The background is an aerial photograph of a city street grid, overlaid with a blue grid pattern. A red crosshair is centered on the page, with a red circle highlighting a building at the intersection. A green crosshair is also present, with a green circle highlighting a building in the lower right quadrant.

# Today's challenges in Lawful Interception

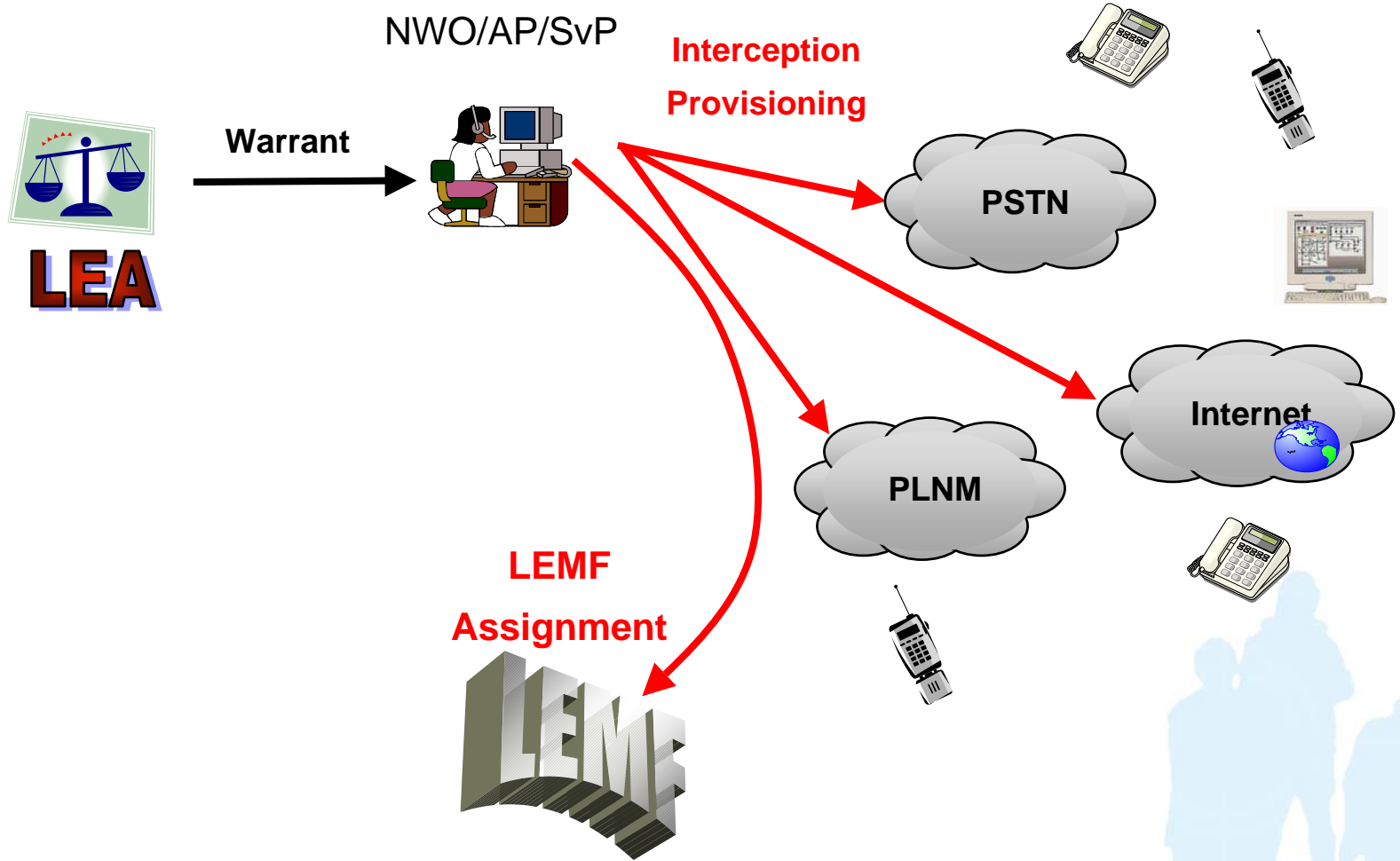
C. Rogialli, October 11<sup>o</sup>, 2005  
RIPE MEETING 51 - Amsterdam

# Lawful Interception – a Definition

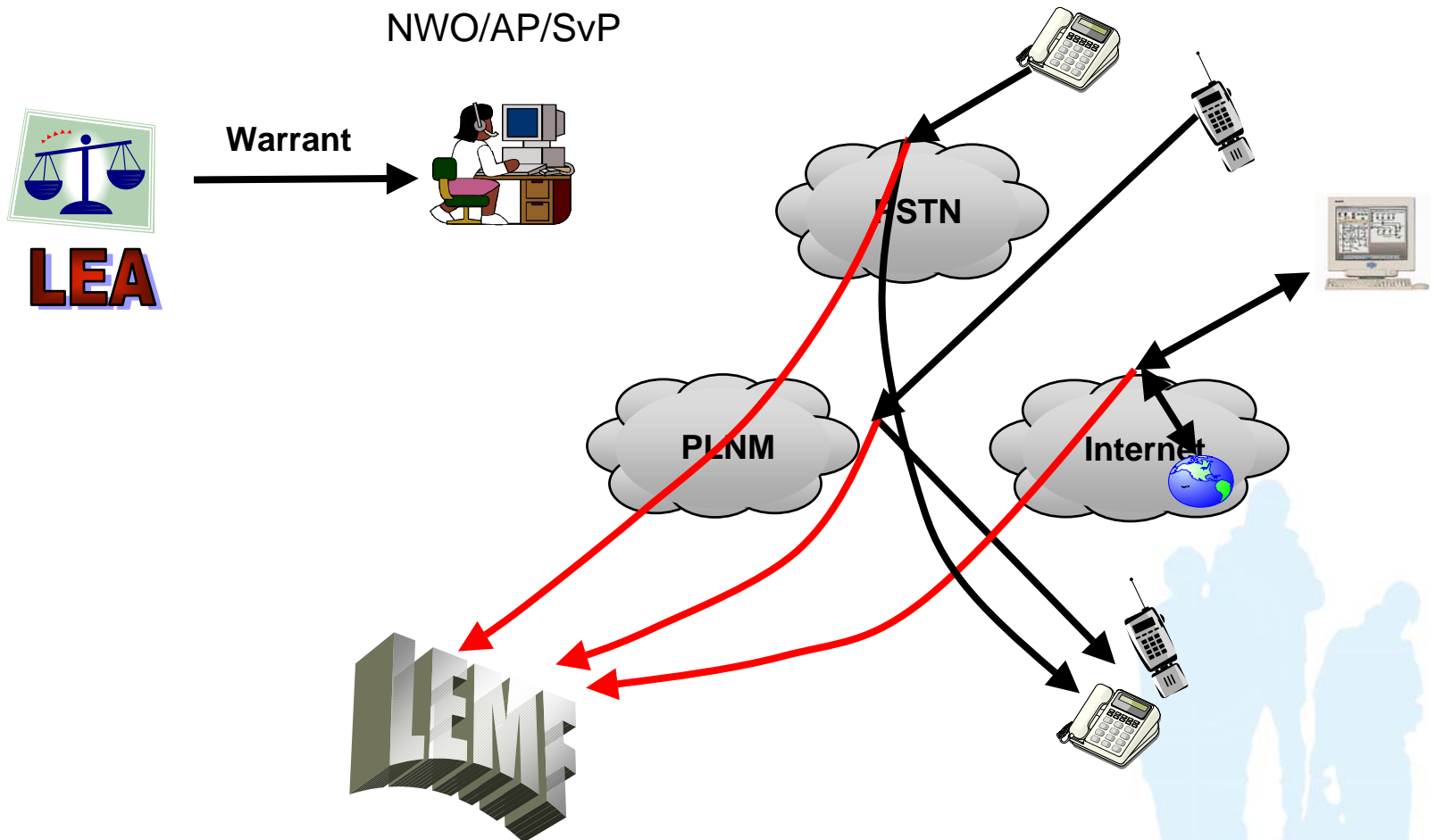
- ❖ Action (based on the law) *performed* by a network operator / access provider / service provider (NWO/AP/SvP), of making available certain information and providing that information to a law enforcement monitoring facility for investigation purposes.



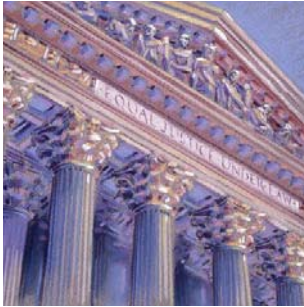
# Lawful Interception concept (1)



# Lawful Interception concept (2)

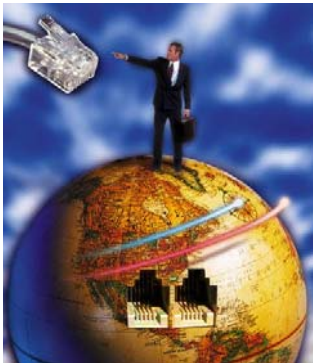


# Entities involved in Lawful Interception



## ❖ Government

- Operates in the interests of the nation;
- Sets the regulatory framework in which Lawful Interception is performed;
- Defines economical parameters for Lawful Interception activities.



## ❖ Operators

- Lawfully operate for the sake of their business and profit, almost totally driven by telecommunications;
- Withstand rules set by the government in terms of lawful interception as an unavoidable;
- Install proper devices to fulfil the relevant obligations;



## ❖ Law Enforcement Agencies

- Operate in the name of crime fighting and nation security;
- Request lawful interception and define the real targets;
- Receive the communication data extracted by the operators;
- Need proper devices to playback and decode the intercepted traffic.

