

MCR CAPTOR



AREA has developed the **MCR Captor** solution to support LEAs in their LI (Lawful Interception) activities requiring IP data acquisition, decoding and analysis. The MCR Captor is totally integrated in the MCR Voice & Data Monitoring Center.

ARCHITECTURE

The MCR Captor line of products, based on MCR System technology, relies on the following components.

MCR CAPTOR

IP Probes installed in an ISP network which allow to:

- acquire IP streams up to 10 Gbps
- apply in real time filtering rules to extract specified IP sessions
- decode IP streams
- store intercepted communication contents

MCR PLAYER - MASTER

Installed at the central LEA or at the ISP site, enables to manage the whole IP Monitoring System and to configure filtering rules on the MCR IP Probes installed on the ISP network infrastructure

MCR PLAYER - WORKSTATIONS

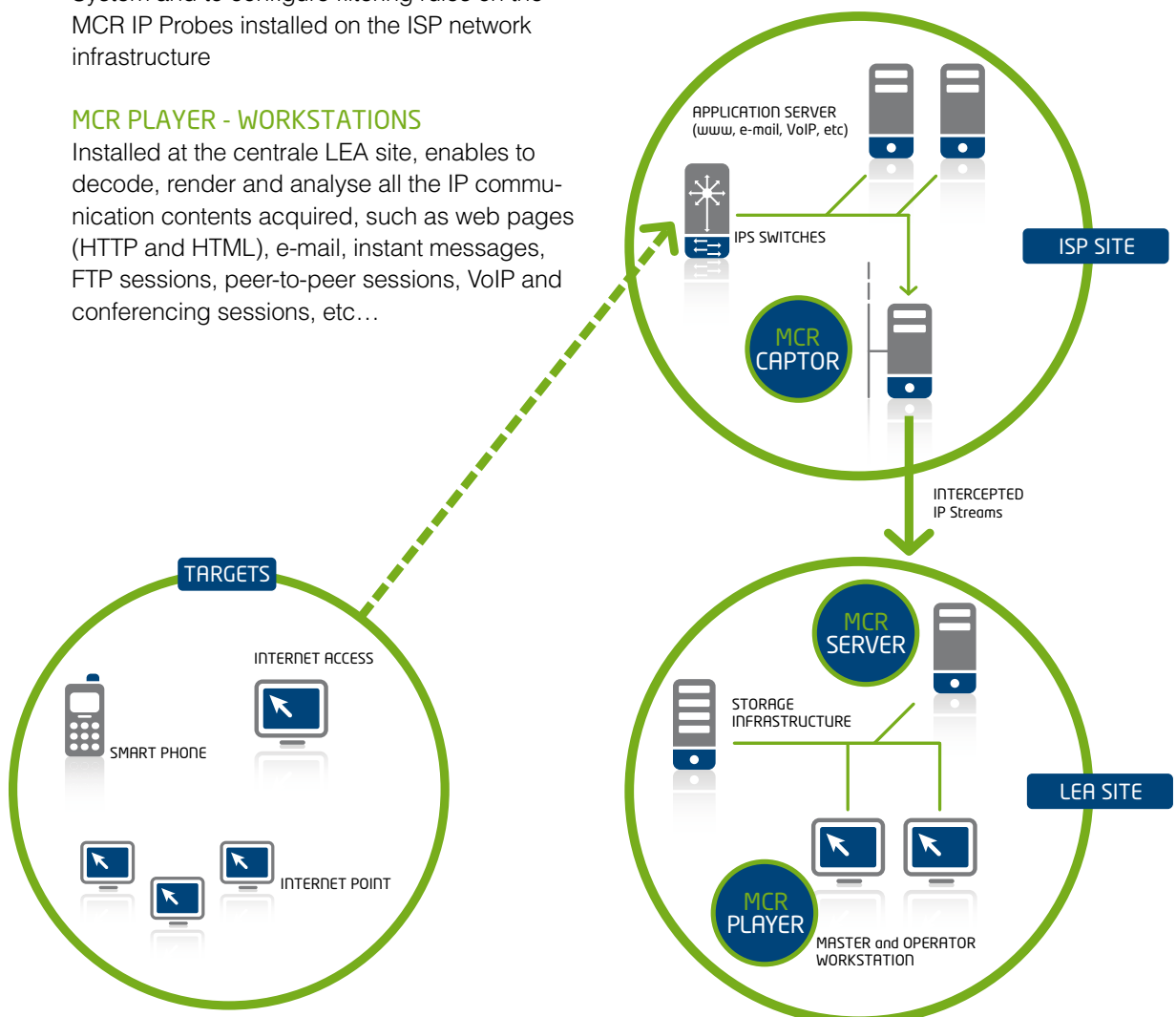
Installed at the centrale LEA site, enables to decode, render and analyse all the IP communication contents acquired, such as web pages (HTTP and HTML), e-mail, instant messages, FTP sessions, peer-to-peer sessions, VoIP and conferencing sessions, etc...

MCR SERVER

It can be installed at the central LEA site, to further process the IP streams acquired by the MCR Captor, applying particular filtering rules on parameters deeply encapsulated into IP streams (for example in interception scenarios where complex pattern behaviors have to be detected).

STORAGE INFRASTRUCTURE

Installed at the central LEA site, it grants the data archiviatiion and database management, according to LEAs storage requirements and Country specific regulation concerning data retention.



MCR CAPTOR PLUS

Given the increasing use of Internet, LEAs need is to have monitoring systems enabling them to effectively carry out IP interceptions which nowadays represent a strategic tool to provide a real added value to investigation activities. MCR Captor enables LEAs to use different approaches to data interception as follows.

