QOSMOS
Your Network is Information

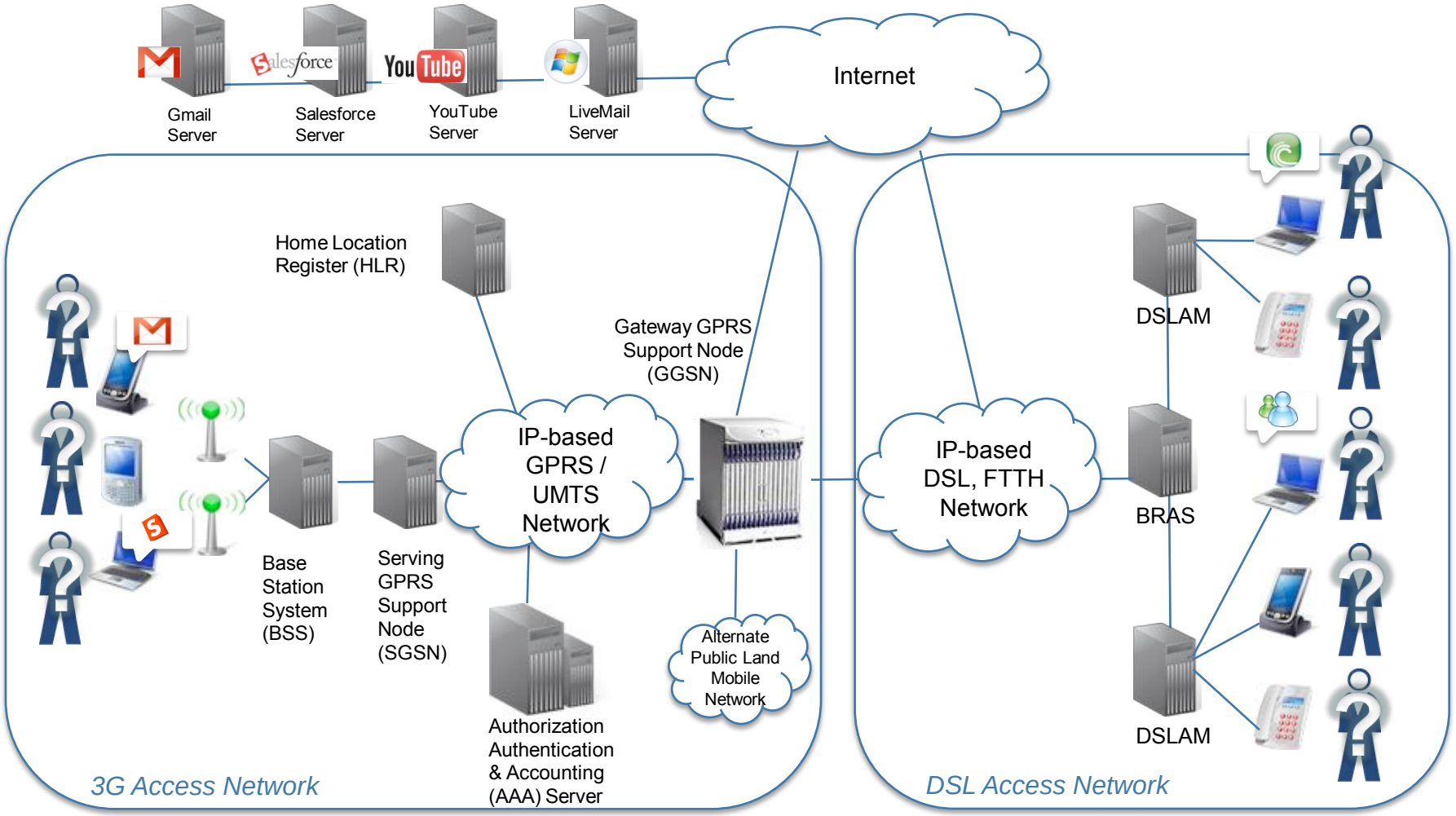
Enabling True Network Intelligence Everywhere

Managing Virtual Identities Across IP Networks

Jean-Philippe Lion
Vice President, EMEA Sales

ISS Prague, June 2009

A New Complex Situation Creates a Number of Challenges to Correctly Identify Targets…

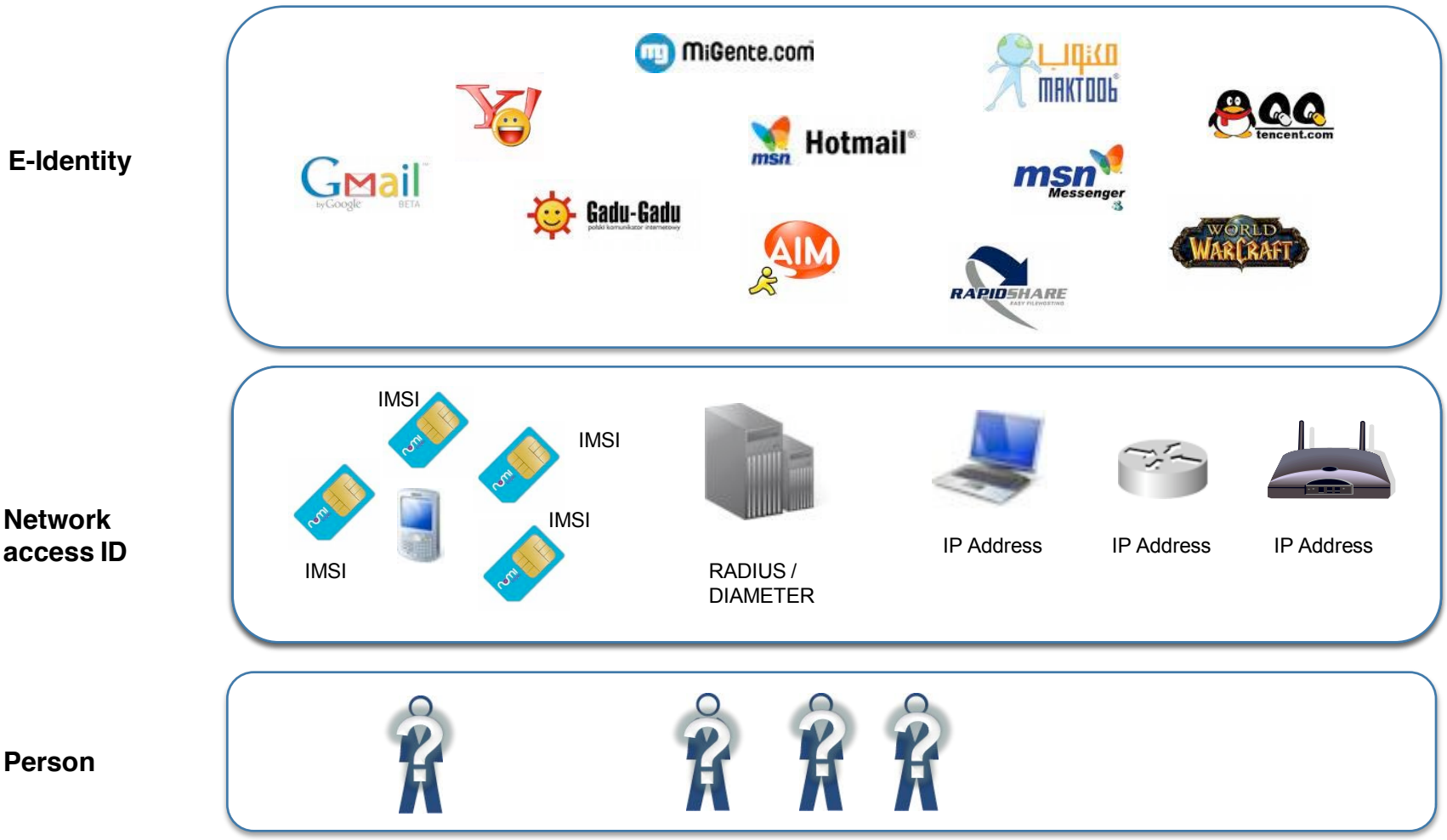


How do you accurately identify targets across multiple applications, multiple physical locations, multiple terminals and multiple identities?

