



CSCF 11A HSS/SLF 11A Operation and Configuration

DISCLAIMER

This book is a training document and contains simplifications. Therefore, it must not be considered as a specification of the system.

The contents of this document are subject to revision without notice due to ongoing progress in methodology, design and manufacturing.

Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

This document is not intended to replace the technical documentation that was shipped with your system. Always refer to that technical documentation during operation and maintenance.

© Ericsson AB 2011

This document was produced by Ericsson AB.

- The book is to be used for training purposes only and it is strictly prohibited to copy, reproduce, disclose or distribute it in any manner without the express written consent from Ericsson.



Course Objectives

- › After completing the course the student will be able to:
- › Describe CSCF, HSS, SLF node functions and interworking
- › Perform surveillance tasks on CSCF, HSS, SLF
- › Explain how to configure CSCF, HSS, SLF in a secure and redundant way
- › Configure and verify the CSCF, HSS, SLF components and interworking interfaces
- › Perform root cause analysis of faults in the CSCF, HSS, SLF
- › Handle Performance management for CSCF, HSS, SLF

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-2



Chapter Headings

1. Introduction.....	3
2. Architecture.....	35
3. User Interface.....	45
4. Fault Management.....	51
5. Configuration Management.....	64
6. Performance Management.....	212
7. Security, Authentication and Redundancy....	231
8. Session Establishment.....	282
9. Configuration Examples.....	296

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-3



Chapter 1 - Introduction

1. Introduction
2. Architecture
3. User Interface
4. Fault Management
5. Configuration Management
6. Performance Management
7. Security, Authentication and Redundancy
8. Session Establishment
9. Configuration Examples

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-4





Standard CSCF Definition

- › The CSCF is an essential node for processing signaling, using SIP as the signaling protocol.
- › The Call Session Control Function (CSCF) is described by 3GPP Release 8 as follows:

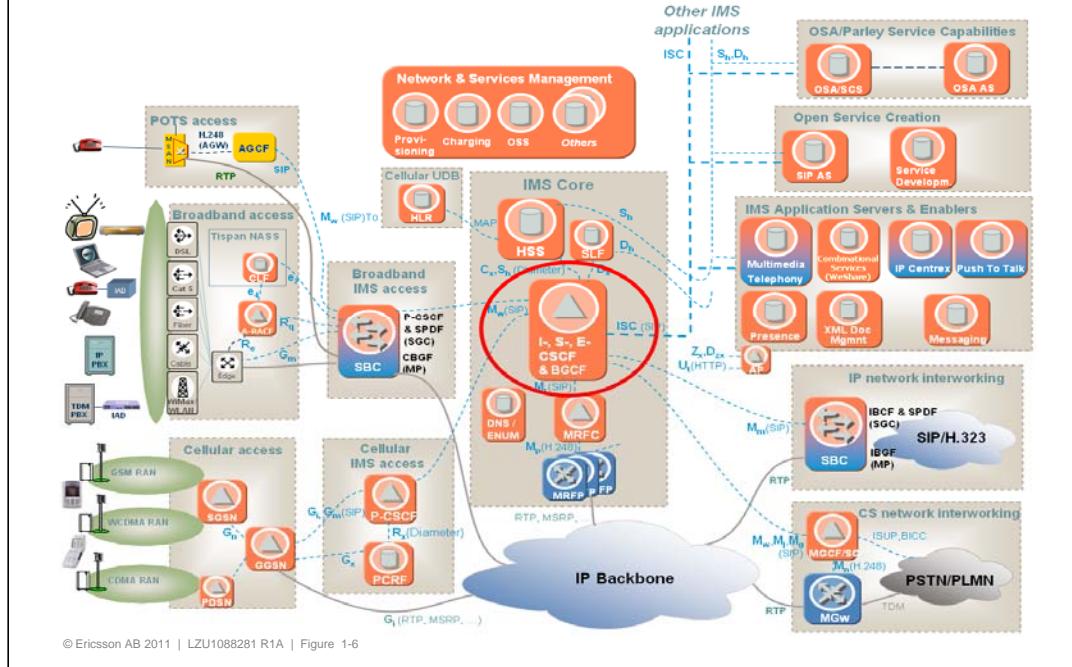
"The CSCF can act as Proxy CSCF (P-CSCF), Serving CSCF (S-CSCF), Emergency CSCF (E-CSCF), or Interrogating CSCF (I-CSCF). The P-CSCF is the first contact point for the UE within the IM subsystem (IMS); the S-CSCF actually handles the session states in the network; the E-CSCF handles certain aspects of emergency sessions; the I-CSCF is mainly the contact point within an operator's network for all IMS connections destined to a subscriber of that network operator, or a roaming subscriber currently located within that network operator's service area.

3GPP TS 23.228

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-5

The CSCF is an essential node for processing signaling, using SIP as the signaling protocol.

Ericsson IMS, logical architecture (with key traffic interfaces)



The Call Session Control Function is defined by 3GPP and 3GPP2. It is using the SIP protocol to establish, terminate and modify a multimedia session.

The CSCF conform to 3GPP TS 24.229.

New features in CSCF 11A :

- Number Portability
- Access Awareness
- Standardized Cx Interface
- Carrier Routing
- NASS Bundled Authentication
- IMS AKA



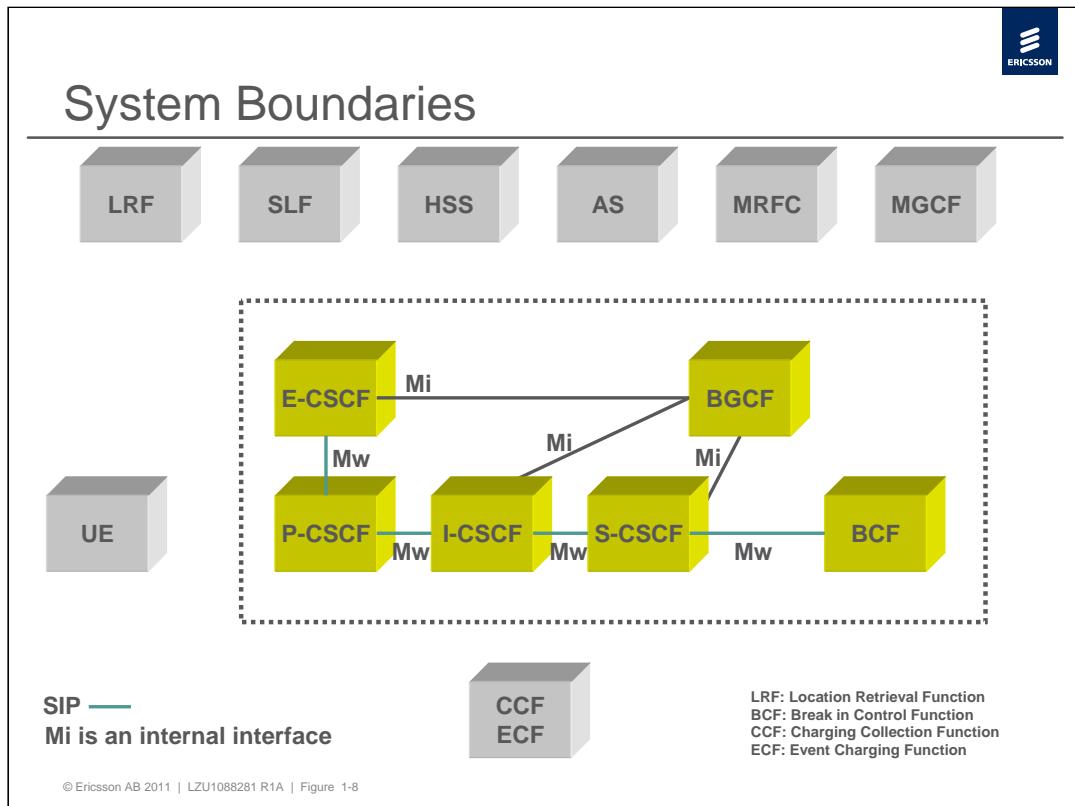
CSCF Supported Protocol Standards

- › 3GPP TS 24.229 SIP
- › IETF SIP RFC 3261
- › IETF DIAMETER RFC 3588 with IMS extensions
- › IETF IPv4 RFC791
- › IETF UDP RFC768
- › IETF TCP RFC793
- › IETF SCTP RFC2960
- › SNMPv3, LDAPv3, IIOP, HTTP, SFTP and SSH
for management access
- › ITU-T X.733 for Alarms

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-7

In the figure the protocol standards supported by the CSCF are listed.

- The CSCF support the 3GPP profile of SIP, as specified in 3GPP TS 24.229.
- The CSCF support IETF SIP, as specified in RFC 3261.
- The CSCF support forwarding of SIP messages, according to SIP method, registration status of the subscriber and appropriate routing mechanism (ENUM, DNS, Record-Route)
- The CSCF support both TCP, UDP and SCTP as transport protocols.
- The CSCF interacts with the HSS and the Billing Gateway using DIAMETER, as specified in RFC 3588
- The CSCF complies with the ITU-T X.733, which defines an information model for all alarms.



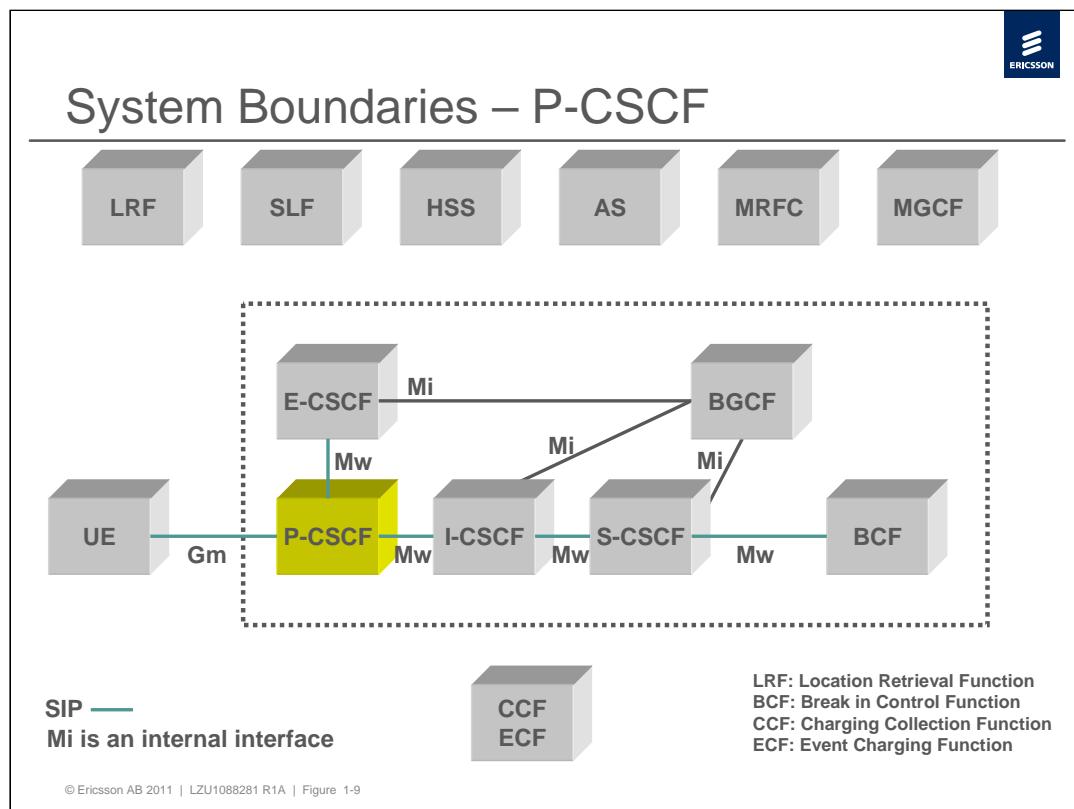
The figure shows the system boundary for the CSCF 11A product and the different nodes and interfaces included in the product.

Mw Reference Point - The Mw reference point allows the communication and forwarding of signalling messaging between CSCFs, e.g. during registration and session control.

Mi Reference Point - This reference point allows CSCFs to forward the session signalling to the Breakout Gateway Control Function for the purpose of interworking with GSTN networks.

In IMS Core 11A the BGCF function is integrated in and only accessible from S-CSCF, I-CSCF and E-CSCF, i.e. Mi is an internal interface.

The different logical nodes (except BGCF) can be flexibly distributed, either co-located on common host(s) or distributed on separate hosts.



The P-CSCF is the first point of contact for the User Equipment (UE), either directly (mobile networks) or via an SBG (fixed networks). The P CSCF forwards the SIP messages received from the UE to an I-CSCF or S-CSCF (and vice versa).

Gm Reference Point - The Gm reference point supports the communication between UE and IMS (P-CSCF), e.g. related to registration and session control.



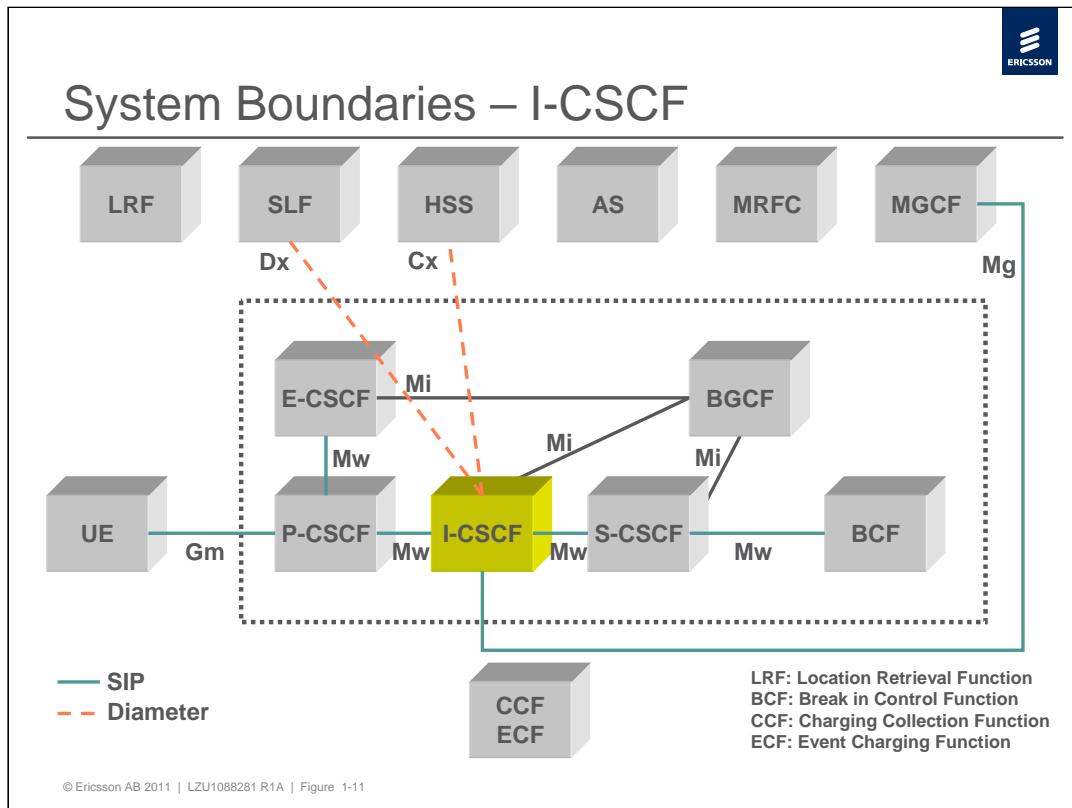
Proxy Call Session Control Function (P-CSCF)

The P-CSCF is the first point of contact for the User Equipment (UE), either directly (mobile networks) or via an SBG (fixed networks). It can be located in the home or a visited network.

Performs the following main tasks:

- › Forwards SIP requests from the access network to the SIP server in the home network (and vice versa).
- › Keeps track of registrations and supervises active call sessions.
- › Performs User agent restriction
- › Stores the UE Contact info (IP address and port) as part of the registration process.
- › Performs call prioritization for Emergency Calls
- › Performs Signaling compression using SigComp

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-10



The I-CSCF is the contact point inside an operator's network for all SIP requests destined to a user of that network operator. It locates the S-CSCF that was assigned to the user at registration through interaction with HSS.

Dx Reference Point - This interface between I-CSCF and SLF is used to retrieve the address of the HSS which holds the subscription for a given user.

This interface is not required in a single HSS environment.

Cx Reference Point - The Cx interface is used for authentication, authorization and location of a user between I-CSCF and HSS.

Dx Reference Point - The Dx interface is used when more than one HSS node is used. SLF does then return to I-CSCF the name of the HSS that serves the user.

Ma Reference Point – This interface between I-CSCF and the Application Servers is used to forward SIP requests destined to a Public Service Identity (PSI) hosted by an Application Server directly to the Application Server.

Mg Reference Point - The Mg reference point allows the MGCF to forward incoming session signalling (from the GSTN) to the I-CSCF for the purpose of interworking with PSTN networks.



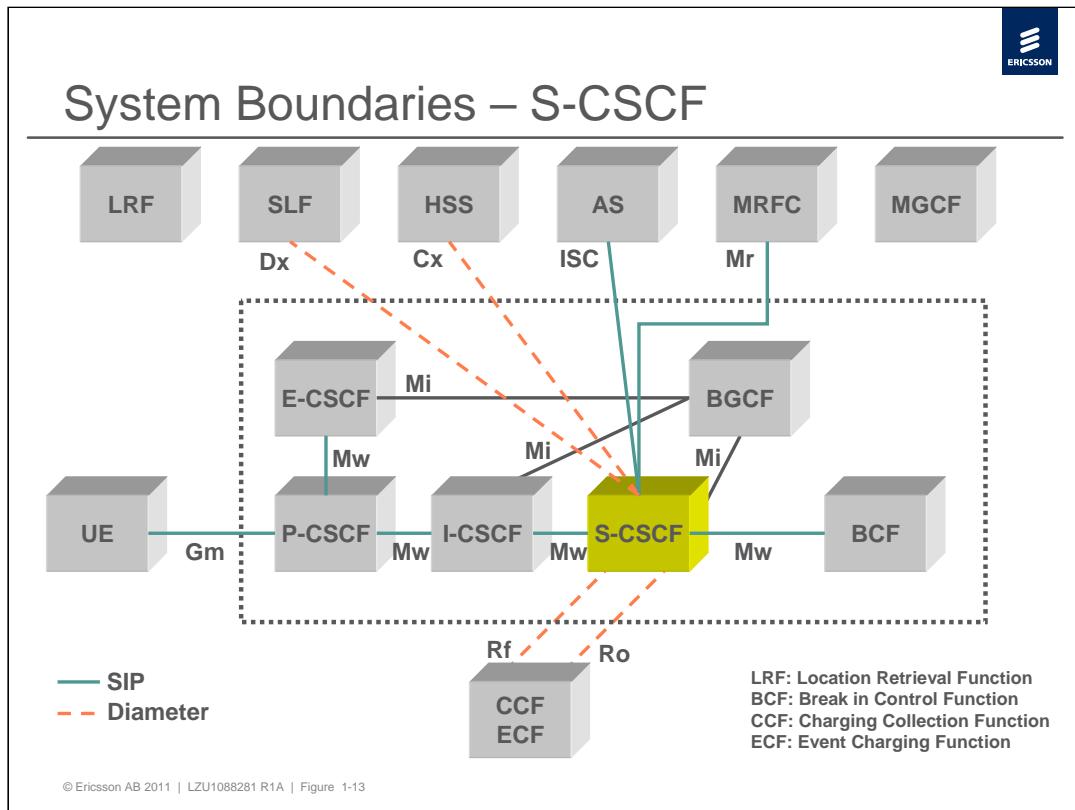
Interrogating Call Session Control Function (I-CSCF)

The I-CSCF is the home network entry point for SIP registration (initial, re-registration and de-registration) requests and for all terminating Requests. It is located in the home network.

It performs the following main tasks:

- › Requests the HSS for the registration status
- › Fetches user's Capabilities from HSS and assigns an S-CSCF during initial registration
- › Routes SIP requests received from another network towards the terminating S-CSCF.

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-12



The S-CSCF performs the registration and session control services for the endpoint. This includes routing of originating requests to the terminating network and routing of terminating requests to the P-CSCF.

The S-CSCF also decides whether an application server is required to receive information related to an incoming SIP request outside a dialog to ensure appropriate service handling.

Cx Reference Point - The Cx interface is used for authentication, authorization and location of a user between S-CSCF and HSS. It is also used to download provisioned user data from the HSS to the S-CSCF.

ISC Reference Point - This interface between S-CSCF and the Application Servers is used to provide services for the IMS.

Mr Reference Point - The Mr reference point allows interaction between an S-CSCF and an MRFC. The interface is used to route requests from S-CSCF to MRFC after a SIP request matches the triggers in the initial filter criteria.

Rf Reference Point - The Rf interface is used between the S-CSCF and the CCF for off-line charging purposes.

Ro Reference Point - The Ro interface is used between the S-CSCF and the ECF for on-line charging purposes. It is based on the Diameter credit control application that defines the credit control request and answer messages.

Dx Reference Point - This interface between I-CSCF and SLF is used to retrieve the address of the HSS which holds the subscription for a given user.

This interface is not required in a single HSS environment.



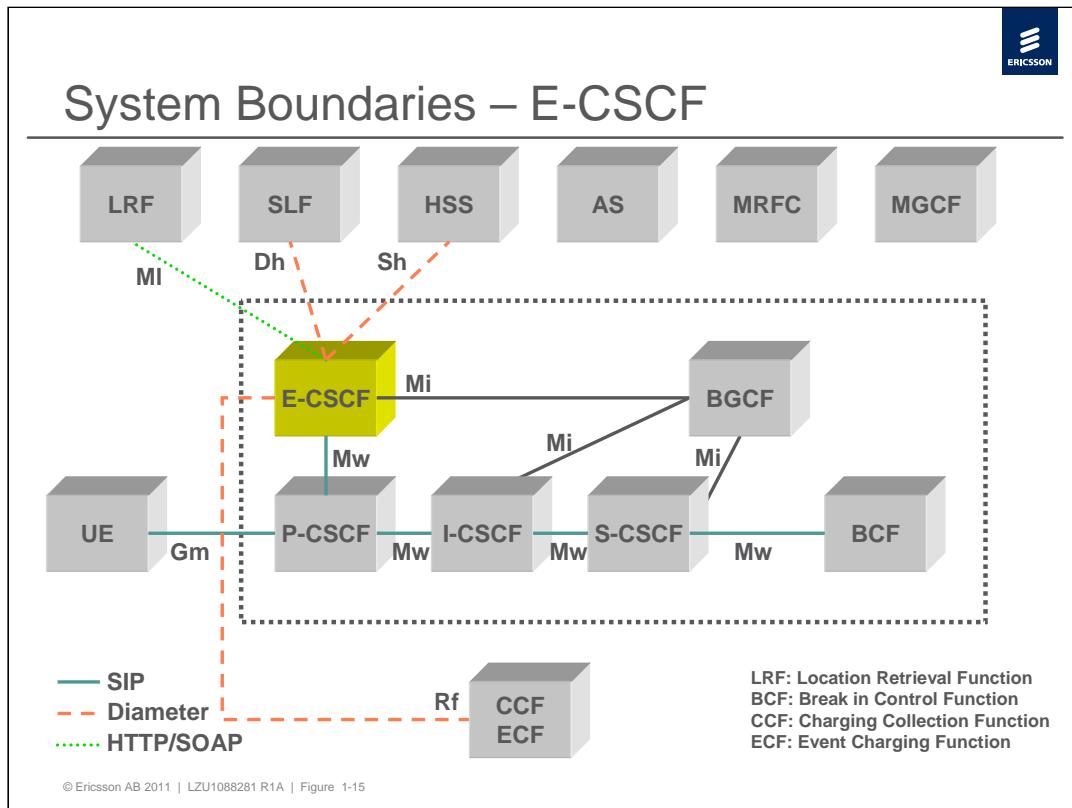
Serving Call Session Control Function (S-CSCF)

The S-CSCF performs session control services for the UE and decides whether an application server is required to receive information related to an incoming SIP request. It is located in the home network.

It performs the following main tasks:

- › Subscriber registration - acts as a SIP Registrar.
- › Downloading and caching of the HSS user profile with service trigger data.
- › Trigger based invocation of the application servers in order to provide multimedia services.
- › Number internationalization from local numbers to global numbers.
- › Querying the ENUM DNS for translation of E.164 numbers and domain names.
- › Routing of sessions
- › Supervision of ongoing sessions
- › Forking of Multimedia sessions
- › Accounting data output

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-14



The E-CSCF performs the handling of emergency calls. Upon receiving an emergency call the E-CSCF access the LRF for the selection of an Emergency Call Centre and routes the call to it.

Sh Reference Point - The Sh interface is used by E-CSCF towards HSS to obtain the reference location information.

Dh Reference Point - The Dh interface is used by E-CSCF towards the SLF to obtain the relevant HSS address in a multi-HSS network.

MI Reference Point - The MI Interface is used by E-CSCF towards LRF to obtain an address or telephone number to the emergency centre.

Rf Reference Point - The Rf interface is used between the E-CSCF and the CCF for off-line charging purposes.



Emergency

Call Session Control Function (E-CSCF)

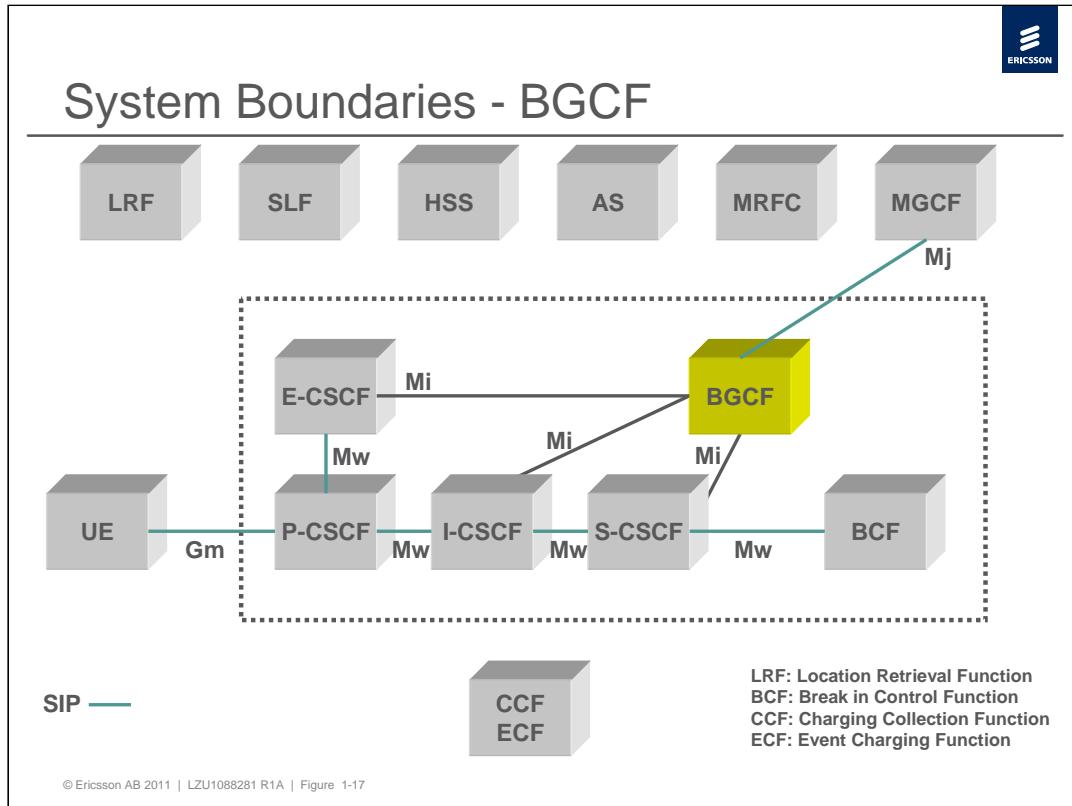
The E-CSCF performs the handling of emergency calls.

It is located in the home network.

It performs the following main tasks:

- › Queries HSS for the reference location information
- › Accesses the Emergency Number database for the selection of an Emergency Call Center (HTTP/SOAP Interface)
- › Routes the call towards the Emergency Call Center
- › Supports routing of emergency calls also for unregistered users
- › Accounting data output
- › Retrieval based on Access Location Info or IP-Address

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-16



BGCF performs a number analysis that provides for flexible breakout routing. The selection of external network is dependent on the calling party domain, the calling party number, the called party number and configurable information in the BGCF. In addition, the selection is also dependent on the RN (Routing Number) and/or CIC (Carrier Identification Code) if these parameters are forwarded by the CSCF to the BGCF.

Mj Reference Point - This reference point allows the Breakout Gateway Control Function to forward the session signalling to the Media Gateway Control Function for the purpose of interworking to the PSTN networks.



Breakout Gateway Control Function (BGCF)

The BGCF performs a number analysis and provides flexible breakout routing if a called number doesn't belong to an IMS user. In addition BGCF can also perform selection based on Routing Number (RN) and Carrier Identification Code (CIC).

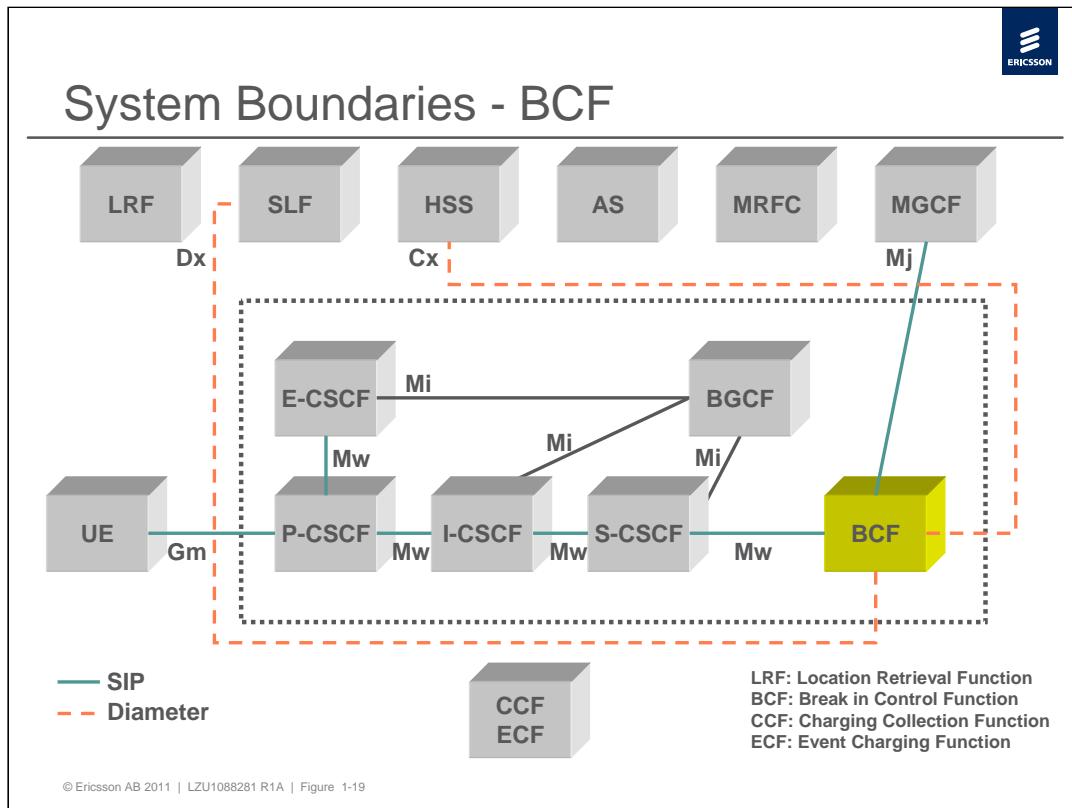
Selection of routing destination can be based on:

- › Calling Party Number
- › Called Party Number
- › Routing Number
- › Carrier Identification Code
- › Calling Party Domain
- › Media Type

The BGCF also provides the possibility to modify the Request-URI by means of Regular Expressions

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-18

In IMS Core11A the BGCF function is integrated in and only accessible from S-CSCF, I-CSCF and E-CSCF



The Break-in control function gives the possibility for users connected to other networks (e.g. PSTN) to execute originating IMS services.

Dx Reference Point - This interface between BCF and SLF is used to retrieve the address of the HSS which holds the subscription for a given user.

This interface is not required in a single HSS environment.

Cx Reference Point – This interface is used to determine if the calling user is served by this IMS domain or not and if the user is registered.

Mj Reference Point - This reference point allows the Media Gateway Control Function to forward the session signaling to the Break in Control Function for the purpose of interworking to the PSTN networks.



Break-in Control Function (BCF)

The BCF gives the possibility for IMS users temporarily connected to other networks (e.g. PSTN) to execute originating IMS services. It is located in the home network.

It performs the following main tasks:

- › Signals HSS in order to determine if the calling user is served by this IMS network or not and if the user is registered
- › Forwards SIP requests to the originating S-CSCF if the user is registered.
- › Rejects SIP Requests if the user is not served by this IMS network or the user is not registered

BCF only handles INVITE dialogs, including the messages CANCEL and ACK for unsuccessful messages. All other messages are rejected

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-20



CSCF Interfaces and Protocols

Interface	Protocol
Signaling	
CSCF-MRFC (Mr)	SIP/UDP or TCP
CSCF-CSCF (Mw)	SIP/UDP or TCP
CSCF-AS (ISC)	SIP/UDP or TCP
CSCF-UE (Gm)	SIP/UDP or TCP
CSCF-IMS NW (Mm)	SIP/UDP or TCP
CSCF-MGCF (Mg)	SIP/UDP or TCP
CSCF-BGCF (Mi)	Co-Located at the moment
CSCF-HSS (Cx)	Diameter/TCP or SCTP
CSCF-Accounting (Rf)	Diameter/TCP or SCTP
CSCF-ENUM/DNS	DNS
CSCF-SLF (Dx)	Diameter/TCP or SCTP
Operation, Administration and Maintenance	
CSCF-SNM	SNMPv3, FTP, SFTP, SSH, LDAPv3, IIOP, HTTP

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-21

The figure shows the protocols used for the different reference points.

SIP will be used together with SDP (Session Description Protocol) as defined by IETF RFC 3261. SIP is transported using either TCP or UDP.

The CSCF supports the DIAMETER base protocol RFC 3588 and the relevant extensions as defined by the IETF and 3GPP/3GPP2, along with accounting extensions specified by the relevant standards bodies. DIAMETER is transported using TCP.

The CSCF supports SNMPv3, LDAPv3, IIOP, HTTP, FTP, SFTP and SSH for management access.

Physical network access to the CSCF is via 10/100 Mbps Ethernet.



Standard HSS and SLF Definition

- › The Home Subscriber Server (HSS) is a logical entity defined in 3GPP Release 8 as:
“The HSS is the **master database** for a given user. It is the entity containing the **subscription related information** to support the network entities actually handling calls/sessions”.
- › The Subscription Locator Function (SLF) is a logical entity defined in 3GPP Release 8 as:
The entity which “is queried by I- or S-CSCF or Application Servers to get the name of the HSS containing the required subscriber specific data. The SLF is not required in a single HSS environment.”

3GPP TS 23.002

SLF can also be used as a load balancer in network deployments where several HSS Front Ends are deployed in the operator's network.

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-22

The Ericsson Home Subscriber Server (HSS) is a real time telecommunication node used in a number of Ericsson technologies. HSS is the master database for the users in the network: it supports IMS, EPC, WLAN subscription handling and relation between them such as authentication or when IRAT (Inter Radio Access Type) mobility applies.

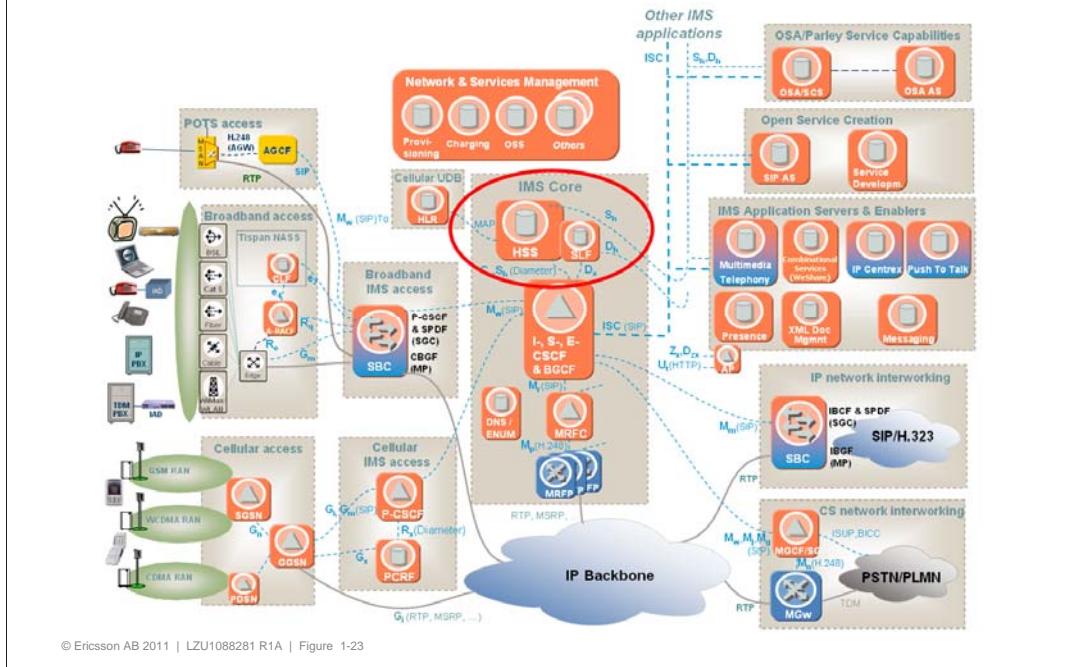
The SLF is a real time telecommunication node that allows the Call Session Control Function (CSCF) and Application Servers (AS) to find the address of the Home Subscriber Server (HSS) that holds the user data for a given user, when multiple and separately addressable HSS nodes have been deployed in the network.

SLF can be used in network deployments where several HSS Front Ends are deployed in the operator's network. In this scenario the SLF is configured to work as a load balancer.

HSS and SLF follow the relevant 3GPP, Internet Engineering Task Force (IETF), Third Generation Partnership Project 2 (3GPP2) and Open Mobile Alliance (OMA) specifications.

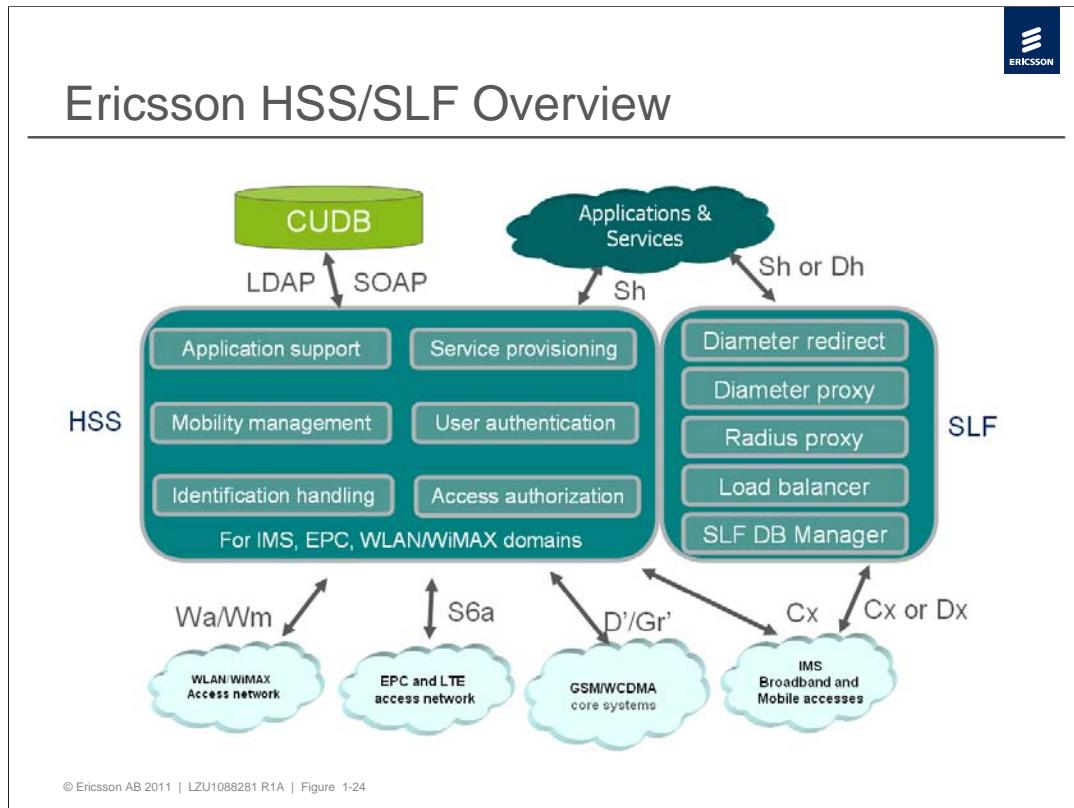


Ericsson IMS, logical architecture (with key traffic interfaces)



The HSS is the master database that contains all user and subscriber information, and keeps track on which core network node is handling the user. The HSS contains the user data that is downloaded to the S-CSCF and stores temporary data with the location of the S-CSCF where a user is registered.

HSS provides the following capabilities: Profile database, User security information generation, User security support, Identification, Access authorization, Mobility management, Service information support, Registration/de-registration.



This picture reviews Ericsson HSS/SLF supported procedures and functions as well as external interfaces.

The Ericsson HSS provides two possible deployments: as HSS Classic and as HSS Front-End (HSS-FE). In a HSS Classic deployment both application logic and data reside within the HSS/SLF node. In a HSS-FE deployment, the HSS/SLF node acts as a data-less front-end that executes the application logic, while application's user data is stored in an external back-end database (BE-DB) accessible from the front-end.



Ericsson HSS/SLF 11A Logical Structure

HSS can be deployed with any combination of:

- › IMS Subscription Manager module
- › EPC Subscription Manager module
- › WLAN Subscription Manager module
- › Subscriber Data Access Manager
- › Authentication Vector Generator
- › Subscription Locator Function

Benefits

- › Flexible scalability
- › Flexible network architecture



TSP 6.0 platform (middleware SW framework)
HW: NSP 5.0 (for upgrades only)
HW: NSP 6.0 (for all packages)

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-25

IMS Subscription Manager (ISM) Module provides a variety of functionalities and procedures related to e.g. subscription management, mobility management procedures, session establishment control, user authentication, and access authorization in the IMS network.

Subscription Data Access (SDA) Module provides the application layer with user-related data within a network. Moreover, it acts as repository for application servers profile data managed as transparent data in HSS server.

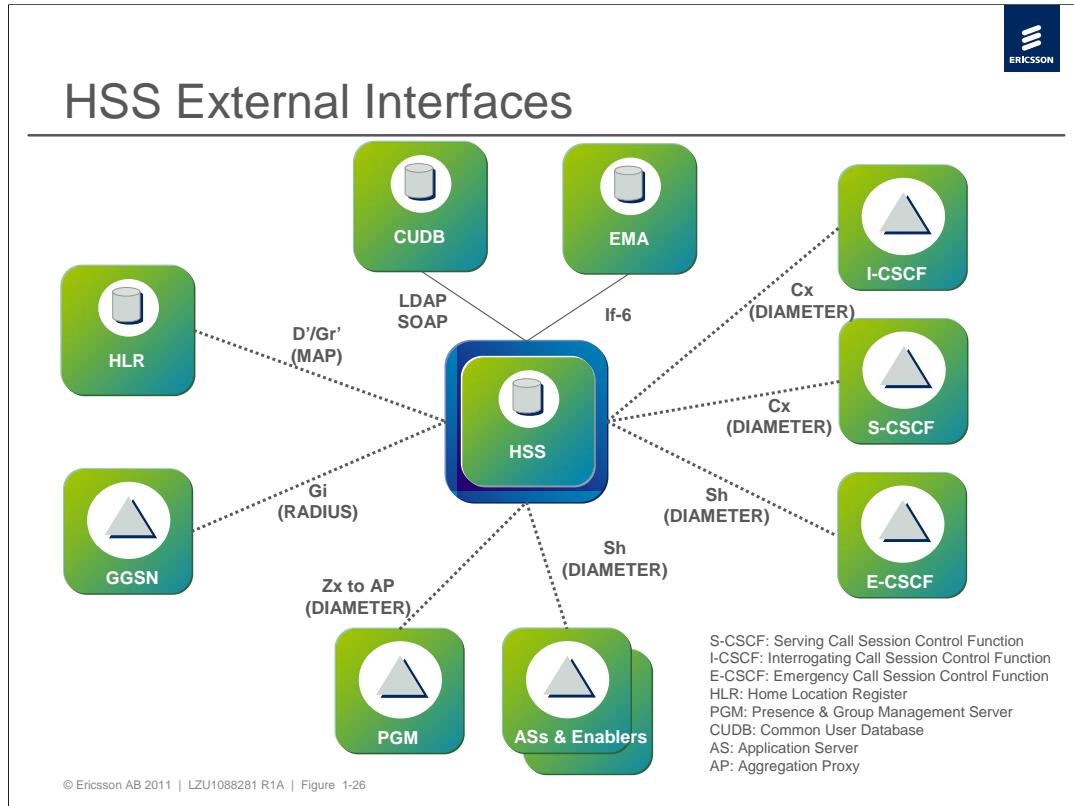
EPC Subscription Manager (ESM) Module provides the handling of subscriptions, authentication, authorization, user traffic protection and mobility management in the EPC domain.

WLAN Subscription Manager (WSM) Module provides subscription management, authentication, authorization and user traffic protection in the context of WLAN accesses.

HSS includes in addition two functions implicitly available to one or several commercial modules within:

Authentication Vector Generator (AVG) function performs the algorithms relevant for the generation of authentication vector in association with:

- ISIM- and USIM-based authentication for IMS.
- USIM-based authentication for EPC.
- USIM-based authentication for WLAN.



The **Cx interface** is used for authentication, authorization, and location of a user, and to download user data from the HSS to the S-CSCF. Diameter protocol is used.

The **Sh interface** is used by IMS application servers to retrieve user non-transparent data or store and retrieve user application data stored in HSS. The interface between HSS and E-CSCF is also defined as Sh. Diameter protocol is used.

The **Zx interface** is used by the Aggregation Proxy for authentication and authorization of a user when utilizing the Ut reference point. Diameter protocol is used. HSS supports **D'/Gr'** interface with HLR/AuC for requesting authentication vectors or location/user state of the GSM/WCDMA user. Ericsson GGSN interworks with the SM module in HSS over **Gi-interface** to realize the Single Sign-On procedure. RADIUS protocol is used.

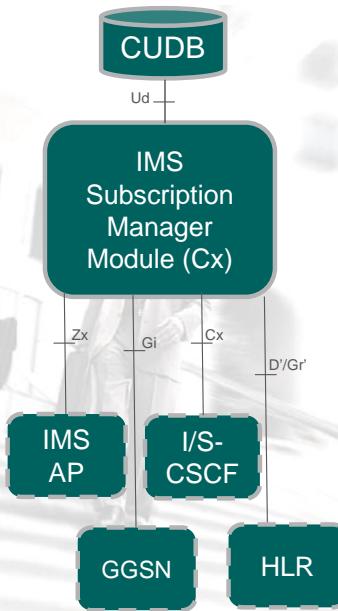
In a HSS-FE deployment, HSS-FE communicates with an external back-end database (BE-DB) over LDAP/SOAP interface.

The **If-6 interface** is used between EMA and HSS to provision user data in the HSS. The LDAP protocol is used. EMA supports the following operations towards HSS using the HSS LDAP interface: Create subscriber, profile, public id and trigger data; Modify existing subscriber information; Delete subscriber and connected data.

The HSS supports SNMPv3, LDAPv3, IIOP, HTTP, FTP, SFTP and SSH for management access.

IMS Subscription Manager Module

- › IMS subscription management
- › Distinct PSI support
- › Service profile configuration
- › Configured profiles support
- › Charging support
- › IMS user authentication, wire-line and wireless accesses
 - SIP Digest, IMS SSO (GIBA, NBA) and IMS AKA (USIM/ISIM)
- › IMS session handling and mobility management
- › IMS user profile management and service authorization
- › Implicit registration support
- › Barring support
- › Roaming restriction based on IMS network domain
- › Authentication of XCAP users
- › Identity convergence
- › Multiple private and public identities
- › Max. No. of contacts
- › Roaming awareness, wire-line and wireless accesses
- › CSCF restoration
- › Optional capabilities
- › ISM Inter-working with AUC
- › Wildcard ID (wlMPU and wPSI)



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-27

IMS Subscription Manager (ISM) module. ISM provides user mobility management, session establishment procedures, authentication, user traffic protection and authorization support for IMS. It serves the subscription related management functionality in IMS network supporting the functionality based on 3GPP Cx reference point and Ericsson proprietary Zx reference point. HSS supports the Gi reference point (only the accounting related functionality) within the Single Sign On (SSO) authentication for wireless access.

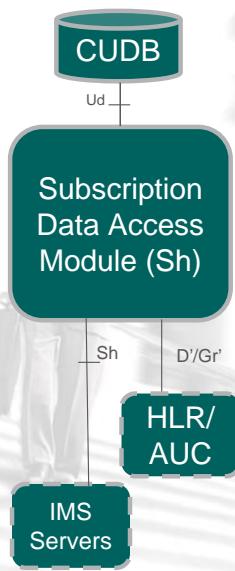
New features in HSS 11A:

- Identity Convergence
- Access Awareness
- NASS Bundled Authentication
- ESM Module
- ISIM support of IMS AKA
- HW features (TSP6/NSP6)
- Authentication Vector Generation



Subscription Data Access Module

- › IMS user data access
- › Subscription and Notification support
- › AS accessibility control management
- › Wireline emergency data access
- › CS/PS data retrieval support
- › Transparent data support

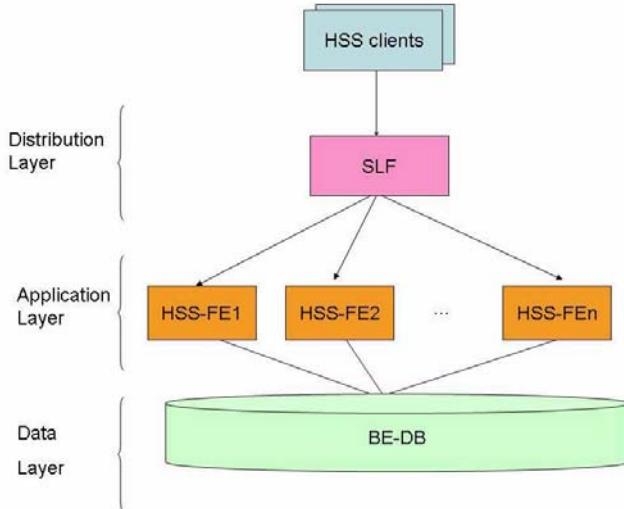


© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-28

SDA provides application layer support. It serves the accessibility of IMS subscription data as defined in 3GPP Sh reference point. This offers a powerful and centralized mechanism to provide IMS applications with the relevant subscriber data they need to run the corresponding IMS service. Besides SDA acts as a repository offering the possibility of storing application dependant data. HSS interfaces HLR/AuC for requesting location/user state of the GSM/WCDMA user. This module requires the availability of ISM module.



HSS FE Deployment Configuration



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-29

Data Layered Architecture (DLA) refers to an architectural approach for the realization of network functional entities (e.g. an HSS) in which data and logic are separated in different layers, implemented by separate network elements. That is, application data is hosted in a network element, referred as back-end, while application logic is hosted in a different network element, referred as front-end.

The DLA is composed of the following layers:

1) Distribution Layer (i.e SLF module acting as load balancer and supporting signaling proxy mode of operation)

- Distributes requests to Front Ends (FEs) with a mechanism that attempts to achieve a uniform load across all FEs of the corresponding application.
- Hides structure of FEs from clients

2) Application Layer (e.g. HSS-ISM, SDA, ESM or WSM configured as front-end servers interacting with external back-end database)

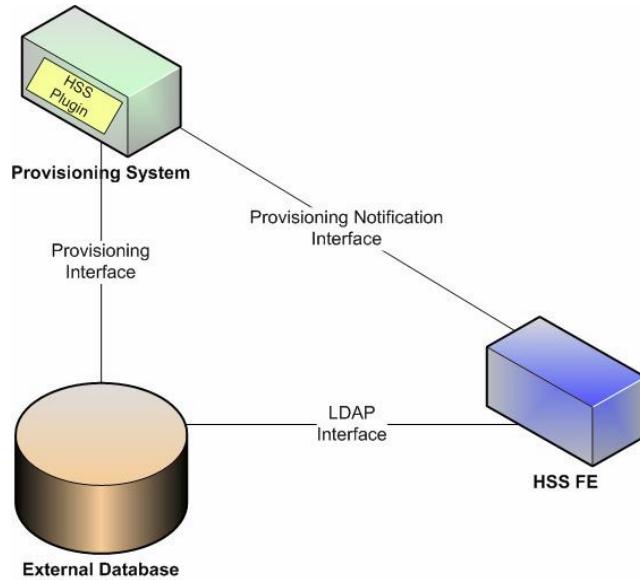
- FEs provide application logic
- FEs are data-less, and hence any FE can attend any request to that application

3) Data Layer (i.e. HSS-FE remote database, where HSS subscription profiles are stored)

- Provides scalable HSS profile data storage.
- High available, including geographic redundancy and persistent data storage of HSS profiles



HSS Front End configuration



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-30

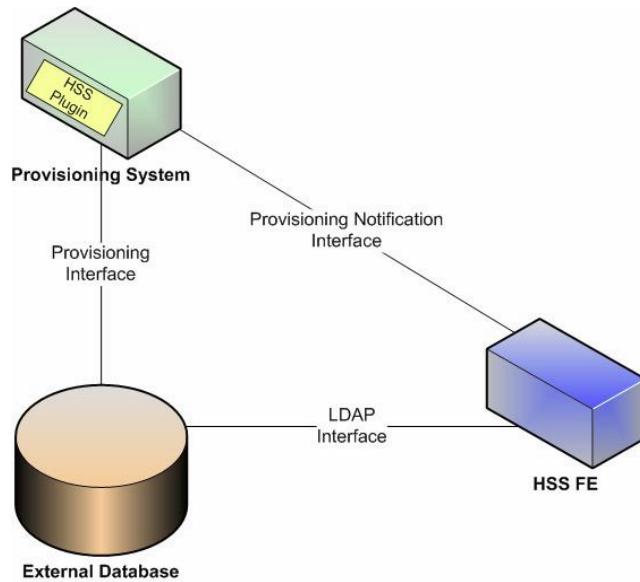
The HSS FE deployment is one of the supported deployment options (the other option is monolithic HSS).

This feature reflects a new realization for the HSS/SLF product, the HSS Front End (HSS FE), which is the entity where the logic of the HSS application resides. The HSS FE is stateless and user data-less. The HSS FE reads subscriber data from a BE-DB to perform the HSS procedures. In the Ericsson portfolio the back end database (BE-DB) is called Common User Data Base (CUDB). This type of configuration applies to every module in HSS, except SLF. The figure shows the HSS FE type of configuration.

Subscribers are stored in a BE-DB instead of the TelORB database. Therefore, subscriber capacity is limited mainly by the capacity of the BE-DB. This allows that the subscriber capacity isn't a limited factor for HSS increasing the performance capacity. As a result of the needed read/write operations to the BE-DB, HSS-FE type of configuration decrements the performance compared to a HSS Classic Deployment.



HSS Front End configuration



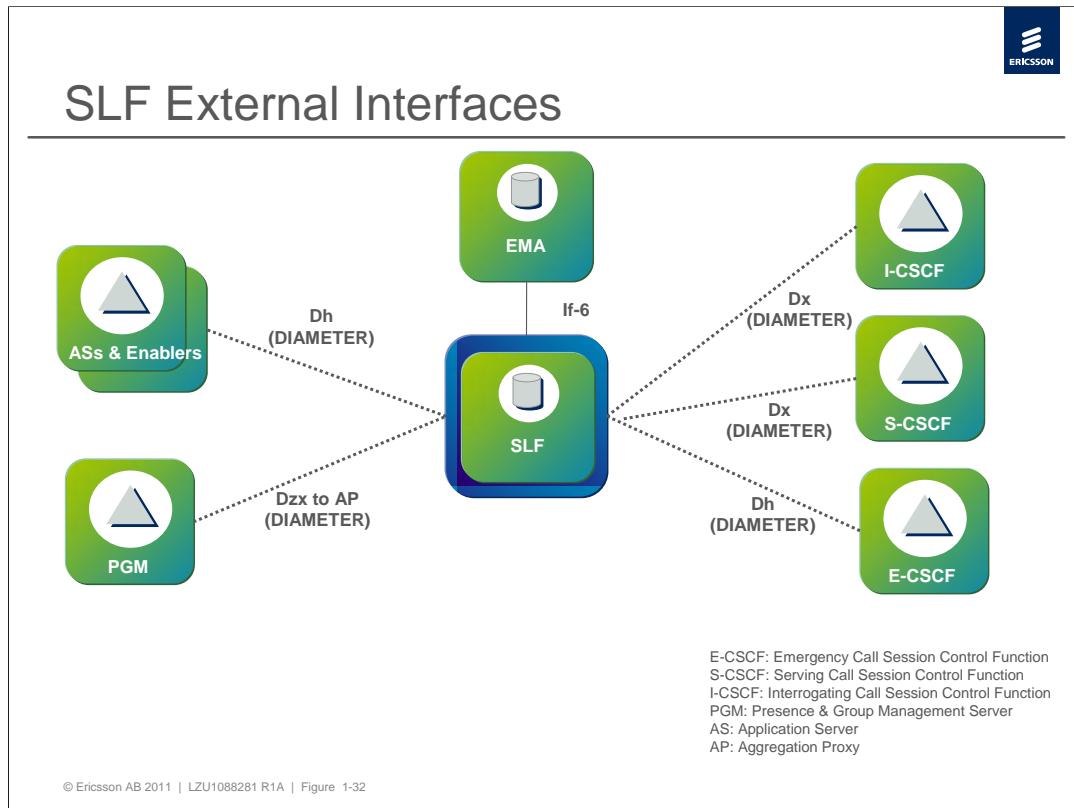
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-31

The External Database is the data repository where related subscriber data is stored. The protocol used for accessing this External Database is LDAP v3 so the External Database needs to be defined as a directory server implementing a given object class data model tree.

The HSS FE type of configuration needs to read subscriber data from the External Database to perform the HSS procedures. HSS FE can be configured to store IMS subscriber data temporarily and reuse them along a network procedure, avoiding frequent search operations to the External Database in a single HSS FE configuration. HSS FE always updates the External Database with any change in subscriber data before answering the received requests, even though these data are involved in a network procedure.

Since some data may be accessed at the same time in different network procedures, a collision detection function is provided in order to avoid data inconsistency in the external database.

OAM interface is heavily impacted. A new object class in each module has been added to manage the external database.



The **Dx interface** is used when more than one HSS node is used. The SLF then returns to the CSCF the name of the HSS that serves the user. Diameter protocol is used.

The **Dzx interface** is used when more than one HSS node is used. The SLF then returns to the AP the name of the HSS that serves the user. Diameter protocol is used.

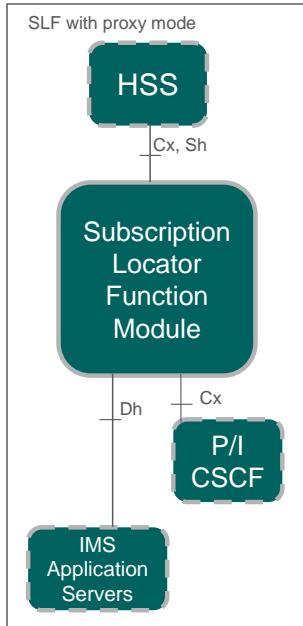
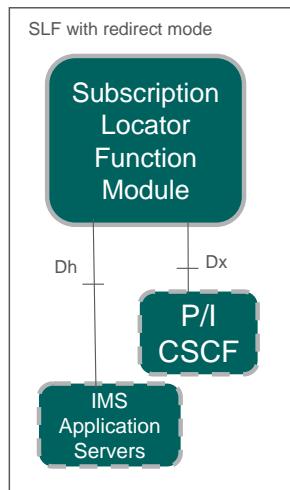
The **Dh interface** is used by when more than one HSS node is used. The SLF then returns to the AS the name of the HSS that serves the user. Diameter protocol is used.

The **If-6 interface** is used between EMA and SLF to provision user data in the SLF. The LDAP protocol is used.

The HSS supports SNMPv3, LDAPv3, IIOP, HTTP, FTP, SFTP and SSH for management access.

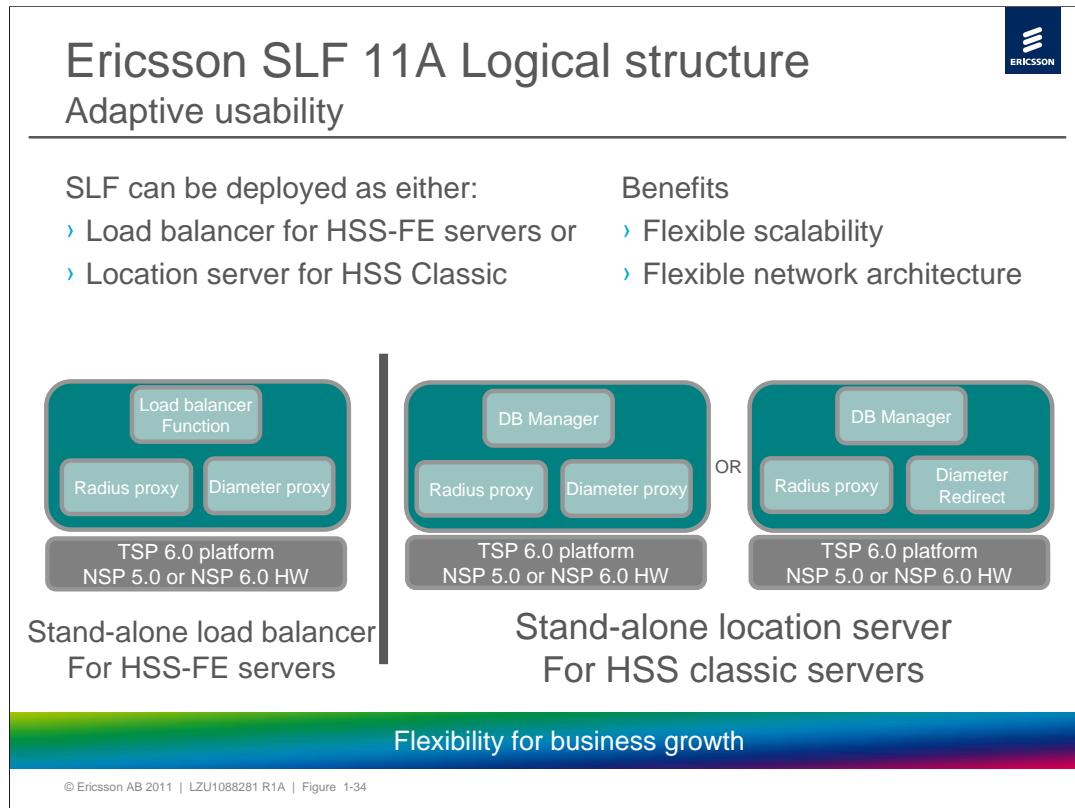
SLF Subscription Locator Function in IMS

- › Scalability when more than one HSS server is used
- › Data management
- › Scalability
- › Network redundant configuration
- › Public service identifiers (PSI)
- › Wildcard PSI
- › Wildcard locator function
- › Domain distributed location
- › DB manager
- › Dynamic load balancer
- › Diameter redirect support
- › Diameter proxy
- › RADIUS proxy



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-33

The SLF module, depending on the selected operational option, can work as a 3GPP Subscription Locator Function (SLF) or as a 3GPP Diameter Proxy Agent in the HSS classic servers deployed for IMS, or as load balancer along with HSS Front-End servers deployed for LTE/EPS and IMS.