# A triviality...

**TE**lecom **Co**mpanies and **Go**vernment agencies  
are **NOT** created equal !

❖ They **have**:

- Different Purposes
- Different Structure
- Different Knowledge
- Different Liabilities
- Different Activities
- Different Constraints

❖ So they **need**:

- Different Systems
- Different Approaches



# Different Key Values

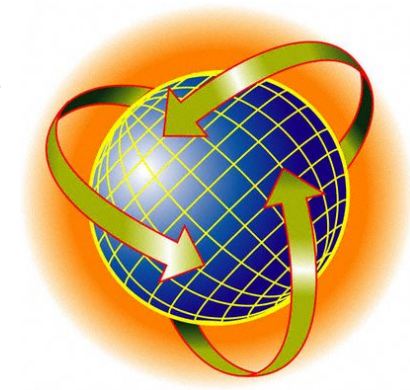
## ❖ For the government Agencies

- Overall solution effectiveness
- Return on investment (in investigative terms !)
- Adherence to existing operating procedures
- Low level of the technicalities to be handled
- “Surgical precision”

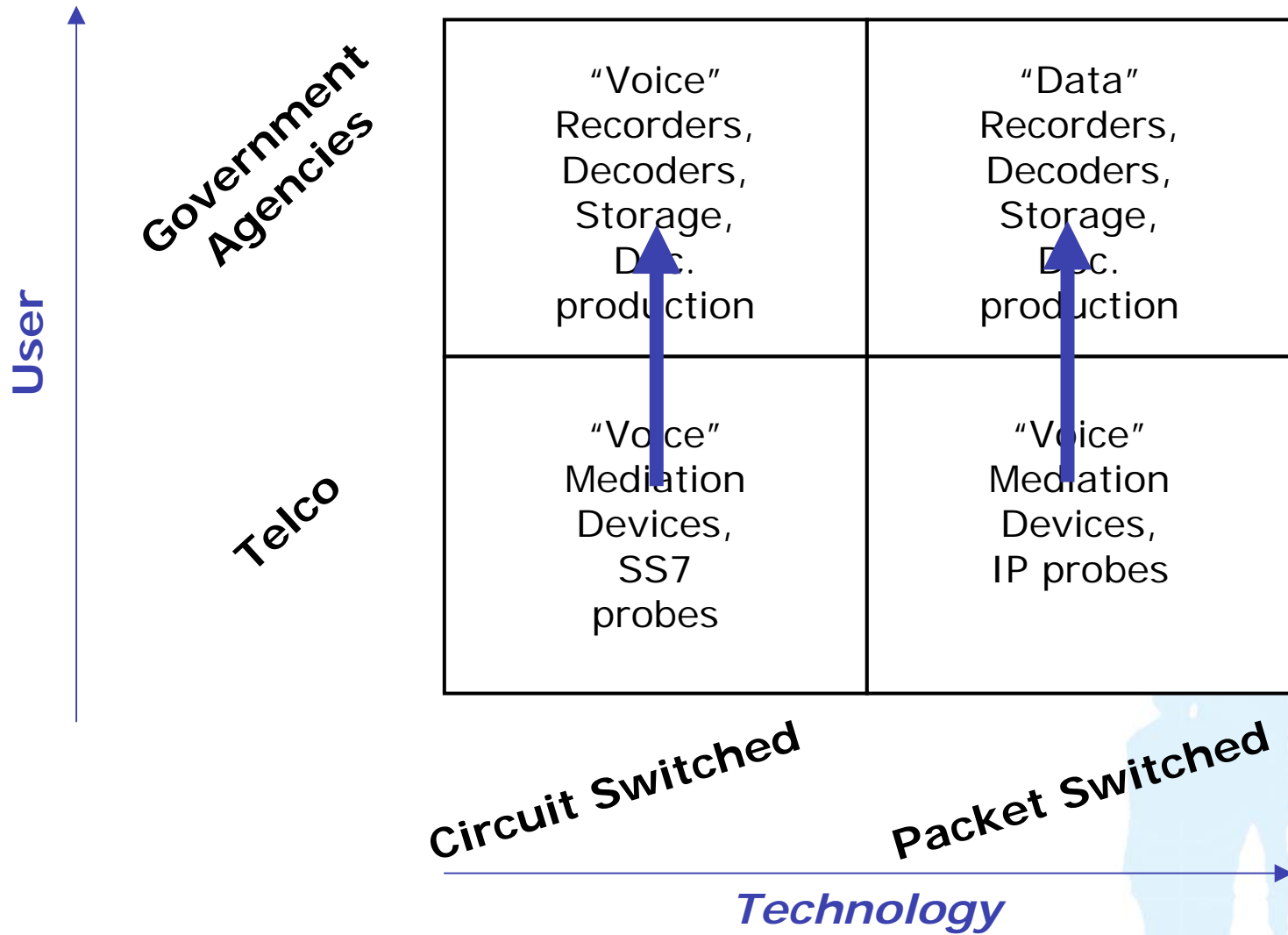


## ❖ For the Telecom operators

- Reliability
- Reduced maintenance and management hassles
- Low installation and running expenses
- Integration with the existing network
- Use of proven COTS hardware
- Possibility to document the obligation fulfilment



# Lawful Interception Application fields



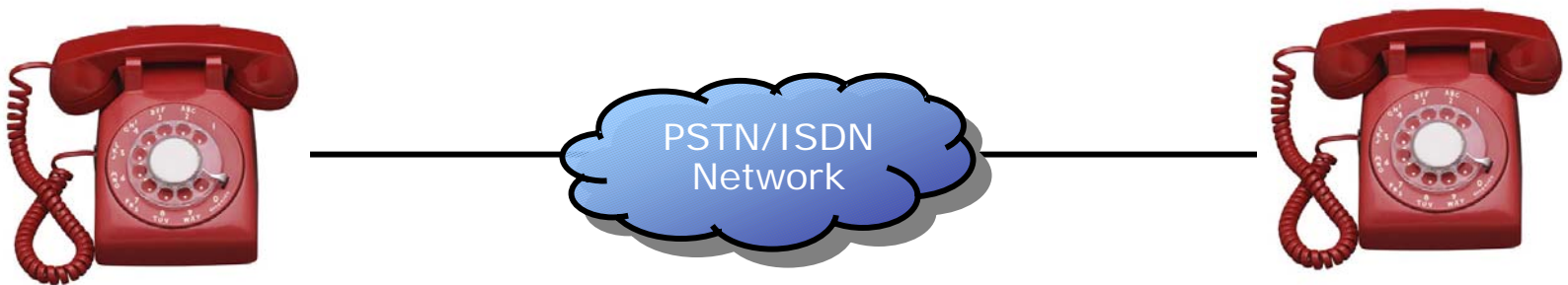
# LI in Circuit Switched and Packet Switched Networks



(that is, why do we face different issues in the two worlds)

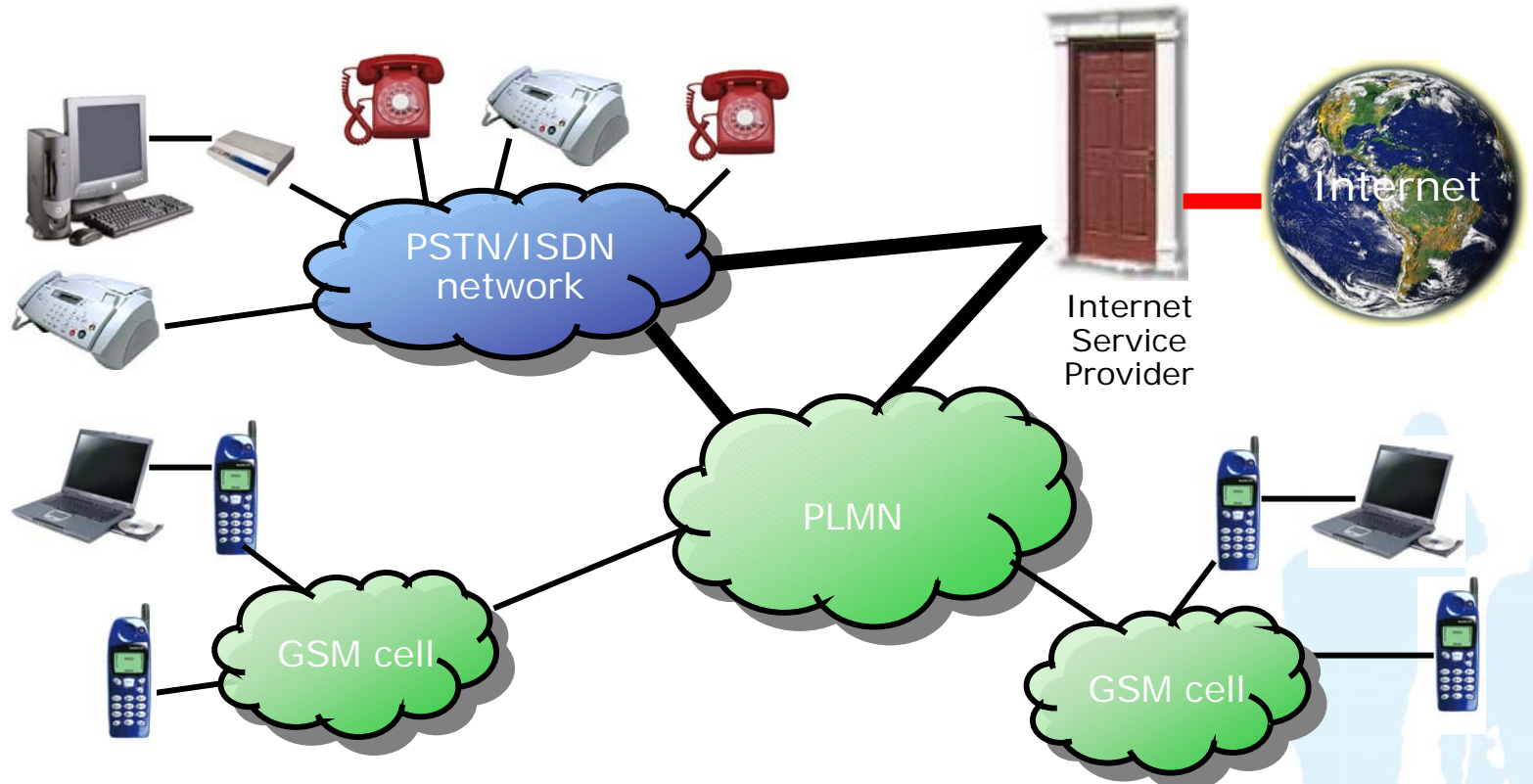
# Once upon a time ...

