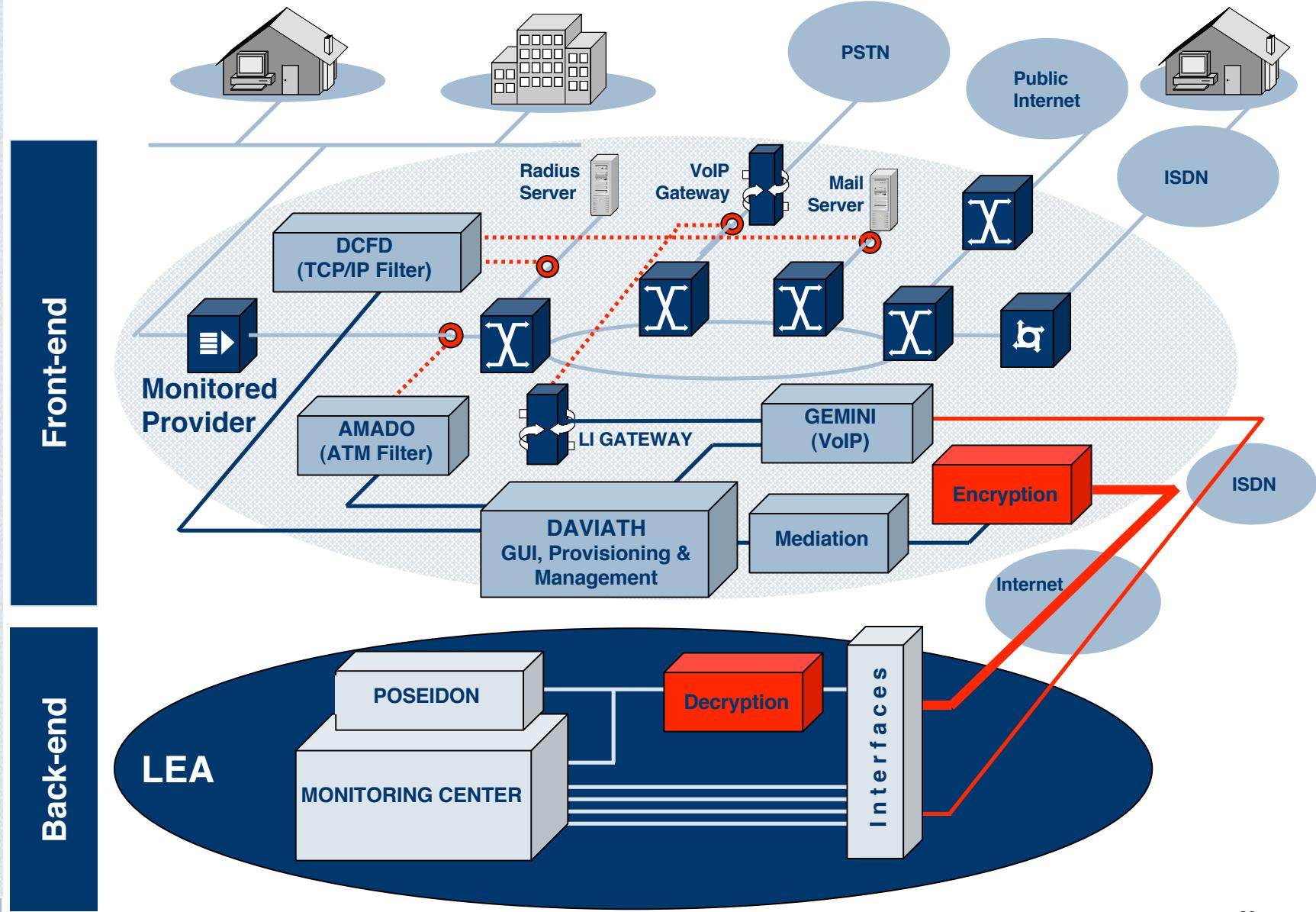


Hand Shake Interfaces, designed many years ago for voice application

Level	Functional Units	GTEN Unit(s)
Operator Interface		
Management Provisioning		
Delivery		
Probe		
Tap		
Network		



LI - Product Environment as Result of Old “Standards”





Reasons for taking a new direction:

- If you want to create a innovative solution, you have to study current solutions and theyr limits
- Together with a friend (Dr. Kornel Terplan) í have written a book last year describing LI – Technology and Methods plus Solutions from all over the world
- As a result of the gained Knowledge our new LI – Technology Concept was born



GTEN

Information Technology

Intelligence Support Systems

Technologies for Lawful Intercepts

Paul Hoffmann and Kornel Terplan

Intelligence Support Systems: Technologies for Lawful Intercepts addresses the information and intelligence needs of service providers, law enforcement agencies, representatives of governments and international standard bodies, and product and service vendors.

This volume offers solutions for many technological challenges, explaining how to provide networking equipment and probes for lawful intercepts, and detailing methods for reducing the performance impacts on network equipment that result from intercepts. It explores how to access, collect, and deliver information in real-time and how to improve mediation efficiency while serving multiple functions. The book also covers data retention and preservation issues and examines how to standardize intercept technologies for various service portfolios and infrastructure components.

Focusing on intelligence support systems (ISS), the text demonstrates how the information that an ISS gathers can be applied toward security, and illustrates how an ISS interfaces with billing, ordering, provisioning, authenticating, and law enforcement systems.

Features:

- Addresses the intelligence needs of service providers, law enforcement, government, and vendors
- Presents ISS basics and summarizes law enforcement requirements, legal background, and lawful intercept architectures
- Covers service portfolios, networking technologies, and infrastructure components
- Examines lawful intercept frameworks and tools offered by vendors, and provides case studies of ISS solutions for various technologies
- Discusses operational principles and technical recommendations for the U.S., Europe, and Japan
- Explains cost components, positive business models, and cost reimbursement strategies
- Explores outsourcing issues, consulting roles, sourcing guidelines, and contract management issues

AU2855



Auerbach Publications
Taylor & Francis Group
www.taylorandfrancis.com



Hoffmann
Terplan

Intelligence Support Systems

Intelligence Support Systems

*Technologies for
Lawful Intercepts*



Paul Hoffmann and Kornel Terplan



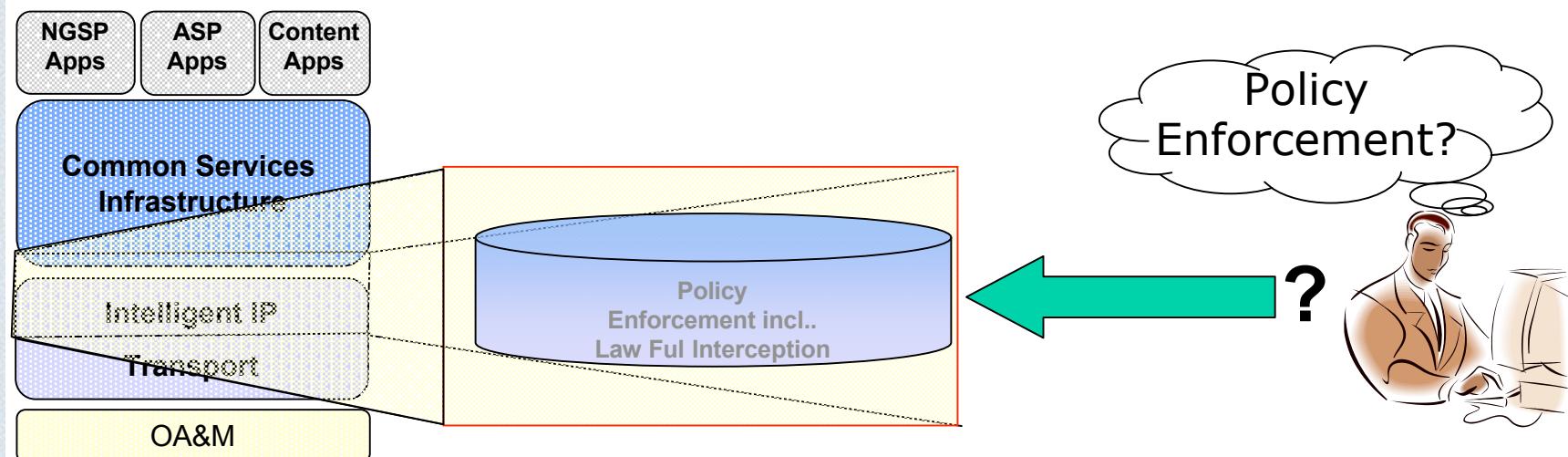
Advice for innovative IP Network Provider in Near - and – Middle East/Africa:

- Dont implement old Standards which are made for old Networks
- This is easy for those who dont have to implement standards like CALEA, ETSI etc.
- And even more easy for new IP – Network Provider



Today's Network Infrastructure inadequate for Service Control Needs

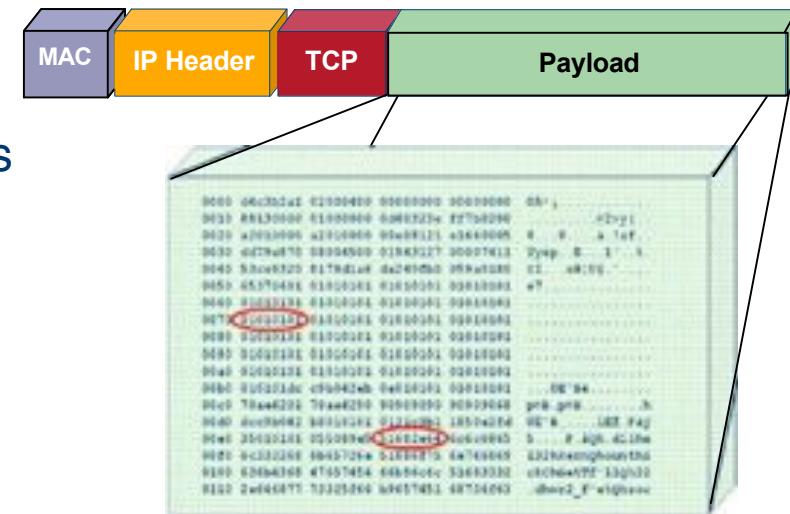
- Devices optimized for OSI Layers 2-4 processing
- Router performance suffers as intelligence functionality is added & turned on
- Pace of feature enhancements too long to support needed roll-out and competitive response timetables
- Provisioning fixed-function appliances for required network intelligence is cost prohibitive and risky