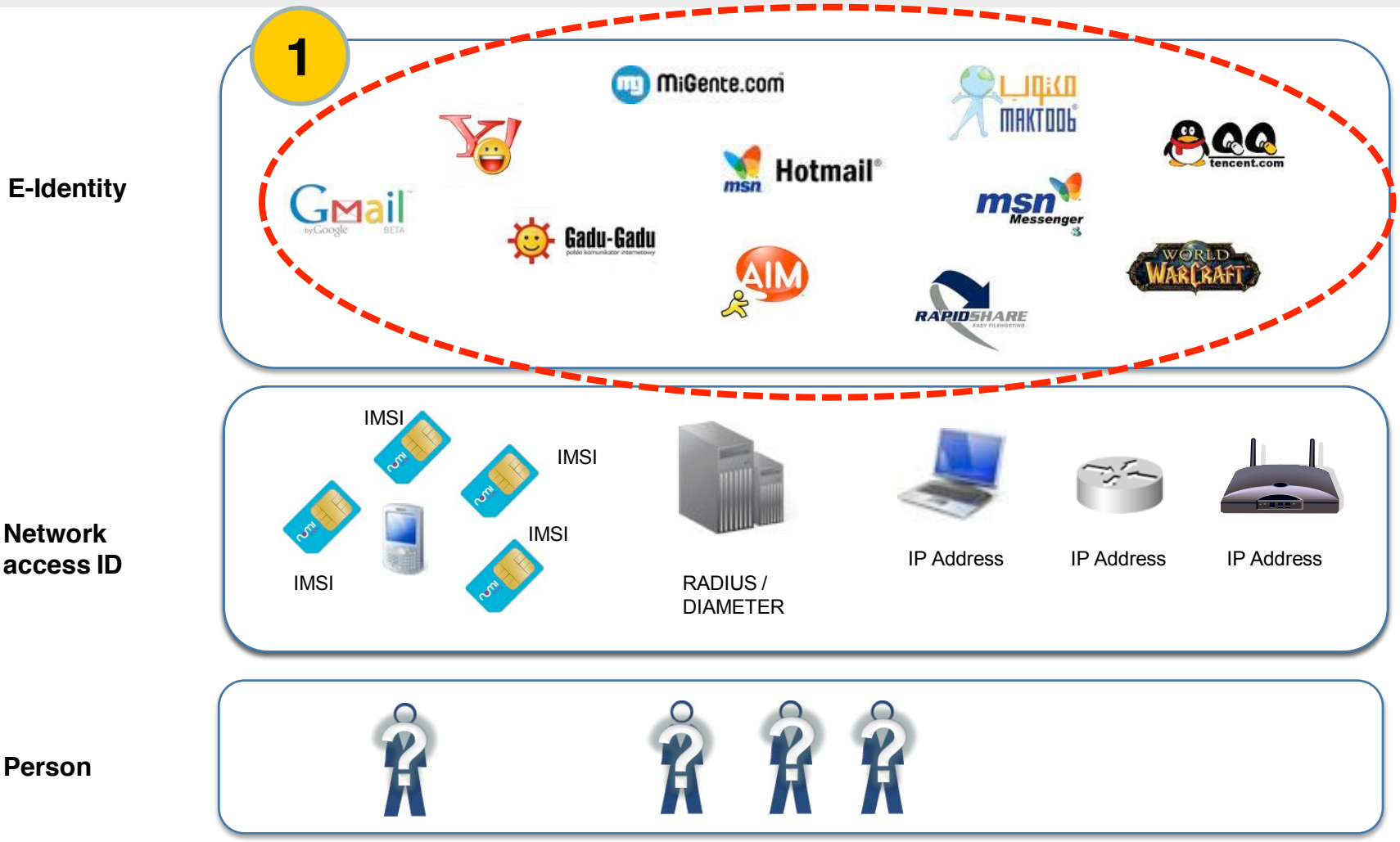
QOSMOS
Your Network is Information

Contents

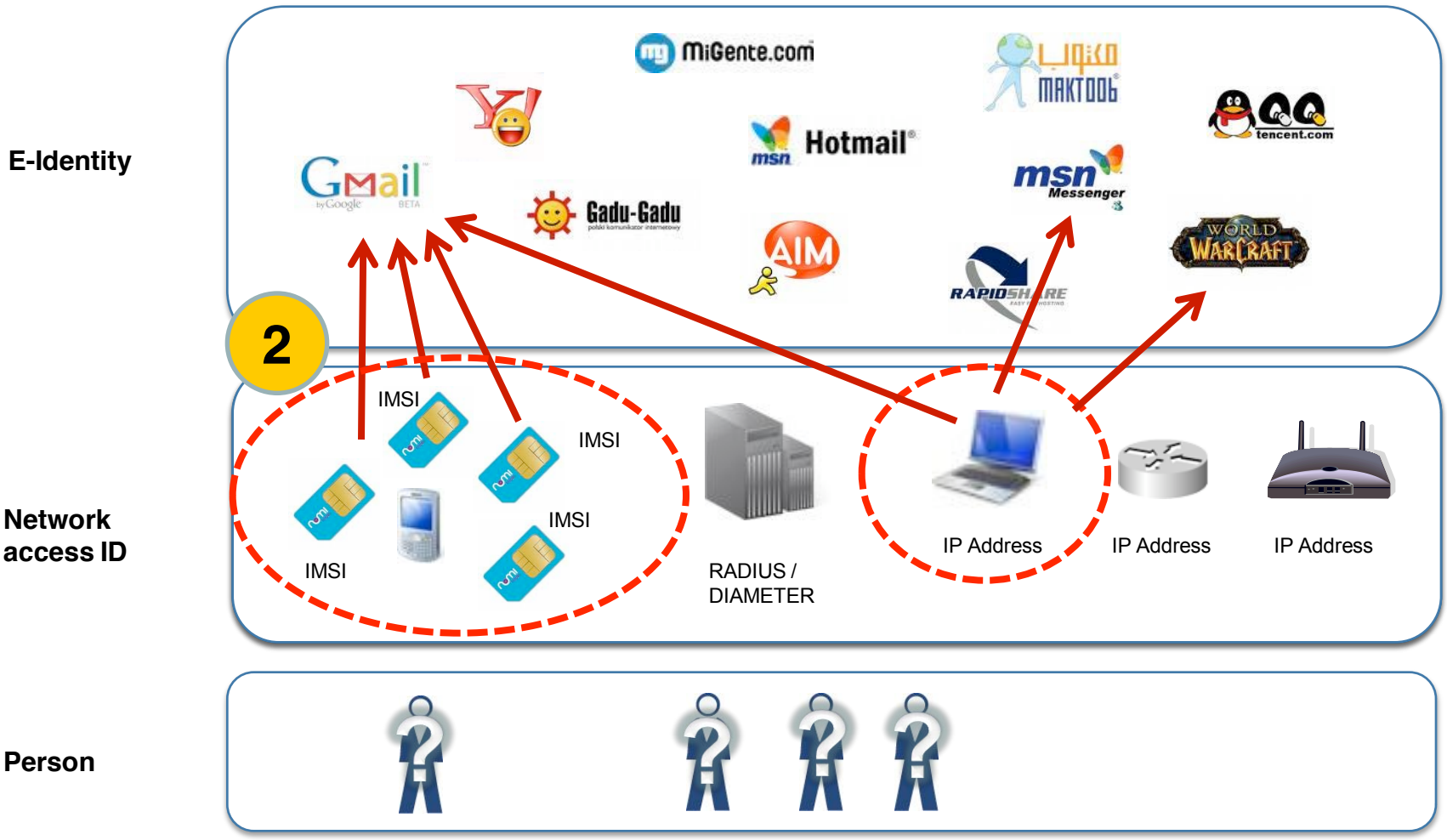
How do you Identify Targets Across Multiple (Virtual) e-Identities and Multiple Network Access IDs?