- ... the mass telecommunications were only bound to the fixed PSTN network;
  - no additional functionalities were provided by the handsets;
  - the transport Network was unique in type and technology, it was based upon Circuit Switching, and the only type of payload transported was VOICE.
- ❖ In this *“fairy tales”* world, the interception:
- operated over a single network, with good-to-excellent results;
  - had to deal with a single type of payload (typically ISDN voice over 64 kbps);
  - due to the circuit switching technology, may e operated in any point of the network between the end points.



## ...then it was the turn of fax, modems and mobiles

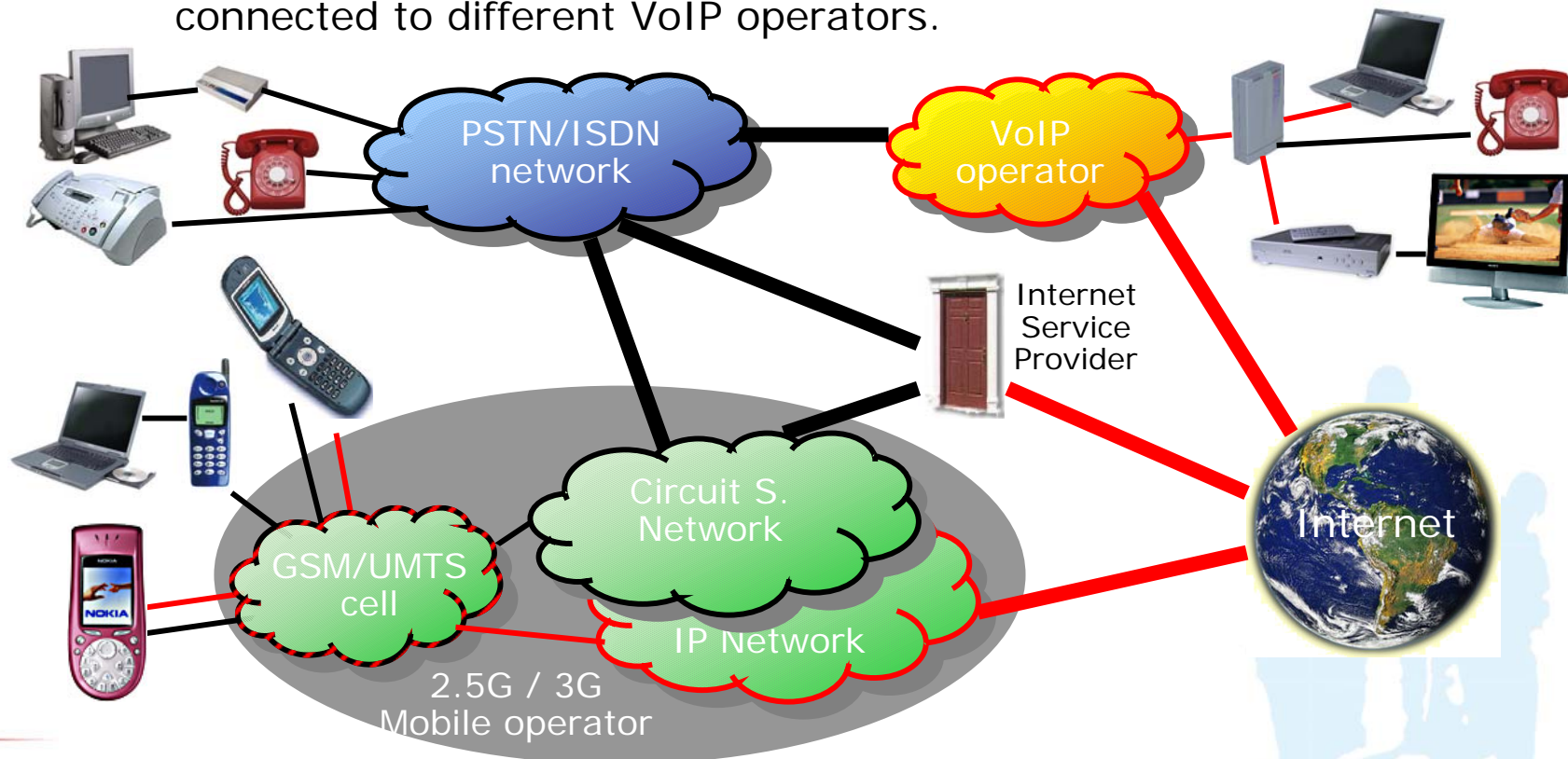
- ❖ Fax and Modems still use analog modulation over the CS network in order to transport images, data and internet services.
- ❖ The mass interception was therefore still possible with CS methodologies, with the only complication of demodulation.



## ...and, suddenly, the security **nightmare** !!!

A lot of mass telecommunication traffic today doesn't traverse ANY part of the well-controlled Circuit Switched network !

- ✓ IP multimedia traffic between GPRS/UMTS mobile phones;
- ✓ the traffic to and from Internet exchanged on high bandwidth ISPs (ADSL, FTTH, cable...);
- ✓ Telephone traffic between two REAL VoIP terminals, maybe connected to different VoIP operators.



# Lawful interception compulsory services

- ❖ Depending on the local legislation, the Operator may be requested to provide:
  - Interception based upon target identity
    - ❑ It is requested to replicate ALL the traffic generated by a single, identifiable target among the multitude of users of the Operator itself.
  - Investigative interception based upon parametric search
    - ❑ It is requested massive filtering of the transported traffic in order to spot UNKNOWN users showing suspect behaviours (in example, exchanging mails containing specific keywords).
  - Interception over Telecom operator's services
    - ❑ It is requested to replicate IN CLEAR any transaction made by an user towards a Service exercised by the telecom .
  - Free access to the network
    - ❑ It is requested to guarantee proper network access to "black boxes" owned by the law enforcement agencies themselves.

# New issues connected with IP interception

## ❖ User Identification

- Whilst the correspondence between user credentials and user identity is rarely questioned in the “Voice” world, this is not necessarily true for the IP networks;

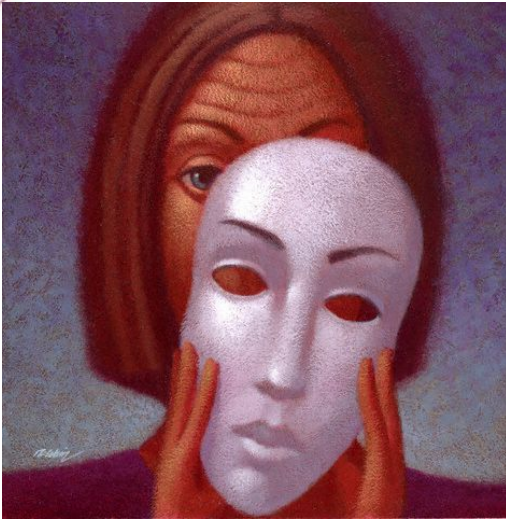
## ❖ Traffic dispersion

- The packet switching world poses new issues in terms of tapping points and capture efficiency;

## ❖ Mass cryptography

- In the IP world, cryptography is extensively used and at hand of everybody....

# User Identification Issues



❖ Availability of reliable user information

- No more anonymous access to the network will be provided by world's telecom operators;

❖ Trusted identity systems

- Any mean shall be used to guarantee the correlation between user's credentials and the physical person accessing the network;

❖ Availability of the user parameters at the capture point

- Any network feature hiding user's identity at the capture point (e.g. NAT) shall be taken into account and suitable workarounds for the authority shall be provided.



# Traffic dispersion issues

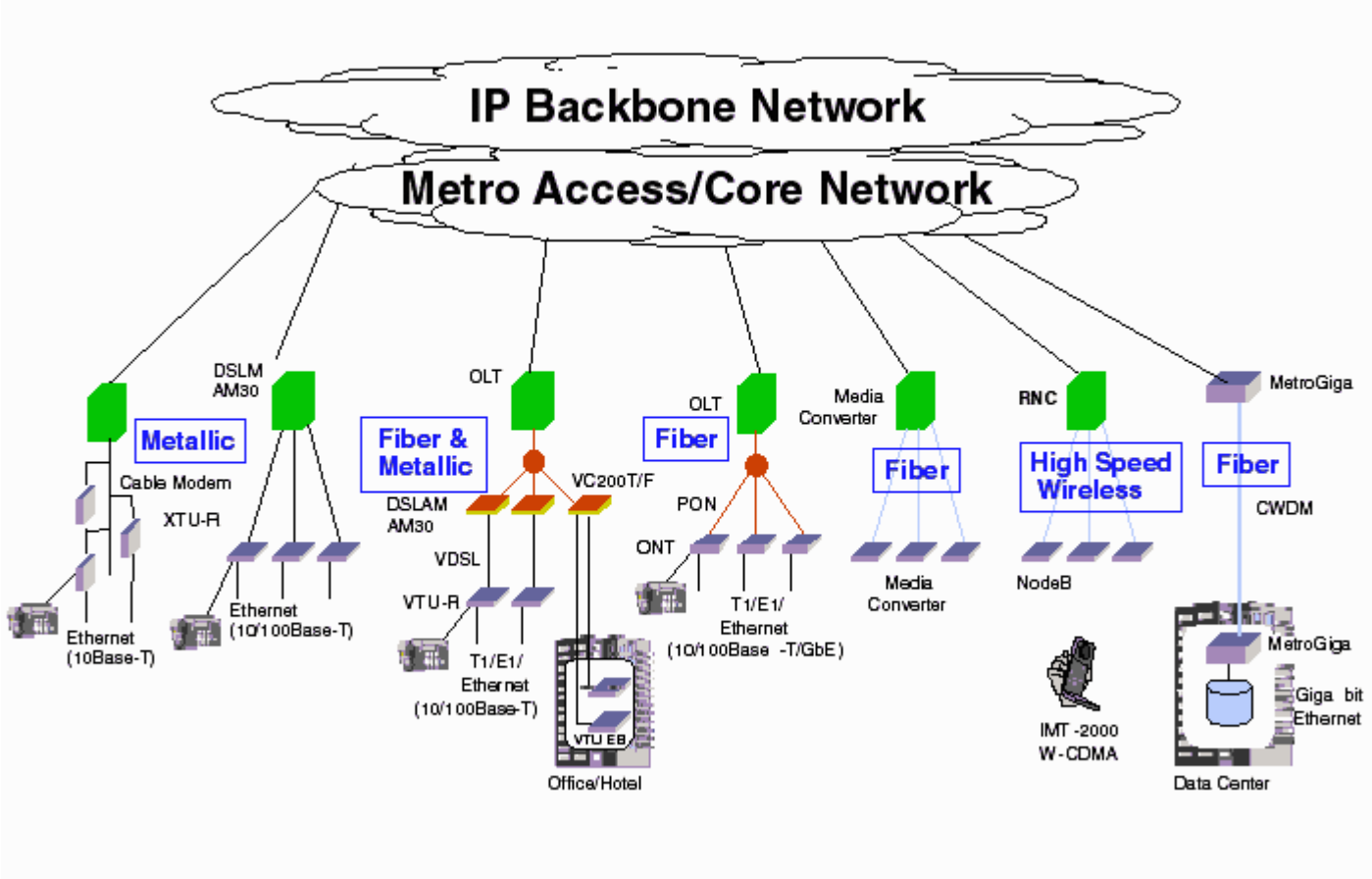


- ❖ Arpanet was originally conceived in order to deploy a military network able to survive huge, nation-level disasters...

