Real Time Traffic Analysis.

PROTEI

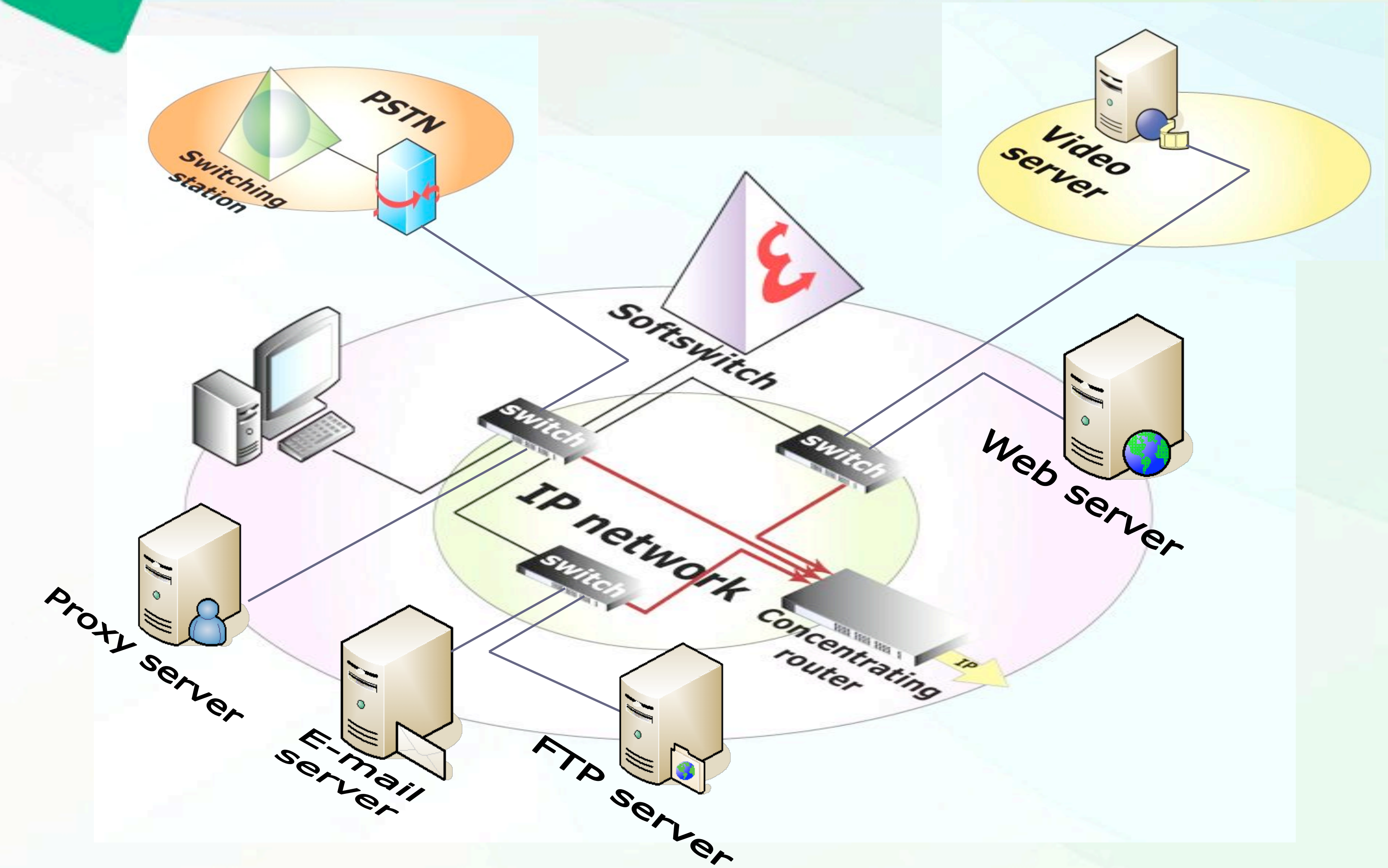
2008

Multiservice Networks

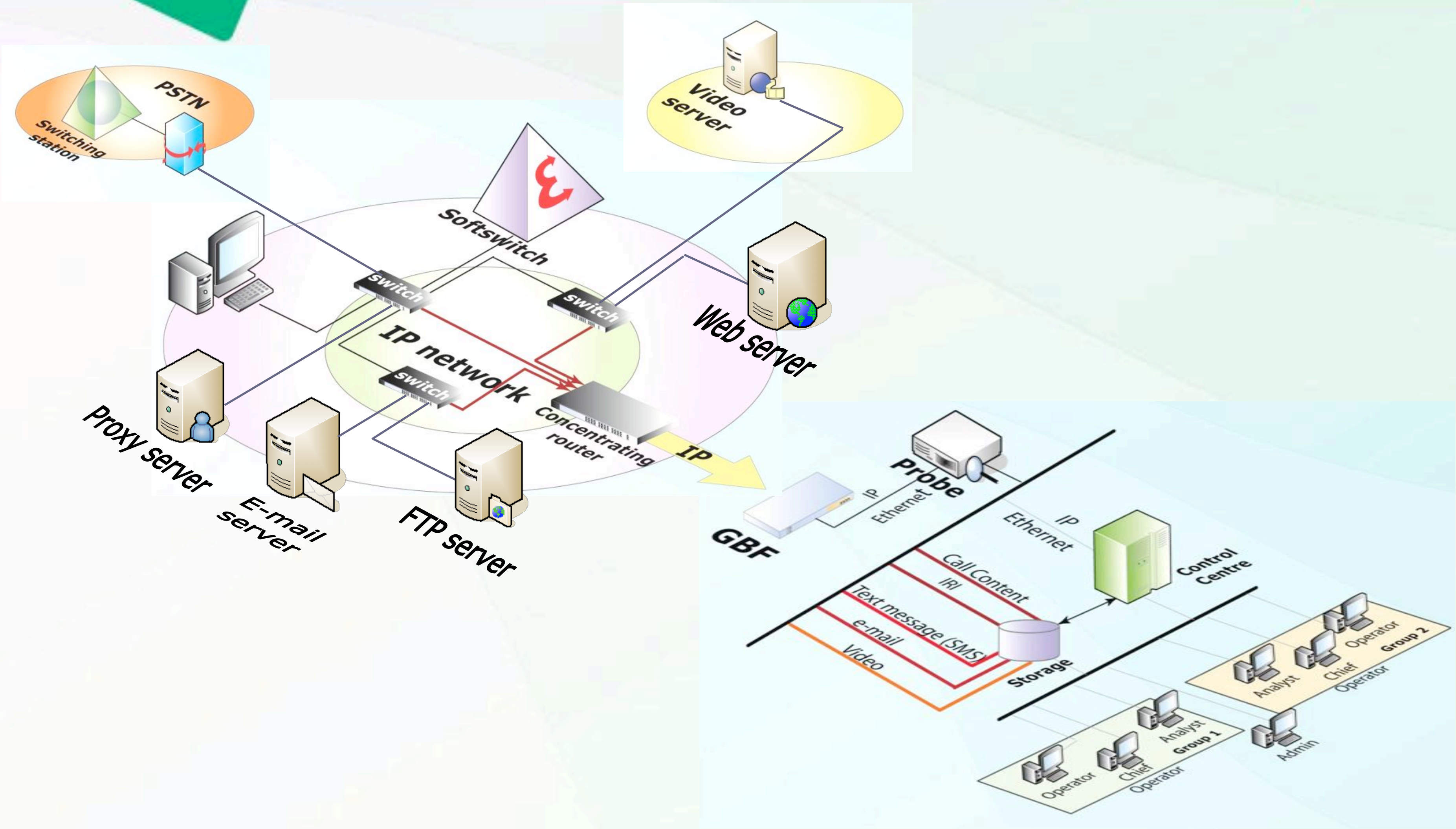
Current situation in telecoms networks

- Constantly increasing volumes of traffic;
- Growth of new types of traffic (video, online games, voice, etc.);
- Servers located outside the operator’s network;
- Transfer of several types of traffic in one session;
- Constantly growing range of added services and user applications.

Modern multiservice networks



Intercept in multiservice networks



Component parts:

Real-time traffic analysis subsystem:

- **GBF** (Traffic intercept filter) **– top-level monitoring device, filtration and intercept of all network traffic**;
- **Probe** (Intercept server) **– signaling message intercept device, routing of voice information (RTP) and other types of traffic**;
- **Control Centre** (Monitoring and intercept centre) **– information distribution system, control of access privileges and functionality**;
- **Storage** (Information repository) **– high security data archive with high-speed access**;