Market Conditions Summary: *Responding to End-User Expressed Issues*

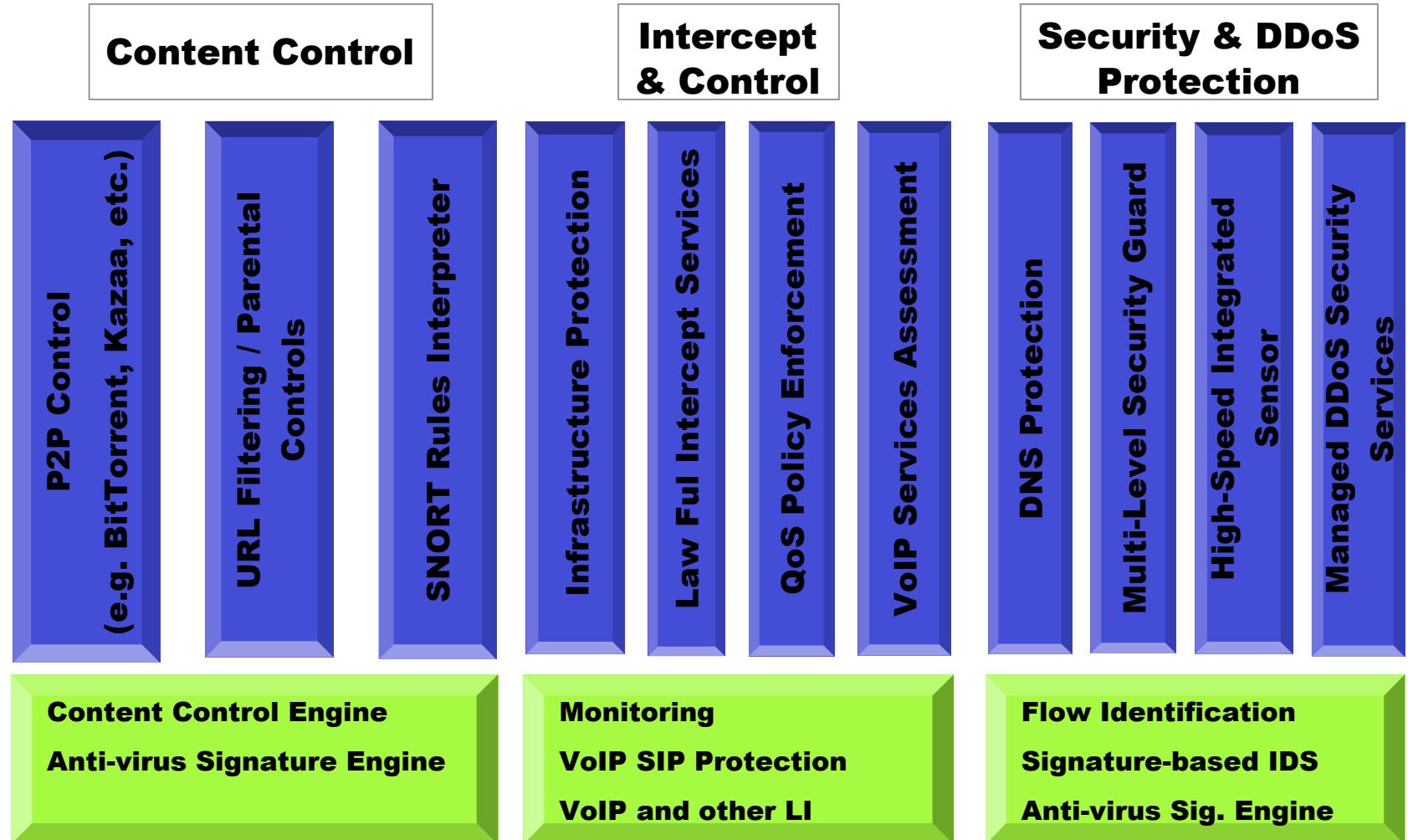
- Application layer attacks and service protocols demand deeper packet inspection & analysis & LI - Function
- General purpose computing solutions have hit a performance ceiling
- The fixed-function appliances model does not scale
- Network infrastructure equipment features are slow to evolve and limit customer's ability to build competitive advantages for their business



Partial SQL Slammer Worm Packet



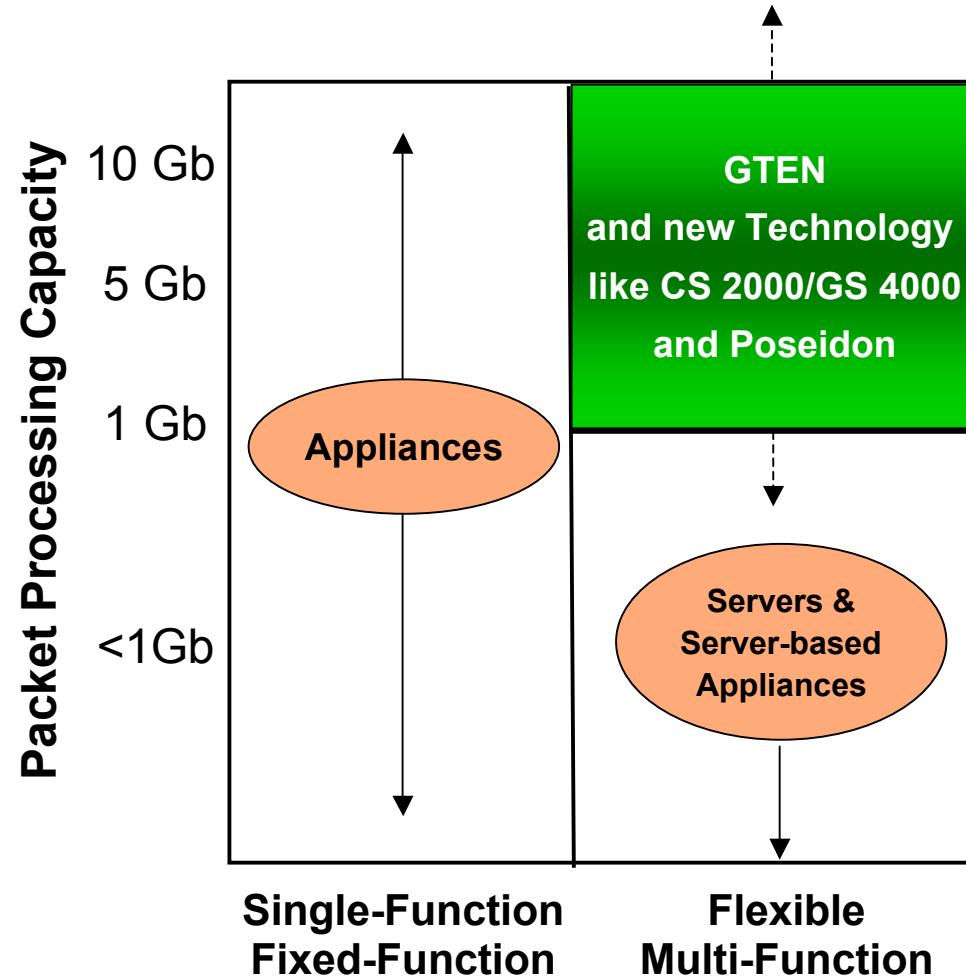
IP Network - Solution Domains with LI as Part of the Job





Market Conditions

An Underserved Market Segment Revealed

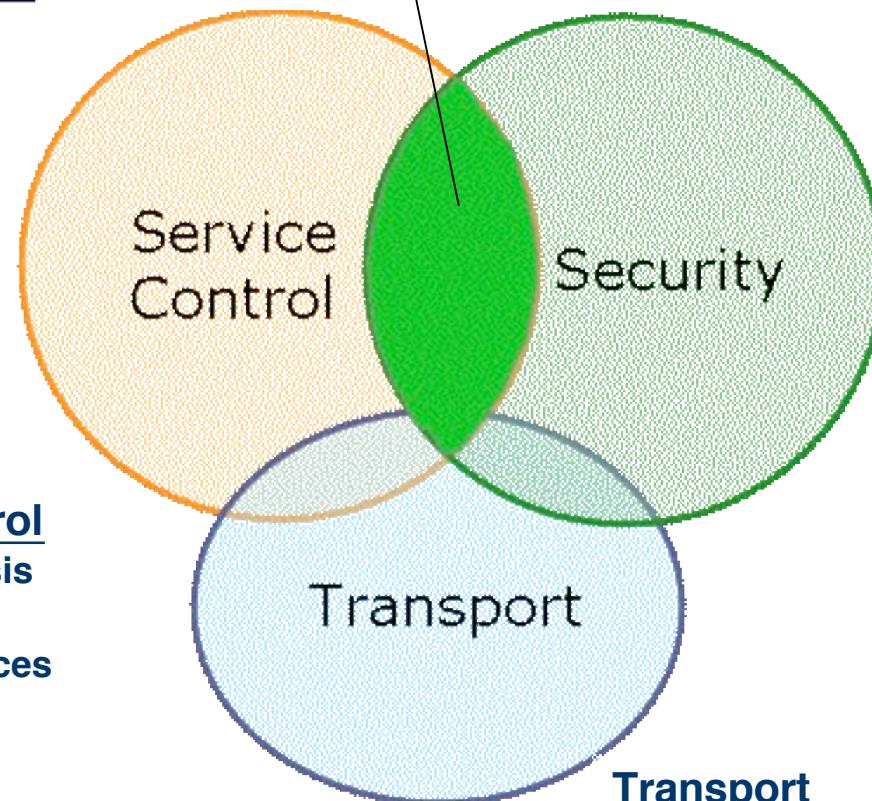




IP Services Control

GTEN taking care for old and new demands

GTEN



Service Control

- L2-L7 analysis
- P2P Control
- Tiered Services

Security

- State & flow tracking
- In-line filtering/blocking
- Signature detection
- Protocol anomaly detection
- Traffic anomaly
- Combined functions

Transport

Transport

- Aggregation
- Routing
- Switching



Carrier/LEA Re-Thinking Appliance Strategies

Fixed-function Appliances



Adaptable, Scalable Processing Resources



IP Services Delivery Requirements

- **Interception as part of Service Delivery**
- Peer-2-Peer Ctrl
- VoIP Control
- Content Filter
- Traffic Analysis
- Access Control
- Security Apps

"Applying the development approach from IT software industry to telecoms"



The right LI – System partner helps Carrier to make money

- LI – System not longer an „iland“ without Return on Investment

Value Proposition

Improve Average Revenue Per User

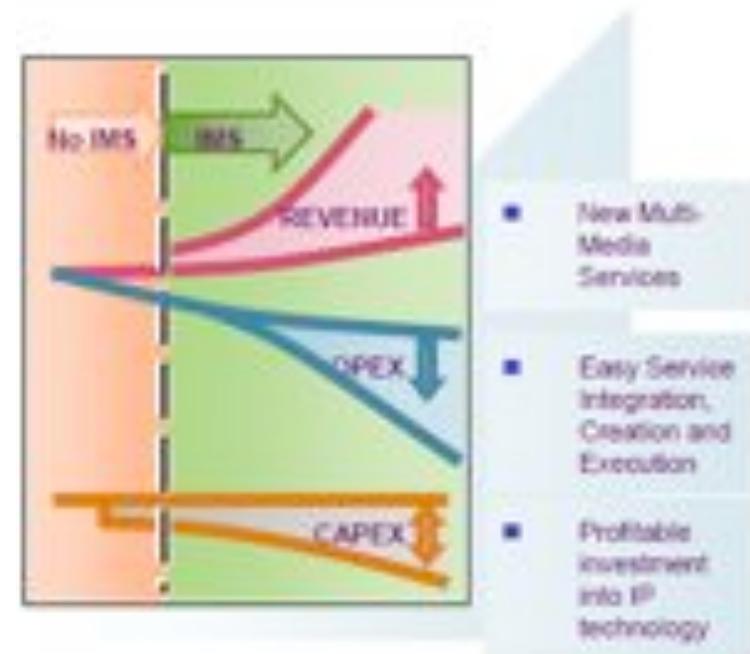
- Offer content based value added services
- Per user features, control and SLAs
- Security Services – DDoS, VoIP, AV
- VoIP/IMS Services – Peering, Personalized
- Traffic Management – QoS, Optimization

Reduced Capital Expenses

- Multiple Services Per Device
- Lower CAPEX Cost Per Megabit of Service
- Longer Deployment Life in Network
- Support More Users with Existing Network

Reduce Operational Expenses

- Manage peering & transit costs
- Reduce cost per service per megabit
- Reduce cost to deploy new services
- Improve efficiency of network resources