ORDINARY INVESTIGATION APPROACH

This approach is usually based on the monitoring of a well specified target who has been previously identified by means of an investigation. The target can be an IP address, an e-mail address, a chat or a VoIP ID.

An enhanced feature of the MCR Captor allows LEAs to use, as filtering criteria, the accounting information of IP subscribers, such as usernames or passwords, included into RADIUS streams.

INTELLIGENCE AND CRIME PREVENTION APPROACH

This approach is used in strategic scenarios where targets are not well identified and in crime prevention activities. This kind of interception, in fact, is useful both to discover relevant information exchanged through communication contents (e-mails, web pages, forum, etc.), to detect suspect behaviors and to

identify the subjects they belong to,

An example is the monitoring of the IP traffic going to a particular website by means of its IP address and URL. DNS traffic can be processed to analyse every connection to a specific website. Moreover, in case a potentially dangerous behavior is detected the MCR System enables LEA operators to activate the interception of the whole IP traffic developed by the subject whose actions on the web have been highlighted.

Another application of the MCR Captor in intelligence approaches is the word detection. The MCR Captor can process a whole aggregated IP stream and extract the contents (such as HTTP pages or e-mails) in which specified words are detected.

The processing of the acquired IP streams can be done both by the MCR Captor and by an MCR Server, according to the processing load required by the requested filtering rules. Generally speaking, the intelligence and crime prevention approach requires higher processing assets than the simple selection of the IP stream belonging to a known IP address.

The global acquisition and filtering capability of the MCR Captor is the following.

MCR Captor strength points are the following.

IP INTERCEPTION FEATURES	PARAMETERS
Interception of IP streams related to well known targets	IP address - E-mail ID - User account ID (Radius) - Chat ID - VoIP ID
Massive IP analysis (parametric acquisition)	Keyword based filtering on: - www - E-mail - Web-Mail - Chat - forum or newsletters
Massive IP interception (no filtering during acquisition, capture of all the IP streams passing through the monitored high-throughput source)	Port filtering and statistic analysis on: - E-mail - Chat - www - VoIP - FTP - Peer-to-peer
Interception of dedicated IP service servers	- E-mail servers - Peer-to-peer servers - Web servers

INTEROPERABILITY, STANDARD AND INTEGRATION INTO TARGET NETWORKS

MCR Captor enables LEAs to monitor IP contents exchanged through any kind of fixed and mobile data target/access networks: dial-up, xDSL or fibre (fixed networks), and WLAN, GPRS or UMTS (mobile networks).

MCR Captor are configured to fit the network technology adopted by Telco operators (i.e. GB Ethernet, STM, PoS) and can capture high bit-rate IP streams (up to 10 Gbps) through SPAN ports, being passive, or by means of tapping devices, being active.

Even if MCR System is widely adaptable to fit vendor-specific or Country-specific interception scenarios, AREA monitoring system is compliant to emerging LI standards such as ETSI (TS 101 671, TS 102 232) and CALEA.

FLEXIBILITY AND SCALABILITY

Thanks to its architecture, the IP Monitoring System can be easily adapted to all the changes that can occur in number of monitored targets, ISP network modifications and protocols to be monitored. The system can be upgraded or downgraded simply changing the number of the MCR Captor installed into target networks.

MCR Captor can support interception activities carried out simultaneously by different LEAs since that it can manage a huge number of concurrent interception instances.

EASY OF USE

Each of the components of the IP Monitoring System, namely MCR Captor, MCR Servers and MCR Player workstations can be managed by a single central console, the MCR Player master workstation.

All the acquired IP contents are rendered through the same user application, the MCR Player.

A central administration console enables the authorized users to set up filtering rules to activate/deactivate IP interceptions on any MCR Captor installed into ISPs network infrastructure.

MCR CAPTOR MAIN FEATURES

Data decoding and rendering

MCR Captor is equipped with a decoding engine which allows the rendering of the acquired IP contents on the MCR Player user interface.

The decoding engine is entirely developed in-house by AREA R&D and it is continuously enhanced according to upcoming data protocols.

System reliability

MCR Captor store and organize all data received through the handover interfaces into a powerful and reliable DBMS, developed by AREA on Oracle® and SQL Server® technologies, selected as the most reliable DB technologies to minimize the occurrence of serious faults. An advanced automatic backup policy is adopted and a RAID 5 mechanism is configured on probes, servers and storage infrastructure to avoid data loss. Moreover, the handover capability is redounded in order to avoid that a single fault can affect the whole system recording capacity.

Data maintenance

According to specific LEA requirements and to Country specific regulations, AREA provides top-level storage infrastructures such as Storage Area Network (SAN).

Security

The IP Monitoring System is configured to be protected from any virus threats, malware in general and hackers attacks. On probes, servers and workstations a top-level anti-virus software is installed and a firewall infrastructure is properly configured according to the latest policies issued by authoritative IT security companies and communities.

The integration with Microsoft Windows® Server platform gives unlimited possibilities to define authentication policies about users groups, privileges and accesses.

```
...VER > 1000
#pragma once
#endif // _MSC_VER > 1000
#ifndef _AFXWIN_H_
#error include 'stdafx.h' before including this file
#endif
#include "resource.h" // main symbols
// CDMotionApp:
// See DMotion.cpp for the implementation of the class
//
class CDMotionApp : public CWinApp
{
public:
    CDMotionApp();
};
```