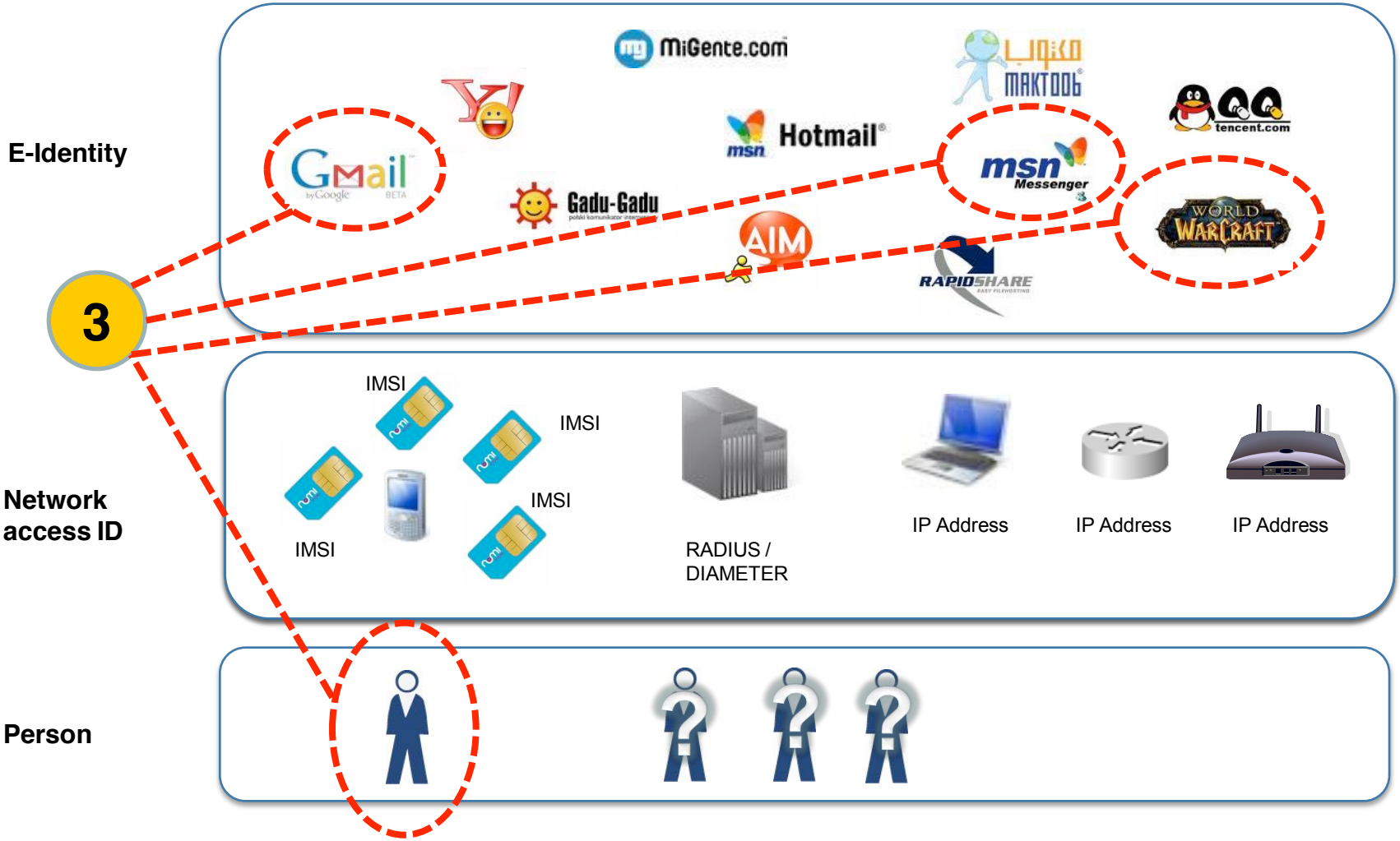
Step 1: Track Usage of All or Suspected Virtual IDs



