STAR-GATE™

Annex: Intercepting Packet Data

Compliance with CALEA and ETSI Delivery and Administration Standards.

USA
Tel: +1-703-818-2130
Fax: +1-703-818-2131
E-mail: marketing.citi@cominfosys.com

Israel
Tel: +972-3-766-4119
Fax: +972-3-766-4747
E-mail: marketing@icominfosys.com

Http://www.cominfosys.com

In this document…

INTRODUCING *STAR-GATE*™ ENHANCEMENTS FOR PACKET DATA NETWORKS 3

OVERVIEW 3

Comprehensive Solution 5

FUNCTIONAL DESCRIPTION 6

Communication Monitoring Components 6

Data Flow 7

TECHNICAL SOLUTIONS 9

Network Based Delivery Solution 9

GPRS Access and Delivery Solution 12

ISP LAN Access and Delivery Solution 16

ISP WAN Access and Delivery Solution 21

Contact Information 26

Introducing *STAR-GATE*™ Enhancements for Packet Data Networks

Overview

Criminals today look increasingly to Internet media to facilitate illegal business. Many have turned to the Internet because of its availability, its simplicity and the knowledge that, unlike traditional telecommunication media, Internet transmissions are not being intercepted by law enforcement agencies.

Legalization of Internet surveillance is taking place worldwide, and operators of Internet Protocol (IP) networks will soon be required to provide communication interception services for law enforcement agencies. Networks falling under the new requirements include:

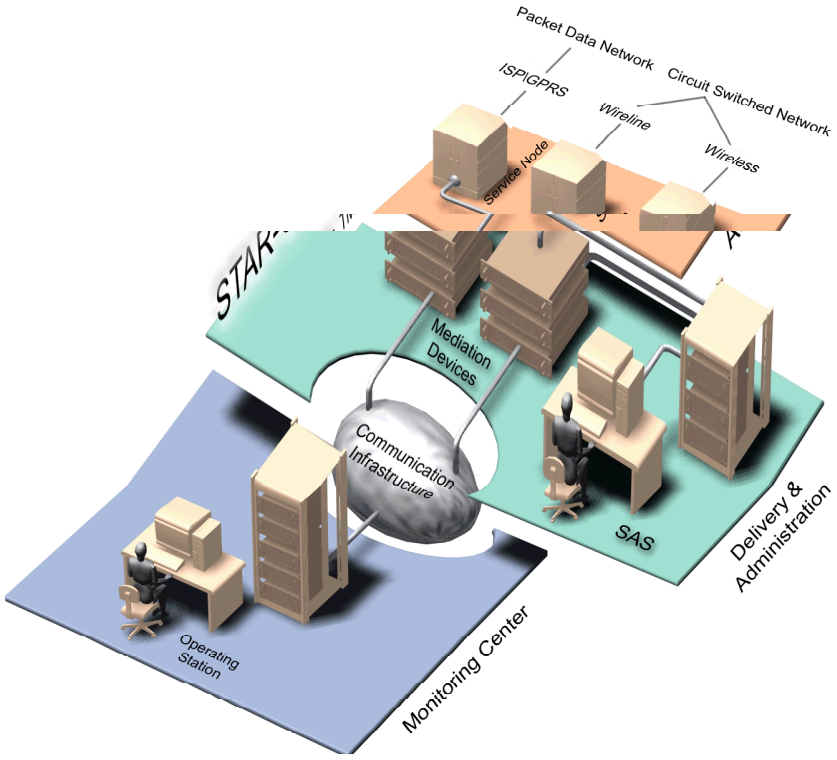
- GPRS networks
- ISPs
- CDMA 1XRTT
- VoIP
- UMTS packet data

The requirements of IP networks are similar to those of circuit switched operators: to intercept all communications of users who have been targeted by law enforcement agencies. The implementation, however, is quite different.

The ability to intercept various forms of Internet media presents great legal and technological challenges.

Comverse Infosys, a pioneer and leader in the development of Lawful Interception (LI) products, is proud to present the solution to the challenge: STAR-GATE for Packet Data

The following diagram illustrates STAR-GATE's architecture:



STAR-GATE provides a turnkey solution for telecom network operators. The solution is based on the following components:

Surveillance Administration Subsystem (SAS)	Provides administrative functions to both circuit switched and packet data networks.
Access Device (AD) *Optional*	Taps and filters network traffic, and forwards intercepted data to the Mediation Device.
Mediation Device (MD)	Designed for a circuit switched and packet data environments, it delivers intercepted communications to predefined sites.

The Mediation Device performs all tasks necessary to deliver intercepted communications to the appropriate law enforcement agency accurately, securely and in compliance with the law. Its basic tasks include:

- **Collecting** intercepted data from the access provider.
- **Converting** messages into the required LI-standard format.
- **Delivering** intercepted communications to the appropriate law enforcement agency.