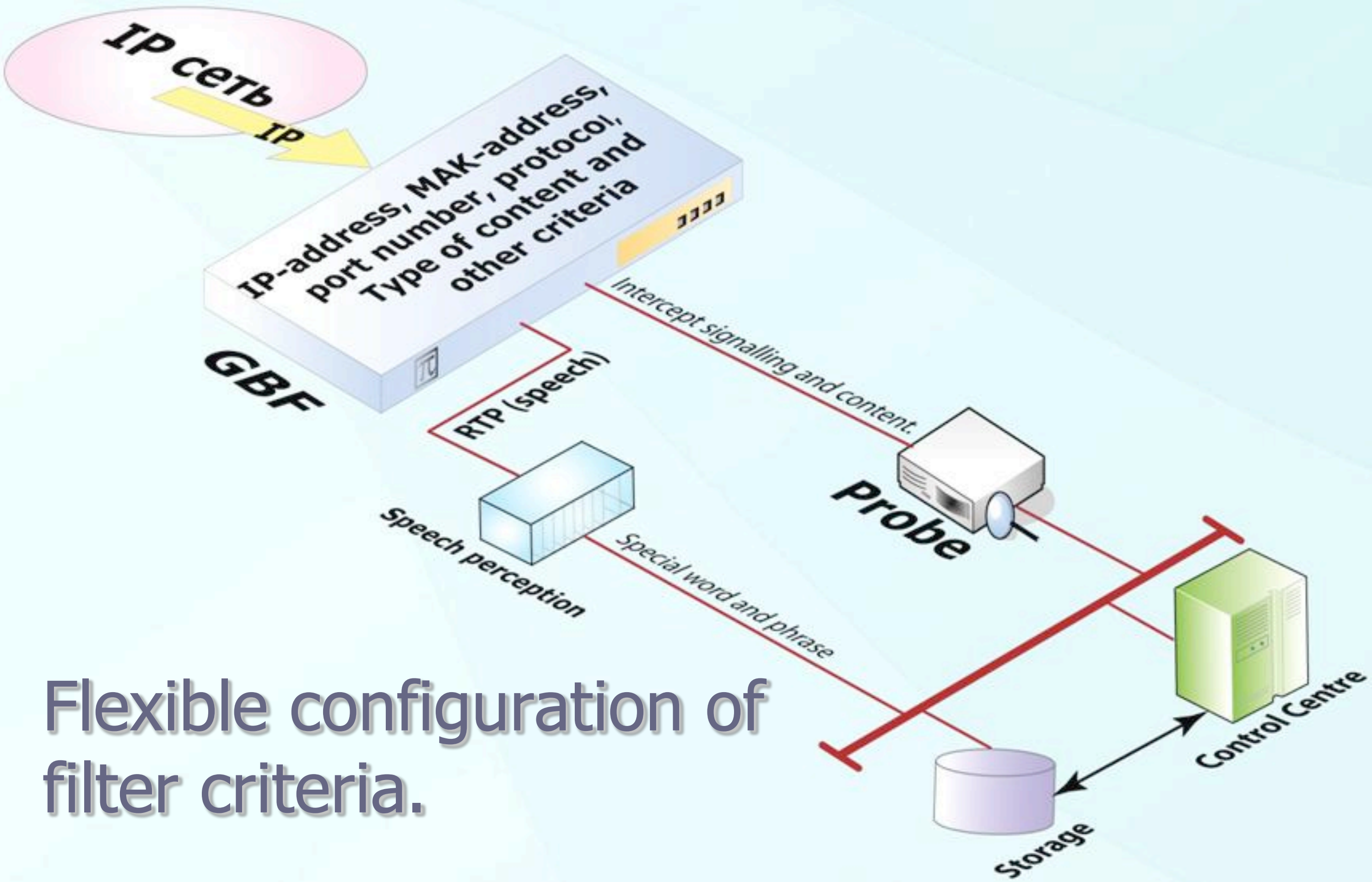
Specifics of real-time traffic analysis

- Suitable for packet-switched networks and circuit-switched networks (using gateways).
- Separate processing of different types of traffic (voice, e-mail, video etc.)
- Wide range of criteria for traffic analysis (type of application-layer content, user ID, IP address, network domain name, etc.)
- Time limits for processing packets (priorities and multi-level queuing)
- Storage of target information only, notification of its detection at Control Centre

Advantages over conventional LI:

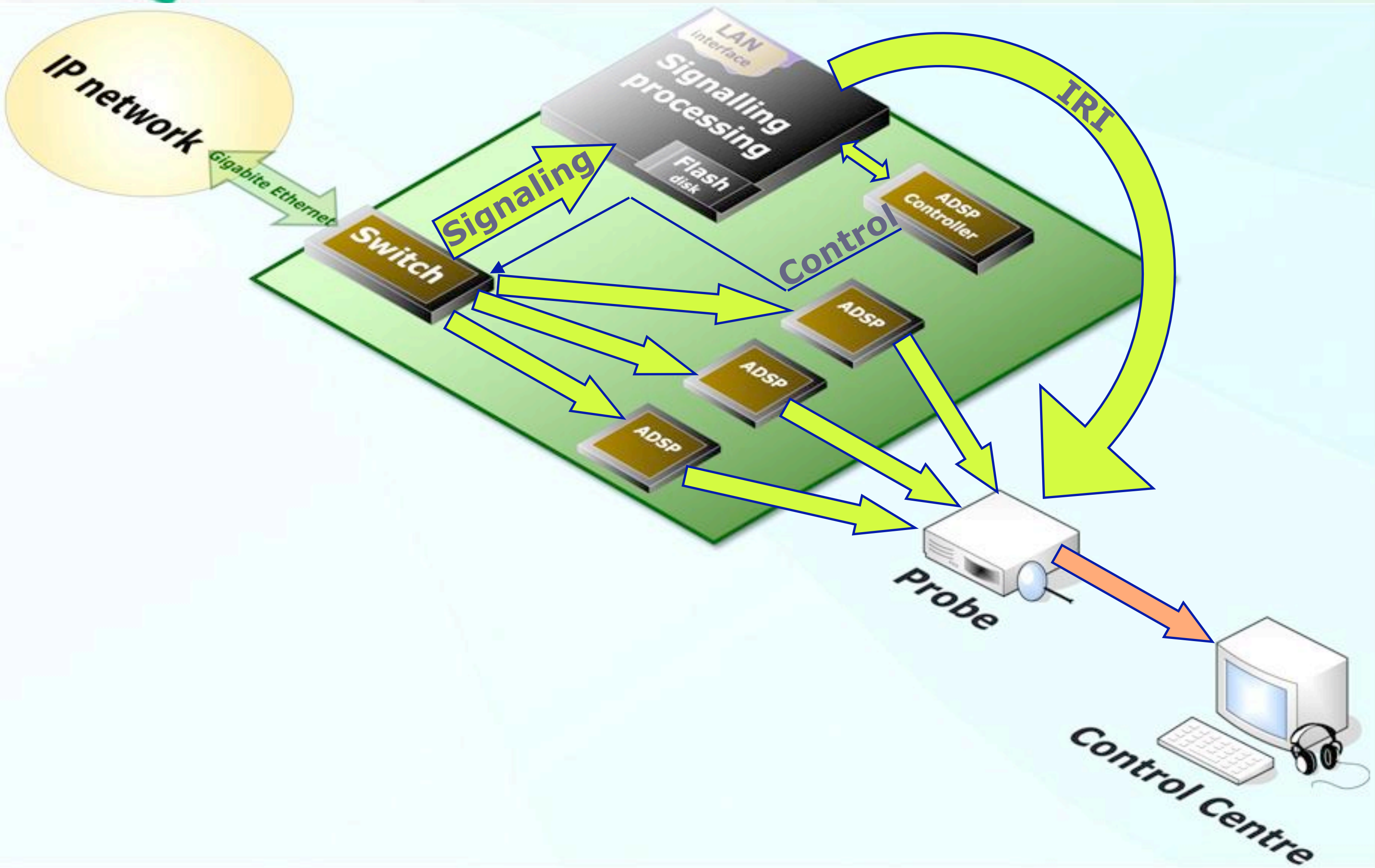
1. Can operate on any existing communications network.
2. Intercept and fast analysis of any type of information according to individual criteria.
3. Single control centre for monitoring all traffic streams.
4. Passive intercept guarantees that intercept activities remain undetectable.
5. Capacity for remote connection over secure channels.

Selection and analysis criteria


IP сеть
IP
IP-address, MAK-address, port number, protocol, Type of content and other criteria
GBF
RTP (speech)
Intercept signalling and content.
Probe
Speech perception
Special word and phrase
Control Centre
Storage

Flexible configuration of filter criteria.

Information processing principles



Commercial applications

1. Detection of users visiting “forbidden” network resources.
2. Detection of unauthorised access and malicious subscribers (in conjunction with AAA systems).
3. Automatic analysis of traffic in real-time, storage of relevant data.
4. Checking parameters of subscriber connections to specific network resources.
5. Usage of information for billing purposes under combined tariffs.
6. Statistics:
    1. Determining most frequently visited network resources.
    2. Determining areas of interest to network users.
    3. Finding unaccounted network traffic.

Security aspects

Transport

Secure connections used in all sections of network

Intercept points

Placement of subject under monitoring remains undetectable both to subject and to network operator

Configuration

System configuration and configuration of intercept & analysis criteria can only be set from the Control Centre and only by authorised personnel.