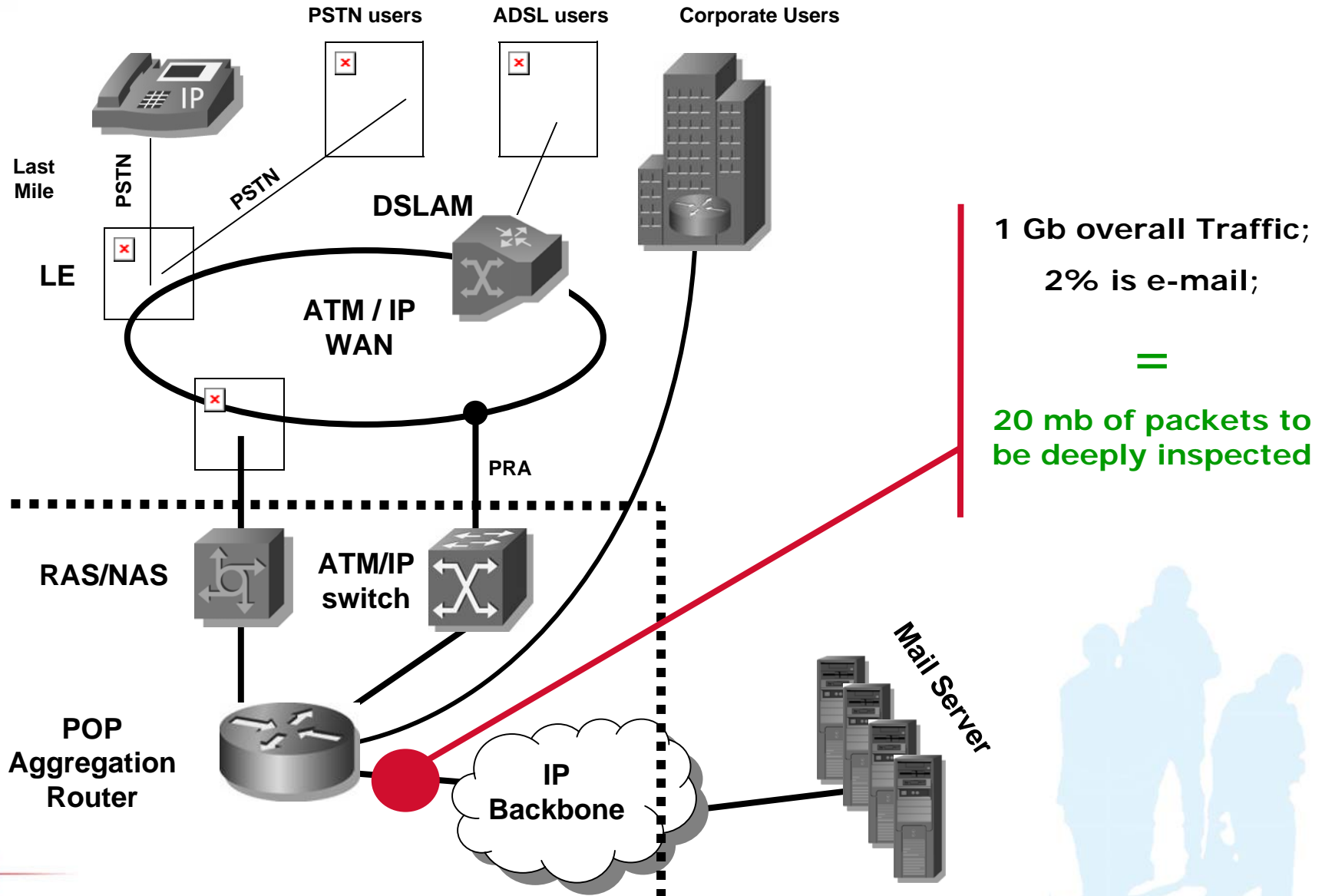


- ❖ As a result, IP routing follows BY DESIGN several different routes even towards the same target address.
- ❖ As a consequence, the tapping point is not at all indifferent to the Lawful Interception Activities!

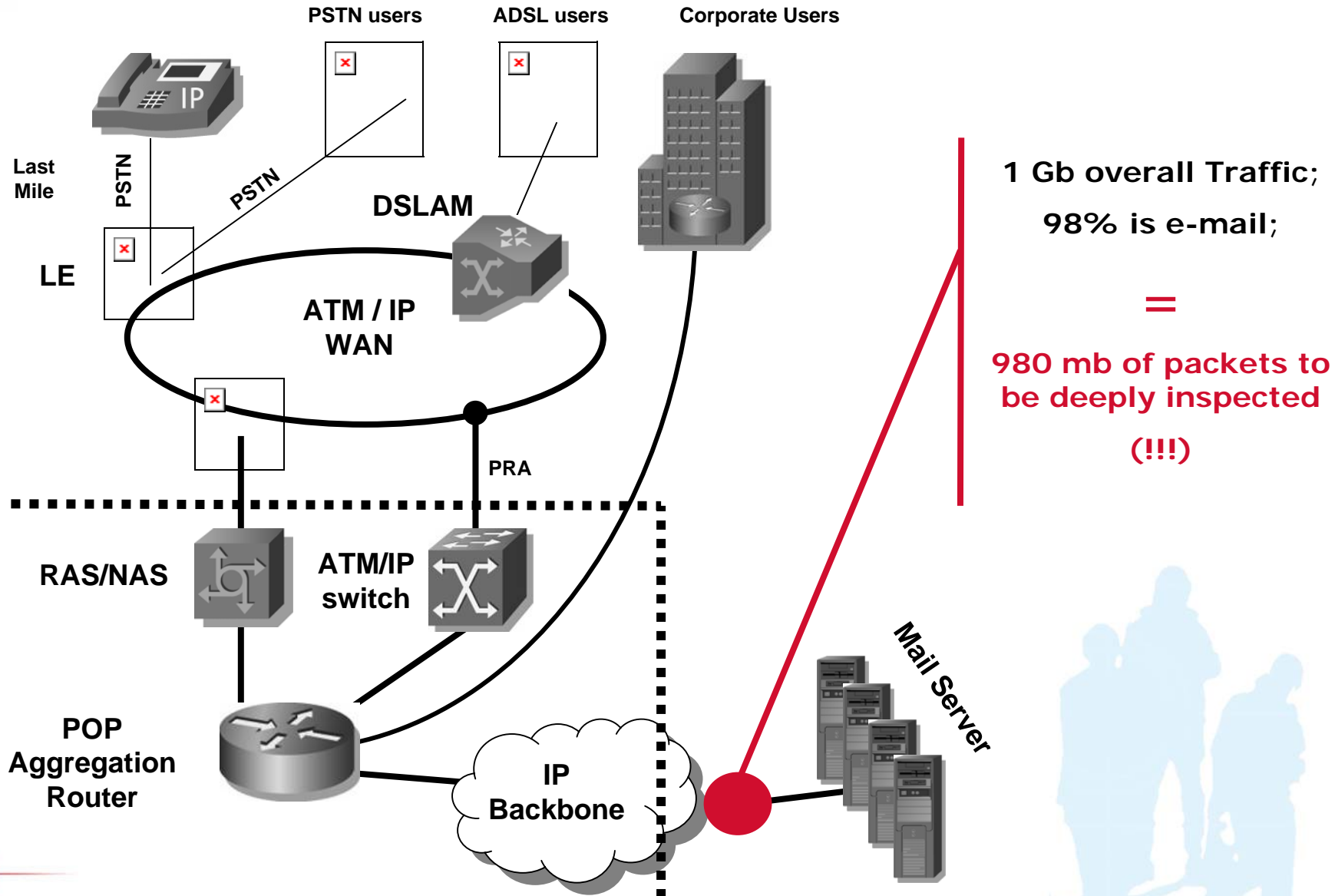
# Tappin' around the net



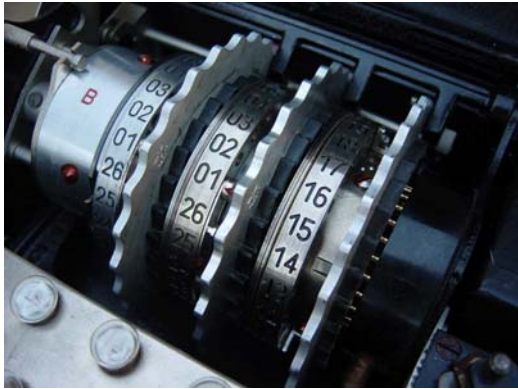
# E-mail Probing in the access network



# E-mail Probing in the Central Office



# Mass Cryptography issues



❖ Over the PSTN network, communication encryption was at disposal of few users; moreover, the few devices available offered backdoors for the agencies;

❖ Over the internet, encryption is at disposal of **EVERYBODY**. Not in any case backdoors are available;

❖ Whilst the operator may not be held responsible for user-level encryption, it may as well be obliged to provide in-clear interception of the services offered by itself.