Comprehensive Solution

Unifying the access and delivery of communication surveillance into a single product, STAR-GATE offers a comprehensive product that serves all functional needs, and provides the following advantages:

- **Wide Range of Protocols:** STAR-GATE provides full support for various protocols for communication content and intercept related information. Regardless of the protocols used by the access provider and the law enforcement agency, STAR-GATE translates intercepted data into the LI-standard format and delivers it to the appropriate agency.
- **Wide range of technologies:** STAR-GATE is specifically designed to accommodate LI standards for mobile packet data networks such as GPRS for GSM, GPRS for TDMA, 1XRTT for CDMA, EDGE and UMTS. In addition, the product provides an excellent LI solution for fixed packet data networks such as Internet Service Provider backbones. STAR-GATE supports various ISP LAN technologies like Ethernet Half and Full Duplex, Fast Ethernet Half and Full Duplex, and FDDI.
- **Multiple nodes:** Each STAR-GATE Mediation Device (MD) can be connected to several different types of access provider's nodes concurrently. Multi-node support reduces initial setup costs and simplifies deployment by offering capacity management that is unavailable in switch-only solutions. The enhanced capacity can be deployed efficiently in a regional framework that adheres to the published configuration guidelines.
- **Multicasting:** The MD can deliver intercepted call data and contents to different law enforcement agencies simultaneously, supporting a different delivery protocol per agency, if necessary.

Functional Description

This section provides an overview of STAR-GATE for Packet Data operations and describes the following subjects:

- Communication monitoring components
- Data flow
- Main features

Communication Monitoring Components

The process of monitoring communications consists of three primary stages: access, delivery and collection/processing.

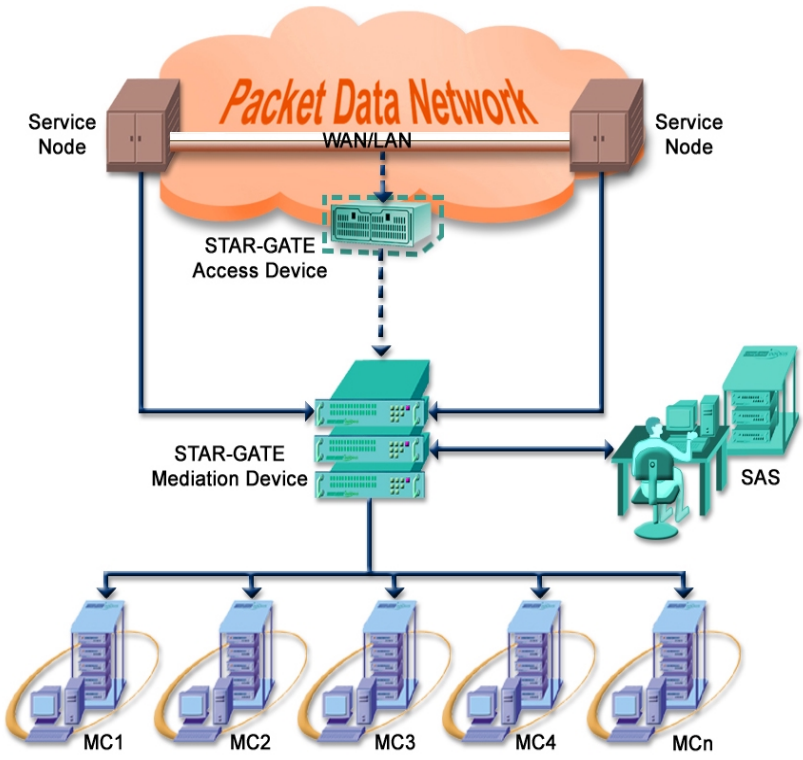
STAR-GATE performs the first two stages of access and delivery using the following products:

Access: Passive tapping devices or network switches are used to intercept communication content. STAR-GATE can optionally provide this functionality using the Access Device.

Delivery: Intercepted communication contents and related information are distributed via the network to the monitoring center. This function is performed by STAR-GATE using a Mediation Device.

All administrative operations are performed by the STAR-GATE Surveillance Administration Subsystem (SAS).

The following diagram illustrates the STAR-GATE integrated configuration, which consists of an SAS, Mediation Device and Access Device (optional).



STAR-GATE for Packet Data Networks

Data Flow

Access

In circuit switched networks, switch vendors can provide access services. However, monitoring packet data networks is a new requirement and switch vendors as yet cannot provide access for lawful interception. STAR-GATE's solution to this obstacle is the Access Device (AD).

The Access Device performs the following functions:

1 **Tapping:** The Access Device obtains raw data from the Service Provider's LAN and intercepts all targeted subscriber transactions.

2 **Filtering:** The Access Device filters the data communicated to or from targeted subscribers. Data packets are intercepted according to the defined interception criteria, which depend on the network type. For example, in a GPRS network, the interception criterion is IMSI. In an ISP network, it can be the IP address, TCP port or e-mail address, for both source and destination.

3 **Forwarding:** The Access Device forwards the target's intercepted packets to the MD for further processing and delivery to the LEA's monitoring centers.