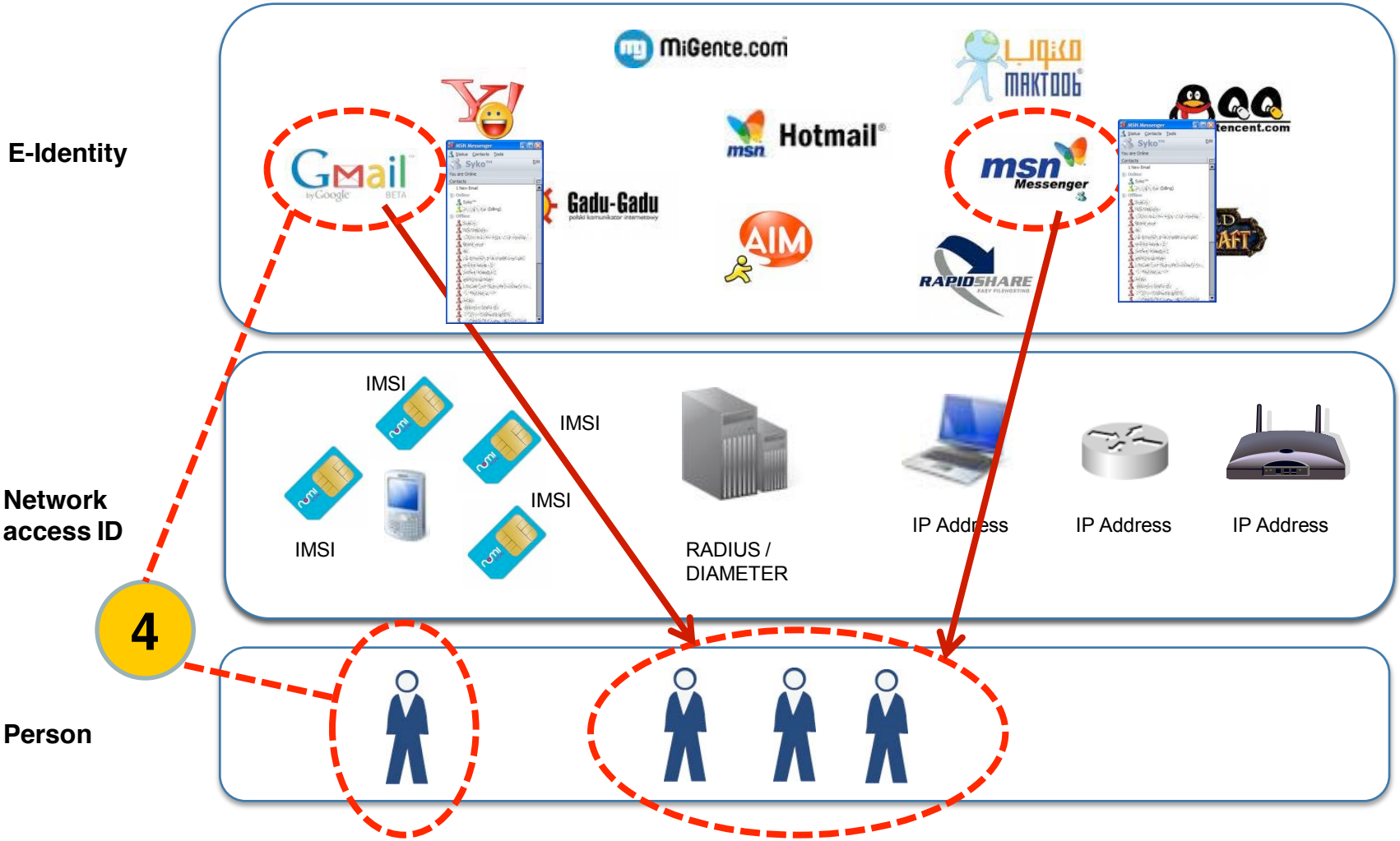
Step 2: Link Virtual IDs to Network Access IDs



Step 3: Intercept all Traffic from Virtual IDs and Link to Physical Person



Step 4: Extract Contact List to Understand Links Between People



QOSMOS
Your Network is Information

Contents

Challenge #1: Identify Targets Using the Steps Previously Described

- **New challenges for LEAs**
  - People are no longer linked to physical subscriber lines
  - The same person can communicate in several ways: VoIP, IM, Webmail, etc.
  - How to launch interception across all communication with a single trigger?
- **Answer**
  - Identify users and intercept all type of communication initiated by the same user when a trigger such as “user login” is detected
  - Identify Internet access point and physical device of targeted user
  - Link trigger to IP address, MAC address, IMSI, IMEI, etc.
  - Show all communication on the same screen, in real-time: Webmail, Instant Messaging, FTP, P2P, Financial Transactions

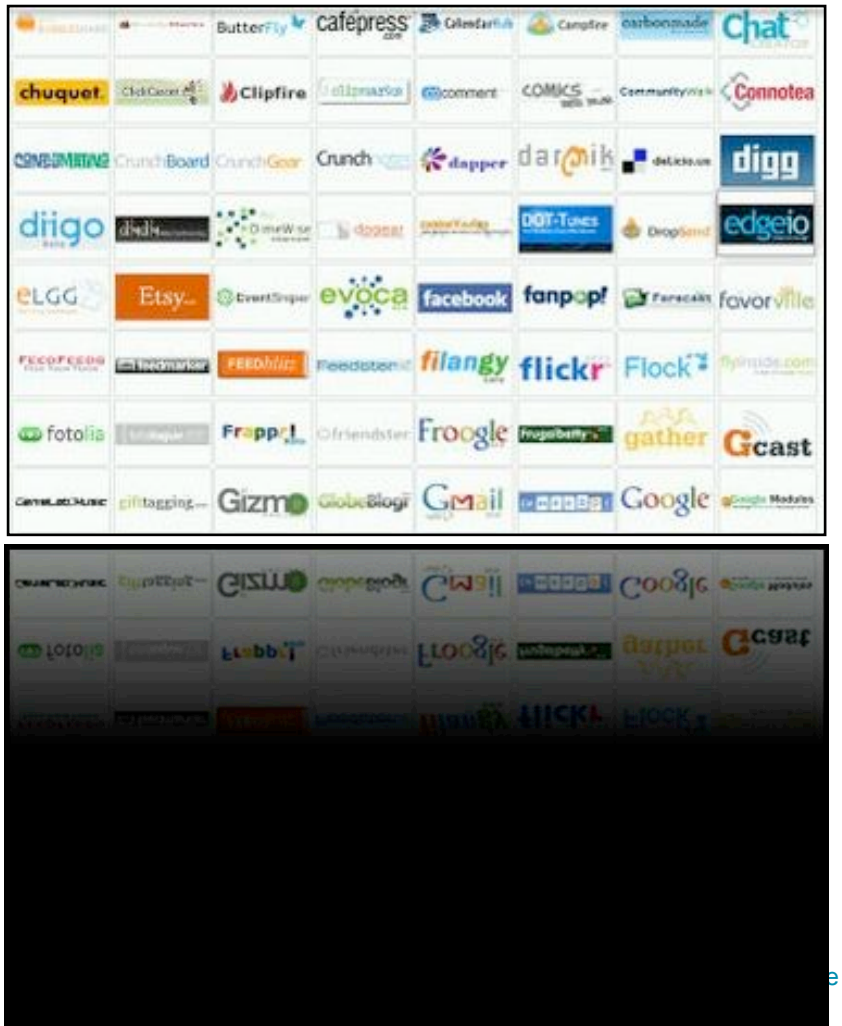
1. Trigger = IM activity on monitored user login

2. Link user login to:
- IP address
- or IMSI

3. Intercept IM + Webmail + VoIP from a particular user on a certain PC or mobile to a specific person in real-time!

Challenge #2: Need to Understand Different Applications Behind The Same Protocol

- **HTTP is not only used by Web browsing**
  - HTTP is also used by: LiveMail, Gmail, YahooMail, GoogleEarth, GoogleMap, Salesforce, iGoogle, mashups, and hundreds of other applications...
- **A user typically has different IDs in different applications**
- **Answer**
  - Understand all the applications using a particular protocol (such as HTTP)
    - Deep and stateful analysis of IP packets
    - Connection context and session management
    - Connection expiration management
    - IP fragmentation management
    - Session inheritance management



Challenge #3: Ability to Recognize Regional Protocols

- **Targets may use regional services for Webmail, Instant Messaging, Social Networking, etc.**
  - Used by large a number of people in local country and local language
  - Targets can also use services from outside their country of origin, in local language or other languages
- **Answer**
  - Extend protocol expertise to local Webmail, Instant Messaging, Social Networking, etc.