Market IMS Value Proposition



Managed Services Infrastructure: Value Added Services Scenario

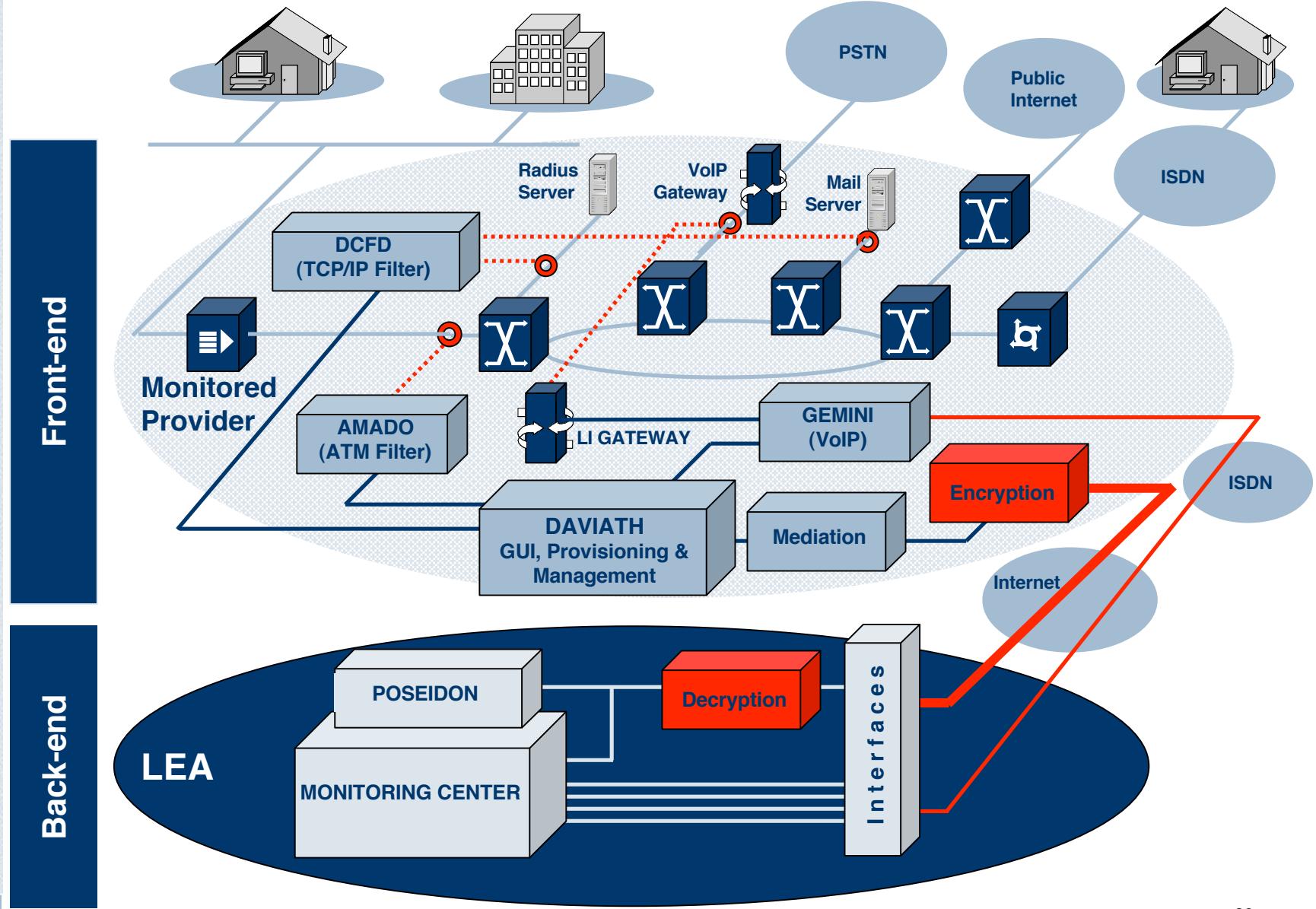
Network Provider may offer Clean Bandwidth Service for Customer. Example:

- Revenue opportunity directly linked with pace and number of services rolled-out
- Capex breakeven in under 12 months for each service
- Differentiate your business via:
 - ♣ Services mix
 - ♣ Ease of deployment

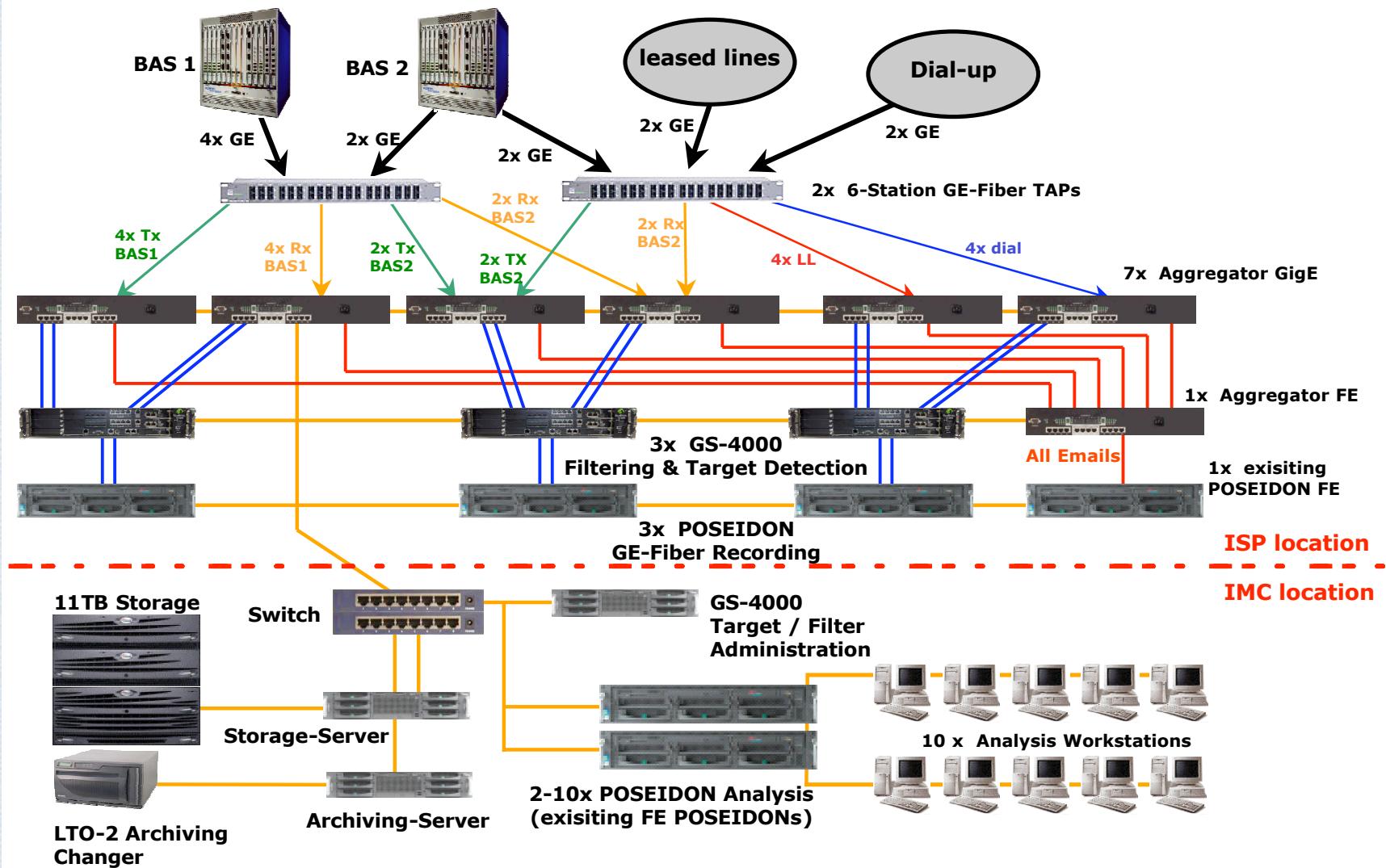
Penetration Rates	75%	75%	100%	100%	90%
Traffic Reporting					
	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5
Hardware Expense	\$ 430,000	\$ -	\$ -	\$ -	\$ -
Support Expense	\$ 64,500	\$ 64,500	\$ 64,500	\$ 64,500	\$ 64,500
Operational Expense	\$ 361,440	\$ 361,440	\$ 361,440	\$ 361,440	\$ 361,440
Total Expense	\$ 855,940	\$ 425,940	\$ 425,940	\$ 425,940	\$ 425,940
Revenue	\$ 903,600	\$ 903,600	\$ 903,600	\$ 903,600	\$ 903,600
Net Income	\$ 47,660	\$ 477,660	\$ 477,660	\$ 477,660	\$ 477,660
DDoS Mitigation					
	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5
Hardware Expense	\$ 918,000	\$ -	\$ -	\$ -	\$ -
Support Expense	\$ 91,800	\$ 91,800	\$ 91,800	\$ 91,800	\$ 91,800
Operational Expense	\$ 1,084,320	\$ 1,084,320	\$ 1,084,320	\$ 1,084,320	\$ 1,084,320
Total Expense	\$ 2,094,120	\$ 1,176,120	\$ 1,176,120	\$ 1,176,120	\$ 1,176,120
Revenue	\$ 2,710,800	\$ 2,710,800	\$ 2,710,800	\$ 2,710,800	\$ 2,710,800
Net Income	\$ 616,680	\$ 1,534,680	\$ 1,534,680	\$ 1,534,680	\$ 1,534,680
P2P Traffic Control					
	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5
Hardware Expense	\$ -	\$ 760,000	\$ -	\$ -	\$ -
Support Expense	\$ -	\$ 38,000	\$ 38,000	\$ 38,000	\$ 38,000
Operational Expense	\$ -	\$ 722,880	\$ 722,880	\$ 722,880	\$ 722,880
Total Expense	\$ -	\$ 1,520,880	\$ 760,880	\$ 760,880	\$ 760,880
Revenue	\$ -	\$ 2,710,800	\$ 2,710,800	\$ 2,710,800	\$ 2,710,800
Net Income	\$ -	\$ 1,189,920	\$ 1,949,920	\$ 1,949,920	\$ 1,949,920
VoIP Traffic Control					
	YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5
Hardware Expense	\$ -	\$ -	\$ 380,000	\$ -	\$ -
Support Expense	\$ -	\$ -	\$ 38,000	\$ 38,000	\$ 38,000
Operational Expense	\$ -	\$ -	\$ 481,920	\$ 481,920	\$ 481,920
Total Expense	\$ -	\$ -	\$ 899,920	\$ 519,920	\$ 519,920
Revenue	\$ -	\$ -	\$ 1,807,200	\$ 1,807,200	\$ 1,807,200
Net Income	\$ -	\$ -	\$ 907,280	\$ 1,287,280	\$ 1,287,280
Net Income Projections					
Net Income Projections	\$ 664,340	\$ 3,202,260	\$ 4,869,540	\$ 5,249,540	\$ 5,249,540



LI - Product Environment from yesterday



LI - Monitoring of a complete Country based on modern IP – Network Requirements





Part of the Solution: Reconstruction of Intercepted Data (only available for LEA,s)

- **Philosophy:**
- **Transport of data only when necessary**

Login Screen



GTEN

Login - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Adressen Wechseln zu

POSEIDON 3.0
Network Recorder and Analyzer

Login

Username:

Password:

Secure Mode

Login

Copyright ©2002 GTEN All rights reserved

Applet gestartet Internet

Start page - Administrator

The screenshot shows the 'GTEN POSEIDON - Microsoft Internet Explorer' window. The title bar includes the application name and the browser type. The address bar displays the URL: <http://10.28.1.142/servlet/Frame?sp=analysis>. The top menu bar contains 'Datei', 'Bearbeiten', 'Ansicht', 'Favoriten', and 'Extras'. On the right side of the header, there are links for 'Wechsel zu', '10.28.1.142 | logout', and the date and time '3/16/2004 9:31'. Below the header is a toolbar with various icons. The main content area has a yellow header bar with the text 'Enter Poseidon'. Below this, there are five entries with descriptions:

- Event Viewer**: View alerts (and details) that have been triggered for configured alarms.
- TCP Reconstruction**: Search and reconstruct TCP sessions (e.g., Web, Mail, Instant Messaging, etc.).
- Traffic Analysis**: Start Analysis on a recording, static, or stopped dataset.
- Data Management**: Transfer specific intervals of recorded data to and from a remote system.
- Configuration**: Configure the recorder, system, alarms, user accounts, and manage logs and jobs.

At the bottom left, there is a yellow callout box labeled 'System Information' containing the following data:

Recording Interfaces:	1 HDX Ethernet
Activity:	1 user logged in, 0 jobs running
Free Space:	127G
Total Space:	127G

At the bottom of the window, there are buttons for 'Fertig' (Done) and 'Internet'.