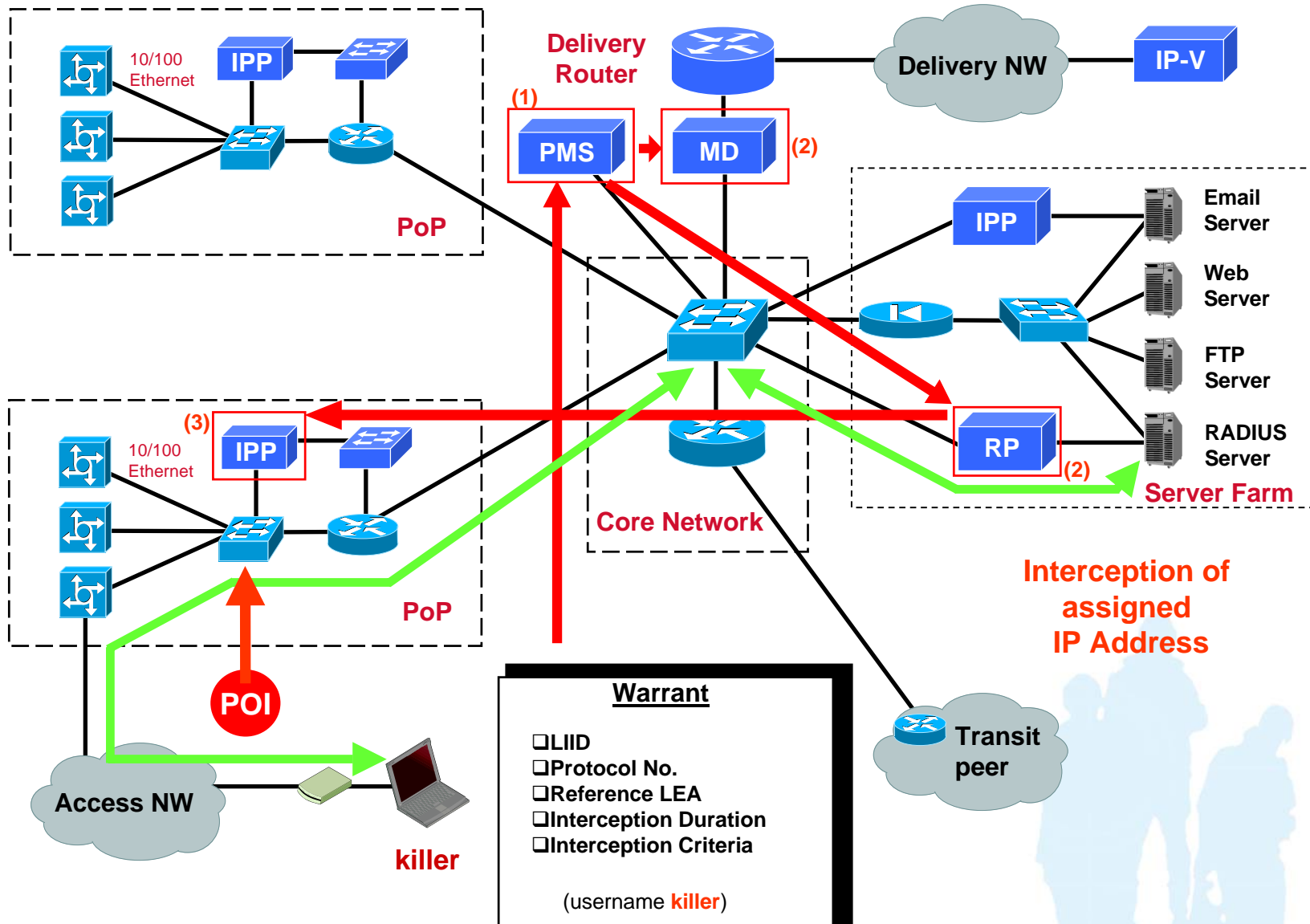
# The ISP in front of the authority. Viable options for the IP LI.



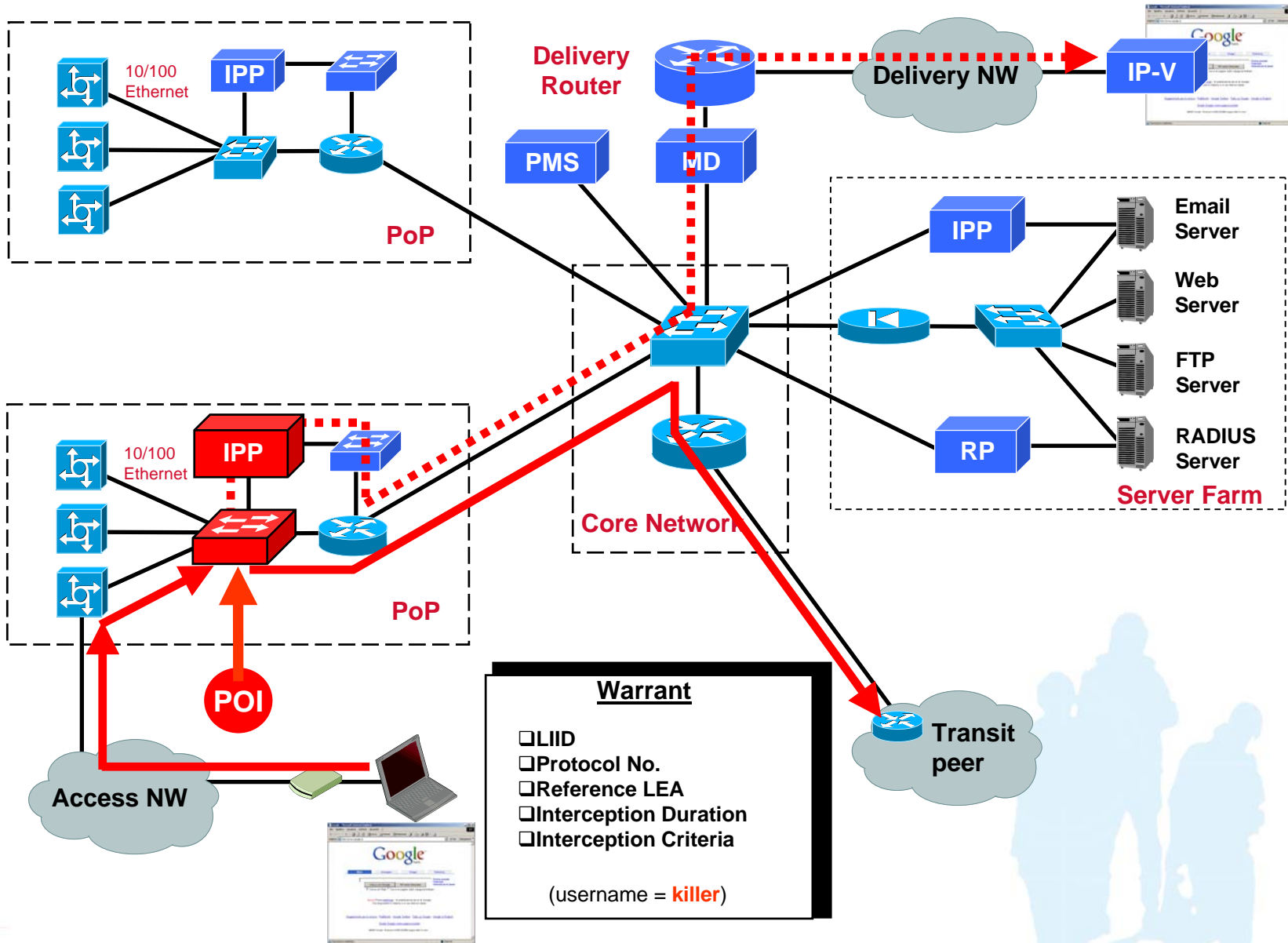
# In-Band and Out-Band interception

- ❖ In-band interception implies the use of IIF implemented in the network devices; it can be successfully used with any kind of interception based upon user identity:
  - Circuit based traffic;
  - Packet traffic over mobile networks (es. GPRS);
  - Packet traffic over carrier-grade modern switches in ISPs.
  
- ❖ Out-band interception implies the use of network probes; it is the only key when:
  - Parametric (keyword) interception is requested;
  - The authority doesn't trust the operator itself or the operator's personnel in investigative matters.