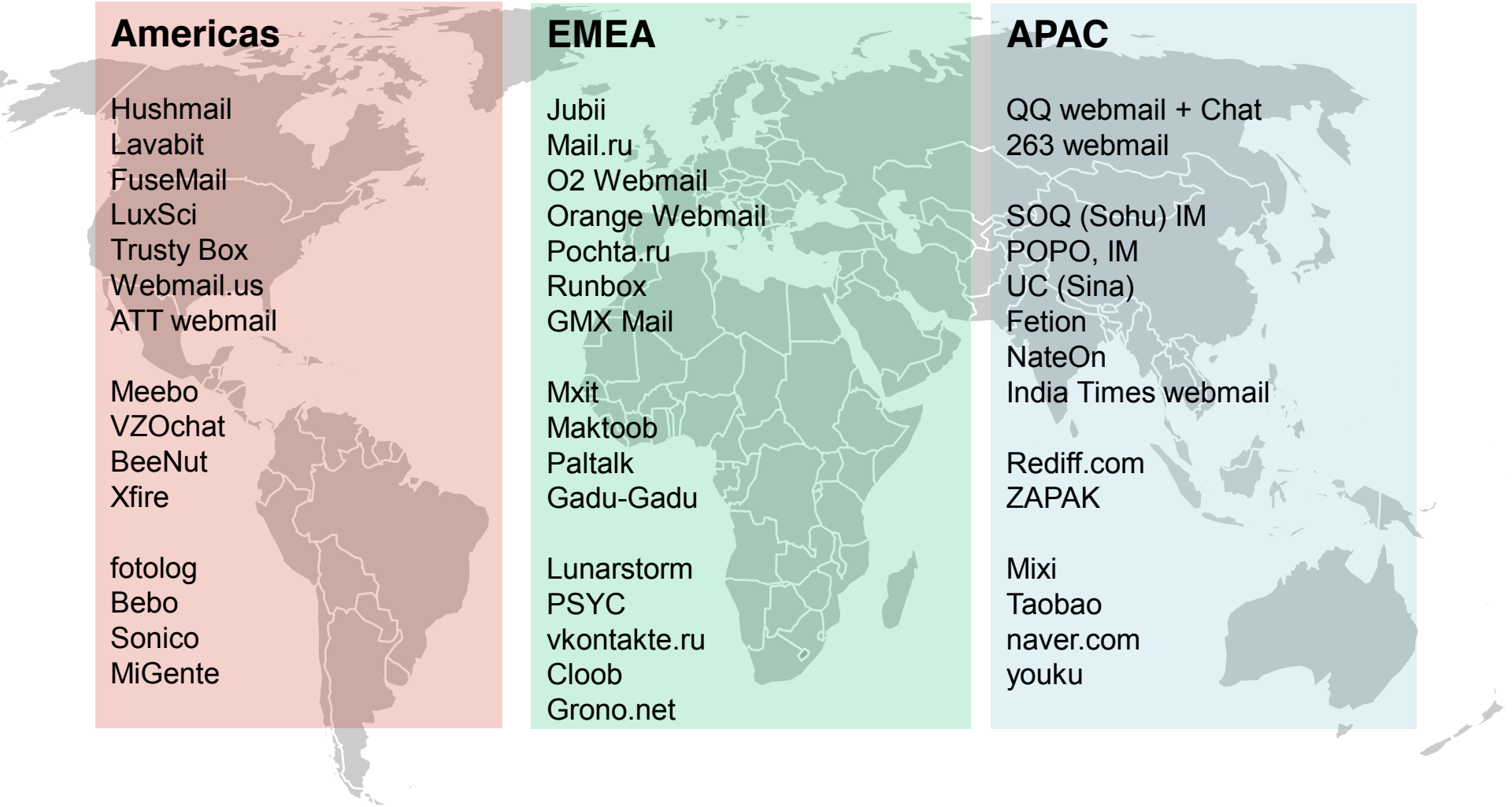
Gadu-Gadu ...nie tylko komunikator!

Poland

腾讯网 qq.com

China

Examples of Regional Protocols



Americas

Hushmail
Lavabit
FuseMail
LuxSci
Trusty Box
Webmail.us
ATT webmail

Meebo
VZOchat
BeeNut
Xfire

fotolog
Bebo
Sonico
MiGente

EMEA

Jubii
Mail.ru
O2 Webmail
Orange Webmail
Pochta.ru
Runbox
GMX Mail

Mxit
Maktoob
Paltalk
Gadu-Gadu

Lunarstorm
PSYC
vkontakte.ru
Cloob
Grono.net

APAC

QQ webmail + Chat
263 webmail

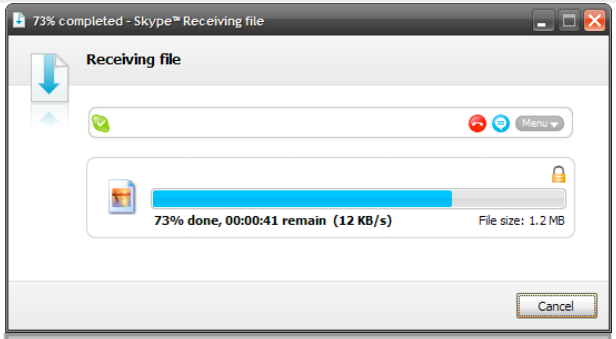
SOQ (Sohu) IM
POPO, IM
UC (Sina)
Fetion
NateOn
India Times webmail

Rediff.com
ZAPAK

Mixi
Taobao
naver.com
youku

Challenge #4: Many Applications have Evolved from their Initial Use

- **Applications are used differently than their originally intended purpose**
  - File transfer in Skype
  - Instant Messaging in WOW
  - Financial transactions in Second Life
  - Use of “Dead Mailboxes” within Webmail => shared storage space and folders (same login/password for different users)
- **Answer**
  - Understand real application usage by correlating multiple sessions and packets
  - Ensure a full view of application / service / user, independently of protocol