Delivery

STAR-GATE's Mediation Device mediates between the access provider, the law enforcement agency and the Surveillance Administration Subsystem (SAS), and performs the following functions:

1 **Network Interfacing:** The Mediation Device receives intercepted information from the access provider. The information is collected by the Mediation Device and can include both communication content and data.

2 **Conversion:** The Mediation Device converts the collected data format into the requisite LI-standard format.

3 **Delivery:** The Mediation Device delivers the data directly to the appropriate law enforcement agency. Data is sent via LAN to the site router and from there to the collection module located at the law enforcement agency site. There are two communication delivery options: GTP* and FTP.
The Mediation Device can buffer files using mass memory or RAM disk, or use stream buffers for very rapid delivery, depending on the recipient's needs.

4 **Target Provisioning:** The Mediation Device receives and sends administrative data from and to STAR-GATE's Surveillance Administration Subsystem.

Buffering

STAR-GATE offers a completely secure solution and ensures that no data is lost due to communication failures. To this end, the Mediation Device operates according to a store and forward principle, and a recovery mechanism identifies communication failures and recurringly attempts to reestablish the communication connection and to complete unsuccessful delivery missions.

Technical Solutions

This section provides an overview of STAR-GATE's technical solutions for packet data networks, and describes the following options:

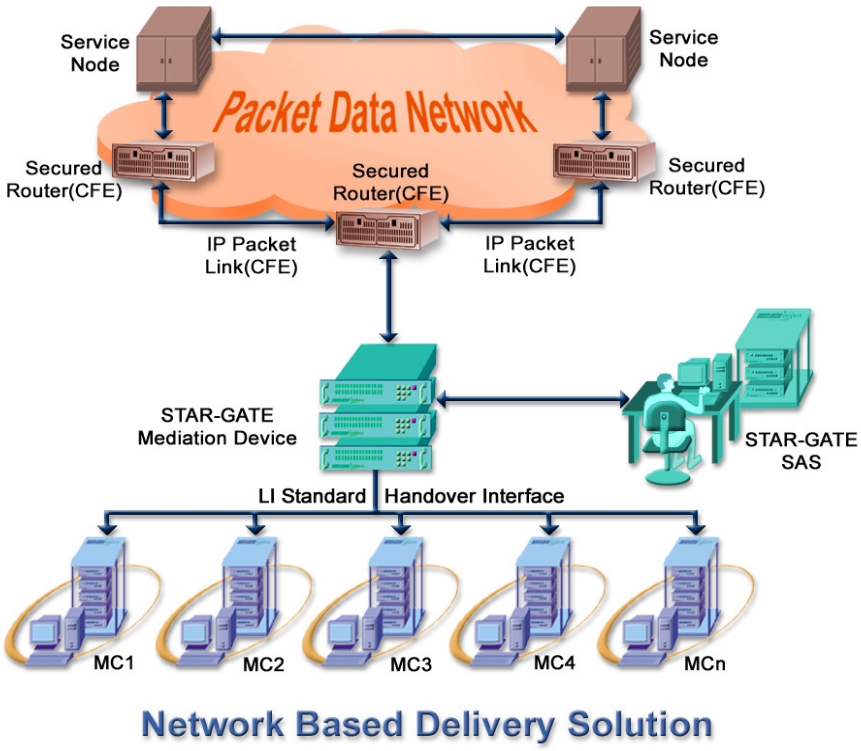
- Switch based delivery solution
- GPRS access and delivery solution
- ISP access and delivery solution

Network Based Delivery Solution

This section describes a typical switch based solution and presents the following items:

- System Architecture
- Functionality
- Capacity

System Architecture



Network Based Delivery Solution

The configuration is similar to the generic STAR-GATE solution for circuit switched networks. Communication is accessed via the network infrastructure equipment, therefore, this solution requires that a dedicated monitoring feature be installed in the service node.

The service node provides both Communication Contents and Intercept Related Information to STAR-GATE's Mediation Device.

STAR-GATE's Mediation Device interfaces between the packet data network nodes and the LEA monitoring centers. It collects the Interception Related Information and Communication Content from the associated service nodes, converts them into the required format and delivers the outputs to the monitoring centers defined for the particular target.

Functionality

The switch-based STAR-GATE solution supports the following access and delivery abilities:

- **Interception Criteria**: IMSI, MSISDN, IMEI for GPRS, IP address;

TCP port, Username, E-mail address for ISP.

- **Intercepted Traffic**: All internal network traffic.
- **IRI**: Depending on switch capability the Mediation Devices provides all specified LI standard events.
- **Target Provisioning to Service Nodes**: Forwarding of target provisioning requests from the Surveillance Administration Subsystem (SAS) to the Service Nodes.
- **Target Synchronization**: Synchronization of the switch target list and the SAS database.
- **Interception Area:** Supports location based filtering.