The SLF module can be configured in two mutually exclusive distribution modes: as DBManager or as Load Balancer.

DBManager configuration is supported for HSS Classic deployed servers. It handles the association of subscriber identities (i.e. public) to a specific HSS server. SLF redirects or proxies the requests towards the correct HSS node, depending on the selected mode of operation:

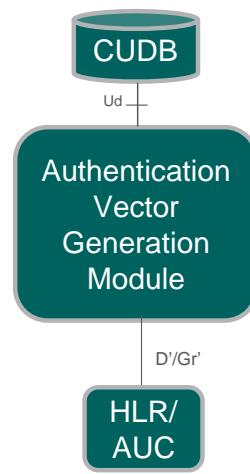
- **Redirect (used in IMS):** This configuration is applicable to the following Diameter interfaces: Dx, Dh and the Ericsson proprietary Dzx. SLF will respond incoming Diameter queries with the location of addressed user identity, when more than one HSS entity exists in the network. This feature implements the 3GPP specified Diameter Redirect routing of HSS Clients. The redirection response provided by SLF includes the identity of the HSS node entity associated to the received public identity received in the request.
- **Proxy (used in IMS and EPC):** This configuration is applicable for the following interfaces: S6a, Cx, Sh, Ericsson proprietary Zx and Gi RADIUS messages towards the appropriate HSS entity, based on identified user location information. For Diameter messages, the resulting response after proxy operation includes the address of the HSS entity selected. If the address of the serving HSS entity is cached, the clients may adopt direct routing for consecutive operation what would lead to a reduction on the SLF capacity.

Load Balancer: SLF supports a dynamic load balancing mechanism based on pre-configured weighted load balancing mechanism improved by dynamically adapting the traffic flow to each HSS-FE according to their load.



Authentication Vector Generation Module

- › Used to serve authentication vectors to any of the following HSS modules:
 - ISM
 - SDA
 - ESM
 - WSM



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-35

HSS AVG module handles the AKA authentication identities and related security data. More specifically, the identities supported by the HSS AVG module include IMSI for USIM ICC users and IMPI for ISIM ICC users. Security data associated to these identities includes the secret subscriber key K.

The secret subscriber key K is defined and stored in ciphered form and the encrypted K (eK) is deciphered only for calculation of the authentication vectors.

HSS AVG module can serve authentication vectors to HSS ISM, HSS SDA, HSS ESM and HSS WSM modules.



Chapter 2 - Architecture

1. Introduction
- 2. Architecture**
3. User Interface
4. Fault Management
5. Configuration Management
6. Performance Management
7. Security, Authentication and Redundancy
8. Session Establishment
9. Configuration Examples



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-36



Telecom Server Platform (TSP)

- › Both CSCF, HSS and SLF are based on Ericsson TSP platform.
- › TSP characteristics include:
 - High system availability
 - Duplicated HW for fault tolerance
 - Scalability: addition of processor boards increases capacity linearly
 - Use of standardised HW components
 - Support for SW upgrades during operation
 - Support for geographical network redundancy
 - Real-time performance

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-37

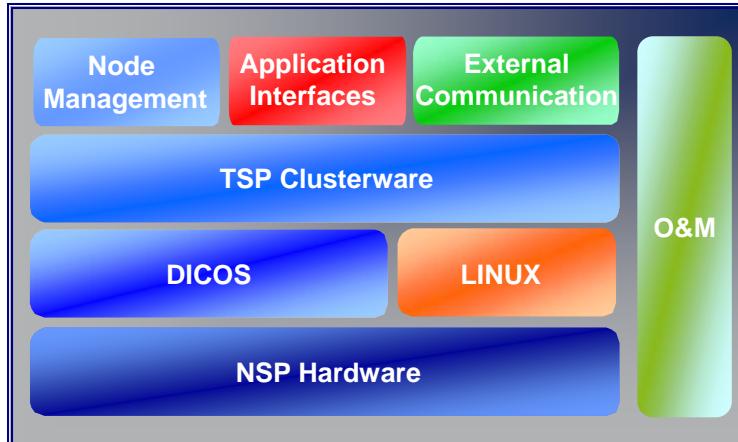
TSP is Ericsson's choice of carrier-class server technology for all new multimedia applications and control functionality. Designed for server solutions where high availability is required, TSP has been introduced in second-generation networks. Networks built with TSP technology enable operators to configure their nodes by packaging different kinds of functionality on the same mechanical structure. In this way, operators can reduce the amount of site equipment and simplify network operation.

TSP is more robust and fault-tolerant than any comparable open server technology. It offers the characteristics listed in the figure above.

TSP is well suited for building small, medium-sized or large systems from the same components and functional units. Being highly scalable, TSP enables operators to expand their networks at the desired rate.



TSP Architecture



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-38

TSP employs a component-based architecture that consists of several functional units within a framework of open interfaces. The component that imparts the special characteristics is TSP Clusterware. Each TSP Processing Module uses one of the two operating systems: Linux or Dicos. The latest TSP releases support the following cluster types:

- Dicos in combination with Linux (“DicosMax”)
- Linux only

Included in the TSP system are state of the art SS7 signalling, a distributed IP-stack and built in node management. The node management includes support for many protocols needed for interoperability between TSP and different Operations and Support Systems (OSS).

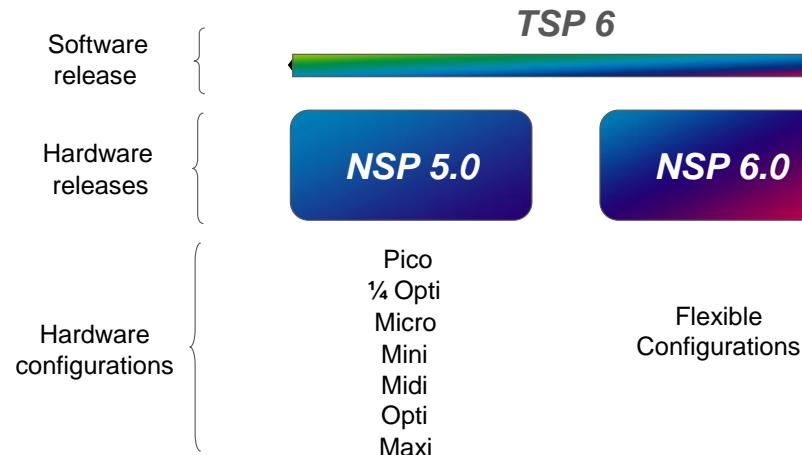
TSP Clusterware is a distributed real time processing environment and is the actual heart of TSP, especially when it comes to traffic and subscriber data management. It proves a robust platform for telecommunications applications.

TSP Clusterware is suitable for controlling telecom applications. It can be loaded onto a group of processors. The group of processors will behave like one single system. Applications can run on top of Clusterware. Different parts of the application can run on different processors. One part can communicate with another in a transparent manner. If there is a need to increase the processing capacity more processors can be added in run-time without disturbing ongoing activities. The increase of the capacity is a linear function of the number of processors; therefore TSP Clusterware is described as a truly scalable system.

The programs that run on the TSP Clusterware are written in C/C++ or Java.



TSP6 Hardware Releases



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-39

TSP is currently based on NSP hardware of different releases.

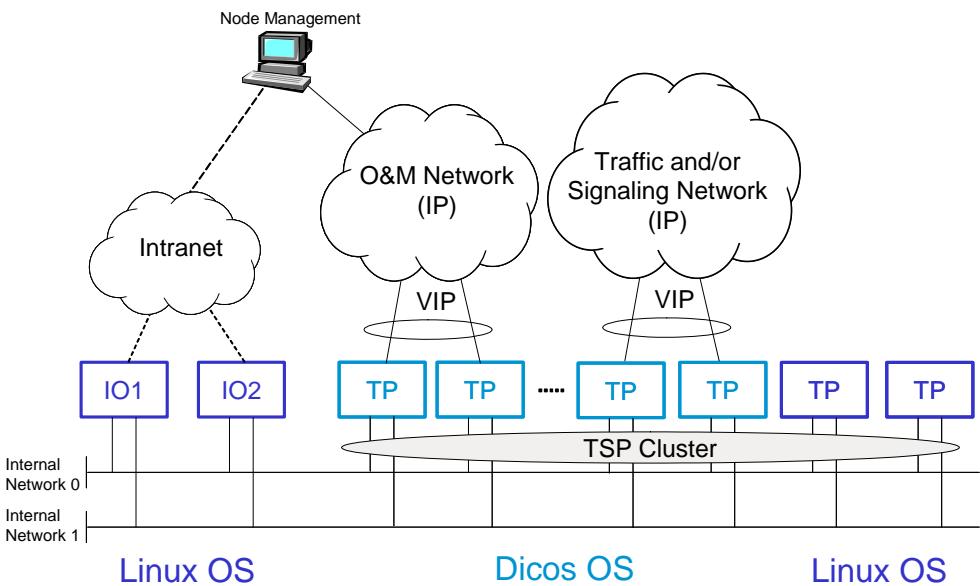
NSP 5.0 is based on Pentium M processors (1.8 GHz) with 2 GB RAM.

NSP 6.0 is based on QuadCore Intel Xeon L5408 processor (2.13 GHz) with 12 GB DDR SDRAM.

For NSP 5.0 hardware there is a limited number of standard configurations listed above.

TSP 6 platform, which is required by HSS/SLF 11A, can be deployed on top of NSP 5.0 or NSP 6.0. For new installation NSP 6.0 is used.

TSP hardware and external connections



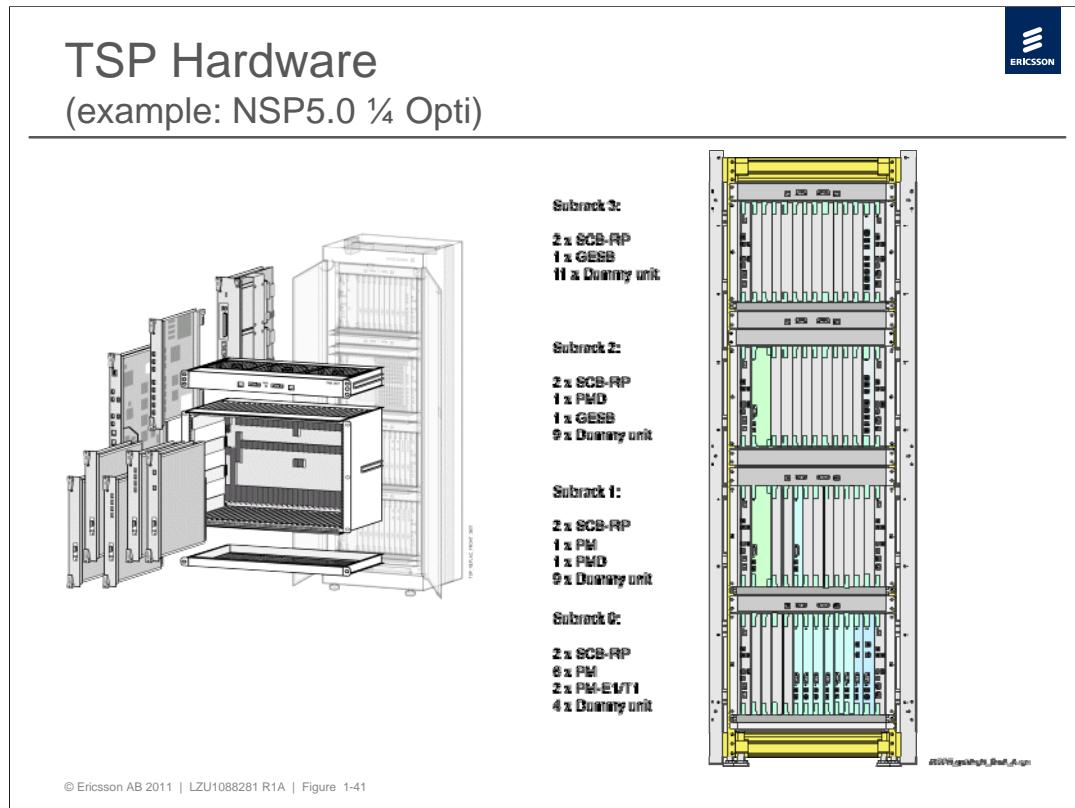
The TSP hardware platform is based on commercially available hardware with high capacity and dependable node performance. Use of standard HW means low costs for installation, operation and maintenance.

The hardware platform includes IO (input/output) modules, hard drive modules (NSP6), processor modules with their peripherals, ethernet switches, power supplies and fans. NSP6.0 allows up to 6 x 300 GB SAS disk boards to store all executable units needed for start-up and backup and for application data. The internal processor communication takes place on a duplicated 10/100 Mbps Ethernet bus. The processors are hot swappable.

Both Linux and Dicos can support connections towards external IP networks, e.g. O&M and traffic networks. TSP is using the VIP (Virtual IP address) concept for external IP connections. Each application in the TSP (for example HSS) needs to have its own VIP as well as the O&M function.

TSP Clusterware among other things facilitates communication between different processes that execute on different processors. The lightweight protocol IPC (Inter Process Communication) is used for this communication.

It is also possible to connect to the IOs for IO management purposes like upgrade and correction package handling as well as to perform external backup of the IOs.



The hardware in TSP is implemented using GEM (Generic Ericsson Magazine) hardware.

GEM, is a generic platform component used in several products. GEM is a high-capacity, flexible and scalable magazine in which several functions can be combined. This means that considerably fewer magazine and board types are needed in each node.

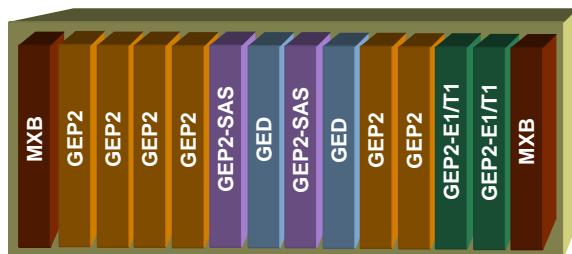
The use of standard switch boards, such as Ethernet, makes the GEM an open magazine prepared for future developments. By basing all the technologies on the same building practice, Ericsson can use common mechanical components and common control processors, Ethernet switches and interface boards. At a site installation, this gives operators the advantage of having one cooling system, one power supply system, and uniform alarm system handling.

The GEM concept can be used to build anything from a small node to a very large one, using the same types of board and magazine. As capacity requirements grow, operators can add one or more GEMs with a suitable combination of devices, thereby smoothly extending the node without interruption of traffic.

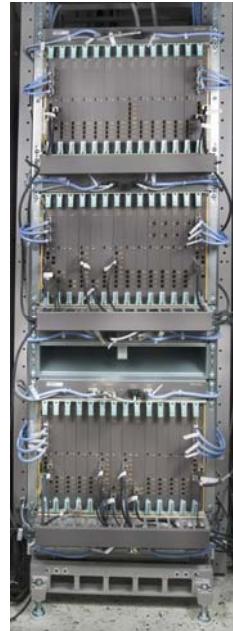
Via the GEM backplane all plug-in units are provided with dual - 48V power, duplicated 10/100 Ethernet and a maintenance bus. This causes the elimination of many cables, resulting in a very compact system.



TSP Hardware (example: NSP 6.0)



- › MXB
- › GEP2
- › GEP2-SAS + GED
- › GEP2-E1/T1



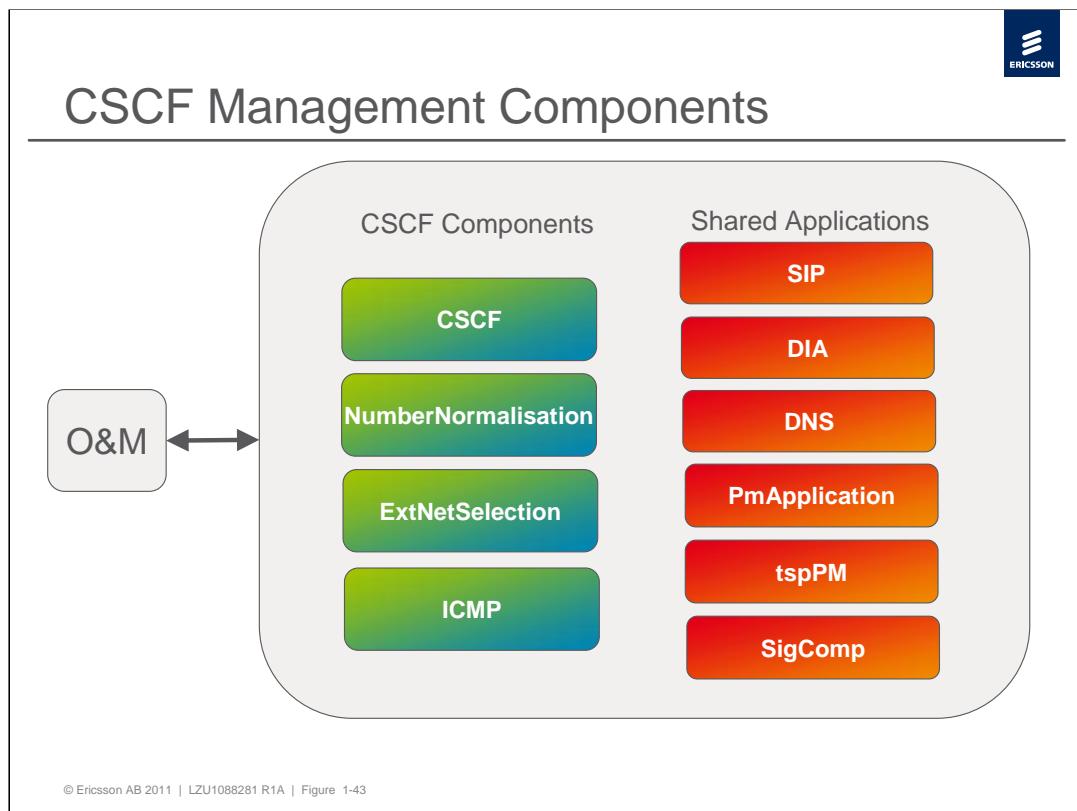
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-42

The NSP 6.0 consists of one BYB 501 cabinet, equipped with up to three EGEM subracks. The doors can be locked. Mounting kits for high earthquake risk areas are available.

The different processor types are all based on the same processor board. Their different roles are:

- Traffic processor
- Loader
- Node management
- IO, controlling a GED disk board
- File server, controlling a GED disk board

For more information, please see NSP 6.0 Hardware Description



The figure shows the simplified internal interworking architecture between the CSCF component and other TSP based components.

The names in the figure are the same as the system defined names (ApplicationName) used when accessing the components via LDAP browser for configuration management.

NumberNormalisation and ExtNetSelection are only interworking with the S-CSCF component and can be regarded as sub-components to the CSCF. The other components in the figure interwork with other applications as well.

The S-CSCF, I-CSCF, P-CSCF and E-CSCF components implement the 3GPP and 3GPP2 specific functionality of the respective logical entities which means that they can be co-located on one TSP or stand alone on several TSPs.

NumberNormalisation implements the Number Normalization function which converts local telephone numbers and national numbers to fully internationalized numbers.

ExtNetSelection implements a simplified BGCF function in order to route a session to an external network (PSTN or H.323) based on the A-number, B-number, RN or CIC parameter.

SIP implements the SIP stack as specified by RFC 3261.

SigComp specifies a signaling compression mechanism of requests and responses specified in RFC 3320.

DIA implements the Diameter stack used for HSS (Cx), SLF (Dx) and charging (Rf) communication.

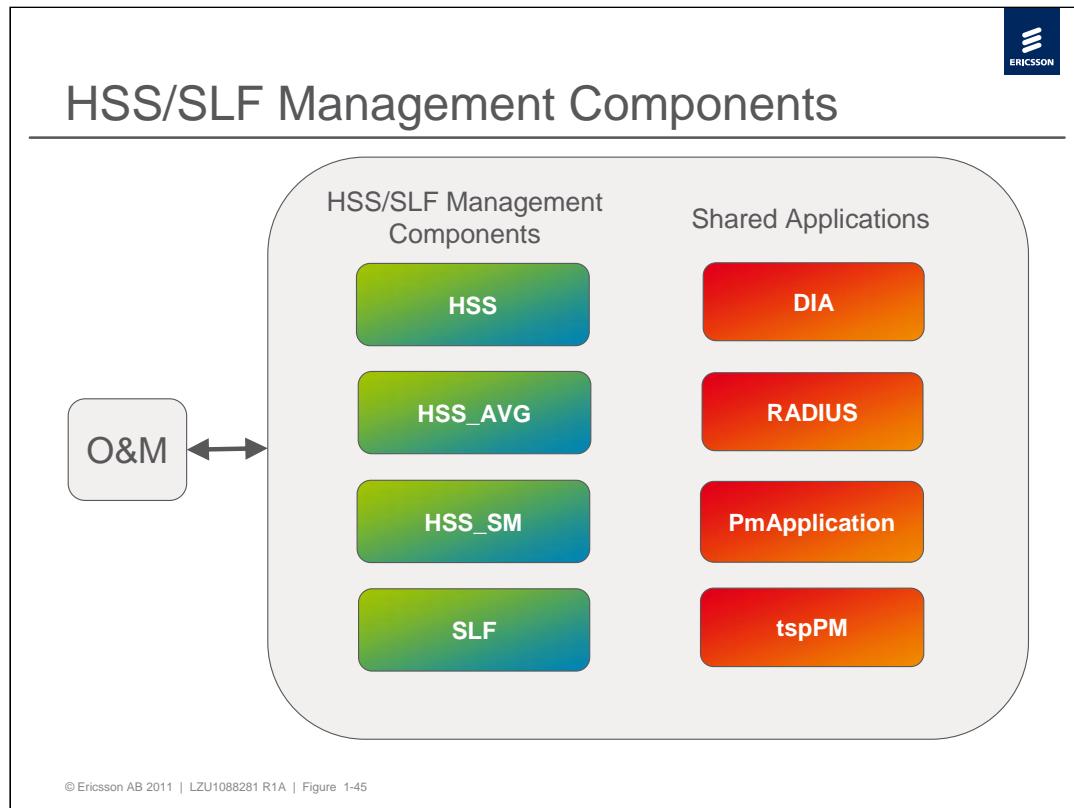
DNS implements the interface towards ENUM/DNS.

PmApplication provides applications/components with a single framework to report and manage performance measurements.

ICMP provides the possibility to handle communication problems with gateways/hosts.

tspPM provides applications/components with an improved framework to report and manage performance measurements.

All the components interact with the O&M component.



The figure shows HSS/SLF Management components which are relevant for the IMS implementation.

The names in the figure are the same as the system defined names (ApplicationName) used when accessing the components via LDAP browser for configuration management.

HSS components implement the 3GPP and 3GPP2 specific functionality of the respective logical entities, it includes ISM and SDA.

HSS_AVG implements Authentication Vector Generator module of HSS/SLF.

HSS_SM implements an ISM Session Manager module that provides a support for Single-Sign-On authentication mechanism in HSS

SLF implements Subscription Locator Function module of HSS/SLF.

DIA implements the Diameter stack used for HSS (Cx), SLF (Dx) and charging (Rf) communication.

RADIUS implements the RADIUS stack and configurations for communication with a Network Access Server (e.g. GGSN)

PmApplication provides applications/components with a single framework to report and manage performance measurements.

tspPM provides applications/components with an improved framework to report and manage performance measurements.

All the components interact with the O&M component.



Chapter 3 – User Interface

1. Introduction
2. Architecture
- 3. User Interface**
4. Fault Management
5. Configuration Management
6. Performance Management
7. Security, Authentication and Redundancy
8. Session Establishment
9. Configuration Examples

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-46





TSP Node Management Toolbox

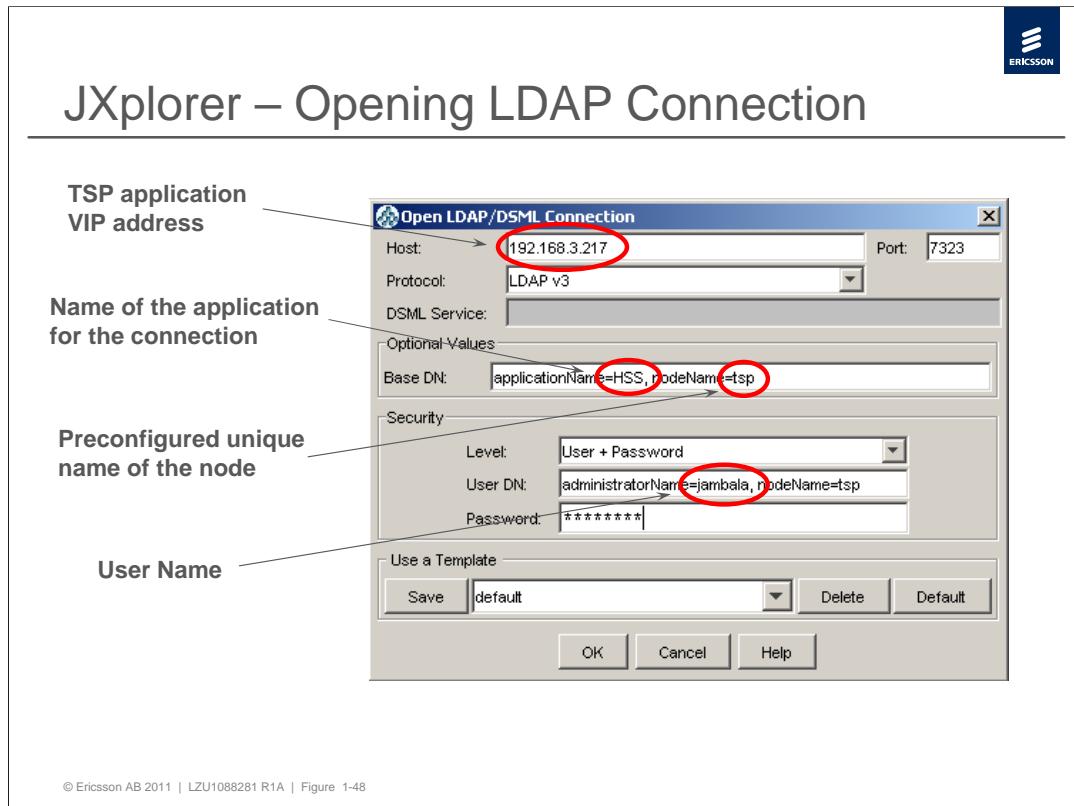
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-47

TSP contains an embedded web based user interface that allows the remote monitoring and configuring of the node through a web browser. This management interface is called **Node Management Toolbox** and is described in the CPI document, *Node Management Toolbox User Guide*. Alarms and notifications are viewed via the Fault Management part of the toolbox.

The **TelORB Manager** is available from the Node Management Toolbox and it is described in the CPI, *TelORB Manager*. TelORB Manager includes the user interfaces for Inventory, Upgrades and Backup together with tabs for platform specific configuration tasks.

TSP supports a common configuration and provisioning interface conforming to Lightweight Directory Access Protocol (LDAP). The **CM Browser** is the recommended but not mandatory LDAP browser that is available from the Node Management Toolbox. The CM browser is used to connect to the different applications for configuration management.

JXplorer is used as the CM Browser in TSP. JXplorer is an open source Java application that allows you to browse and search any LDAP directory. It uses Java 1.4 (or better) and supports LDAP v3 (RFC 2251).



The figure shows the JXplorer screen for opening an LDAP connection towards the HSS application.

There are a number of fields that needs to be filled in.

The **Host** field should be filled in with the TSP VIP address or alias. VIP is a shared IP address that can be used to address distributed functions in the TSP node.

The Jambala Information Manager (JIM) manages objects in the TSP DBN database. It presents a hierarchical view of the data, where each Managed Object is uniquely identified by its place in the hierarchy.

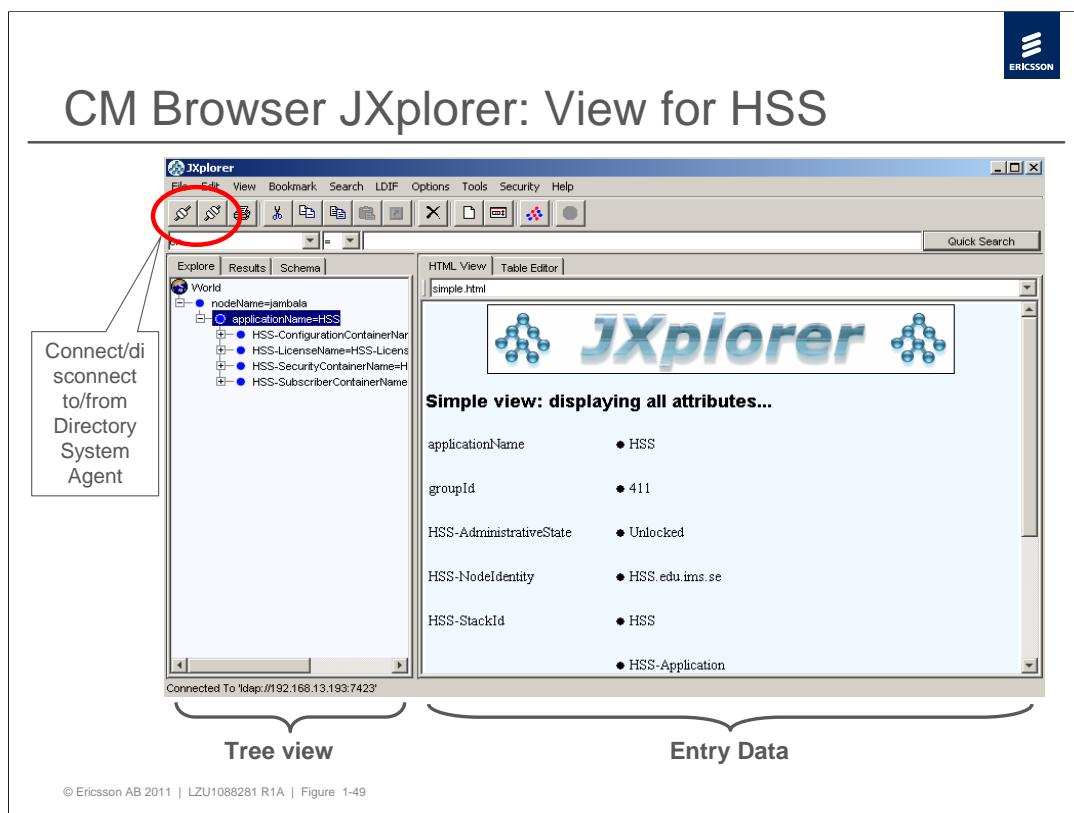
In the object hierarchy there are predefined objects. At the root of the MO hierarchy is the node object that represents the system. The children of the root node are the application nodes.

In the figure the **nodeName** represents the root node and in this example it has the name *jambala*.

The children of the root node are the application nodes, in the figure a connection towards the HSS application is done by giving the **applicationName** the value *HSS*. The nodeName and the applicationName makes up the DN (Distinguished Name) which is unique.

To login, user and password needs to be given, which normally are the same as for logging in to the toolbox.

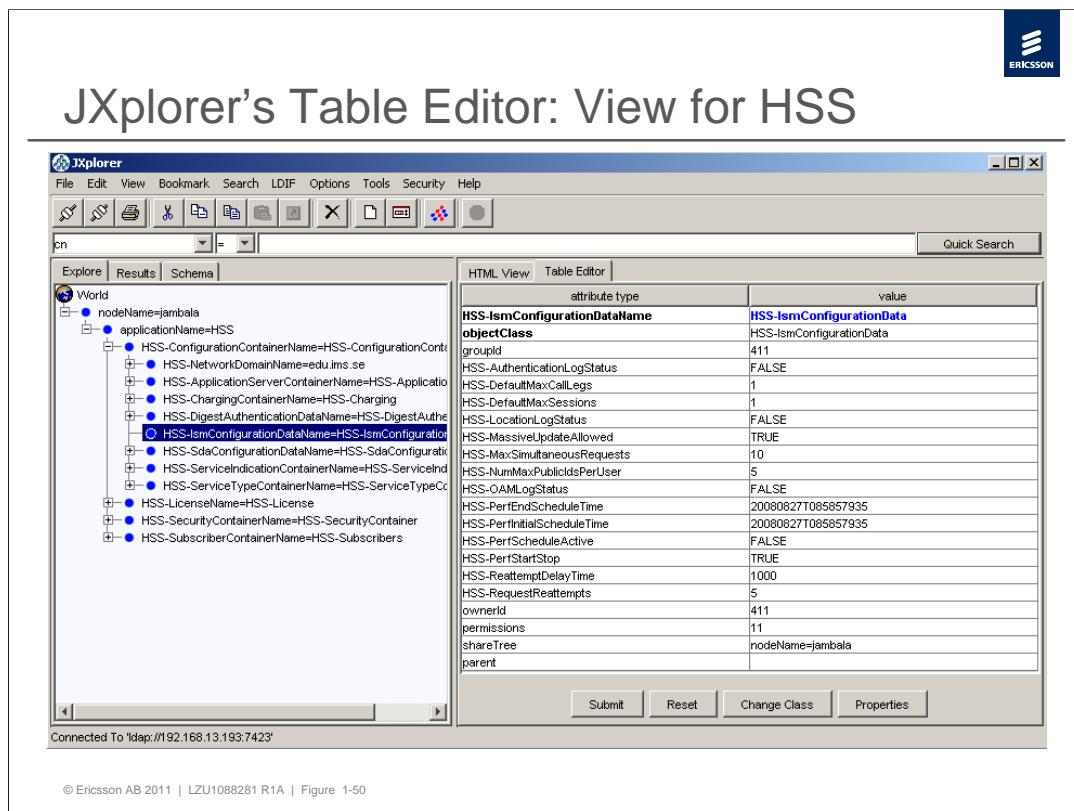
The login details can then also be saved as a template.



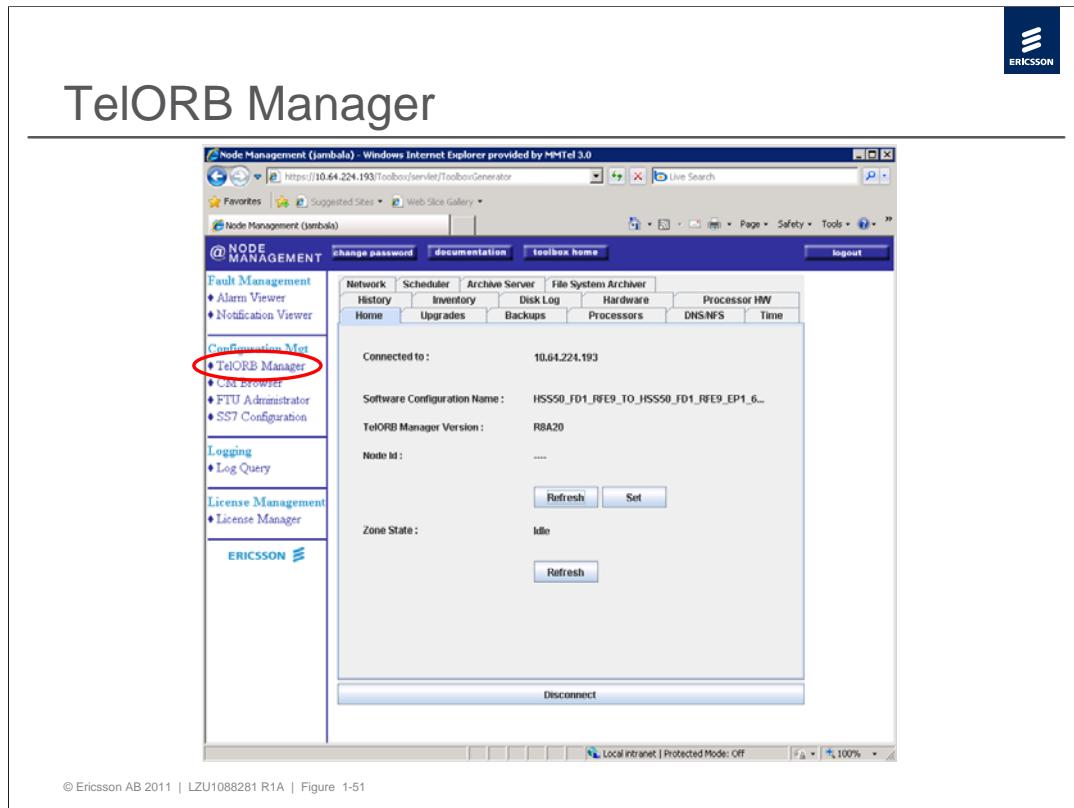
The figure shows the JXplorer view for the HSS.

It displays the structure of the directory data as a tree view in the left panel, and the data of any particular entry in the right hand pane.

The Table Editor is used to change the data for an entry.



The figure shows the Table Editor view for HSS.



The **TelORB Manager** is available from the Node Management Toolbox and it is described in the CPI, *TelORB Manager*. TelORB Manager includes the user interfaces for Inventory, Upgrades and Backup together with tabs for platform specific configuration tasks.



Chapter 4 – Fault Management

1. Introduction
2. Architecture
3. User Interface
- 4. Fault Management**
5. Configuration Management
6. Performance Management
7. Security, Authentication and Redundancy
8. Session Establishment
9. Configuration Examples

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-52





CSCF Alarms

› Critical

- CSCF Mandatory Data Not Configured
- CSCF SIP Interface Already Used
- CSCF SIP Interface Not Operational
- CSCF Credit Control Answers Indicate End User Service Denied
- E-CSCF Mandatory Data Not Configured
- BCF Mandatory Data Not Configured

› Major

- CSCF SIP Interface Reduced Capacity
- CSCF Charging Answers Indicate Protocols Errors
- CSCF Charging Answers Indicate Permanent Failures
- CSCF Charging Request Transmission Problem
- CSCF Charging Backup File System Unavailable
- CSCF Credit Control Answers Indicate Permanent Failures
- CSCF Credit Control Answers Indicate Protocol Errors
- E-CSCF Receives No LRF Response
- CSCF Degraded HSS Redundancy
- CSCF ENUM Responses Resulting In Malformatted RN
- CSCF ENUM Responses Resulting In Malformatted CIC

› Minor

- CSCF User Subscriber Media Profile Id Not Defined
- CSCF SIP Request Timed Out
- CSCF ICMP Protocol Not Operational

› Warnings

- CSCF Application Locked For Maintenance
- CSCF Application Shutting Down
- P-CSCF Rejected Messages On Unprotected Server Port

Threshold alarms, related to Performance Management Counters, are also possible.

See also CPI "CSCF Troubleshooting Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-53

Alarms regarding to CSCF are detected within the sub-system of applications and reported to the TSP platform Fault Management System, where the alarms are logged. The information about the detected alarms are displayed to the Alarm Viewer and sent to the SNMP and 3GPP IRP CORBA alarm gateways. The tool Alarm Viewer is found in the Node Management Toolbox..

In the figure the alarms specifically connected to the CSCF application are listed. TSP platform alarms can of course affect the CSCF as well.

The CSCF alarms are of either Critical or Major or Minor or Warning severity.

The CPI document *CSCF Fault Management Parameters* describe the alarms. It is found in ALEX.



HSS Alarms: ISM

› Critical

- Installation, Application Failed to Start in ISM

› Minor

- Authentication, User Locked in ISM
- Performance, TotalNumberOfUserPublicIdPairsStored in ISM
- Performance, IsmMapAtiTimeoutResponses in ISM
- Performance, IsmMapSaiTimeoutResponses in ISM

› Warnings

- Administrative State, Shutting down in Progress for ISM/SDA
- Administrative State, Manually Locking for ISM/SDA

See also CPI "ISM Fault Management Configuration Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-54

Alarms regarding to HSS are detected within the sub-system of applications and reported to the TSP platform Fault Management System, where the alarms are logged.

The information about the detected alarms are displayed to the Alarm Viewer and sent to the SNMP and 3GPP IRP CORBA alarm gateways. The tool Alarm Viewer is found in the Node Management Toolbox.

In the figure the alarms specifically connected to the ISM module of HSS are listed. TSP platform alarms can of course affect the HSS as well.

The ISM alarms are of either Critical, Minor or Warning severity.

The CPI document *ISM Fault Management Configuration Guide* describes the alarms. It is found in ALEX library.



HSS Alarms: SM and AVG

› Critical (SM and AVG)

- Installation, Application Failed to Start in SM
- Installation, Application Failed to Start in AVG

› Warnings (SM)

- Administrative State, Manually Locking for SM
- Administrative State, Shutting down in Progress for SM
- Session Information, SGSN MCC-MNC not Available in SM

See also CPI: "SM Fault Management Configuration Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-55

In the figure the alarms specifically connected to Session Manager and Authentication Vector Generator modules of HSS are listed.

The Session Manager alarms are of either Critical or Warning severity while AVG only has one Critical alarm.

The CPI documents *SM Fault Management Configuration Guide* and *AVG Fault Management Configuration Guide* describe the alarms. They are found in ALEX library.



HSS Alarms: SDA

› Critical

- Installation, Application failed to Start in SDA

› Minor

- Performance, TotalNumberOfApplicationServersStored in SDA
- Performance, SdaMapAtiTimeoutResponses in SDA

› Warnings

- Administrative State, Shutting down in Progress for ISM/SDA
- Administrative State, Manually Locking for ISM/SDA

See also CPI “SDA Fault Management Configuration Guide”

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-56

In the figure the alarms specifically connected to the SDA submodule of HSS are listed.

The SDA alarms are of either Critical, Minor or Warning severity.

The CPI document *SDA Fault Management Configuration Guide* describes the alarms. It is found in ALEX library.



SLF Alarms

› Critical

- Installation, Application Failed to Start in SLF

› Warnings

- Communication, HSI Server Information Unavailable
- Administrative State, Manually Locked Completed for SLF
- Administrative State, Shutting down in Progress for SLF

See also CPI "SLF Fault Management Configuration Guide"

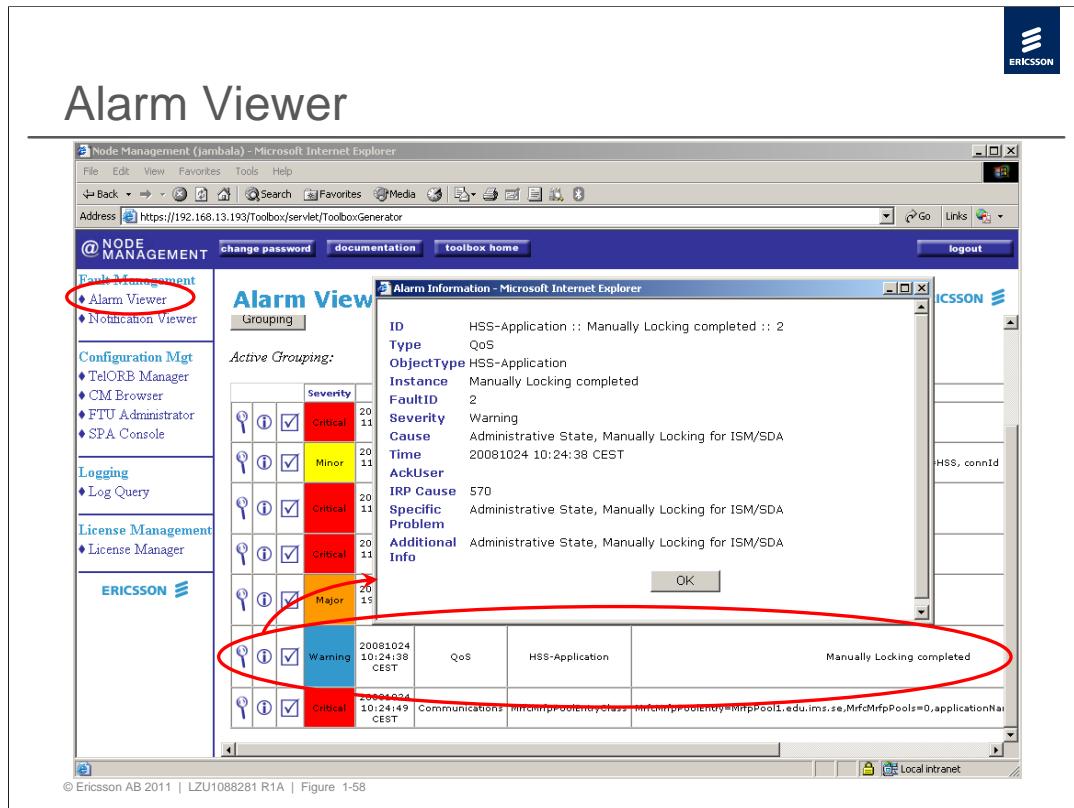
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-57

Alarms regarding to SLA are detected within the sub-system of applications and reported to the TSP platform Fault Management System, where the alarms are logged.

In the figure the alarms specifically connected to the SLF are listed. TSP platform alarms can of course affect the SLF as well.

The SLF alarms are of either Critical or Warning severity.

The CPI document *SLF Fault Management Configuration Guide* describes the alarms. It is found in ALEX library.



The figure shows the *Administrative State, Manually Locking for ISM/SDA* alarm and the alarm details.

The alarms connected to ISM have one of the following object types:

- HSS
- ISMInstaller
- HSS-Application
- HSS-User

The alarms connected to ISM Session Manager have one of the following object types:

- AAA
- AAA-AccountingService
- AAA-AppData

The alarms connected to SDA have one of the following object types:

- HSS
- HSS-Sh
- HSS-Application
- SDAInstaller

The alarms connected to SLF have one of the following object types:

- SLF
- SLFInstaller
- SLF-ConfigurationData



System Logs

Type of log	Contents of the log file	Location in the file system
Dicos system log, syslog	This is the log for the platform events.	/opt/telorb/axe/tsp
Traffic processors' console logs, Proc_mX_sX	The data stream from each processor is dumped into size-limited console log files.	/opt/telorb/axe/tsp/consolelogs
Application logs, applog.DIAMETER applog.OAM_Log_Message etc.	Applications send log messages to an applog-client and then into a file on the IO machines. Messages are time-stamped.	/opt/telorb/axe/tsp/applog
PMF logs, AyyyyMMdd.hhmm-hhmm_<name>	The log file where Performance Management data is logged in XML format in the end of scan period.	/opt/telorb/axe/tsp/NM/PMF/reporterLogs

All log files are found on the IO processors

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-59

HSS provides log events for faulty situations that might occur in the system. It is one of the most helpful tools to locate the source of a problem, available in a graphical interface included in the Node Management Toolbox. The HSS and SLF Log files can be found in the Application Log (applog).

Three different types of logging information are provided by ISM:

- Services Log
- Authentication Log
- Operation and Maintenance Log

Three different types of logging information are provided by the Session Manager functions:

- Application Log
- RADIUS Log
- Tracing Log

Three different types of logging information are provided by SDA:

- Services Log
- Operation and Maintenance Log

Three different types of logging information are provided by SLF:

- SecurityLog
- DIAMETER Log
- Operation and Maintenance Log



Error dumps and Crashcollector

Type of info	Contents	Location in the file system
Error Dumps Ex: DicosCapsuleText.. ..Dump.172.16.0.9-1	Error dump files are generated If there is a crash or a failure in a processor or a process.	/var/log/dumps
Crashcollector, crashcollector_<date>_<time>.. .._Proc_mX_sX.tar.gz	Due to the creation of error dump the following files are collected and "tarred" into the crashcollector file: error dump(s), syslog, traffic processors' console logs and traffic processors' kernel configuration.	/opt/telorb/axe/tsp/crashcollector/

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-60

Error Dumps and CrashCollector:

Another type of logging mechanism is the error dump mechanism. This mechanism creates Error Dump file on the IO processors in the case of a process crash or a traffic processor crash. Each dump contains a register dump and a call chain that give information about the execution flow. Dump files should be trouble reported to the local Ericsson Support Organization.

The Crash Dump files are compressed into a CrashCollector file together with all the TSP platform logs and traffic processors configuration files. The CrashCollector file should be sent to the local Ericsson Support Organization for analysis.

The screenshot shows a web browser window with the URL <https://192.168.3.221/Toolbox/servlet/ToolboxGenerator>. The page title is "The Logging Query Tool". The left sidebar menu under "@ NODE MANAGEMENT" includes "Fault Management" (with Alarm Viewer and Notification Viewer), "Configuration Mgt" (with TelORB Manager, CM Browser, and FTU Administrator), "Logging" (with Log Query circled in red), and "License Management" (with License Manager). The right side of the interface shows a large, open server rack diagram.

See also CPI "Logging Query Tool User Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-61

TSP as a platform provides its applications with a logging framework that allows them to log the events into an SQL database. The logging database is presented by the **Logging Query Tool** graphical user interface.

The tool is reachable from the TSP Node Management toolbox as shown in the figure.

The tool is described in the CPI *Logging Query Tool User Guide*.



Database Selection

The screenshot shows the Node Management interface. At the top, there are links for 'change password', 'documentation', and 'toolbox home'. The main menu on the left includes 'Fault Management' (with 'Alarm Viewer' and 'Notification Viewer'), 'Configuration Mgt' (with 'TelORB Manager', 'CM Browser', and 'FTU Administrator'), 'Logging' (with 'Log Query' circled in red), and 'License Management' (with 'License Manager'). A message in the center says 'Please select a database :'. Below it are two radio buttons: one selected for 'Current(logging)' with a 'Select' button next to it, and another for 'Backup(backup)'. The Ericsson logo is at the bottom right of the interface.

See also CPI "Logging Query Tool User Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-62

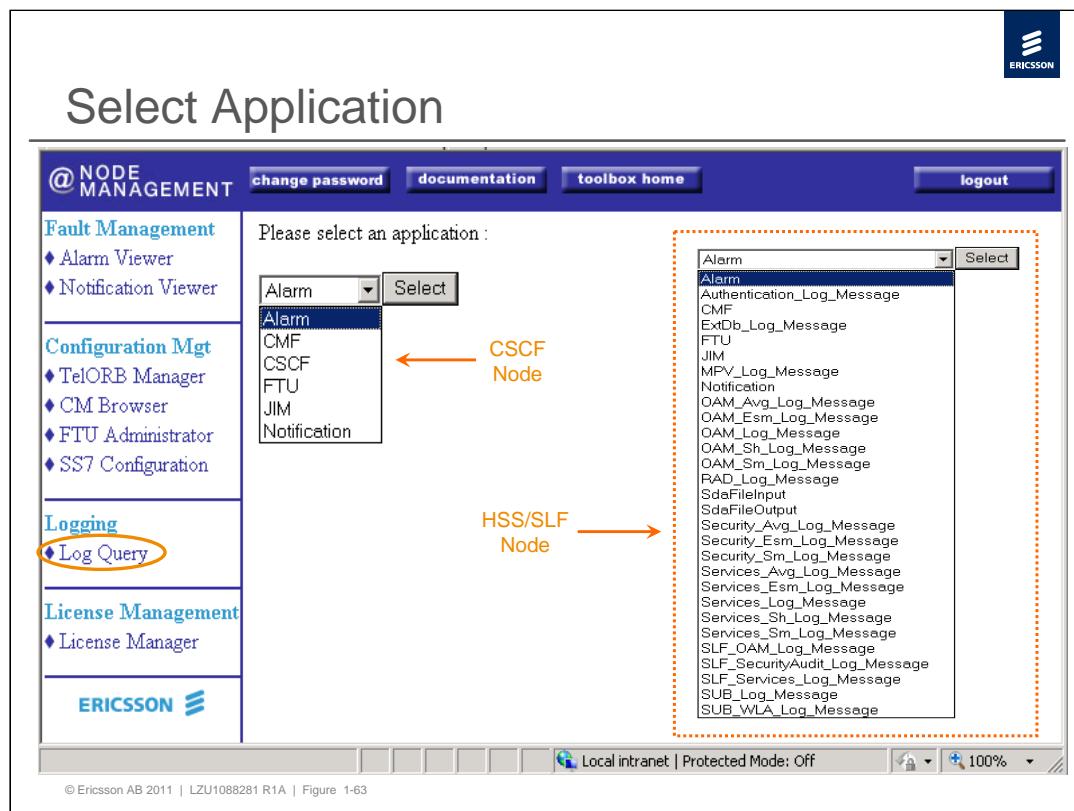
A selection between two databases has to be done, Current or Backup.

The active Logging Database (Current in the figure) is targeted to store a few days of log history. The default value is 4 days but it can be changed, see CPI *Logging User Guide*.

The Logging Database has to be archived regularly. The archiving is automatically initiated every day at a predefined time (default 00.00). The records that are older than a given number of days (e.g. 4) are moved to the archive.

Archive files can be loaded back into the so called Backup Database in order to become visible for the Logging Query Tool. How to load the archive files into the Backup Database is also described in the *Logging User Guide*.

When the archive files are loaded into the Backup Database they can be viewed by selecting Backup in the figure above.



The logging database contains as many tables as the number of used logtypes. Every logtype contains the TelorbDate field which holds the time and date when the log was created.

The platform itself provides the following logtypes:

Alarm - All alarms are logged.

(See CPI: *Fault Management User Guide*)

Notification - All notifications are logged.

(See CPI: *Fault Management User Guide*)

JIM and CMF - This logtype describes the configuration and provisioning events.

(See CPI: *Configuration Management User Guide*)

Applications have their own logtypes. On the left side of the figure, the typical options for a CSCF node are showed. In case of a HSS/SLF node, a typical list of the applications would be instead the one on the right side of picture.

The screenshot shows a web-based management interface for CSCF 11A HSS/SLF 11A. At the top, there's a navigation bar with links for 'change password', 'documentation', and 'toolbox home'. Below the navigation bar is a sidebar with several sections: 'Fault Management' (Alarm Viewer, Notification Viewer), 'Configuration Mgt' (TelORB Manager, CM Browser, FTU Administrator), 'Logging' (Log Query, which is circled in red), and 'License Management' (License Manager). The main area contains a table with search criteria fields. The table has columns for the field name and its value, with a checked checkbox column. Fields include additionalText, typeName, domainName, TelorbDate, perceivedSeverity, notificationId, probableCause, ackUserId, alarmId, ackState, managedObjectClass (set to CSCF), managedObjectInstance, and specificProblem. Below the table are buttons for 'Criteria' (dropdown set to [private] test), 'Load', 'Delete', and 'Save as...'. There are also dropdowns for 'Sorted by' (set to TelorbDate) and 'Descending' (radio button selected), and a 'Results per page' input field (set to 5). A checkbox 'Show results in a new window' is unchecked. At the bottom, there are links for 'Select application' and 'Help'.

The figure shows the possible search criterias for the alarm logtype. In the figure a search is done for alarms concerning CSCF. The actual criteria can be saved as a filter by pressing the *Save as* button and later loaded using the *Load* button.

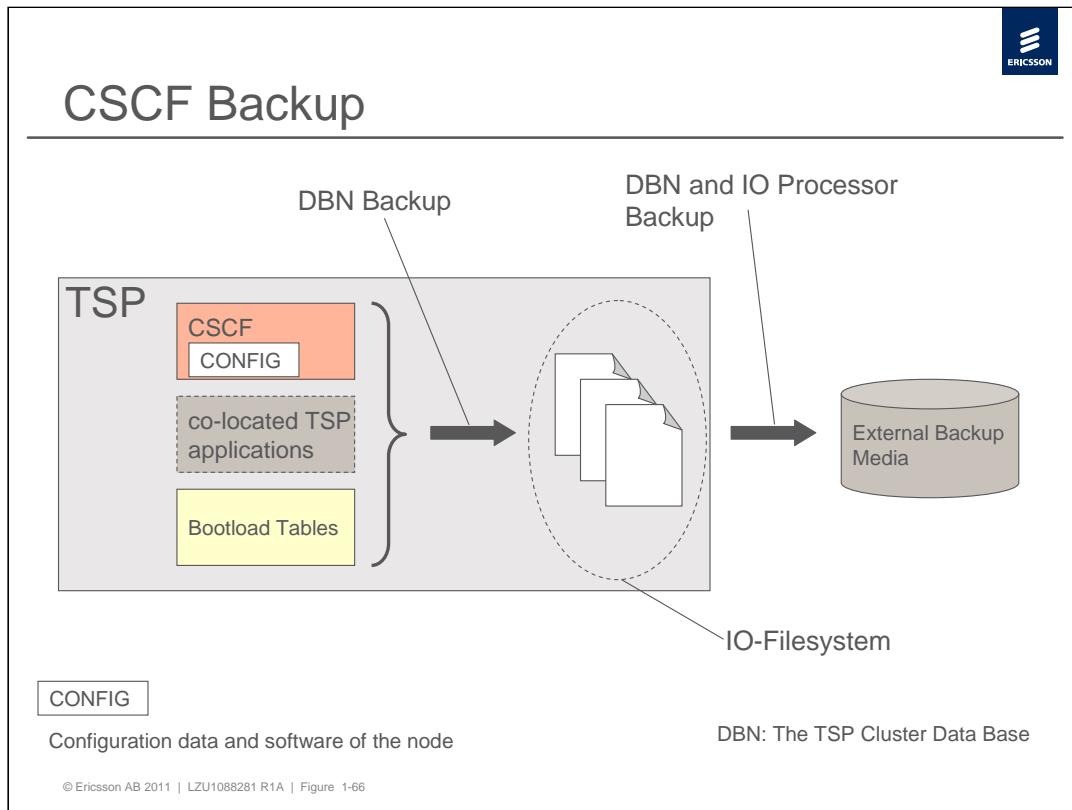


Chapter 5 – Configuration Management

1. Introduction
2. Architecture
3. User Interface
4. Fault Management
- 5. Configuration Management**
6. Performance Management
7. Security, Authentication and Redundancy
8. Session Establishment
9. Configuration Examples

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-65





Since the CSCF runs on the TSP platform it is backed up as part of a TSP backup.

DBN backup

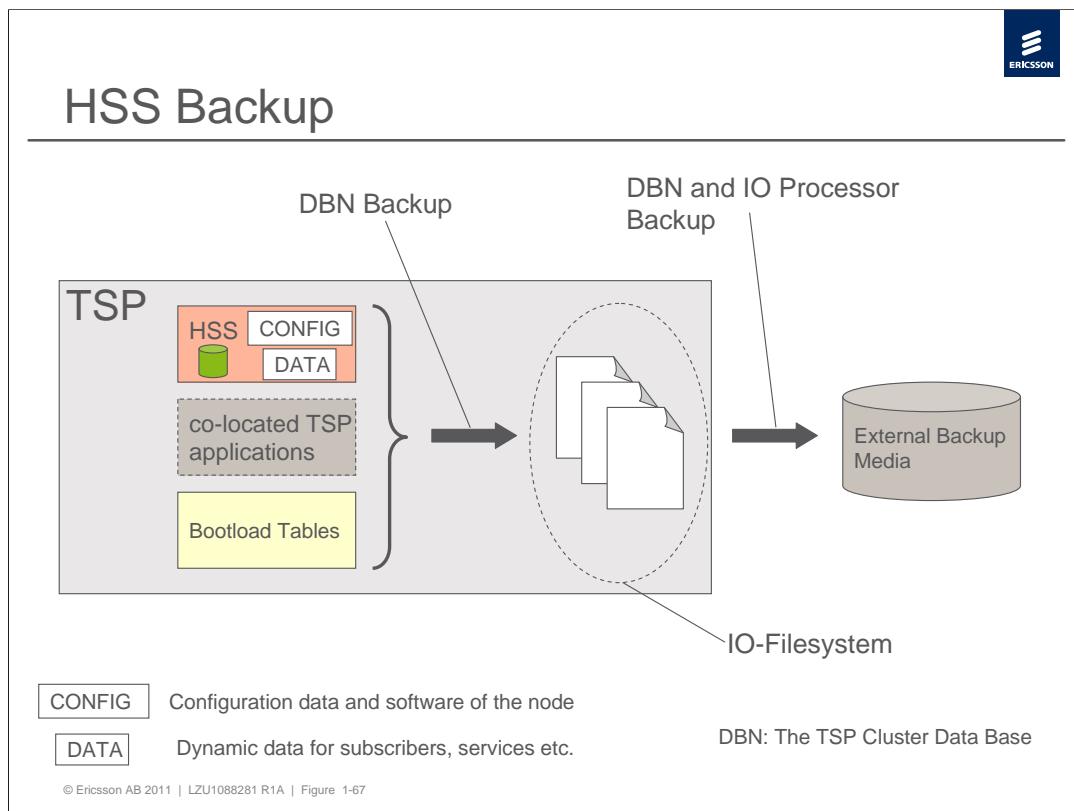
The DBN backup consists of the cluster database (i.e. the CSCF configuration data) and the bootload tables for the traffic processors. The DBN backup can be handled through the Telorb manager and is stored in backup files on the hard discs of the IOs.

DBN database backups can be configured to be taken automatically at predefined intervals or predefined times.

Creating a DBN backup causes no significant degradation in the system performance, because the backup runs in the background. Depending on the application and the amount of data in the database, a backup can take from 5 minutes up to one hour.

IO backup

The backup procedure takes a backup of all TSP specific data currently stored on the IO processors, that is the data on the (shared) safe file system. This backup can be used to restore the IO processors in the case of serious IO faults.



Since the HSS runs on the TSP platform it is backed up as part of a TSP backup.