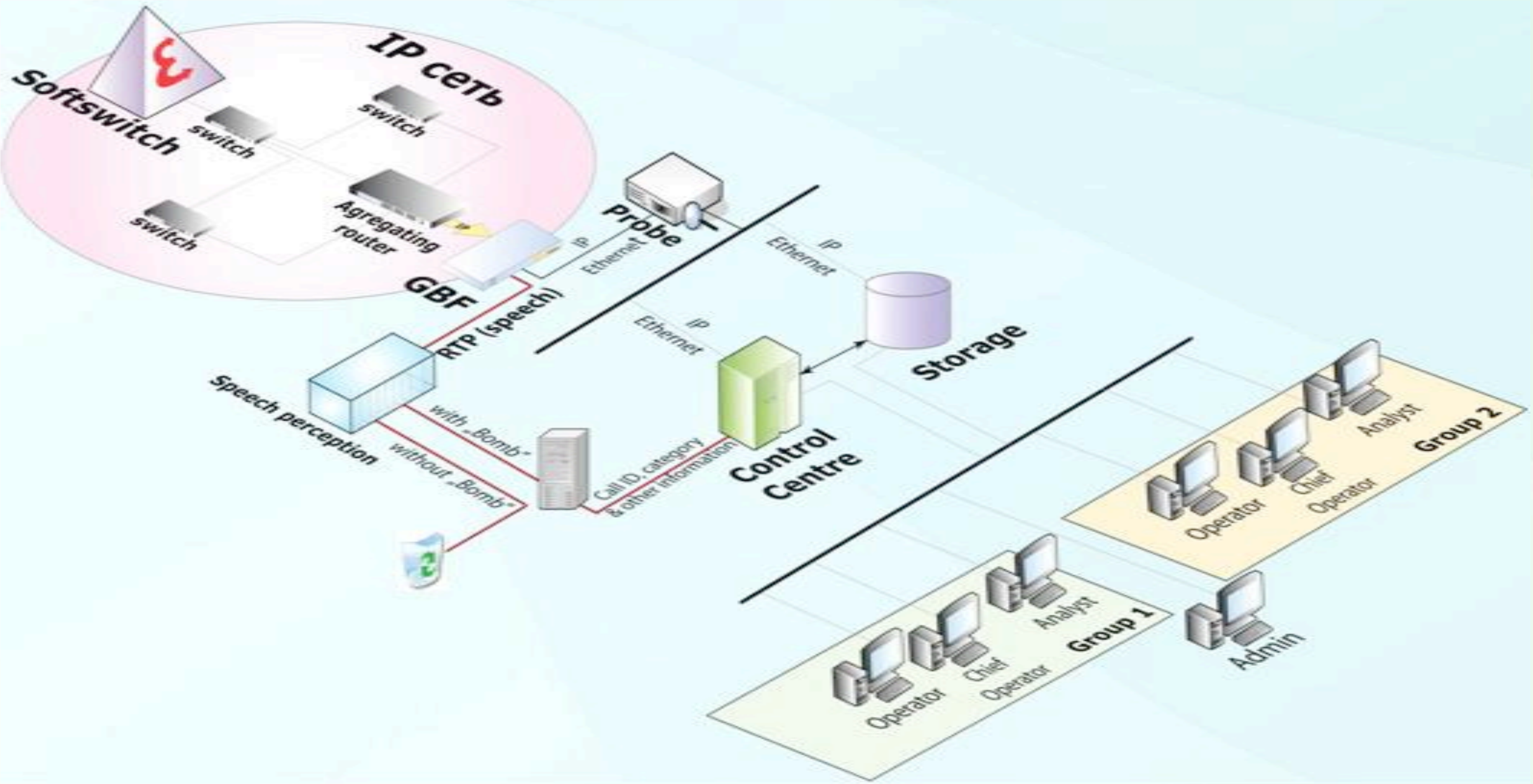
Information storage

Information is stored in encrypted format in specialised databases

Independent control groups

Several groups can operate independently, parallel monitoring cannot be detected.

Additional options. Speech Perception.



Additional options. Traffic analysis.

Speech recognition.

- Detection of key words and phrases in the speech stream.
- Configurable sensitivity for recognition of separate phrases.
- Expandable vocabulary.
- Extra recognition dictionaries and languages can be added.
- Automatic notification on recognition of key words in conversation of monitored subscriber.
- Highlights only necessary information about a potentially suspect user.

Thank you for your attention.

Robert Leitch,
PROTEI Ltd.

Tel: +7 (812) 449-47-27
E-mail: info@protei.com; sorm@protei.ru;
http://www.protei.com

In Prague: +44 77 488 05 143