Capacity

- Number of targets: 1024
- Number of MCs: 30
- Number of simultaneously attached targets: 400
- Number of service nodes per-MD: 10
- Maximum overall traffic: Full Wire Speed
- Number of simultaneous active sessions: 100 (assuming average session throughput of 50kbps)

GPRS Access and Delivery Solution

This section describes a STAR-GATE solution for GPRS containing an integrated Access Device. The following subjects are described:

- GPRS network architecture
- STAR-GATE System
  - Concept
  - Architecture
  - Functionality
  - Capacity

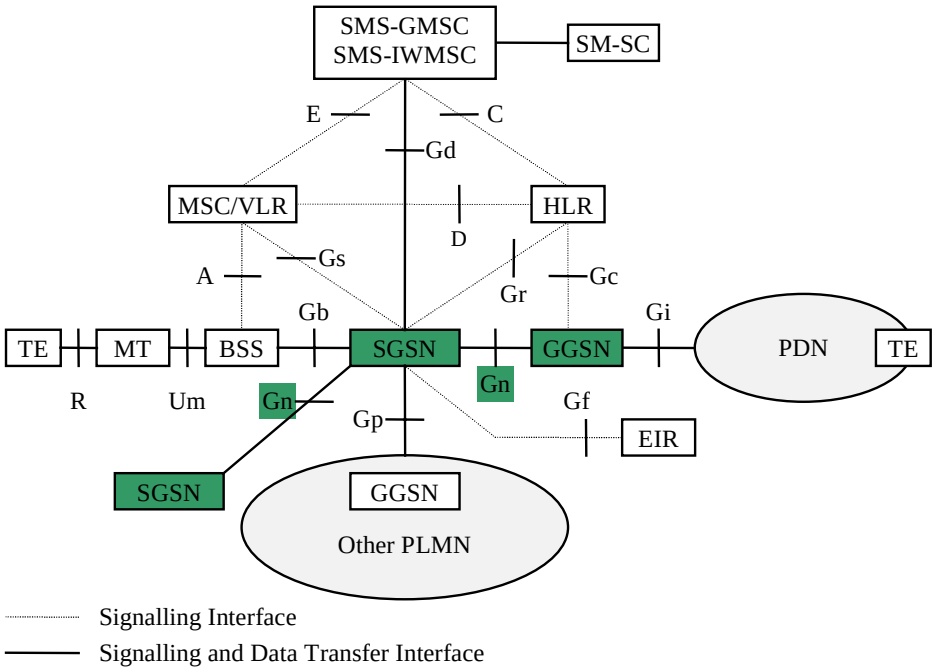
GPRS Network Architecture

A GPRS Support Node (GSN) provides GPRS support services. A single PLMN may contain more than one GSN. The Gateway GPRS Support Node (GGSN) is the node accessed by the packet data network based on the PDP address. The GGSN contains routing information for attached GPRS users. The routing information is used to tunnel PDUs to the MS's current point of attachment, i.e. the Serving GPRS Support Node (SGSN).

Typically, when a subscriber initiates a session, a 'context' is established between the user and the gateway to a Packet Data Network (e.g. Internet). The context originates in the user's terminal equipment and mobile device, continues through the Radio Interface and SGSN, and access the packet data network through the GGSN. A tunnel must be established between the SGSN and the GGSN for every session, whether initiated by the user or the network. This tunnel is established via GPRS tunneling protocol (GTP), for further information about GTP, see GSM 9.60 Specifications. The GTP contains the information required to setup the tunnel and to identify the user, type of session, etc.

The connection between two GSNs is established via the Gn interface.

The following figure represents the GPRS logical architecture. This diagram was taken from the GSM GPRS Specification 3.60.



Concept

The GPRS Access Device filters according to GSN IP address and the UDP Port used for GTP (port number 3386) and is defined in each port connected to a GSN. The filter ensures that transactions that comply with the filter condition (i.e. only GTP messages) are forward to the mirror port.

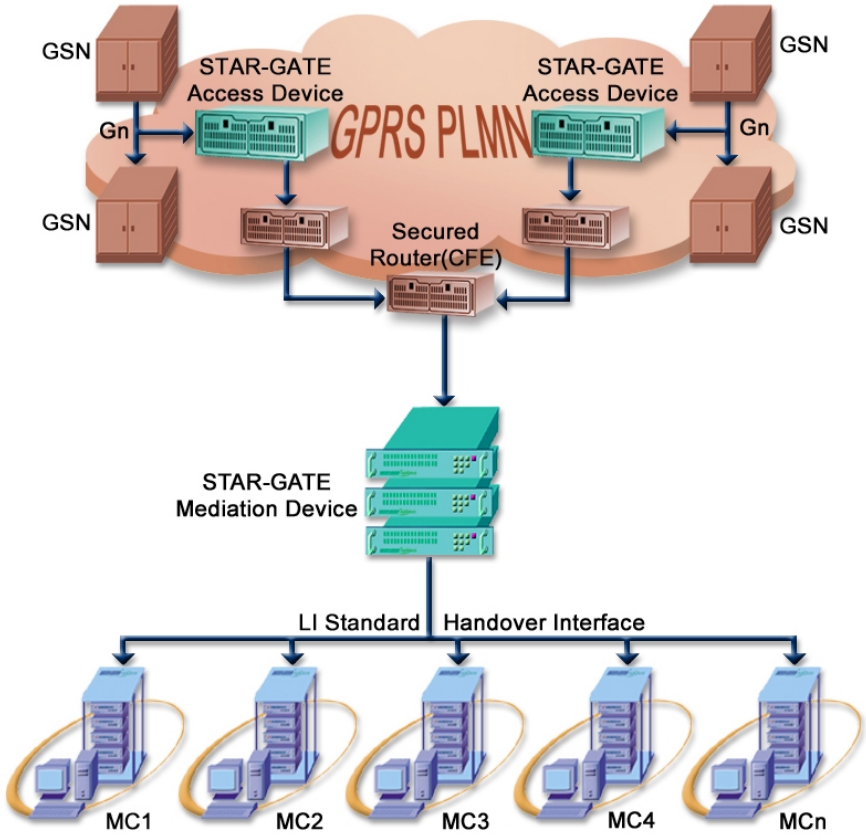
The STAR-GATE Access Device performs GTP interception and decoding operations using the IMSI value that appears in the Tunnel ID field in the GTP header. The Access Device intercepts communications of IMSI values that match those defined in its target list. The target list is controlled by the Mediation Device and contains the IMSI of activated targets.