DBN backup

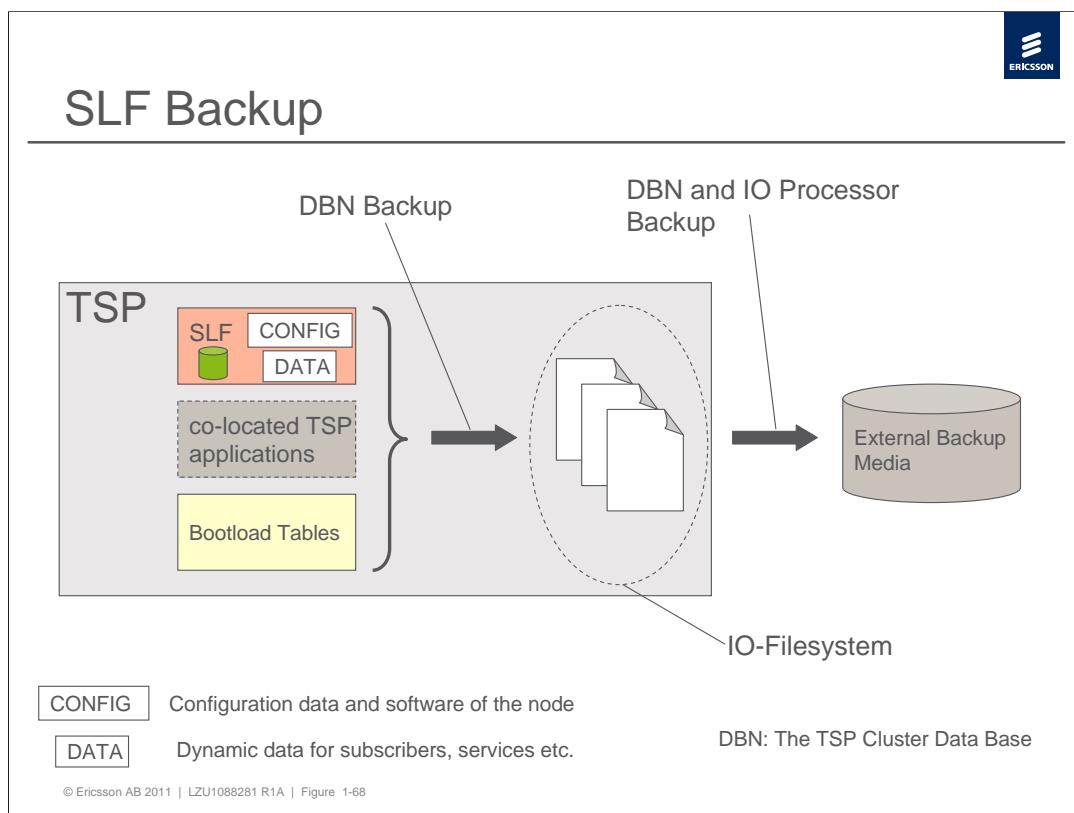
The DBN backup consists of the cluster database (i.e. the HSS configuration data) and the bootload tables for the traffic processors. The DBN backup can be handled through the TelORB Manager and is stored in backup files on the hard discs of the IOs.

DBN database backups can be configured to be taken automatically at predefined intervals or predefined times.

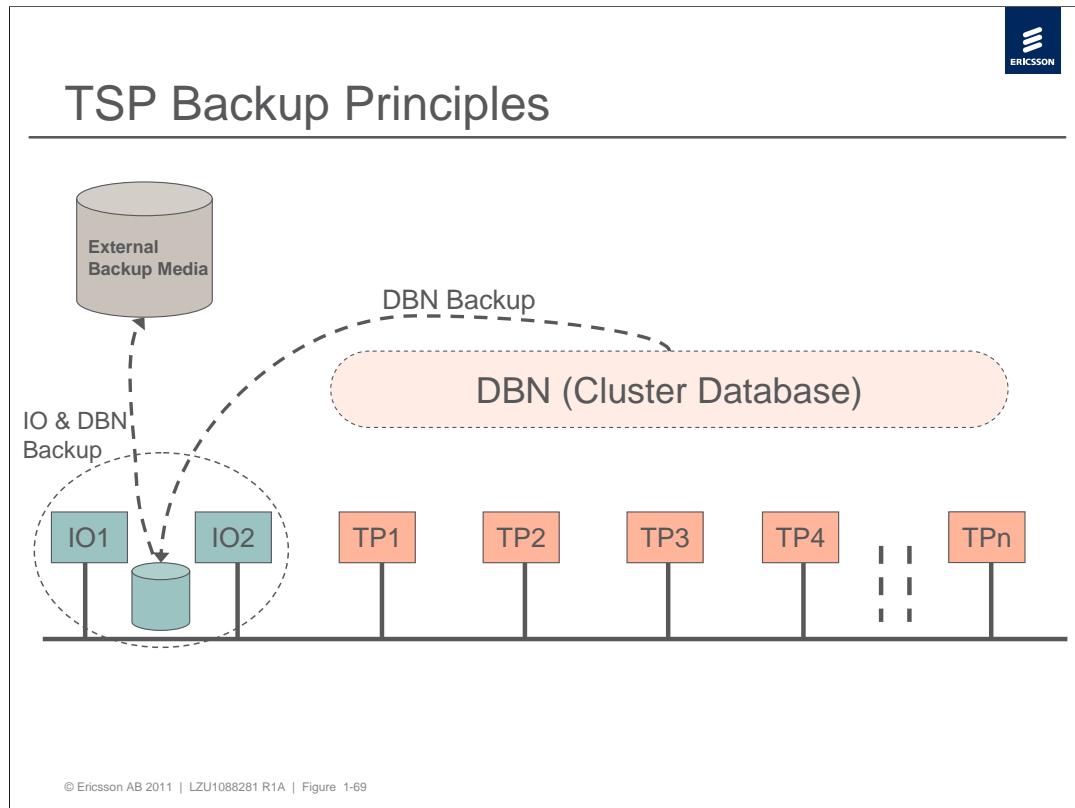
Creating a DBN backup causes no significant degradation in the system performance, because the backup runs in the background. Depending on the application and the amount of data in the database, a backup can take from 5 minutes up to one hour.

IO backup

The backup procedure takes a backup of all TSP specific data currently stored on the IO processors, that is the data on the (shared) file system. This backup can be used to restore the IO processors in the case of serious IO faults.



Since the SLF runs on the TSP platform it is backed up as part of a TSP backup.



The figure shows the backup principles.

The different backup methods are described in *TSP, Backup and Restore User Guide*

The OPIs are:

DBN backup from database to IO processors

- *Creating a DBN Backup*
- *Scheduling DBN Backups*

DBN backup from IO processors to external media

- *Archiving a DBN Backup to an Archive Server*

IO processors backup to external media

- *Backing up IO Processors*

Note that the DBN backup to external media is also a part of an IO backup.



CSCF Backup Considerations

Backup Interval	Daily : DBN backup using scheduled backup. Weekly : IO processor backup to central backup media using scheduled backup
Amount of DBN data	Less than 1 MB
Data consistency	Not applicable
Service impact	Small

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-70

A DBN backup should be performed daily and an IO backup weekly.



HSS Backup Considerations

Backup Interval	Daily : DBN backup using scheduled backup. Weekly : IO processor backup to central backup media using scheduled backup.
Amount of DBN data	The amount of data differ between operators since it is dependent on site data like amount of users, used features, and so on. The values must be calculated for each site. Example: HSS application: 4.2 MB. User data: For 500k users: 467 MB. The user data is compressed in the backup and the level of compression depends on data size (the compression factor is estimated to be 10)
Data consistency	The backup must be synchronized with other nodes.
Service impact	Small.

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-71

A DBN backup should be performed daily and an IO backup weekly.



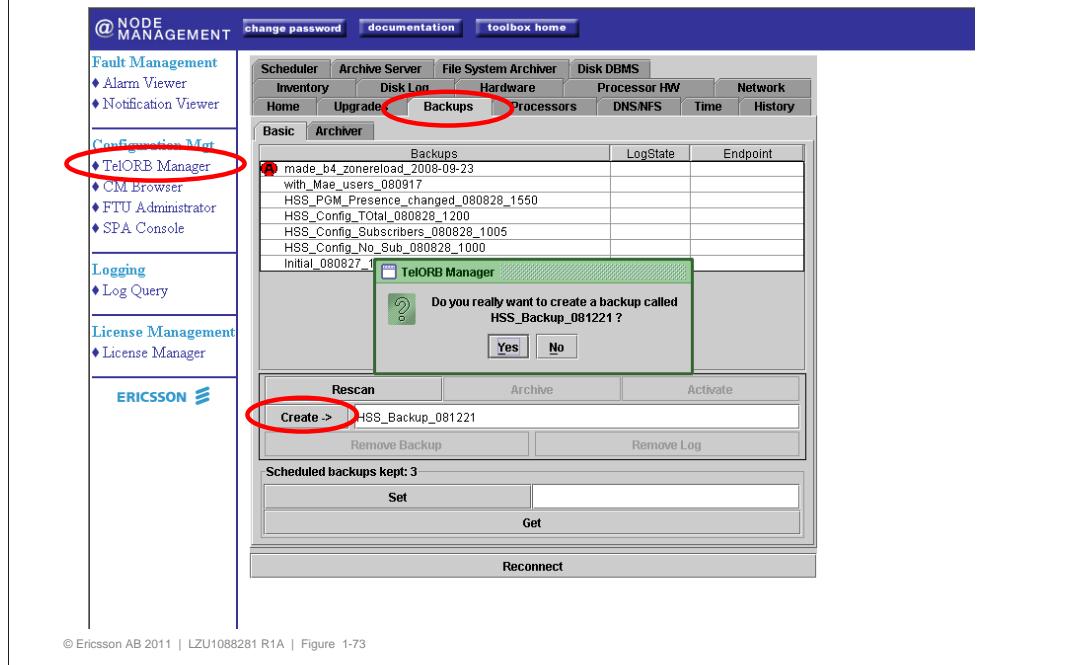
SLF Backup Considerations

Backup Interval	Daily : DBN backup using scheduled backup. Weekly : IO processor backup to central backup media using scheduled backup.
Amount of DBN data	The amount of data depends on the amount of entries provisioned and can be calculated as follows: Backup size (MB) = 2.4 + Number_of_entries × Entry_size (MB) / 32.85 where 2.4 is the backup size for the SLF application only and 32.85 is the backup compression factor. The reference entry sizes are: ›Public Identity: 360 bytes ›MSISDN: 326 bytes
Data consistency	The backup must be synchronized with other nodes.
Service impact	Small or medium.

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-72

A DBN backup should be performed daily and an IO backup weekly.

How to perform manual DBN backup



A DBN backup is performed using the TelORB manager. It is possible to create an instant (manual) backup or to schedule backups.

The figure shows how to create a manual backup.



DBN Backup Notification

Notification Viewer

Filter: Notification Limit: 10

Active Filters:

Time	ObjectType	Instance	Type
20:11:59	NotificationID	387	
20:11:59	ObjectType	backup	
20:11:59	Instance	17	
20:11:59	Type	Backup Finished Successfully	
20:11:59	Time	20081024 14:29:29 CEST	
20:11:59	NAME	HSS_Backup_081221	
			OK
20:00:00			
20:00:01	20081024	HSS-SdaConfigurationData	SDA
20:00:01	CEST		2004 Database, Synchronization Process Stopped in SDA
20:14:29:15	20081024	backup	16 Backup Started
20:14:29:15	CEST		
20:14:29:29	20081024	backup	17 Backup Finished Successfully
20:14:29:29	CEST		

See also CPI "Backup and Restore User Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-74

Notifications are issued at backup start and backup completion.

The screenshot shows the Ericsson Node Management interface. The top navigation bar includes links for change password, documentation, and toolbox home. Below this is a secondary navigation bar with tabs for Scheduler, Archive Server, File System Archiver, Disk DBMS, Inventory, Disk Log, Hardware, Processor HW, Network, Home, Upgrades, Backups, Processors, DNS/NFS, Time, and History. The 'Backups' tab is selected. On the left, a sidebar lists Fault Management (Alarm Viewer, Notification Viewer), Configuration Mgt (TelORB Manager, CM Browser, FTU Administrator, SPA Console), Logging (Log Query), and License Management (License Manager). The main content area displays a table titled 'Backups' with columns for Backups, LogState, and Endpoint. A new backup entry, 'HSS_Backup_081221', is highlighted with a red circle. Below the table are buttons for Rescan, Archive, Create, Remove Backup, Remove Log, Set, and Get. At the bottom is a 'Reconnect' button.

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-75

The new backup automatically becomes the active backup, i.e. the one used for system restore at a zone reload.



Configuring Scheduled DBN Backup

The screenshot shows the Ericsson Node Management interface. On the left, there's a sidebar with links like Fault Management, Configuration Mgt, Logging, and License Management. The main area has tabs for Scheduler, Archive Server, File System Archiver, and Disk DBMS. The Scheduler tab is selected and highlighted with a red circle. A sub-menu under Scheduler includes Inventory, Disk Log, Hardware, Processor HW, Network, and History. Below these are Home, Upgrades, Backups, Processors, DNS/NFS, Time, and History buttons. A table lists scheduled backups: DBN_backup and DDB1_backup, both set to Disabled. A modal dialog box titled "Modify DBN_backup Scheduling" is open, also circled in red. It contains fields for "From" (Year: 2008, Month: 10, Day: 27, Hour: 11, Minute: 40) and "To" (Year: 2008, Month: 12, Day: 01, Hour: 00, Minute: 00). The "Interval" section shows Days: 0, Hours: 05, Minutes: 00. At the bottom of the dialog are "OK" and "Cancel" buttons. Below the dialog, a yellow box contains the text "Description: Creates a DBN backup". At the bottom of the main window are buttons for "Modify", "View Details", "Enable", "Refresh", and "Reconnect". A red arrow points from the "Modify" button in the yellow box to the "Modify" button in the dialog. A red circle highlights the "Modify" button in the dialog. A red circle also highlights the "From" field in the dialog. A red arrow points from the "From" field in the dialog to the "From" field in the yellow box. A red circle highlights the "From" field in the yellow box.

See also CPI "Backup and Restore User Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-76

The figure shows how to set a periodic scheduled backup.

The screenshot shows the Ericsson Node Management interface. On the left, there's a sidebar with links for Fault Management, Configuration Mgt, Logging, and License Management. The main area has tabs for Scheduler, Archive Server, File System Archiver, Disk DBMS, Inventory, Disk Log, Hardware, Processor HW, Network, Home, Upgrades, Backups, Processors, DNS/NFS, Time, and History. The Backups tab is selected. In the scheduler table, there are two entries: 'DBN_backup' with 'Next Occurrence' set to '2008-10-27 11:49' and 'Status' as 'Idle', and 'DDB1_backup' with 'Status' as 'Disabled'. A red circle highlights the 'Enable' button at the bottom right of the scheduler table. Another red circle highlights the 'Next Occurrence' column header. At the bottom of the interface, there are buttons for Modify, View Details, Refresh, and Reconnect. A note at the bottom right says 'See also CPI "Backup and Restore User Guide"'.

Name	Next Occurrence	Status
DBN_backup	2008-10-27 11:49	Idle
DDB1_backup		Disabled

See also CPI "Backup and Restore User Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-77

After enabling the scheduler the time for the next backup is indicated.

IO Backup – Configuring the Archiver

The screenshot shows the 'File System Archiver' configuration screen. The 'File System Archiver' tab is highlighted with a red circle. Below it, the 'Type' dropdown is set to 'IO' (also circled in red). An 'Add' button is also circled in red. A modal dialog box titled 'Add IO Archiver' is displayed, showing the 'Name' field set to 'IO_Backup_20081221' and the 'Archive Server' dropdown set to 'EEE'. The 'OK' and 'Cancel' buttons are visible at the bottom of the dialog.

See also CPI "Backup and Restore User Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-78

An IO backup is also performed using the TelORB manager. It is possible to create an instant (manual) backup or to schedule backups.

The figure shows how to create/configure the archiver for an IO backup. It is assumed that the archive server is already configured.



IO Backup – starting the archiver

@ NODE MANAGEMENT [change password](#) [documentation](#) [toolbox home](#)

Fault Management
♦ Alarm Viewer
♦ Notification Viewer

Configuration Mgt
♦ TelORB Manager
♦ CM Browser
♦ FTU Administrator
♦ SPA Console

Logging
♦ Log Query

License Management
♦ License Manager

ERICSSON

Scheduler Archive Server File System Archiver Disk DBMS
Inventory Disk Log Hardware Processor HW Network
Home Upgrades Backups Processors DNS/NFS Time History

Name	Archive Server	Status
IO_Backup_20081221	EEE	Idle

Archive IO
Archive Server: EEE
Ok **Cancel**

Type: IO Add
Archive Remove
Refresh Abort

Reconnect

See also CPI "Backup and Restore User Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-79

The figure shows how to start the archiver.

IO Backup – archiving in progress

@ NODE MANAGEMENT change password documentation toolbox home

Fault Management
♦ Alarm Viewer
♦ Notification Viewer

Configuration Mgt
♦ TelORB Manager
♦ CM Browser
♦ FTU Administrator
♦ SPA Console

Logging
♦ Log Query

License Management
♦ License Manager

ERICSSON

Scheduler	Archive Server	File System Archiver	Disk DBMS
Inventory	Disk Log	Hardware	Processor HW
Home	Upgrades	Backups	Processors
		DNS/NFS	Time
			History

Name	Archive Server	Status
IO_Backup_20081221	EEE	Idle
Manual_IO	EEE	Running

Type: IO

Archive

Refresh

Add

Remove

Abort

Reconnect

See also CPI "Backup and Restore User Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-80

The figure shows the ongoing archiving.



IO Backup Verification (1/2)

```
192.168.13.213 - PuTTY
total 5914368
-rw-r--r-- 1 telorb users      492108 2008-07-04 16:22 DBN_After_R11B_01.tgz
-rw-r--r-- 1 telorb users      520271 2008-10-09 12:22 DBN_CSCF_R11B_080704_1.tgz
-rw-r--r-- 1 telorb users     82034688 2008-10-27 13:50 incomplete
-rw-r--r-- 1 telorb users  5967322955 2008-07-04 18:35 IO_2008_07_04_18_14_50.tgz
telorb@tspinstsrv:~/backup_archive/ee1cscf01> ll
total 5919540
-rw-r--r-- 1 telorb users      492108 2008-07-04 16:22 DBN_After_R11B_01.tgz
-rw-r--r-- 1 telorb users      520271 2008-10-09 12:22 DBN_CSCF_R11B_080704_1.tgz
-rw-r--r-- 1 telorb users  87326720 2008-10-27 13:50 incomplete
-rw-r--r-- 1 telorb users  5967322955 2008-07-04 18:35 IO_2008_07_04_18_14_50.tgz
telorb@tspinstsrv:~/backup_archive/ee1cscf01> ll
total 5924508
-rw-r--r-- 1 telorb users      492108 2008-07-04 16:22 DBN_After_R11B_01.tgz
-rw-r--r-- 1 telorb users      520271 2008-10-09 12:22 DBN_CSCF_R11B_080704_1.tgz
-rw-r--r-- 1 telorb users  92405760 2008-10-27 13:50 incomplete
-rw-r--r-- 1 telorb users  5967322955 2008-07-04 18:35 IO_2008_07_04_18_14_50.tgz
telorb@tspinstsrv:~/backup_archive/ee1cscf01> ll
total 5945344
-rw-r--r-- 1 telorb users      492108 2008-07-04 16:22 DBN_After_R11B_01.tgz
-rw-r--r-- 1 telorb users      520271 2008-10-09 12:22 DBN_CSCF_R11B_080704_1.tgz
-rw-r--r-- 1 telorb users  113721344 2008-10-27 13:50 incomplete
-rw-r--r-- 1 telorb users  5967322955 2008-07-04 18:35 IO_2008_07_04_18_14_50.tgz
telorb@tspinstsrv:~/backup_archive/ee1cscf01>
```

See also CPI "Backup and Restore User Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-81

The figure shows the ongoing archiving from the target server side.



IO Backup Verification (2/2)

```
192.168.13.213 - PuTTY
telorb@tspinstsrv:~/backup_archive/ee1cscf01> ll
total 11704908
-rw-r--r-- 1 telorb users 492108 2008-07-04 16:22 DBN_After_R11B_01.tgz
-rw-r--r-- 1 telorb users 520271 2008-10-09 12:22 DBN_CSCF_R11B_080704_1.tgz
-rw-r--r-- 1 telorb users 5967322955 2008-07-04 18:35 IO_2008_07_04_18_14_50.tgz
-rw-r--r-- 1 telorb users 6005754283 2008-10-27 14:10 IO_2008_10_27_13_52_47.tgz
telorb@tspinstsrv:~/backup_archive/ee1cscf01> ll
total 11704908
-rw-r--r-- 1 telorb users 492108 2008-07-04 16:22 DBN_After_R11B_01.tgz
-rw-r--r-- 1 telorb users 520271 2008-10-09 12:22 DBN_CSCF_R11B_080704_1.tgz
-rw-r--r-- 1 telorb users 5967322955 2008-07-04 18:35 IO_2008_07_04_18_14_50.tgz
-rw-r--r-- 1 telorb users 6005754283 2008-10-27 14:10 IO_2008_10_27_13_52_47.tgz
telorb@tspinstsrv:~/backup_archive/ee1cscf01>
```

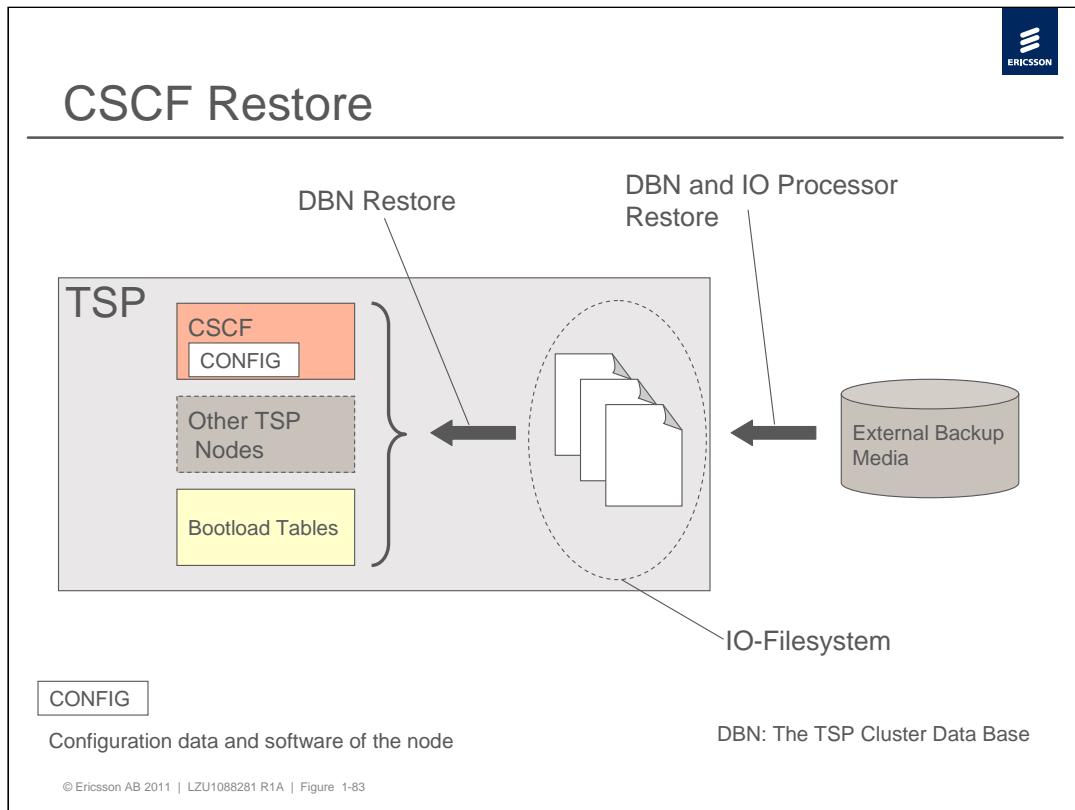
Notification Viewer

		20081027 13:52:47 CET	FileSystemBackup	Manual_IO	108	IO, Archiving Started
		20081027 14:13:00 CET	FileSystemBackup	Manual_IO	109	IO, Archiving Succeeded

See also CPI "Backup and Restore User Guide"

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-82

Archiving is successfully completed.



Since the CSCF runs on the TSP platform it is backed up as part of a TSP restore.

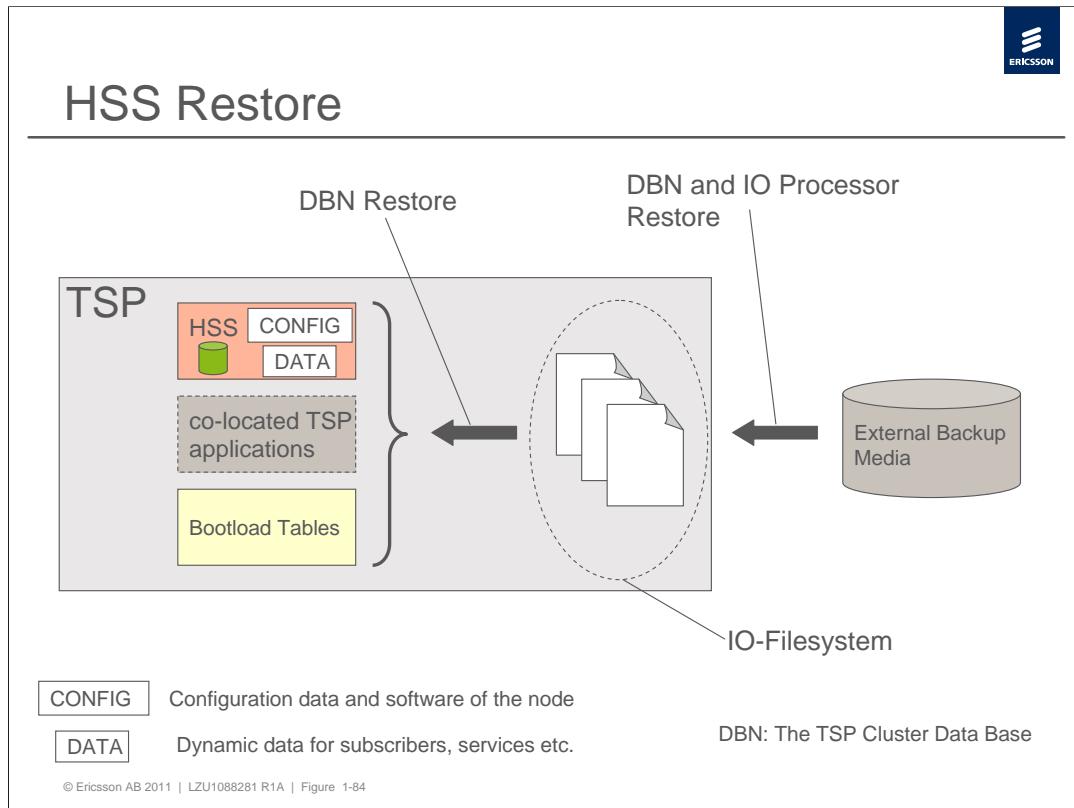
There are two types of restore, DBN restore and IO restore.

DBN restore

To restore the traffic processors from a previous backup, a zone reload needs to be performed as a part of the restore operation. This should (ideally) never need to be performed, as it would result in an In Service Performance (ISP) outage.

IO restore

Only the safe/mirrored file system of the IO processor is backed up. A restore therefore requires both the backup of those files and the original installation media.



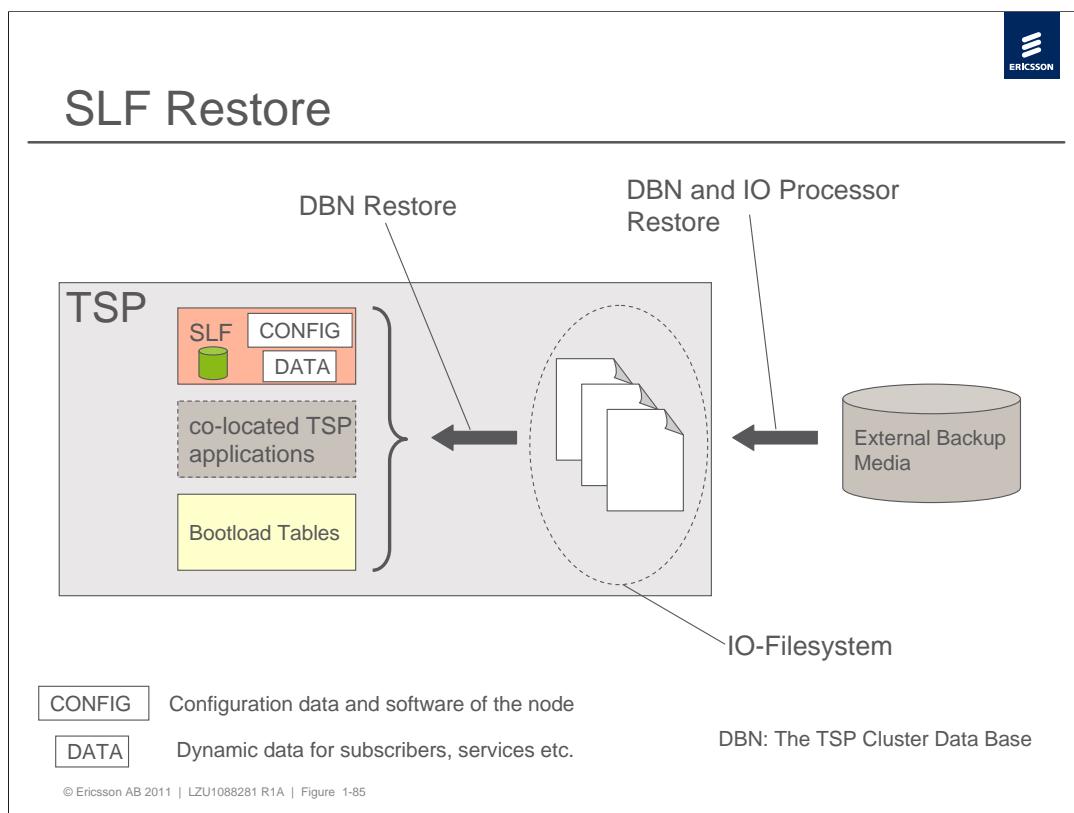
Since the HSS runs on the TSP platform it is restored up as part of a TSP restore.

DBN restore

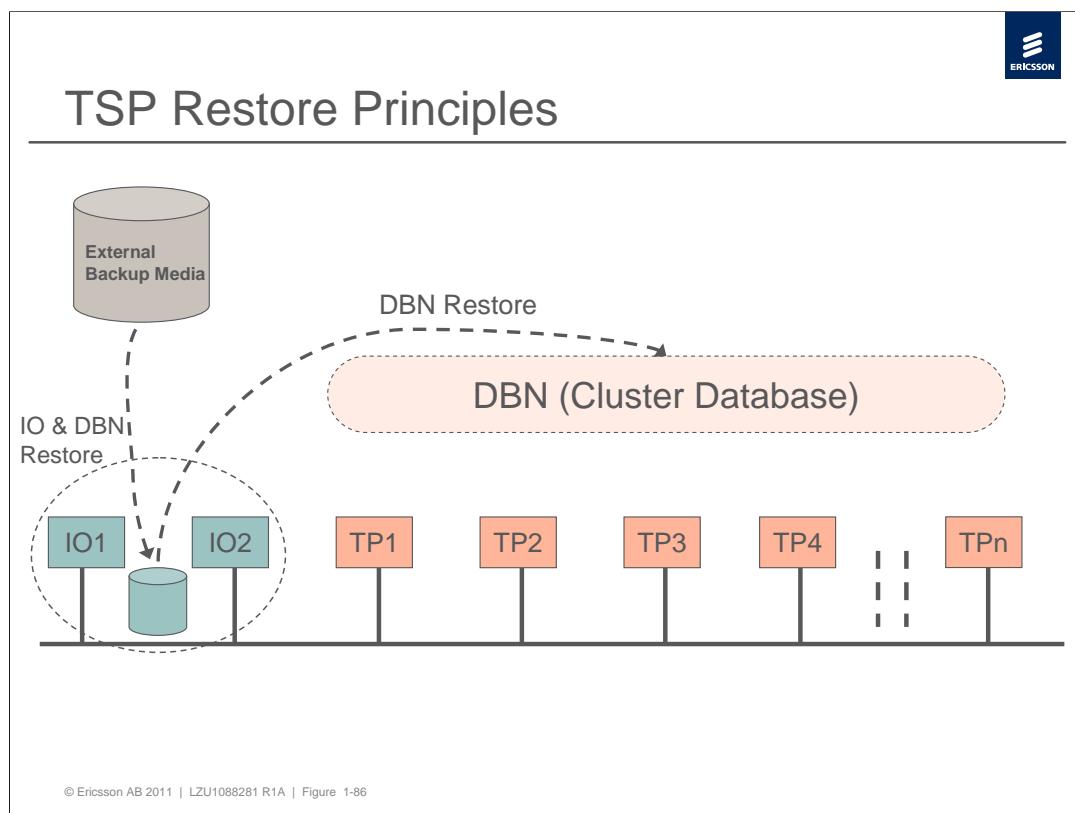
To restore the traffic processors from a previous backup, a zone reload needs to be performed as a part of the restore operation. This should (ideally) never need to be performed, as it would result in an In Service Performance (ISP) outage.

IO restore

Only the safe/mirrored file system of the IO processor is backed up. A restore therefore requires both the backup of those files and the original installation media.



Since the SLF runs on the TSP platform it is restored up as part of a TSP restore.



The figure shows the restore principles.

The different backup methods are described in *Backup and Restore User Guide*

The OPIs are:

DBN restore from IO processors

- *TelORB Manager description*

DBN restore from external media

- *Retrieving DBN Backups from an Archive Server*

IO processors restore from external media

- *Restoring IO from an Archive Server*

Note that the IO restore contains retrieving DBN backup as well.



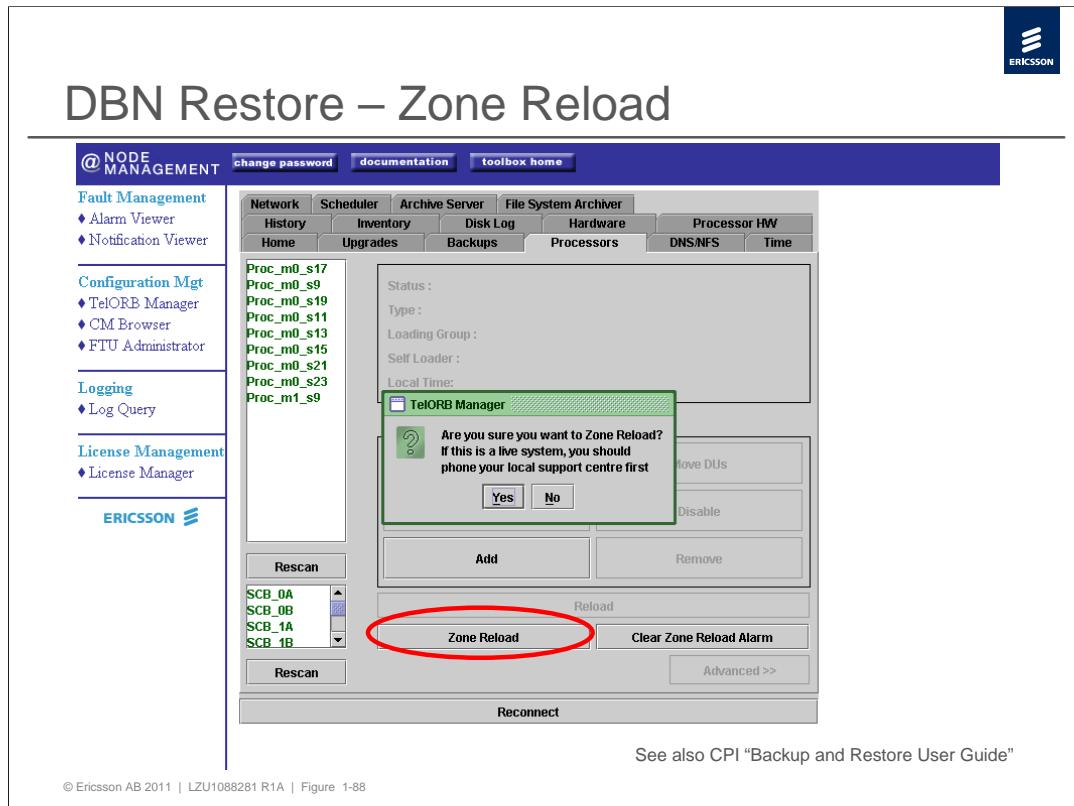
DBN Restore – Backup "activation"

The screenshot shows the Ericsson Node Management interface. The left sidebar includes links for Fault Management, Configuration Mgt (TelORB Manager, CM Browser, FTU Administrator, SPA Console), Logging (Log Query), and License Management (License Manager). The main area has tabs for Scheduler, Archive Server, File System Archiver, Disk DDMS, Inventory, Disk Log, Hardware, Processor HW, Network, Home, Upgrades, Backups, Processors, DNS/NFS, Time, and History. The 'Backups' tab is selected. A modal dialog box titled 'TelORB Manager' asks 'Do you really want to activate backup HSS_Backup_081221 ?' with 'Yes' and 'No' buttons. Below the dialog are buttons for Rescan, Archive, and Activate (which is circled in red). Other buttons include Create >, Remove Backup, Remove Log, Set, and Get. At the bottom are buttons for Reconnect and a note: 'See also CPI "Backup and Restore User Guide"'.

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-87

See also CPI "Backup and Restore User Guide"

The figure shows how to change the active backup. At zone reload the cluster is recovered from the active backup.



Under the *Processors* tab in the TelORB Manager the lower unframed area contains buttons related to reload of a processor, a switch or the whole TSP node. The following buttons are shown in the lower reload related area regardless if a processor or a switch is selected.

Reload: Reload the selected processor or the selected switch.

Zone Reload: Reloads the whole cluster, DBN restore. This is a very serious operation leading to service unavailability for some time. The system will revert to the state it had when the active backup was taken. ***Should not be used unless the administrator is absolutely sure that the system must be reloaded.***

Clear Zone Reload Alarm: After a zone reload, a System Reloaded from Backup alarm appears in the alarm list. The alarm is removed from the alarm list by clicking this button.

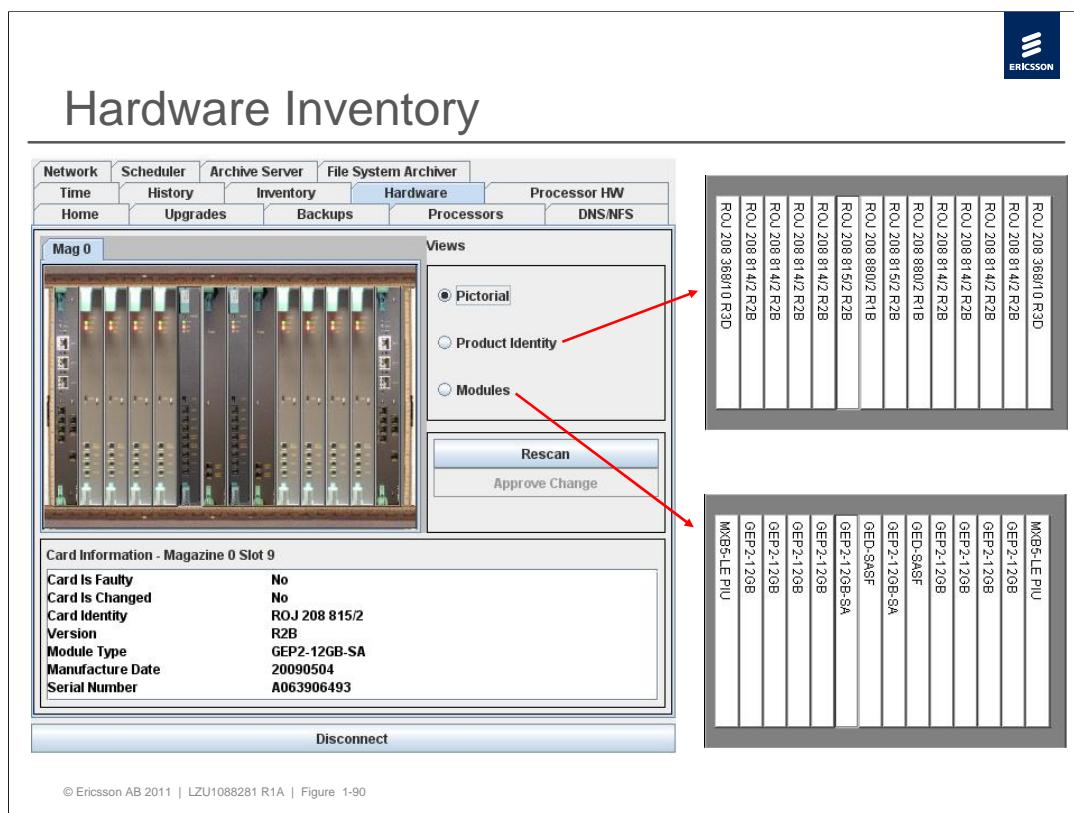


IO Processors Restore

- › In the case of a single IO crash the OPI "Replacing IO Processor" should be followed. No IO Backup is then needed to restore a single IO. IO1 can be restored from IO2 and vice versa.
- › In the case of simultaneous IO crash the OPI "Restoring IO from an Archive Server" (or "Restoring IO from Tape") is to be followed. Both IOs are restored from a backup. The procedure involves a zone reload.

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-89

An important note regarding IO processor restore is found on the picture above.



The Hardware Inventory is based on the EGEM (Enhanced Generic Ericsson Magazine) principles. A magazine has 26 slot positions numbered 0-25. The boards in the magazine can be of various types.

The figure shows the Hardware tab. The magazine can be displayed with different views. The following views can be selected:

Pictorial shows pictures of the actual boards.

Product Identity shows the product identities of the actual boards.

Modules shows the module types of the actual boards.

When clicking on one board the information fields present the status as follows:

Card is faulty This is from the Hardware Inventory point of view. It indicates if the hardware identifier can be read. The board may be working even if the Hardware Inventory can not read the identifier and flags the slot as faulty.

Card is Changed The board on the slot position has been changed. Note that removing a board or inserting a board in an empty slot will be detected as a change.

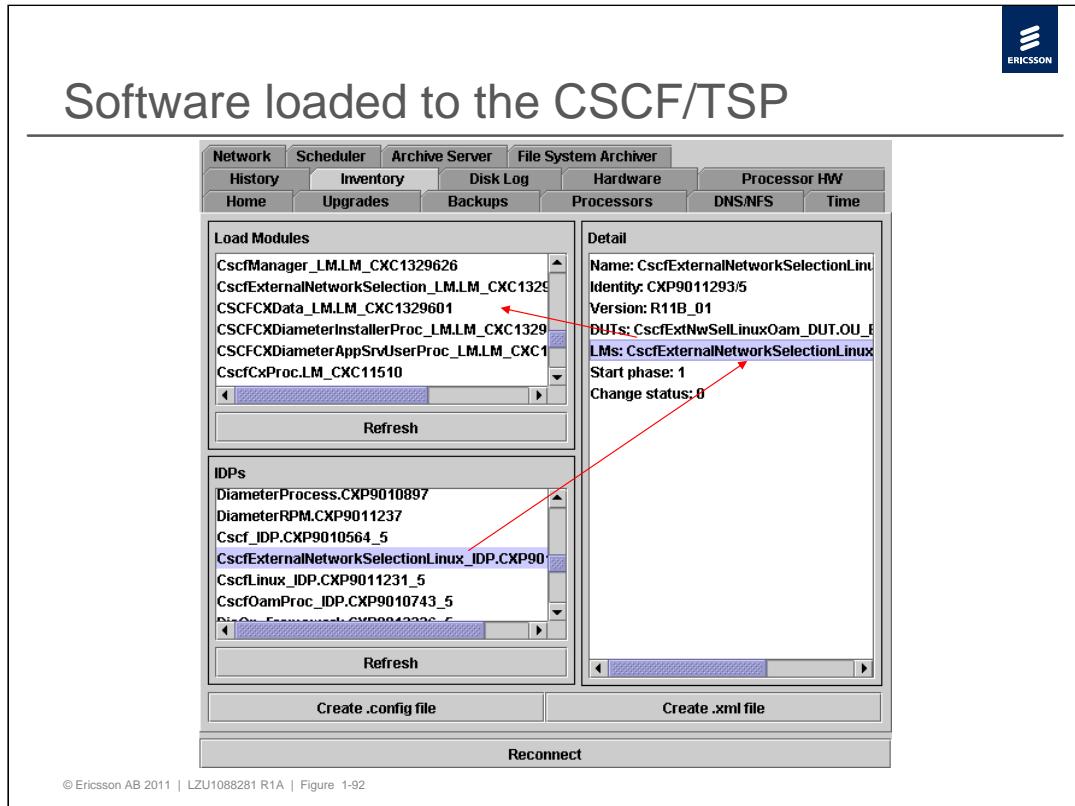
Card Identity The Ericsson product number.

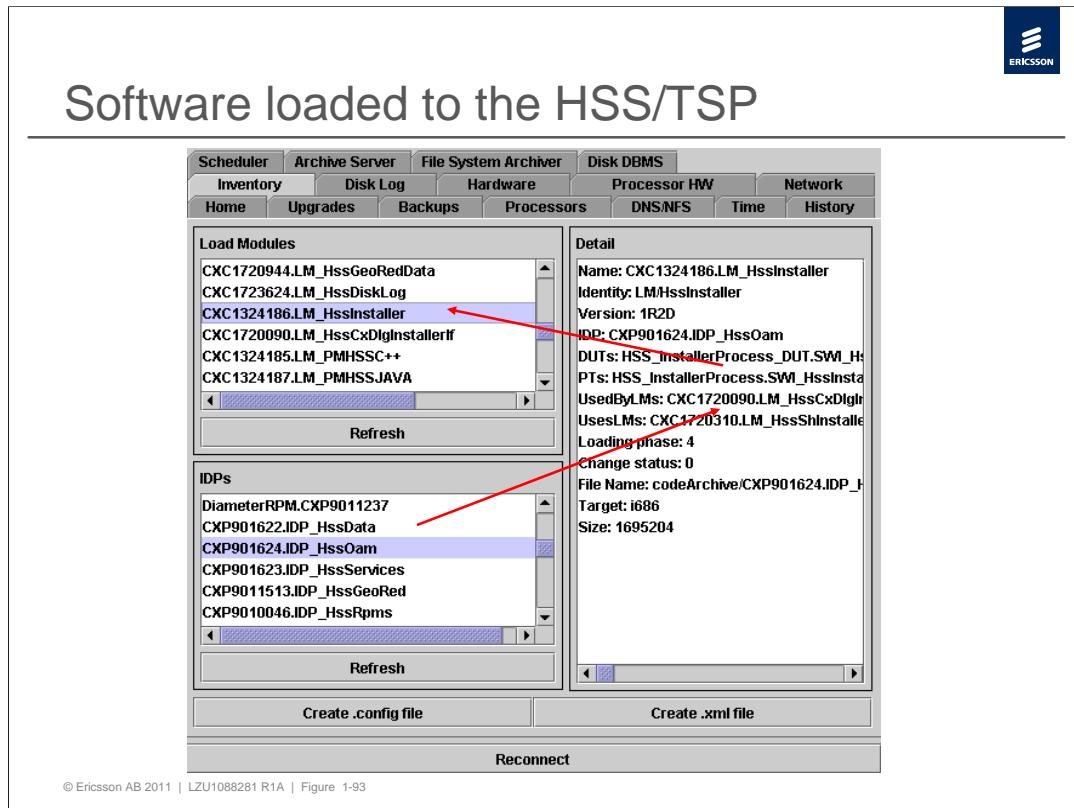
Version The product version.

Module Type The type code of the board.

Manufacture Date The date when the board was manufactured, in the format YYYYMMDD

Serial Number The unique serial number of the board currently inserted in the selected slot.





The inventory tab provides a complete listing of the software included in the system in terms of Internal Delivery Packages and Load Modules.

IDPs

This area contains the listing of all Internal Delivery Packages. Click on one of the listed IDPs to show detailed IDP information in the Detail area. In the figure one of the CSCF IDPs is clicked and in the detail area the load modules included in this IDP are shown.

Load Modules

This area contains the listing of all Load Modules. Click on one of the listed Load Modules to show detailed Load Module information in the Detail area. Load Module is a compiled and linked code. It is the smallest piece of code that can be loaded separately on the target machine.

Create .config file creates an up-to-date configuration file, based on the system configuration data.

Create .xml file, creates an xml-file representing the current SW and HW configuration of the TSP system.

The files can be found in the following folder:

`/opt/telorb/axe/loadingGroup01_1`



TSP Processors

Network	Scheduler	Archive Server	File System Archiver													
Time	History	Inventory	Hardware	Processor HW												
Home	Upgrades	Backups	Processors	DNS/NFS												
Proc_m0_s1 Proc_m0_s5 Proc_m0_s3 Proc_m0_s7 Proc_m0_s17 Proc_m0_s19 Proc_m0_s21 Proc_m0_s23																
Status : In Service Type : Intel Pc Loading Group : ProcessorLoadingGroup Self Loader : Yes Local Time: 2009-07-27 09:29:42																
<table border="1"> <tr> <td>Supply DUs</td> <td>Move DUs</td> </tr> <tr> <td>Enable</td> <td>Disable</td> </tr> <tr> <td>Add</td> <td>Remove</td> </tr> <tr> <td colspan="2">Reload</td> </tr> <tr> <td>Zone Reload</td> <td>Clear Zone Reload Alarm</td> </tr> <tr> <td colspan="2">Advanced >></td> </tr> </table>					Supply DUs	Move DUs	Enable	Disable	Add	Remove	Reload		Zone Reload	Clear Zone Reload Alarm	Advanced >>	
Supply DUs	Move DUs															
Enable	Disable															
Add	Remove															
Reload																
Zone Reload	Clear Zone Reload Alarm															
Advanced >>																
Rescan																
MXB_OA MXB_OB																
Rescan																
Disconnect																

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-94

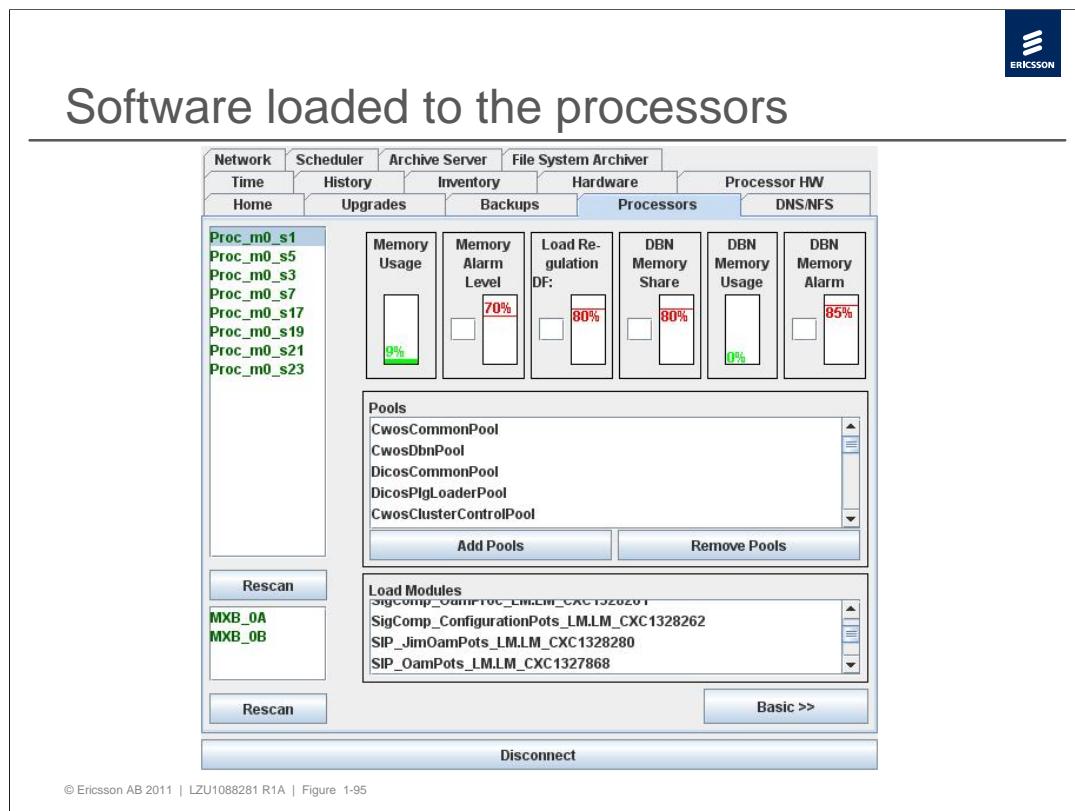
The Processors tab has two different modes, basic and advanced. Toggle between the two modes by clicking the Advanced/Basic button in the lower right corner of the tab. The figure shows the Basic mode of the Processor tab. There are two lists on the left side, the processor list and the switch list. These lists are common to both modes.

The upper list shows the processors attached to the system. Processors are displayed in different colors:

- Red if the processor is disabled
- Blue if the processor is starting up
- Green if the processor is running.

Clicking on one of the processors shows the processor information. If the processor you want to look at does not appear on the list, click the Rescan button below the list.

The lower list shows the Ethernet switches of the system. A switch that is displayed as red means there is no contact with that switch. Switches displayed in green are running. Clicking on one of the switches shows the information of that switch. If the switch you want to look at does not appear on the list, click the Rescan button below the list.



The information in the Advanced area under the Processors tab relates to only one processor. Here it is possible to view the load of a certain processor and set alarm limits for overload.

It is also possible to see to the list of all pools of which the selected processor is a member as well as buttons for adding and removing pools from the selected processor. A member of a pool can execute processes and store data related to a certain application.

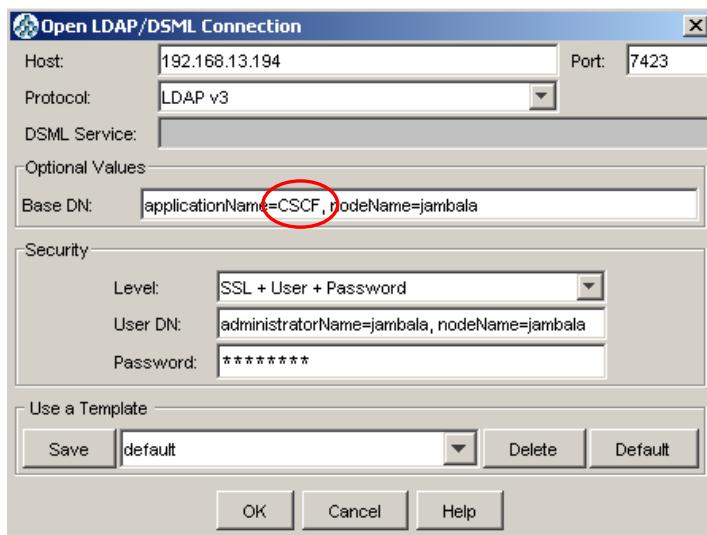
Processors running the HSS application should belong to HSS related pools which are several different. Some of them are shown on the figure.

Processors running the SLF application should belong to SLF related pools which are also several different.

The load modules allocated to a certain processor can also be viewed.



Login to the TSP CSCF application



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-96

The Application name for the CSCF application is *CSCF*.

CSCF Administrative State

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view shows a node named 'nodeName=al1tsp01' under 'World', which contains an entry for 'applicationName=CSCF'. This entry has several attributes listed in the table view on the right. One attribute, 'CscfAdministrativeState', is highlighted with a red border. The table view also lists other attributes like 'objectClass', 'applicationName', 'BcfDomainNameEntry', 'BcfEnabled', 'BcfOperationalState', 'CscfActiveUserMethod', and various 'CscfAkaAlgorithmEntry' entries.

attribute type	value
objectClass	CSCF-Application
applicationName	CSCF
BcfDomainNameEntry	Bcf domain name
BcfEnabled	FALSE
BcfOperationalState	0
CscfActiveUserMethod	
CscfAdministrativeState	1
CscfAkaAlgorithmEntry	1:hmac-md5-96,aes-cbc:enabled
CscfAkaAlgorithmEntry	2:hmac-sha-1-96,aes-cbc:enabled
CscfAkaAlgorithmEntry	3:hmac-md5-96,des-edc3-cbc:enabled
CscfAkaAlgorithmEntry	4:hmac-sha-1-96,des-edc3-cbc:enabled
CscfAkaAlgorithmEntry	5:hmac-md5-96,null:enabled
CscfAkaAlgorithmEntry	6:hmac-sha-1-96,null:enabled
CscfAkaStalenessTimer	1440
CscfASFalloverTimeInvite	5
CscfASFalloverTimeNonInvite	5

CPI: CSCF Common Configuration Management Parameters

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-97

This parameter is configurable:

0 = Locked

1 = Unlocked

2 = Shutting Down

The parameter *CscfAdministrativeState* shows the administrative state of the CSCF.

This attribute indicates the current administrative state of the CSCF. The attribute is used to lock, unlock or shut down the node.

When the node is locked, all requests will be rejected and all ongoing sessions will be disconnected. Only when the node is locked certain attributes such as *CscfDomainName* may be changed. SIP interfaces can only be added or removed when the node is locked.

When *CscfAdministrativeState* has been set to shutting down all existing sessions will be ongoing, but all new session requests to the CSCF after the shutting down configuration will receive a 503 - Service Unavailable. After all users have de-registered and the *CscfUsageState* is 0 (idle), the *CscfAdministrativeState* will be set to locked.

Possible Values and Meanings:

0 = Locked

1 = Unlocked

2 = Shutting down

I, S and P- CSCF Operational State

attribute type	value
CscfGaugeInterval	2
CscfGlobalNumberNormalizationPhoneContext	edu.mmtel.net
CscfIDHashedEntry	3833619631
CscfISPBehavior	4
CscfISPOperationalState	1
CscfMaxContactsBehavior	2
CscfMaxNonSupervisedSessionDuration	1440
CscfMaxNumberContactsPerUser	10
CscfNBAAccessNetworkType	

This parameter is Non-configurable:

0 = Disabled

1 = Enabled

CPI: CSCF Common Configuration Management Parameters

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-98

This attribute indicates the current operational state of the CSCF. This operational state is based on the current configuration of the node and it's ability to handle traffic.

State requirements for a co-located CSCF.

ISP-CSCF operational state requirements for CscfBehavior = 4 is:

- 4 UDP instances → 1 for I, 1 for S and 2 for P (1 for Gm and 1 for Mw)
- If a TCP instance has been configured it must have same IP-address and port of the corresponding UDP interface
- Parameters CscfCXOriginRealm, CscfCXOriginHost, CscfCXDestinationRealm, CscfCXDestinationHost, CscfChargingInterOpId must be configured.

If at least one of the above requirements is not fulfilled, CscfISPOperationalState will be *Disabled*.

For further information of the state see CPI: *CSCF Common Configuration Management Parameters*.

CSCF ISP Behavior

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view shows a node named 'nodeName=alttsp01' under 'World'. Under this node, there is a child node 'applicationName=CSCF' which contains several attributes: CscfAccessNetworkAssertionKey=0, CscfCharging=0, CscfGenericNumberPortabilityKey=0, CscfHssQuarantineKey=0, CscfIkiKey=0, CscfMedia=0, CscfNumPortabilityKey=0, CscfNwIfContainerKey=0, CscfResourceBroker=0, and CscfSipMsgPreProcessingKey=0. On the right, the 'Table Editor' tab is selected, displaying a table of attributes and their values. One row, 'CscfISPBehavior', has its value '4' highlighted with a red border. Below the table are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. At the bottom left of the interface, it says 'Connected To ldap://10.64.224.193:7423'.

attribute type	value
CscfGaugeInterval	2
CscfGlobalNumberNormalizationPhoneContext	edu.mmtel.net
CscfIDHashedEntry	3833619631
CscfISPBehavior	4
CscfISPOperationalState	1
CscfMaxContactsBehavior	2
CscfMaxNonSupervisedSessionDuration	1440
CscfMaxNumberContactsPerUser	10
CscfNBAAccessNetworkType	

This parameter is configurable:

- 0 = none
- 1 = I-CSCF
- 2 = S-CSCF
- 3 = P-CSCF
- 4 = ISP
- 5 = IS

CPI: CSCF Common Configuration Management Parameters

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-99

This attribute determines the behavior of the CSCF application. It can only be set if *CscfAdministrativeState* = 0 (locked).

Possible Values and Meanings

- 0 = none
- 1 = I-CSCF
- 2 = S-CSCF
- 3 = P-CSCF
- 4 = colocated I, S and P
- 5 = colocated I and S

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view under 'World' shows an entry for 'nodeName=altcsp01' which contains an 'applicationName=CSCF' entry. This entry has several attributes: CscfTrustedGateway (10.64.229.164/32), CscfTrustedGateway (10.64.229.132/32), CscfTrustedNetwork (TRUE), CscfUnallocatedRoutingEnabled (FALSE), and CscfUsageState (1). The 'CscfUsageState' row is highlighted with a red border. On the right, the 'Table Editor' tab is selected, displaying the attribute type and value pairs. Below the table are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A status bar at the bottom indicates 'Connected To ldap://10.64.224.193:7423'.

This parameter is Non-configurable:
0 = Idle
1 = Active
2 = Busy

CPI: CSCF Common Configuration Management Parameters

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-100

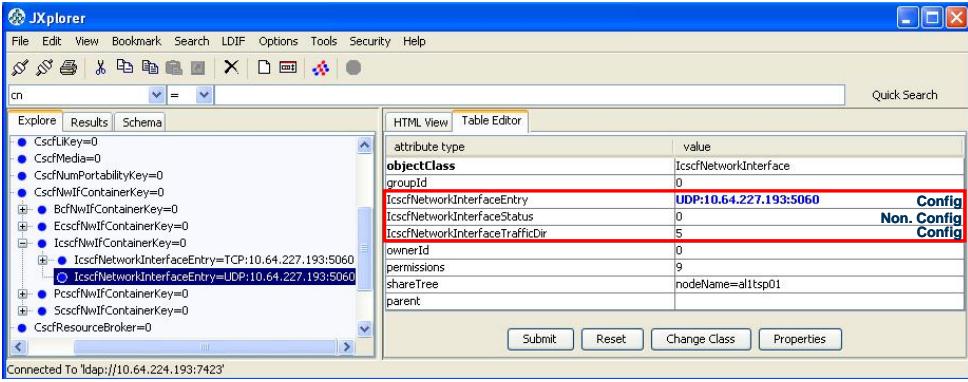
This attribute indicates the current usage state of the CSCF. This usage state is based on the number of registrations and sessions maintained by the CSCF.

Possible values and meanings:

0 = idle (No calls and all users have deregistered)

1 = active

2 = busy



The screenshot shows the JXplorer LDAP browser interface. On the left, the navigation pane displays a tree structure of LDAP objects under the 'cn' root, including various CSCF-related entries like CscfLkKey=0, CscfMedia=0, and IcscfNetworkInterfaceEntry. On the right, the 'Table Editor' tab is selected, showing a table with attributes for an IcscfNetworkInterfaceEntry object. The table includes columns for 'attribute type' and 'value'. The 'IcscfNetworkInterfaceEntry' row has its value set to 'UDP:10.64.227.193:5060'. The 'IcscfNetworkInterfaceStatus' row has its value set to '0'. The 'IcscfNetworkInterfaceTrafficDir' row has its value set to '5'. The 'Config' column for these three rows is highlighted in red, indicating they are being edited. Other visible attributes include 'groupId' (0), 'ownerId' (0), 'permissions' (9), and 'shareTree' (nodeName=al1sp01). Buttons at the bottom of the editor include 'Submit', 'Reset', 'Change Class', and 'Properties'. A status bar at the bottom of the window indicates 'Connected To ldap://(10.64.224.193:7423)'.