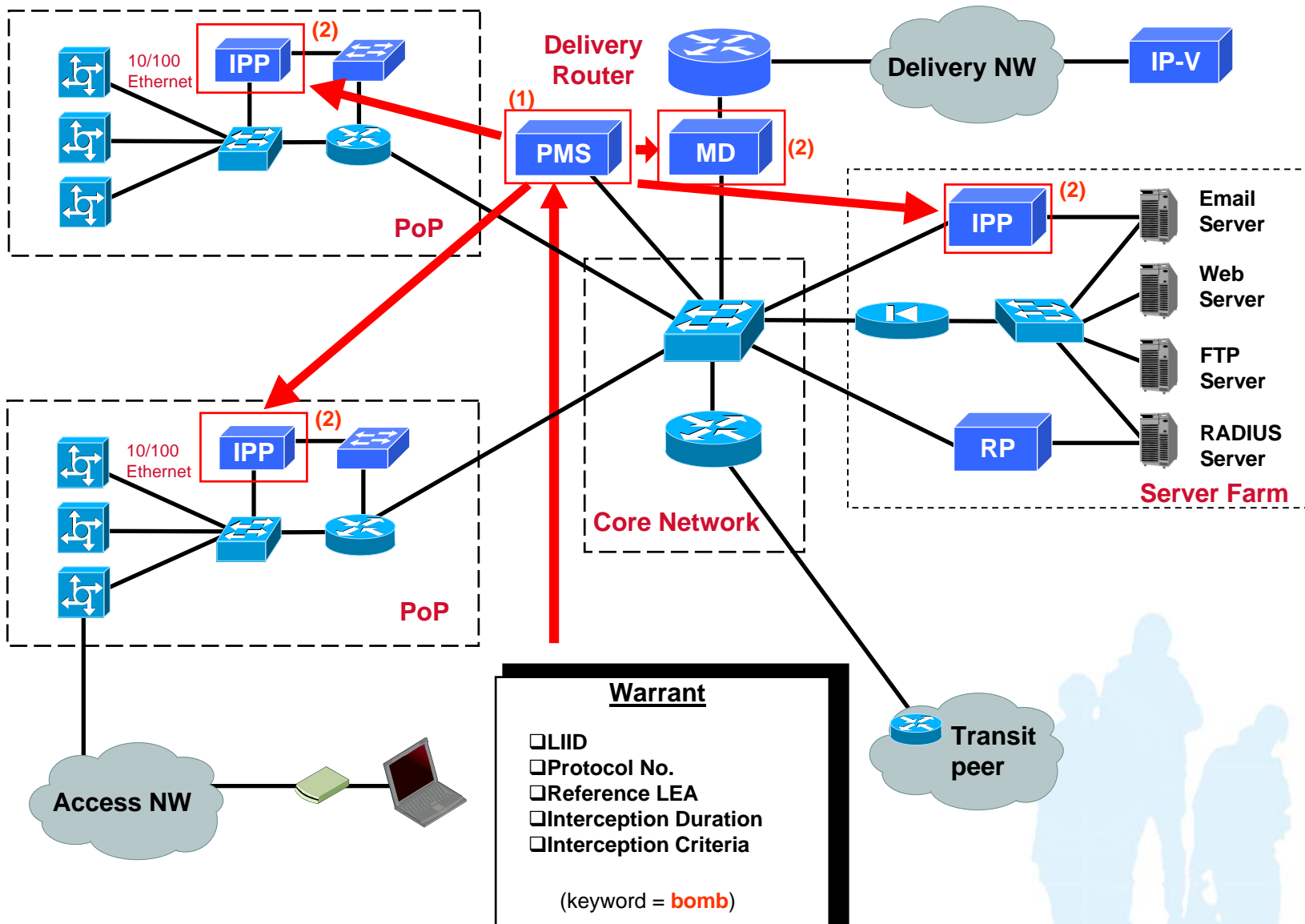
# Typical Out-band Interception



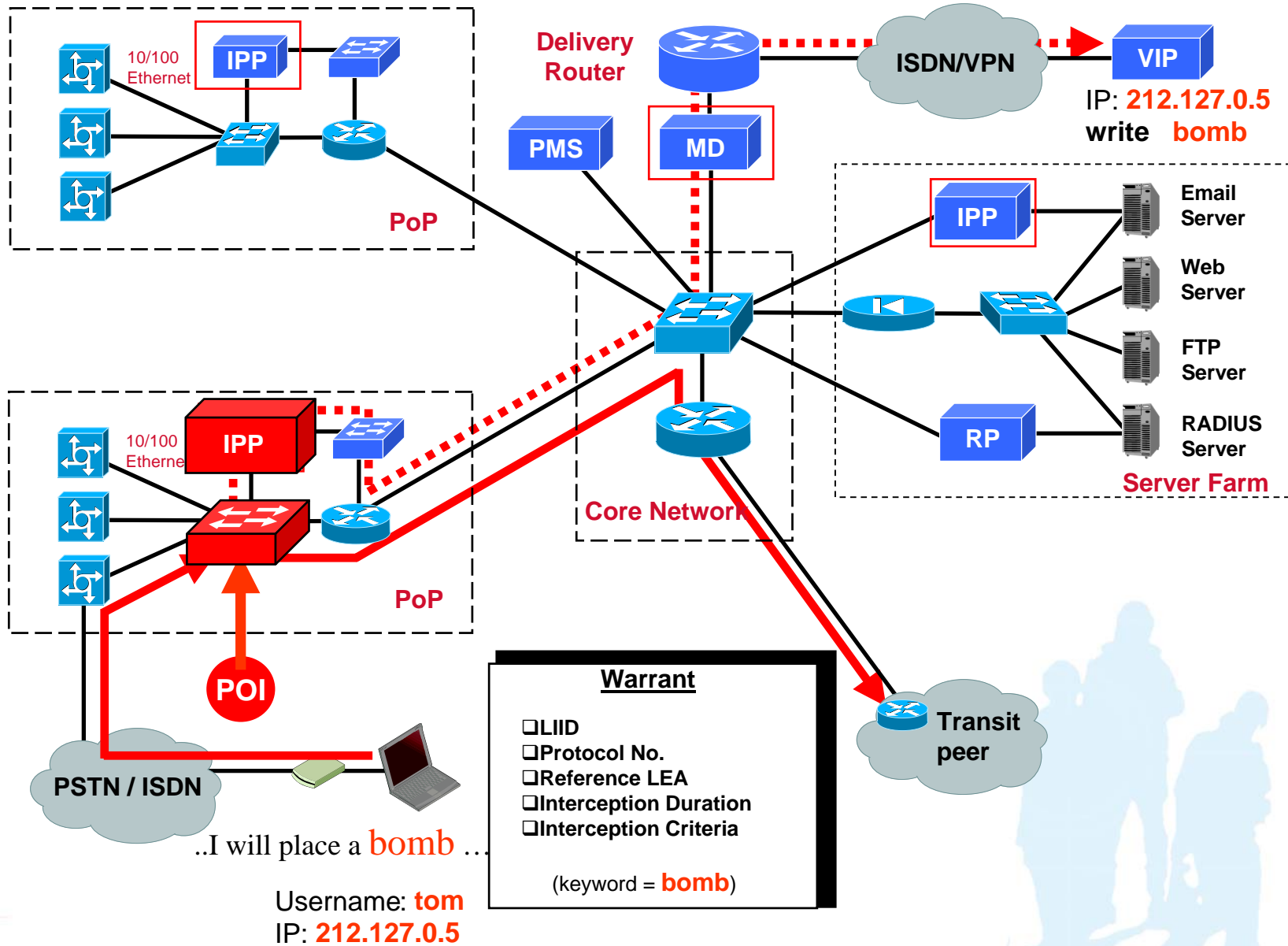
# Typical Out-band Interception



# Parametric Out-band Interception



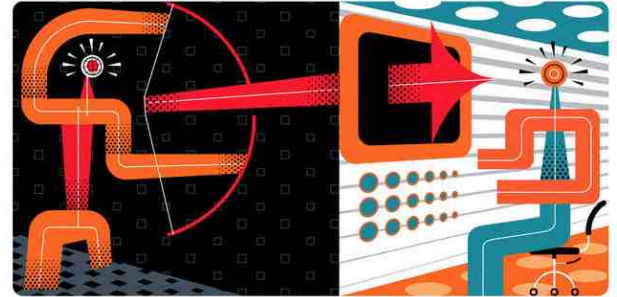
# Parametric Interception (Interception)



# Tactical probing vs. strategic interception (1)

## ❖ Tactical probes – a definition:

- devices that are installed at operator's premises on a "per need" basis.



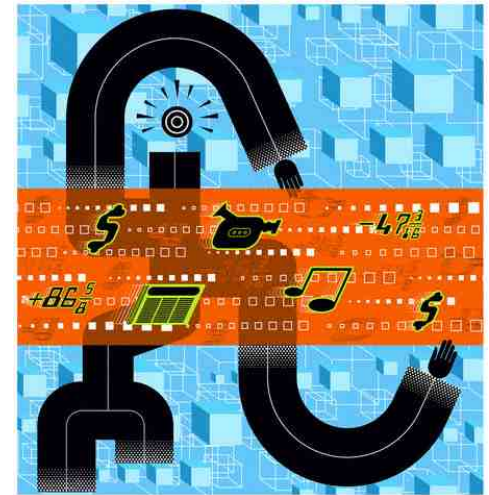
## ❖ Some "common sense" assertions about Tactical probing devices:

- small
- stealthy
- easily movable
- typically operated by agencies personnel
- dedicated to a few specific interception tasks at a time
- totally extraneous respect to the hosting network by definition



# Tactical probing vs. strategic interception (2)

- ❖ Strategic Interception – a definition:
  - An interception network permanently deployed at operator's premises to serve any present or future interception request.
  
- ❖ Some "common sense" assertions about Strategic probing devices:
  - solid
  - integrated
  - permanently connected to the network
  - typically maintained by telco personnel
  - dedicated to a **huge** spread of interception tasks at a time
  - may be integrated with the hosting network



# A duofold option for the ISP

1. Open the door to Agencies for Tactical Activities
  - ✓ as a pro, some responsibilities and costs are charged over the Agency rather than over the operator;
  - ✓ as a drawback, the operator will need to support (eventually upon network reconfiguration) the agency's activities, **on a per need basis !**
2. Make Room for Strategic interception systems
  - ✓ The operator will face some not recurring costs, only eventually covered by the gouvernement;
  - ✓ However, the impact over the network will be minimized.

An only thing is important...