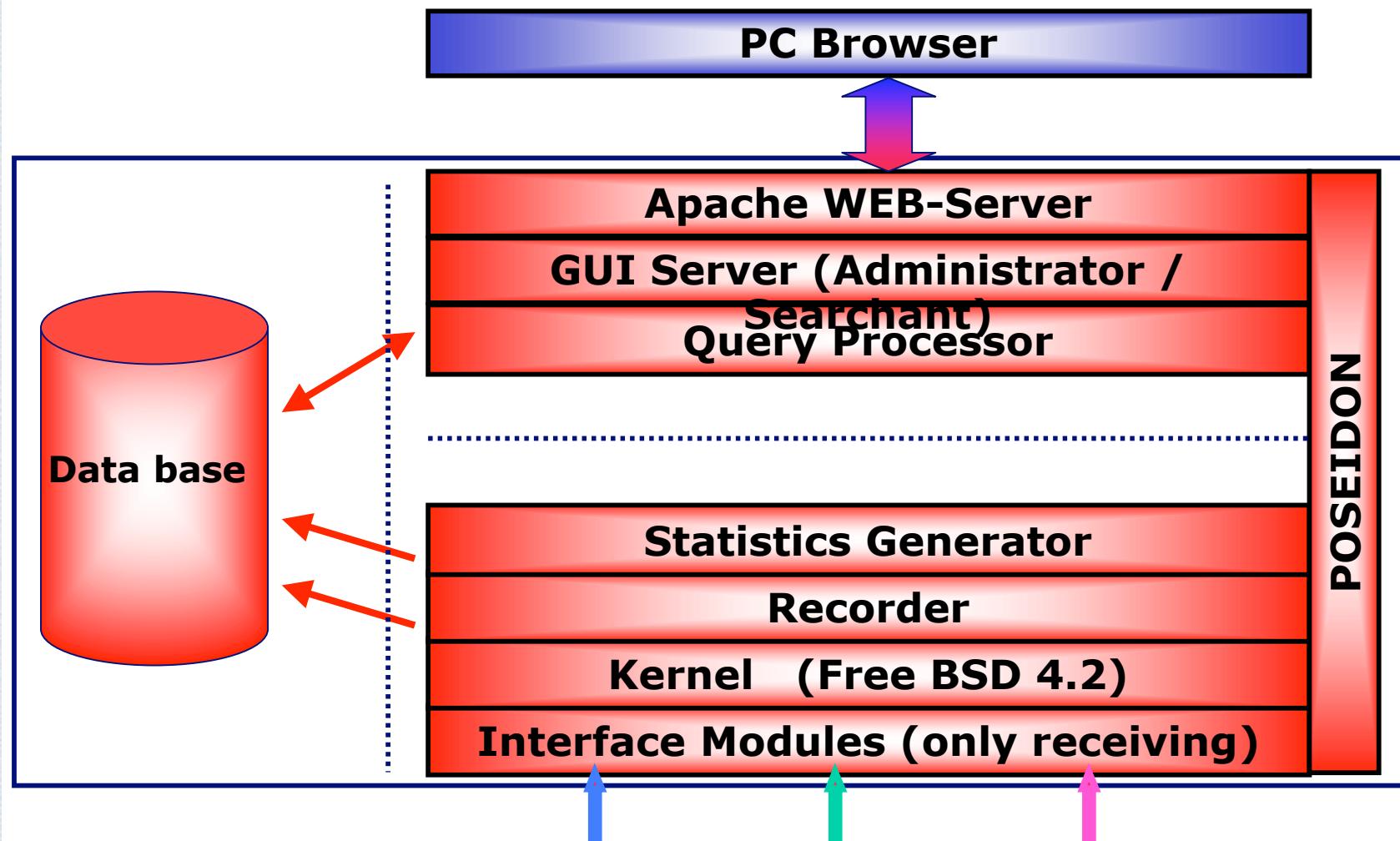
GTEN

POSEIDON Applications

- Non-intrusive network security monitoring system
 - ♣ With alerting functions on user-defined events
 - ♣ With WEB-GUI (Administrator and User View)
- Collects, records and analyses IP-traffic transported through different networks like
 - ♣ Ethernet (as well Fast and Gigabit Ethernet)
 - ♣ ATM
 - ♣ POS
 - ♣ E1/T1, E3/T3
- Collects, records and analyzes **VoIP** calls



POSEIDON Architecture





Reconstruction of IP-data

– Protocols

Frame Relay, HDLC, Cisco HDLC, PPP, BayPPP, MLPPP, VLAN (ISL & IEEE 802.1q), Ethernet (IEEE 802.3), IP, ATM & IP, PoS & IP, WCP and STAC Compression (MPLS & IPv6 optional)

– Complete Analysis on all protocol layers

♣ **PPP** (PAP, IPCP, LCP)

♣ **Ethernet**

- IP
- UDP
- ICMP
- TCP
 - **FTP**
 - **HTTP**
 - **SMTP**
 - **POP3**
 - **IMAP4**
 - **TELNET**
 - **CHAT / IRC**
 - **VoIP (optional)**

– Email reconstruction incl. all attachments

– VoIP reconstruction [H.323v4 – H.225, H.245, Q.931, RTP, RTCP, SCCP, SIP, MGCP(IPDC, SGCP)]



List of all sessions – Applications

Application Reconstruction - Microsoft Internet Explorer

Application Reconstruction

Query

Interface: POS1-001.GTEN.COM\\F3

Start: Relative: -1 hour

End: Relative: now

Do DNS?

Filter:

Search String:

Case Sensitive Base64 Encoded

View By: All Applications Top N: 20

Click to generate summary

Applications Web Pages Emails FTP Chats Sessions

ID	Start Time	Client IP	Server IP	Summary
508	03/16/2004 12:42:36	213.217.105.68	213.185.64.121	www.e7.gmc.net/cgi/gmfunctions.js
513	03/16/2004 12:42:36	213.217.105.68	213.185.64.121	www.e7.gmc.net/cgi/mailnews
514	03/16/2004 12:42:42	213.217.105.68	217.212.240.118	www.saab.de/main.DE/ideyc_stop2.xml
515	03/16/2004 12:42:39	213.185.64.20	213.217.105.68	From:"Jürgen Greulich" <juergen.greulich@gmc.de> To: namikjay@gtен.com Sub: Bild
519	03/16/2004 12:42:46	213.217.105.68	194.95.254.55	www.bremen.de/web/owa/p_suche
521	03/16/2004 12:42:42	213.217.105.68	194.95.254.55	www.bremen.de/web/owa/p_suche www.bremen.de/web/owa/p_anz_suchfenster www.bremen.de/...
526	03/16/2004 12:42:44	213.217.105.68	217.212.240.118	www.saab.de/main.DE/ideyc_stop2.xml
538	03/16/2004 12:43:26	213.217.105.68	213.185.64.100	From:"Jürgen Greulich" <juergen.greulich@gmc.de> To: namikjay@gtен.com Sub: Bild
539	03/16/2004 12:43:26	213.217.105.68	195.254.12.101	dynamic.toolbar.com/dynamic_toolbar disp/3.0/sitedisp.dll
541	03/16/2004 12:43:26	213.217.105.68	194.95.254.55	www.bremen.de/web/owa/p_a_z_topframe www.bremen.de/web/owa/P_A_bis_Z_leiste
543	03/16/2004 12:43:36	213.185.64.20	213.217.105.68	From:"Jürgen Greulich" <juergen.greulich@gmc.de> To: peter.weinlich@gtен.com Sub: Bild
544	03/16/2004 12:43:36	213.217.105.68	213.185.64.121	www.e7.gmc.net/cgi/center
545	03/16/2004 12:43:37	213.217.105.68	213.185.64.121	www.e7.gmc.net/cgi/gmfunctions.js
581	03/16/2004 12:43:41	213.217.105.68	213.185.64.121	www.e7.gmc.net/cgi/gmfunctions.js
582	03/16/2004 12:43:41	213.217.105.68	213.185.64.121	www.e7.gmc.net/cgi/mailindex
572	03/16/2004 12:43:42	213.217.105.68	209.225.34.135	ne.get@4u.com/cgi-bin/print_temp.cgi
573	03/16/2004 12:43:46	213.217.105.68	194.95.254.55	www.bremen.de/web/owa/P_A_bis_Z www.bremen.de/web/owa/P_A_bis_Z
574	03/16/2004 12:43:45	213.217.105.68	213.185.64.121	www.e7.gmc.net/cgi/gmfunctions.js
582	03/16/2004 12:43:44	213.217.105.68	213.185.64.121	www.e7.gmc.net/cgi/mailprint

Reconstruction Options: Auto View Show Server Show Client

View Options: << Back Next >> Total 284



List of emails – Application view

Application Reconstruction - Microsoft Internet Explorer

Query

Interface: POS1-001.GTEN.COM:63

Start: Relative: -1 hour

End: Relative: now

Do DNS?

Filter: port smtp or port pop3 or port imap

Search String:

Case Sensitive Base64 Encoded

Submit

Summary

View By: All Applications Top N: 20

Summary	Sessions	Packets	BW(s)
All Session Flows	54	5425	4518744
smb(25)	54	5425	4518744
212.63.53.14n>213.217.105.66	6	120	8468
62.145.24.154n>213.217.105.66	5	100	7057
213.165.64.20>213.217.105.66	5	343	197270
212.63.34.138n>213.217.105.66	4	90	5699
213.217.105.66n>218.15.192.168	4	16	1198
213.217.105.66n>216.21.229.199	2	8	598
213.217.105.66n>211.99.38.95	2	4	256
213.217.105.66n>202.76.147.37	2	43	9025
213.217.105.66n>65.54.253.99	1	4	299
213.217.105.66n>65.54.187.5	1	22	1833

Applications Web Pages Emails FTP Chats Sessions

ID	Start Time	Client IP	Server IP	Summary
1	03/16/2004 11:54:30	213.165.64.20	213.217.105.66	[redacted] From: "Jürgen Greulich" <juergen.greulich@gmx.de> To: "Peter Weinlich" <Peter.Weinlich@ghen.co...
7	03/16/2004 11:58:27	213.165.64.20	213.217.105.66	[redacted] From: "Jürgen Greulich" <juergen.greulich@gmx.de> To: christopher.white@ghen.com Sub: Moin
10	03/16/2004 11:59:48	64.12.137.8	213.217.105.66	[redacted] From: [redacted] Sub: I'mc Are you okay?
27	03/16/2004 12:18:47	212.234.161.19	213.217.105.66	[redacted] From: [redacted] JST.ETS.LORG Sub: Oxford meeting
28	03/16/2004 12:19:50	192.88.97.5	213.217.105.66	[redacted] From: [redacted] JST.ETS.LORG Sub: [IJ] Oxford meeting
34	03/16/2004 12:26:45	213.217.105.66	64.156.215.6	[redacted] From: "Peter Weinlich" <Peter.Weinlich@ghes.com> To: peter44h@yahoo.de Sub: The file you a...
39	03/16/2004 12:47:33	213.165.64.20	213.217.105.66	[redacted] From: "Jürgen Greulich" <juergen.greulich@gmx.de> To: namikay@gten.com Sub: Bild
40	03/16/2004 12:43:26	213.217.105.66	213.165.64.100	[redacted] From: "Jürgen Greulich" <juergen.greulich@gmx.de> To: namikay@gten.com Sub: Bild
41	03/16/2004 12:43:36	213.165.64.20	213.217.105.66	[redacted] From: "Jürgen Greulich" <juergen.greulich@gmx.de> To: peter.weinlich@ghen.com Sub: Bild
42	03/16/2004 12:45:06	213.165.64.20	213.217.105.66	[redacted] From: "Jürgen Greulich" <juergen.greulich@gmx.de> To: namikay@gten.com Sub: Bild
46	03/16/2004 12:48:39	213.217.105.66	202.76.147.37	[redacted] From: [redacted] UETZL...

Reconstruction Options: Auto View Show Server Show Client View Options << Back Next >> Total 11



Reconstructed email – Application

Application Reconstruction - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras

Adressen: [Http://10.28.1.142/servlet/UTCPReconPage5SessionRecon/recorder=PO51-001.GTEN.COM&face=s13&begin=1079440005.976016&end=1079440009.6](http://10.28.1.142/servlet/UTCPReconPage5SessionRecon/recorder=PO51-001.GTEN.COM&face=s13&begin=1079440005.976016&end=1079440009.6) Wechsel zu Links

Prior Email Next View App View Show header

Client IP: 213.217.106.88 Server IP: 64.158.215.8 Session ID: 34 Filter: port smtp or port pop3 or port imap

Email Reconstruction

Save as eml

From: "Peter Weinlich" <Peter.Weinlich@gtен.com>

To: <peter44hd@yahoo.de>

Date: Tue, 16 Mar 2004 13:23:49 +0100

Subject: The file you are waiting for

Attachments: VOLVO_V70.pdf 0

Dear Peter,

attached please find the file you asked for.

If you need any help, just call me.