CPI: CSCF Common Configuration Management Parameters

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-101

The *IcscfNetworkInterfaceEntry* defines the network interface the I-CSCF uses to receive and send SIP traffic. The I-CSCF must be configured with one UDP interface. Maximum one UDP and one TCP interface can be added. Network Interface Entries can only be added or removed when the node is in locked state.

A TCP port may only be configured if it already exist a UDP port with the same port number and port role.

The *IcscfNetworkInterfaceStatus* attribute indicates the current status of this network interface.

Possible Values and Meanings

0 = okay

1 = no traffic direction set

2 = port already in use

3 = port open failed

4 = partial failure

The *IcscfNetworkInterfaceTrafficDir* can only be set to 5 (Irrelevant)

Note: Port-Alignment has been introduced with CSCF 5.0 release

The figure consists of two side-by-side screenshots of the JXplorer LDAP browser interface. Both screenshots show the 'Table Editor' view for a 'PcsrfNetworkInterface' object.

Gm Interface (Top Screenshot):

- Object Class:** PcsrfNetworkInterface
- attribute type / value:**
 - PcsrfNetworkInterfaceEntry: UDP:10.64.227.192:5060 (Configured)
 - PcsrfNetworkInterfaceProtection: None (Configured)
 - PcsrfNetworkInterfaceStatus: 0 (Non. Config)
 - PcsrfNetworkInterfaceTrafficDir: 1 (Configured)
 - PcsrfPortStatus: NA

Mw Interface (Bottom Screenshot):

- Object Class:** PcsrfNetworkInterface
- attribute type / value:**
 - PcsrfNetworkInterfaceEntry: UDP:10.64.227.192:5062 (Configured)
 - PcsrfNetworkInterfaceProtection: None (Configured)
 - PcsrfNetworkInterfaceStatus: 0 (Non. Config)
 - PcsrfNetworkInterfaceTrafficDir: 2 (Configured)
 - PcsrfPortStatus: NA

Both screenshots include a left-hand tree view of the LDAP schema and a bottom status bar indicating the connection is to 'ldaps://10.64.224.193:7423'.

The *PcscfNetworkInterfaceEntry* defines the network interface the P-CSCF uses to receive and send SIP traffic. The P-CSCF must be configured with at least two UDP interfaces, one interface for Gm traffic between the UE and the P-CSCF, the other for Mw traffic between the P-CSCF and the I/S-CSCF. Optionally protected IPsec interfaces can be added as well (there can be several and to be used for IMS AKA). Maximum one UDP and one TCP interface can be added for each type. Network Interface Entries can only be added or removed when the node is in locked state.

A TCP port may only be configured if it already exist a UDP port with the same port number and port role.

The *PcscfNetworkInterfaceStatus* attribute indicates the current status of this network interface.

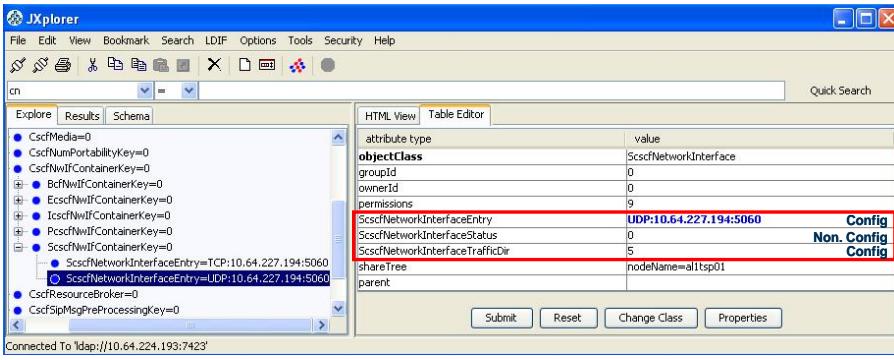
Possible Values and Meanings:

0 = okay; 1 = no traffic direction set; 2 = port already in use; 3 = port open failed; 4 = partial failure

The *PcscfNetworkInterfaceTrafficDir* defines if this interface is used for unprotected Gm, unprotected Mw, or bidirectional IPsec protected traffic Network Interface Status. . *PcscfNetworkInterfaceTrafficDir* can only be removed when the node is in locked state.

Possible Values and Meanings, 1 = unprotected Gm, 2 = unprotected Mw, 4 = bidirectional protected traffic.

Nb: The values 1 and 2 can only be set for “None” protected interfaces and 4 can only be set for “IPSec” protected interfaces. See Chapter 7 “Security & Authentication” for more info about IPSec.



The screenshot shows the JXplorer LDAP browser interface. On the left, the navigation pane displays a tree structure of LDAP entries under the 'cn' root, including various CSCF-related parameters like CscfMedia=0, CscfNumPortabilityKey=0, and ScscfNwIfContainerKey=0. On the right, the 'HTML View' tab is selected, showing a table editor for a specific entry. The entry is of type 'ScscfNetworkInterface'. The table contains the following fields:

attribute type	value
objectClass	ScscfNetworkInterface
groupId	0
ownerId	0
permissions	9
ScscfNetworkInterfaceEntry	UDP:10.64.227.194:5060
ScscfNetworkInterfaceStatus	0
ScscfNetworkInterfaceTrafficDir	5
shareTree	nodeName=a1itsp01
parent	

Buttons at the bottom of the table editor include Submit, Reset, Change Class, and Properties.

CPI: CSCF Common Configuration Management Parameters
 © Ericsson AB 2011 | LZU1088281 R1A | Figure 1-103

The *ScscfNetworkInterfaceEntry* defines the network interface the S-CSCF uses to receive and send SIP traffic. The S-CSCF must be configured with one UDP interface. Maximum one UDP and one TCP interface can be added. Network Interface Entries can only be added or removed when the node is in locked state. A TCP port may only be configured if it already exist a UDP port with the same port number and port role.

The *ScscfNetworkInterfaceStatus* attribute indicates the current status of this network interface.

Possible Values and Meanings

0 = okay

1 = no traffic direction set

2 = port already in use

3 = port open failed

4 = partial failure

The *ScscfNetworkInterfaceTrafficDir* can only be set to 5 (Irrelevant)



E-CSCF Network Interface

The screenshot shows the JXplorer LDAP browser interface. On the left, the navigation pane displays a tree structure of configuration parameters under 'cn'. On the right, the 'Table Editor' view shows a list of attributes for an 'EcsfNetworkInterfaceEntry' object. The attributes listed are:

attribute type	value	status
objectClass	EcsfNetworkInterface	Config
EcsfNetworkInterfaceEntry	UDP:10.64.227.195:5060	Config
EcsfNetworkInterfaceStatus	0	Non. Config
EcsfNetworkInterfaceTrafficDir	5	Config
groupId	0	
ownerId	0	
permissions	9	
shareTree	nodeName=al1tsp01	
parent		

Buttons at the bottom of the editor include 'Submit', 'Reset', 'Change Class', and 'Properties'. A status message at the bottom left indicates 'Connected To ldap://10.64.224.193:7423'.

CPI: CSCF Common Configuration Management Parameters

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-104

The *EcsfNetworkInterfaceEntry* defines the network interface the E-CSCF uses to receive and send SIP traffic. The E-CSCF must be configured with one UDP interface. Maximum one UDP and one TCP interface can be added. Network Interface Entries can only be added or removed when the node is in locked state. A TCP port may only be configured if it already exist a UDP port with the same port number and port role.

The *EcsfNetworkInterfaceStatus* attribute indicates the current status of this network interface.

Possible Values and Meanings

0 = okay

1 = no traffic direction set

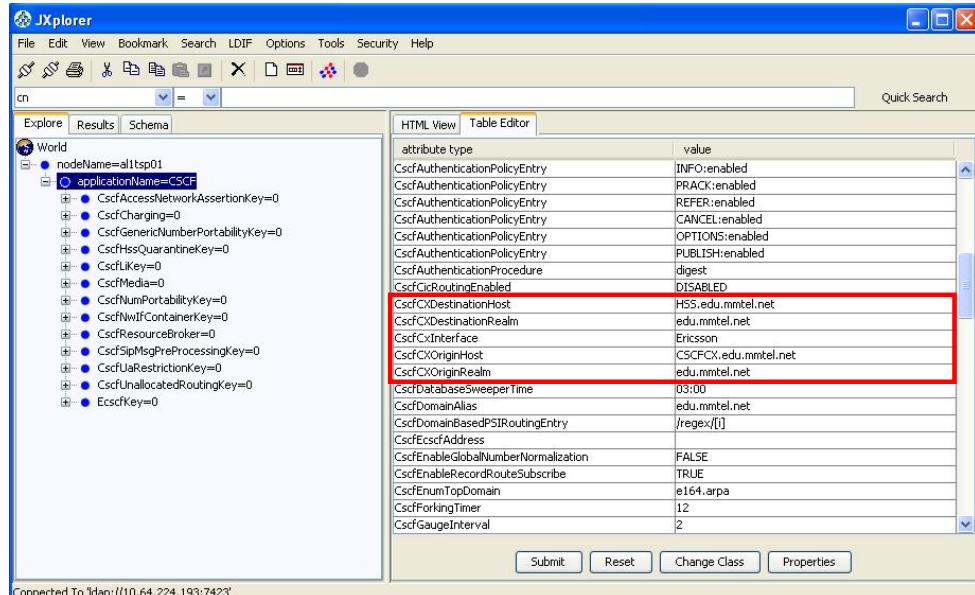
2 = port already in use

3 = port open failed

4 = partial failure

The *EcsfNetworkInterfaceTrafficDir* can only be set to 5 (Irrelevant)

CSCF Cx Interface Data



attribute type	value
CscfAuthenticationPolicyEntry	INFO:enabled
CscfAuthenticationPolicyEntry	PRACK:enabled
CscfAuthenticationPolicyEntry	REFER:enabled
CscfAuthenticationPolicyEntry	CANCEL:enabled
CscfAuthenticationPolicyEntry	OPTIONS:enabled
CscfAuthenticationPolicyEntry	PUBLISH:enabled
CscfAuthenticationProcedure	digest
CscfCircuitRoutingEnabled	DISABLED
CscfCXDestinationHost	HSS.edu.mmtel.net
CscfCXDestinationRealm	edu.mmtel.net
CscfCxInterface	Ericsson
CscfCXOriginHost	CSCFCX.edu.mmtel.net
CscfCXOriginRealm	edu.mmtel.net
CscfDatabaseSweeperTime	03:00
CscfDomainAlias	edu.mmtel.net
CscfDomainBasedPSIRoutingEntry	/regex/{1}
CscfEcsfAddress	
CscfEnableGlobalNumberNormalization	FALSE
CscfEnableRecordRouteSubscribe	TRUE
CscfEnumTopDomain	e164.arpa
CscfForcingTimer	12
CscfGaugeInterval	2

Connected To 'ldap://10.64.224.193:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-105

The *CscfCXDestinationHost* identifies the endpoint that the Diameter message is sent to. This value is used for the Destination-Host AVP (Attribute Value Pair) in the Diameter message. When SLF is present in the network this parameter should be set to *NotConfigured* on I-CSCF and E-CSCF.

The *CscfCXDestinationRealm* identifies the realm the Diameter message is to be routed to. The absence of the *CscfCXDestinationHost* will cause a message to be sent to any Diameter server supporting the application within the realm specified in Destination-Realm AVP.

The *CscfCXOriginHost* identifies the endpoint that originated the Diameter message. This value is used in the origin-Host AVP.

The *CscfCXOriginRealm* identifies the realm of the originator of the Diameter message. This value is used in the origin-Realm AVP.

These parameters are mandatory to define otherwise the *CscfOperationalState* will be *disabled*.

The *CscfCxInterface* is only kept for backward compatibility on O&M interface but the value of this parameter will be disregarded by CSCF.

The screenshot shows the JXplorer interface for managing CSCF Charging Data. The left pane displays a hierarchical tree structure under 'nodeName=jambala' with various charging-related entries like 'CscfCharging=0', 'CscfCharging=1', and 'CscfChargingTriggers=0'. The right pane shows a table editor for a selected object. A red box highlights the 'ScscfChargingTriggerName' row, which contains 'Scscf-Charging-Trigger-INVITE'. Another red box highlights the 'ScscfChargingTriggerList' row, which contains 'Scscf-Charging-Trigger-INVITE' and 'Scscf-Charging-Trigger-REGISTER'. Below the table are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

attribute type	value
objectClass	ScscfChargingTriggerGroupsClass
ScscfChargingProfileName	Offline_Charging_All_True
ScscfChargingTriggerConditionTypeCNF	FALSE
ScscfChargingTriggerName	Scscf-Charging-Trigger-INVITE
ScscfChargingTriggerPriority	1
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=jambala
parent	

CPI: CSCF Charging Configuration Management Parameters
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-106

In the figure the CSCF charging data is shown.

The charging triggers are highlighted.

The charging triggers determine if the CSCF generates a charging event related to a certain SIP message or response.

There is a common trigger list for offline and online charging.

ScscfChargingTriggerConditionTypeCNF specifies how the charging triggers expressions (defined in child entries) are logically linked. If this parameter is set to True, a logical OR will be implemented; if set to False instead the expressions will be linked by a logical AND.

If the logical OR or the logical AND (depending on the configuration of the aforementioned parameter) have been finally evaluated as true, the AVP settings of the Charging Profile specified in *ScscfChargingProfileName* will be used when sending a Diameter request to a Charging Collection Function (e.g. Ericsson Multi Mediation).

CSCF Charging Data: Profiles (1/3) General configuration

CPI: CSCF Charging Configuration Management Parameters
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-107

In the figure the CSCF charging data is shown.

The charging profiles are highlighted.

The charging profiles determine the contents of the charging messages (ACR for offline and CCR for online) in terms of charging specific AVPs.

The Parameter ScscfChargingCase determines the type of charging. Possible values are:

- NoCharging = No charging will be generated
- OfflineChargingOnly = Offline Charging only
- OfflineAndOnlineCharging = Offline Charging and online charging. Both are running in parallel if the OCS (Online Charging System) address is available, otherwise only offline charging is performed.
- OnlineChargingPrecedence=Online charging has precedence. Online charging if the OCS address is available, otherwise offline charging.
- OnlineChargingOnly=Online charging only

CSCF Charging Data: Profiles (2/3) Example of AVPs for Offline Charging

attribute type	value
<code>ScscofflineChargingAccessNetworkInformation</code>	<code>start=false;interim=false;stop=false;event=false</code>
<code>ScscofflineChargingAVP</code>	<code>Offline_Charging_All_True</code>
<code>ScscofflineChargingCalledPartyAddress</code>	<code>start=true;interim=true;stop=true;event=true</code>
<code>ScscofflineChargingCallingPartyAddress</code>	<code>start=true;interim=true;stop=true;event=true</code>
<code>ScscofflineChargingCarrierSelectRoutingInfo</code>	<code>start=true;interim=true;stop=true;event=true</code>
<code>ScscofflineChargingEventNPTimestamp</code>	<code>start=false;interim=false;stop=false;event=false</code>
<code>ScscofflineChargingEventTimestamp</code>	<code>start=true;interim=true;stop=true;event=true</code>
<code>ScscofflineChargingGPRSRoamingStatus</code>	<code>start=false;interim=false;stop=false;event=false</code>
<code>ScscofflineChargingImsChargingIdentifier</code>	<code>start=true;interim=true;stop=true;event=true</code>
<code>ScscofflineChargingNumberPortabilityRoutingInfo</code>	<code>start=true;interim=true;stop=true;event=true</code>
<code>ScscofflineChargingRoleOfNode</code>	<code>start=true;interim=true;stop=true;event=true</code>
<code>ScscofflineChargingSDPSessionDescription</code>	<code>start=true;interim=true;stop=true;cache=false</code>
<code>ScscofflineChargingServedPartyIpAddress</code>	<code>start=true;interim=true;stop=true;event=true</code>
<code>ScscofflineChargingSIPRingingTimestamp</code>	<code>start=false;interim=false;stop=false</code>
<code>ScscofflineChargingUserName</code>	<code>start=true;interim=true;stop=true;event=true</code>
<code>ScscofflineChargingUserSessionId</code>	<code>start=true;interim=true;stop=true;event=true</code>
<code>groupId</code>	<code>0</code>
<code>ownerId</code>	<code>0</code>
<code>permissions</code>	<code>9</code>
<code>shareTree</code>	<code>nodeName=alitsp05</code>
<code>parent</code>	

Connected To 'ldap://10.64.224.194:7423'

CPI: CSCF Charging Configuration Management Parameters

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-108

Below the parameters in the figure are described (an example for the offline charging profile):

Each Accounting Request (ACR) record type, *Start*, *Interim*, *Stop*, *Event* are possible to set to *True* or *False* for different charging parameters.

This means for example according to the data in the figure that the *ScscofflineChargingEventTimestamp* with the AVP code 55 will be part of both ACR-start, ACR-interim, ACR-event and ACR-stop messages.

CSCF Charging Data: Profiles (3/3)

Ericsson Service Information

attribute type	value
objectClass	ScscfOfflineChargingEricssonServiceInformationClass
groupId	0
ownerId	0
permissions	9
ScscfOfflineChargingAuthenticationMethod	start=false;interim=false;stop=false;event=false
ScscfOfflineChargingCalledPartyOriginalAddress	start=false;interim=false;stop=false;event=false;cache=false
ScscfOfflineChargingDialAroundIndicator	start=false;interim=false;stop=false;event=false
ScscfOfflineChargingEricssonServiceInformation	UPGRADED_INVITE
ScscfOfflineChargingImssServiceIdentification	start=false;interim=false;stop=false;event=false;cache=false
ScscfOfflineChargingSIPRequestTimestampFraction	start=false;interim=false;stop=false;event=false
ScscfOfflineChargingSIPResponseTimestampFraction	start=false;interim=false;stop=false;event=false
ScscfOfflineChargingTransactionInfo	start=false;interim=false;stop=false;event=false
shareTree	nodeName=alitsp05
parent	

CPI: CSCF Charging Configuration Management Parameters
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-109

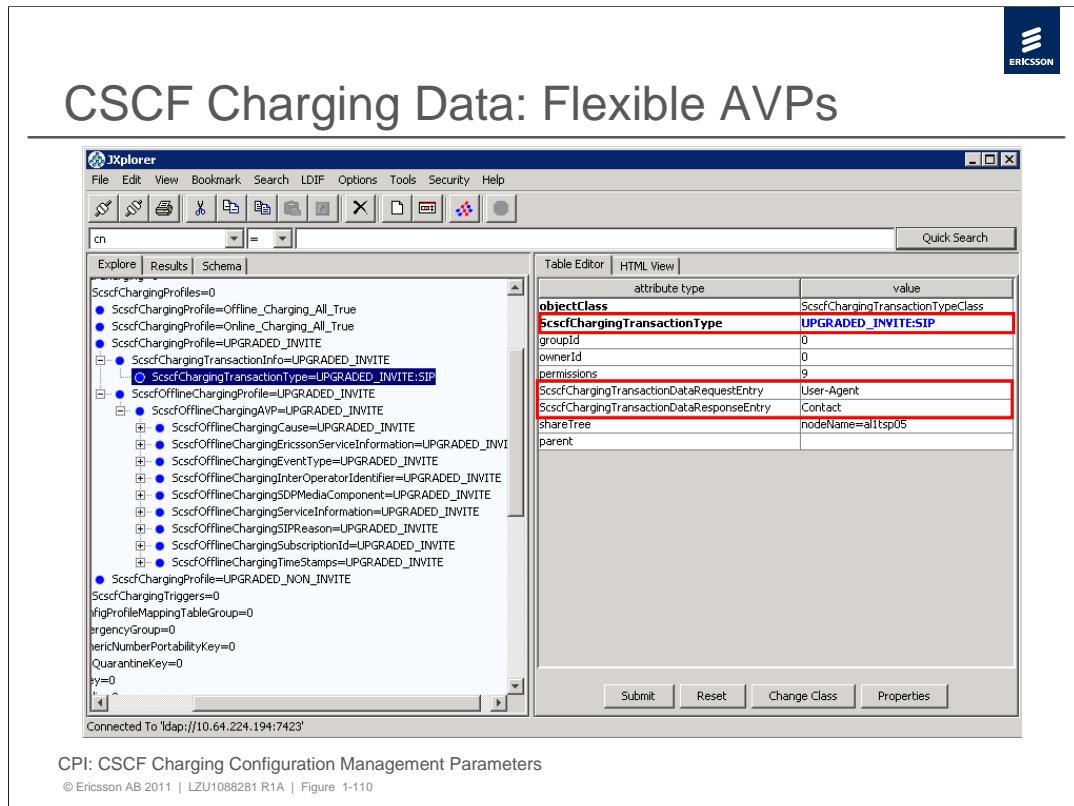
Ericsson offers the possibility to the operator to provide additional information to the charging/billing system, compared with what 3GPP specifies. With the Ericsson specific AVPs (highlighted in the picture), the operator is able to choose the best solution according to operator's charging philosophy and in order to meet the user expectation and acceptance of the new service.

Examples of the Ericsson specific AVPs are:

ScscfOfflineChargingAuthenticationMethod is used to report the authentication method of a registered subscriber to the charging system via an AVP called Authentication-Method. This AVP is available both for Offline and Online Charging. Possible values: NoAuthentication=0; AkaAuthentication=1; NassBundledAuthentication=2; DigestAuthentication=3; SsoAuthentication=4

Note that Authentication type = NoAuthentication represents 2 cases: authentication disabled in the CSCF node and authentication enabled but performed in a trusted gateway.

ScscfOfflineChargingTransactionInfo is used to include the content of the SIP header specified by configurations (see next slide) can be sent to the charging server. This AVP is available both for Offline and Online Charging.



Flexible charging AVP is a new capability allowing the operator to define message header values to be recorded in AVPs of ACRs and CCRs. CSCF supports up to 20 flexible AVP configurations. This means the operator can configure up to 20 flexible AVP configurations for matching SIP message headers. Within the limit of 20 configurations, the operator decides the breakdown of the number of Request Header matching configurations and the number of Response Header matching configurations.

If the configured Header field is found in the message, a flexible AVP called Transaction-Info AVP will be used to output the content of the matching SIP header. These Transaction-Info AVPs are for both the Rf and Ro interfaces and for SCSCF only. These Transaction-Info AVPs are available for all ACR types (i.e., Start, Interim, Stop, Event) and CCR types (initial, update, terminate).

ScscfChargingTransactionType – specifies what kind of transaction type is of interest, for example SIP. Syntax: <profileName>:SIP

ScscfChargingTransactionDataRequestEntry – specifies which Header field name to be matched in a SIP request.

ScscfChargingTransactionDataResponseEntry – specifies which Header field name to be matched in a SIP response.



CSCF Emergency Call Handling Data

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn

Quick Search

Explore Results Schema

World

- nodeName=allsp05
 - applicationName=CSCF
 - CscfAccessNetworkAssertionKey=0
 - CscfAuthenticationGroup=0
 - CscfCharging=0
 - CscfConfigProfileMappingTableGroup=0
 - CscfEmergencyGroup=0
 - CscfEmergency=default
 - CscfGenericNumberPortabilityKey=0
 - CscfHssQuarantineKey=0
 - CscfKey=0
 - CscfNwifContainerKey=0
 - CscfNumPortabilityKey=0
 - CscfProfileGroup=0
 - CscfRegistrationGroup=0
 - CscfResourceBroker=0
 - CscfSipMsgPreProcessingKey=0
 - CscfUaRoutingKey=0
 - CscfUnallocatedRoutingKey=0
 - CscfKey=0

HTML View Table Editor

attribute type	value
CscfEmergency	default
objectClass	CscfEmergencyClass
PcscfAltServiceIndicationContent-Type	/
PcscfECBehavior	prioritizeECCall
EcscfCalledNumberManipulation	FALSE
EcscfDefaultPSAPNumber	+4687163044
EcscfEmergencyRFCAddress	192.168.100.21
EcscfEmergencyPhoneContext	edu.mmtel.net
EcscfFetchRefLocationInfo	TRUE
EcscfHttpDigestPw	*****
EcscfHttpDigestUsername	
EcscfHttpLocalAddress	10.64.227.195
EcscfHttpRequestTimer	500
EcscfPutPsapNumberInRn	FALSE
EcscfSoapBehavior	1
groupId	10
ownerId	0
PcscfAltServiceIndication	
PcscfECNumberList	112
PcscfEcscfAddress	all1cscf.edu.mmtel.net
permissions	9
CscfEmergencyPhoneContext	+46
CscfIgnoreIfcForEmergencyCall	FALSE

Submit Reset Change Class Properties

Connected To 'ldap://10.64.224.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-111

Beside the CscfEmergency=default instance, there cannot be any other instances. It contains the parameters for configuring Emergency Call Handling data. Note: for backwards compatibility, some of the parameters can also be configured in the CscfSipMsgPreProcessingKey and EcscfKey instances.

PcscfECBehavior sets the P-CSCF behavior upon the detection of an emergency call. Possible values are:

•**redirectECCall:** If an emergency call is detected, a 380 non-compressed negative response will be sent back in order to redirect the call, therefore indicating that the IMS network will not handle it. In addition a text specified by the parameter *PcscfAltServiceIndication* will be added in the body of such 380 message.

•**prioritizeECCall:** Emergency call detection is performed. Emergency calls to numbers defined in the *PcscfECNumberList* will be prioritized and calls detected as normal ones will not be prioritized.

EcscfCalledNumberManipulation if set to True the called number can be manipulated (by invoking the Number Normalization feature) before it is sent to LRF

EcscfDefaultPSAPNumber defines a default number to be used within the E-CSCF as input to number normalization and external selection, if no telephone number has been received from the LRF (not available or faulty) and no telephone number is available in the Request-URI of the incoming INVITE or a routable SIP address is not available.



CSCF Emergency Call Handling Data

JXplorer interface showing the configuration of CSCF Emergency Call Handling Data.

The left pane shows the LDAP tree structure under 'cn' with various attributes like node name, application name, and emergency-related parameters.

The right pane displays the 'Table Editor' with the following data:

attribute type	value
CscfEmergency	default
objectClass	CscfEmergencyClass
PccfAltServiceIndicationContent-Type	/
PccfECBehavior	prioritizeECCall
EcsfcCalledNumberManipulation	FALSE
EcsfcDefaultPSAPNumber	+4667163044
EcsfcEmergencyLRFAddress	192.168.100.21
EcsfcEmergencyPhoneContext	edu.mmtel.net
EcsfcFetchRefLocationInfo	TRUE
EcsfcHttpDigestPw	*****
EcsfcHttpDigestUserName	
EcsfcHttpLocalAddress	10.64.227.195
EcsfcHttpRequestTimer	500
EcsfcPutPsapNumberInRn	FALSE
EcsfcSoapBehavior	1
groupID	0
ownerId	0
PccfAltServiceIndication	
PccfECNumberList	112
PccfEcsfAddress	all@ecsfc.edu.mmtel.net
permissions	9
SccsfEmergencyPhoneContext	+46
SccsfIgnoreIcfForEmergencyCall	FALSE

Connected To 'ldap://10.64.224.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-112

EcsfcEmergencyLRFAddress is used to store the address for the LRF node available in the network. If the address has not been defined, no interaction with the LRF will be performed.

EcsfcEmergencyPhoneContext defines the emergency phone context to be used as input to number normalization together with the telephone number received from the LRF, or if the telephone number received from the LRF is a non-international number.

EcsfcFetchRefLocationInfo if set to True, E-CSCF will try to fetch the reference access location info from HSS (only if PANI header is missing in the incoming INVITE). Note: as a pre-requisite, the Diameter interface between E-CSCF and HSS must be properly configured on both sides.

EcsfcHttpDigestUserName and *EcsfcHttpDigestPw* define the credentials used in case HTTP Digest Authentication is enabled towards the LRF

EcsfcHttpLocalAddress defines the IP address the E-CSCF uses to receive and send HTTP traffic to and from the LRF.

EcsfcPutPsapNumberInRn determines where to place the PSAP number received from the LRF. If set to True it will be placed as a Routing Number (RN) in the user part of the Request-URI; otherwise (False) it will completely replace the Request-URI.

EcsfcSoapBehavior determines if the retrieval of a PSAP number shall be based on the location (parameter set to 1 and SOAP1.1 is used) or based on IP-address (parameter set to 2 and SOAP1.2 is used)

PccfECNumberList contains the list of numbers to be regarded as Emergency Numbers

CSCF User-Level Media Authorization Activation

The screenshot shows the JXplorer LDAP browser interface. The left pane displays a tree view of LDAP entries under 'World' and 'nodeName=jambals'. The right pane shows a table editor for configuration parameters. One parameter, 'CscfSmpAuthorization', is highlighted with a red border. The table has columns for 'attribute type' and 'value'.

attribute type	value
CscfResourceBrokerEntry	3:7:TCP,192.168.7.99,5062,2,
CscfScscfFailoverTimer	7
CscfSendRequestUpOnly	FALSE
CscfServiceUserIdentitySelection	alwaysUseDefault
CscfServiceRouteHeaderEnablePCscf	TRUE
CscfSessionRefreshDefault	30
CscfSessionRefreshMax	60
CscfSessionRefreshMin	2
CscfSigCompEnabled	FALSE
CscfSmpMKey	IoAddr
CscfSmpAuthorization	Active
CscfSSOAuthentication	FALSE
CscfTimerBValue	32000
CscfTimerCValue	180000
CscfTimerDValue	32000
CscfTimerFValue	32000
CscfTimerT1Value	500
CscfTimerT2Value	4000
CscfTimerT4Value	5000
CscfTraceIDEntry	
CscfTrustedASEntry	192.168.7.4

Connected To 'ldap://192.168.13.194:7423'

CPI: CSCF Common Configuration Management Parameters

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-113

CscfSmpAuthorization disables or enables the Subscribed Media Profile (SMP) Authorization function. Possible values: Active, Inactive.



CSCF User-Level Media Authorization

Subscribed Media Profile

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn

Explore Results Schema

World

- > ● nodeName=jambala
 - > ● applicationName=CSCF
 - > ● CscfCharging=0
 - > ● CscfHssQuarantineKey=0
 - > ● CscfLkKey=0
 - > ● CscfMedia=0
 - > ● CscfMaxMediaFlowTables=0
 - > ● CscfMaxMediaFlowTable=cscf
 - > ● CscfMediaAuthorizationPolicy=0
 - > ● CscfPayloadBlackWhiteLists=0
 - > ● CscfPayloadBlackWhiteList=cscf
 - > ● CscfSmpAuthorizationPolicy=0
 - > ● CscfSmpAuthorizationPolicyId=1
 - > ● CscfNumPortabilityKey=0
 - > ● CscfNwIfContainerKey=0
 - > ● CscfSipMsgPreProcessingKey=0
 - > ● CscfUaRestrictionKey=0
 - > ● CscfUnallocatedRoutingKey=0
 - > ● EcscfkKey=0

HTML View Table Editor

attribute type	value
CscfSmpAuthorizationPolicyId	1
CscfSmpMaxMediaFlowTableName	cscf
CscfSmpPayloadBlackWhiteListName	cscf
objectClass	CscfSmpAuthorizationPolicyEntry
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=jambala
parent	

Submit Reset Change Class Properties

Connected To 'ldap://192.168.13.194:7423'

CPI: CSCF Common Configuration Management Parameters

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-114

CscfSmpAuthorizationPolicyId is a key to the SMP policy data, used to be compared with Subscriber Media Profile value during the authorization.

CscfSmpMaxMediaFlowTableName is an identity of the max flow per media type table for S-CSCF SMP Authorization.

CscfSmpPayloadBlackWhiteListName is an identity of the payload black and white list for SMP Authorization. During SMP Authorization the list is always interpreted as white.

The screenshot shows the JXplorer LDAP browser interface. The left pane displays the LDAP tree structure under the 'cn' root, with several entries expanded, such as 'CscfEmergencyGroup=0', 'CscfGenericNumberPortabilityKey=0', 'CscfHssQuarantineKey=0', 'CscfLike=0', and 'CscfMedia=0'. One entry, 'CscfMaxMediaFlowTable=cscf', is highlighted with a red arrow. The right pane shows the 'Table Editor' with attribute-value pairs for a selected object. The following attributes are listed:

attribute type	value
CscfMediaAuthorizationPolicy	0
objectClass	CscfMediaAuthorizationPolicyContainer
CscfEarlyMediaGatingPolicy	OpenDownLinkGates
CscfMaxDownLinkBandwidth	200
CscfMaxMediaFlowTableName	cscf
CscfMaxUplinkBandwidth	200
CscfMediaBearerAuthorizationPolicy	Inactive
CscfMediaCodecAnalysisAccordingToBlackList...	FALSE
CscfMediaOnHoldBehavior	NoFlowStatusChange
CscfPayloadBlackWhiteListName	cscf
CscfRxDestHostAddress	
CscfRxDestRealmAddress	
CscfRxOrigHostAddress	
CscfRxOrigRealmAddress	
CscfUseBearerAuthIncludeApplicationId	FALSE
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=al1tsp05
parent	

Connected To 'ldap://10.64.224.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-115

CscfMaxMediaFlowTableName is an identity of the max flow per media type table for P-CSCF Media Authorization.

CscfMediaBearerAuthorizationPolicy enables the P-CSCF to either activate or inactivate the Media Authorization and/or Bearer authorization function. Possible values:

- Inactive
- MediaAuthOnly = Only the media in the SDP negotiation is authenticated
- MediaAndBearerAuth = Media and Bearer, by invoking the PCRF, are authenticated

CscfMediaCodecAnalysisAccordingToBlackListLogic activates the black list when set to True (and the white list when is set to False).

CscfPayloadBlackWhiteListName is an identity of the payload black and white list for P-CSCF Media Authorization.

Max Media Flow Table

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view under 'World' shows a node named 'nodeName=al1tsp05' which contains various CSCF-related entries. One entry, 'CscfMaxMediaFlowTable=cscf', is selected and expanded, revealing its attributes. On the right, the 'Table Editor' tab is active, displaying a table of attributes and their values:

attribute type	value
CscfMaxFlowPerMediaTypeApplication	10
CscfMaxFlowPerMediaTypeAudio	10
CscfMaxFlowPerMediaTypeControl	10
CscfMaxFlowPerMediaTypeData	10
CscfMaxFlowPerMediaTypeImage	10
CscfMaxFlowPerMediaTypeMessage	10
CscfMaxFlowPerMediaTypeModel	10
CscfMaxFlowPerMediaTypeMultipart	10
CscfMaxFlowPerMediaTypeText	10
CscfMaxFlowPerMediaTypeVideo	10
CscfMaxMediaFlowTable	cscf

Below the table, other attributes are listed:

objectClass	value
CscfMaxMediaFlowTableClass	
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=al1tsp05
parent	

At the bottom of the editor are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

Connected To 'ldap://10.64.224.194:7423'

The CscfMaxMediaTableName is used as a key both for User-level and Network-level media authorizations.

The remaining parameters specify the number of Media Components that are allowed for each Media Type.



Payload Black/White List

JXplorer interface showing the Payload Black/White List configuration.

The left pane shows the LDAP tree structure under 'cn' with various node names like 'nodeName=al1tsp05' and 'applicationName=CSCF'. A specific entry 'CscfPayloadBlackWhiteList=cscf' is selected.

The right pane displays the 'Table Editor' for the selected entry. The table has two columns: 'attribute type' and 'value'.

attribute type	value
CscfPayloadBlackWhiteList	cscf
objectClass	CscfPayloadBlackWhiteListClass
CscfPayloadBlackWhiteEntry	cscf:audio:ilbc
CscfPayloadBlackWhiteEntry	cscf:audio:pcmu
CscfPayloadBlackWhiteEntry	cscf:audio:telephone-event
CscfPayloadBlackWhiteEntry	cscf:audio:isac
CscfPayloadBlackWhiteEntry	cscf:audio:eg711u
CscfPayloadBlackWhiteEntry	cscf:audio:eg711a
CscfPayloadBlackWhiteEntry	cscf:audio:g723
CscfPayloadBlackWhiteEntry	cscf:audio:g729
CscfPayloadBlackWhiteEntry	cscf:audio:ipcmvb
CscfPayloadBlackWhiteEntry	cscf:audio:amr:1
CscfPayloadBlackWhiteEntry	cscf:audio:pcma

Below the table are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. The status bar at the bottom indicates 'Connected To 'ldap://10.64.224.194:7423''.

The Payload Black/White List determines which codecs are allowed (not allowed).

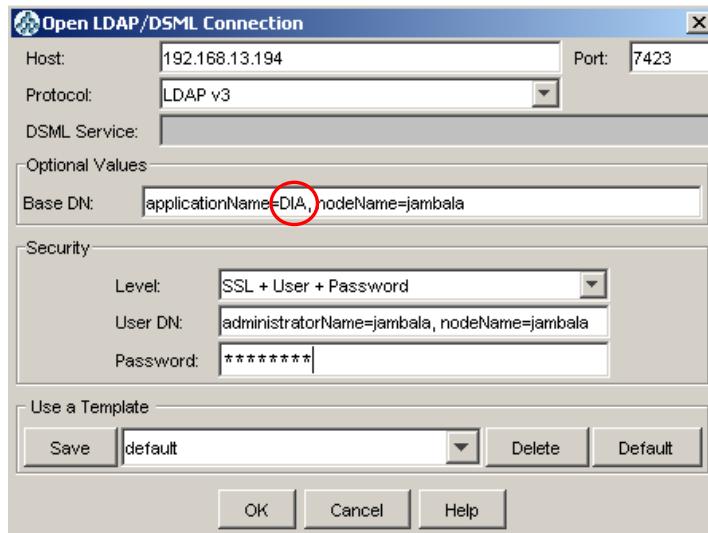
In case of User-level Media Authorization, this list is always seen as White List, which means all the codecs in the SDP of the INVITE message must be present in this list, otherwise the request will be rejected.

In case of a Network-level Media Authorization instead, the list can be either White or Black. The parameter

CscfMediaCodecAnalysisAccordingToBlackListLogic in the *CscfMediaAuthorizationPolicy* container specifies if the list is White (FALSE) or Black (TRUE). If the SDP contains at least one codec that has been specified in the Black list, the request will be rejected.



Login to the Diameter application (CSCF)



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-118

The Application name for the Diameter application is *DIA*.

In the Diameter application it is possible to configure and verify the Cx Interface towards the HSS, the Rf and Ro interface towards MM and Rx interface towards PCRF.

In the Diameter application it is also possible to configure Sh interface between E-CSCF and HSS and Dh interface between E-CSCF and SLF.

Diameter application identities are as follows:

16777216 – Cx interface

16777236 – Rx interface

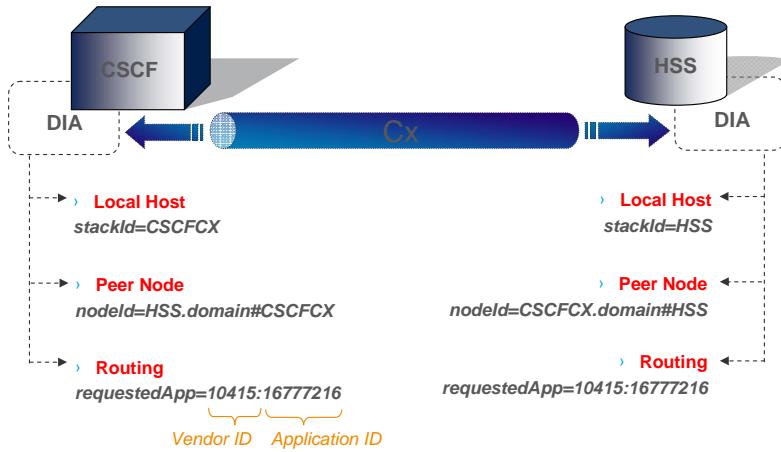
16777217 – Sh and Dh interfaces

3 – Rf interface

4 – Ro interface



Diameter Link Basic Example



CPI: Diameter Parameter List

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-119

A Diameter link is established by configuring 3 main sets of parameters:

- Local Host information, including local IP-address, local port number, supported applications, transport protocol, etc.
- Peer Node information, including remote IP-address, remote port number, etc.
- Routing information, including the applications used for incoming and outgoing messages and node Ids (only in case of outgoing messages)

The screenshot shows the JXplorer LDAP browser interface. The left pane displays a tree structure of LDAP objects under 'World' and 'nodeName=jambala'. The right pane shows a table editor for modifying attributes. Many attributes are highlighted with red boxes, indicating they are being modified or are important parameters. A vertical sidebar on the right lists 'CPI: Diameter Parameter List'.

attribute type	value
hostId	CSCFCX.edu.ms.se
objectClass	DIA-CFG-OwnNodeConfig
portNr	3868
productName	Ericsson Diameter
realm	edu.ms.se
stackId	CSCFCX
supportedVendorIds	0
supportedVendorIds	10415
allowConnectFromUnknownNode	FALSE
disVendorId	10415
disabled	TRUE
firmwareRevision	1
groupid	0
ipAddressesList	0.0.0.0:799
loadRegulationEnabled	FALSE
maxInboundSctpStreams	1
maxNumberOffRetries	3
maxOutboundSctpStreams	1
maxRequestPendingTime	10
ownerId	0
permissions	63
sendErrorAtOverload	FALSE
shareTree	applicationName=DIA,nodeName=jambala
supportedAuthAppIds	16777216
supportedVendorSpecificApps	0:0415:16777216:16777216
supportedVendorSpecificApps	1:0:16777216:16777216
tcTimer	10
transportLayerType	1
watchdogTimeidle	8

In the figure the local host data for the CSCF side of the Cx interface is shown.

Some of the parameters are highlighted.

PortNr - This is the local listener port number that the remote diameter nodes are using for communication with this node.

enabled - This boolean can be set to FALSE whenever the node should suspend its activity. It may be used instead of clearing all "enabled" parameters for neighbourNodes separately.

ipAddressesList – It is a list of IPv4 addresses (string) that makes the own node accessible when using transport protocol TCP. The first address in the list is considered the primary one. This list is checked to find out if any of the IP addresses in the list are repeated, and if so, an LDAP error will be raised, and the operation will not take place.

supportedAuthAppIds – This attribute is a list of applications that supports Authentication or Authorization requests. The Authentication Application ID defined by 3GPP for the Cx interface is 16777216.

transportLayerType defines the transport layer to be used when setting up a connection to this node. Values: 0 = Not defined (creation value), 1 = TCP, 2 = SCTP and 3 = First SCTP, then TCP.

The following Diameter vendor IDs are commonly found:

0:IETF, 10415:3GPP, 13019:ETSI, 193:Ericsson

The screenshot shows the JXplorer interface with the title "Cx(/Dx)Interface data - Peer Node". The left pane displays a tree view of the LDAP structure under "cn=World", including nodes like "nodeName=al1tsp01", "applicationName=DIA", "stackContainerId=CSCFCX", "connId=HSS.edu.mmtel.net#CSCFCX", "connId=CSCFCX#HSS.edu.mmtel.net#conn1", "routingContainerId=CSCFCX", "stackId=CSCFCX", "stackContainerId=CSCFRF", "stackContainerId=CSCFRO", "stackContainerId=CSCFRX", "configuration=Diameter", "dictionaryContainerName=dictionaryContainerName", "stackContainerId=HSS_ESM", "stackContainerId=HSS_SM", "stackContainerId=HSS", and "securityContainerName=securityContainerName". The right pane shows a table editor for the selected "connId=HSS.edu.mmtel.net#CSCFCX#conn1" entry. The table has two columns: "attribute type" and "value". The values for the highlighted parameters are:

attribute type	value
nodeId	HSS.edu.mmtel.net#CSCFCX
objectClass	DIA-CFG-NeighbourNode
connIds	0:CSCFCX#HSS.edu.mmtel.net#conn1
diaVendorId	193
enabled	TRUE
firmwareRevision	1
groupId	0
initiateConnection	TRUE
ipAddressesList	0:10.64.227.196
isDynamic	FALSE
ownerId	0
permissions	9
portNr	3872
productName	Ericsson Diameter
realm	edu.mmtel.net
shareTree	applicationName=DIA,nodeName=al1tsp01
supportedAuthAppIds	16777216
supportedVendorsIds	193
supportedVendorsIds	10415
supportedVendorSpecificApps	0:0:10415:16777216:0
supportedVendorSpecificApps	1:193:16777228:0
supportedVendorSpecificApps	2:10415:16777217:0
supportedVendorSpecificApps	3:193:16777227:0
transportLayerType	1
parent	
sctpAddressesList	
supportedAcctAppIds	

Connected To 'ldap://10.64.224.193:7423'

CPI: Diameter Parameter List

In the figure the Cx Interface Peer Node (HSS) data is shown. In the case SLF is present in the system the SLF has to be configured as a peer node as well (Dx interface).

Some of the parameters are highlighted.

connIds - is a list of those connIds that uses this diaNeighbourNodeId.

enabled - This Boolean flag can be set by the traffic part or the OAM administrator when there is any reason that the Diameter Server does not accept request from this node. It must be set to *TRUE* by default when the Neighbor Node is created.

ipAddressessList – It is a list of IPv4 addresses that makes the neighbor node accessible when using transport protocol TCP. The first address in the list is considered the primary one.

portNr – is the remote port number used for the communication with the Diameter Peer node.

supportedAuthAppIds – This attribute is a list of applications that supports Authentication or Authorization requests. The Authentication Application ID defined by 3GPP for the Cx interface is 16777216.

transportLayerType - defines the transport layer to be used when setting up a connection to this node. Values: 0 = *Not defined (creation value)*, 1 = *TCP*, 2 = *SCTP* and 3 = *First SCTP, then TCP*.

The following Diameter vendor IDs are commonly found:

0:IETF, 10415:3GPP, 13019:ETSI, 193:Ericsson

Cx(/Dx)Interface data - Connection

The screenshot shows the JXplorer interface with the following details:

- Left Panel (Explore View):** Shows the LDAP tree structure under the 'cn' root. A specific connection entry is selected: `connId=CSCFCX#HSS.edu.mmtel.net#conn1`.
- Right Panel (Table Editor):** Displays the attributes of the selected connection. The table has two rows: 'attribute type' and 'value'. The 'objectClass' row is highlighted with a red border.

attribute type	value
connId	CSCFCX#HSS.edu.mmtel.net#conn1
objectClass	DIA-CFG-Conn
blockReason	Not blocked
connectedAddress	10.64.227.196
enabled	TRUE
groupID	0
linkStatus	Up
ownerID	0
permissions	9
shareTree	applicationName=DIA,nodeName=al1tsp01
transportLayerType	1
ipAddressesList	
parent	
sctpAddressesList	

Buttons at the bottom of the right panel include: Submit, Reset, Change Class, and Properties.

CPI: Diameter Parameter List

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-122

The "connId" window provides information about the connection to the peer-node, like link status, blocking reasons (if link is blocked), etc.

The most relevant attributes are:

enabled - This boolean flag is set to TRUE when the Diameter Node accepts a connection request from this Peer Node on this connection or when the Diameter Node sets up a connection toward this Peer Node connection (depending on the value set in *initiateConnection* attribute for the Peer Node). When set to FALSE, no connection is allowed.

linkStatus - indicates the status of the connection. Values: *initial*, *up*, *down*, *suspect* and *reopen*.

blockReason - This attribute contains information if the connection is blocked for any reason. For a list of possible values please refer to the Diameter Parameter List document in CPI.

connectedAddress - This attribute contains the TCP or SCTP address that is used for this connection (this is a "read-only" attribute).

The screenshot shows the Ericsson CX interface with the following details:

- Explorer Pane:** Shows a tree structure under 'World' with nodes like 'nodeName=jambala' and 'applicationName=DIA'. Under 'DIA', there's a 'stackContainerId=CSCFCX' node which further contains 'peerNodeContainerId=CSCFCX' and 'routingContainerId=CSCFCX'.
- Table Editor Pane:** Displays a table of parameters for a selected node. The highlighted parameters are:

attribute type	value
action	4
objectClass	DIA-CFG-AppRouting
requestedApp	10415:16777216
nodeId	0
nodeIds	0:HSS.edu.ims.se#CSCFCX
ownerId	0
permissions	9
shareTree	applicationName=DIA,nodeName=jambala
parent	
- Bottom Status Bar:** Shows 'Connected To ldap://192.168.13.194:7423'
- CPI Information:** A vertical bar on the right indicates 'CPI: Diameter Parameter List'.

In the figure the Cx Routing Data for the CSCF side is shown when no SLF is present in the system.

Some of the parameters are highlighted.

entryId - This attribute represents an entry in the Realm Routing Table (RRT). The RRT is realm based, and for a certain realm and a given *stackId*, there may be at most two RRTs, depending on the need of an application to process incoming traffic and generate outgoing messages. The *entryId* consists of the parts which are *realm*, *stackId* and *isIncomingRequest*. The *isIncomingRequest* field in the *entryId* attribute is *true* for routing incoming requests, and *false* for outgoing requests.

action - The routing action from requests for a certain realm and a given request type that belongs to the Diameter application specified in the *requestedApp* attribute.

Values: 0 – local, 1 – relay, 2 – proxy, 3 – redirect, 4 – none, 5 – other.

All actions except none (4) are valid when the *isIncomingRequest* is set to *TRUE*.

requestedApp - This attribute is the vendor's Diameter application whose messages are recognized by the RRT.

nodeIds - One or more servers that the message is to be routed to. If *action=none*, these servers must be defined as Neighbour Nodes. If *action=redirect*, these servers can be any defined node. This list cannot be left empty if *action=redirect*, or *action=none*. For remaining actions, this list must be empty.

Cx/Dx Interface data – Routing (with SLF)

attribute type	value
action	4
objectClass	DIA-CFG-AppRouting
requestedApp	10415:16777216
groupid	0
nodeIds	0:sit.edu ims.se#CSCFCX
ownerId	0
permissions	9
shareTree	applicationName=DIA,nodeName=jambala
parent	

Connected To 'ldap://192.168.13.194:7423'
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-124

In the figure the Dx Routing Data for the I/S-CSCF side is shown when SLF is present in the system (also valid for E-CSCF Sh interface).

Some of the parameters are highlighted.

entryId - This attribute represents an entry in the Realm Routing Table (RRT). The RRT is realm based, and for a certain realm and a given *stackId*, there may be at most two RRTs, depending on the need of an application to process incoming traffic and generate outgoing messages. The *entryId* consists of the parts which are *realm*, *stackId* and *isIncomingRequest*. The *isIncomingRequest* field in the *entryId* attribute is *true* for routing incoming requests, and *false* for outgoing requests.

action - The routing action from requests for a certain realm and a given request type that belongs to the Diameter application specified in the *requestedApp* attribute.

Values: 0 – local, 1 – relay, 2 – proxy, 3 – redirect, 4 – none, 5 – other.

All actions except none (4) are valid when the *isIncomingRequest* is set to *TRUE*.

requestedApp - This attribute is the vendor's Diameter application whose messages are recognized by the RRT.

nodeIds - One or more servers that the message is to be routed to. If *action=none*, these servers must be defined as Neighbour Nodes. If *action=redirect*, these servers can be any defined node. This list cannot be left empty if *action=redirect*, or *action=none*. For remaining actions, this list must be empty.

The screenshot shows the JXplorer LDAP browser interface. On the left, there's a tree view of objects under 'cn=cn'. On the right, there's a table editor for the selected 'cn=cn' object. The table has columns for 'attribute type' and 'value'. Several parameters are highlighted with red boxes:

attribute type	value
hostId	CSCFRF.edu.ims.se
objectClass	DIA-CFG-OwnNodeConfig
portNr	19999
productName	Ericsson Diameter
realm	edu.ims.se
stackId	CSCFRF
supportedVendorIds	0
supportedAuthAppIds	10415
allowConnectFromUnknownNode	FALSE
diaVendorId	10415
enabled	TRUE
firmwareRevision	1
logLevel	0
ipAddressesList	0.192.168.7.99
loadRegulationEnabled	FALSE
maxInboundSctpStreams	1
maxNumberOfRetries	3
maxOutboundSctpStreams	1
maxRequestPendingTime	5
ownerId	0
permissions	63
sendErrorAtOverload	FALSE
shareTree	applicationName=DIA nodeName=jambala
supportedAccAppIds	3
supportedVendorSpecificApps	0.0.1677216.3
frTimer	10
transportLayerType	1
watchdogTimeidle	6
parent	...

Connected To 'ldap://192.168.13.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-125

In the figure the local host data for the CSCF side of the Rf interface is shown. Some of the parameters are highlighted.

PortNr - This is the local listener port number that the remote diameter nodes are using for communication with this node.

enabled - This boolean can be set to FALSE whenever the node should suspend its activity. It may be used instead of clearing all "enabled" parameters for neighbourNodes separately.

ipAddressesList – It is a list of IPv4 addresses (string) that makes the own node accessible when using transport protocol TCP. The first address in the list is considered the primary one. This list is checked to find out if any of the IP addresses in the list are repeated, and if so, an LDAP error will be raised, and the operation will not take place.

supportedAuthAppIds – This attribute is a list of applications that supports Authentication or Authorization requests. The Accounting Application ID defined by IETF for the Rf interface is 3.

transportLayerType defines the transport layer to be used when setting up a connection to this node. Values: 0 = Not defined (creation value), 1 = TCP, 2 = SCTP and 3 = First SCTP, then TCP.

The following Diameter vendor IDs are defined in the figure.

0 : IETF defined base Diameter Protocol

10415: 3GPP defined Diameter Extensions

The screenshot shows the JXplorer LDAP browser interface. The left pane displays a tree view of LDAP entries under the 'World' root, including nodes like 'nodeName=a1tsp05', 'applicationName=CSCF', and various stack container and peer node entries. The right pane shows a table of attributes and their values for a selected entry. Several attributes are highlighted with red boxes: 'objectClass', 'connIds', 'diaVendorId', 'enabled', 'firmwareRevision', 'groupID', 'initiateConnection', 'ipAddressesList', 'isDynamic', 'ownerID', 'permissions', 'portNr', 'productName', 'realm', 'sctpHandlerLogLevel', 'shareTree', 'supportedAccAppIds', 'supportedVendorIds', and 'transportLayerType'. Below the table are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A status bar at the bottom indicates the connection is to 'ldap://10.64.224.194:7423'.

attribute type	value
nodeId	mmfe.edu.mmtel.net#CSCFRF
objectClass	DIA-CFG-NeighbourNode
connIds	0:CSCFRF#mmfe.edu.mmtel.net#conn1
diaVendorId	0
enabled	TRUE
firmwareRevision	0
groupID	0
initiateConnection	TRUE
ipAddressesList	0:10.64.224.135
isDynamic	FALSE
ownerID	0
permissions	9
portNr	3869
productName	MultiMediation
realm	edu.mmtel.net
sctpHandlerLogLevel	DEFAULT
shareTree	applicationName=DIA.nodeName=a1t...
supportedAccAppIds	3
supportedVendorIds	10415
traceSctpHandler	193
transportLayerType	1

Submit | Reset | Change Class | Properties

CPI: Diameter Parameter List

In the figure the Rf Interface Peer Node (MultiMediation) data is shown. Some of the parameters are highlighted.

connIds - is a list of those connIds that uses this diaNeighbourNodeId.

enabled - This Boolean flag can be set by the traffic part or the OAM administrator when there is any reason that the Diameter Server does not accept request from this node. It must be set to *TRUE* by default when the Neighbor Node is created.

ipAddressessList – It is a list of IPv4 addresses that makes the neighbor node accessible when using transport protocol TCP. The first address in the list is considered the primary one.

portNr – is the remote port number used for the communication with the Diameter Peer node.

supportedAccAppIds – This attribute is a list of applications that supports Accounting requests. The Accounting Application ID defined by IETF for the Rf interface is 3.

transportLayerType - defines the transport layer to be used when setting up a connection to this node. Values: 0 = *Not defined (creation value)*, 1 = *TCP*, 2 = *SCTP* and 3 = *First SCTP, then TCP*.

The following Diameter vendor IDs are shown in the figure.

0 : IETF defined base Diameter Protocol

10415: 3GPP defined Diameter Extensions

193: Ericsson defined Diameter Extensions

Rf Interface data – Routing

The screenshot shows the JXplorer LDAP browser interface. The left pane displays a hierarchical tree structure under 'cn=World'. One node is expanded to show 'applicationName=DIA', 'stackContainerId=CSCFCX', 'stackContainerId=CSCFRF', 'peerNodeContainerId=CSCFRF', 'modelId=edu.ims.se#CSCFRF', 'routingContainerId=CSCFRF', 'entryId=ee1m0f1.edu.ims.se#CSCFRF', 'isIncomingRequest=false', 'authReqContainerName=authReqContainerName', 'stackId=CSCFRF', 'stackContainerId=CSCFRO', 'stackContainerId=CSCFRX', 'configuration=Diameter', 'dictionaryContainerName=dictionaryContainerName', 'stackContainerId=PCRF', and 'securityContainerName=securityContainerName'. The right pane shows a table editor with columns 'attribute type' and 'value'. Several rows are highlighted in red: 'action' (value 4), 'objectClass' (value 'DIA-CFG-AppRouting'), 'requestedApp' (value '0-3'), 'groupid' (value 0), 'nodeIds' (value '0rf.edu.ims.se#CSCFRF'), 'ownerId' (value 0), 'permissions' (value 9), 'shareTree' (value 'applicationName=DIA,nodeName=jambala'), and 'parent' (empty). At the bottom of the right pane are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

Connected To 'ldap://192.168.13.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-127

CPI: Diameter Parameter List

In the figure the Rf Routing Data for the CSCF side is shown.

Some of the parameters are highlighted.

entryId - This attribute represents an entry in the Realm Routing Table (RRT). The RRT is realm based, and for a certain realm and a given *stackId*, there may be at most two RRTs, depending on the need of an application to process incoming traffic and generate outgoing messages. The *entryId* consists of the parts which are *realm*, *stackId* and *isIncomingRequest*. The *isIncomingRequest* field in the *entryId* attribute is *true* for routing incoming requests, and *false* for outgoing requests.

action - The routing action from requests for a certain realm and a given request type that belongs to the Diameter application specified in the *requestedApp* attribute.

Values: 0 – local, 1 – relay, 2 – proxy, 3 – redirect, 4 – none, 5 – other.

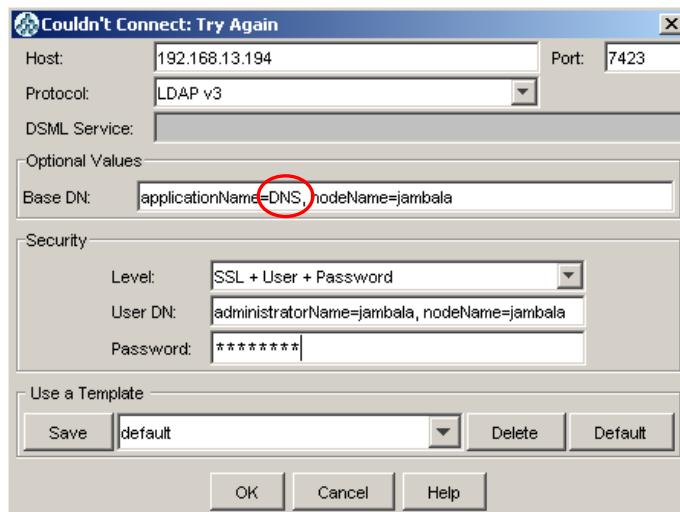
All actions except none (4) are valid when the *isIncomingRequest* is set to TRUE.

requestedApp - This attribute is the vendor's Diameter application whose messages are recognized by the RRT.

nodeIds - One or more servers that the message is to be routed to. If *action=none*, these servers must be defined as Neighbour Nodes. If *action=redirect*, these servers can be any defined node. This list cannot be left empty if *action=redirect*, or *action=none*. For remaining actions, this list must be empty.



Login to the DNS application



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-128

The Application name for the DNS application is *DNS*.

The screenshot shows the Ericsson iXplorer LDAP browser interface. The left pane displays a tree view under 'World' with nodes 'nodeName=jambala' and 'applicationName=DNS'. The right pane shows a table of attributes for the 'applicationName=DNS' entry. The table has columns 'attribute type' and 'value'. Several attributes are highlighted with a red border: 'applicationName' (value: DNS), 'DnsCacheSize' (value: 0), 'DnsLocalAddress' (value: 192.168.7.99), 'DnsRetransmissionTimer' (value: 100), 'DnsServerEntry' (value: 192.168.7.3:53), and 'DnsUnavailabilityCacheTTL' (value: 60). Other visible attributes include 'groupId' (value: 0), 'objectClass' (value: DNS-Application), 'ownerId' (value: 0), 'permissions' (value: 9), and 'shareTree' (value: nodeName=jambala). At the bottom of the right pane are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A status bar at the bottom of the window indicates 'Connected To ldap://192.168.13.194:7423'.

attribute type	value
applicationName	DNS
DnsCacheSize	0
DnsLocalAddress	192.168.7.99
DnsRetransmissionTimer	100
DnsServerEntry	192.168.7.3:53
DnsUnavailabilityCacheTTL	60
groupId	0
objectClass	DNS-Application
ownerId	0
permissions	9
shareTree	nodeName=jambala

CPI: DNS Configuration Management Parameters
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-129

Example of data defined for the connection to the DNS/ENUM is shown in the figure.

DnsCacheSize - This attribute defines the maximum number of the cache objects can be saved in the DNS cache pot.

DnsLocalAddress - This attribute defines source IP addresses used when sending DNS queries (up to 10 IP addresses can be configured).

DnsRetransmissionTimer - This attribute defines the retransmission timer in *ms* for the DNS stack, to retransmit queries to the external DNS server.

DnsServerEntry - This attribute defines the IP address and port of the DNS server (syntax: *ipAddress:ipPort*).

DnsUnavailabilityCacheTTL - Defines the time in seconds the DNS will store gateways (for instance I-CSCFs) in the system, that the application has registered as 'unavailable' in the cache.

In order to be more resilient against forged DNS queries, it is possible for the DNS client to send queries from unpredictable UDP source IP addresses. The chosen source IP address is randomly selected from the configured *DnsLocalAddress* entries (max 10). Moreover, the DNS client will generate up to 10 UDP source ports (per configured IP address) and randomly choose among them when sending the DNS query.



Number Portability

From RFC3482:

"NP is a regulatory imperative seeking to liberalize local telephony service competition, by enabling end-users to retain telephone numbers while changing service providers"



Two possible schemas:

- All Call Query (ACQ)
- Onward Routing (OR)

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-130

NP changes the fundamental nature of a dialed E.164 number *from a hierarchical physical routing address to a virtual address*. There are considered to be three types of number portability (NP): service provider number portability (SPNP; e.g. from Operator A to Operator B), location portability (not to be confused with terminal mobility; e.g. from fixed Location A to fixed Location B), and service portability (e.g. from Plain Old Telephony Service (POTS) to Integrated Services Digital Network (ISDN) services).