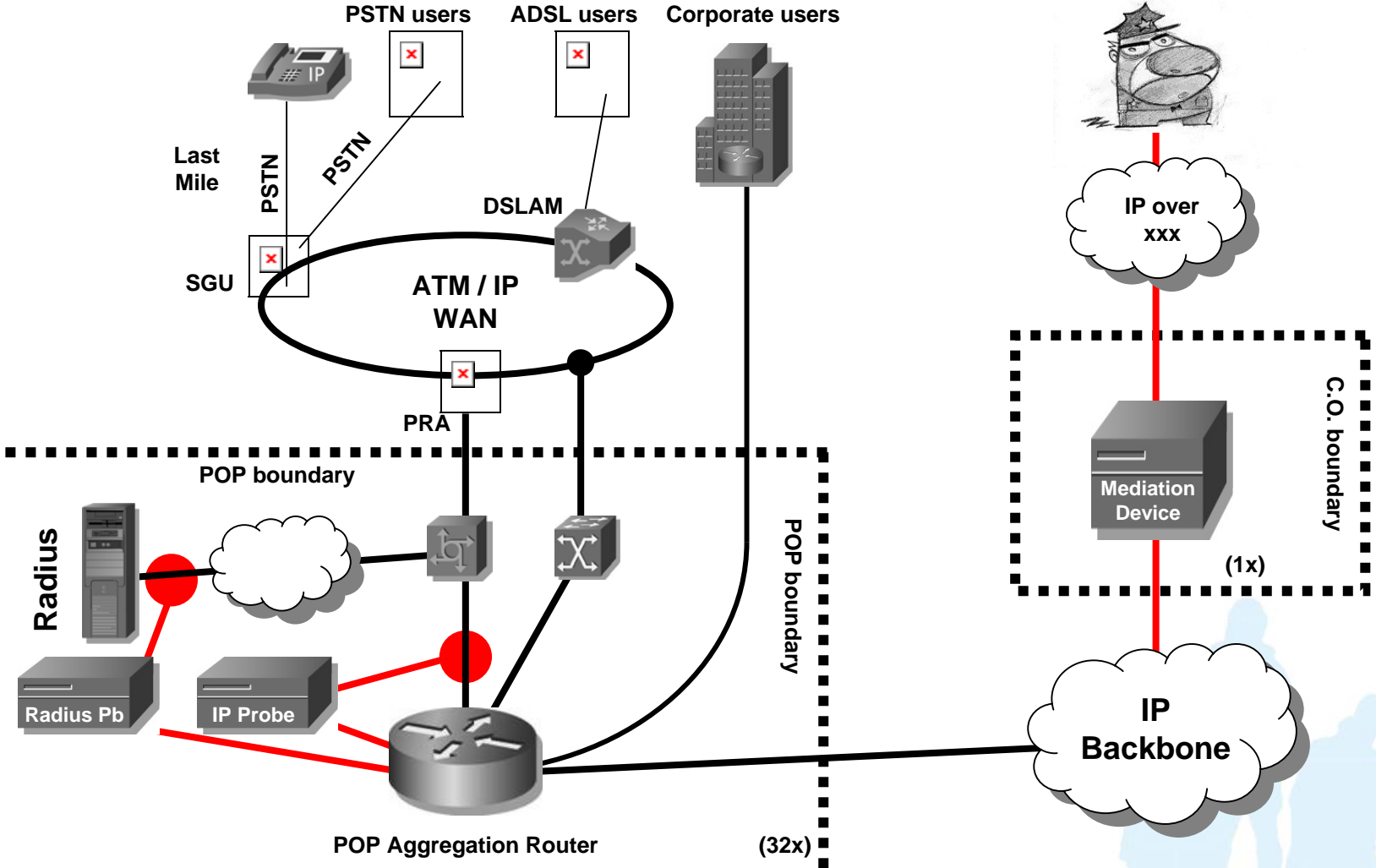
**...JUST PUT THE  
RIGHT PROBE IN  
THE RIGHT  
ENVIRONMENT !**



# A Mixed Approach to LI



# Classic approach – general principles



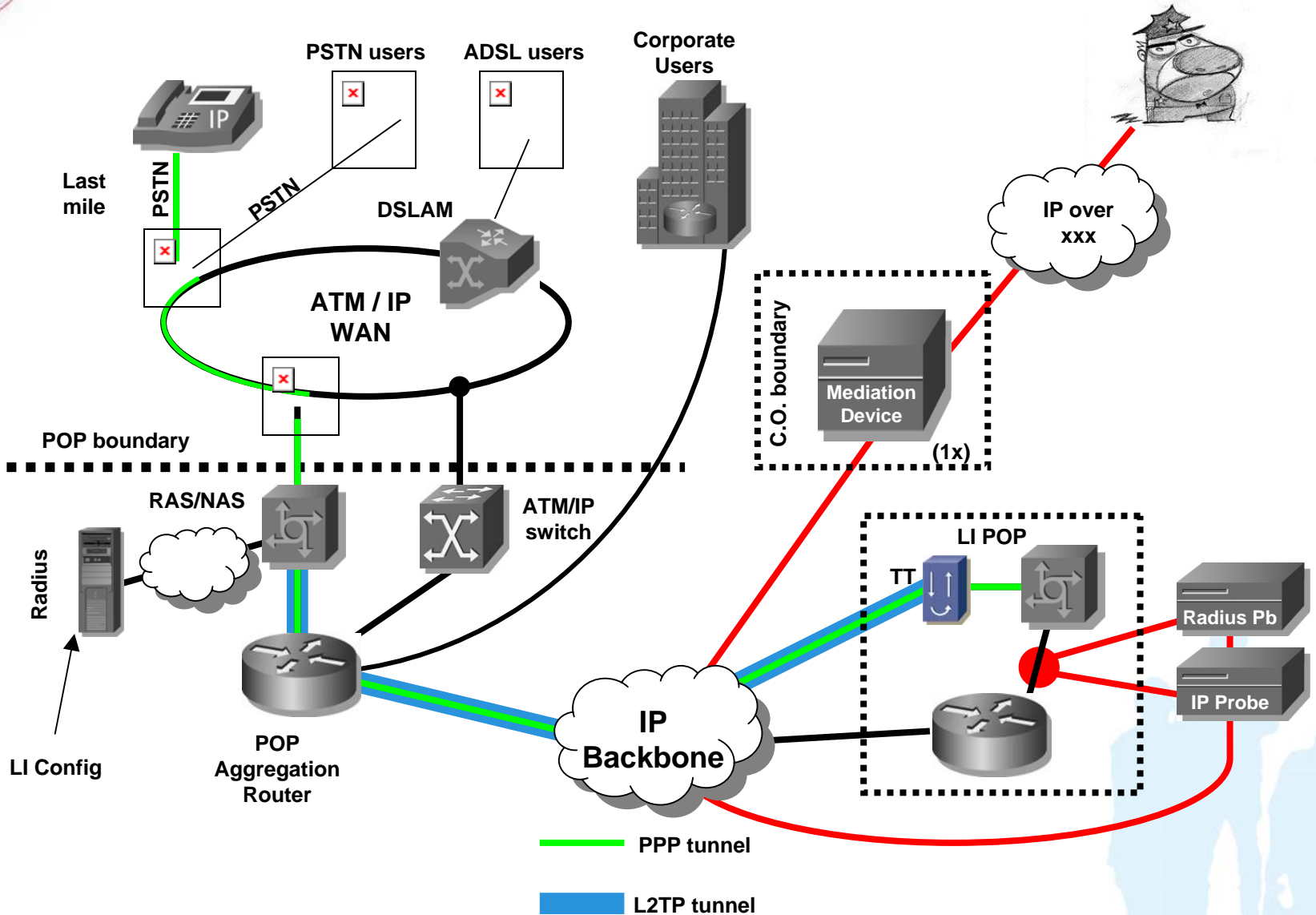
## PROs

- ❖ Extensive capture allows many forms of parametric interception (e.g. Keyword search or e-mail addresses);
- ❖ The solution is totally unobtrusive and is completely impactless on the network architecture;
- ❖ The solution functionalities may be extended to effective network traffic monitoring as an added value.

## CONS

- ❖ many probes to be placed;
- ❖ large investment needed;
- ❖ a lot of space (with access control requirements) to be reserved in the POP;
- ❖ tapping may be a NIGHTMARE, but the use of span ports may impact network performance;
- ❖ distributed and secure network connectivity between system elements to be provided;
- ❖ Some peering traffic is lost (i.e., the peering traffic closing on the same BRAS).

# Hijack approach – general principles



## PROs

- ❖ few probes to be placed;
- ❖ low investment needed;
- ❖ Few space with access control requirements may be reserved anywhere in the network;
- ❖ tapping is quite simple;
- ❖ Reduced need of secure network connectivity between system elements;
- ❖ No peering traffic is lost.

## CONS

- ❖ The possibility of parametric interception are limited;
- ❖ The solution needs a slight network re-design;
- ❖ Not suitable for extensive traffic monitoring.