The Access Device extracts the GTP headers of the related messages. The Access Device checks the Tunnel ID field and matches the IMSI value with those listed in the target list. Having located a match, the Access Device forwards to the Mediation Device messages as Communication Contents. It uses all other GTP signaling messages to build the “PDP Context Activation” and “PDP Context Deactivation” events, which are forwarded to the Mediation Device as Intercept Related Information.

System Architecture

The Access Device taps the Gn interfaces between the SGSN and GGSN and accesses the Communication Content (CC).

The Mediation Device receives the CC, converts it into the appropriate format, extracts relevant IRI information, formats it and delivers both CC and IRI to the monitoring center(s).



System Architecture for GPRS Network

Functionality

- **Interception criteria**: IMSI. The Access Device scans all network GTP signaling and data transactions, intercepting traffic that relates only to the specified targets' IMSI values. The IMSI is contained in the GTP header of each relevant message
- **Intercepted traffic**: All network internal traffic between the SGSNs and the GGSNs
- **IRI**: Session Start time, Session End time.

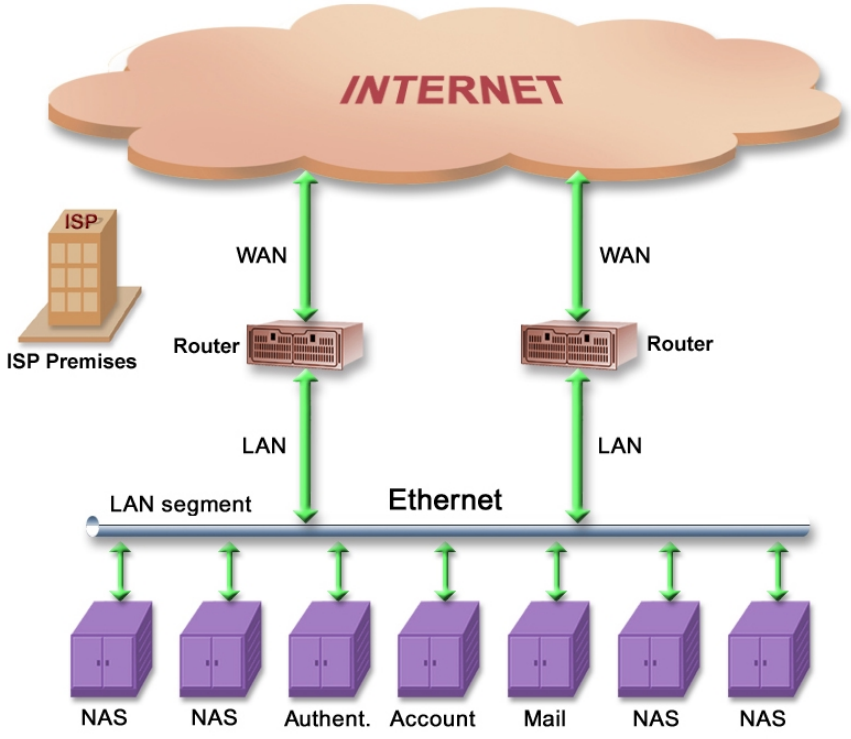
Capacity

- Number of targets: 200
- Number of MCs: 30
- Number of simultaneously attached targets: 200
- Number of GSNs: 10
- Maximum overall traffic: Full Wire Speed
- Number of simultaneous active sessions: 100 (assuming average session throughput of 50kbps)

ISP LAN Access and Delivery Solution

This section describes a STAR-GATE solution for ISP containing an integrated Access Device. The following subjects are described:

- ISP network architecture
- STAR-GATE System
  - Concept
  - Architecture
  - Functionality
  - Capacity