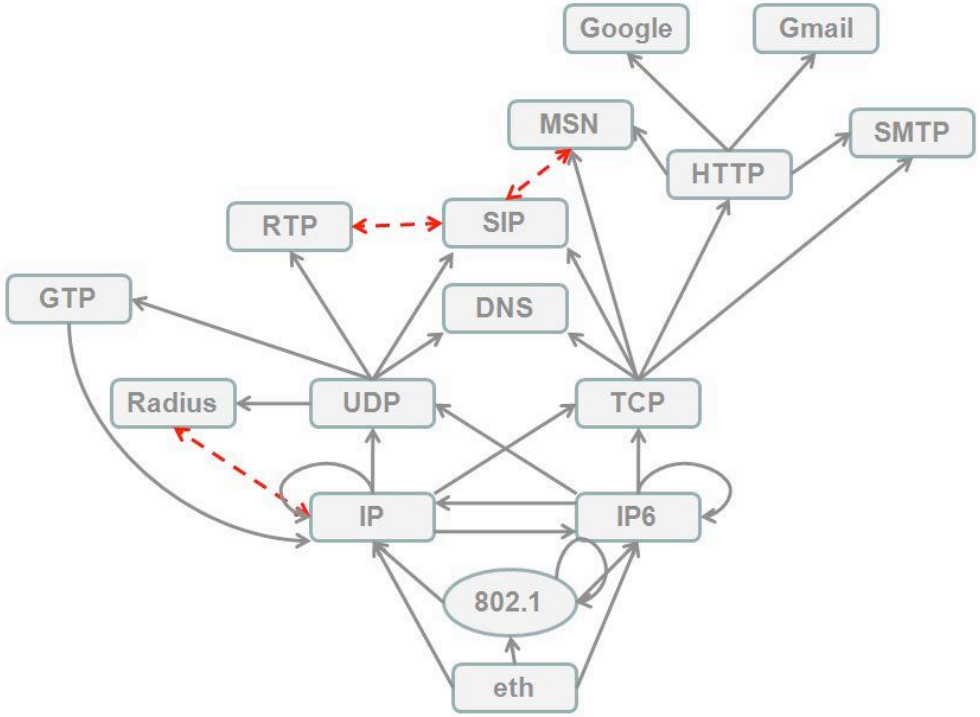


Skype file transfer

World Of Warcraft Instant Messaging

Challenge #5: Recognizing Correct Identity Means Going BEYOND OSI Reference Model

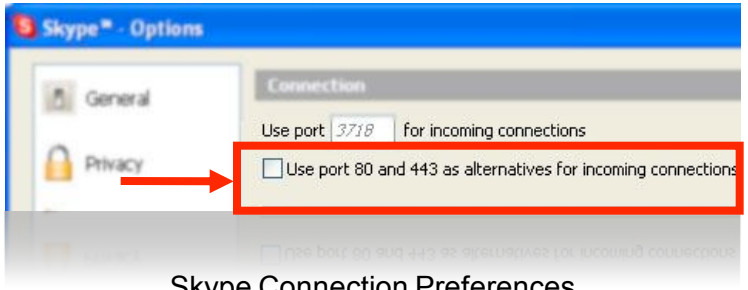
- **Users can easily hide their identity**
- **New, complex communication protocols do not follow OSI model**
  - Examples: P2P, Instant Messaging, 2.5G/3G (GTP), DSL Unbundling, (L2TP), VPN (GRE), etc.
- **Protocols are frequently encapsulated**
  - Example: multiple encapsulations in an operator DSL network (ATM / AAL5 / IP / UDP / L2TP / PPP / IP / TCP / HTTP)
- **Answer**
  - Extract user identity information in real-time, independently of OSI model and dig into encapsulation within several complex IP layers



Qosmos protocol graph

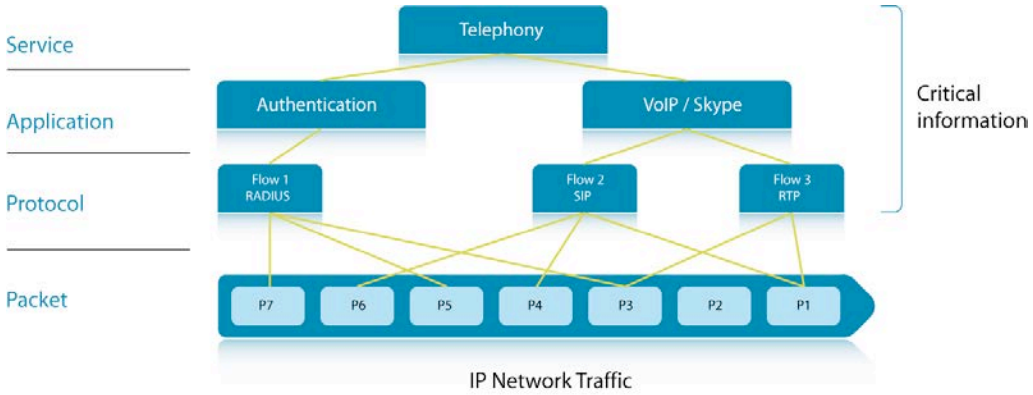
Challenge #6: Not Possible to Rely on IANA Ports to Track Applications and Users

- **Applications can no longer be linked to specific ports**
  - Port 80 = “The crime boulevard”
  - Skype runs on port 80, port 443, or on random ports
  - RTP does not use predefined ports
  - SIP negotiates and defines the ports used for data communication (RTP)



Skype Connection Preferences

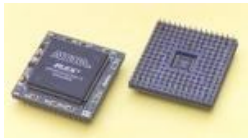
- **Answer**
  - Inspect complete IP flows rather than “packet by packet”
  - Track control connections: e.g. FTP data, SIP/RTP or P2P traffic
  - Ensure a full view of application / service / user independently of protocol



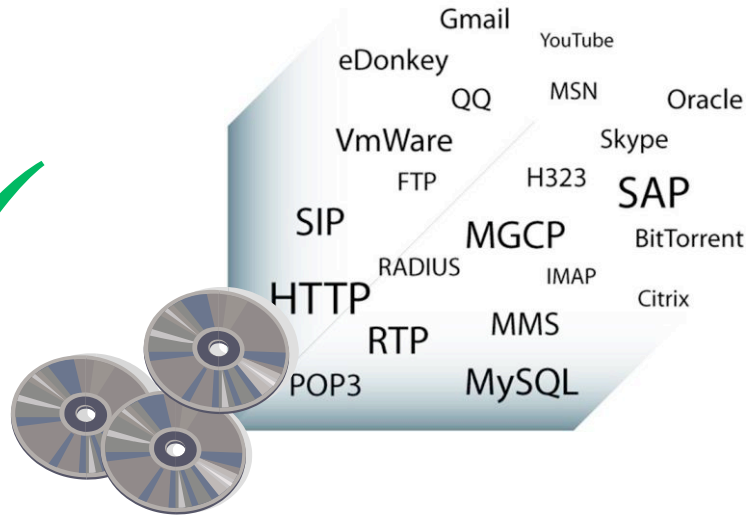
IP Network Traffic

Challenge #7: Adapt Rapidly to New Protocols

- **Difficult to handle an increasing numbers of protocols with dedicated ASICs**
  - Long development times (MONTHS)
  - Limited flexibility