Kind Regards,
Peter Weinlich

<>

Received: from [10.28.1.1] (he1o@gtен-bre-svr-01.gten.net)
by bre-fw-01.gten.de with esmtp (Exim 4.22)
id 1B3Dc8-00002T-6h

Fertig Internet



Reconstructed email – Application

Application Reconstruction - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras |

Adressen: [Http://10.28.1.142/servlet/ITCRecon/Page5SessionRecon?recorder=PO51-001.GTEN.COM&face=s3&begin=1079440005.976016&end=1079440009.6](http://10.28.1.142/servlet/ITCRecon/Page5SessionRecon?recorder=PO51-001.GTEN.COM&face=s3&begin=1079440005.976016&end=1079440009.6) Wechsel zu Links

Print Email Ned View App View Show Header

Client IP: 213.217.105.88 Server IP: 64.156.215.8 Session ID: 34 Filter: port smtp or port pop3 or port imap

Email Reconstruction

Save as eml

From: "Peter Weinlich" <Peter.Weinlich@gtен.com>

To: <peter44bb@yahoo.de>

Date: Tue, 16 Mar 2004 13:23:49 +0100

Subject: The file you are waiting for

Attachments: VOLVO V70.pdf 9

Dear Peter,

attached please find the file you asked for.

If you need any help, just call me.

Kind Regards,
Peter Weinlich

<>

Received: from [10.28.1.1] (helo=gtен-bre-svr-01.gten.net)
by bre-fw-01.gten.de with esmtp (Exim 4.22)
id 1B3Dc8-00002T-6h

Fertig Internet



GTEN

Reconstructed email – ASCII

```
Application Reconstruction - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ...
Adress: http://10.28.1.142/servlet/TCPreconPageSessionRecon?action=refresh&showHdr=on&enableJS=false&appType=2&reassessOpt=ascii&checkHdr=on
Client IP: 213.217.105.66 Server IP: 64.156.215.8 Session ID: 34 Filter: port smtp or port pop3 or port imap

220 YBsmtp mta13.mail.sod.yahoo.com ESMTP service ready
EHLO bre-fw-01.gten.de
250-mta13.mail.sod.yahoo.com
250-8BITMIME
250-SIZE 10485760
250 PIPELINING
MAIL FROM:<Peter.Weinlich@gten.com> SIZE=297611
RCPT TO:<peter44hb@yahoo.de>
DATA
250 sender <peter.weinlich@gten.com> ok
250 recipient <peter44hb@yahoo.de> ok
354 go ahead
Received: from [10.28.1.1] (helio-gten-bre-svr-01.gten.net)
        by bre-fw-01.gten.de with esmtp (Exim 4.23)
        id 1B3DcB-0000J7-6h
        for peter44hb@yahoo.de; Tue, 16 Mar 2004 13:24:06 +0100
content-class: urn:content-classes:message
Subject: The file you are waiting for
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_001_01C40B51.86F45370"
Date: Tue, 16 Mar 2004 13:23:49 +0100
X-MimeOLE: Produced By Microsoft Exchange V6.0.5762.3
Message-ID: <E87D0F0EAE5D0444B8D1D915426840000A1774@gten-bre-svr-01.gten.net>
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Topic: The file you are waiting for
Thread-Index: AcQLUYjin6DSWEupTh+ES4pFK1iFKe==
From: "Peter Weinlich" <Peter.Weinlich@gten.com>
To: <peter44hb@yahoo.de>
X-Scan-Signature: 63adba17e7f1cb339cc27560ea1cedb5

This is a multi-part message in MIME format.

----=_NextPart_001_01C40B51.86F45370
Content-Type: text/plain;
        charset="iso-8859-1"
```



Reconstructed WEB-site – Application

Application Reconstruction - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras |

Zurück → ⌘ Zurück ⌘ Wechseln zu Links ⌘

Adressen: ⌘ Wechseln zu ⌘ Links ⌘

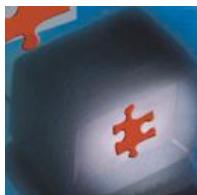
Print Web Pages Ned View App View Show Header URL: c.ae-eu.falkag.net/dat/bgf/200403/11/ex_palme_tun_18.htm Disable Scripting

Client IP: 213.217.105.88 Server IP: 62.26.121.2 Session ID: 2 Filter:

GET /dat/bgf/200403/11/ex_palme_tun_18_480x100.swf?act1=http%3A//62.26.220.5/secver/link.asp%3Fcmd%3Dur1%26kid%3D72953%21
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Via: 1.1 bre-fw-01:8080 (Squid/2.4.STABLE6+filter0.6)
X-Forwarded-For: unknown

Fertig Internet

Voice over IP session list



VOIP Calls - Microsoft Internet Explorer

Analysis CDR QoS Help

Data Format: Nikon dataset Data Source: POST-001-GTEN.COM/ID

Begin Time: Mar 16 06:07:46 2004 End Time: Mar 16 14:07:46 2004 Filter: None

Update

Call View Message View Packet View RAS View

ID	Call Duration (sec)	Calling IP Address	Called IP Address	Calling Party Number
1	22.990068	213.217.105.117	62.52.24.227	4952419009115
2	64.262750	213.217.105.123	62.52.24.227	4952419009111

Messages in Call 1

Signalling	Media	Message	Date/Time
0.000000	0.000000	Setup	01.02.24.227, 0730
0.208554	0.208554	Unknown(1)	01.02.24.227, 0730
1.800551	1.403867	Call Proceeding	01.02.24.227, 0730
1.817488	1.348157	Ringing	01.02.24.227, 0730
10.001517	0.044059	Connect	01.02.24.227, 0730
40.875955	31.980069	Release Complete	01.02.24.227, 0730

Message Elements

Fields Packets

Setup

- Arrival Time: 3/16/2004 12:21:40,274204
- Packet Length: 457
- TPKT**
 - Version: 3
 - Reserved: 0
 - Data Length: 453
- G931**
 - Protocol Discriminator: 0.931
 - Call Reference Value Length: 2
 - CRef Flag: destination
 - Call Reference Value: 1
 - Message Type: Setup
 - Bearer-Capability
 - Length: 3
 - Coding Standard: ITU-T Standardized Coding
 - Information Transfer Capability: 3.1 kHz Audio
 - Transfer Mode: Circuit Mode
 - Information Transfer Rate: 64 kBit/sec
 - User Information Layer 1 Protocol: Recommendation G.711 A-law
 - Display**
 - Length: 13
 - Display Information: 4952419009105
 - Calling-Party Number**
 - Length: 16

HEX/ASCII EBCDIC

000000:	94 98 99 99 03 06 01 93 98 02
000001:	00 01 05 04 03 90 90 A3 28 0D
000002:	34 39 35 32 34 31 39 30 38 39 4 9 5 2 4 1 9 0 8 9
000003:	31 30 35 6C 0F 00 00 34 39 35 1 0 5 1 . . . 4 9 5
000004:	32 34 31 39 30 38 39 31 30 35 2 4 1 9 0 8 9 1 0 5
000005:	70 0C 80 30 34 32 31 33 30 33 p + . 0 4 2 1 3 0 3
000006:	39 30 34 30 7E 01 54 05 2B F0 9 0 6 0 - , T + .
000007:	06 00 08 91 4A 00 04 00 05 D9 - + . . . 2 - . .
000008:	69 75 08 0C 01 06 00 7C 85 74 3 4 - . . . 1 - 5
000009:	C9 BC 43 62 9C 04 00 00 81 10 - . C - . . . + -
00000A:	69 6C 6E 6F 76 61 70 6B 6F 6E 1 n m o v s p h o n
00000B:	65 20 49 50 34 20 10 12 56 35 n . I P 4 0 0 . Y S
00000C:	2E 30 31 20 72 63 32 20 5B 30 - 0 1 . e c 2 . [0
00000D:	34 2D 15 36 32 37 5D 00 01 05 4 - 5 6 2 7] + .
00000E:	00 37 54 63 6C 39 30 71 F9 0F - T T 0 1 9 0 9 -
00000F:	52 E9 99 20 11 9C 8D 00 99 33 R -
000010:	00 02 01 00 CD 1C 02 00 07 00 R -
000011:	65 09 49 75 05 88 11 00 72 04 - . 5 0 -
000012:	80 8A E9 09 D3 11 9C 8D 00 90 -
000013:	33 00 02 D1 00 CA 06 13 00 00 3 -
000014:	00 0C 20 13 00 08 05 00 01 00 -
000015:	05 D9 69 75 40 08 80 1C 40 00 - . 5 0 9 - . .



VoIP Playback of Voice & Video

GTEN

VoIP Cells - Microsoft Internet Explorer

Analysis CDR QoS Help H323 Protocol Analysis

Data Format: Nilesun dataset Begin Time: Apr 22 06:29:01 2004 Filter: Rows: Update

Data Source: Export-ImportDemo-02 End Time: Apr 22 12:39:01 2004

Call Viewer Message View Packet View RAS View

Calls

Call Duration (sec)	Calling IP Address	Called IP Address	Calling Party Number
39.450163	10.28.2.39	10.28.2.37	NA
1.4524368	10.28.2.37	10.28.2.39	NA

Messages in Call 1

Signalling	Media	Message	Date	
0.200000	0.200000	10.28.2.39, 1289	Setup	10.28.2.39, 1729
0.204281	0.204281	10.28.2.39, 1289	Alerting	10.28.2.37, 1729
0.204659	0.204659	10.28.2.39, 1289	Connect	10.28.2.37, 1729
0.204730	0.204730	10.28.2.39, 1270	Terminal Capability Set	10.28.2.37, 1780
0.208230	0.208230	10.28.2.39, 1270	Master Slave Determination	10.28.2.37, 1780
			Terminal Capability Set	10.28.2.37, 1780
			Master Slave Determination	10.28.2.37, 1780
			Terminal Capability Set Ack	10.28.2.37, 1780
			Master Slave Determination Ack	10.28.2.37, 1780

Audio / Video Playback Buttons

Message Elements

Fields Packets

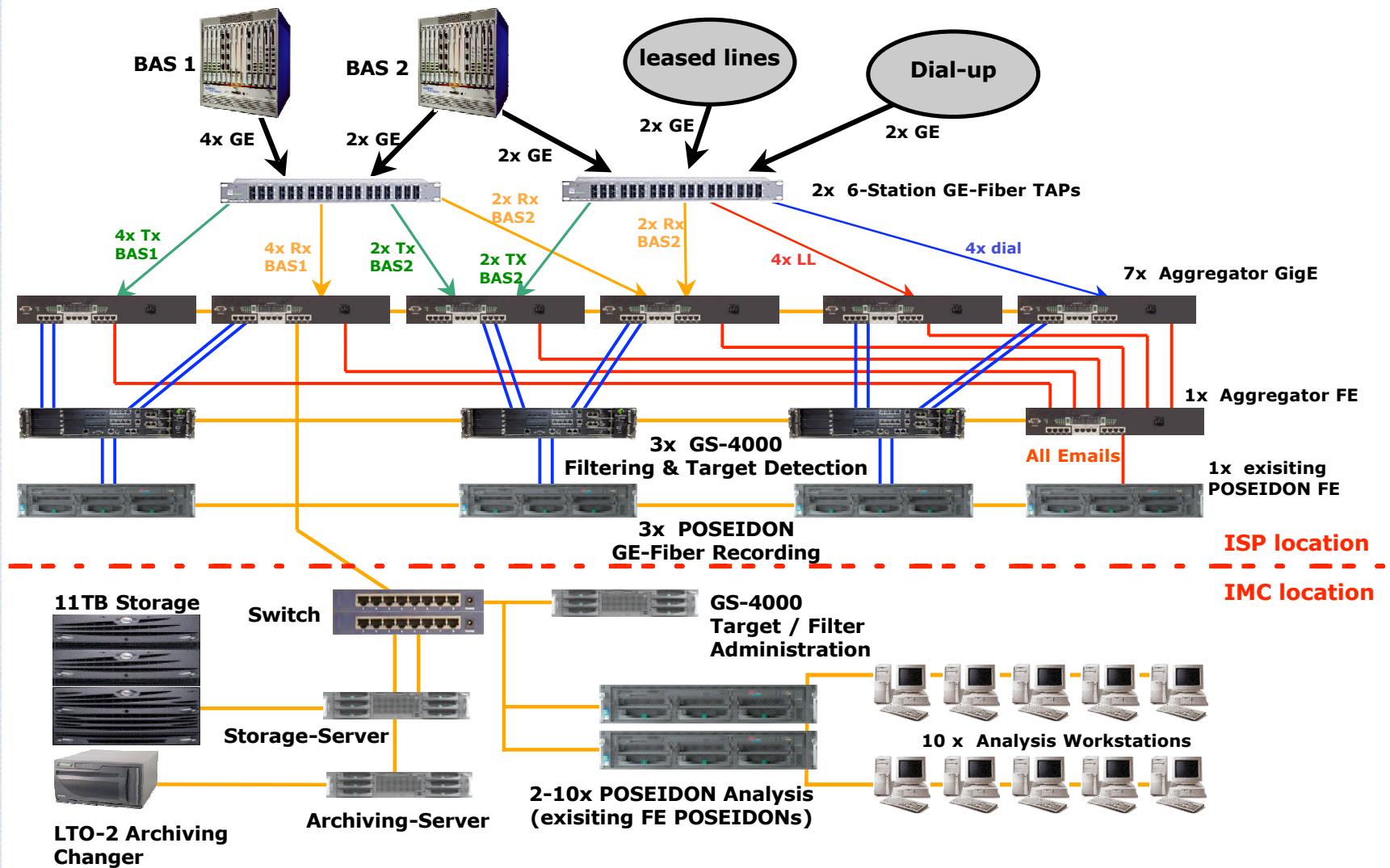
Setup

Arrival Time: 4/22/2004 8:57:51.660127
Packet Length: 289
Protocol Discriminator: 0.931
Call Reference Value Length: 2
CRef Flag: destination
Call Reference Value: 27517
Message Type: Setup
Bearer-Capability
Length: 3
Coding Standard: ITU-T Standardized Coding
Information Transfer Capability: Unrestricted Digital Information
Transfer Mode: Packet Mode
Information Transfer Rate: Packet Mode