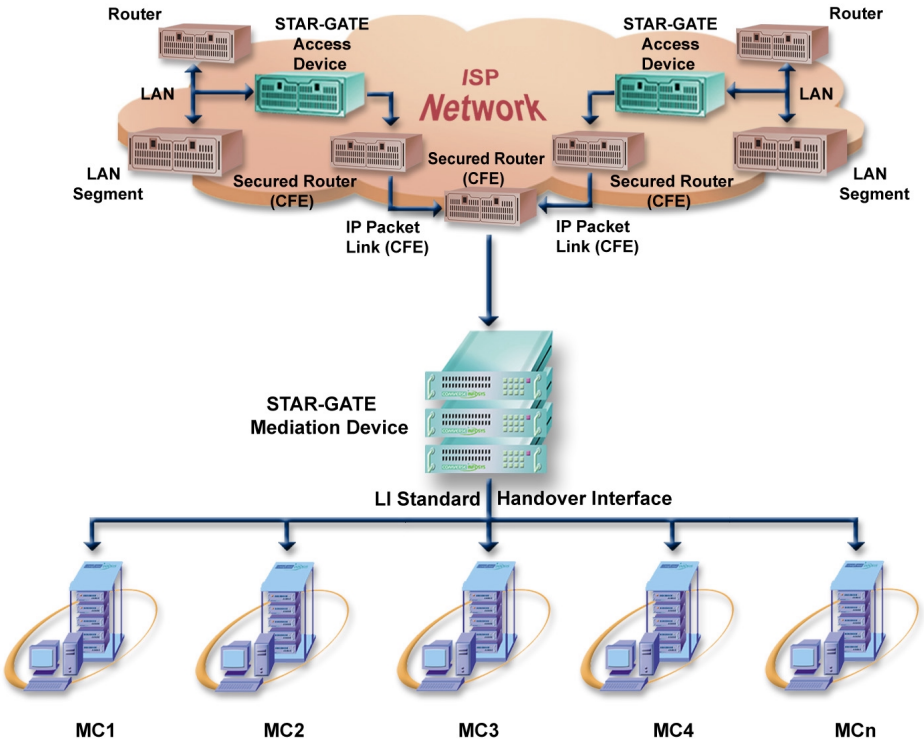


ISP Network Architecture

The ISP network infrastructure usually contains several LAN segments connected via switches. LAN technology can vary and is usually Fast Ethernet, or Gigabit Ethernet. The ISP contains various types of servers; of these, only some apply to the STAR-GATE Mediation Device. Relevant servers are:

- **Network Access Server (NAS)** – A compound device consisting of a set of modems and a protocol-based access server.
- **Authentication Server** – Fulfills two functions for dial-up users:
  - Identifies and validates the user.
  - Dynamically loads per-user configurations such as an IP address for the duration of the call.
- **E-mail Server** - Fulfills two functions for E-mail users:
  - Identifies and validates the user using POP3
  - Sends and receives E-mail messages using SMTP

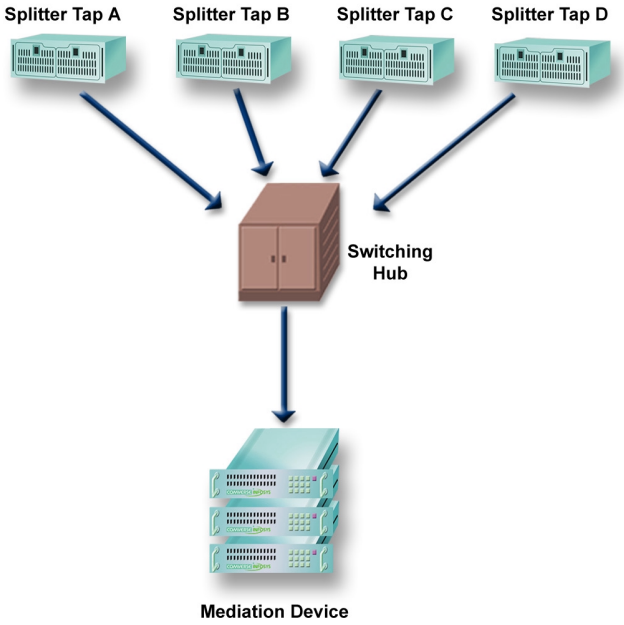
ISP LAN System Architecture



The Access Device taps the LAN interface between the Routers and LAN segments and accesses the Communication Content (CC). Passively tapping the monitored LAN, it filters relevant IP packets for further real-time processing at full "wire speed" and forwards them to the Mediation Device.

The Mediation Device receives the communication content, converts it into the appropriate format, extracts relevant IRI information, formats it and delivers both call contents and IRI to the monitoring center(s).

LAN Access Device Components



The Splitters function is to split the links at each Tap point and duplicate both sides of the link.

The splitters allow monitoring the full-duplex traffic between, for example, two Fast Ethernet devices. The Taps are fully IEEE 802.3u compliant for use in 100BaseTX Fast Ethernet networks in full-duplex mode.

They are designed such that interruption of network traffic will not occur. If power is lost, data is still passed through the Splitter. Power failure in the Splitter will not cause any interruption on the monitored link.