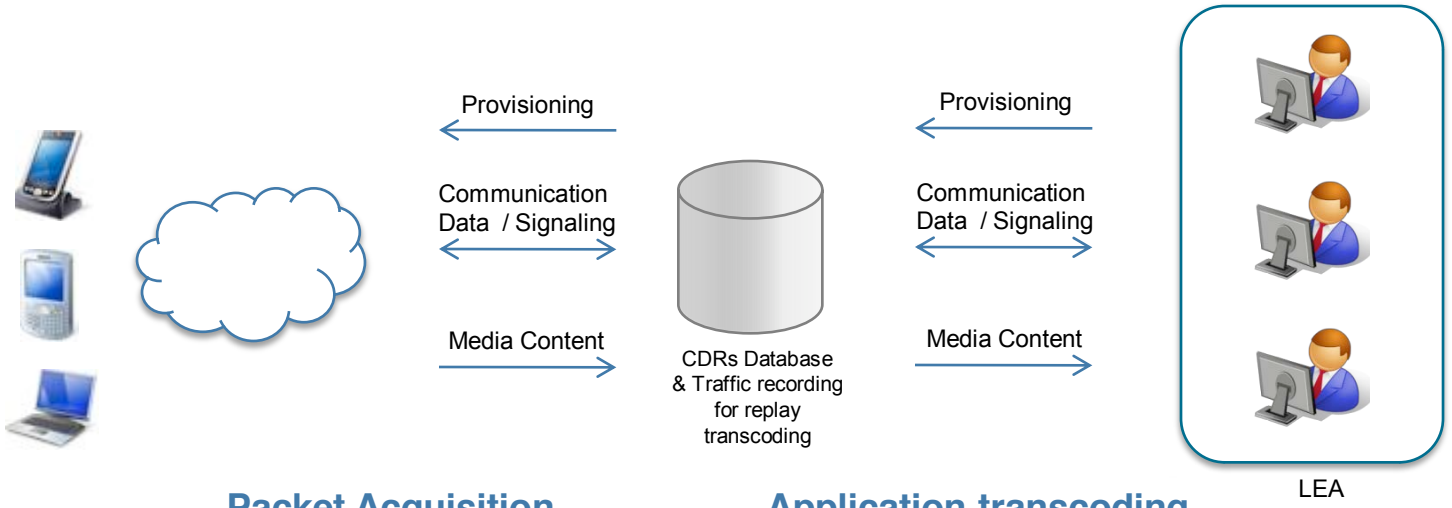
- **Answer**
  - Use a **software-based approach**, ensuring greater flexibility, easy updates and short development time (DAYS)
  - Shorten lead times to answer quickly to mounting threat patterns
  - Ensure high packet processing performance by using the latest standards-based, multi-core architecture
  - Make the software portable across different hardware platforms
    - Appliances, routers, IP DSLAMs, GGSNs, Set-Top-Boxes, PCs, etc.



QOSMOS
Your Network is Information

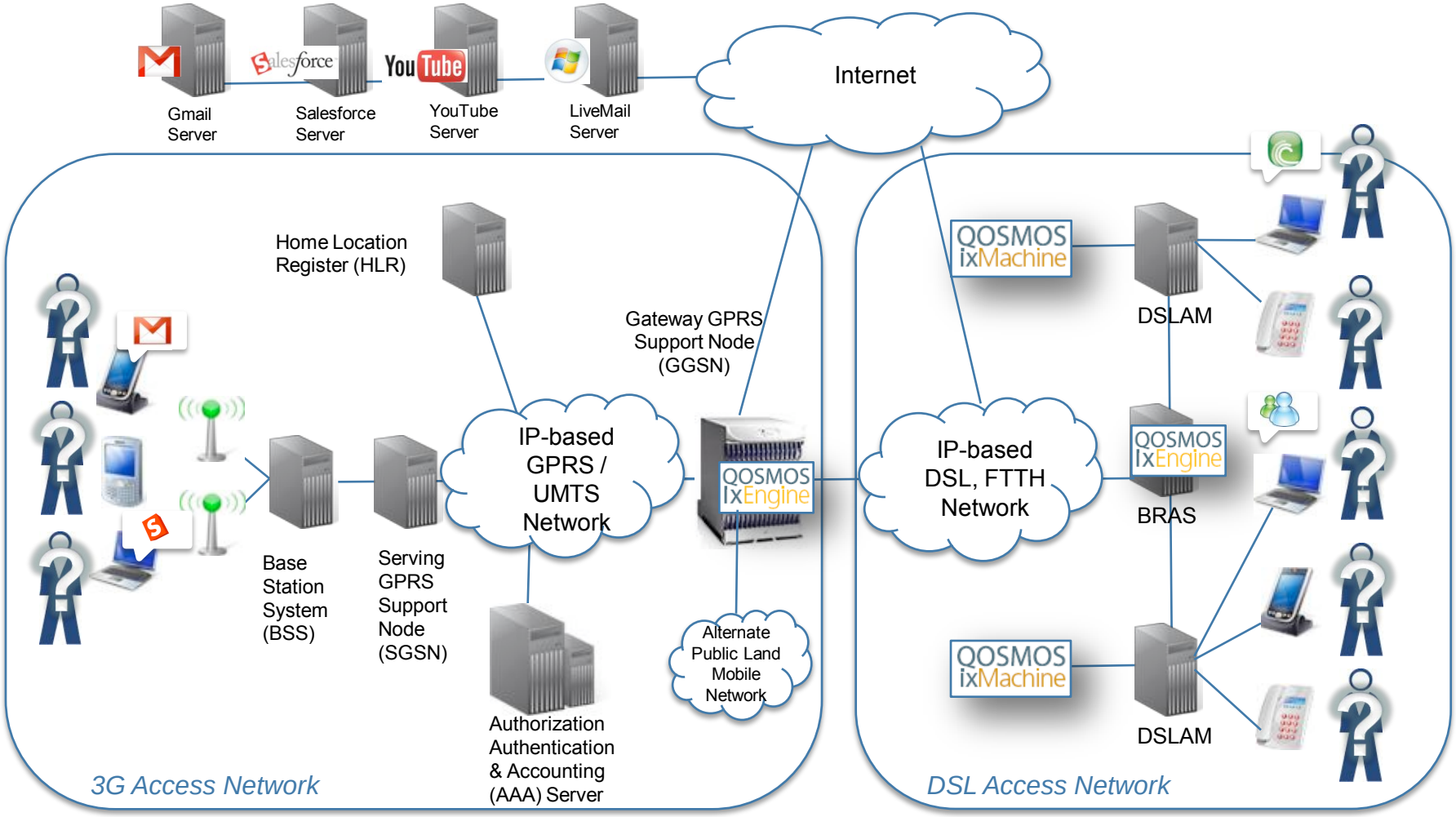
Contents

Qosmos Legal Intercept Solutions



- **Qosmos and its integrator partners offer a complete interception solution including:**
  - Flow classification
  - Applicative classification
  - Information extraction
  - Selective recording
  - *Application transcoding (mail, etc.)*
  - *Visualization*