NP implementations attempt to make NP transparent to subscribers by incorporating a translation function to map a dialed, potentially ported E.164 address, into a network routing address (either a number prefix or another E.164 address) which can be hierarchically routed.

The *donor network* is the network that first assigned a telephone number to a subscriber, out of a number range administratively assigned to it.

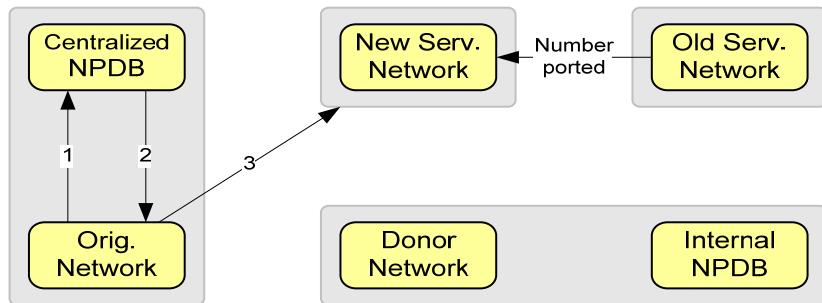
The current service provider (new SP), or *new serving network*, is the network that currently serves the ported number.

The *old serving network* (or old SP) is the network that previously served the ported number before the number was ported to the new serving network.

Since a Telephone Number can port a number of times, the old SP is not necessarily the same as the donor network, except for the first time the TN ports away, or when the TN ports back into the donor network and away again. While the new SP and old SP roles are transitory as a TN ports around, the donor network is always the same for any particular TN.



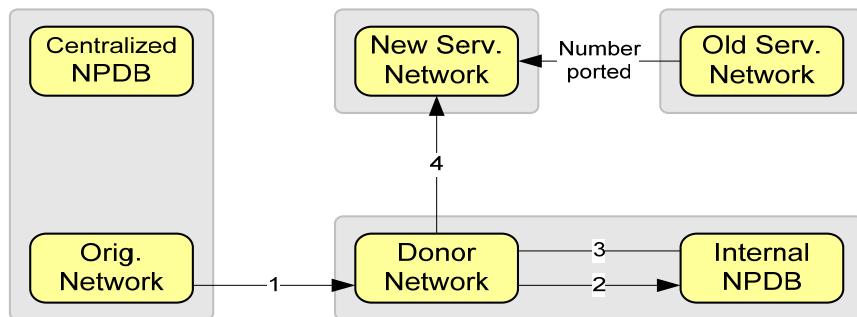
Number Portability - All Call Query (ACQ)



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-131

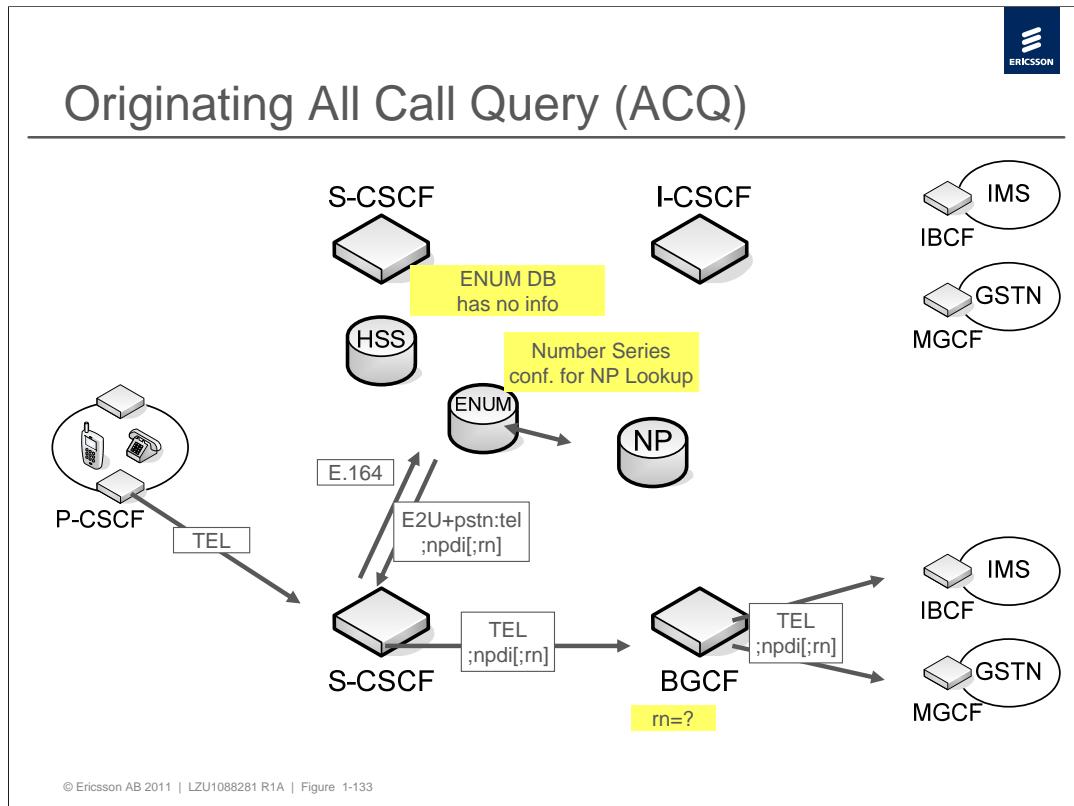
- 1) The Originating Network receives a call from the caller and sends a query to a centrally administered Number Portability Database (NPDB), a copy of which is usually resident on a network element within its network or through a third party provider.
- 2) The NPDB returns the routing number associated with the dialed directory number. The routing number is discussed later in Section 6.
- 3) The Originating Network uses the routing number to route the call to the new serving network.

Number Portability - Onward Routing (OR)



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-132

- 1) The Originating Network receives a call from the caller and routes the call to the donor network
- 2) The donor network detects that the dialed directory number has been ported out of the donor switch and checks with an internal network-specific NPDB
- 3) The internal NPDB returns the routing number associated with the dialed directory number
- 4) The donor network uses the routing number to route the call to the new serving network

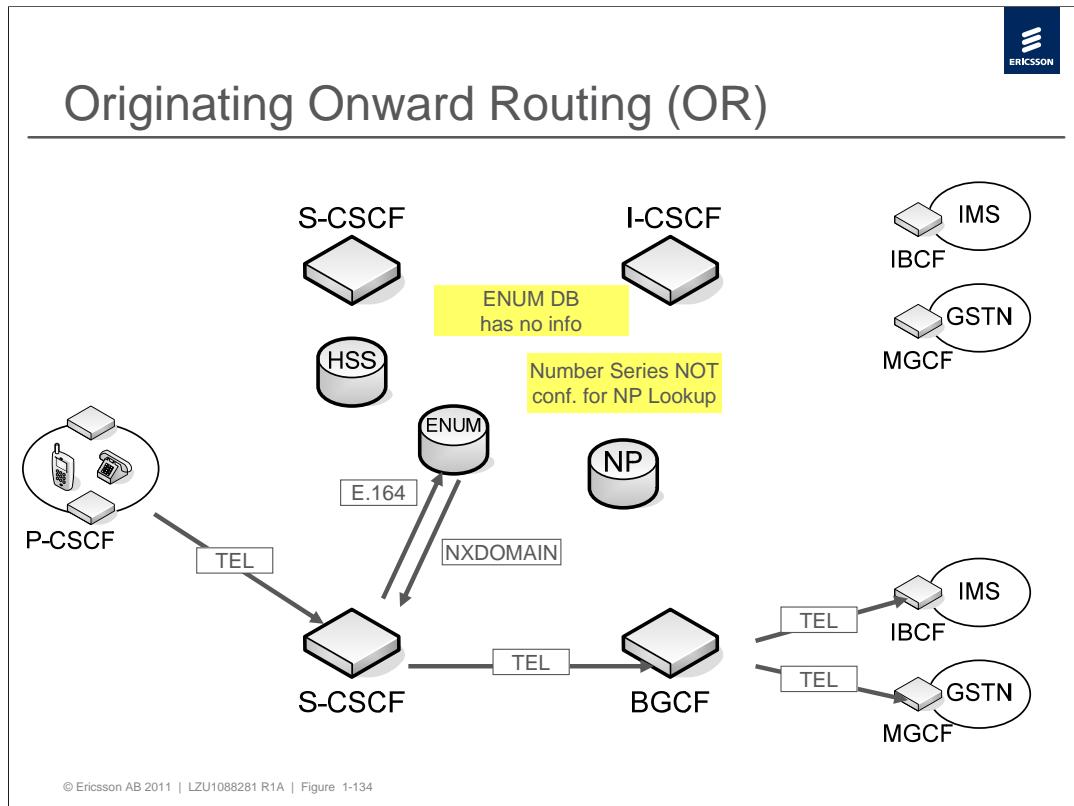


Pre-Conditions:

- No ENUM entry exists for the B-party phone number. The B-party phone number belongs to an operator that expects ACQ behavior.
- The number series that the B-party phone number belongs to has been configured as "NP Lookup" in IPWorks. (Indicating ACQ behavior is required)

Procedure:

1. No information found in ENUM database.
2. IPWorks checks its database to see if a NP Lookup should be performed, and finds that the number series has been configured for "NP Lookup".
3. IPWorks access the NP database configured for the number series and synthesizes a reply. *npdi* indicates that a NP query has been performed.
4. The S-CSCF uses the newly resolved TEL URI to forward the call.
5. If present (together with "npdi"), BGCF uses "rn" to do number analysis (otherwise called number is used) and forwards the call. The BGCF does not reformat the number or the "rn" parameters.



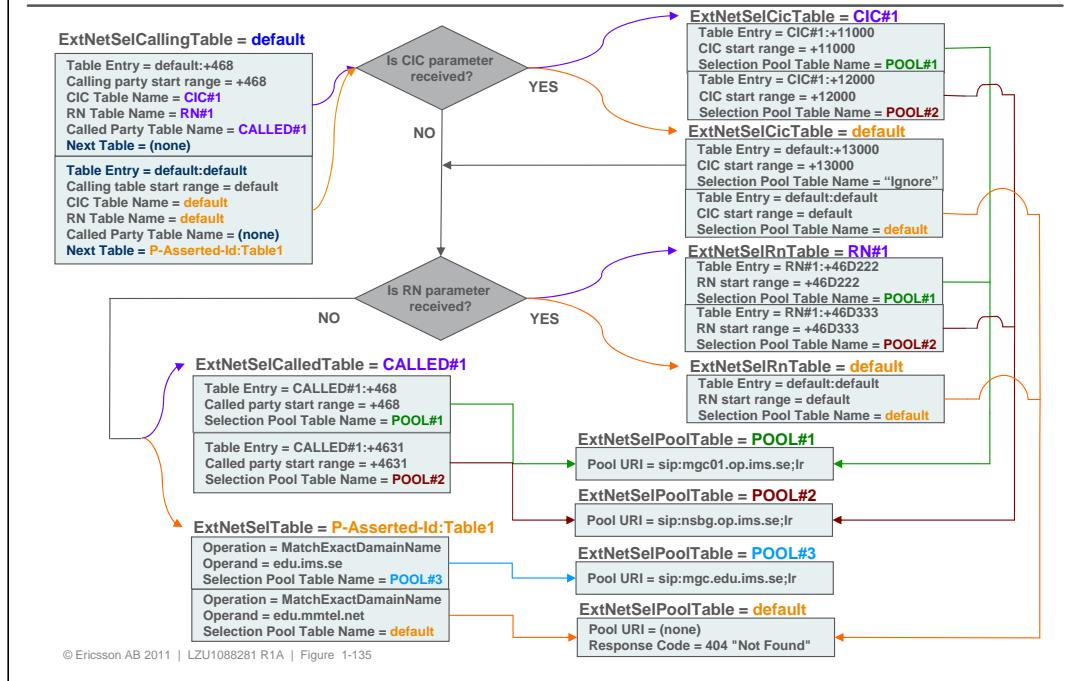
Pre-Conditions:

- No ENUM entry exists for the B-party phone number. The B-party phone number belongs to an operator that expects OR behavior.
- The number series that the B-party phone number belongs to has been configured as "No NP Lookup" in IPWorks. (Indicating OR behavior is required)

Procedure:

1. No information found in ENUM database.
2. IPWorks checks its database to see if a NP Lookup should be performed, and finds that the number series has been configured for "No NP Lookup".
3. IPWorks returns NXDOMAIN to S-CSCF.
4. The S-CSCF uses the original called number to forward the call.

External Network Selection Tables



The External Network Selection Tables are configured in the application named ExtNetSelection.

Here it is possible to configure Calling tables (A-number), Called Tables (B-Number), CIC tables (Carrier Identification Number), RN tables (Routing Number) and External Network Pools (Destination addresses to external networks, i.e. MGC addresses).

The calling table will point to a CIC table, to a RN table and to a Called table (in this exact order), which in turn will point to an external network pool. CIC and RN analysis are only performed if a CIC or RN parameter is received in the Request-URI or in the ENUM response.

There is always a default table present, pointing towards a default destination or, alternatively, leading to an error code to return.

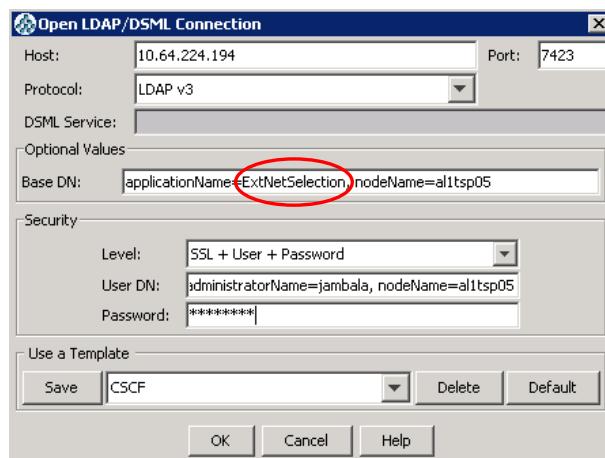
Tables must be created in the reverse order: Pool tables first and then Called, RN, CIC, and finally Calling tables.

The details of the configuration is covered in the practical exercise and also described in the CPI documents.

Note: in the example above, it is assumed that the parameter *ExtNetSelectionInitialTableName* (in the ExtNetSel-Application Object Class) is set to *calling:default*

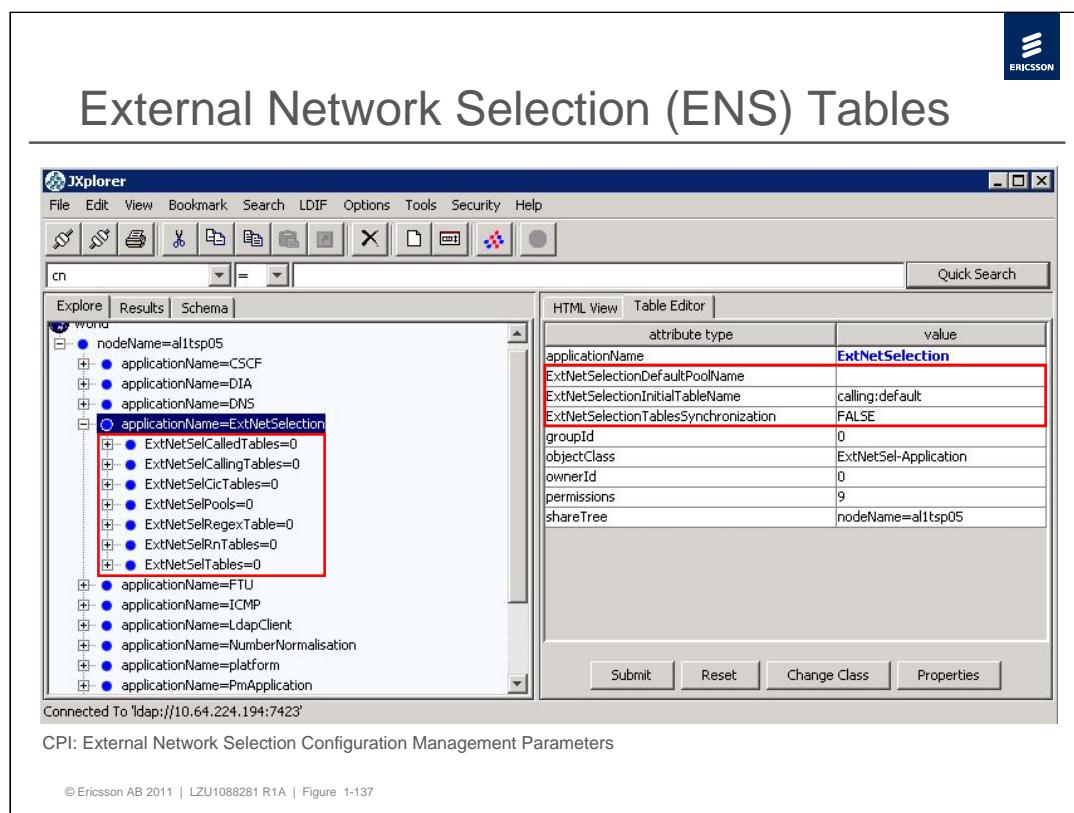


Login to the External Network Selection



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-136

The Application name for the Break-Out Gateway Control Function (BGCF) application is *ExtNetSelection*.



The figure shows the different tables to be defined for the External Network Selection (ENS) application. The tables are the *ExtNetSelCalledTables*, *ExtNetSelCallingTables*, *ExtNetSelCicTables*, *ExtNetSelRnTables*, *ExtNetSelTables*, *ExtNetSelRegexTable* and the *ExtNetSelPools*.

In all tables (except for *ExtNetSelRegexTable* and *ExtNetSelTables*) there has to exist a default entry which is created by the system and named *default*.

The final step of the ENS analysis is the selection of a pool entry containing a SIP URI for an outgoing Gateway (e.g. MGC or SBG) and/or an error code to be returned.

For the application instance, the parameters are:

ExtNetSelectionTablesSynchronization - After a configuration of the ENS tables this parameter should be set to *TRUE*, in order to activate the changes made. The application creates new tables of the configuration and then sets the *ExtNetSelectionTablesSynchronization* back to *FALSE* when it is ready.

ExtNetSelectionDefaultPoolName defines the pool to be used in case a loop or other error is encountered during the selection process.

ExtNetSelectionInitialTableName defines the name of the ENS table where the pool selection process will start. The syntax is <criteria>:<tableName>, where the criteria can be set to *calling*, *P-Asserted-Identity*, *CIC*, *RN* or *called*.

ENS Calling Table

The screenshot shows the JXplorer LDAP browser interface. On the left, the LDAP tree view under 'World' shows a node named 'al1tsp05' which contains several application entries: DIA, DNS, and ExtNetSelection. Under ExtNetSelection, there are entries for ExtNetSelCalledTables=0, ExtNetSelCallingTables=0, and ExtNetSelTables=0. The ExtNetSelCallingTables=0 entry has a child entry 'ExtNetSelCallingTableEntry=default'. On the right, the 'Table Editor' tab is selected, displaying a table with attributes and their values. The table includes:

attribute type	value
objectClass	ExtNetSelCallingTableEntryClass
ExtNetSelCalledPartyTableName	CALLED#1
ExtNetSelCallingTableEntry	default:+4687163301
ExtNetSelCallingTableNextTableName	
ExtNetSelCallingTableStartRange	+4687163301
ExtNetSelCicTableName	CIC#1
ExtNetSelRnTableName	RN#1
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=al1tsp05
parent	

Connected To 'ldap://10.64.224.194:7423'

CPI: External Network Selection Configuration Management Parameters

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-138

The parameters in the figure defines an External Network Selection Calling Table.

ExtNetSelCalledPartyTableName - This parameter must correspond to the name of an existing Called Party Table

ExtNetSelCallingTableEntry - This attribute defines the calling table entry and consists of the table name and the number range. The table name and the number range shall be separated with a colon. The table name must correspond to the value of the *ExtNetSelCallingTable*.

ExtNetSelCallingTableStartRange - This attribute defines the number range to match the PSTN number of the calling party. The number range must correspond to the *ExtNetSelCallingTableEntry* in the same table. The number string requires the international format ("+" included).

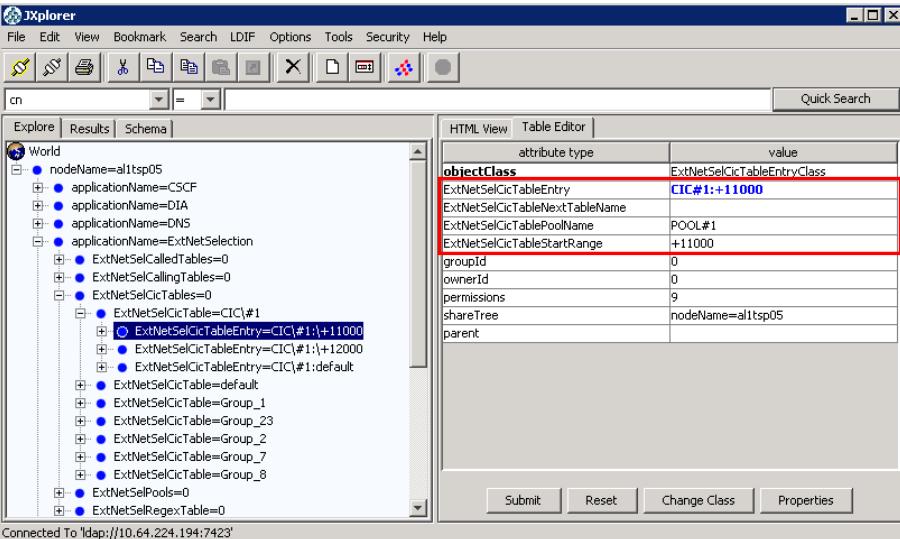
ExtNetSelCicTableName – This parameter must correspond to the name of an existing CIC table.

ExtNetSelRnTableName – This parameter must correspond to the name of an existing RN table.

ExtNetSelCallingTableNextTableName – Determines in which table the analysis should continue, in case a match is found with the specified range. The syntax is <criteria>:<tableName>, where the criteria can be set to *calling*, *P-Asserted-Identity*, *CIC*, *RN* or *called*.

Note: *ExtNetSelCallingTableNextTableName* and *ExtNetSelCalledPartyTableName* are mutually exclusive! Only one of the two can be configured for a given Calling table row.

ENS CIC (Carrier Identification Code) Table



The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view shows a node named 'al1tsp05' under 'World'. Under 'al1tsp05', there are several application entries: CSCF, DIA, DNS, and ExtNetSelection. The 'ExtNetSelection' entry has several sub-entries: ExtNetSelCalledTables=0, ExtNetSelCallingTables=0, and ExtNetSelCicTables=0. The 'ExtNetSelCicTables=0' entry contains an 'ExtNetSelCicTable' entry with the value 'CIC#1'. This entry has attributes: ExtNetSelCicTableEntry=CIC#1:+11000, ExtNetSelCicTableName=ExtNetSelCicTable, ExtNetSelCicTablePoolName=POOL#1, ExtNetSelCicTableStartRange=+11000, groupId=0, ownerId=0, permissions=9, shareTree=nodeName=al1tsp05, and parent=. At the bottom of the interface, it says 'Connected To ldap://10.64.224.194:7423'.

CPI: External Network Selection Configuration Management Parameters
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-139

ExtNetSelCicTableEntry - This attribute defines the Carrier Identification Code table entry and consists of the table name (CIC#1) and the number range (+11000). The table name and the number range shall be separated with a colon. The table name must correspond to the value of the *ExtNetSelCicTable*.

ExtNetSelCicTablePoolName - Defines the External Network Pool to use. The *ExtNetSelPoolTableEntry* must have been configured before this parameter can be set.

ExtNetSelCicTableStartRange - This attribute defines the number range to match the CIC number received in the Request-URI or in the ENUM response.

ExtNetSelCicTableNextTableName – Determines in which table the analysis should continue, in case a match is found with the specified range. The syntax is <criteria>:<tableName>, where the criteria can be set to *calling*, *P-Asserted-Identity*, *CIC*, *RN* or *called*. Note: this parameter is mutually exclusive with the parameter *ExtNetSelCicTablePoolName*!

Syntax:

ExtNetSelCicTableEntry=ExtNetSelCicTable:CIC Start Range

ENS RN (Routing Number) Table

The screenshot shows the JXplorer LDAP browser interface. On the left, the 'Explore' panel displays a tree structure of LDAP objects under 'cn'. One node is expanded to show 'ExtNetSelRnTableEntry=RN#1:+46111'. On the right, the 'Table Editor' panel shows the attributes for this entry:

attribute type	value
objectClass	ExtNetSelRnTableEntry
ExtNetSelRnTableEntry	RN#1:+46111
ExtNetSelRnTableName	
ExtNetSelRnTablePoolName	POOL#1
ExtNetSelRnTableStartRange	+46111
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=a11sp05
parent	

Below the browser window, the text 'CPI: External Network Selection Configuration Management Parameters' and '© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-140' is visible.

ExtNetSelRnTableEntry - This attribute defines the Routing Number (or Network Routing Number) table entry and consists of the table name (*RN#1*) and the number range (+46D22). The table name and the number range shall be separated with a colon. The table name must correspond to the value of the *ExtNetSelRnTable*.

ExtNetSelRnTablePoolName - Defines the External Network Pool to use. The *ExtNetSelPoolTableEntry* must have been configured before this parameter can be set.

ExtNetSelRnTableStartRange - This attribute defines the number range to match the RN number received in the Request-URI or in the ENUM response.

ExtNetSelRnTableNextTableName – Determines in which table the analysis should continue, in case a match is found with the specified range. The syntax is <criteria>:<tableName>, where the criteria can be set to *calling*, *P-Asserted-Identity*, *CIC*, *RN* or *called*. Note: this parameter is mutually exclusive with the parameter *ExtNetSelRnTablePoolName*!

Syntax:

ExtNetSelRnTableEntry=ExtNetSelRnTable:RN Start Range

The screenshot shows the JXplorer LDAP browser interface. The left pane displays a tree view of LDAP entries under the 'cn' root, including applicationName=DIA, applicationName=DNS, applicationName=ExtNetSelection, and applicationName=FTU. The 'ExtNetSelCalledTable' entry under 'ExtNetSelection' is expanded, showing sub-entries like 'ExtNetSelCalledTables=0', 'ExtNetSelCalledTable=CALLED#1', and 'ExtNetSelCalledTable=default'. The right pane shows the 'Table Editor' for the 'ExtNetSelCalledTableEntry' object class. The 'attribute type' column lists 'objectClass', 'ExtNetSelCalledTableEntry', 'ExtNetSelCalledTableNextTableName', 'ExtNetSelCalledTablePoolName', 'ExtNetSelCalledTableStartRange', 'groupId', 'ownerId', 'permissions', 'shareTree', and 'parent'. The 'value' column contains 'ExtNetSelCalledTableEntryClass', 'CALLED#1:+468', '+468', '0', '0', '9', 'nodeName=a1tsp05', and an empty string respectively. The 'ExtNetSelCalledTableEntry' row is highlighted with a red border.

CPI: External Network Selection Configuration Management Parameters
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-141

ExtNetSelCalledTableEntry - This attribute defines the called table entry and consists of the table name (*CALLED#1*) and the number range (+468). The table name and the number range shall be separated with a colon. The table name must correspond to the value of the *ExtNetSelCalledTable*.

ExtNetSelCalledTablePoolName - Defines the External Network Pool to use. The *ExtNetSelPoolTableEntry* must have been configured before this parameter can be set.

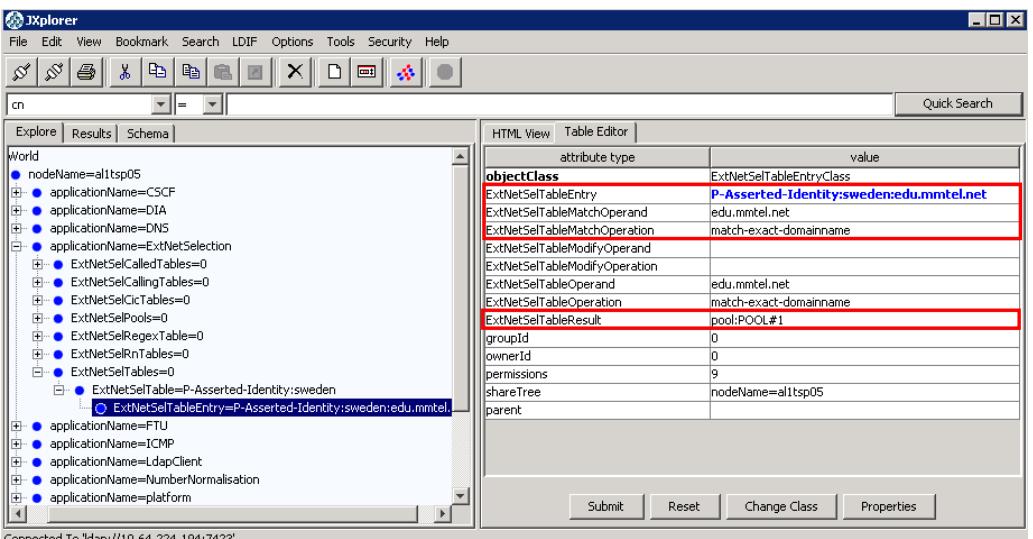
ExtNetSelCalledTableStartRange - This attribute defines the number range to match the PSTN number of the called party.

ExtNetSelCalledTableNextTableName – Determines in which table the analysis should continue, in case a match is found with the specified range. The syntax is <criteria>:<tableName>, where the criteria can be set to *calling*, *P-Asserted-Identity*, *CIC*, *RN* or *called*. Note: this parameter is mutually exclusive with the parameter *ExtNetSelCalledTablePoolName*!

Syntax:

ExtNetSelCalledTableEntry=ExtNetSelCalledTable:B-Number Start Range

ENS Generic Table (1/2) P-Asserted-Identity



The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view under 'World' shows various entries like 'nodeName=al1tsp05', 'applicationName=CSCF', etc. A specific entry 'ExtNetSelTableEntry=P-Asserted-Identity:sweden:edu.mmtel.net' is selected. On the right, the 'Table Editor' tab is active, displaying a table with attributes and their values:

attribute type	value
objectClass	ExtNetSelTableEntryClass
ExtNetSelTableEntry	P-Asserted-Identity:sweden:edu.mmtel.net
ExtNetSelTableMatchOperand	edu.mmtel.net
ExtNetSelTableMatchOperation	match-exact-domainname
ExtNetSelTableModifyOperand	
ExtNetSelTableModifyOperation	
ExtNetSelTableOperand	edu.mmtel.net
ExtNetSelTableOperation	match-exact-domainname
ExtNetSelTableResult	pool:POOL#1
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=al1tsp05
parent	

Buttons at the bottom include 'Submit', 'Reset', 'Change Class', and 'Properties'. The status bar at the bottom says 'Connected To ldap://10.64.224.194:7423'.

CPI: External Network Selection Configuration Management Parameters
 © Ericsson AB 2011 | LZU1088281 R1A | Figure 1-142

The so called Generic Table provides a template for configuring different types of data, used both for selection purposes or for supporting other tables' logics. This template allows also for easy introduction of new features in future releases of the software, as well as for possible feature customizations. A Generic Table for example can be configured as a P-Asserted-Identity domain table, Request-URI table, Calling Party domain table, Media Type table. More possibilities might be added in future SW releases, thus it is advised to check the document "External Network Selection Configuration Management Parameters" in the relevant CPI library.

A P-Asserted-Identity domain table can be used for selection purposes, based on the domain name found in the P-Asserted-Identity header.

Parameters for a P-Asserted-Identity domain table are:

ExtNetSelTableEntry = P-Asserted-Identity:<tableName>:<domain>

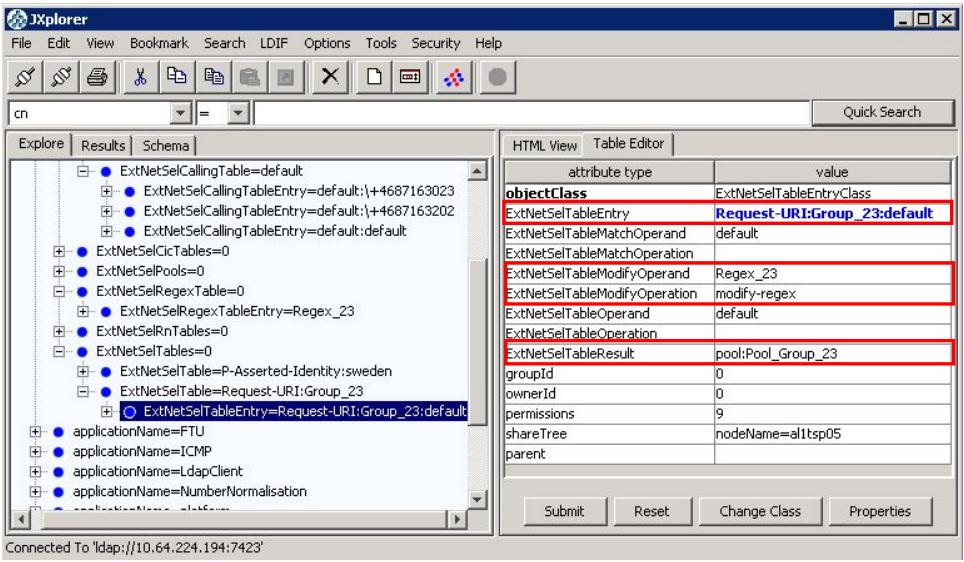
ExtNetSelTableMatchOperand = <domain>

ExtNetSelTableMatchOperation = match-exact-domainname

ExtNetSelTableResult = <typeOfTable>:<nameOfNextTable> e.g. pool:POOL1

Where <typeOfTable> can assume the following values: "pool", "calling", "P-Asserted-Identity", "CIC", "RN", or "called".

ENS Generic Table (2/2) Request-URI



The screenshot shows the JXplorer LDAP browser interface. The left pane displays a tree view of LDAP entries under the 'cn' root, including various ExtNetSelTableEntry and ExtNetSelTableModifyOperation entries. The right pane shows a table editor for an object of class 'ExtNetSelTableEntry'. The table has two rows highlighted with red boxes:

attribute type	value
objectClass	ExtNetSelTableEntryClass
ExtNetSelTableEntry	Request-URI:Group_23:default
ExtNetSelTableMatchOperand	default
ExtNetSelTableMatchOperation	
ExtNetSelTableModifyOperand	Regex_23
ExtNetSelTableModifyOperation	modify-regex
ExtNetSelTableOperand	default
ExtNetSelTableOperation	
ExtNetSelTableResult	pool:Pool_Group_23

Below the table are buttons for Submit, Reset, Change Class, and Properties.

CPI: External Network Selection Configuration Management Parameters
 © Ericsson AB 2011 | LZU1088281 R1A | Figure 1-143

A Request-URI table can be used for modifying the Request-URI and add parameters to the request line, before the call is routed towards the gateway. This action requires the support of a ExtNetSelRegexTableEntry.

Parameters for a Request-URI table are:

ExtNetSelTableEntry = Request-URI:<tableName>:default

ExtNetSelTableModifyOperand = <RegexTableName>

ExtNetSelTableModifyOperation = modify-regex

ExtNetSelTableResult = <typeOfTable>:<nameOfNextTable> e.g. pool:POOL1

Where <typeOfTable> can assume the following values: "pool", "calling", "P-Asserted-Identity", "CIC", "RN", or "called".

The screenshot shows the JXplorer LDAP browser interface. The title bar reads "ENS Regular Expression Table". The left pane is titled "Explore" and shows a tree view of LDAP entries under "cn". One entry is expanded, showing sub-entries like "ExtNetSelCallingTable=default", "ExtNetSelRegExpression", and "ExtNetSelRegexTableEntry=Regex_23". The right pane has tabs "HTML View" and "Table Editor". Under "Table Editor", there is a table with columns "attribute type" and "value". The table contains the following rows:

attribute type	value
objectClass	ExtNetSelRegexTableEntryClass
ExtNetSelRegExpression	/^(sip:.)+(@.)+\$;/1;rn= ^7777777 2/
ExtNetSelRegexTableEntry	Regex_23
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=allsp05
parent	

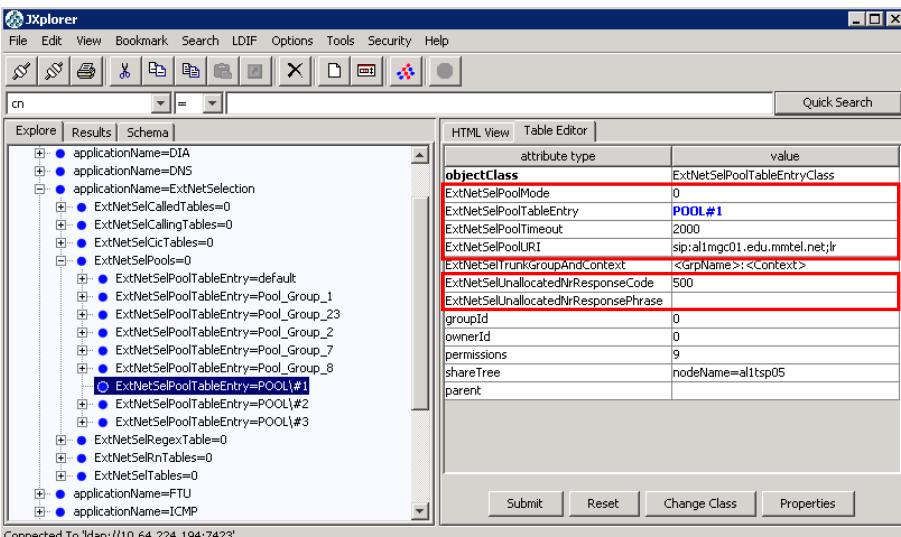
Buttons at the bottom include "Submit", "Reset", "Change Class", and "Properties". A status message at the bottom left says "Connected To 'ldap://10.64.224.194:7423'".

The ExtNetSelRegexTableEntry supports the Request-URI table, by defining the Regular Expression rules to apply to the Request-URI.

ExtNetSelRegexTableEntry is the name of the table, used as a reference in the Request-URI table.

ExtNetSelRegExpression defines the Regular Expression rules to apply. In the example above, the Request-URI would be modified by adding an rn=+7777777 parameter.

If the string was /;rn=[^;@]*// then the rn parameter would be removed (if present), before routing the request to the selected gateway.



The screenshot shows the JXplorer LDAP browser interface. The left pane displays a tree view of LDAP entries under the 'cn' root, including applicationName=DIA, applicationName=DNS, applicationName=ExtNetSelection, applicationName=ExtNetSelCalledTables=0, applicationName=ExtNetSelCallingTables=0, applicationName=ExtNetSelCicTables=0, applicationName=ExtNetSelPools=0, applicationName=FTU, and applicationName=ICMP. The right pane shows the 'HTML View' of the selected 'ExtNetSelPoolEntry' object, which has the value 'POOL#1'. The table contains the following attributes:

attribute type	value
objectClass	ExtNetSelPoolTableEntryClass
ExtNetSelPoolMode	0
ExtNetSelPoolEntry	POOL#1
ExtNetSelPoolTimeout	2000
ExtNetSelPoolURI	sip:al1mgc01.edu.mmtel.net;lr
ExtNetSelTrunkGroupAndContext	<GrpName>:<Context>
ExtNetSelUnallocatedNrResponseCode	500
ExtNetSelUnallocatedNrResponsePhrase	
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=al1tsp05
parent	

Connected To 'ldap://10.64.224.194:7423'

CPI: External Network Selection Configuration Management Parameters
 © Ericsson AB 2011 | LZU1088281 R1A | Figure 1-145

ExtNetSelPoolMode - This attribute defines if the pool is considered to be in allocated number mode. (0: Allocated Number Pool; 1: Unallocated Number Pool)

ExtNetSelPoolTableEntry - The entry represents a unique name of the external network pool

ExtNetSelPoolTimeout - Defines the time in milliseconds when a breakout gateway needs to respond to a request before it is considered as unreachable.

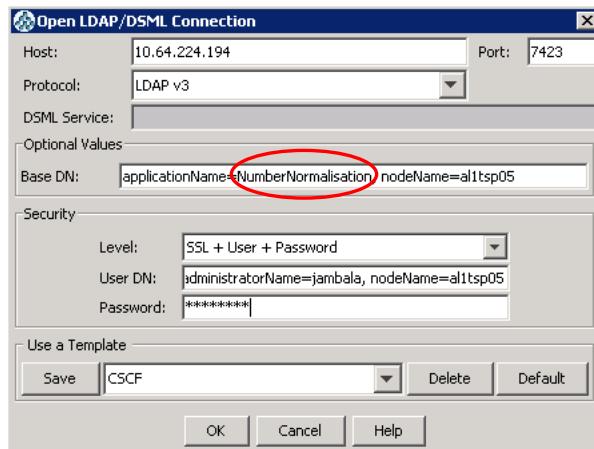
ExtNetSelPoolURI - This attribute defines the SIP-URI of the external network pool and must be configured when ExtNetSelPoolMode is set to 0. Can be defined in different ways. The FQDN is mandatory, for example, *sip:pool.x.com*. Port number and the loose routing tag are optional, for example, *sip:pool.x.com:5060;lr*.

ExtNetSelUnallocatedResponseCode - This is the response code sent back if a lookup is matching the pool and the pool is an unallocated number pool. This attribute is relevant when ExtNetSelPoolMode is set to 1.

ExtNetSelUnallocatedResponsePhrase - This is the response phrase sent back if a lookup is matching the pool and the pool is an unallocated number pool. This attribute is relevant when ExtNetSelPoolMode is set to 1.



Login to the NumberNormalisation Application



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-146

The Application name for the Number Normalization application is *NumberNormalisation*.

Number Normalization

The screenshot shows the JXplorer LDAP browser interface. The left pane displays a tree view of LDAP entries under the 'cn' search filter. The 'applicationName=NumberNormalisation' entry is expanded, showing sub-entries like 'NumNormImsiData=0', 'NumNormContext=468', etc. The right pane shows a table editor for the selected object. The 'numberNormalisationTableSync' attribute is highlighted with a red border and has a value of '0'. Other attributes listed include 'applicationName' (NumberNormalisation), 'objectClass' (NumberNormalisation), 'groupID' (0), 'ownerID' (0), 'permissions' (9), 'shareTree' (nodeName=a1tsp05), and 'parent' (empty). Below the table are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. At the bottom left, it says 'Connected To ldap://[10.64.224.194:7423]'. The status bar at the bottom indicates 'CPI: Number Normalization Management Data'.

attribute type	value
applicationName	NumberNormalisation
objectClass	NumberNormalisation
groupID	0
numberNormalisationTableSync	0
ownerID	0
permissions	9
shareTree	nodeName=a1tsp05
parent	

After changes in the NumberNormalisation application are finished, the confirmation is made permanent through setting the *numberNormalisationTableSync* parameter to 1. This means that the Number Normalization will be notified that new configuration shall be used. The application creates new tables of the configuration and then sets the *numberNormalisationTableSync* to 0 when it is ready. When *numberNormalisationTableSync* is 1 no configuration is allowed in the Number Normalization.

It is not allowed to set the table sync parameter to 1 more frequently than every 15 seconds.

Note: a user cannot set the value to 0. It can only be set to 0 by the application itself.

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view displays various application names and a specific entry for 'NumNormProfile=46'. This entry has several child nodes under 'NumNormProfile=46' such as 'NumNormInnData=0', 'NumNormContext=+468', and 'NumNormDefaultContext=edu.mmtel.net'. On the right, the table editor shows the attributes for this profile. The 'NumNormProfile' attribute is highlighted with a red border and contains the value '46'. Other visible attributes include 'numNormProfileContext' (value '+468'), 'numNormProfileDomNameEr' (value 'se'), 'numNormProfileName' (value 'sweden'), 'numNormProfileUserEqPhoneEr' (value '1'), 'ownerId' (value '0'), 'permissions' (value '9'), 'shareTree' (value 'nodeName=alitsp05'), and 'parent' (value '').

attribute type	value
objectClass	NumNormProfile
groupId	0
NumNormProfile	46
numNormProfileContext	edu.mmtel.net
numNormProfileContext	+468
numNormProfileDomNameEr	se
numNormProfileName	sweden
numNormProfileUserEqPhoneEr	1
numNormProfileWarningText	
ownerId	0
permissions	9
shareTree	nodeName=alitsp05
parent	

CPI: Number Normalization Management Data
Connected To 'ldap://10.64.224.194:7423'
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-148

numNormProfileContext - Defines an array of 128 possible contexts associated with a profile set up. The numNormProfileContext attribute consists of an array of strings defining the Country Code (CC), Country-code Top-level Domains (ccTLD), or nth Level Domain (nthLD) name. (If using stockholm.ericsson.se, then ".se"=ccTLD and "stockholm.ericsson.se" is the nthLD, where n=3).

If a phone-context is present in the input URI then the CC, nthTLD, or ccTLD is used to search the profile context values to decide if this is the profile to use.

If no phone-context is present in the input URI, then nthLD name or ccTLD in the provided context is used to search the profile context values to decide if this is the profile to use.

No two profiles may have the same CC, nthLD, or ccTLD.

numNormProfileUserEqPhoneEr - For the configured list of domain names given by numNormProfileDomNameEr. The numNormProfileUserEqPhoneEr attribute defines if the Number Normalization function inserts user=phone parameter if it is missing in the received SIP URI. If set, user=phone parameter is inserted. (0 = Do not add user=phone, 1 = Add user=phone)

numNormProfileDomNameEr - Defines an array of up to 128 domain names against which user=phone error correction is applicable. The user=phone error correction is applied only if the numNormProfileUserEqPhoneEr parameter is set.

Example: "operator1.com" or "+468"

The screenshot shows the JXplorer LDAP browser interface. On the left, the 'Explore' panel displays a tree structure under 'World' with nodes like 'nodeName=al1tsp01' and 'applicationName=NumberNormalisation'. On the right, the 'Table Editor' panel shows a table of attributes for an object. Several attributes are highlighted with red boxes: 'numNormContextNsnIndex' (value: National_Numbers), 'numNormContextOsnIndex' (value: Operator_Numbers), 'numNormContextRule' (value: se), and 'numNormContextSubRulesIndex' (value: Sub_Index1). The table has columns 'attribute type' and 'value'. Buttons at the bottom include 'Submit', 'Reset', 'Change Class', and 'Properties'. A status bar at the bottom left says 'Connected To 'ldap://10.64.224.193:7423''.

attribute type	value
objectClass	NumNormContext
groupId	0
NumNormContext	1
numNormContextNsnIndex	National_Numbers
numNormContextOsnIndex	Operator_Numbers
numNormContextRule	se
numNormContextSubAreaCode	6
numNormContextSubRulesIndex	Sub_Index1
ownerId	0
permissions	9
shareTree	nodeName=al1tsp01
parent	

numNormContextRule - Defines the string of the rules context consisting of digits or domain name.

numNormContextSubRulesIndex - Defines the string for the index to the substitution rules. The string must be set to the same value as the *numNormSubstitutionRuleIndex* object in the NumNormSubstitutionRule Object Class.

numNormContextNsnIndex - Defines the string for the index to the Nsn table. The string must be set to the same value as the *numNormNsnDataIndex* object in the NumNormNsnData Object Class.

numNormContextOsnIndex - Defines the string for the index to the Osn table. The string must be set to the same value as the *numNormOsnDataIndex* object in the NumNormOsnData Object Class.

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view under 'World' shows a node named 'al1tsp01' which contains an 'applicationName=NumberNormalisation' entry. This entry has several child objects, including 'NumNormProfile=0', 'NumNormProfile=Group', and 'NumNormNsData=0'. The 'NumNormNsData=0' object is selected and highlighted with a red box. On the right, the 'Table Editor' tab is active, displaying a table of attributes for this object. The table includes columns for 'attribute type' and 'value'. The 'NumNormNsData' attribute has a value of '0'. Other attributes listed include 'numNormNsDataIndex', 'numNormNsDataNumbers', 'numNormNsDataNumbers', 'numNormNsDataNumbers', 'numNormNsDataNumbers', and 'numNormNsDataNumbers'. The 'numNormNsDataNumbers' attribute is also highlighted with a red box. The table continues with 'ownerId', 'permissions', 'shareTree', and 'parent' attributes.

attribute type	value
objectClass	NumNormNsData
groupId	0
NumNormNsData	0
numNormNsDataIndex	National_Numbers
numNormNsDataNumbers	0:46
numNormNsDataNumbers	1:112
numNormNsDataNumbers	2:911
numNormNsDataNumbers	3:11414
ownerId	0
permissions	9
shareTree	nodeName=al1tsp01
parent	

Connected To 'ldap://10.64.224.193:7423'

CPI: Number Normalization Management Data

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-150

National Significant Numbers

numNormNsDataNumbers - Defines an array of 255 possible NSN numbers associated with a country (or profile). The NSN are significant to all contexts. The first string defines the context to be associated with the output normalized number.

- 0: NSN context=+CC or domain name
- 1: NSN Num#1
- 2: NSN Num#2
- n: NSN Num#n

The n: is always present at the start of a string and indicates the order of evaluation

numNormNsDataIndex - Defines the string for the index to the NSN data. The string must be set to the same value as the numNormContextNsIndex object in the NumNormContext Object Class

Note: the numbers defined in this list will not be normalized.

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view under 'World' shows a node named 'al1sp01' with an 'applicationName=NumberNormalisation' child, which has a 'NumNormProfile=0' child. This child has three entries: 'NumNormContext=0', 'NumNormOsnData=0' (which is selected), and 'NumNormSubstitutionRule=0'. On the right, the 'Table Editor' tab is active, displaying a table of attributes for the selected object. The table includes columns for 'attribute type' and 'value'. The following table represents the data shown in the screenshot:

attribute type	value
objectClass	NumNormOsnData
groupId	0
NumNormOsnData	0
numNormOsnDataContextAndNumbers	0:190
numNormOsnDataContextAndNumbers	1:414
numNormOsnDataContextAndNumbers	2:404
numNormOsnDataIndex	OSN_Index_1
ownerId	0
permissions	9
shareTree	nodeName=al1sp01
parent	

Below the table, there are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. At the bottom left, it says 'Connected To 'ldap://10.64.224.193:7423''. The footer of the browser window displays 'CPI: Number Normalization Management Data' and '© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-151'.

Operator Service Numbers

numNormOsnDataContextAndNumbers - Defines an array of 255 possible OSN numbers. The first string defines the context to be associated with the output normalized number.

String 0: OSN context0

String 1: OSN Num#1

String 2: OSN Num# 2

String n: OSN Num#n The n: is always present at the start of a string and indicates the order of evaluation.

numNormOsnDataIndex - Defines the string for the index to the OSN data. The string must be set to the same value as the numNormContextOsnIndex object in the NumNormContext Object Class

Note: the numbers defined in this list will not be normalized.

The screenshot shows the JXplorer LDAP browser interface. The left pane displays a tree view of LDAP entries under the 'World' root, including nodes for applicationName like 'CSCF', 'DIA', 'DNS', etc., and a 'NumNormProfile' node under 'applicationName=NumberNormalisation'. The right pane shows a 'Table Editor' for a 'NumNormSubstitutionRule' object. The table has two columns: 'attribute type' and 'value'. The 'attribute type' column lists attributes like 'objectClass', 'groupId', 'NumNormSubstitutionRule', 'numNormSubstitutionRuleData', 'NumNormSubstitutionRuleIndex', 'ownerId', 'permissions', 'shareTree', and 'parent'. The 'value' column contains corresponding values, with several rows highlighted in red. The highlighted rows are:

attribute type	value
objectClass	NumNormSubstitutionRule
groupId	0
NumNormSubstitutionRule	swe_rule_1
numNormSubstitutionRuleData	0:/^([0-9]{4})\$/+468716\1/:TRUE
numNormSubstitutionRuleData	1:/^46.*\$/+1/:TRUE
numNormSubstitutionRuleData	2:/^00.*\$/+1/:TRUE
numNormSubstitutionRuleData	3:/^0.*\$/+461/:TRUE
numNormSubstitutionRuleData	4:/^([1-9][0-9]*)\$/+468\1/:TRUE
NumNormSubstitutionRuleIndex	swe_rule_1

Below the table are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. At the bottom left, it says 'Connected To ldap://10.64.224.194:7423'. The bottom status bar reads 'CPI: Number Normalization Management Data' and '© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-152'.

The figure shows the number normalization rules for the domain name context `edu.mmtel.se`. The doamin name is the default entry ohter entries must be defined in order to match the phone context value provisioned for every subscriber.

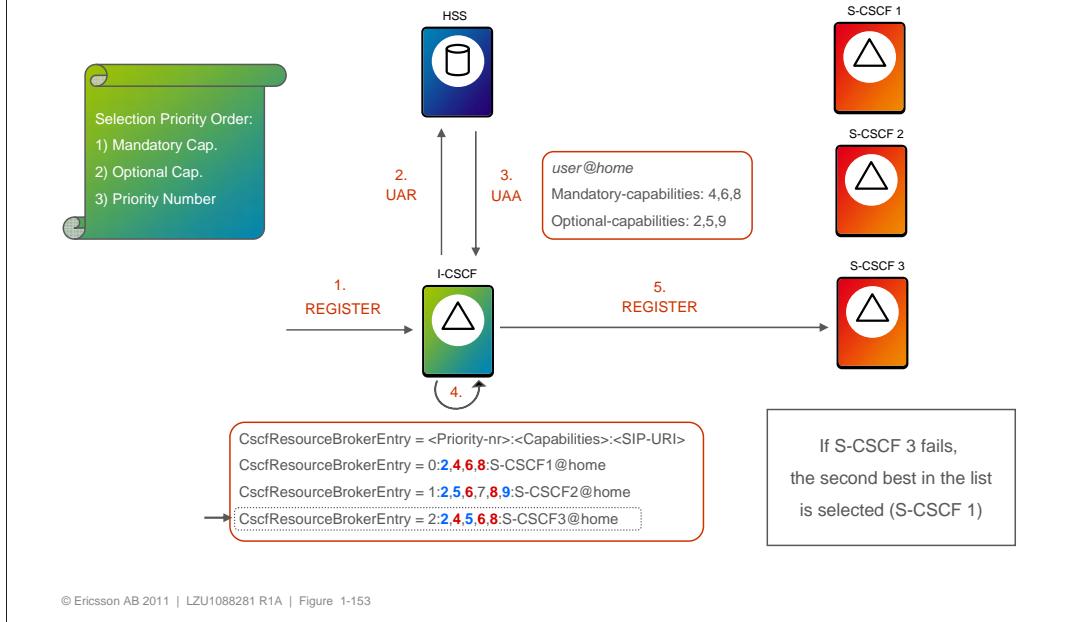
NumNormSubstitutionEntry - Defines the context, either Domain or Global. Global number contexts can either be a full international number or the leading part of a fully international number. The '+' is mandatory for a global phone context. If the '+' is not present, then the context is treated as a domain name context.

NumNormSubstitutionExpressionEntry - The list is colon separated. For example, `0:/^(.*)_$/+\1/:TRUE`. '0' defines the order of evaluation of the expression. The lowest order is evaluated first. The value between the leading '/' and trailing '/' '`/^(.*)_$/+\1/`' is the substitution expression. It is used to determine if the number matches and how to manipulate the number. The leading and trailing '/' is POSIX 1003.2 extended regular expressions. TRUE is the Terminal Match. It defines if the remaining expression should be evaluated if the Substitution Expression matches the number.

In the figure the rules mean:

0. If the number is 4 digits long, do nothing.
1. If the number starts with 46, add a '+'.
2. If the number starts with 00, replace 00 with a '+'
3. If the number starts with 0, replace 0 with '+46'
4. If the first digit is 1-9 and the second digit is 0-9 then add '+468'

Flexible S-CSCF Selection



The Flexible S-CSCF Selection allows to steer the users or services to certain S-CSCF for better user experience. This feature is compliant with 3GPP standards.

I-CSCF selects an S-CSCF based on information received in the UAA (User Authorization Answer) from HSS. The UAA includes either the Server-Name AVP containing the name of the assigned S-CSCF or the Server-Capabilities AVP containing the required capabilities of the S-CSCF to be assigned and optionally a list of preferred S-CSCF names.

The Server-Name AVP overrides the Mandatory and Optional Capabilities in case both AVPs are present in the UAA.

Each capability is represented by an integer value. Both Mandatory and Optional capabilities share the same number series (that is, the same number for both mandatory and optional capabilities is not allowed).

Upon reception of a UAA containing Server-Capabilities AVP, I-CSCF evaluates the following:

- 1) Which S-CSCFs support all the Mandatory capabilities
- 2) If several entries support the Mandatory capabilities, which S-CSCFs support the most of the Optional capabilities
- 3) If several entries support the same number of Mandatory and Optional capabilities, the entry with the lowest Priority-nr (highest priority) is selected



Service Capabilities in HSS

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view under 'World' shows various application names like DIA, FTU, HSS_AVG, HSS_ESM, HSS_SM, and HSS. Under HSS, there are containers for Configuration, Network Domain, Application Server, Charging, Digest Authentication, Im Configuration, SdA Configuration, and Service Indication. A specific entry 'HSS-ServiceTypeContainerName=HSS-Si' is selected, which points to 'HSS-ServiceTypeObjectID=mtras'. This entry has a list of 'HSS-TriggerPriority' values from 101 to 117. On the right, the 'Table Editor' shows the attributes for this object. The 'HSS-ServiceCapabilities' attribute is set to 1, and 'HSS-ServiceOptionalCapabilities' is set to 5. Other attributes include objectClass (HSS-ServiceType), groupID (0), ownerID (0), permissions (9), shareTree (nodeName=tsp01tsp07geo), and parent (empty). Buttons at the bottom include Submit, Reset, Change Class, and Properties.

attribute type	value
HSS-ServiceTypeObjectID	mtras
objectClass	HSS-ServiceType
groupID	0
HSS-ServiceCapabilities	1
HSS-ServiceOptionalCapabilities	5
HSS-ServiceOptionalCapabilities	2
HSS-ServiceOptionalCapabilities	3
HSS-ServiceOptionalCapabilities	4
HSS-ServiceOptionalCapabilities	6
HSS-ServiceOptionalCapabilities	7
HSS-ServiceOptionalCapabilities	8
HSS-ServiceOptionalCapabilities	9
HSS-ServiceOptionalCapabilities	10
HSS-ServiceOptionalCapabilities	11
HSS-ServiceOptionalCapabilities	12
HSS-ServiceOptionalCapabilities	13
HSS-ServiceOptionalCapabilities	14
HSS-ServiceOptionalCapabilities	15
HSS-ServiceOptionalCapabilities	16

HSS-ServiceCapabilities specifies the mandatory capabilities that an S-CSCF must support in order to be selected for serving a subscriber associated with a particular Service profile. This configuration is applicable to all the subscribers that are linked to the same Service profile.

HSS-ServiceOptionalCapabilities specifies instead the optional capabilities. The more the optional capabilities are supported by an S-CSCF, the more possibilities that such an S-CSCF will be selected to serve the requesting subscriber.

Several capabilities (both mandatory and optional) can be specified for the same Service profile. A maximum of 16 capabilities can be defined.

The screenshot shows the JXplorer LDAP browser interface. On the left is a tree view of LDAP entries under 'cn'. One entry, 'CscfResourceBroker', is expanded, showing its sub-entries like 'CscfAccessNetworkAssertion', 'CscfAuthenticationGroup=0', etc. On the right is a 'Table Editor' window for the 'CscfResourceBrokerEntry' object. The table has two columns: 'attribute type' and 'value'. The rows are:

attribute type	value
CscfResourceBrokerEntry	0
CscfResourceBrokerEntry	0:2,4,6,8:sip:scscf01.edu.mmtel.net
CscfResourceBrokerEntry	1:2,5,6,7,8,9:sip:scscf02.edu.mmtel.net
CscfResourceBrokerEntry	2:2,4,5,6,8:sip:scscf03.edu.mmtel.net
IcscfLocalZonePolicyEnabled	TRUE
objectClass	CscfResourceBrokerClass
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=a1tsp05
parent	

At the bottom of the Table Editor are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A status bar at the bottom of the browser window says 'Connected To ldap://10.64.224.194:7423'.

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-155

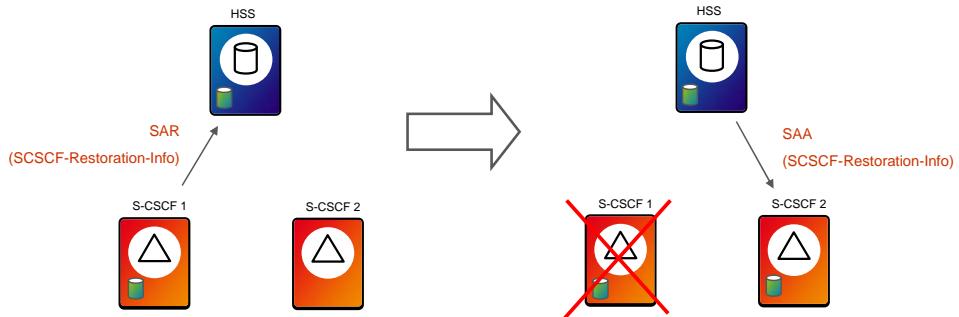
The syntax for *CscfResourceBrokerEntry* is <Priority-nr>:<Capabilities>:<SIP-URI>

IcscfLocalZonePolicyEnabled enables an I-CSCF to only select S-CSCFs included in its local zone. When the I-CSCF receives a Diameter UAA with AVP Server-Name from the HSS, the received server name is compared with the S-CSCF names in the *CscfResourceBrokerEntry*. If a match is found, the S-CSCF received from HSS is selected. If no match is found I-CSCF will request Capabilities from HSS and re-select an S-CSCF. If there is no Resource Broker entry defined, I-CSCF will try to match the received server name with the name of the collocated S-CSCF (if any). If there is no match, capabilities will be requested to HSS.



IMS Restoration Support

- › The S-CSCF stores semi-permanent information in HSS
- › In case of failure of a S-CSCF, another S-CSCF can fetch the stored info and restore the contact info related to the IMPU



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-156

Although S-CSCF is a highly available node, periodic maintenance and occasional failures are unavoidable. Due to system failure, S-CSCF service interruption is inevitable, it is acceptable that established sessions will be affected and would be terminated. After the failure, S-CSCF will most likely be back in service automatically with a system restart. However, it might have lost some of the user information needed to provide services to the registered users.

Information such as whether the user is registered, which Public and Contact identities are registered...etc. is required to complete originating and terminating calls. Such data is referred to as the “restoration information”. 3GPP has defined the Restoration Procedure for retaining, updating and restoring of the restoration information. With the Restoration Procedure, restoration information is stored in HSS and retrieved by S-CSCF. Any S-CSCF supporting the Restoration Procedure stores and updates the restoration information of its users in the specified situations. The Restoration Procedure allows any recovered or failed-over S-CSCF to restore the restoration information and provide services to the users accordingly.