In order to concentrate the two sides of the “tapped” LAN links and to perform initial filtering and load balancing of the packets before they are received by the “MDs”, the splitters are connected to 3-4 layer switching hubs.

The 3-4 layer switching hub can perform “many to many” port mirroring in addition to filtering and load balancing capabilities on the mirror ports to which the “MDs” are be connected to.

Functionality

- **Interception Criteria**:
  - Source or destination MAC address (for example intercepting Cable modem users)
  - Source or destination IP address
  - Source or destination TCP port - for intercepting application specific data, such as all E-mail messages
  - Source or destination user name (requires login data interception)
  - Source or destination e-mail address
  - Subscriber #
  - Specific keyword on packet level
- **Intercepted traffic**: All network internal traffic
- **IRI:** Session start time, Session end time
- **LAN support**:
  - Ethernet 10BaseT
  - Ethernet 100BaseTX – half duplex
  - Ethernet 100BaseTX – full duplex
  - Ethernet 100BaseFX
  - Ethernet 1000Base-LX
  - Ethernet 1000Base-SX

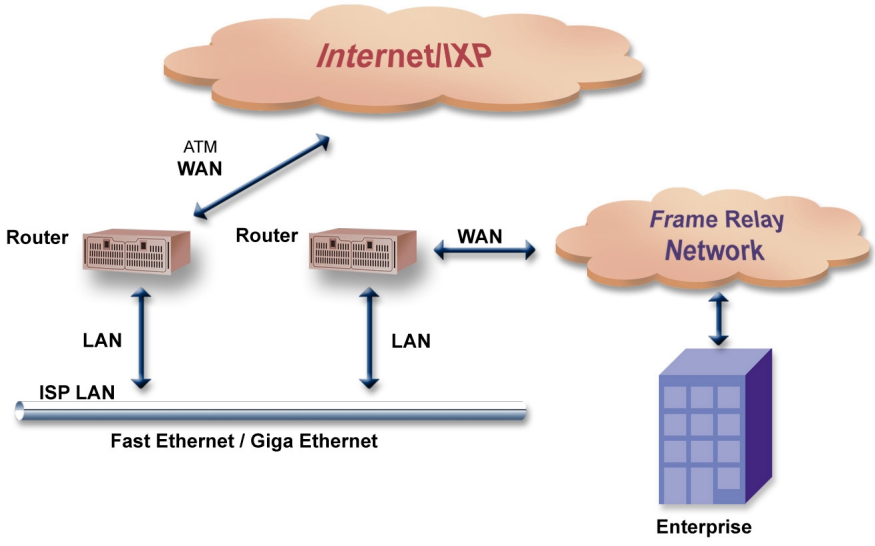
Capacity

- Number of targets: 200
- Number of MCs: 30
- Number of simultaneously attached targets: 200
- Number of ISP LAN segments per-Access Device: 5
- Maximum overall traffic: Full Wire Speed
- Number of simultaneous active sessions: 100 (assuming average session throughput of 50kbps).

ISP WAN Access and Delivery Solution

This section describes a STAR-GATE solution for ISP WAN containing an integrated Access Device. The solution is also applicable for IXP (Internet Exchange Provider) and bandwidth/backbone providers. The following subjects are described:

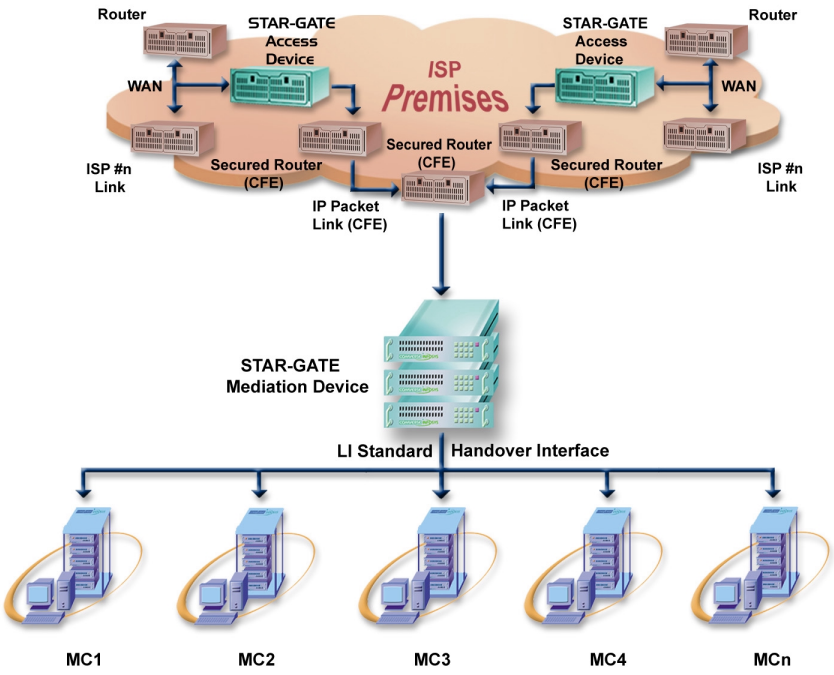
- ISP WAN architecture
- STAR-GATE System
  - Concept
  - Architecture
  - Functionality
  - Capacity



ISP WAN architecture

- An ISP will usually at least one WAN link to the Internet. The WAN technology can vary depending on the required bandwidth and redundancy. Relevant links are: E1, T1, E3, OC3… using link protocols such as PPP, Frame Relay and ATM.