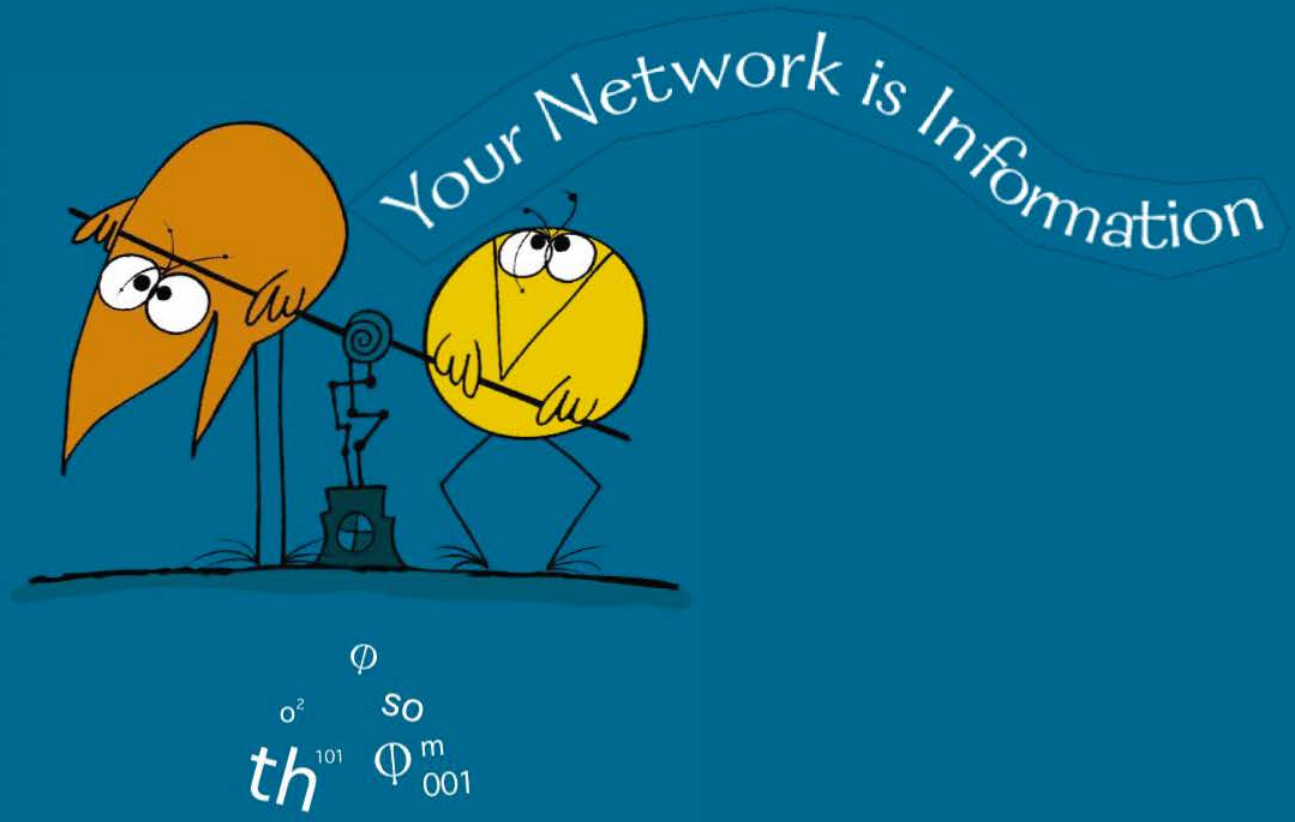
Summary: It Is Possible To Accurately Identify Targets!



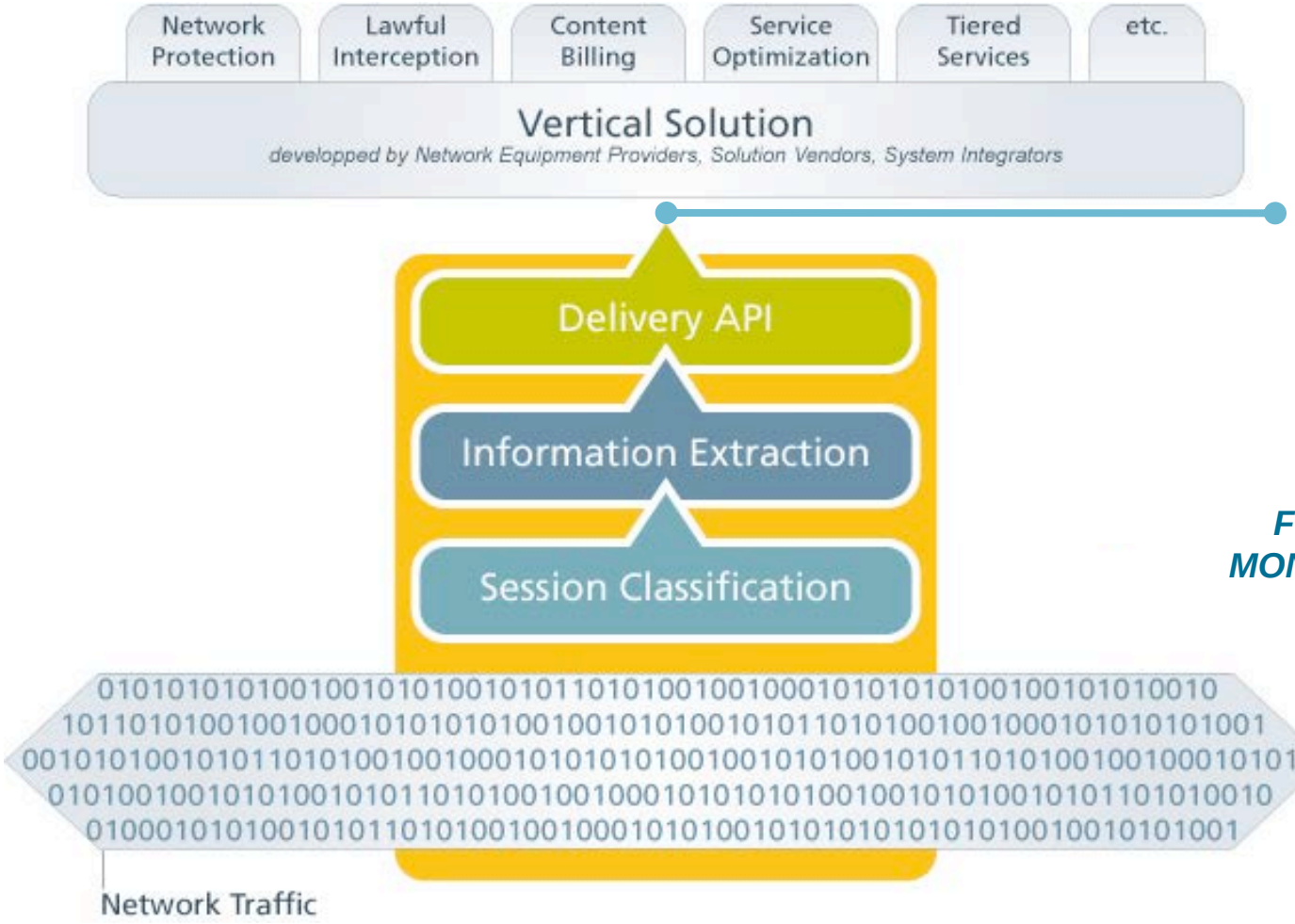
SPECIAL OFFER: Get your free evaluation of ixEngine at the Qosmos booth!

QOSMOS

Your Network is Information



Network Intelligence: Making Sense out of Network Traffic



Structured Network Intelligence

For use in PROTECTION, MONETIZING and OPTIMIZING solutions

Qosmos Product Portfolio

QOSMOS ixEngine

Information eXtraction Engine
(Software Libraries)

ixEngine

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

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
(Appliances)

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)

- ixMOS 10 / 100 / 1 000 / 10 000