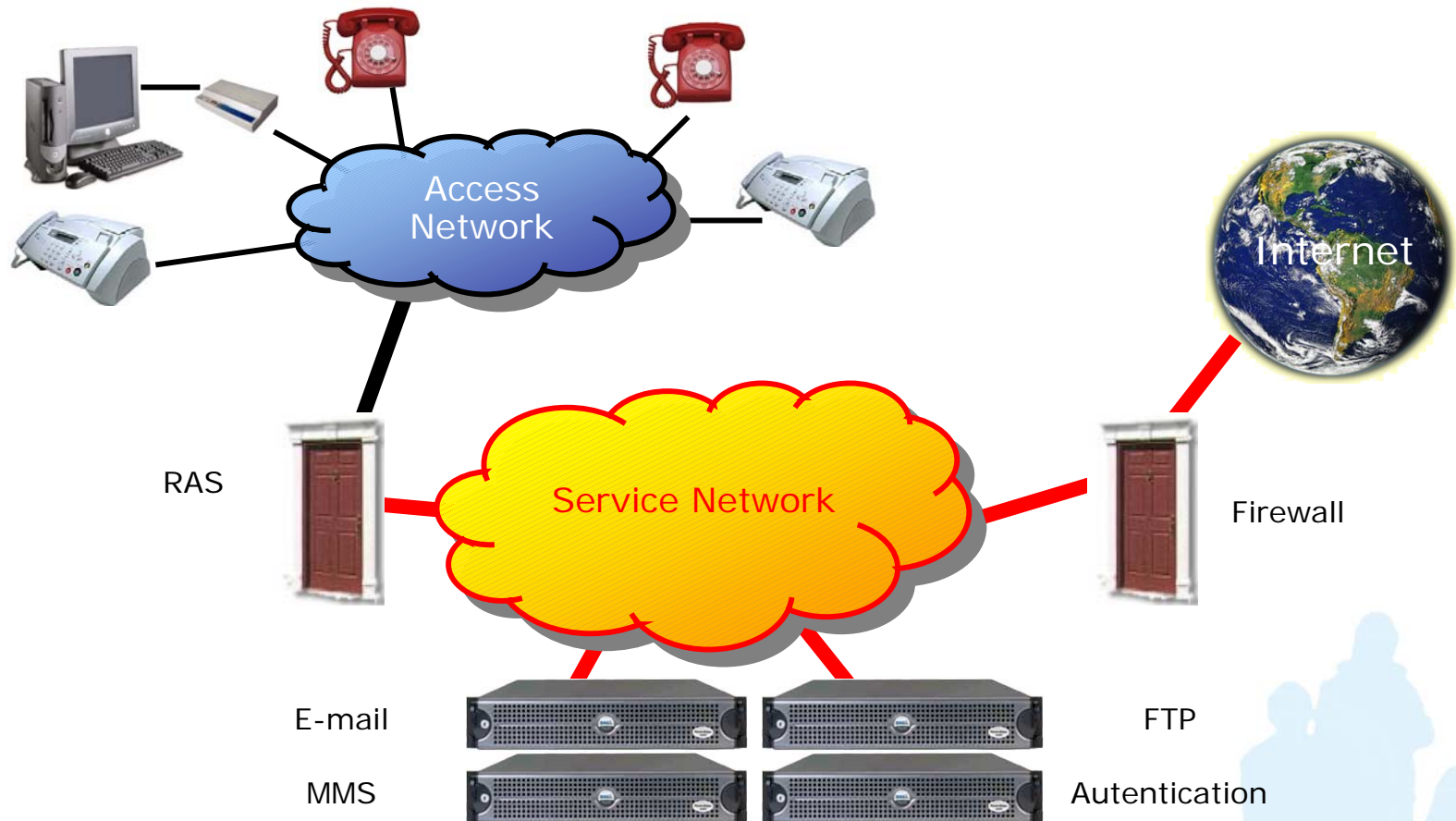
# A Service Approach to LI



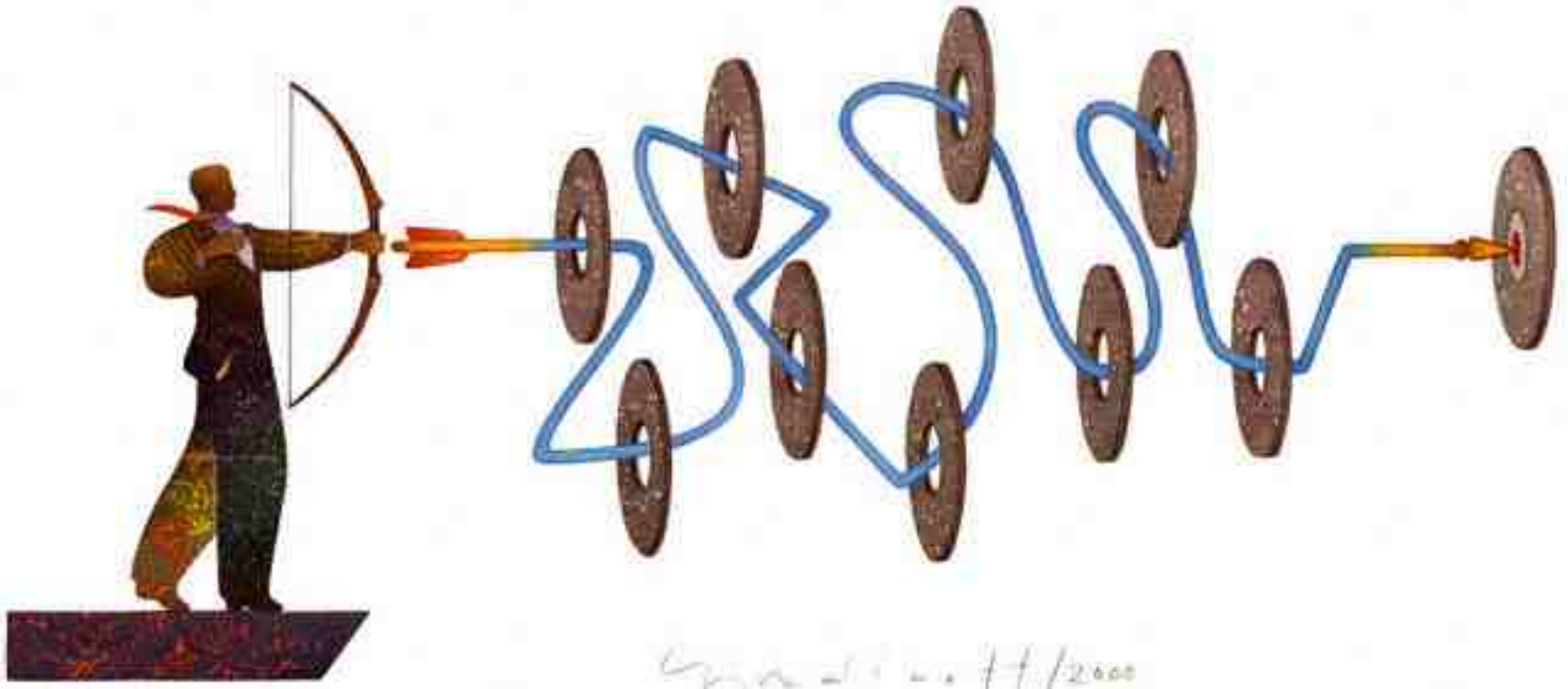
# Service interception approach

- ❖ Any time the telco operator offers some services on its own, it may be obliged to intercept them. Examples are:
  - VoIP services;
  - FTP/mail/webmail services;
  - Videocall over PSTN line;
  - ...
- ❖ In ALL those cases, the operator will be asked to get rid of any interception aspect, including traffic encryption !
- ❖ So the solution may lay in Service interception rather than transport interception.

# Service interception – an example



# LI – A flexible approach



# A flexible LI architecture is the key

- ❖ The answer to operators interception needs cannot be a “spot” solution for a specific interception issue or a specific service...
- ❖ ... but rather an extensive approach covering – at least in perspective - all interception needs at a time.

# IP Network Probing

- Different probing devices are at disposal of the Network Engineer, granting overall coverage of any IP LI needs:



- **General-purpose IP Probes:**

- IP probes performing parametric interception may be placed in front of a network server (e.g. e-mail);
  - *The interception is triggered basing upon service access, regardless the location of the network site accessing the "batch" service.*
- IP probes performing typical interception may be used to capture generic IP transactions basing upon IP address, CLI, or keyword;
  - *A specific access probe may be needed to trigger the interception;*

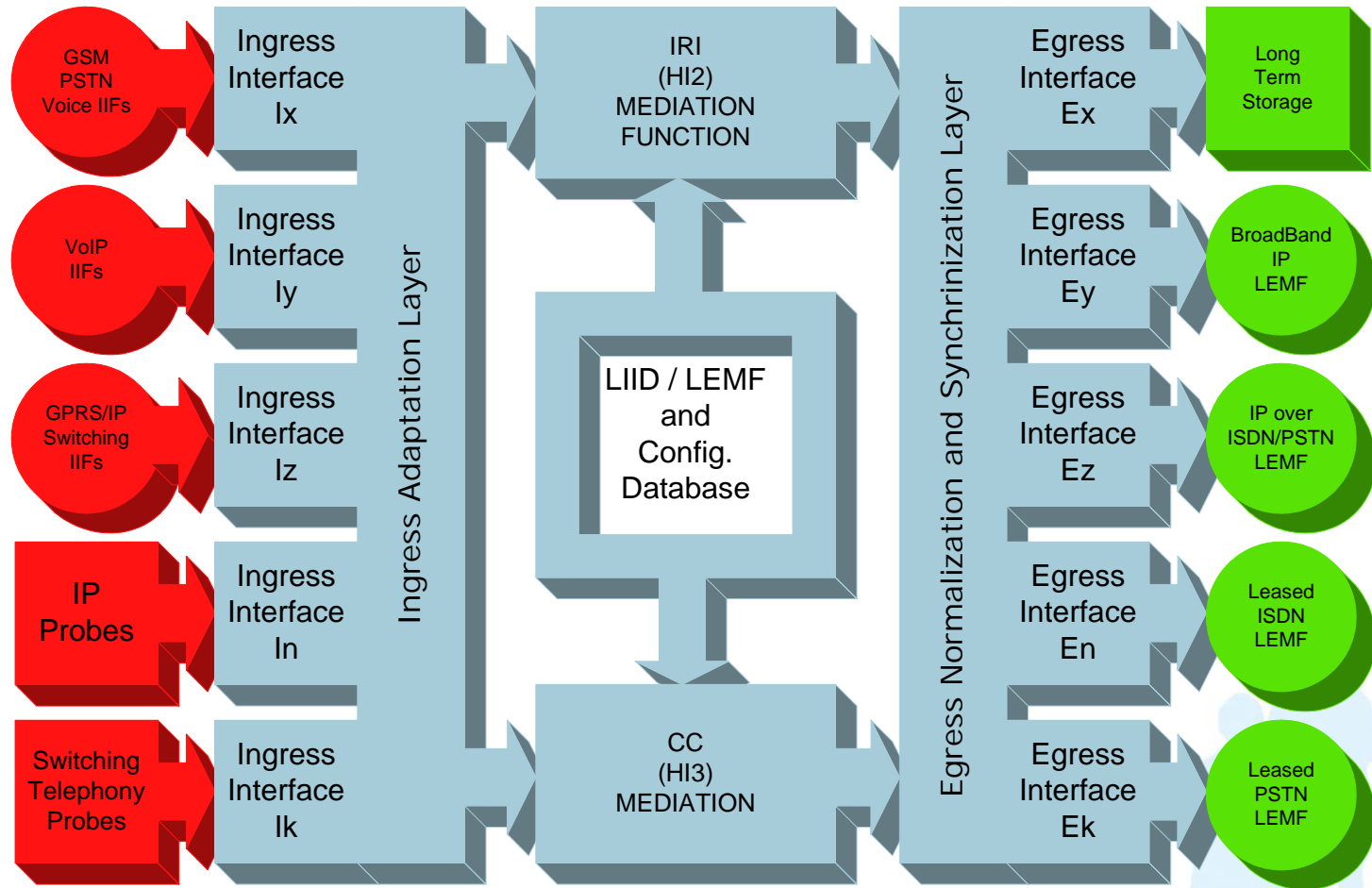
- **Access (RADIUS) Probes:**

- access probes are able to detect a "known" user accessing the network;
- they provide trigger to IP probes as well as access logging capabilities.

# Mediation Device

- ❖ It is the central server performing LI information handover from the provider's domain to the LEA's domain.
- ❖ It allows for a simpler and centralised LI network management, whilst optimising network resources usage.
- ❖ It grants a superior level of control in IP LI activities.
- ❖ It may be extended to support further capture methodologies, both out-band and in-band.

# Mediation Device flexible architecture



# Provisioning and Maintenance System

- ❖ It is the central configuration device for the entire LI network.
  
- ❖ It allows the operation of the LI system using minimum personnel.
  
- ❖ By supporting different privilege levels, it is the “natural” Man-Machine Interface for:
  - Maintenance Operators (alarms and devices mgmt);
  - LEA Operators (Warrants mgmt);
  - Billing Opertors (where applicable).

# THANK YOU

For any further info:

Carlo Rogialli

[carlo.rogialli@rcslab.it](mailto:carlo.rogialli@rcslab.it)

TECHNOLOGY FOR A SAFER WORLD