Restoration Support in S-CSCF

The screenshot shows the JXplorer LDAP browser interface. On the left, there is a tree view of LDAP entries under the 'cn' root. On the right, there is a table editor for an 'objectClass' entry. The table has two rows:

attribute type	value
SccfRestoration	default
SccfRestorationOriginatingNonRegisterAllowed	TRUE
SccfRestorationProcedure	1

Below the table are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. At the bottom left of the interface, it says 'Connected To ldap://10.64.224.194:7423'.

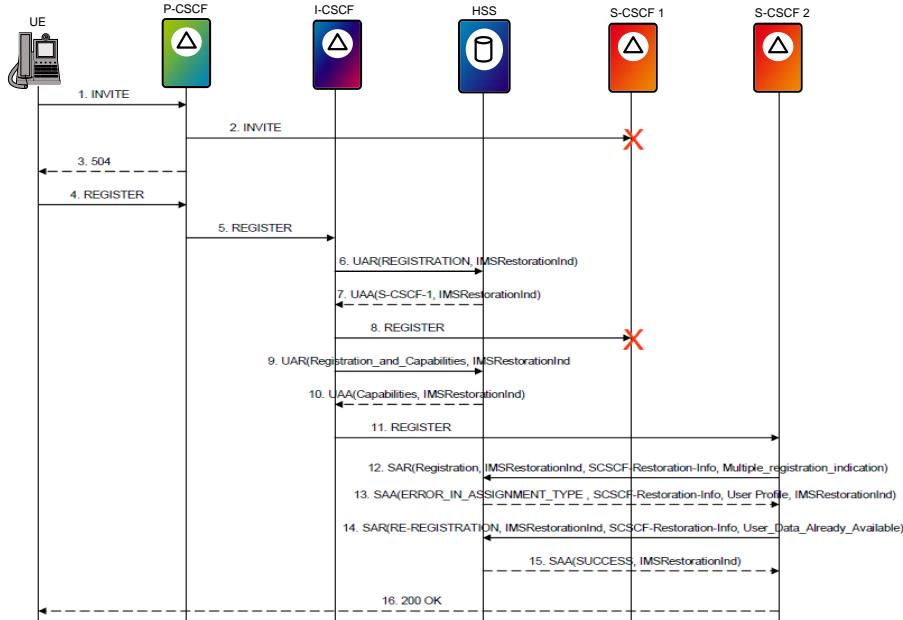
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-157

SccfRestorationProcedure is used to enable and disable the Restoration feature in the S-CSCF. 0 means the feature is disabled and 1 means the feature is enabled.

When Restoration Procedure is enabled,

SccfRestorationOriginatingNonRegisterAllowed is used to determine the action to be taken by the S-CSCF when an originating non-Register request from a user who is not registered at the S-CSCF is received. If the Restoration Procedure is enabled and an originating non-Register request is received and if the user is not found in the S-CSCF and if this parameter is set to "TRUE", the S-CSCF will trigger the Restoration Procedure and process the request regardless of the configuration of whether Authentication on non-Register request is required. In the same situation if this parameter is set to "FALSE", the S-CSCF will reject the request with a 504 Response Code.

Example: Restoration during Originating INVITE request at S-CSCF failure



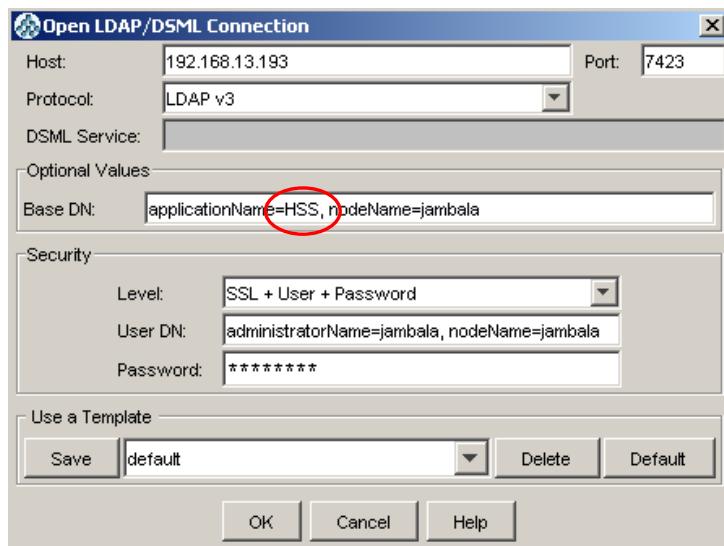
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-158

1. An Originating non-Register request (e.g. an INVITE) is sent by an UE whose user has not been failed over.
2. P-CSCF forwards the request to the S-CSCF indicated by the Service Route.
3. The S-CSCF is not reachable and P-CSCF times out on the request. P-CSCF returns a 504 Response back to the UE.
4. Upon reception of the 504 Response, the UE triggers an initial registration. In this situation the UE belongs to a user who has at least one of his IMPU previously registered.
5. P-CSCF forwards the request to the I-CSCF.
6. I-CSCF sends a UAR message to HSS to ask for S-CSCF information.
7. In this case, the IMPU is registered; HSS returns the registered SCSCF.
8. I-CSCF forwards the request to the registered S-CSCF.
9. The S-CSCF is not reachable, I-CSCF sends another UAR message to HSS to ask for S-CSCF capabilities.
10. HSS returns the S-CSCF capabilities to the I-CSCF.
11. I-CSCF reselects an S-CSCF. I-CSCF forwards the request to the selected S-CSCF.
12. Upon reception of the re-registration request, since the IMPU is not registered in the S-CSCF, the S-CSCF sends a SAR message to HSS to register the IMPU.

13. Since HSS already has the IMPU marked as registered and the requesting S-CSCF is different from the stored S-CSCF; HSS returns an **ERROR_IN_ASSIGNMENT_TYPE** and ignores the SCSCF-Restoration Information sent by the S-CSCF. Due to the UAR message with **User_Authorization_Type** (UAT) set to “**REGISTRATION_AND_CAPABILITIES**” sent by the I-CSCF, HSS updates the S-CSCF name of the user even though the response code is “**ERROR_IN_ASSIGNMENT_TYPE**”. S-CSCF rebuilds the user information with all the SCSCF-Restoration-Info AVPs and user profile data received. If the IMPU is shared by multiple IMPIs, there will be multiple SCSCF-Restoration-Info AVPs (one per IMPI/IMPU or IMPI/IRS pair) sent to the S-CSCF. S-CSCF restores user information with all SCSCF-Restoration-Info AVPs received. All restored contacts are considered registered at the S-CSCF.
14. If the contact that S-CSCF is trying to register is not in the SCSCF-Restoration-Info (i.e. registration of a new contact of a registered IMPU) or the restoration information is changed for this contact (e.g. expiration time changed), S-CSCF sends another SAR message to update the restoration information including all the restored contacts within the SCSCF-Restoration-Info AVP of the same IMPI/IMPU pair triggering the restoration.
15. If the second SAR was sent as in step 14, HSS updates the restoration information of the IMPI/IMPU pair and returns an SAA with success.
16. 200OK is sent back to the UE. The 200 OK resulted from the registration updates the Service Route at the P-CSCF, therefore subsequent originating non-Register requests will be served by the reselected S-CSCF.



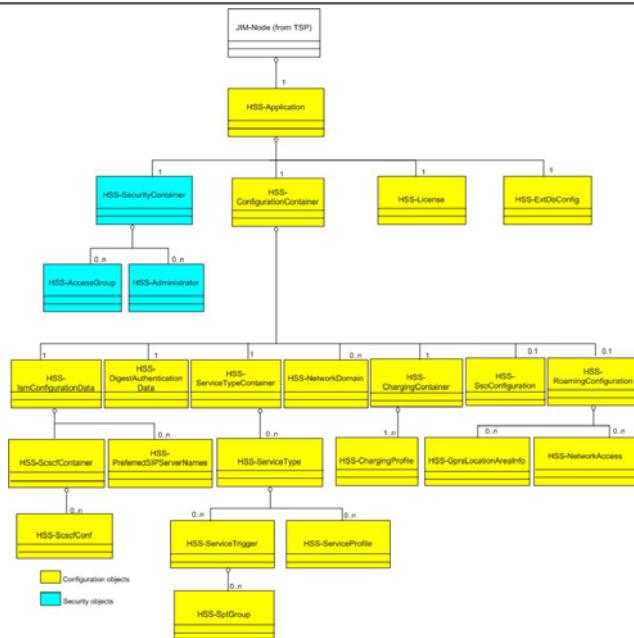
Login to the HSS (ISM and SDA) application



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-160

The Application name for the ISM and SDA applications is *HSS*.

ISM/SDA Configuration Object Class Model



This picture presents ISM and SDA Configuration Object Class Model.

HSS Administrative State

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view shows a node named 'nodeName=al1tsp01' which contains an 'applicationName=HSS' entry. This entry has several child entries: 'HSS-ConfigurationContainerName=HSS-ConfigurationContainer', 'HSS-LicenseName=HSS-License', 'HSS-SecurityContainerName=HSS-SecurityContainer', and 'HSS-SubscriberContainerName=HSS-Subscribers'. On the right, the 'Table Editor' tab is selected, displaying a list of attributes and their values for the 'applicationName=HSS' entry. One attribute, 'HSS-AdministrativeState', is highlighted with a red border. The value for this attribute is 'Unlocked'. Other visible attributes include 'objectClass' (HSS), 'applicationName' (HSS), 'objectClass' (HSS-Application), 'groupID' (811), 'HSS-InstallationType' (Monolithic), 'HSS-NodeIdentity' (HSS.edu.mmtel.net), 'HSS-StackId' (HSS), 'ownerId' (813), 'permissions' (9), 'shareTree' (nodeName=al1tsp01), and 'HSS-IsDataCacheUsed' (false). At the bottom of the editor, there are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

attribute type	value
applicationName	HSS
objectClass	HSS-Application
groupID	811
HSS-AdministrativeState	Unlocked
HSS-InstallationType	Monolithic
HSS-NodeIdentity	HSS.edu.mmtel.net
HSS-StackId	HSS
ownerId	813
permissions	9
shareTree	nodeName=al1tsp01
HSS-IsDataCacheUsed	false
parent	

CPI: ISM LDAP Interface Description

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-162

HSS-AdministrativeState attribute identifies the state for the ISM modules.

Possible values:

- Unlocked (set at installation time)
- Locked

ISM Configuration Parameters

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view displays the LDAP structure under 'cn' with nodes like 'nodeName=alitsp01' and 'applicationName=HSS'. Under 'HSS', there are several containers: 'HSS-ConfigurationContainer', 'HSS-ChargingContainer', 'HSS-ApplicationServerContainer', 'HSS-DigestAuthenticationContainer', 'HSS-ImConfigurationContainer', 'HSS-RoamingConfig', 'HSS-SdaConfigurationContainer', 'HSS-ServiceIndicatorContainer', 'HSS-ServicesSupportContainer', 'HSS-ServiceTypeContainer', 'HSS-SsoConfig', 'HSS-License', and 'HSS-SecurityContainer'. The 'HSS-ImConfigurationContainer' node is expanded. On the right, the 'Table Editor' tab is selected, showing a list of attributes and their values for this container. A red box highlights the following attributes and their values:

attribute type	value
HSS-IsmConfigurationDataName	HSS-IsmConfigurationData
objectClass	HSS-IsmConfigurationData
groupID	811
HSS-AuthenticationLogStatus	TRUE
HSS-DefaultMaxNumberOfContracts	1
HSS-DefaultMaxSessions	1
HSS-LocationLogStatus	TRUE
HSS-MassiveUpdateAllowed	TRUE
HSS-MaxSimultaneousRequests	100
HSS-OAMLogStatus	TRUE
HSS-PerEndScheduleTime	200907091140436157
HSS-PerInitialScheduleTime	200907091140436157
HSS-PerfScheduleActive	FALSE
HSS-PerfStartStop	FALSE
HSS-ReattemptDelayTime	1000
HSS-RequestReAttempts	5
ownerId	811
permissions	11
shareTree	nodeName=alitsp01
parent	

At the bottom of the interface, there are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A status bar at the bottom left indicates 'Connected To ldap://10.64.224.193:7423'.

CPI: ISM LDAP Interface Description

HSS-LocationLogStatus flag states whether Location Log (related to general traffic messages) is active or not. Possible values: FALSE/TRUE

HSS-AuthenticationLogStatus flag states whether Authentication Log (related to authentication traffic messages) is active or not. Possible values: FALSE/TRUE

HSS-OAMLogStatus flag states whether OAM Log (related to Operation and Maintenance Information) is active or not. Possible values: FALSE/TRUE

HSS-DefaultMaxSessions attribute states the default value for HSS-MaxSessions in an HSS User.

HSS-DefaultMaxCallLegs attribute states the default value for HSS-MaxCallLegs in an HSS User.

HSS-MaxSimultaneousRequests represents the maximum number of request messages that can be sent without having a response simultaneously at any moment.

HSS-NumMaxPublicIdsPerUser states the maximum number of Public Identities per user that can be currently defined.

HSS-MassiveUpdateAllowed indicates whether a change in HSS-ChargingProfile, HSS-ServiceProfile and/or HSS-ServiceTrigger object class is notified to the S-CSCF for the affected users immediately.

SDA Configuration Parameters

The screenshot shows the JXplorer LDAP browser interface. The left pane displays the LDAP tree structure under 'nodeName=al1tsp01'. The right pane shows the 'Table Editor' with a list of SDA configuration parameters. Several parameters are highlighted with red boxes: **HSS-SdaMaxSimultaneousRequests**, **HSS-SdaMaxSizeOfUserTd**, **HSS-SdaOamLogStatus**, and **HSS-SdaServiceLogStatus**. Below these, **HSS-SdaSynchronizerIsRunning** is also highlighted.

attribute type	value
HSS-SdaConfigurationDataName	HSS-SdaConfigurationData
objectClass	HSS-SdaConfigurationData
groupID	811
HSS-SdaCpuLimitArmThr	70
HSS-SdaCpuInitDiscarmThr	65
HSS-SdaMassiveNotificationStatus	FALSE
HSS-SdaMaxSimultaneousRequests	10
HSS-SdaMaxSizeOfUserTd	252144
HSS-SdaOamLogStatus	TRUE
HSS-SdaPerfEndScheduleTime	20090709T140436874
HSS-SdaPerfInitialScheduleTime	20090709T140436874
HSS-SdaPerfScheduleActive	FALSE
HSS-SdaPerfStartStop	FALSE
HSS-SdaReattemptDelayTime	1000
HSS-SdaRequestReattemptS	5
HSS-SdaServiceLogStatus	TRUE
HSS-SdaSynchronizerIsRunning	FALSE
HSS-SdaSynchronizerStartTime	0.0
ownerId	811
permissions	11
shareTree	nodeName=al1tsp01
parent	

CPI: SDA LDAP Interface Description

HSS-SdaMaxSimultaneousRequests represents the maximum number of SDA messages that can be waiting for a response simultaneously per peer at any moment.

HSS-SdaMaxSizeOfUserTd indicates the maximum number of bytes allowed of transparent data per user.

HSS-SdaOamLogStatus is a flag that states whether the OAM Log (related to Operation and Maintenance Information) is active or not.

HSS-SdaServiceLogStatus is a flag that states whether the Services Log is active or not.

HSS-SdaSynchronizerTime indicates the time when the synchronizer starts.

HSS-SdaSynchronizerIsRunning shows when the synchronizer is running.



SDA Configuration Parameters

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn Quick Search

Explore Results Schema

World

- nodeName=alltsp01
- applicationName=HSS
- HSS-ConfigurationContainerName=HSS-ConfigurationContainer
- HSS-NetworkDomainName=edu.mmtel.net
- HSS-ApplicationServerContainerName=HSS-ApplicationServers
- HSS-ApplicationServerId=ap1.edu.mmtel.net
- HSS-ApplicationServerId=imitas.edu.mmtel.net
- HSS-ApplicationServerId=mmsc.edu.mmtel.net
- HSS-ApplicationServerId=shublinkas.edu.mmtel.net
- HSS-ChargingContainerName=HSS-Charging
- HSS-DigestAuthenticationDataName=HSS-DigestAuthenticationData
- HSS-IsmConfigurationDataName=HSS-IsmConfigurationData
- HSS-RoamingConfigId=HSS-RoamingConfiguration
- HSS-SdaConfigurationDataName=HSS-SdaConfigurationData
- HSS-ServiceIndicationContainerName=HSS-ServiceIndication
- HSS-ServicesSupportContainerName=HSS-ServicesSupportContainer
- HSS-ServiceTypeContainerName=HSS-ServiceTypeContainer
- HSS-SsoConfigId=HSS-SsoConfiguration
- HSS-LicenseName=HSS-License
- HSS-SecurityContainerName=HSS-SecurityContainer
- HSS-SubscriberContainerName=HSS-Subscribers

HTML View Table Editor

attribute type	value
HSS-ApplicationServerId	imitas.edu.mmtel.net
objectClass	HSS-ApplicationServer
groupID	0
HSS-ApplicationServerName	sip:alltsp01@imitas.edu.mmtel.net
HSS-PullForBarringInformation	TRUE
HSS-PullForChargingInformation	TRUE
HSS-PullForImPublicIdentity	TRUE
HSS-PullForImUserState	TRUE
HSS-PullForInitialFilterCriteria	TRUE
HSS-PullForLocationInformation	TRUE
HSS-PullForMsisdn	TRUE
HSS-PullForSccfName	TRUE
HSS-PullForTransparentData	TRUE
HSS-PullForUserState	TRUE
HSS-SubsInfoForImUserState	FALSE
HSS-SubsInfoForInitialFilterCriteria	FALSE
HSS-SubsInfoForSccfName	TRUE
HSS-SubsInfoForTransparentData	TRUE
HSS-UpdateForTransparentData	TRUE
ownerId	0
permissions	9
shareTree	nodeName=alltsp01
parent	

Submit Reset Change Class Properties

Connected To 'ldap://10.64.224.193:7423'

CPI: SDA LDAP Interface Description

The HSS Application Server Object stores all information related to Application Server supported by SDA.

HSS-ApplicationServerName is the application server's SIP URI.

Other highlighted parameters indicate whether Sh-Pull, Sh-Update or Sh-SubsNotif operations are allowed for the different Data References.

Licenses

The screenshot shows the JXplorer LDAP browser interface. On the left, the schema browser displays a tree structure under 'cn' with nodes like 'World', 'nodeName=alitsp01', 'applicationName=HSS', 'HSS-ConfigurationContainerName=HSS-ConfigurationContainer', 'HSS-LicenseName=HSS-License', 'HSS-SecurityContainerName=HSS-SecurityContainer', and 'HSS-SubscriberContainerName=HSS-Subscribers'. On the right, the 'Table Editor' shows the attributes for the 'HSS-LicenseName' entry. The attributes listed are:

attribute type	value
HSS-LicenseName	HSS-License
objectClass	HSS-License
groupID	813
HSS-IdConvergenceLicense	TRUE
HSS-ImsAkaLicense	FALSE
HSS-ImsIsActive	TRUE
HSS-MaxNumberOfApplicationServersLicense	20
HSS-MaxNumberOfContactsLicense	FALSE
HSS-MaxNumberOfUserPublicIdPairs	20000
HSS-PsCsDataRequestLicense	FALSE
HSS-RoamingAwarenessLicense	TRUE
HSS-SdalsActive	TRUE
HSS-SingleSignOnLicense	TRUE
HSS-TransparentDataLicense	TRUE
ownerId	813
permissions	8
shareTree	nodeName=alitsp01
parent	

Connected To 'ldap://10.64.224.193:7423'

CPI: ISM LDAP Interface Description

HSS-ImsAkaLicense enables the IMS AKA feature for USIM users.

HSS-MaxNumberOfApplicationServersLicense states the maximum number of Application Servers that can be licensed in HSS Application for the SDA module.

HSS-MaxNumberOfUsersLicense states the maximum number of users that can be handed.

HSS-PsCsDataRequestLicense enables SDA to handle the requests in order to ask for Location Information and User State related to GSM/WCDMA and Location Data related to the Wireline Access Network.

HSS-RoamingWirelineLicense enables the Roaming Awareness Wireline Access feature.

HSS-RoamingWirelessLicense enables the Roaming Awareness Wireless feature.

HSS-SingleSignOnLicense enables the SSO feature.

HSS-TransparentDataLicense enables SDA to handle transparent data and service indication objects

All these attributes are read-only.

Digest Authentication Parameters

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view shows a node named 'alitsp01' which contains an 'HSS-DigestAuthenticationData' object. The right panel displays the attributes of this object in a table format. Several attributes are highlighted with red boxes: 'HSS-AuthDomain' (sip:alitsp01@edu.mmtel.net), 'HSS-AuthLock' (TRUE), 'HSS-AuthLockAlarm' (FALSE), 'HSS-AuthMaxNumberOfNonce' (5), 'HSS-AuthNonceReusabilityLimit' (10), 'HSS-AuthNonceTimeLength' (900), 'HSS-AuthNonceTimeWindowSize' (6), 'HSS-AuthOpRequired' (FALSE), 'HSS-AuthRealmName' (edu.mmtel.net), 'HSS-PwdEncrypt' (TRUE), and 'ownerId' (811). The 'permissions' attribute is set to 11. The 'shareTree' attribute has a value of 'nodeName=alitsp01'. At the bottom of the right panel are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

attribute type	value
HSS-DigestAuthenticationDataName	HSS-DigestAuthenticationData
objectClass	HSS-DigestAuthenticationData
groupId	811
HSS-AuthDomain	sip:alitsp01@edu.mmtel.net
HSS-AuthLock	TRUE
HSS-AuthLockAlarm	FALSE
HSS-AuthMaxNumberOfNonce	5
HSS-AuthNonceReusabilityLimit	10
HSS-AuthNonceTimeLength	900
HSS-AuthNonceTimeWindowSize	6
HSS-AuthOpRequired	FALSE
HSS-AuthRealmName	edu.mmtel.net
HSS-PwdEncrypt	TRUE
ownerId	811
permissions	11
shareTree	nodeName=alitsp01
parent	

CPI: ISM LDAP Interface Description

Connected To 'ldap://10.64.224.193:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-167

HSS-AuthDomain contains a SIP URI that identifies the protection domain (all SIP URIs with the same value for the user info, host and port part).

HSS-AuthLock states if an identity shall be locked due to the exceeding of the maximum number of failed SIP or XCAP authentication attempts. Possible values: *TRUE/FALSE*.

HSS-AuthLockAlarm states if an alarm shall be issued when an identity becomes locked due to the exceeding of the maximum number of failed SIP or XCAP authentication attempts. Possible values: *FALSE/TRUE*.

HSS-AuthMaxNumberOfNonce states the maximum number of nonces per Public Identity. This maximum number is related to the number of simultaneous registrations for the Public Identity..

HSS-AuthMinPasswordLength/HSS-AuthMaxPasswordLength store the minimum (creation value 4) / maximum (creation value 16) password length for a Digest authentication. Only used for password provisioning.

HSS-AuthNonceReusabilityLimit is used to keep the maximum reusability limit for the generated nonce.

SSO Authentication Parameters

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view displays the LDAP structure under 'World' with 'nodeName=alltsp01'. A specific entry for 'HSS-SessionMngrDiameterId' is selected. On the right, the 'Table Editor' tab is active, showing the attributes for this entry:

attribute type	value
HSS-SsoConfigId	HSS-SsoConfiguration
objectClass	HSS-SsoConfiguration
groupID	811
HSS-SessionMngrDiameterId	alltsp01.edu.mmTEL.net
HSS-SessionMngrDiameterRealm	edu.mmTEL.net
HSS-SsoMaxFraudulentAttempts	2
HSS-SsoMaxXcapUnauthAttempts	2
ownerId	811
permissions	11
shareTree	nodeName=alltsp01
parent	

Below the table, buttons for 'Submit', 'Reset', 'Change Class', and 'Properties' are visible. The status bar at the bottom indicates 'Connected To ldap://10.64.224.193:7423'.

CPI: ISM LDAP Interface Description

HSS-SessionMngrDiameterId attribute contains the Session Manager Diameter host identifier.

HSS-SsoMaxFraudulentAttempts attribute indicates the maximum number of consecutive SSO SIP fraudulent authentication attempts for a user before raising a notification.

HSS-SsoMaxXcapUnauthAttempts attribute indicates the maximum number of consecutive SSO XCAP unauthorized attempts for a user before raising a notification.

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view under 'World' shows a node named 'jambala' which contains an 'applicationName=HSS' entry. This entry has several sub-entries, including 'HSS-ChargingContainerName=HSS-Charging', which is highlighted with a red box and a red arrow pointing to it from the left margin. To the right of the tree view is a table editor titled 'HTML View' showing attribute-value pairs for the selected object. The table has columns for 'attribute type' and 'value'. Several rows are highlighted with red boxes: 'HSS-ChargingProfileId' (value: DefaultChargingProfile), 'HSS-PrimaryCcf' (value: aaa://ee1mm01.edu.ims.se:19999;transport=tcp), 'objectClass' (value: HSS-ChargingProfile), 'groupIid' (value: 411), 'HSS-PrimaryEcf' (value: aaa://ee1mm01.edu.ims.se:19999;transport=tcp), 'HSS-SecondaryCcf' (value: aaa://ee1mm01.edu.ims.se:19999;transport=tcp), 'HSS-SecondaryEcf' (value: aaa://ee1mm01.edu.ims.se:19999;transport=tcp), 'ownerId' (value: 411), 'permissions' (value: 9), 'shareTree' (value: nodeName=jambala), and 'parent' (value: null). At the bottom of the table editor are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

attribute type	value
HSS-ChargingProfileId	DefaultChargingProfile
HSS-PrimaryCcf	aaa://ee1mm01.edu.ims.se:19999;transport=tcp
objectClass	HSS-ChargingProfile
groupIid	411
HSS-PrimaryEcf	aaa://ee1mm01.edu.ims.se:19999;transport=tcp
HSS-SecondaryCcf	aaa://ee1mm01.edu.ims.se:19999;transport=tcp
HSS-SecondaryEcf	aaa://ee1mm01.edu.ims.se:19999;transport=tcp
ownerId	411
permissions	9
shareTree	nodeName=jambala
parent	null

Connected To 'ldap://192.168.13.193:7423'
CPI: ISM LDAP Interface Description
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-169

HSS Charging Profile objects contain information related to charging. Each object specifies a charging profile.

HSS-PrimaryCcf / HSS-SecondaryCcf attributes are used to identify the Primary / Secondary Charging Collection Function.

HSS-PrimaryEcf / HSS-SecondaryEcf attributes are used to identify the Primary / Secondary Event Charging Function.

Service Triggers (Initial Filter Criteria)

The screenshot shows the JXplorer LDAP browser interface. On the left, the schema tree is expanded to show nodes like 'cn', 'World', 'nodeName=al1tsp01', and 'applicationName=HSS'. Under 'nodeName=al1tsp01', there's a 'HSS-ServiceTypeContainerName=HSS-ServiceTypeContainer' node, which contains 'HSS-ServiceTypeContainerId=mtas'. This node has several sub-nodes, one of which is 'HSS-TriggerPriority=407'. On the right, the 'Table Editor' view is open, showing attributes for this object. The 'HSS-TriggerPriority' attribute is listed with a value of '407'. Other visible attributes include 'objectClass' (HSS-ServiceTrigger), 'groupid' (0), 'HSS-ConditionType' (AND), 'HSS-DetectionPoint' (INVITE), 'HSS-IsActive' (TRUE), 'HSS-NegatedDetectionPoint' (FALSE), 'HSS-RequestedURI' (empty), 'HSS-TriggerDescription' (Originating Invite), 'HSS-TriggerType' (ORIGINATING), 'ownerId' (0), 'permissions' (9), and 'shareTree' (nodeName=al1tsp01). The 'HSS-RegistrationTypes' and 'HSS-SIPHeaders' attributes are also present but empty. Buttons at the bottom of the editor include 'Submit', 'Reset', 'Change Class', and 'Properties'.

CPI: ISM LDAP Interface Description

HSS Service Trigger object stores all the information related to each of the service triggers which can be part of the different Service Profile.

HSS-TriggerPriority is used to identify each Service Trigger.

HSS-ConditionType indicates the relationship among the different criteria in one HSS-ServiceTrigger. Possible values: AND, OR.

HSS-DetectionPoint indicates under which circumstances the trigger can be evaluated.

HSS-IsActive indicates that this Trigger is enabled in all Service Profiles of this Service Type.

HSS-RequestedURI sets a trigger condition based on the content of the Request-URI for the request.

HSS-SIPHeaders a bag of structures each one identifying a SIP Header of this trigger.

HSS-TriggerDescription is used to describe the trigger.

HSS-TriggerType is used to identify the type of this trigger. Possible values: ORIGINATING, TERMINATING_REGISTERED, TERMINATING_UNREGISTERED, NOT_ORIGINATING, NOT_TERMINATING_REGISTERED, NOT_TERMINATING_UNREGISTERED

Service triggers are also known under the name of Initial Filter Criteria (IFC).



Service Profiles

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn Quick Search

Explore Results Schema

World

- nodeName=allsp01
 - applicationName=HSS
 - HSS-ConfiguratorContainerName=HSS-ConfigurationContainer
 - HSS-NetworkDomainName=edu.mmtel.net
 - HSS-ApplicationServerContainerName=HSS-ApplicationServers
 - HSS-ChargingContainerName=HSS-Charging
 - HSS-DigestAuthenticationDataName=HSS-DigestAuthentication
 - HSS-IsmConfigurationDataName=HSS-IsmConfigurationData
 - HSS-RoamingConfigId=HSS-Roaming-Configuration
 - HSS-SdaConfigurationDataName=HSS-SdaConfigurationData
 - HSS-ServiceIndicationContainerName=HSS-ServiceIndication
 - HSS-ServiceSupportContainerName=HSS-ServiceSupportContainer
 - HSS-ServiceTypeContainerName=HSS-ServiceTypeContainer
 - HSS-ServiceType=mts
 - HSS-TriggerPriority=401
 - HSS-TriggerPriority=407
 - HSS-TriggerPriority=409
 - HSS-TriggerPriority=411
 - HSS-TriggerPriority=419
 - HSS-ServiceProfileId=tispdn
 - HSS-ServiceType=Presence
 - HSS-ServiceType=PresenceXDMIS
 - HSS-ServiceType=RLSDMIS
 - HSS-ServiceType=SharedDMIS
 - HSS-SsoConfigId=HSS-SsoConfiguration
 - HSS-LicenseName=HSS-License
 - HSS-SecurityContainerName=HSS-SecurityContainer
 - HSS-SubscriberContainerName=HSS-Subscribers

attribute type	value
HSS-DefaultApplicationServer	sip:alltsp02.edu.mmtel.net;lr
HSS-ServiceProfileId	tispdn
objectClass	HSS-ServiceProfile
groupID	0
HSS-DefaultASHandling	
HSS-Trigger2ApplicationServers	407:sip:al1mtas.edu.mmtel.net;call=orig;lr;
HSS-Trigger2ApplicationServers	401:sip:al1mtas.edu.mmtel.net;lr;call=orig;
HSS-Trigger2ApplicationServers	411:sip:al1mtasoutunreg.edu.mmtel.net;call=t...
HSS-Trigger2ApplicationServers	419:sip:conference.edu.mmtel.net;lr;call=term;
HSS-Trigger2ApplicationServers	409:sip:al1mtasout.edu.mmtel.net;call=term_r...
ownerId	0
permissions	9
shareTree	nodeName=allsp01
parent	

CPI: ISM LDAP Interface Description

Connected To 'ldap://10.64.224.193:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-171

HSS Service Profile is an object that holds a set of information that describes how to configure the Application Servers providing a specific Service. There can be several Service Profiles assigned to a Service Type.

HSS-Trigger2ApplicationServers identifies a specific service trigger (belonging to the same Service Type), an Application Server to which the trigger is assigned and the Default Handling of the S-CSCF for that pair, service trigger and Application Server. If a trigger belonging to the Service Type is not included into this bag, it means that this trigger is assigned to the Default Application Server.

CPI: CSCF Common Configuration Management Parameters

Connected To 'ldap://10.64.224.194:323'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-172

Service triggers which may be common to multiple users can be locally administered and stored at the S-CSCF, also known as Shared IFC. Locally administered service triggers are identical in structure to service triggers explicitly defined in the Service Profile of a subscriber. However the User Service Profile downloaded from the HSS to the S-CSCF includes a reference to the locally administered service triggers, instead of the explicit definition of the service trigger. This reduces the amount of data on the Cx interface from the HSS to the CSCF.

SccsSharedIfcEnabled is used to enable and disable the Shared IFC function. Default is set to FALSE, that means the function is not enabled.

SccsSharedIfcSynchronization: After a configuration of Shared IFC parameters, SccsSharedIfcSynchronization has to be set to True to activate the changes. The application puts the new Shared IFC definitions in service and then sets the SccsSharedIfcSynchronization to False when done.

Shared IFC (IFC Class Description on CSCF side)



JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn

Explore Results Schema Quick Search

objectClass attribute type value

ScsIfcName	scsifcName	sip:asname.com;lr
ScsIfcConditionTypeCNF	ScsIfcConditionTypeCNF	TRUE
ScsIfcDefaultHandling	ScsIfcDefaultHandling	SESSION_CONTINUED
ScsIfcEnabled	ScsIfcEnabled	TRUE
ScsIfcName	Service1	
ScsIfcPriority	ScsIfcPriority	0
group	group	0
ownerId	ownerId	0
permissions	permissions	9
shareTree	shareTree	nodeName=alitsp05
parent	parent	

Submit Reset Change Class Properties

The screenshot shows the JXplorer LDAP browser interface. The left pane displays a tree view of object classes under 'cn'. The right pane shows the 'Table Editor' with columns for 'attribute type' and 'value'. A red box highlights the 'ScsIfcName' row, which has a value of 'sip:asname.com;lr'. Another red box highlights the 'Service1' entry in the 'ScsIfcName' column. The bottom right corner of the interface has buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

CPI: CSCF Common Configuration Management Parameters

ScscfSharedIfcId identifies shared IFC set. Same id should be used in the service profile on HSS to refer to this IFC set.

ScscfIfcAsName is the address of the Application Server to invoke when the filter criteria is met.

ScscfIfcConditionTypeCNF indicates if the filter criteria is expressed in Conjunctive Normal Form. When True an OR operation is performed between Service Point Triggers within a group and an AND operation is performed between the groups included in the IFC. When False an AND operation is performed between Service Point Triggers within a group and an OR operation is performed between the groups included in the IFC.

SscfIfcDefaultHandling indicates whether the dialog is to be released if the Application Server could not be reached ("SESSION_CONTINUED" or "SESSION TERMINATED").

ScscfIfcEnabled indicates if the IFC is used.

ScscIfcPriority indicates the priority of the filter criteria. The priority must be unique within a Shared IFC set.

Shared IFC (Service Profile Trigger Description on CSCF side)

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view shows a node named 'alitspos' which contains an entry for 'InitialReg'. This entry has several attributes listed in a table on the right. The attributes 'ScscfSptConditionNegated', 'ScscfSptName', 'ScscfSptTriggerType', 'ScscfSptTriggerContext', and 'ScscfSptTriggerValue' are highlighted with red boxes.

attribute type	value
objectClass	ScscfSptClass
ScscfSptConditionNegated	FALSE
ScscfSptName	InitialReg
ScscfSptTriggerType	METHOD
groupId	0
ownerId	0
permissions	9
ScscfSptTriggerContext	REGISTER
ScscfSptTriggerValue	INITIAL_REGISTRATION
shareTree	nodeName=alitspos
parent	

CPI: CSCF Common Configuration Management Parameters

ScscfSptConditionNegated indicates if the result of the Service Point Trigger evaluation is negated.

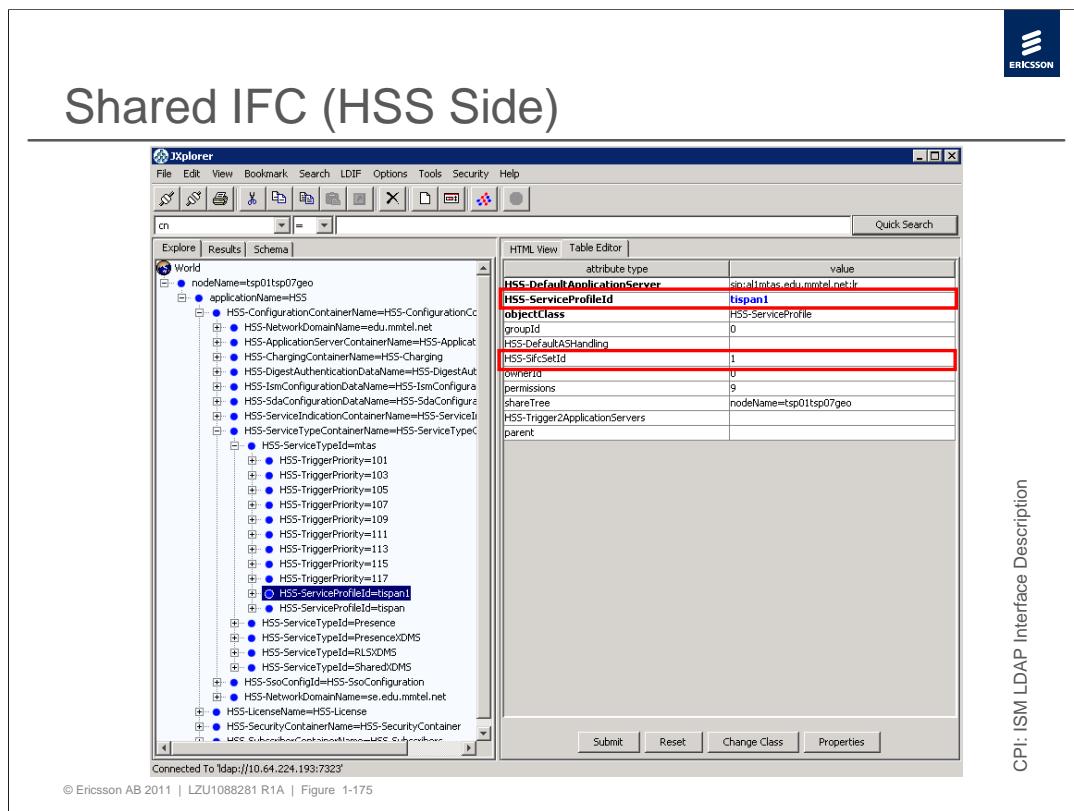
ScscfSptTriggerType indicates the type of Service Point Trigger ("METHOD", "REQUEST_URI", "HEADER", "SESSION_CASE").

ScscfSptTriggerContext parameter captures the context associated with the trigger type:

- When *ScscfSptTriggerType* is "METHOD" this attribute captures the method name.
- When *ScscfSptTriggerType* is "REQUEST_URI" this attribute is not used.
- When *ScscfSptTriggerType* is "HEADER" this attribute captures the header name.
- When *ScscfSptTriggerType* is "SESSION_CASE" this attribute captures the session_case.

ScscfSptTriggerValue parameter captures the value of the trigger associated with the trigger type and context:

- When *ScscfSptTriggerType* is "METHOD" and the *ScscfSptTriggerContext* is "REGISTER" this attribute captures the registration type.
- When *ScscfSptTriggerType* is "METHOD" and the *ScscfSptTriggerContext* is not "REGISTER" this attribute must be <empty>.
- When *ScscfSptTriggerType* is "REQUEST_URI" this attribute captures the Request-URI value expressed as a regular expression.
- When *ScscfSptTriggerType* is "HEADER" this attribute captures the header value as a regular expression.
- When *ScscfSptTriggerType* is "SESSION_CASE" this attribute must be <empty>.

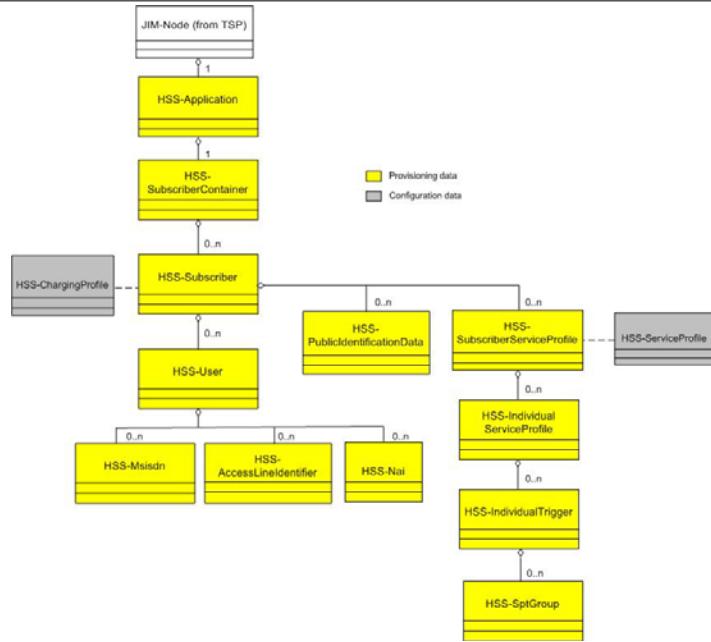


CPI: ISM LDAP Interface Description

HSS-ServiceProfileId attribute identifies the service profile.

HSS-SifcSetId attribute contains the identifier of the Shared Initial Filter Criteria set (configured on S-CSCF) associated to the Service Profile.

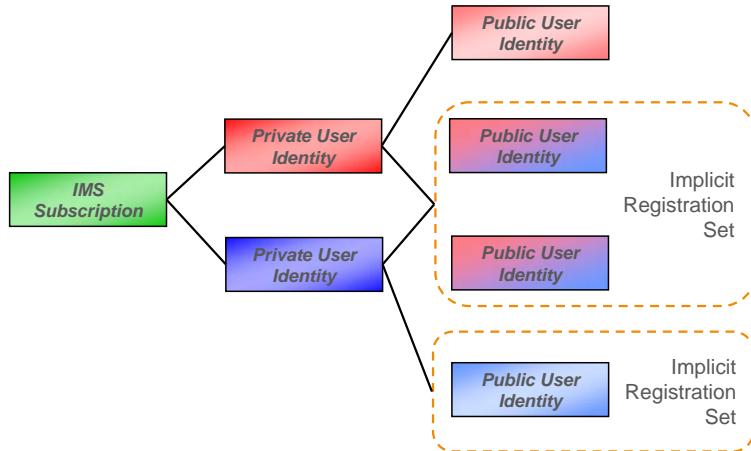
ISM Provisioning Object Class Model



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-176

This picture presents ISM Provisioning Object Class Model. It is only applicable to Monolithic deployment of HSS.

PrivateUserID vs PublicUserID



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-177

A Private User Identity has one or more Public User Identities. Each Public User Identity can be registered from several User Equipments (UE). That allows more than one contact address to be connected to the same Public User Identity. Each user is connected to a Subscription, which can cover more than one Private User Identity.

One or more implicit registration set can be configured for a user.

If at registration the public user identity to be registered belongs to such a set, all public user identities in the implicit registration set are fetched from the user profile and registered at the same time.

All public user identities within an implicit registration set share the same expiration timer for the same contact. At re-registration a SIP REGISTER with a new expiration time is sent from one public user identity and affects all identities within the same set.

Subscriber Data – Subscriber ID

attribute type	value
HSS-SubscriberID	4687163901@edu.mmtel.net
objectClass	HSS-Subscriber
groupId	0
HSS-ChargingProfileId	DefaultChargingProfile
HSS-DeauthmatedId	(non string data)
HSS-IsPsContainer	FALSE
HSS-LocationData	sip:10.64.227.194:5060
HSS-LocationData	CSCFCX.edu.mmtel.net
HSS-PrivacyIndicator	FALSE
HSS-SubscriberBarringInd	FALSE
ownerId	0
permissions	9
shareTree	nodeName=alltsp01
HSS-DefaultReferenceAccessLocation	
parent	

CPI: ISM LDAP Interface Description

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-178

HSS-PrivacyIndicator This attribute indicates if data sharing with the Application Servers is allowed or not. Type: Boolean Visibility: read-write Required: optional Creation Value: "FALSE". Values: If FALSE, data sharing with the Application Servers is allowed. If TRUE, data is protected. "TRUE"

HSS-SubscriberBarringInd This attribute indicates if the subscriber, and all its users, are barred or not. Type: Boolean Visibility: read-write Required: optional Creation Value: "FALSE" "TRUE"

HSS-ChargingProfId Attribute used to identify the Charging Profile. Type: case sensitive string Visibility: write-once Primary key



Subscriber Data – Private User ID

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn

Explore Results Schema

World

- nodeName=tsp01tsp07geo
 - applicationName=HSS
 - HSS-ConfigurationContainerName=HSS-ConfigurationContainer
 - HSS-LicenseName=HSS-License
 - HSS-SecurityContainerName=HSS-SecurityContainer
 - HSS-SubscriberContainerName=HSS-Subscribers
 - HSS-SubscriberID=4687040008@edu.mmtel.net
 - HSS-PrivateUserID=sip:4687040008@edu.mmtel.net
 - HSS-PublicIDValue=tel:+4687040008
 - HSS-SubscribedID=4687040009@edu.mmtel.net
 - HSS-SubscribedID=4687040010@edu.mmtel.net
 - HSS-SubscribedID=4687040011@edu.mmtel.net
 - HSS-SubscribedID=4687040012@edu.mmtel.net
 - HSS-SubscribedID=4687040013@edu.mmtel.net
 - HSS-SubscribedID=4687040014@edu.mmtel.net
 - HSS-SubscribedID=4687040050@edu.mmtel.net
 - HSS-SubscribedID=468716123@se.edu.mmtel.net
 - HSS-SubscribedID=4687991235@edu.mmtel.net
 - HSS-SubscribedID=4687991236@edu.mmtel.net
 - HSS-SubscribedID=alolson@edu.mmtel.net
 - HSS-SubscribedID=andy@edu.mmtel.net
 - HSS-SubscribedID=bjorn@edu.mmtel.net
 - HSS-SubscribedID=crengtul@edu.mmtel.net

attribute type	value
HSS-PrivateUserID	4687040008@edu.mmtel.net
objectClass	HSS-User
groupID	0
HSS-AllowedAuthMechanism	Digest
HSS-LocationData	sip:cscf02.edu.mmtel.net:5060
HSS-LocationData	CSCFC02.edu.mmtel.net
HSS-ReferenceAccessLocation	
HSS-RoamingAllowed	TRUE
HSS-SipLocked	FALSE
HSS-UserBarringInd	FALSE
HSS-UserIm	
HSS-UserState	registered
ownerID	0
permissions	9
shareTree	nodeName=tsp01tsp07geo
HSS-Ext	
HSS-PrimaryHA1Password	
HSS-SecondaryHA1Password	
HSS-UserPassword	
parent	

CPI: ISM LDAP Interface Description

HSS-AllowedAuthMechanism contains the authentication mechanisms supported by the user. In case both NBA and Digest values are provisioned, if the SIP Authentication Scheme received from the S-CSCF is UNKNOWN, then NBA is selected first. SSO and NBA mechanisms can be only set if HSS-SingleSignOnLicense is set to TRUE. SSO, NBA and Digest are currently supported. If Digest is supported and the user is not a PSI (HSS-IsPsiContainer attribute within HSS-Subscriber object class), HSS-UserPassword or HSS-PrimaryHA1Password must be present.

HSS-LocationData is the location data currently used by the subscriber's public identities. This attribute contains information about location to be used for originating and terminating calls.

HSS-RoamingAllowed indicates whether the User is allowed to roam or not.

HSS-SipLocked states if the user is blocked for SIP authentication purposes.

HSS-UserBarringInd indicates if the user is barred or not, at a user level. A user is barred when this indicator and/or HSS-SubscriberBarringInd of its corresponding HSS-Subscriber are set to TRUE.

HSS-UserState shows the user registration state. Its value depends on the registration value in HSS-PublicIdState attribute of HSS-PublicIdentificationData Object Class. An operator could change the value of HSS-UserState only from registered or unregistered to not_registered (administrative deregistration). If HSS-UserState is not_registered it is not possible to update HSS-UserState to registered or unregistered.

Values: unregistered (when one or more of the user's public identities are in Unregistered state and the rest in Not Registered), registered (when one or more of the user's public identities are in Registered state), not_registered (when all the user's public identities are in Not Registered state).

HSS-UserPassword contains the user password to be used in the SIP Digest authentication.

HSS-PrimaryHA1Password contains the A1 hashed value to be used in SIP Digest authentication when the digest user name received matches with the provisioned private identity. Only one of the *HSS-UserPassword* or *HSS-PrimaryHA1Password* attributes must be set to a value different from empty one.

HSS-SecondaryHA1Password contains the A1 hashed value to be used in SIP Digest authentication when the digest user name received matches with the user part (removing the realm part) of the provisioned private identity.

At digest authentication a digest challenge response is calculated using a nonce and a H(A1) value. The H(A1) is a hashed result of the user's digest user name, digest realm and digest password. The digest username is the IMPI provisioned in the HSS, usually in the format *username@realm* as per the 3GPP standard. However some UEs do not include the realm in the username for the digest authorization data. The CSCF and the HSS provide additional support for these UEs. The HSS downloads one H(A1) value that was computed using a digest username without a realm. Alternatively the HSS downloads two H(A1) values where one is associated to the username with a realm and one is associated to the username without a realm.

For example, some terminals do not include the realm in the user name even when 3GPP standards specify it must include it. If the HSS provisions the IMPI in the “*username@realm*” format as per the 3GPP standard and the UEs do not include the realm in the digest username included in the Authorization header, then to deal with these UEs, secondary H(A1) support is required in the HSS.

Subscriber Data – Public ID Value

attribute type	value
HSS-PublicIdValue	sip:4687163901@edu.mmtel.net
objectClass	HSS-PublicIdentificationData
groupId	0
HSS-AuthorizedVisitedAccessLineList	
HSS-ImpliedRegSetId	1
HSS-IsDefault	TRUE
HSS-LocationData	sip:10.64.227.194:5060
HSS-LocationData	CSCFx.edu.mmtel.net
HSS-PrivateIdPairState	4687163901@edu.mmtel.net:registered
HSS-PublicIdState	registered
HSS-SessionSharingInd	FALSE
HSS-SubscriberServiceProfileId	mainprofile7163901
HSS-WirelineAccessAllowed	
HSS-XcapAllowed	TRUE
HSS-XcapLocked	FALSE
ownerId	0
permissions	9
shareTree	nodeName=al1tsp01
HSS-MaxNumberOfContacts	
HSS-PrivateId	
HSS-XcapPassword	
parent	

CPI: ISM LDAP Interface Description

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-181

HSS-PublicIdState shows the Public Identity registration state. This attribute indicates if the Public Identity is registered, not registered or unregistered. A public identity is in *unregistered* state when it is registered as a consequence of a terminating call due to an *unregistered* service. An operator could change the value of HSS-PublicIdState only from registered or unregistered to *not_registered* (administrative deregistration). If HSS-PublicIdState is *not_registered* it is not possible to update HSS-PublicIdState to registered or unregistered. The value registered is not applicable to HSS-PublicIdState if the Public Identity is a PSI.

HSS-LocationData contains information about location to be used for originating and terminating calls. It comprises the following three different values: Originating S-CSCF (serves the registered public identities for the originating calls), Terminating S-CSCF (serves the registered public identities for the terminating calls) and Diameter Server Identifier (identifies the diameter server).

HSS-UserServiceProfileId is a reference to HSS-UserServiceProfile to identify what is the User Service Profile assigned for this Public Identity.

HSS-MaxNumberOfContacts - This is a feature over Ericsson Cx interface allowing the HSS to define a Maximum Number of Contacts (MNoC) to be registered per IMPU. This value is further downloaded to the S-CSCF during the registration process. With this feature the operator is able to limit the number of devices that can be registered with the same IMMU and IMPI. A typical use is for fixed telephony where an operator could limit the number of fixed phones of a household.

Subscribers Data – User Service Profile ID

attribute type	value
HSS-SubscriberServiceProfileId	mainprofile7163901
objectClass	HSS-SubscriberServiceProfile
ownerId	0
HSS-ConfiguredServiceProfiles	lspan
HSS-MaxSessions	11
HSS-PhoneContext	edu.mmtel.net
HSS-SubscribedMediaProfile	1
permissions	9
shareFree	nodeName=alitsp01
parent	

CPI: ISM LDAP Interface Description

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-182

HSS-ConfiguredServiceProfiles contains all the Service Profiles (HSS-ServiceProfileId attribute values) associated to the User Service Profile.

HSS-SubscribedMediaProfile is used to identify the set of session description parameters that the user is authorized to request.

Subscribers Data for Mobile Access - MSISDN

The screenshot shows the JXplorer LDAP browser interface. On the left, the 'Explore' panel displays a tree structure of LDAP entries under 'World'. One entry is expanded, showing 'nodeName=alitsp01', 'applicationName=HSS', 'HSS-ConfigurationContainerName=HSS-ConfigurationContainer', 'HSS-LicenseName=HSS-License', 'HSS-SecurityContainerName=HSS-SecurityContainer', 'HSS-SubscriberContainerName=HSS-Subscribers', and several 'HSS-SubscriberID' entries. One specific entry is selected: 'HSS-Msisdn=4687163901'. On the right, the 'Table Editor' panel shows a table with attributes for this selected entry. The table has two columns: 'attribute type' and 'value'. The rows are:

attribute type	value
HSS-Msisdn	4687163901
objectClass	HSS-Msisdn
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=alitsp01
parent	

At the bottom of the interface, there are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A status bar at the bottom left indicates 'Connected To ldap://10.64.224.193:7423'.

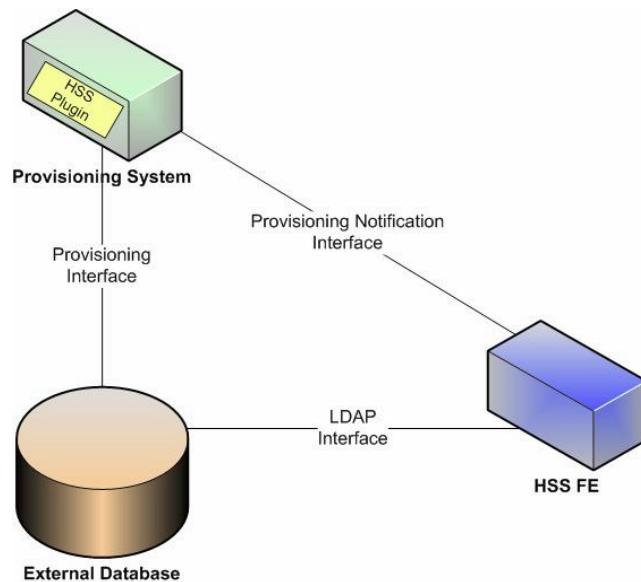
CPI: ISM LDAP Interface Description

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-183

HSS-Msisdn identifies the Mobile Station International Subscriber Directory Number assigned to a user. MSISDN length is checked to be within 5 and 15 digits, both included. MSISDN being an Access Identifier is used by the Single Sign On authentication mechanism.



HSS Front End configuration



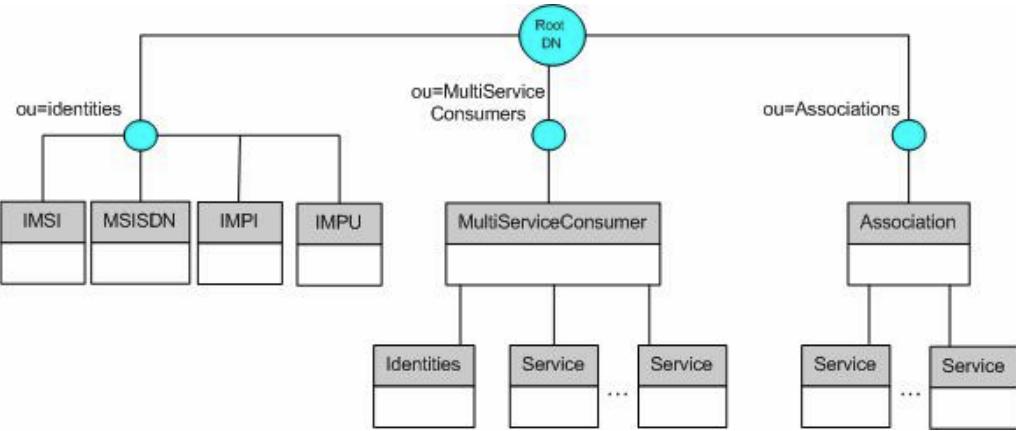
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-184

The HSS FE deployment is one of the supported deployment options (the other option is monolithic HSS).

This feature reflects a new realization for the HSS/SLF product, the HSS Front End (HSS FE), which is the entity where the logic of the HSS application relies. The HSS FE is stateless and user data-less. The HSS FE reads subscriber data from a BE-DB to perform the HSS procedures. In the Ericsson portfolio the back end database (BE-DB) is called Common User Data Base (CUDB). This type of configuration applies to every module in HSS, except SLF. The figure shows the HSS FE type of configuration.



Provisioning datamodel (CUDB)



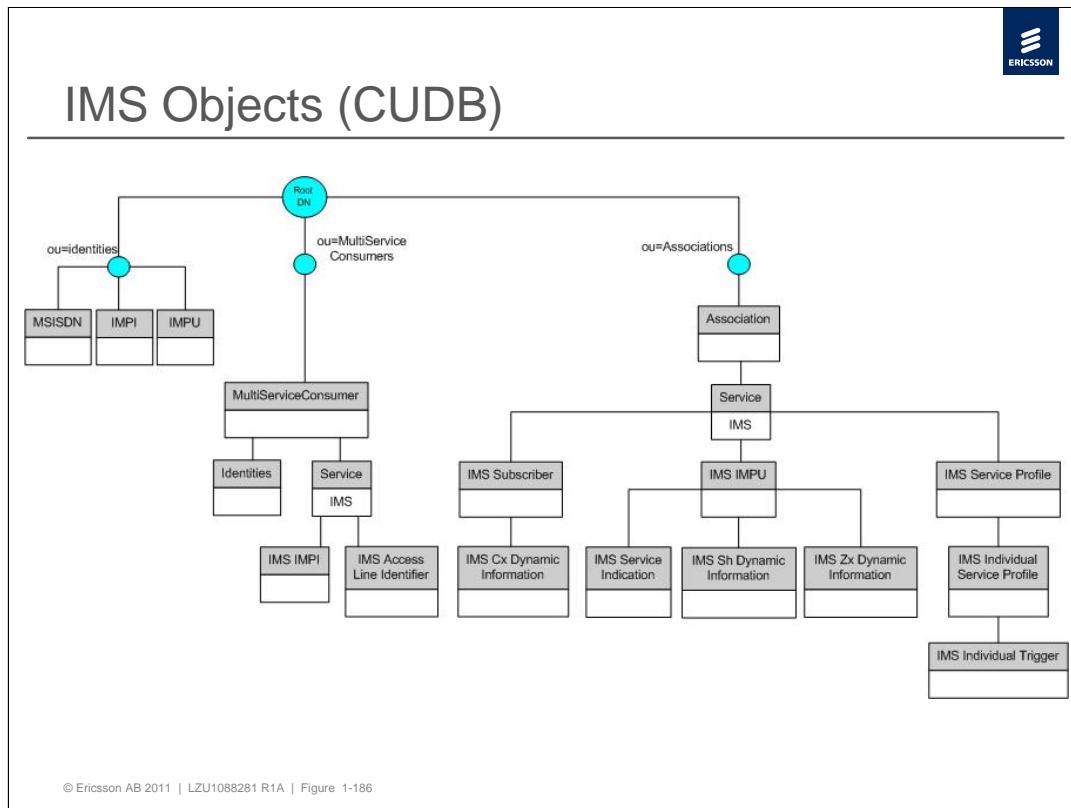
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-185

The Provisioning System is in charge of provisioning the External Database.

The user related provisioning is performed in the BE-DB. Therefore, there is not an LDAP provisioning interface in HSS-FE type of configuration. HSS is notified on the provisioning changes by means of a new SOAP provisioning notifications interface.

Since in the HSS FE type of configuration the provisioning is not part of the HSS but an external provisioning system is in charge of it, a mechanism to maintain the subscriber data consistency along the network is needed. HSS provides to the provisioning system a Validator software that implements these provisioning constraints required for user data consistency. The figure depicts the external database objects model for provisioning purposes.

HSS FE needs to inform the network nodes about changes in the subscriber data, so it needs to be informed by the provisioning system about these changes through a provisioning notification interface.



IMS Subscriber object contains information related to the IMS subscriber. An instance of this object must be created when the corresponding Service instance with its *serv* attribute initialized to "IMS" is created.

IMS Cx Dynamic object contains the Cx-related dynamic information of the IMS subscriber. An instance of this object must be created when the corresponding *ImsSubs* instance is created. Other ways to create instances of this object are not allowed.

IMS IMPU object contains information related to an IMS Public Identity.

IMS Zx Dynamic object contains the Zx-related dynamic information of the IMS Public Identity. An instance of this object must be created when the corresponding *ImsImpu* instance is created.

IMS Sh Dynamic object contains the Sh-related dynamic information of the IMS Public Identity. An instance of this object must be created when the corresponding *ImsImpu* instance is created.

IMS Service Profile object contains service data associated to a specific IMPU.

IMS Individual Service Profile object contains service data associated to a specific IMPU.

IMS Individual Trigger object contains all the information related to each of the service triggers which can be part of different Service Profiles.

IMS Service Indication object contains service related to data associated to an specific service/IMPU pair.



HSS External Database Configuration

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

Quick Search

attribute type value

HSS-EsmExtDbConfigLogActive	TRUE
HSS-EsmExtDbConfigOrigVipList	10.10.10.10
HSS-EsmExtDbConfigOrigVipList	10.10.10.11
HSS-EsmExtDbConfigRootDnList	1:ou=Associations,dc=operator,dc=com
HSS-EsmExtDbConfigRootDnList	2:ou=mMSCs,dc=operator,dc=com
HSS-EsmExtDbConfigRootDnList	3:dc=impi,ou=identities,dc=operator,dc=com
HSS-EsmExtDbConfigRootDnList	4:dc=impu,ou=identities,dc=operator,dc=com
HSS-EsmExtDbConfigRootDnList	5:dc=imsi,ou=identities,dc=operator,dc=com
HSS-EsmExtDbConfigRootDnList	6:dc=msisdn,ou=identities,dc=operator,dc=com
HSS-EsmExtDbConfigRootDnList	7:dc=ipaddress,ou=identities,dc=operator,dc=com
HSS-EsmExtDbConfigUrlList	0:ldap://10.10.10.117:389\$cn=manager,dc=operator,dc=com
HSS-EsmExtDbConfigUrlList	1:ldap://10.10.10.117:389\$cn=manager,dc=operator,dc=com

Submit Reset Change Class Properties

See also CPI "LDAP Interface Description"

Working Offline

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-187

The picture represents HSS External Database Configuration for the ESM module. External Database Configuration for ISM/SDA has a similar structure

HSS-EsmExtDbConfigLogActive indicates whether the log information related to the external database access, is logged or not.