10.28.2.39 <-> 10.28.2.37

00040: 92 15 E3 F3 2E 0E 50 18 FF FF
00050: C1 FF 00 00 08 02 65 7D 05 04
00060: 03 88 C0 A5 28 11 4D 69 63 68
00070: 61 27 73 20 4E 6F 74 65 62 6F
00080: 6F 6B 00 78 00 CB 05 10 AB 06
00090: 00 09 91 44 00 02 01 40 0F 00
00100: 4D 00 69 00 63 00 4
00110: 27 00 73 00 20 00 4
00120: 74 00 65 00 62 00 4
00130: 6B 22 C0 B5 00 53 4
00140: 63 72 6F 73 6F 66 4
00150: 65 74 4D 65 65 74 4

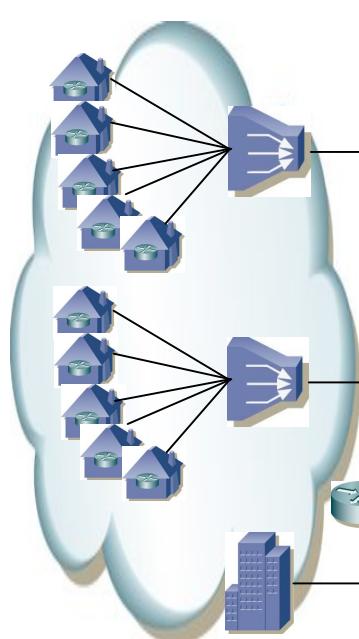
LI - Monitoring of a complete Country Based on modern IP – Network Requirements



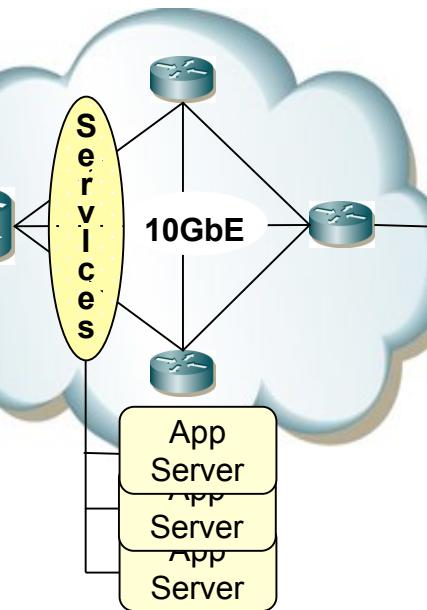


New Services Offerings Requiring up to 10GbE Deployment in Aggregation Points. LI can be build inside same “Service Points”

Access Network



Aggregation Network

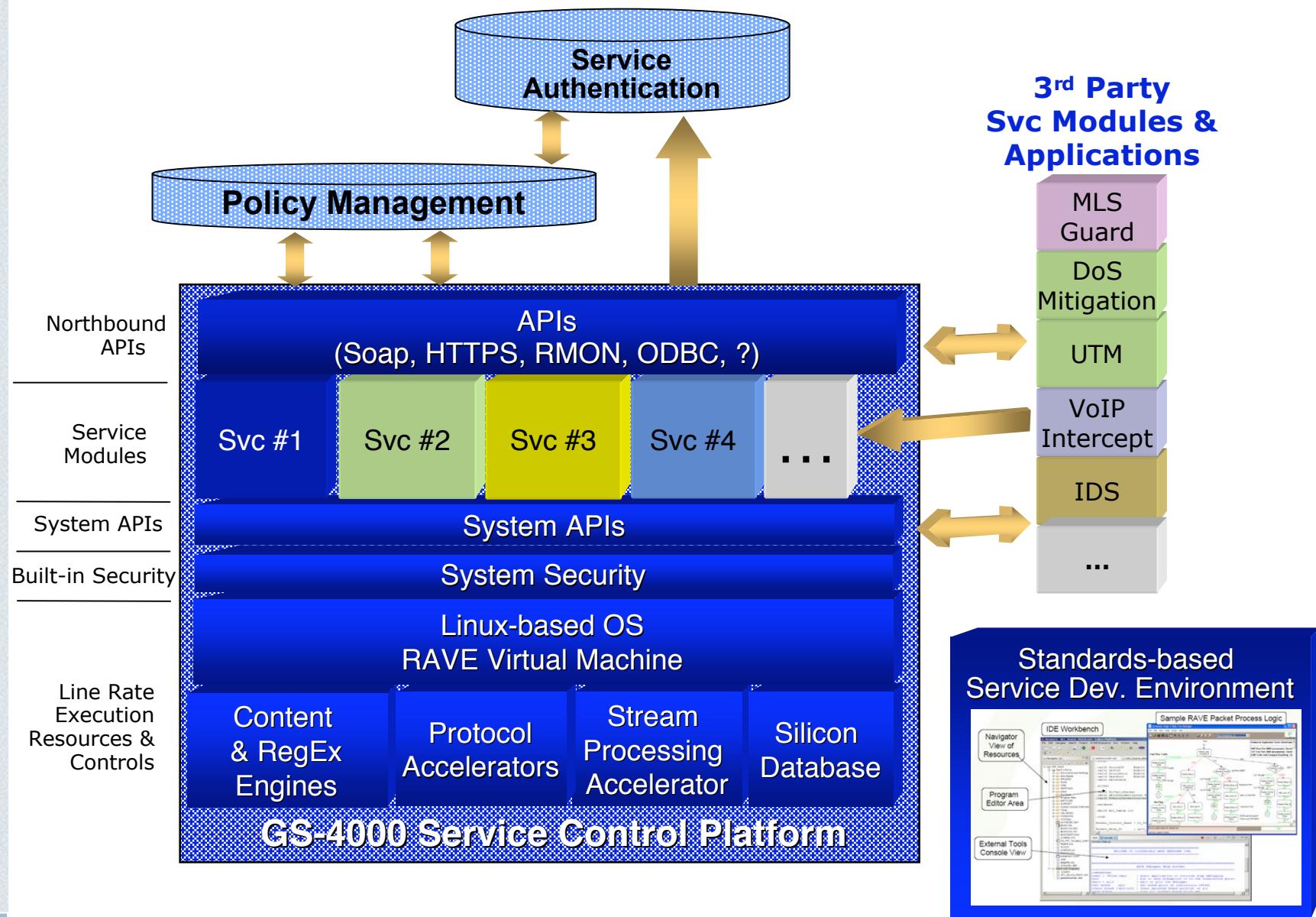


- **10GbE rolling out in the aggregation network**
- Optimal location for Service Control & Policy Enforcement + **Interception**
- Requiring 10Gbps of:
 - ♣ Inspection;
 - ♣ Classification; and
 - ♣ Control

CIR is forecasting the market for 10-Gbps ports on telecommunications and data communications equipment will grow from 221,000 ports in 2006 to 1.2 million by 2010; *Light Reading, Nov 2005.*



Functional Architecture of modern Aggregation Units





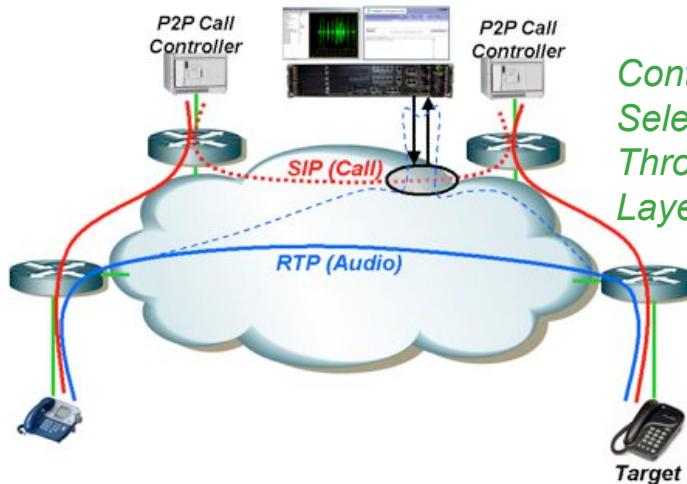
GTEN

- A Few Application Example out of many possible ones for the new -All in One Plattform-:



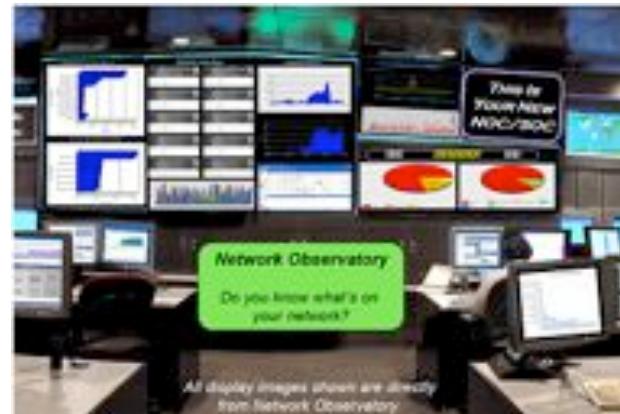
GTEN

Traffic Mirroring / Intercept Selective Interception, Replication, Session Hijacking



*Controlled IP Network
Selective Monitoring
Through Application
Layer Route Manipulation*

*Traditional IP
Traffic Mirroring
and Monitoring*



GS-4000 Traffic Monitoring:

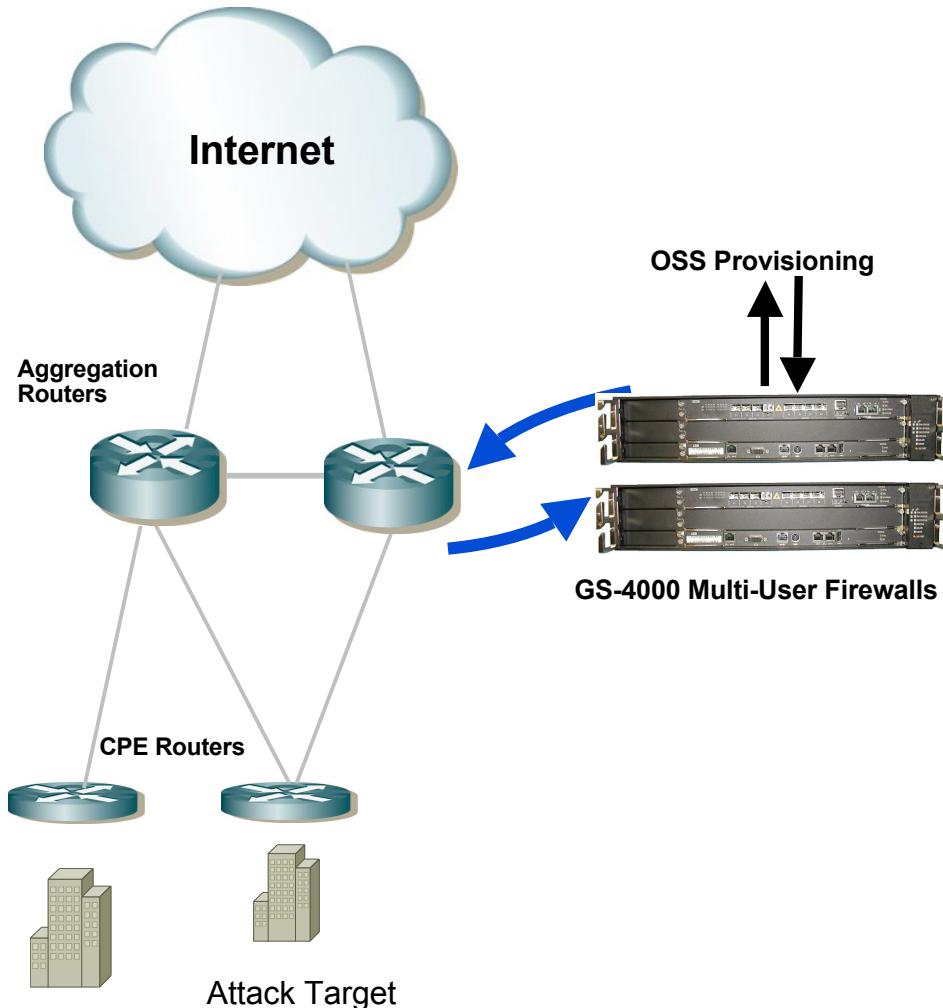
- Multiple Deployment Methods
 - Passive Tap Deployment with Intercept & Arrival Rate
 - Span Port with Inject Path for Session Controls
 - Active In-line for Selective Session Controls
 - HW Raw, MAC or GRE Distribution
 - SW Custom Delivery (iSCSI, FC/IP)
- Multiple Targeting Mechanisms
 - Flow Targeting (Webmail Sessions)
 - Content (Any Packets w/BOMB)
 - Content Flow (Bad Conversations)
 - Non-Port Protocol (SIP, Skype)
 - Circuit / 5-Tuple (MPLS, VLAN, etc.)
- Algorithm Based Reporting
 - Packet Accurate Netflow, IPFix
 - Host Fingerprinting
 - Custom Traffic Profiling

GTEN has significant Government & Carrier Experience with numerous GTEN & Partner Solutions in "Traffic Mirroring"



Solution Example: Managed Multi-User Firewalls

Carrier Network Deployment & Provisioning



Service Provider Firewall Hallmarks:

- Multiple Independent Rule Sets
 - Per Subscriber Rule Sets
 - Mobility (Rule Sets Move As Needed)
 - Secure Separation of Rule Space
- Service Provider Subscriber Definition
 - IP Blocks
 - MPLS
 - VLAN (Virtual WAN/LAN Interfaces)
- Scalability & Capacity Planning
 - Multi-Gigabit Performance
 - Customer Flow Capacity Control
 - Customer Policy Capacity Controls
 - No Flow/Policy Degradation

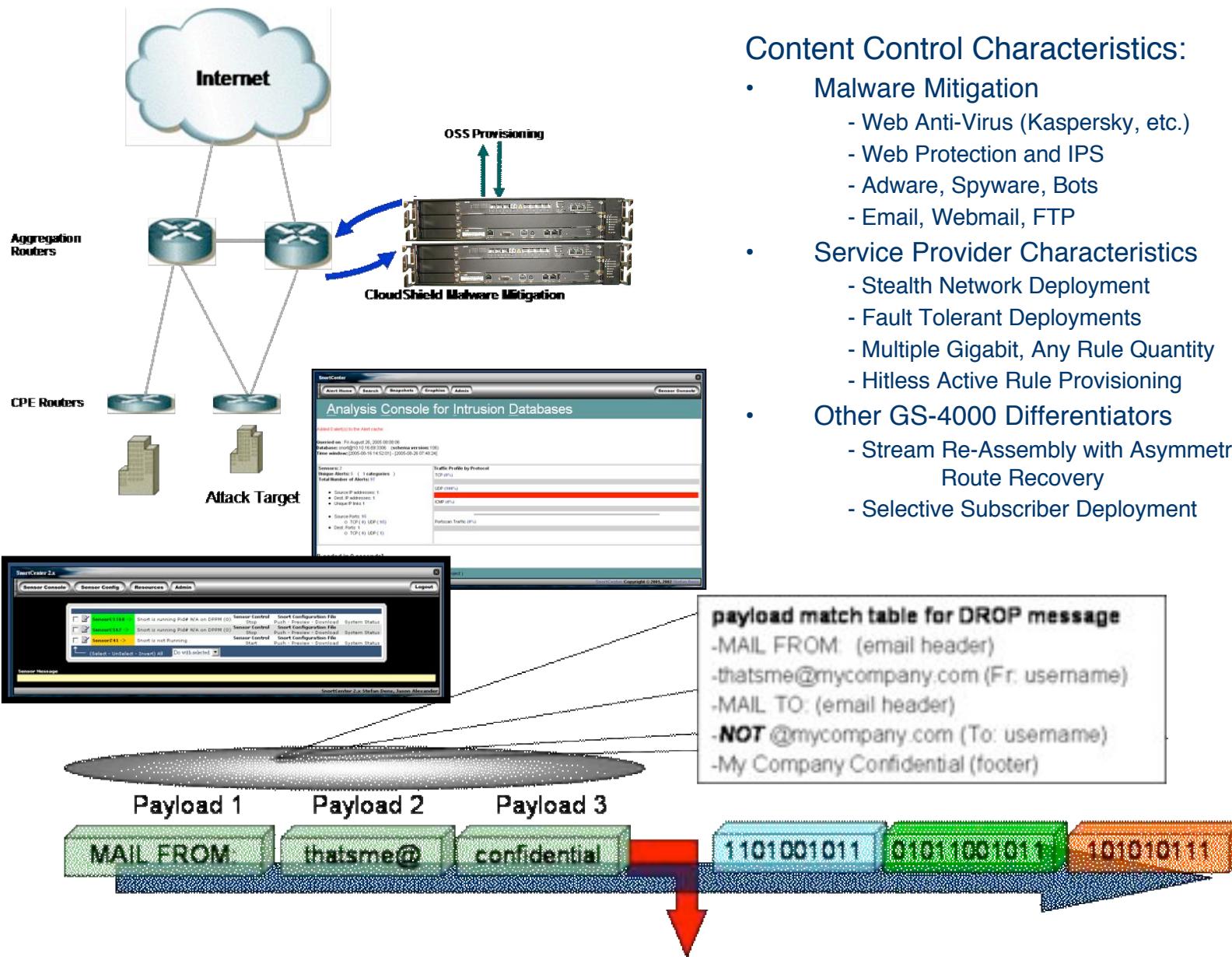
Multi-User Firewalls Are Different:

- 7-Tuple Customer Policy Definitions
 - SIP, DIP, SP, DP, Proto, VLAN, MPLS
- Policies Provisioned Per Customer
- OSS Policy Provisioning (SOAP)
- Dynamic Policy Migration
- Dynamic Customer Detection (DHCP)
- Transparent & Transparent NAT/PAT
- Asymmetric State Synchronization
- IPv6, Encapsulation, Multi-L2/2.5



Solution Example: Malware Mitigation

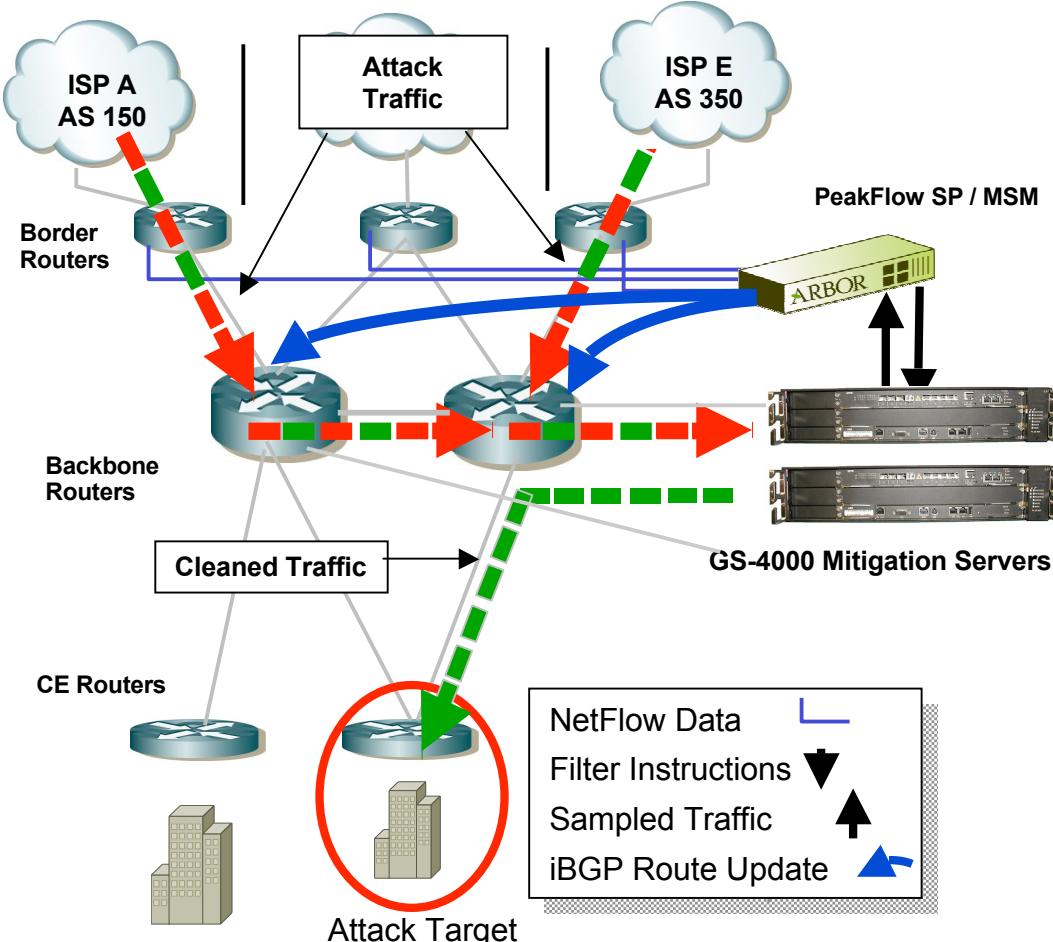
In the network content inspection & control





Solution Example: DDoS Mitigation

Multi-Function, Multi-Customer DDoS Mitigation Solution



Market Leading Mitigation:

- Supports Multiple Analysis Vendors
 - Arbor Networks plus Open API
- Scalable Deployments
 - BGP Peered & Clusters
 - Multiple Gigabits Per Blade
 - Shared Mitigator Deployment
- Flexibility
 - Extensible Mitigation Techniques
 - Netflow Generation
 - Content Based Scrubbing
 - Additional Services Capabilities

Broadest Built-in Attack Filters:

- SYN & ACK Floods (**Fastest Proxies**)
- Invalid TCP (SYN-FIN, FIN, SYN-RST and TCP-Null)
- DNS Floods (**Patented**)
- Fragmentations (UDP, TCP, ICMP)
- ICMP Floods
- Zombie Attacks
- Worms
- Bogon/ Private IP Space
- Block Large Frames (>1500, >9000)
- TCP with Empty Payload
- Layer 7 Attacks (**Patented**)

