## Modular IP Probing System (MIPS) RCS IP probing system

General Features

MIPS is the RCS range of high-end Internet probes, designed for use in large static capture systems installed at the Network Operator's site or to deploy high capacity intelligence probes. With superior scalability and integration capability, MIPS can accommodate all possible requirements without restricting bandwidth, throughput or filtering performance.

Main features

- The 100% modular architecture in MIPS probes guarantees maximum flexibility, scalability and upgrade potential.
- The system is built literally on a series of building blocks that can mixed together and combined at your discretion to:
  - create target functionalities.
  - generate required processing power to run critical demand tasks.

- MIPS probe is assembled using established components:
  - a pre-processor module, selected on the basis of the monitored link rate.
  - any number of post-processors and egress modules, selected on the basis of actual filtering and handover requirements.
  - any number of physical CPUs, based on global MIPS modularity principles.
- MIPS can be easily extended, upgraded or reconfigured after the first installation, often without affecting running activities.
- MIPS probes offer the following capabilities and more: static and dynamic IP target interception over hundreds of contemporary targets.
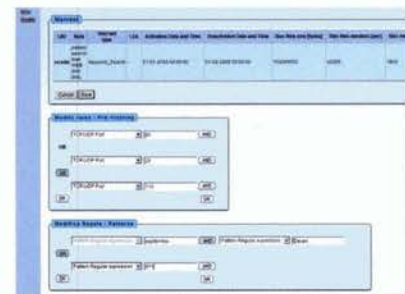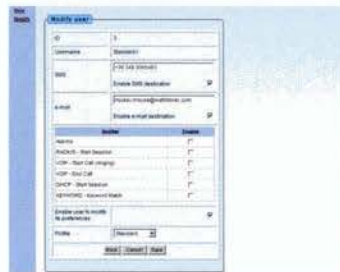
- e-mail interception based on source and/or destination (or BCC) address combinations for hundreds of contemporary targets.
- chat and e-mail interception based on keyword search and regular expression spotting.
- chat nickname login, and access to specified chat rooms.
- VoIP audio and multimedia calls interception based on signalling data (SIP/H.323).
- Attachment text searches.
- MIPS will retrieve the complete internet flux for any kind of match: during keyword searches, any MIPS module (IRC, mail or whatever) will return the entire Internet content for the best analysis value.
- All MIPS probes can be sized to run different filters AT THE SAME TIME, whatever the configuration and whatever the traffic volume or redundancy level.

Network configuration

- By appropriately cascading existing pre/post processing capabilities, and complex mail-keyword targeting rules.
- By adding specialized post-processing modules from our catalogue or by instructing us to develop a bespoke client module for you.
- By developing your own post processors!
- RCS MIPS probes may be easily implemented on blade server architectures, bringing substantial benefits in terms of space and processing efficiency.
- RCS MIPS probes have a unique provisioning interface, which makes the configuration of complex interception rules exceptionally transparent and straightforward.
- A powerful rule synthesis engine allows users to enter the interception criteria using almost natural language.
- A configuration engine provides standard, protected SNMP interfaces to allow integration of the MIPS probes into higher level configuration and control architectures.

System configuration

MIPS probes fully integrate with RCS mediation architecture, constituted by DM (IP Mediation Device) and AM (integrated Administration Module), allowing the construction of permanent probing networks with buffering capabilities and adaptation to any national handover standard whenever required. Full integration with the Visualization System (IVS), making it easier for end users to quickly decode traffic and understand target behaviour.

Whenever requested, customizable interface modules can adapt MIPS probe output to any post-analysis LEA system, such as RCS SFERA.

Pre-Processor modules: available for 1GbE and 10Gb Ethernet technologies, either optical or electrical; IP over ATM compatibility is also offered.
- Pre-Processor modules: available for 1GbE and 10Gb Ethernet technologies, either optical or electrical; IP over ATM compatibility is also offered.
- Post-Processor triggering modules: capable of triggering interceptions upon user or service credentials, these modules are available for several protocols, including Radius, DHCP, DNS, SIP, and H.323.
- Post-Processor deep inspection modules: performing application level and flow-aware interceptions, there are currently many different types of deep inspection module available, including e-mail, chats, generic textual protocols.
  - Egress modules: probe outputs can be adapted to any downstream protocol as standard for both ETSI and CALEA handover protocol families.

rcs

The power of technology.
The worth of safety.