HSS-EsmExtDbConfigOrigVipList defines IP addresses to be randomly used as originating IP address when HSS acts as LDAP client towards the external database.

HSS-EsmExtDbConfigRootDnList defines which are the root DNs to be used when accessing the external database.

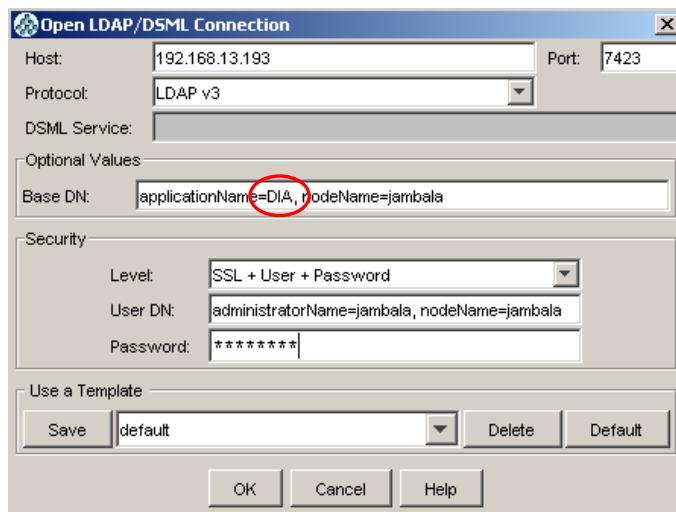
HSS-EsmExtDbConfigUrlList is an array of case sensitive strings each one containing the necessary information to access an external database. Each string contains the following information:

- URL: IP address and port of LDAP server.
- User Name: it is the DN administrator name to be used in the authentication of LDAP protocol.
- Password: it is the password to be used in the authentication of LDAP protocol.
- Authentication method: The supported authentication method to be used in the authentication of LDAP protocol.

More information can be found in *LDAP Interface Description for Accessing External Database in HSS_FE Interwork Description*.



Login to the Diameter application (HSS)



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-188

The Application name for the Diameter application is *DIA*.

In the Diameter application it is possible to configure and verify the Cx Interface towards CSCF, Zx interface towards Aggregation Proxy, Sh interface toward Application Servers or E-CSCF and Sih interface towards ISM Session Manager (SM).

In the Diameter application it is also possible to configure Dh interface between SLF and Application Servers or E-CSCF, Dzx interface between SLF and Aggregation Proxy as well as Dx interface between SLF and I-CSCF.

Diameter application identities are as follows:

16777216 – Cx and Dx interfaces

16777217 – Sh and Dh interfaces

16777227 – Sih interface

16777228 – Zx and Dzx interfaces

Diameter Interface (HSS side) – Stack Id

The screenshot shows the Ericsson iXplorer LDAP browser interface. The left pane displays the LDAP tree structure under 'cn' with nodes like 'nodeName=jambala' and 'stackContainerId=HSS'. The right pane shows a table editor for the 'cn' entry, specifically for the 'stackContainerId=HSS' node. The table lists various attributes and their values. Several attributes are highlighted with red boxes: 'portNr', 'supportedVendorIds', 'ipAddressesList', 'supportedAuthAppIds', and 'transportLayerType'. The table has columns for 'attribute type' and 'value'. At the bottom of the table are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A vertical sidebar on the right is labeled 'CPI: Diameter Parameter List'.

attribute type	value
hostId	HSS.edu.hss.se
objectClass	DIA-CFG-OwnNodeConfig
portNr	3868
productName	Ericsson Diameter
realm	edu.hss.se
stackId	HSS
supportedVendorIds	193
supportedVendorIds	10415
allowConnectFromUnknownNode	FALSE
dnsVendorId	10415
enabled	TRUE
firmwareRevision	1
ownerId	0
ipAddressesList	0.192.168.7.101
loadRegulationEnabled	TRUE
maxInboundSctpStreams	1
maxNumberOffRetries	0
maxOutboundSctpStreams	1
maxRequestPendingTime	10
ownerId	0
permissions	63
sendErrorAtOverload	TRUE
shareTree	applicationName=DIA nodeName=jambala
supportedAuthAppIds	16777216
supportedVendorSpecificApps	0.10415.16777216.0
supportedVendorSpecificApps	1.193.16777228.0
supportedVendorSpecificApps	2.10415.167772217.0
supportedVendorSpecificApps	3.193.16777227.0
tcTimer	10
transportLayerType	1
transportLayerType	0

In the figure the local host data for the HSS side of the Cx interface is shown. Some of the parameters are highlighted.

PortNr - This is the local listener port number that the remote diameter nodes are using for communication with this node.

enabled - This boolean can be set to FALSE whenever the node should suspend its activity. It may be used instead of clearing all "enabled" parameters for neighbourNodes separately.

ipAddressesList – It is a list of IPv4 addresses (string) that makes the own node accessible when using transport protocol TCP. The first address in the list is considered the primary one. This list is checked to find out if any of the IP addresses in the list are repeated, and if so, an LDAP error will be raised, and the operation will not take place.

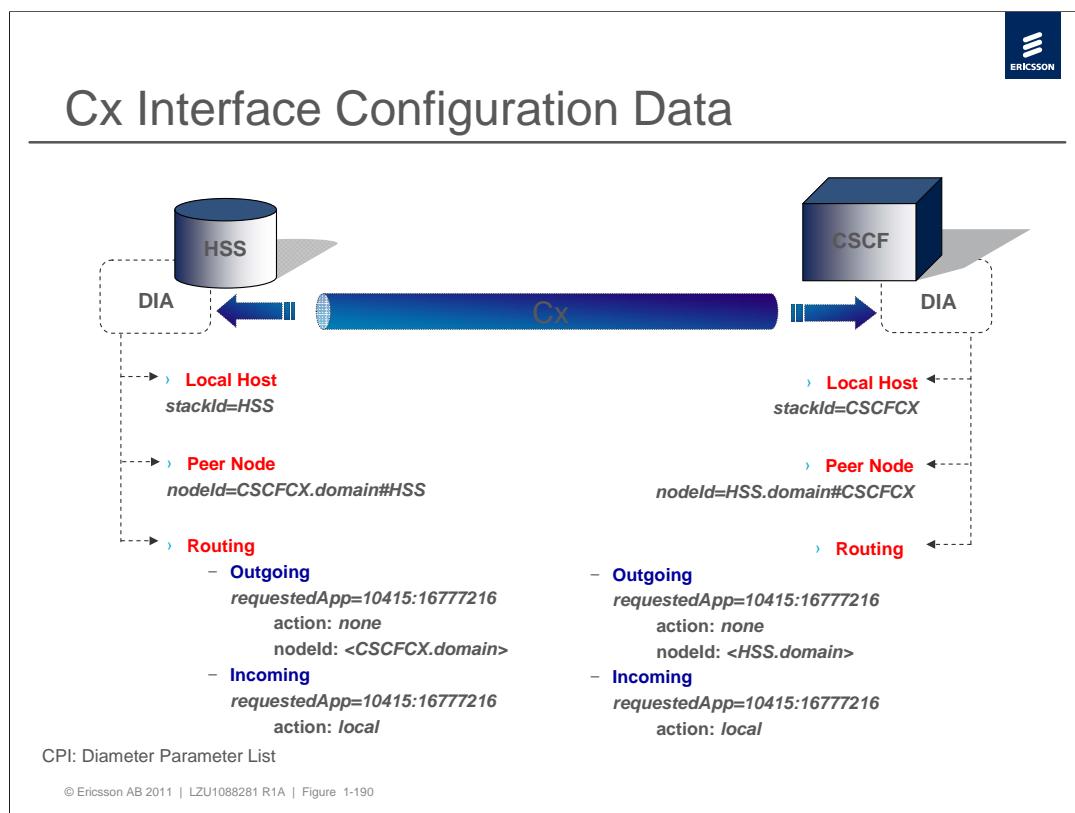
supportedAuthAppIds – This attribute is a list of applications that supports Authentication or Authorization requests. The Authentication Application ID defined by 3GPP for the Cx interface is 16777216.

transportLayerType defines the transport layer to be used when setting up a connection to this node. Values: 0 = Not defined (creation value), 1 = TCP, 2 = SCTP and 3 = First SCTP, then TCP.

The following Diameter vendor IDs are defined in the figure.

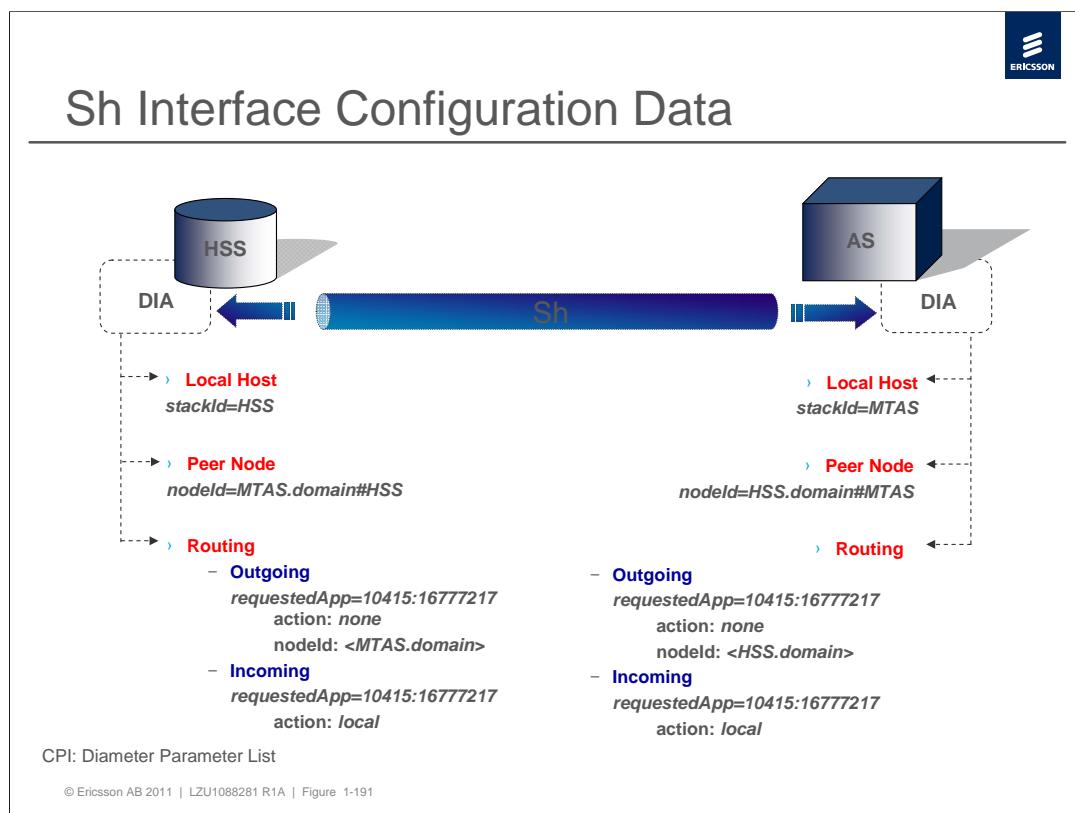
0 : IETF defined base Diameter Protocol

10415: 3GPP defined Diameter Extensions



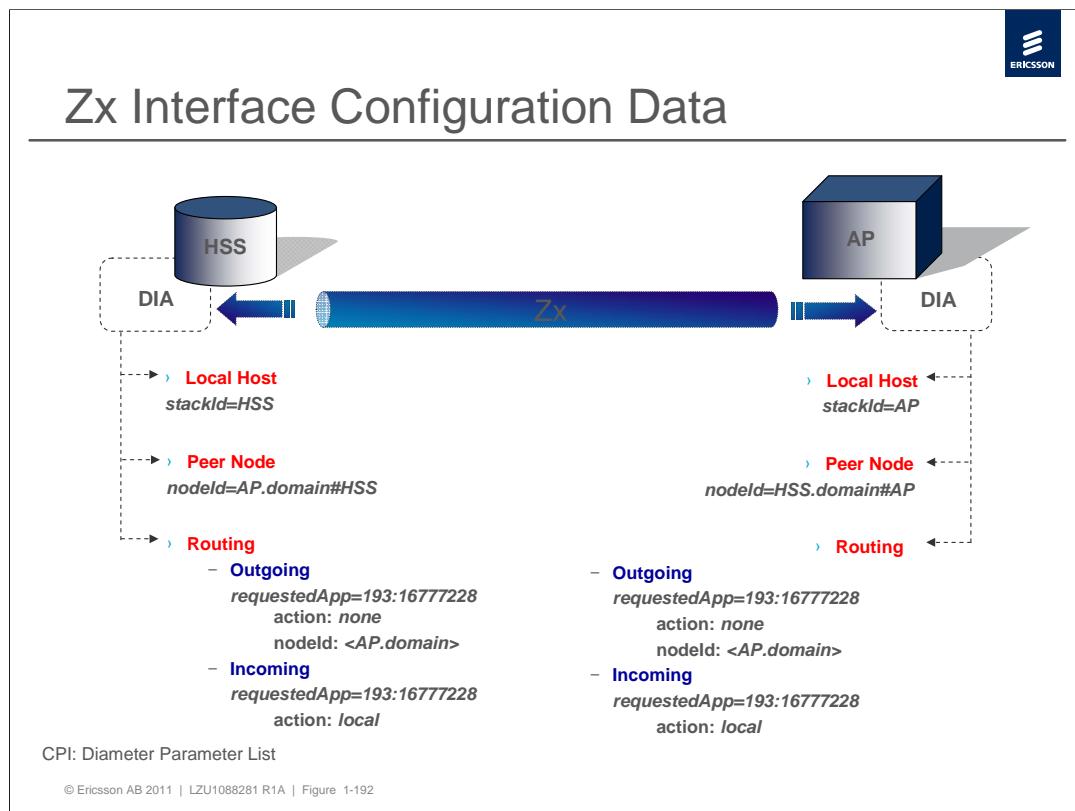
The diagram above shows which parameters must be configured in the Diameter application on the HSS node, in order to enable the Cx interface towards CSCF.

For more details, please refer to CPI document “Diameter Parameter List”



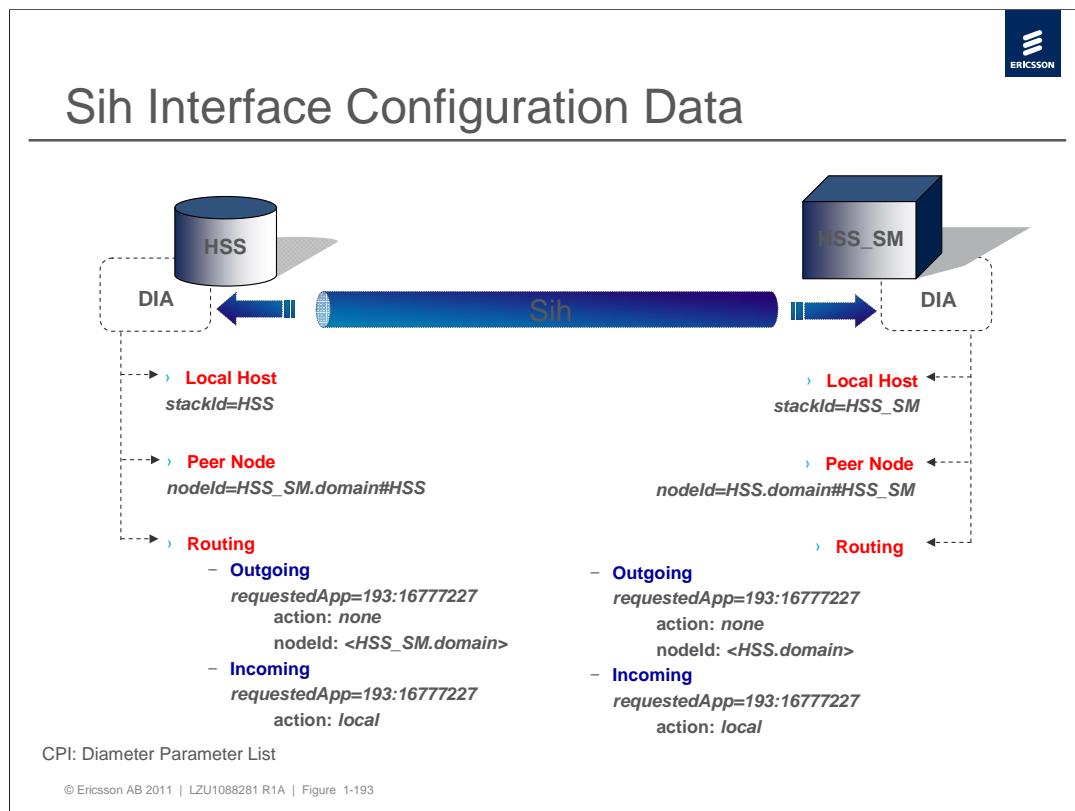
The diagram above shows which parameters must be configured in the Diameter application on the HSS node, in order to enable the Sh interface towards an AS (e.g. MTAS).

For more details, please refer to CPI document “Diameter Parameter List”



The diagram above shows which parameters must be configured in the Diameter application on the HSS node, in order to enable the Zx interface towards an Aggregation Proxy (part of PGM solution).

For more details, please refer to CPI document “Diameter Parameter List”

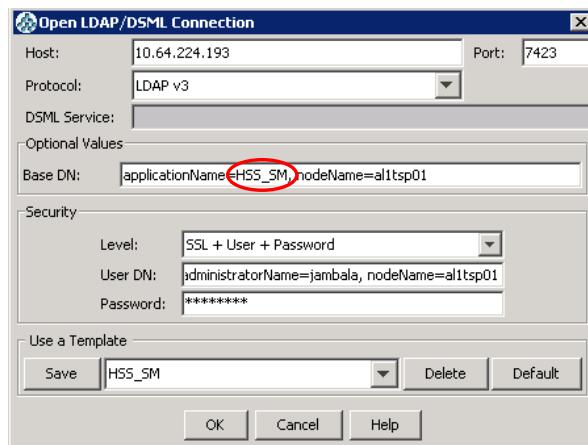


The diagram above shows which parameters must be configured in the Diameter application on the HSS node, in order to enable the Sih interface towards the Session Manager module.

For more details, please refer to CPI document “Diameter Parameter List”



Login to the TSP HSS_SM application



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-194

The Application name for the ISM Session Manager is *HSS_SM*.

ISM Session Manager functionality is required for the mobile access Single Sign-On authentication support.

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view shows a node named 'HSS_SM' under 'applicationName'. On the right, the 'Table Editor' view displays a list of attributes and their values for the 'HSS-SmConfigurationData' object class. Several attributes are highlighted with red boxes: 'HSS-SmAdministrativeState' (Unlocked), 'HSS-SmMassiveSessionRemovalEnabled' (TRUE), 'HSS-SmMassiveSessionRemovalStartTime' (01:00), 'HSS-SmMaxSessionTime' (86400), 'HSS-SmOamLogStatus' (FALSE), 'HSS-SmReattemptDelayTime' (1000), 'HSS-SmSecurityLogStatus' (FALSE), and 'HSS-SmServicesLogStatus' (FALSE). The 'parent' attribute also has a red box around it.

attribute type	value
HSS-SmConfigurationDataName	HSS-SmConfigurationData
objectClass	HSS-SmConfigurationData
groupId	711
HSS-SmAdministrativeState	Unlocked
HSS-SmInstallationType	Monolithic
HSS-SmMassiveSessionRemovalEnabled	TRUE
HSS-SmMassiveSessionRemovalStartTime	01:00
HSS-SmMaxSessionTime	86400
HSS-SmOamLogStatus	FALSE
HSS-SmReattemptDelayTime	1000
HSS-SmSecurityLogStatus	FALSE
HSS-SmServicesLogStatus	FALSE
HSS-SmSgsnMcMncAlarmEnabled	TRUE
ownerId	711
permissions	11
shareTree	nodeName=al1tsp01
parent	

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-195

HSS-SmAdministrativeState - This attribute identifies the state for the SM application. {Locked, Unlocked}

HSS-SmMassiveSessionRemovalEnabled - This attribute indicates if the SM massive session removal function is enabled or not. If enabled the unfinished and invalid sessions are removed from the SM database in a massive operation

HSS-SmMassiveSessionRemovalStartTime - This attribute indicates the time in the day when the SM massive session removal function must start

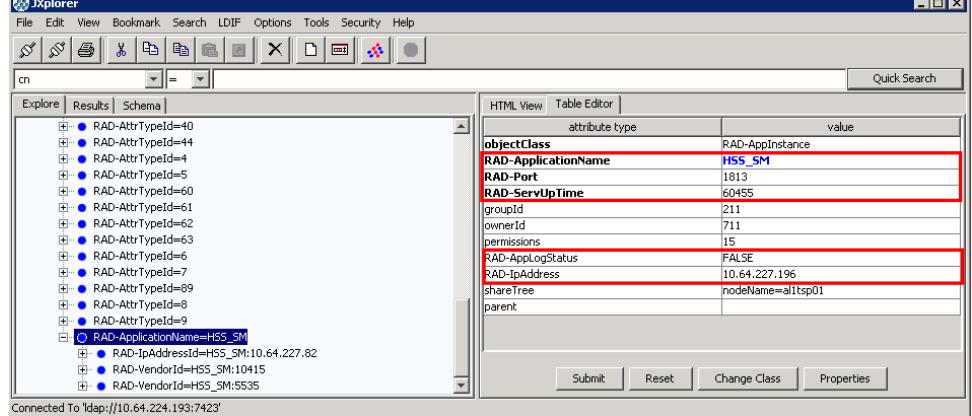
HSS-SmMaxSessionTime - This attribute represents the maximum allowed inactivity period between two consecutive session updates before considering the session as unfinished (but still valid) until the massive removal procedure removes it.

Logs on O&M, Security and Services level can be activated by setting the following attributes to TRUE:

HSS-SmOamLogStatus

HSS-SmSecurityLogStatus

HSS-SmServicesLogStatus



The screenshot shows the JXplorer LDAP browser interface. The left pane displays a tree view of LDAP attributes under the node 'cn'. The right pane shows a table editor for the selected object. The table has columns for 'attribute type' and 'value'. Several attributes are highlighted with red boxes: 'RAD-ApplicationName' (value: HSS_SM), 'RAD-Port' (value: 1813), 'RAD-ServUpTime' (value: 60455), 'RAD-AppLogStatus' (value: FALSE), and 'RAD-IpAddress' (value: 10.64.227.196). At the bottom of the table editor are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

Note: this object is accessible through the RADIUS application!

Connected To 'ldap://10.64.224.193:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-196

The Gi interface between a RADIUS server (i.e. Session Manager) and a RADIUS client (e.g. GGSN) is defined in the RADIUS stack itself. The stack has an LDAP interface, which is accessible through the RADIUS application.

Some of the attributes are explained here:

RAD-ApplicationName - This attribute identifies the name of the application that uses RADIUS.

RAD-Port - UDP Port to receive RADIUS packets.

RAD-ServUpTime - Number of hundred of seconds the application has been running from the moment the node was started.

RAD-AppLogStatus - A flag that states whether RADIUS Log is active or not.

RAD-IpAddress - IP address identifying the RADIUS application instance. Used as "Sender Address" in all transmitted UDP packets. This is the "virtual" IP address at which all RADIUS requests are received. If this attribute is not properly configured, the platform itself assigns the IP address. It is highly recommended to configure this attribute.

The screenshot shows the JXplorer LDAP browser interface. The title bar reads "RADIUS stack – Gi Interface (client)". The left pane is titled "Explore" and shows a tree view of LDAP entries under the "cn" base. The right pane is titled "Table Editor" and displays a table of attributes for a selected object. The table has columns for "attribute type" and "value". The "objectClass" row is highlighted in red. Other rows include "RAD-DuplicatedSpanTime" (value: 30), "RAD-Identifier" (value: GGSN), "RAD-IpAddressId" (value: HSS_SM:10.64.227.82), and "RAD-SharedSecret" (value: 5504ALL). The bottom of the interface shows buttons for "Submit", "Reset", "Change Class", and "Properties". A status message at the bottom left says "Connected To 'ldap://10.64.224.193:7423'".

Note: this object is accessible through the RADIUS application!

The RAD-RadiusClient object class is used to define a RADIUS client entity (e.g. GGSN).

Some of the parameters are explained here:

RAD-IpAddressId - Valid RADIUS client IP address. It is composed by the application name (that should be the same stored in RAD-AppInstance) and the IP Address of the RADIUS client.

RAD-DuplicatedSpanTime - Time in seconds when the application discards duplicated RADIUS Requests messages.

RAD-Identifier - Valid RADIUS client identifier (e.g. GGSN).

RAD-SharedSecret - Shared secret used to validate client identities RADIUS.

Sih Interface (SM side) – Stack Id

attribute type	value
hostId	HSS-SM.edu.mninet.net
objectClass	DIA-CFG-DiameterContainer
portNr	3073
productName	Ericsson Diameter
realm	edu.mninet.net
stackId	HSS_SM
supportedVendorIds	0
supportedVendorIds	10415
supportedVendorIds	10415
allowConnectFromUnknownNode	FALSE
disabled	TRUE
enabled	TRUE
maxInboundStreams	1
maxNumberofRetries	3
maxOutboundStreams	1
maxRequestPendingTime	10
ownerId	0
overflows	63
sendErrorAtOverload	TRUE
shareTree	applicationName=OIA.nodeName=alissip0
supportedMultiAppIds	16777227
supportedVendorSpecificApps	0:193-16777227:0
rtTime	10
transportLayerType	1
watchdogTmeidle	6
power	
scbAddressesList	
supportedVendorIds	

CPI: Diameter Parameter List

In the figure the local host data for the HSS_SM side of Sih interface is shown. Some of the parameters are highlighted.

enabled is a Boolean can be set to FALSE whenever the node should suspend its activity. It may be used instead of clearing all "enabled" parameters for neighbourNodes separately.

allowConnectFromUnknownNode indicates if the stackId is allowed to attend requests from nodes that are not included in the *NeighborNode* objects list. In other words, if connection with dynamically discovered neighbor nodes is allowed or not. From the moment in which an administrator sets this value to FALSE, connection to new dynamically discovered nodes will be rejected, but existing connections with previous dynamic nodes are preserved.

ipAddressesList is a list of IPv4 addresses (string) that makes the own node accessible when using transport protocol TCP. The first address in the list is considered the primary one. This list is checked to find out if any of the IP addresses in the list are repeated, and if so, an LDAP error will be raised, and the operation will not take place. In the figure the address 192.168.8.110 is the address for the HSS where AAA module resides.

portNr is the local listener port number that the remote diameter nodes are using for communication with this node.

loadRegulationEnabled: if set to TRUE, the diameter stack will check the processor load when an incoming request is received. If an overload situation prevails the incoming request will be rejected. Depending on the setting of the attribute *sendErrorAtOverload* an answer with error code DIAMETER_TOOR_BUSY may be sent back to the other node.



Sih Interface (SM side) – Peer Node

The screenshot shows the Ericsson Diameter Manager interface for managing a peer node. The left pane displays the LDAP tree under the 'World' root, showing various containers like 'applicationName=HSS', 'stackContainerId=HSS_CX', etc. The right pane shows the configuration details for a specific peer node entry.

attribute type	value
nodeId	HSS.edu.mninet.net#HSS_S4
objectClass	DUA-Cf-G-NeighbourNode
connId	0-HSS_SMHSS.edu.mninet.net#conn1
stackVendorId	193
enabled	TRUE
transportLayerType	1
ipAddressList	0.10.64.227.196
isDynamic	FALSE
ownerId	0
peerAddress	0
portNr	3672
productName	Ericsson Diameter
realm	edu.mninet.net
sharedSecretName	secretName=OIA,nodeName=a1top01
supportedAuthAppIds	16777216
supportedVendorId	193
supportedVendorIdApp	10415
supportedVendorSpecificApps	0-10415:16777216:0
supportedVendorSpecificApp	1:193:16777220:0
supportedVendorSpecificApps	2-10415:16777217:0
supportedVendorSpecificApp	3:193:16777227:0

CPI: Diameter Parameter List

Connected To ldap://10.64.224.193:7423

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-199

In the figure the destination host (HSS) data is shown. Some of the parameters are highlighted.

enabled is a Boolean flag can be set by the traffic part or the OAM administrator when there is any reason that the Diameter Server does not accept request from this node. It must be set to *TRUE* by default when the Neighbour Node is created.

ipAddressesList is a list of IPv4 addresses (string) that makes the neighbor node accessible when using transport protocol TCP. The first address in the list is considered the primary one. This list is checked to find out if any of the IP addresses in the list are repeated, and if so, an LDAP error will be raised, and the operation will not take place. The *ipAddressesList* consists of address list with an index, which is called the array index.

portNr is a remote port number used for the communication with the Diameter neighbor node.

linkStatus indicates the status of the connection. Possible values: *initial*, *up*, *down*, *suspect* and *reopen*.

transportLayerType - defines the transport layer to be used when setting up a connection to this node. Possible values: 0 = Not defined (creation value), 1 = TCP, 2 = SCTP and 3 = First SCTP, then TCP.

supportedAuthAppIds – This attribute is a list of applications that supports Authentication or Authorization requests. The Authentication Application ID defined by 3GPP for the Cx interface is 16777227.



Sih Interface (SM side) – Connection Id

The screenshot shows a LDAP browser interface displaying connection information for the HSS side of the HSS_SM - HSS interface. The connection entry is highlighted with a red circle around the 'nodeName=al1sp01' node in the tree view.

attribute type	value
connId	HSS_SM@HSS.edu.mmtel.net#conn1
objectClass	DiameterConn
blockReason	Not blocked
connectedAddress	10.64.227.196
peerId	TRUE
port	0
mountId	n
linkStatus	Up
wireId	0
permissions	9
shareTree	applicationName=DIA,nodeName=al1sp01
transportLayerType	1
ipAddressList	
parent	
sctpAddressesList	

CPI: Diameter Parameter List

Connected To ldap://10.64.227.193:7423

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-200

In the figure the remote host data for the HSS side, of the HSS_SM - HSS interface, is shown. Some of the parameters are highlighted.

blockReason - This attribute contains information if the connection is blocked for any reason.

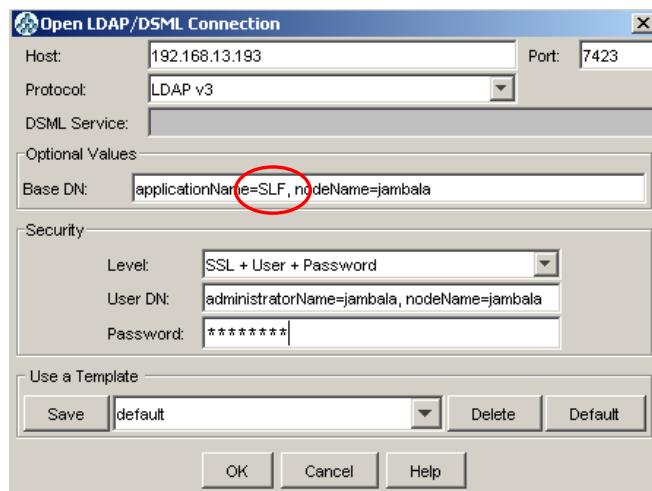
enabled – This parameter enables or disables the connection (TRUE = enabled; FALSE = disabled)

linkStatus - indicates the status of the connection. Values: *initial*, *up*, *down*, *suspect* and *reopen*

transportLayerType - defines the transport layer to be used when setting up a connection to this node. Values: 0 = *Not defined (creation value)*, 1 = *TCP*, 2 = *SCTP* and 3 = *First SCTP, then TCP*.



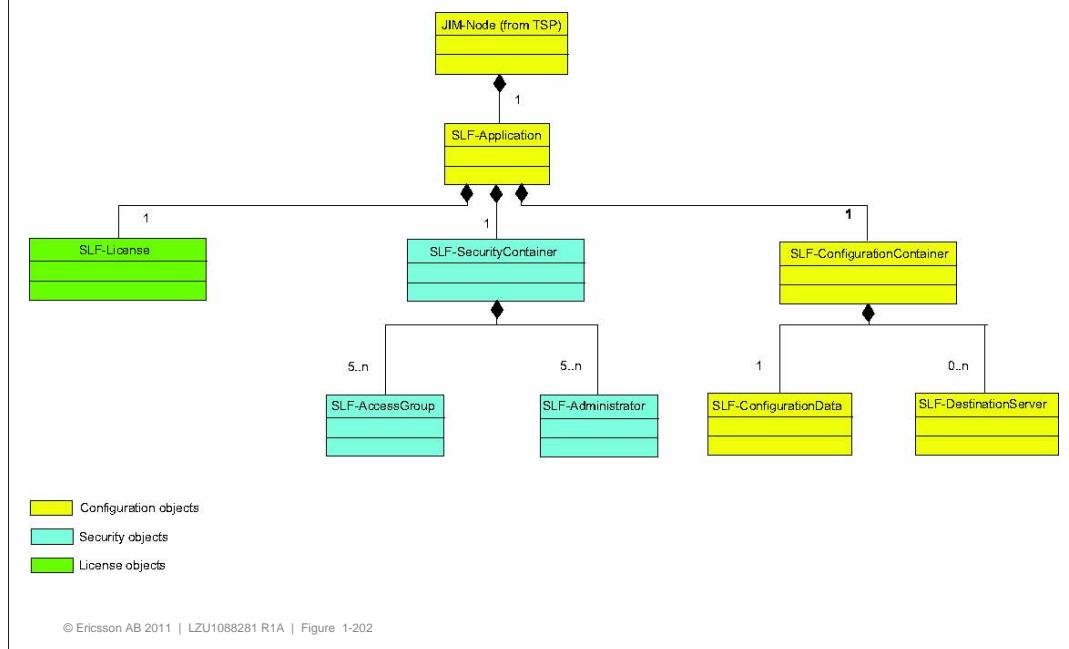
Login to the TSP SLF application



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-201

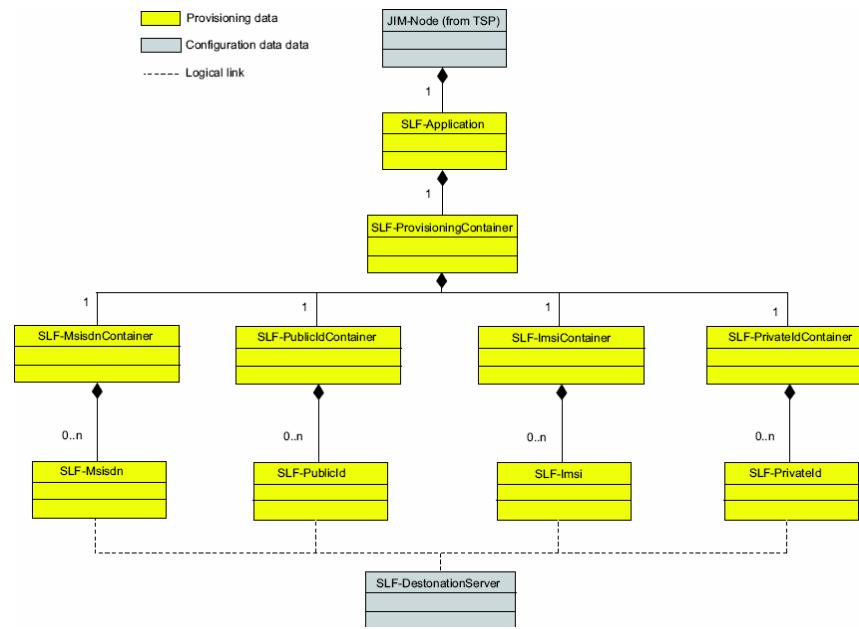
The Application name for the SLF application is *SLF*.

SLF Configuration Object Class Model



This picture presents SLF Configuration Object Class Model.

SLF Provisioning Object Class Model



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-203

This picture presents SLF Provisioning Object Class Model.



SLF Liscence Container

The screenshot shows the JXplorer LDAP browser interface. The left pane displays a tree view of an LDAP entry under 'cn' with the node name 'al1tsp01'. One of the child entries is 'SLF-LicenseName=SLF-License', which is selected and highlighted in blue. The right pane contains a table editor for this entry, showing attributes like 'objectClass', 'SLF-BasicActivationEnabled' (value: TRUE), 'SLF-DBManagerEnabled' (value: TRUE), and 'SLF-LicenseName' (value: SLF-LICENSE). Other attributes listed include 'SLF-DiameterProxyEnabled', 'SLF-DiameterRedirectEnabled', 'SLF-LoadbalancerEnabled', 'SLF-RadiusProxyEnabled', 'groupID', 'ownerID', 'permissions', 'shareTree', and 'parent'. At the bottom of the table editor are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A status bar at the bottom of the browser window indicates a connection to 'ldap://10.64.224.193:7323'.

The availability status of the lisences determines configuration of SLF. The following lisences can be activated:

SLF-BasicActivationEnabled states whether the SLF module is enabled.

SLF-DBManagerEnabled enables the DB Manager subscription mode feature.

SLF-DiameterProxyEnabled enables the Diameter Proxy routing mode feature.

SLF-DiameterRedirectEnabled enables the Diameter Redirect routing mode feature.

SLF-LoadbalancerEnabled enables the Load Balancer subscription mode feature.

SLF-RadiusProxyEnabled enables the Radius Proxy routing mode feature.

SLF Configuration Parameters (DB Manager)

JXplorer interface showing SLF Configuration Parameters:

Left Panel (Tree View):

- World
 - nodeName=jambala
 - applicationName=SLF
 - SLF-ConfigurationContainerName=SLF-ConfigurationContainer
 - SLF-DestinationServerName=10.10.10.10
 - SLF-DestinationServerName=192.168.7.101
 - SLF-DestinationServerName=Fanste
 - SLF-DestinationServerName=hss1
 - SLF-DestinationServerName=hss5
 - SLF-ConfigurationDataName=SLF-ConfigurationData
 - SLF-ProvisioningContainerName=SLF-ProvisioningContainer
 - SLF-SecurityContainerName=SLF-SecurityContainer

Right Panel (Table Editor):

attribute type	value
objectClass	SLF-ConfigurationData
SLF-AdministrativeState	Unlocked
SLF-ConfigurationDataName	SLF-ConfigurationData
SLF-DiameterLogStatus	TRUE
SLF-OAMLogStatus	TRUE
SLF-PerfEndsScheduleTime	20080827T142047616
SLF-PerfInitialScheduleTime	20080827T142047616
SLF-PerfScheduleActive	FALSE
SLF-PerfStartStop	FALSE
SLF-RealmRoutingEnabled	TRUE
SLF-RedirectMaxCacheTime	0
SLF-SecurityLogStatus	TRUE
groupId	412
ownerId	411
permissions	15
shareTree	nodeName=jambala
parent	

Buttons at the bottom: Submit, Reset, Change Class, Properties.

Connected To 'ldap://192.168.13.195:7323'

CPI: SLF LDAP Interface Description

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-205

The figure above shows the configuration parameters for SLF which is lisenced as DB Manager.

SLF-AdministrativeState defines the state for the SLF application. Possible values: Lock, Unlocked.

SLF-DiameterLogStatus is a flag that states whether Diameter Log (related to Diameter traffic messages) is active or not.

SLF-OAMLogStatus is a flag that states whether OAM Log (related to Operation and Maintenance Information) is active or not.

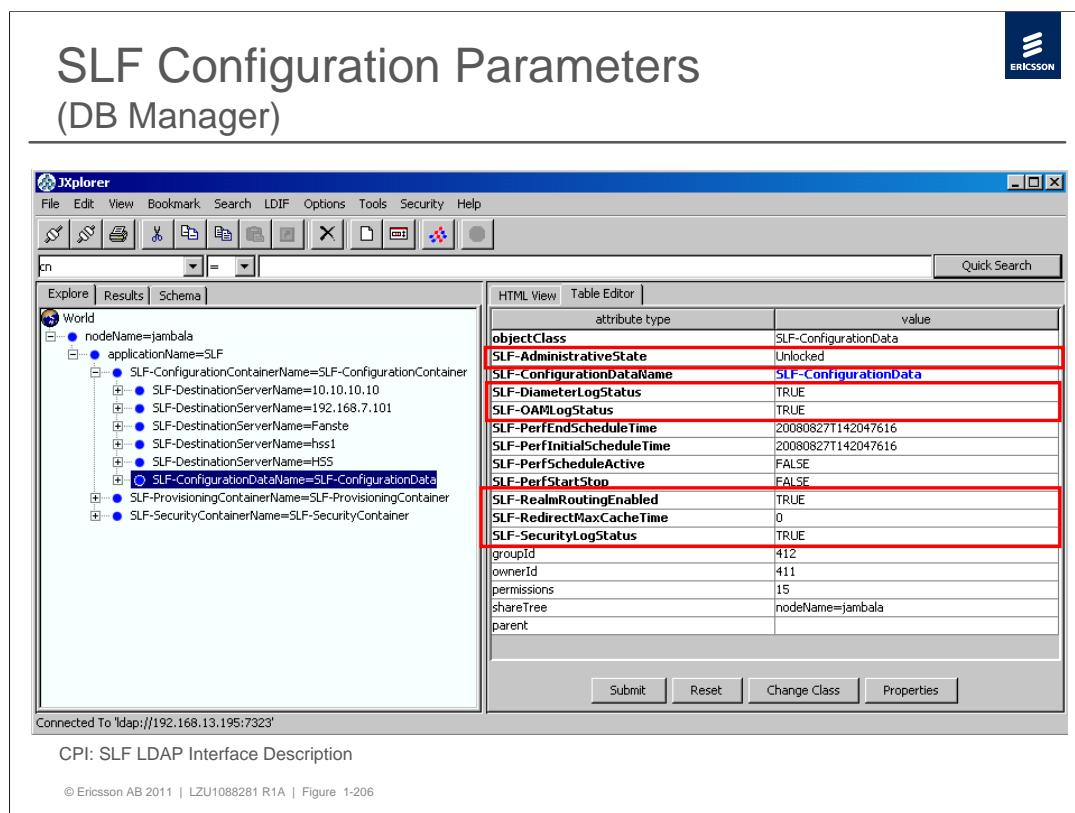
SLF-SecurityLogStatus is a flag that states whether Security Log (related to security events) is active or not.

SLF-RealmRoutingEnabled states if routing by realm is enabled.

SLF-RedirectMaxCacheTime defines the maximum number of seconds the peer and route tables are cached.

When SLF is lisenced as a Load Balancer the following parameters become visible:

SLF-LoadBalancingMethod defines the algorithm used when doing load balancing. If Basic is configured the *SLF-DestinationCapacity* is used to calculate message routing probabilities. If HSS-Load is configured the *SLF-DestinationCapacity* and the load information retrieved using the *SLF-SystemInfoDiameterIdentity* is used to calculate message routing probabilities.



SLF-SystemInfoPollInterval is an interval in seconds between the occasions when the SLF is polling load information from the destination. This attribute is only and only applicable if the parameter *SLF-LoadBalancingMethod* is set to *HSS-Load*. This attribute is also visible if the SLF is licensed to use the DB Manager subscription mode with RADIUS Proxy feature.

SLF-AvailabilityPollInterval is an interval in seconds between the occasions when the load balancing subsystem is polling and updates the availability information for the destinations. This attribute is only visible and applicable if the SLF is licensed to use the Load Balancer subscription mode feature.

SLF-HssLogicalName is used by the SLF when licensed as Load Balancer.

Connected To 'ldap://192.168.13.195:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-207

CPI: SLF LDAP Interface Description

SLF-DestinationServerName is a primary key used to identify the destination server. This is the name to be used for reference in the list of servers related for an identity.

SLF-DiameterIdentity contains the server's Diameter Identity.

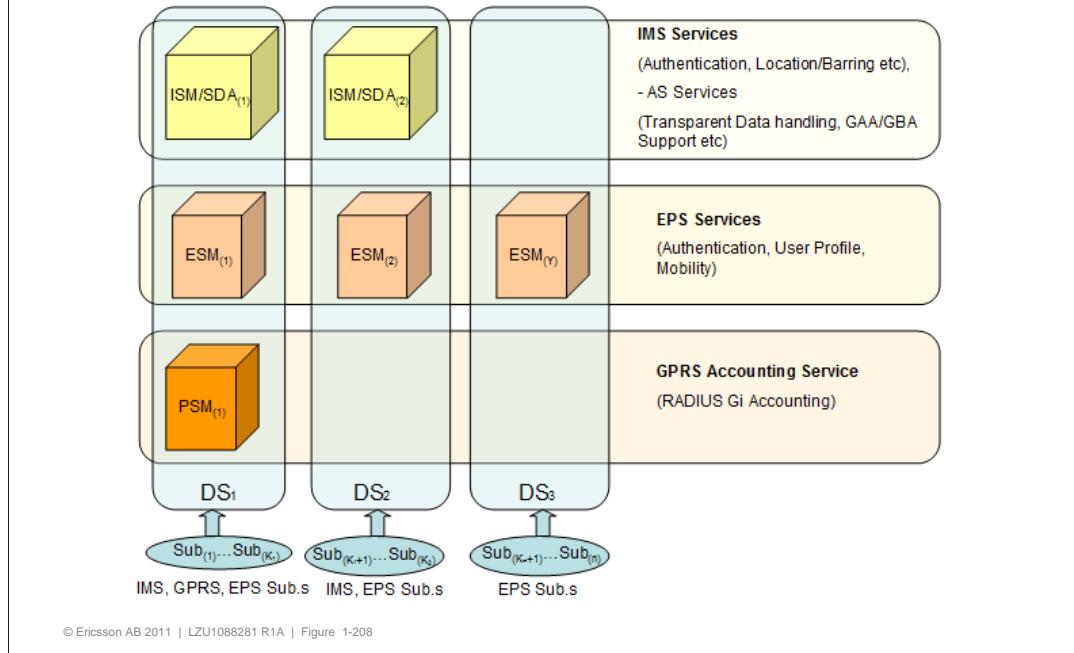
When SLF is licenced as a Load Balancer the following parameters become visible:

SLF-DestinationCapacity is a capacity of a destination. The value is used as a weight in the load balancing algorithm. The attribute has an arbitrary type, and the configured capacity for this destination is weighted against the configured capacity of all other destinations. The parameter is expressing a relation in capacity between the HSSs, not an absolute capacity in a number of subscribers. An example: HSS A: Capacity of 12M subscribers, HSS B: Capacity of 6M subscribers, and HSS C: Capacity of 4M subscribers. This would in SLF be expressed as the following setting of parameter *SLF-DestinationCapacity* in each destination server object: HSS A: 12, HSS B: 6, and HSS C: 4. This could also be expressed as: HSS A: 6, HSS B: 3, and HSS C: 2. These two are the same since it is the relation between the HSS capacities that is important. A 0 value means that this destination will not be selected.

SLF-SystemInfoDiameterIdentity contains the destination server's address, as a Diameter Identity, to the HSI (HSS System Information) Software component.



Domain Distributed Location (DB Manager)



This feature enables operators to deploy different HSS/SLF pool of servers addressing specific domain such as IMS or EPC set of HSS servers and to separate the business deployment scenario where the HSS serving EPC network are isolated from the HSS serving IMS network.

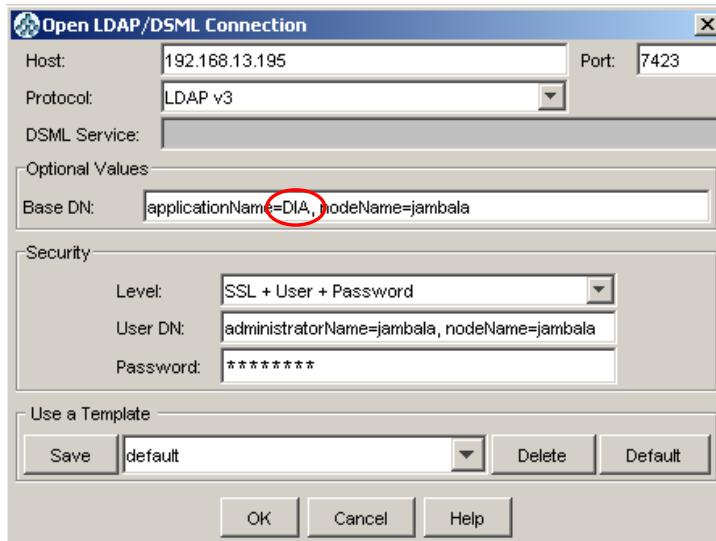
In SLF it is possible to configure a mapping between a set of subscribers' related identities (including all subscribers' Public, Private and MSISDN's used for various IMS services, and IMSI's used for IMS GAA/GBA, for GPRS and for EPS services) to a defined set of non-co-located HSS entities, each one servicing a specific domain, where by domain is intended IMS domain, GPRS access domain and EPS domain. The figure above shows a possible provisioning scenario, where different sets of subscribers are serviced by different HSS nodes.

SLF-ImsiValidForModules attribute (SLF-Imsi object class) specifies for which HSS modules the SLF is allowed to use this provisioned IMSI as routing key. This attribute is cumulative and specifies the set of HSS modules which are allowed to be located by this IMSI and to which traffic for this subscriber is to be sent. The allowed HSS modules are given as an unordered list of module names separated by a comma or as an indication that any module is allowed. HSS modules for which the IMSI is a valid routing key type and to which the traffic for this subscriber is to be sent when specified:

- "ESM": The IMSI is allowed to be used to locate the ESM instance.
- "SDA": The IMSI is allowed to be used to locate the SDA instance.
- "SM": The IMSI is allowed to be used to locate the SM instance.
- "ALL": The IMSI can be used to locate any HSS module for which the IMSI is a valid routing key type.



Login to the Diameter application (SLF)



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-209



Dx Interface data – Stack Id

The screenshot shows the JXplorer LDAP browser interface. The left pane displays the LDAP tree structure under 'cn' with nodes like 'nodeName=jambala' and 'applicationName=DIA'. The right pane shows a table editor for the 'DIA-CFG-OwnNodeConfig' object class. Several parameters are highlighted with red boxes:

attribute type	value
hostId	SLF.eduims.se
objectClass	DIA-CFG-OwnNodeConfig
portNr	3868
productName	Ericsson Diameter
realm	eduims.se
stackId	SLF
supportedVendorIds	10415
supportedVendorIds	193
supportedVendorIds	0
allowConnectFromUnknownNode	TRUE
diaVendorId	10415
enabled	TRUE
firmwareRevision	1
groupid	0
ipAddressesList	0.192.168.7.104
loadRegulationEnabled	TRUE
maxInboundSctpStreams	1
maxNumberOfRetries	3
maxOutboundSctpStreams	1
maxRequestPendingTime	5
ownerId	0
permissions	63
sendErrorOnOverload	TRUE
shareTree	applicationName=DIA,nodeName=jambala
supportedAuthAppIds	16777216
supportedVendorSpecificApps	0:10415:16777216.0
supportedVendorSpecificApps	1:10415:16777217.0
supportedVendorSpecificApps	2:193:16777228.0
tC Timer	10
transportLayerType	1

Connected To 'ldap://192.168.13.195:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-210

CPI: Diameter Parameter List

In the figure the local host data for the SLF side of the Dx interface is shown.

Some of the parameters are highlighted.

PortNr - This is the local listener port number that the remote diameter nodes are using for communication with this node.

enabled - This boolean can be set to FALSE whenever the node should suspend its activity. It may be used instead of clearing all "enabled" parameters for neighbourNodes separately.

ipAddressesList – It is a list of IPv4 addresses (string) that makes the own node accessible when using transport protocol TCP. The first address in the list is considered the primary one. This list is checked to find out if any of the IP addresses in the list are repeated, and if so, an LDAP error will be raised, and the operation will not take place.

supportedAuthAppIds – This attribute is a list of applications that supports Authentication or Authorization requests. The Authentication Application ID defined by 3GPP for the Dx interface is 16777216.

transportLayerType defines the transport layer to be used when setting up a connection to this node. Values: 0 = Not defined (creation value), 1 = TCP, 2 = SCTP and 3 = First SCTP, then TCP.

The following Diameter vendor IDs are defined in the figure.

0 : IETF defined base Diameter Protocol

10415: 3GPP defined Diameter Extensions

193: Ericsson defined Diameter Extensions

Dx Interface data – Peer Node

JXplorer interface showing the configuration of a Peer Node (Diameter Neighbour) in the HSS/SLF 11A system.

The left pane shows the LDAP tree structure under the 'cn' root, with the node 'nodeName=jambala' selected. The right pane displays the 'Table Editor' for the selected node, listing various attributes and their values. Some attributes are highlighted with red boxes:

attribute type	value
nodeId	CSCFCX.edu ims.se#SLF
objectClass	DIA-CFG-NeighbourNode
connIds	0:SLF#CSCFCX.edu ims.se#conn1
diaVendorId	10415
enabled	TRUE
firmwareRevision	1
groupid	100
initiateConnection	FALSE
ipAddressesList	0.192.168.7.99
isDynamic	FALSE
linkStatus	Up
ownerId	100
permissions	9
portNr	3969
productName	Ericsson Diameter
realm	edu ims se
shareTree	applicationName=DIA nodeName=jambala
supportedAuthAppIds	16777216
supportedVendorIds	0
supportedVendorIds	10415
supportedVendorSpecificApps	0:10415:16777216:0
supportedVendorSpecificApps	1:10415:0:16777216
supportedVendorSpecificApps	2:0:16777216:0
supportedVendorSpecificApps	3:0:0:16777216
supportedVendorSpecificApps	4:10415:16777217:0
supportedVendorSpecificApps	5:193:16777217:0
supportedVendorSpecificApps	6:193:16777228:0
transportLayerType	1
parent	
sctpAddressesList	

Connected To ldap://192.168.13.195:7423
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-211

CPI: Diameter Parameter List

In the figure the Dx Interface Peer Node (CSCF) data is shown.

Some of the parameters are highlighted.

connIds - is a list of those connIds that uses this diaNeighbourNodeId.

enabled - This Boolean flag can be set by the traffic part or the OAM administrator when there is any reason that the Diameter Server does not accept request from this node. It must be set to *TRUE* by default when the Neighbor Node is created.

ipAddressessList – It is a list of IPv4 addresses that makes the neighbor node accessible when using transport protocol TCP. The first address in the list is considered the primary one.

portNr – is the remote port number used for the communication with the Diameter Peer node.

supportedAuthAppIds – This attribute is a list of applications that supports Authentication or Authorization requests. The Authentication Application ID defined by 3GPP for the Dx interface is 16777216.

transportLayerType - defines the transport layer to be used when setting up a connection to this node. Values: 0 = *Not defined (creation value)*, 1 = *TCP*, 2 = *SCTP* and 3 = *First SCTP, then TCP*.

The following Diameter vendor IDs are commonly found:

0:IETF, 10415:3GPP, 13019:ETSI, 193:Ericsson

attribute type	value
action	3
objectClass	DIA-CFG-AppRouting
requestedApp	1041516777216
groupd	0
nodeIds	0
ownerId	0
permissions	9
shareTree	applicationName=DIA,nodeName=jambala
parent	

In the figure the Dx Routing Data for the SLF side is shown.

Some of the parameters are highlighted.

entryId - This attribute represents an entry in the Realm Routing Table (RRT). The RRT is realm based, and for a certain realm and a given *stackId*, there may be at most two RRTs, depending on the need of an application to process incoming traffic and generate outgoing messages. The *entryId* consists of the parts which are *realm*, *stackId* and *isIncomingRequest*. The *isIncomingRequest* field in the *entryId* attribute is *true* for routing incoming requests, and *false* for outgoing requests.

action - The routing action from requests for a certain realm and a given request type that belongs to the Diameter application specified in the *requestedApp* attribute.

Values: 0 – local, 1 – relay, 2 – proxy, 3 – redirect, 4 – none, 5 – other.

All actions except none (4) are valid when the *isIncomingRequest* is set to *TRUE*.

requestedApp - This attribute is the vendor's Diameter application whose messages are recognized by the RRT.

nodeIds - One or more servers that the message is to be routed to. If *action=none*, these servers must be defined as Neighbour Nodes. If *action=redirect*, these servers can be any defined node. This list cannot be left empty if *action=redirect*, or *action=none*. For remaining actions, this list must be empty.



Chapter 6 – Performance Management

1. Introduction
2. Architecture
3. User Interface
4. Fault Management
5. Configuration Management
- 6. Performance Management**
7. Security, Authentication and Redundancy
8. Session Establishment
9. Configuration Examples

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-213





CSCF HSS SLF Performance Monitoring

- › Uses the TSP Common Framework for collection, starting and stopping of statistical counters
- › The counters are stored on a 3GPP compliant XML file (configurable output format – DTD or XSD)
- › FTP is used to transfer the XML file to external management systems (i.e. Analyzer) where reports are created

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-214

CSCF, HSS and SLF (all based on the TSP platform) use a common framework for the collection measurements. The measurements are stored in 3GPP Performance Management compliant XML files for transfer to external systems (FTP interface). Performance management attributes can be modified with the CM Browser.

The Performance Management data is used by Sub-network Managers to build performance reports, and is used by the network administrator to assess the performance level of the managed element / sub-network. Some examples of such reports are: SIP Traffic Summary Report, Traffic Hourly Report, SIP characteristics Report in CSCF; number of Cx-Query requests received from a certain peer, number of subscribers currently stored in the ISM and so on.

The element manager does not build any performance report, these reports are generated by the Sub-Network Manager, i.e. the Ericsson Analyzer product.

Configurable parameters include a scan period for measurement values. At the end of the scan period the data is logged as an XML file using the Network File System (NFS).

DTD -> Document Type Declaration

XDS -> XML Schema Definition



Measurement Types

- › Counters – used to report cumulative, incremental integer variables
- › Gauges – represents a dynamic variable that may change in either direction
- › Status Inspections - is a mechanism for high frequency sampling of internal counters at pre-defined rates
- › Discrete Event Registration – is a measurement of a specified event where every Nth event is to be taken into account.

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-215

The operator can define thresholds for four types of measures:

Counter is a measurement type that is used to report cumulative, incremental integer variables. An occurrence of an event increments a counter.

Gauge represents a dynamic variable that may change in either direction. A gauge is real valued. Within a granularity period, a gauge maintains and can represent the minimum value, the maximum value or the mean (average) value of that period. The type of the gauge [min/max/mean] can be configured during design phase only (scan configuration file).

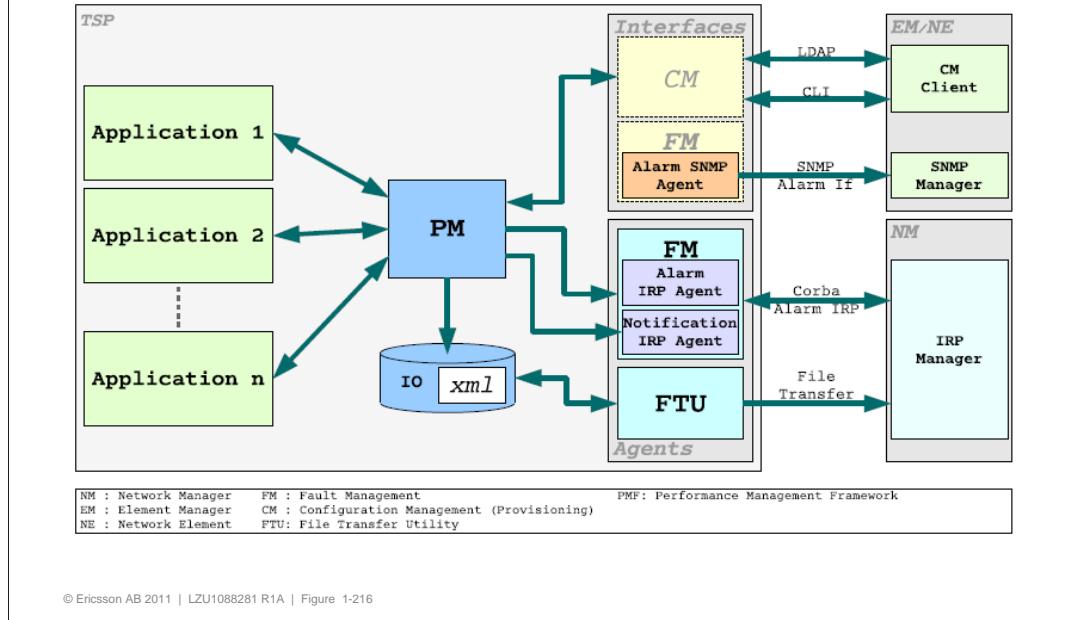
Status Inspection is a mechanism for high frequency sampling of internal counters at pre-defined rates.

Discrete Event Registration – is a measurement of a specified event where every Nth event is to be taken into account.

A threshold is the value at which an alarm is armed or disarmed due to the threshold crossing of the collected data.

Granularity Period The time between the initiations of two successive gatherings of measurement data

Performance Management Interfaces



The figure above presents the relation between PM and the other O&M (CM, FM) components of the TSP based system. The provided external interfaces are also highlighted in the figure.

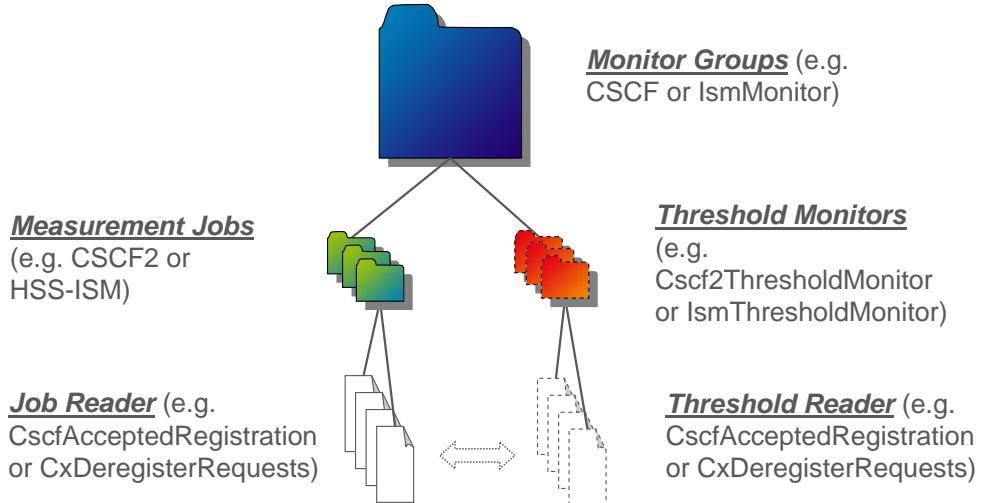
There are two independent implementations of Performance Management in TSP: the legacy PM (oPM) and the new PM (nPM). However, CSCF and HSS applications use the nPM (oPM might still be in use for platform-related measurement).

Applications play the role of the Measurement Provider; they provide measurement data for PM. Measurement data is stored, collected and aggregated on system level and in the end, the results are stored in XML report files. The system administrator can configure the various managed objects through the CM interface (through LDAP and CLI).

According to the configuration, PM can generate threshold based alarms and notifications. The report files can be transferred out of the system through the File Transfer Utility.