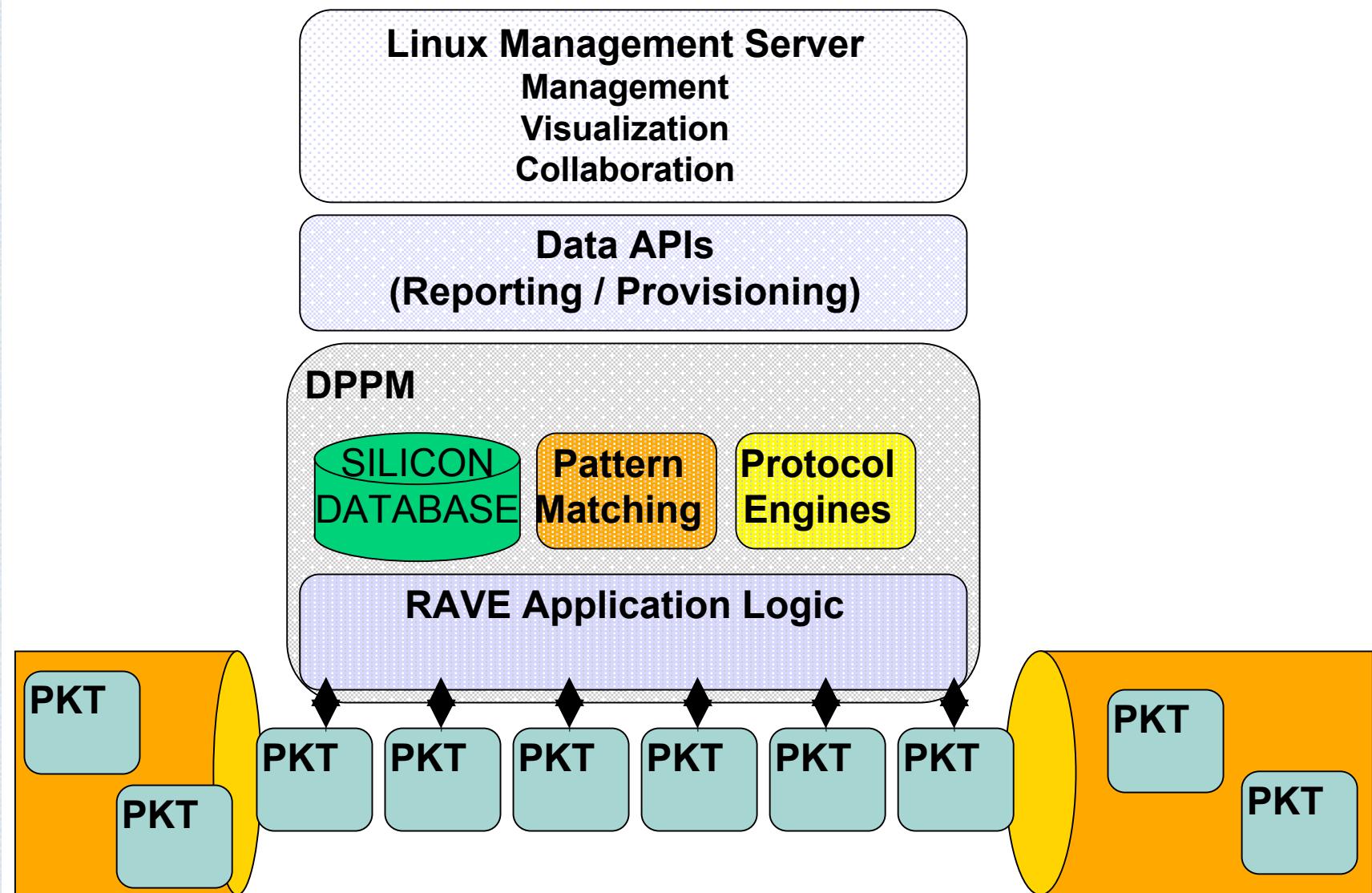


Benefits:

- Plattform allows to run many standard jobs beside LI simultan
- Plattform allows to implement individual customer solutions
- Plattform will not loose a single „bit“
- Plattform internal delay very small



CS-2000/GS-4000 Processing Pipeline

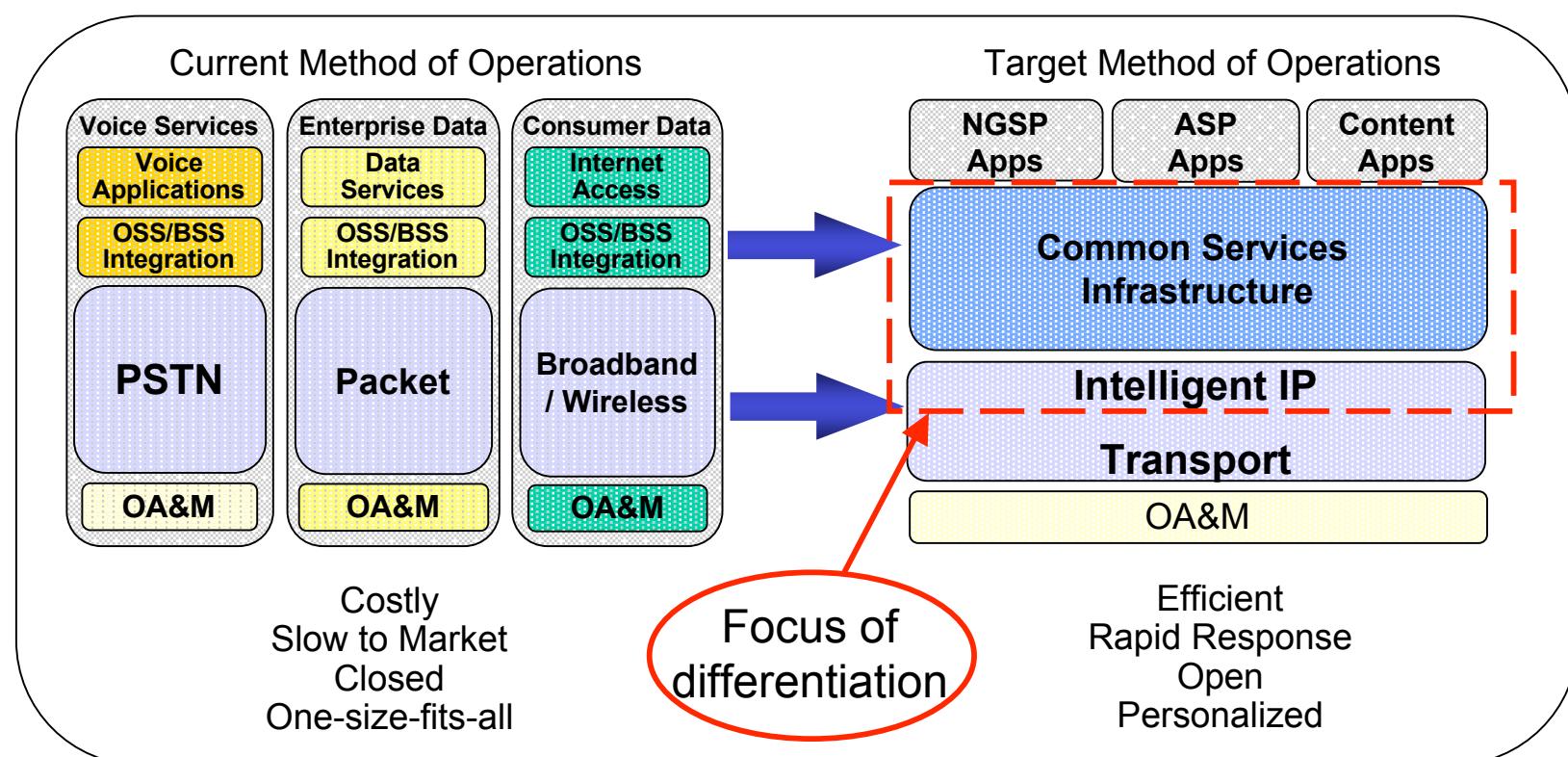




Migration to IP is Critical for Participation in the IP Economy, but also Transparency

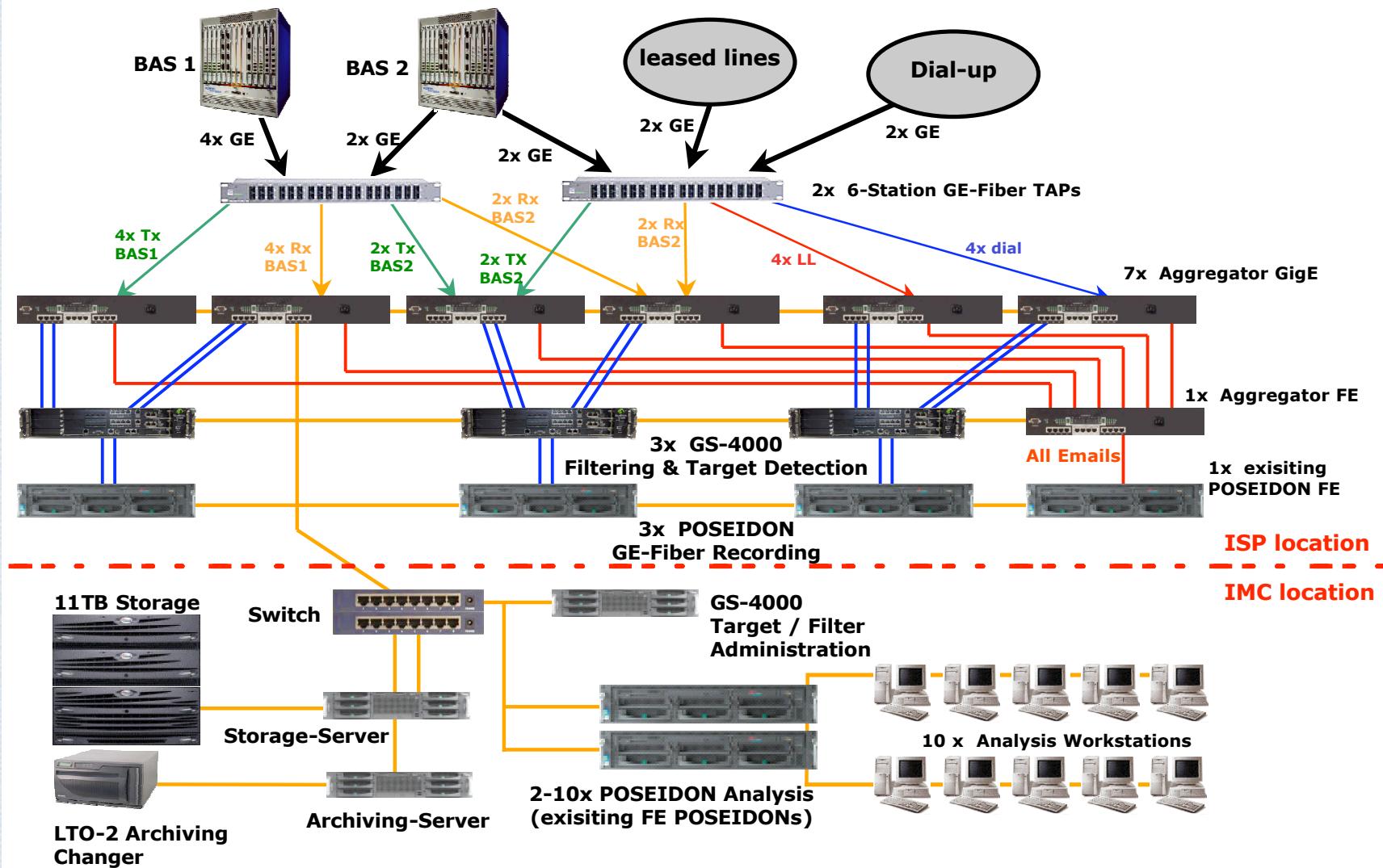
The pace of convergence to a common IP infrastructure is accelerating

- New-age IP service providers have distinct advantages over incumbents
 - ♣ e.g. personalized services
 - ♣ faster service development cycles
 - ♣ More granular, bounded service levels





LI - Monitoring of a complete Country based on modern IP – Network Requirements



A photograph of a globe with a binary code pattern (0s and 1s) overlaid. Several 3D puzzle pieces are floating around it. One piece has the word "GTEN" and a large orange puzzle piece symbol on it. Another piece has a small orange puzzle piece symbol. A red 3D figure is also visible.

Question?

A globe is centered against a background of blue binary code. The globe's surface is covered in binary digits (0s and 1s). Several 3D puzzle pieces are floating around the globe. One piece is white with orange puzzle pieces on it, another is purple with a white puzzle piece, and a third is dark grey with an orange puzzle piece. A small red 3D figure is also visible near the globe.

**Thank you very
much for your
interest**