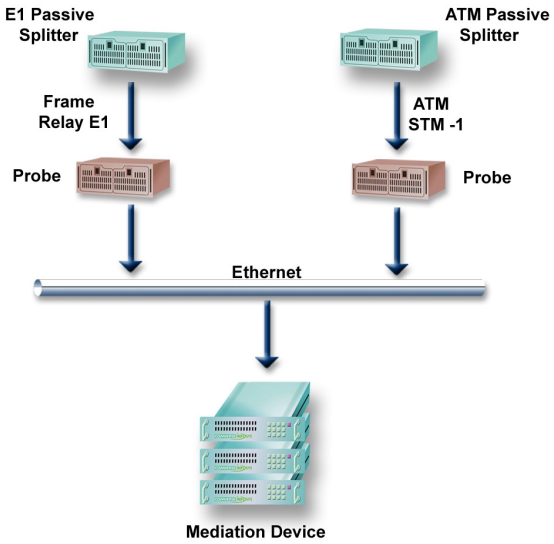
System Architecture



Using passive splitters, the Access Device taps the WAN links going out of the ISP towards the Internet and accesses the Communication Content (CC). Passively tapping the monitored WAN, it filters relevant IP packets for further real-time processing at full "wire speed" and forwards them to the Mediation Device.

The Mediation Device receives the communication content, converts it into the appropriate format, extracts relevant IRI information, formats it and delivers both call contents and IRI to the monitoring center(s).

Access Device Components



Splitters

The Splitters function is to split the links at each Tap point and duplicate both sides of the link.

Fiber optic splitters are available for duplicating OC3 links at custom signal ratios from 10/90 split ratio to 50/50 split ratio.

The same as LAN Splitters, they are designed such that interruption of network traffic will not occur. If power is lost, data is still passed through the Splitter. Power failure in the Splitter will not cause any interruption on the monitored link.

Probes

To cope with the new technologies Comverse Infosys joints commercial third party equipment. The equipment is based on protocol analyzers from industry leading vendors. Its functionality is to cope with the new interfaces and to extract the requested protocols.

Because the most appropriate way to identify a target in an ISP wide area link is by his E-mail address. The probe can filter all SMTP messages in the link and forward them to the MD for further filtering according to a list of E-mail addresses.

Functionality

- **Interception Criteria**:
  - Source or destination IP address
  - Source or destination TCP port - for intercepting application specific data, such as all E-mail messages
  - Source or destination e-mail address
  - Specific keyword on packet level
- **Intercepted traffic**: All traffic IP traffic in the link
- **IRI:** Session start time, Session end time
- **WAN support**
  - Physical Interfaces
    - Serial Interfaces (V.35, X.21…)
    - T1/E1
    - T3/E3
    - OC3/STM-1
  - Link types
    - Frame Relay
    - PPP
    - ATM (RFC 1483)

Capacity

- Number of targets: 200
- Number of MCs: 30
- Number of simultaneously attached targets: 200
- Number of ISP WAN links per-probe: 1-4 (depending on link type)
- Maximum overall traffic: Full Wire Speed
- Number of simultaneous active sessions: 100 (assuming average session throughput of 50kbps).

Contact Information

Contact us at any one of our offices below for more information:

Comverse Infosys Inc
Worldwide Headquarters
Tel: +1 516 677 7300
Fax: +1 516 677 7197
Toll Free: +1 800 967 1028
E-mail: marketing@cominfosys.com

Comverse Infosys Technology Inc.
Tel: +1 703 818 8002
Fax: +1 703 818 2131
E-mail: marketing.citi@cominfosys.com

Comverse Infosys Ltd.
Tel: +972 3 766 4119/5258
Fax: +972 3 766 4747
E-mail:marketing@icominfosys.com

Comverse Infosys UK, Ltd.
Tel: + 44 1923 717347
Fax: +44 1923 717377
E-mail: andrew_dawson-maddocks@comverse.co.uk

Comverse Infosys Hong Kong
Tel: +852 2574 7192
Fax: +852 2904 7676
E-mail:marketing-hk@icominfosys.com

Comverse Infosys GmbH
Tel: +49 6172 941799
Fax: +49 6172 488038
E-mail: franz.woelflick@netsurf.de

Comverse Infosys Brazil
Tel: +55 11 3039 7373
Fax: +55 11 3039 7333
E-mail: marketing@icominfosys.com

Comverse Infosys Netherlands
Tel: +31 79 36 33 111
Fax: +31 79 36 33 110
E-mail: marketingnl@icominfosys.com