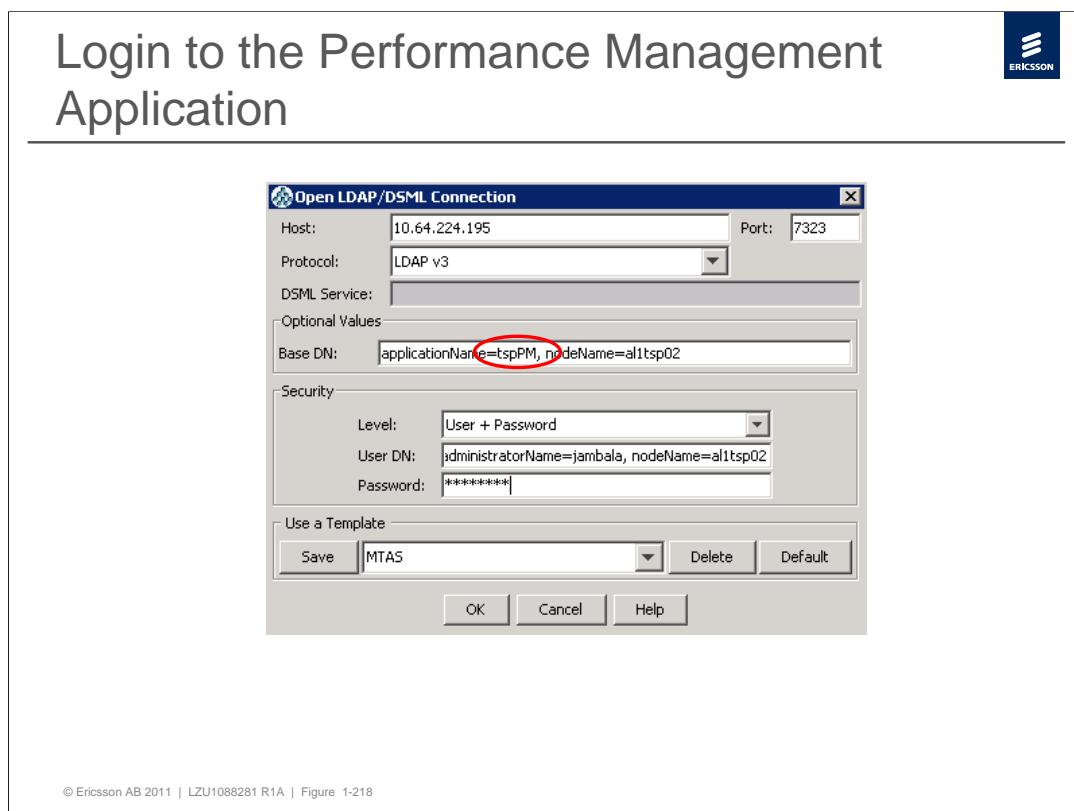
PM Framework Concepts



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-217

A PM monitor (or monitor for short) can be seen as a kind of collection of some measurement type related tasks.

Monitors are divided into Groups. Each group contains Measurement Jobs (where Granularity Period, Monitor Priority, Reporting Format, etc can be configured). A Measurement Job can include several Job Readers (simply speaking a Counter). It is possible to associate an alarm to a specific event, for example the Operator wants an alarm to be raised when [x] number of unsuccessful registration have been recorded. Any of these events must be associated with a Counter (i.e. with a Job Reader). The configuration of such an alarm is done by creating, configuring and enabling a Threshold Reader with the same name of the Job Reader. A Threshold Monitor is only used for switching ON/OFF a group of Threshold Readers and to specify a Granularity Period.



The Application name for the Performance Management is *tspPM* (the new TSP Performance Management framework).

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view displays a hierarchy under 'cn' with various application names like 'applicationName=tData', 'applicationName=tDNS', etc., and a specific entry for 'applicationName=tspPM'. Under 'tspPM', there are several sub-entries starting with 'tspPmMjName=' followed by names such as 'Cscf2ThresholdMonitor', 'Cscf2', 'CscfSipClient', 'CscfSipServer', 'CscfThresholdMonitor', and 'Cscf'. On the right, the 'Table Editor' pane shows the attributes for the 'tspPM' entry. The 'tspPmEnable' attribute is listed with a value of 'TRUE' and is highlighted with a red box. Other attributes shown include 'objectClass', 'groupID', 'ownerID', 'permissions', 'shareTree', 'tspPmMaxAlarmPerMeasType', 'tspPmMaxMeasReaderNr', 'tspPmMaxMonitorNr', 'tspPmMaxPmdbCpuLoad', 'tspPmMaxPmdbMemorySize', 'tspPmMeasReaderNr', 'tspPmMonitorNr', 'tspPmReportingRootDirectory', 'tspPmTimeZone', and 'parent'. At the bottom of the editor are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

CPI: Performance Management User Guide

Connected To 'ldap://10.64.224.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-219

PM Monitor - Cscf.

A PM Monitor is a generic definition in order to define on abstract level the tasks specific to a measurement job. A PM monitor can be seen as a kind of collection of some measurement type related tasks which bound together dynamically.

A task in PM is called a measurement job. It collects accumulated performance measurement result data, analyzes the collected data and assembles XML report files based on the analysis.

tspPmEnable Specifies whether the whole nPM (new PM framework) functionality is enabled or disabled.

Measurement Jobs

The screenshot shows the JXplorer LDAP browser interface. On the left, there is a tree view of LDAP entries under the 'cn' root. One entry for 'tspPmMjName=Cscf' is expanded, showing various sub-entries like 'tspPmTnName' for different monitoring types. On the right, there is a 'Table Editor' tab where specific attributes of the selected entry are listed. The 'tspPmMjName' attribute has a value of 'Cscf'. Other attributes shown include 'tspPmMjGranularityPeriod' (3600), 'tspPmMjMonitorEnabled' (TRUE), 'tspPmMjMonitorNotifyMoEvents' (FALSE), 'tspPmMjMonitorPriority' (4), 'tspPmMjNotifyFileReady' (FALSE), 'tspPmMjReportingDirectory' (Cscf), and 'tspPmMjReportingFormat' (DTD). A red box highlights the 'tspPmMjGranularityPeriod' and 'tspPmMjMonitorEnabled' rows.

attribute type	value
tspPmMjName	Cscf
tspPmMjGranularityPeriod	3600
tspPmMjMonitorEnabled	TRUE
tspPmMjMonitorNotifyMoEvents	FALSE
tspPmMjMonitorPriority	4
tspPmMjNotifyFileReady	FALSE
tspPmMjReportingDirectory	Cscf
tspPmMjReportingFormat	DTD
parent	

Connected To 'ldap://10.64.224.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-220

CP: Performance Management User Guide

tspPmMjName specifies the name of the measurement job.

tspPmMjGranularityPeriod defines a granularity period expressed in seconds. This is the time between the initiations of two successive gatherings of measurement data.

tspPmMjMonitorEnabled specifies whether this measurement job is enabled or disabled.

tspPmMjMonitorNotifyMoEvents specifies whether a notification is to be sent when this monitor is suspended or resumed. This type of notification is not currently implemented.

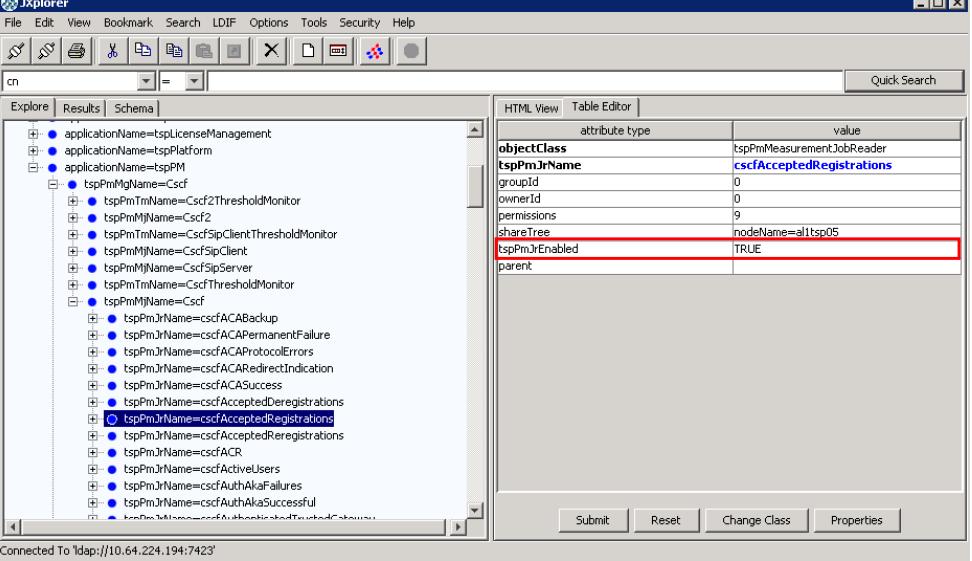
tspPmMjMonitorPriority defines a priority level of this monitor. The lower the value, the higher the priority level. The monitors with the lowest priority will be suspended first in overload situations.

tspPmMjNotifyFileReady specifies whether a notification is to be sent whenever a report file is generated for this measurement job.

tspPmMjReportingDirectory specifies the directory location of the report files generated for this measurement job, relative to the root directory specified by the *tspPmReportingRootDirectory* in *tspPmApplication*.

tspPmMjReportingFormat defines the reporting format to be used in the resulting XML report files.

Job Readers



The screenshot shows the JXplorer LDAP browser interface. In the left pane, under the 'Explore' tab, there is a tree view of LDAP entries. One entry under 'tspPmJrName' is expanded, showing various measurement type names like 'Cscf2ThresholdMonitor', 'Cscf2sipClientThresholdMonitor', etc. In the right pane, the 'Table Editor' tab is selected, displaying a table of attributes for the current object. The 'tspPmJrName' row is visible, with its value 'cscfAcceptedRegistrations' highlighted in blue. The 'tspPmJrEnabled' row is also visible, with its value 'TRUE' highlighted in red. A vertical sidebar on the right is labeled 'CPI: Performance Management User Guide'.

The measurement reader managed object class to be used with Measurement Jobs is *tspPmMeasurementJobReader*. Instances of this class represent the measurement type to be monitored in the measurement job this MO instance is connected to.

The relation between this measurement reader and the measurement type is defined by the names: *tspPmJrName* shall be the same string as the name of the measurement type to be monitored.

When a measurement reader is disabled or deleted, the PM monitor will continue to collect the measurement data for that measurement type until the end of the current granularity period.

tspPmJrEnabled specifies whether the reader is enabled or disabled. The effect of changing this attribute is not immediate: it will be effective only after the end of the current granularity period.



Threshold Monitors

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn

Explore Results Schema |

HTML View Table Editor |

attribute type	value
objectClass	tspPmThresholdMonitor
tspPmTmName	CscfThresholdMonitor
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=al1tsp05
tspPmTmGranularityPeriod	3600
tspPmTmMonitorEnabled	TRUE
parent	

Submit | Reset | Change Class | Properties |

Connected To 'ldap://10.64.224.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-222

CPI: Performance Management User Guide

A Threshold Monitor is a task in PM. It supervises and evaluates accumulated performance measurement result data and checks them against the defined alarm threshold(s). It generates performance alarms when necessary. Threshold values can be defined for any available performance measurement type.

tspPmTmMonitorEnabled Specifies whether this threshold monitor is enabled or disabled.

tspPmTmGranularityPeriod is the period, expressed in seconds, between the initiations of two successive checks of threshold crossing. The effect of changing this attribute is not immediate: it is effective only after the end of the current granularity period.



Threshold Readers

CPI: Performance Management User Guide

A threshold reader represents the measurement type to be monitored in the PM monitor that is connected to.

The relation between the reader and the measurement type is defined by the names. *tspPmJrName* in measurement readers and *tspPmTrName* in threshold readers must be the same string as the name of the measurement type to be monitored.

tspPmTrEnabled Specifies whether the reader is enabled or disabled.

tspPmTr[Critical/Major/Minor/Warning]Level Defines the arm and disarm level of the alarm with critical/major/minor/warning perceived severity in the following format: "arm_level disarm_level" (two float values separated by white space). The disarm level may be omitted (no hysteresis). The empty string means that no critical/major/minor/warning alarm is issued for this threshold reader.

tspPmTrFaultId Specifies the Fault Id field of the alarm to be sent.

tspPmTrAlarmDirection Defines the Alarm Direction for this reader [*Up;Down*]

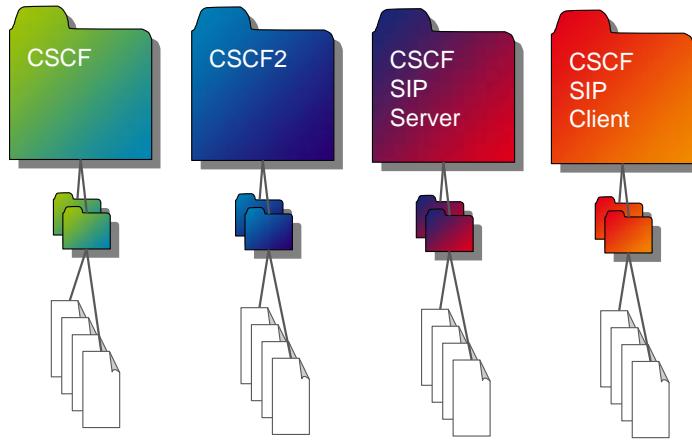
tspPmTrMode Specifies the alarm trigger event [*Crossed;Reached*]

tspPmTrAlarmSpecificProblem Specifies the Specific Problem (Probable Cause in Alarm Viewer) field of the alarm to be sent, which is identical to the alarm slogan.

tspPmTrAlarmProbableCause Specifies the Probable Cause (IRP Cause in Alarm Viewer) field of the alarm to be sent.



CSCF Measures



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-224

The counters for the CSCF have been divided into 4 groups.

The main groups are:

- Counters for CSCF (CSCF and CSCF2)
- Counters for CscfSipServer
- Counters for CscfSipClient



CSCF Measures – Location of XML files

- › Default IMS file directory IO location:

```
/opt/telorb/axe/tsp/NM/PMF/reporterLogs/Cscf  
/opt/telorb/axe/tsp/NM/PMF/reporterLogs/Cscf2  
/opt/telorb/axe/tsp/NM/PMF/reporterLogs/CscfSipServer  
/opt/telorb/axe/tsp/NM/PMF/reporterLogs/CscfSipClient
```

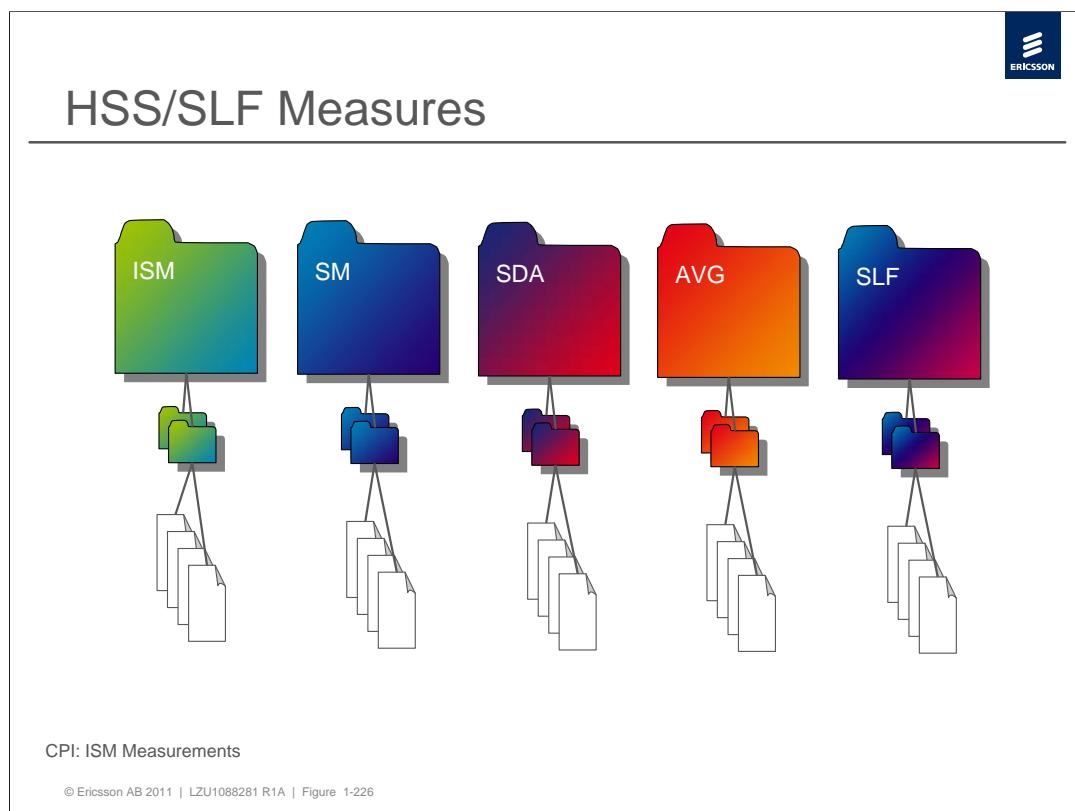
- › Default IMS file directory Linux cluster processor *location*

```
/data/NM/PMF/reporterLogs/Cscf  
/data/NM/PMF/reporterLogs/Cscf2  
/data/NM/PMF/reporterLogs/CscfSipServer  
/data/NM/PMF/reporterLogs/CscfSipClient
```

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-225

The figure shows the default file directory locations for CSCF Performance management XML files on both IOs and Linux processors.

The file path for the Linux cluster processor has to be stated when the FTU is used in order to transfer the XML files to a remote host.



The counters for HSS are divided in several groups, mainly based on the HSS modules. The figure above shows only the groups which are relevant for a HSS used in a pure IMS environment.

The groups are:

- IMS Subscription Manager (ISM)
- Session Manager (SM)
- Subscription Data Access (SDA)
- Authentication Vector Generator (AVG)
- Subscriber Locator Function (SLF)



HSS and SLF Measures – Location of XML files

- › Default IMS file directory IO location:

/opt/telorb/axe/tsp/NM/PMF/reporterLogs/HssISMLogs	(ISM)
/opt/telorb/axe/tsp/NM/PMF/reporterLogs/HssSMLogs	(SM)
/opt/telorb/axe/tsp/NM/PMF/reporterLogs/HssSDALogs	(SDA)
/opt/telorb/axe/tsp/NM/PMF/reporterLogs/HssAVGLogs	(AVG)
/opt/telorb/axe/tsp/NM/PMF/reporterLogs/HssSLFLogs	(SLF)

- › Default IMS file directory Linux cluster processor *location*

/data/NM/PMF/reporterLogs/HssISMLogs
/data/NM/PMF/reporterLogs/HssSMLogs
/data/NM/PMF/reporterLogs/HssSDALogs
/data/NM/PMF/reporterLogs/HssAVGLogs
/data/NM/PMF/reporterLogs/HssSLFLogs

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-227

The figure shows the default file directory locations for HSS and SLF Performance management XML files on both IOs and Linux processors.

The screenshot shows a Microsoft Internet Explorer window displaying the 'FTU Administrator Menu'. The left sidebar lists several management categories: Fault Management, Configuration Mgt, Logging, and License Management. The 'Configuration Mgt' section contains a link to 'FTU Administrator', which is highlighted with a red circle and a red arrow pointing to it from above. The main content area of the page is titled 'FTU Administrator Menu' and contains three main sections: 'Outgoing File Transfer' (with links to Categories, Files, and Transfer Jobs), 'Incoming File Transfer' (with a link to Transfer Jobs), and 'File Cleanup' (with a link to Cleanup Jobs). The bottom status bar of the browser window shows the URL as https://192.168.13.193/FTUAdministrator/index.html.

CPI: File Transfer Utility User Guide

The FTU Administrator Menu includes three administrative links. These links open browser pages called viewers, where the user can create, edit or delete configuration parameters. From each viewer, a configuration editor can also be opened. The three configuration types are as follows:

Categories - configuration of the Category

Files - configuration of the File

Destinations - configuration of the Destination.

The Category is used to identify and group the related Files. For example, files could be categorized as log, performance, configuration or any other file type the user requires. The FTU can transfer all File that belong to a Category at the same time.

The File contains the selected files to transfer, specified temporary storage, a Category assigned to the File and other parameters.

The Destination contains details of the destination node, some Category to transfer, and the time of transfer.

Creation of a Category

Category Editor

Name: HSS Logs
Description: HSS Logs Transfer

Create **Cancel**

```
graph TD; Destination1 --- Category1; Destination1 --- Category2; Destination1 --- Category3; Category1 --- File1; Category1 --- File2; Category2 --- File3; Category2 --- File4; Category3 --- File5;
```

CPI: File Transfer Utility User Guide
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-229

A new file category is created for the HSS PM files.

Definition of Files-to-transfer

Node Management (jambala) - Microsoft Internet Explorer

File Edit View Favorites Tools Help
Address: https://192.168.13.193/Toolbox/servlet/ToolboxGenerator
@ NODE MANAGEMENT change password documentation toolbox home logout

Fault Management
♦ Alarm Viewer
♦ Notification Viewer

Configuration Mgt
♦ TelORB Manager
♦ CM Browser
♦ FTU Administrator (circled)
♦ SPA Console

Logging
♦ Log Query

License Management
♦ License Manager

ERICSSON

Original Files
Category : HSS Logs
Files to transfer: /data/NM/PMF/reporterLogs/HSSLogs/*
Recurse mode: Yes (search in sub-folders as well)
Integrity check: No (search for all files)

Transfer Image
Folder prefix:
File extension:
Update:
View of originals: Snapshot (preserve original files, remove snapshots at cleanup)
Cleanup: Do not keep transferred files

Create (circled) **Cancel** **Local**

Diagram:

```
graph TD; Destination1 --- Category1; Destination1 --- Category2; Destination1 --- Category3; Category1 --- File1; Category1 --- File2; Category2 --- File3; Category2 --- File4; Category3 --- File5;
```

CPI: File Transfer Utility User Guide
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-230

New files to tranfer are defined for Performance Management.

Definition of a Transfer Job

The screenshot shows the 'Outgoing Transfer Job Editor' window. On the left, a sidebar lists various management modules: Fault Management, Configuration Mgt, Logging, License Management, and ERICSSON. The 'CM Recovery' and 'FTU Administrator' items are circled in red. The main form has fields for Name ('HSS Logs'), Enabled (checkbox checked), Destination (Primary and Secondary hosts, ports, and log paths), Compress files (checkbox checked), Scheduled time (2008-12-21), Schedule interval (5 min), Retry delay (30 sec), and Retry timeout (30 min). Categories are set to 'HSS Logs'. A 'Create' button is highlighted with a red circle. To the right, a hierarchical diagram shows 'Destination1' and 'Destination2' each connected to 'Category1', 'Category2', and 'Category3', which in turn connect to 'File1' through 'File5'.

New transfer job is defined for Performance Management.



Chapter 7 – Security & Authentication

1. Introduction
2. Architecture
3. User Interface
4. Fault Management
5. Configuration Management
6. Performance Management
- 7. Security, Authentication and Redundancy**
8. Session Establishment
9. Configuration Examples

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-232





CPI Documents

- › TSP Hardening User Guide
- › CSCF Hardening Guide
- › HSS Security Hardening Guide
- › SLF Security Hardening Guide

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-233

The CPIs (Customer Product Information) describing CSCF, HSS and SLF security are listed in the figure.



CSCF Configuration for Security

- › Authentication
 - The parameter *CscfOverallAuthenticationPolicy* should be set to *enabled*.
 - Authentication settings should be specific for the type of access (Access-aware Authentication for Fixed-Mobile Convergence)
- › Load Regulation
 - Load regulation limit for both processor load and memory consumption should not be higher than 80%.
- › Trusted Application Servers
 - The CSCF has a list of trusted Application Servers in order to verify if the Application Server is allowed to send SIP messages to CSCF.
- › CSCF Performance Counters
 - Counters exists and should be monitored in order to see if unauthorized clients tries to access the IMS Network

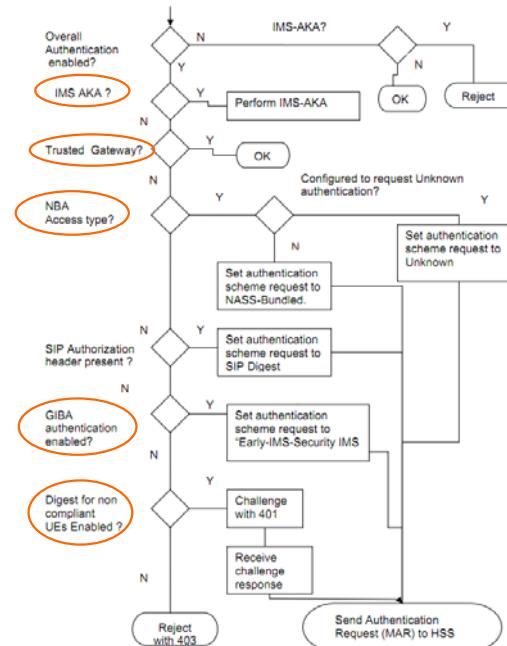
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-234

The figure lists features regarding CSCF node hardening in addition to the TSP platform hardening.

Authentication flow in CSCF at initial registration

Supported Authentication Methods:

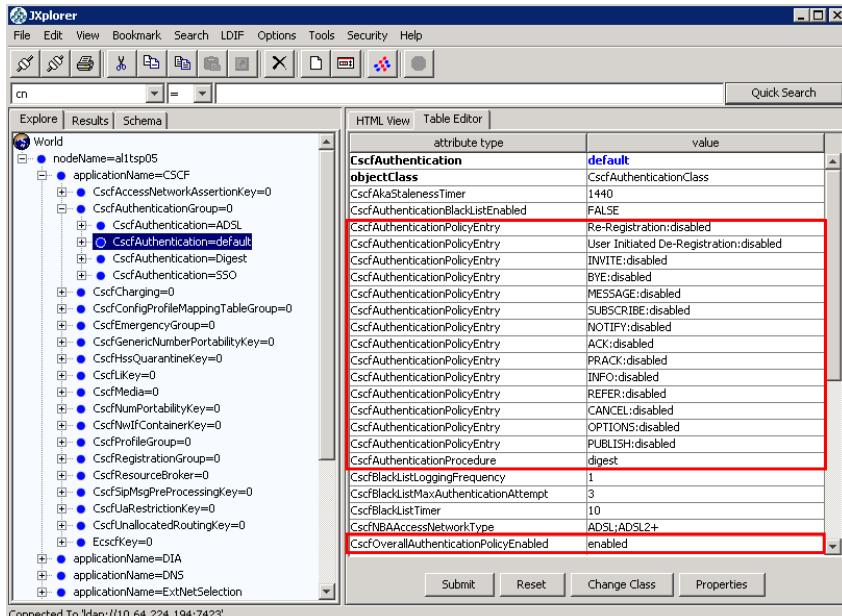
- *IMS AKA*
- *Trusted Gateway*
- *NBA*
- *GIBA*
- *Digest*



Supported Authentication Methods are:

- *IMS AKA*
- *Trusted Gateways*
- *NBA*
- *GIBA*
- *Digest*

CSCF Authentication Enabling



The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view shows a node named 'nodeName=al1tsp05' under 'World'. The 'CscfAuthentication' entry is selected. On the right, the 'Table Editor' pane displays various attributes and their values. A red box highlights several entries: 'CscfAuthenticationPolicyEntry' (value: Re-Registration:disabled), 'CscfAuthenticationPolicyEntry' (value: User Initiated De-Registration:disabled), 'CscfAuthenticationPolicyEntry' (value: INVITE:disabled), 'CscfAuthenticationPolicyEntry' (value: BYE:disabled), 'CscfAuthenticationPolicyEntry' (value: MESSAGE:disabled), 'CscfAuthenticationPolicyEntry' (value: SUBSCRIBE:disabled), 'CscfAuthenticationPolicyEntry' (value: NOTIFY:disabled), 'CscfAuthenticationPolicyEntry' (value: ACK:disabled), 'CscfAuthenticationPolicyEntry' (value: PRACK:disabled), 'CscfAuthenticationProcedure' (value: digest), 'CscfBlackListLoggingFrequency' (value: 1), 'CscfBlackListMaxAuthenticationAttempt' (value: 3), 'CscfBlackListTimer' (value: 10), 'CscfNBAAccessNetworkType' (value: ADSL;ADSL2+), and 'CscfOverallAuthenticationPolicyEnabled' (value: enabled). Below the table are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

Connected To 'ldap://10.64.224.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-236

The *CscfOverallAuthenticationPolicy* defines the overall authentication policy for the CSCF. If this is set to enabled, then all registrations are authenticated, and the authentication of all other requests is based on the *CscfAuthenticationPolicyEntries*. The values of these entries defines the authentication policy for a specific SIP method or registration condition.

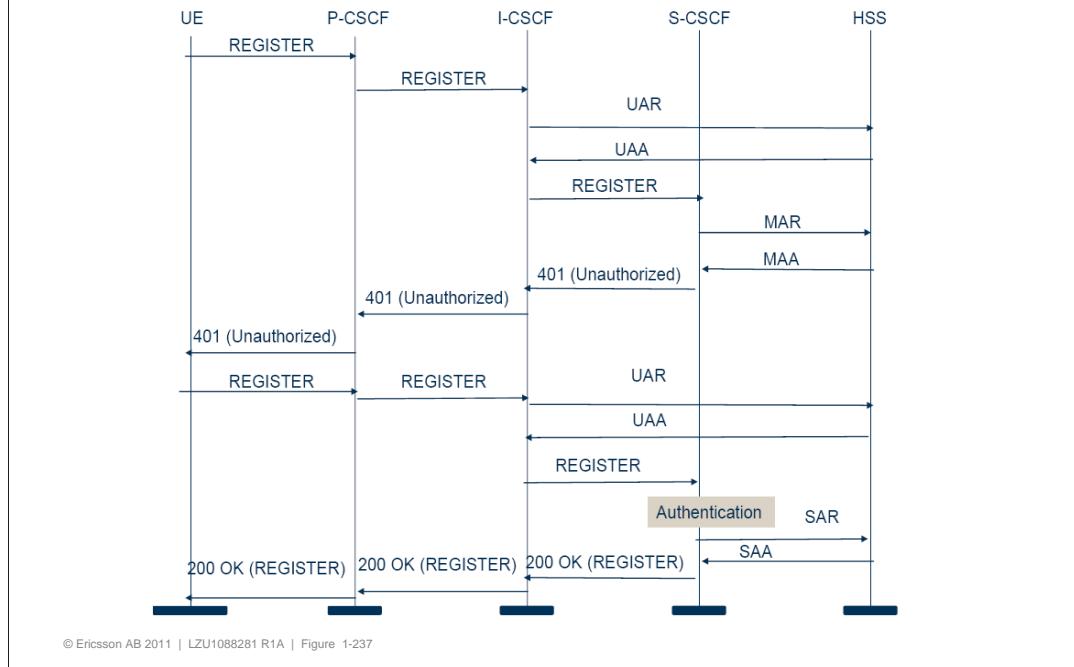
The *CscfAuthenticationProcedure* is used for authentication optimization.

Allowed values are:

Digest: The S-CSCF will apply existing digest authentication procedures.

Optimized: The S-CSCF keeps knowledge of the IP address of the registered contact after a successful authentication and uses that address when authenticating subsequent SIP request messages from the user. Note: the Optimized Digest is an Ericsson-proprietary enhancement.

Digest Authentication at Initial Registration



Digest authentication is based on a Basic HTTP authentication mechanism (RFC2617), with the addition of security improvements.

The client and the server have a shared password. Client needs to show the Server that it knows the password and the easiest way would be to send it within the message (basic HTTP). However a Man-in-the-Middle attack could possibly intercept the password and this is unacceptable. Therefore, client using DIGEST can prove that they know the shared password without sending it over the network. Digest uses hashes and nonces for this. A HASH algorithm is a one-way function that takes an argument of an arbitrary length and produces a fixed length result. It is computationally infeasible to obtain the original argument from a result. Two popular hash algorithms are MD5 (RFC 1321) and SHA1 (RFC 3174). A nonce is a random value that is used only once.

Nonce is sent to the UE which by using the hash algorithm generates a response. The response is sent through the Authorization header to the server. The server calculates its own response and matches that with the received one. If they match the user is authenticated.

The WWW-Authenticate and Authorization header fields are used with registrars, redirect servers and user agents, while Proxy-Authenticate and Proxy-Authorization header fields are used with proxies.

The inclusion of random nonces chosen by the server in the hash prevents replay attacks.

CSCF Digest Blacklist

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view under 'World' shows various nodes like 'nodeName=al1tsp05' and 'applicationName=CSCF'. On the right, the 'Table Editor' tab is selected, displaying a list of attributes and their values. The 'attribute type' column lists various CSCF authentication policy entries. The 'value' column contains specific configurations. Two entries are highlighted with red boxes:

attribute type	value
CscfAuthenticationBlackListEnabled	TRUE
CscfBlackListLoggingFrequency	1
CscfBlackListMaxAuthenticationAttempt	3
CscfBlackListTimer	10

At the bottom of the table editor, there are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A status bar at the bottom of the window indicates 'Connected To ldap://10.64.224.194:7423'.

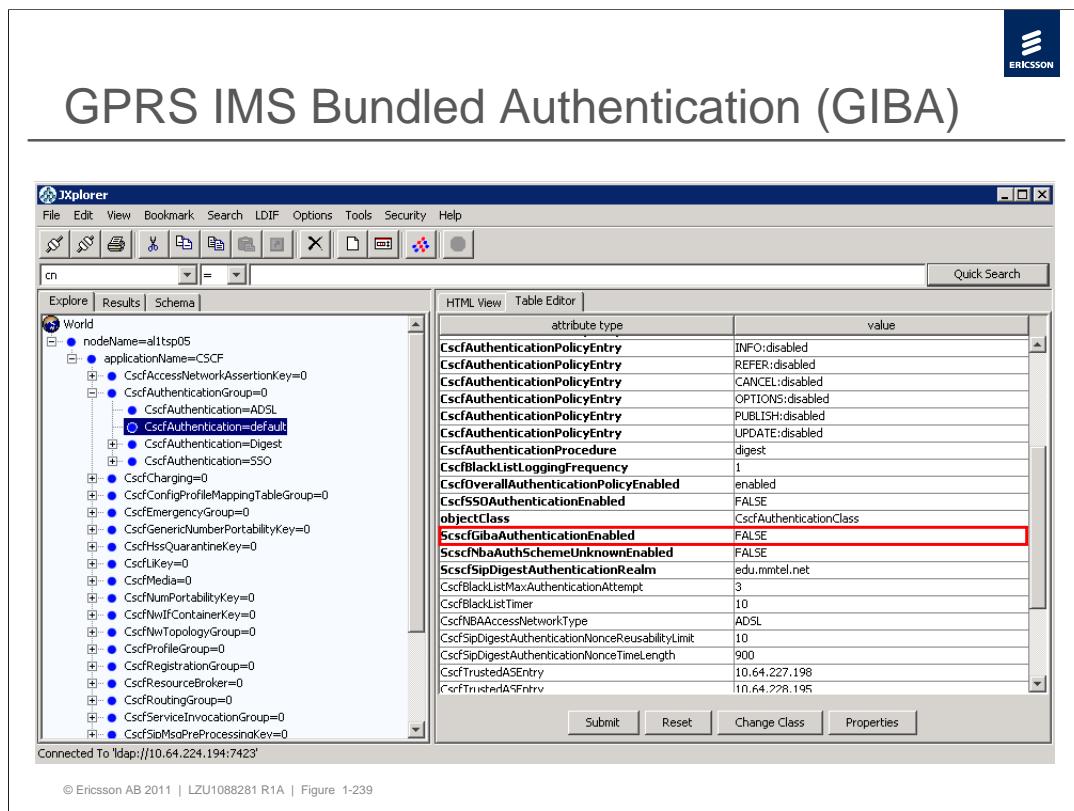
Available to the Digest Authentication schemes is an optional feature for blacklisting suspected SIP clients (identified by its IP address and Private ID), who attempt to pass the authentication challenge by repeatedly submitting authentication requests with different authentication credentials.

CscfAuthenticationBlackListEnabled is used to enable (TRUE) or disable (FALSE) the Blacklist function.

CscfBlackListMaxAuthenticationAttempt is used to configure the limit of the number of consecutive authentication attempts due to failed verification of an authentication response (both Ericsson Cx and 3GPP Cx are supported).

CscfBlackListTimer defines the time period that a user's request will be rejected due to maximum number of failed authentications.

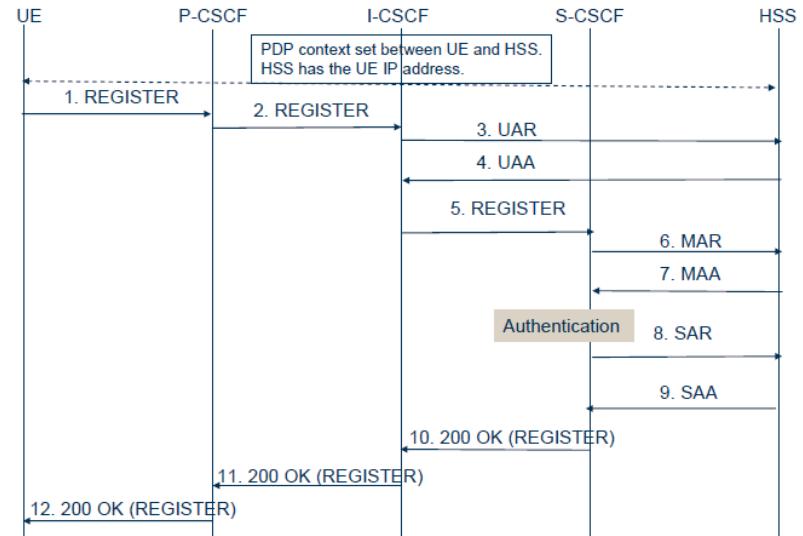
CscfBlackListLoggingFrequency defines the maximum number of blacklist time period before log is issued. Logs will include: start date and time; IMPI; IP address; IMPU; SIP method of the message which triggered the Blacklisting



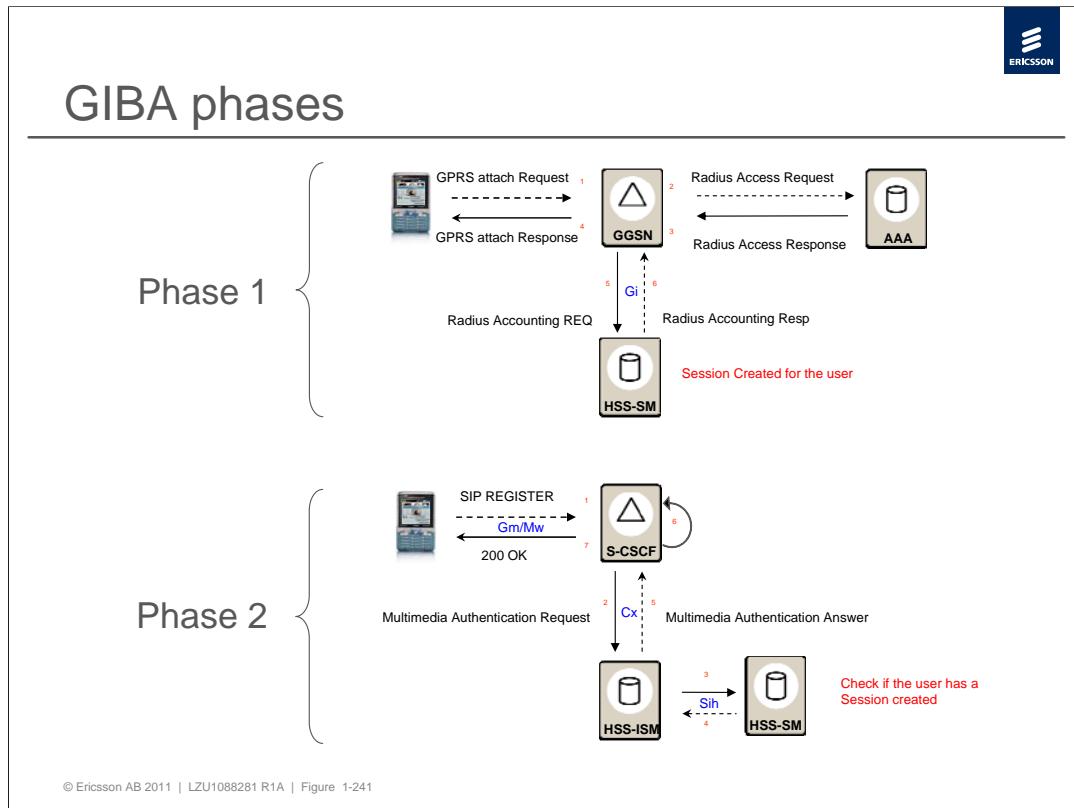
If *ScscfGibaAuthenticationEnabled* is set to TRUE, GPRS IMS Bundled Authentication (GIBA) is enabled. This parameter is access aware. The *ScscfGibaAuthenticationEnabled* cannot be enabled at the same time as the *ScscfSipDigestAuthenticationRealm* is enabled for the same access type profile. See document “CSCF Common Configuration Management Parameters)



GIBA at Initial Registration



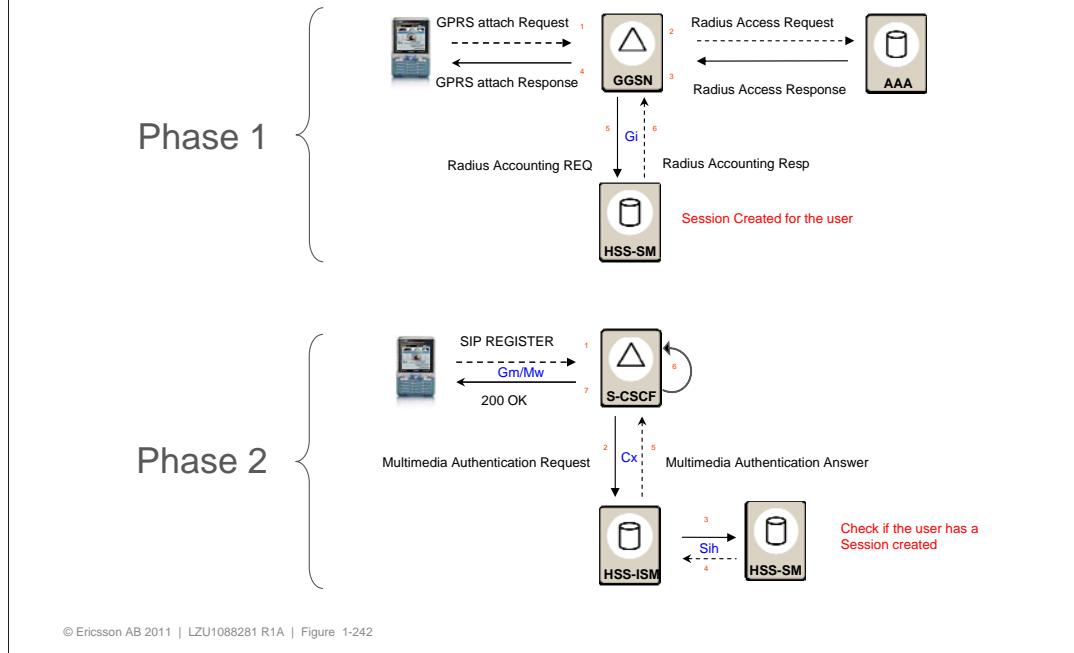
The GIBA authentication mechanism implies that a user, who has already granted access to the IP network through the operator's core network IP infrastructure, and hence, it is already authenticated by the operator, does not need to be authenticated once again in the IMS network. The Session Manager (SM) is a Remote Access Dial In User Service (RADIUS) server (part of HSS) used to support GIBA authentication (not showed in the above picture). It is used to keep track of the Access Network session information and managing the relationship between the IP address and the Access Identifier. The SIP authentication procedure is initiated by the S-CSCF, upon reception of a SIP request. If the S-CSCF decides to authenticate the request (*ScscfGibaAuthenticationEnabled* is set to TRUE), it sends a MAR with the SIP-Authentication-Scheme set to "Early-IMS-Security" and receives Multimedia Authentication Answer (MAA) from HSS with Result-Code set to DIAMETER_SUCCESS and Authentication-Scheme set to "Early-IMS-Security". The S-CSCF checks the IP address received in Framed-IP-Address AVP against the UE IP address from the Via header received in initial REGISTER request. If the IP addresses match, the authentication is successful. S-CSCF stores in the Contact information the IP address and the authentication scheme "Early-IMS-Security". S-CSCF updates the HSS with a SAR and, after storing the user profile received in the SAA, returns a 200OK response to the UE.



PHASE 1:

- 1) MS initiates a GPRS attach towards the GGSN
- 2) GGSN sends a Radius Access Request to the AAA server
- 3) The AAA server answers with a Radius Access Response
- 4) GGSN finalizes the GPRS attach procedures with a final response to the MS
- 5) If GPRS attach was successful, GGSN sends a Radius Accounting Request to the HSS-SM module. The message contains the following attributes:
 - *NAS-IP-Address* = <GGSN IP address>
 - *Framed IP Address* = <client IP address>
 - *Calling Station ID* = <user's MSISDN>
- 6) HSS-SM creates a Session for this user and answers back with a Radius Accounting Response

GIBA procedure



PHASE 2:

- 1) The user tries to access the IMS network by sending a SIP REGISTER message
- 2) If GIBA authentication is allowed S-CSCF requests the user IP address, stored in HSS, through a Multimedia Authentication Request.
- 3) HSS-ISIM contacts the HSS-SM module to check if a session has been created for this user and to fetch the IP address previously stored in HSS-SM
- 4) HSS-SM replies back with a result for this check, including the IP address in the Framed-IP-Address AVP
- 5) A Multimedia Authentication Answer is sent back to S-CSCF. If the GIBA authentication is allowed the following attributes are included in the message:
 - *Result-Code* = DIAMETER_SUCCESS
 - *Authentication-Scheme* = Early-IMS-Security
- 6) The S-CSCF checks the IP address received in Framed-IP-Address AVP against the UE IP address from the Via header received in initial REGISTER request.
- 7) A 200 OK message is sent back to the UE if the match is found and the authentication is successfully completed



NASS Bundled Authentication (NBA)

- › "Single Sign On" for wireline access
- › Provides access to IMS network for legacy equipment that cannot support the IMS access security
- › Allows to reuse the authentication of the NASS to gain access to IMS

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-243

When registering to the IMS subsystem, the location of where the user is accessing from is verified by the NASS (which also handles the authentication / authorization) and if the NASS location is equal to the provisioned location, the user is authorized to access from at IMS level, the user gains access to IMS.

It is assumed that there exist a strong relationship between the access network and the IMS network, and that the users NASS location can be provisioned in the user profile.

The main use case for NASS-IMS bundled authentication is to provide access to the IMS network for legacy equipment that cannot support the IMS access security, but also it is possible to reuse the authentication of the NASS to gain access to IMS.

The UE gets network attachment after the authentication at the NASS level. The CLF in the NASS (Network Attachment SubSystem) holds a binding between the IP address and the location information (contains the Line Identifier), which the user holds for the xDSL connectivity.

The screenshot shows the JXplorer LDAP browser interface. On the left, a tree view displays the LDAP structure under the 'World' base. A specific entry for the CSCF node ('nodeName=al1tsp05') is expanded, showing various authentication-related parameters. On the right, a table editor shows the attributes and their values for this entry. Two specific attributes are highlighted with red boxes: **CscfNbAuthSchemeUnknownEnabled** (value: FALSE) and **CscfNbAAccessNetworkType** (value: ADSL). Other visible attributes include CscfAuthenticationPolicyEntry, CscfAuthenticationProcedure, CscfBlackListLoggingFrequency, CscfOverallAuthenticationPolicyEnabled, CscfSSOAuthenticationEnabled, objectClass, CscfGibaAuthenticationEnabled, CscfNbAAccessNetworkType, CscfSipDigestAuthenticationRealm, CscfBlackListMaxAuthenticationAttempt, CscfBlackListTimer, and CscfNbAAccessNetworkType.

attribute type	value
CscfAuthenticationPolicyEntry	INFO:disabled
CscfAuthenticationProcedure	digest
CscfBlackListLoggingFrequency	1
CscfOverallAuthenticationPolicyEnabled	enabled
CscfSSOAuthenticationEnabled	FALSE
objectClass	CscfAuthenticationClass
CscfGibaAuthenticationEnabled	FALSE
CscfNbAuthSchemeUnknownEnabled	FALSE
CscfSipDigestAuthenticationRealm	edu.umt.net
CscfNbAAccessNetworkType	ADSL
CscfBlackListMaxAuthenticationAttempt	3
CscfBlackListTimer	10
CscfNbAAccessNetworkType	ADSL
CscfSipDigestAuthenticationNonceReusabilityLimit	10
CscfSipDigestAuthenticationNonceTimeLength	900
CscfTrustedASEntry	10.64.227.198
CscfTrustedASEntry	10.64.228.195

Connected To 'ldap://10.64.224.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-244

It is possible to enable the NBA authentication method by defining a list of access network types for which NASS bundled authentication is applicable. The parameter *CscfNbAAccessNetworkType* can hold a semicolon separated list of access network types. If the list is empty, the NBA function is disabled.

In the example above, network types ADSL and ADSL2+ will initiate an NBA authentication.

CscfNbAuthSchemeUnknownEnabled This parameter controls if the CSCF mandates NASS Bundled authentication for all users of the access networks configured in the *CscfNbAAccessNetworkType* or if the CSCF allows the HSS to choose between NASS Bundled authentication or Digest authentication for those access networks.

If it is enabled, then the S-CSCF sends "Unknown" in the MAR. If it is disabled, then the S-CSCF sets the authentication scheme to "NASS-Bundled".

This parameter is not access aware.

Note: The user must be allowed in HSS to authenticate using NBA (please refer to "Allowed Authentication Mechanism in HSS" slide)



Authentication Method Selection Based on Line Profiles configured in HSS

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn

Explore | Results | Schema |

HTML View Table Editor

attribute type	value
HSS-LineName	NBA1
HSS-LineValue	LineId3
objectclass	HSS-AccessLineIdentifier
groupid	0
HSS-AuthenticationMechanism	NBA-LineProfile
ownerId	0
permissions	9
shareTree	nodeName=tsp01tsp07geo
parent	

Connected To 'ldap://10.64.224.193:7323'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-245

The HSS is capable of selecting the authentication mechanism to be used for a **wireline** user based on the Line Profiles provisioned in HSS.

Based on a mechanism in HSS that holds a set of information and logic, it is possible to determine if the user is to be authenticated with HTTP digest authentication or if it is granted the access using NASS Bundled Authentication mechanism (both mechanisms are exclusive). A user can have several line profiles (up to 10), being enough that one of them is allowed for the user to be granted the access. Line Profiles indicating NBA-LineProfile should take precedence over Line Profiles indicating Digest-LineProfile.

Whenever a MAR message is received, HSS will select the authentication method to be applied based on Line Profile data if the following conditions are fulfilled:

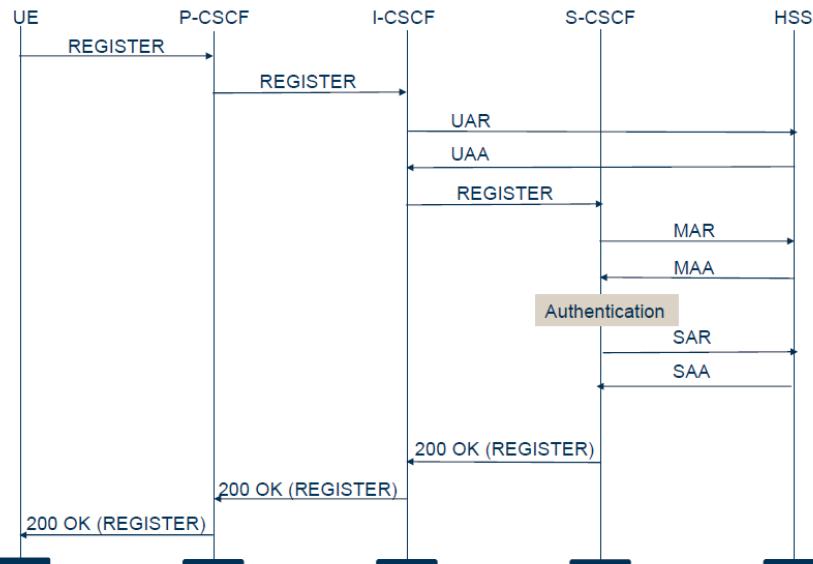
- "Unknown" authentication scheme received
- SSO commercial license is active
- The given IMPI has got at least one Access Line with either NBA-LineProfile or Digest-LineProfile provisioned.
- dsl-location is stored for the IMPI/IMPU pair involved

HSS-LineName identifies the Access Line.

HSS-LineValue identifies physically the Access Line by means of the dsl-location content.

HSS-AuthenticationMechanism contains the authentication type to be supported by the Access Line (NBA-LineProfile, Digest-LineProfile).

NBA Flow at Initial Registration



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-246

When NBA applies (i.e. match found with *CscfNBAAccessType*), the S-CSCF sends a MAR with the SIP-Authentication-Scheme set to either “NASS-Bundled” or “Unknown” (decided by *ScscfNbaAuthSchemeUnknownEnabled*). However, if the AVP shall be set to “NASS-Bundled” the S-CSCF verifies that the dsl-location parameter is included in the PANI header prior to sending the MAR.

The S-CSCF receives the Multimedia Authentication Answer (MAA) with Result-Code set to DIAMETER_SUCCESS and the SIP-Authentication-Scheme AVP set to “NASS-bundled”. One or several Line-Identifier AVP(s) are included. The Line-Identifier AVP may contain a fixed broadband access line identifier associated to the user or it may contain the value “Line_Profile”. If the value “Line_Profile” is included in the Line-Identifier AVP, no further authentication is required in the S-CSCF. It is expected that there will be only one Line-Identifier AVP in this case. If there are any additional Line-Identifier AVPs, they will be ignored. If the value “Line_Profile” is not included in the first Line-Identifier AVP, the SCSCF verifies the dsl-location parameter is included in the PANI header. If the dsl-location parameter is included in the PANI header, S-CSCF compares the string in the Line-Identifier AVP(s) with the string in the dsl-location parameter in the PANI header. If there is a match, the authentication is successful. If the value “Line_Profile” is located in a Line-Identifier AVP other than the first instance, it is treated as a regular fixed broadband access line identifier and it is compared to the dsl-location parameter in the PANI header.

S-CSCF continues the process by updating the HSS with SAR and receiving the user profile with a SAA. If the authentication was successful, a 200OK response is sent to the UE.

Allowed Authentication Mechanism in HSS

attribute type	value
HSS-PrivateUserID	mmtel3017@edu.mntel.net
objectClass	HSS-User
groupID	0
HSS-AllowedAuthMechanism	NBA
HSS-LocationData	sip:10.64.227.194:5060
HSS-LocationData	CSCFCX.edu.mntel.net
HSS-ReferenceAccessLocation	ADSL/dsl-location=line-id26
HSS-RoamingAllowed	TRUE
HSS-SipLocked	FALSE
HSS-UserBarringInd	FALSE
HSS-UserImsi	
HSS-UserState	registered
ownerId	0
permissions	9
shareTree	nodeName=a1tsp01
HSS-UserPassword	
parent	

Submit | Reset | Change Class | Properties

Digest
 HSS-AllowedAuthMechanism ← SSO (valid also for GIBA)
 NBA

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-247

In the HSS-User Object Class (Private ID container) it is possible to specify which authentication mechanisms are supported by the user. This configuration has to be consistent with the configurations in CSCF (please refer to previous slides in this chapter).

HSS-AllowedAuthMechanism contains the authentication mechanisms supported by the user. SSO (valid also for GIBA) and NBA mechanisms can be only set if *HSS-SingleSignOnLicense* is set to TRUE. SSO (GIBA), NBA and Digest are currently supported.

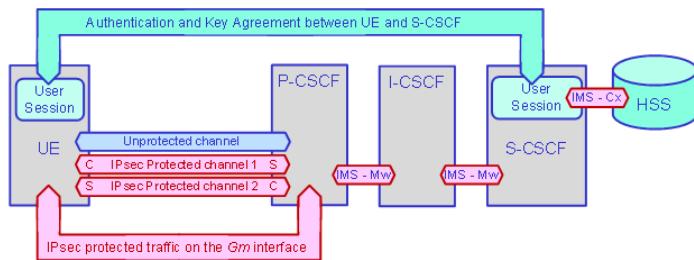
If *HSS-AllowedAuthMechanism* is set to NBA, the *HSS-ReferenceAccessLocation* specifies the access location (line identifier) that is allowed for this user. In the example above, *line-id26* is the allowed location (when ADSL is the access network type).



IMS Authentication and Key Agreement (AKA)

The *IMS AKA* security mechanism allows:

- **Mutual Authentication** between UE and S-CSCF
- **Protection** of all traffic between the UE and the P-CSCF on the Gm interface on dual IPsec channels.



Main steps:

- The UE starts the AKA session on an unprotected channel between the UE and the P-CSCF
- The AKA session registration establishes two IPsec protected channels between the UE and the P-CSCF

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-248

IMS AKA is described in the 3GPP document **TS.33.203** Access security for IP based services

AKA requires all traffic between a UE (3G terminal) and a P-CSCF during a session to be sent on specific IPsec protected channels. AKA uses the IMS Gm interface (SIP protocol) for communication between a UE and a P-CSCF. Both sides have a Client port and a Server port. Session registrations are performed with the SIP REGISTER request message. The UE starts the AKA session registration on an unprotected channel between the UE and the P-CSCF. The AKA session registration establishes two IPsec protected channels between the UE and the P-CSCF.

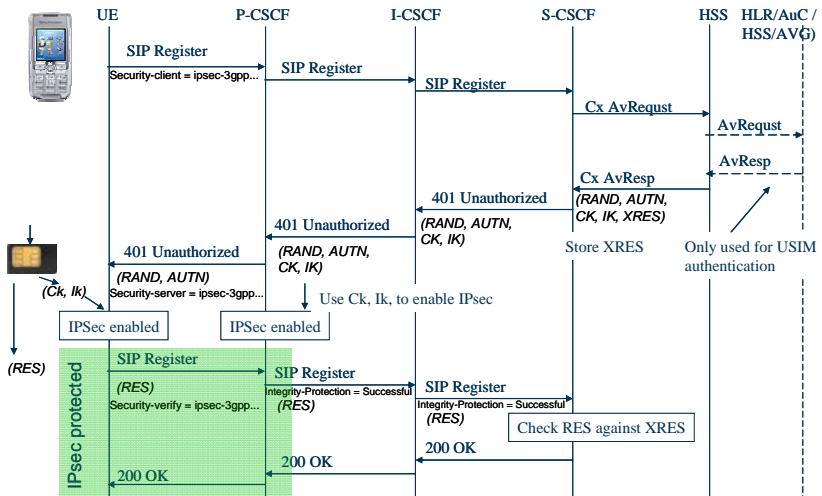
The Security-Client, Security-Server, and Security-Verify headers are used to establish protected port pairs between UE and P-CSCF. The information about port numbers etc. on the UE side is passed to the P-CSCF side in the Security-Client header. The information about port numbers etc. on the P-CSCF side is passed to the UE side in the Security-Server header.

The IMS Gm interface supports two alternative transports protocols **TCP** and **UDP**. The IPsec protected channels are used differently depending on used transport protocol. For the **TCP** protocol IPsec channel 1 is used for request messages from UE to P-CSCF and response messages from P-CSCF to UE. IPsec channel 2 is used for request messages from P-CSCF to UE and response messages from UE to P-CSCF. For the **UDP** protocol IPsec channel 1 is used for all traffic from UE to P-CSCF. IPsec channel 2 is used for all traffic from P-CSCF to UE.

In case the UE indicates in the Require/Proxy-Require/Security-Client headers that the UE wishes to use IMS AKA authentication, then IMS AKA authentication procedure is performed.

IMS AKA Simplified Flow

› ISIM/USIM AKA based access authentication

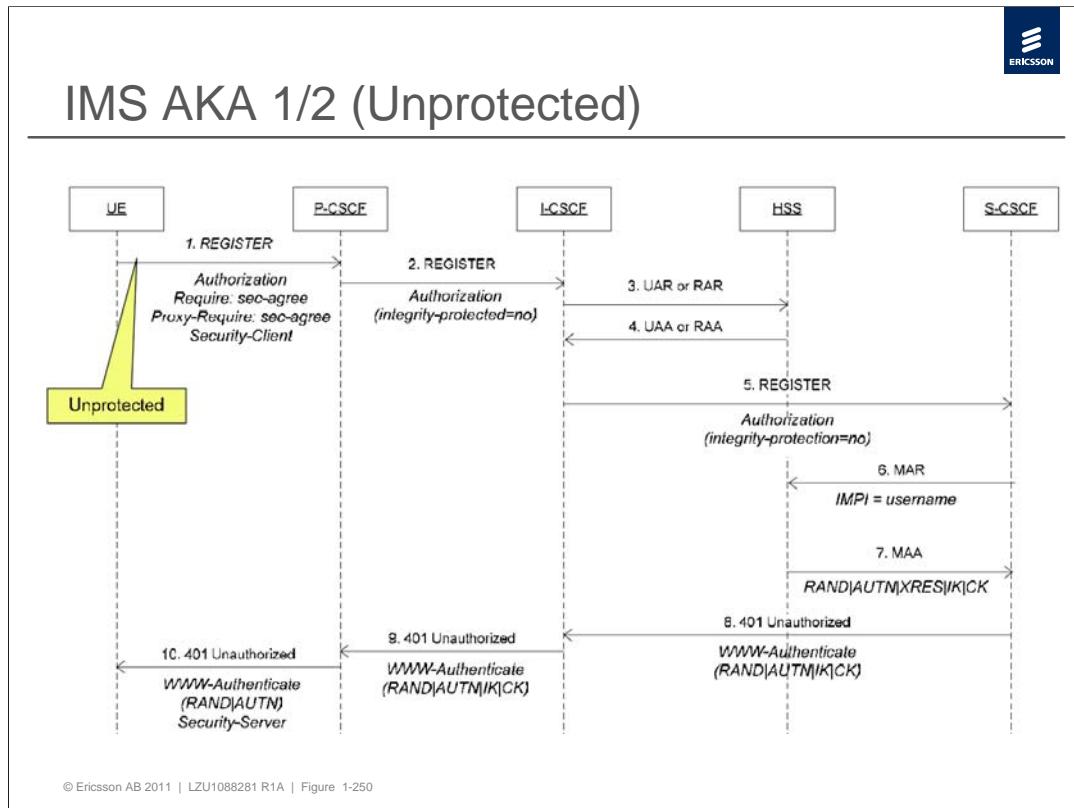


An IMS AKA authentication consists of 2 phases, one where the messages between UE and P-CSCF are sent over unprotected channels and one phase where the messages are encrypted. HSS_AVG module is needed in case the authentication vector is generated by the HSS, otherwise it can be retrieved from a HLR.

ISIM users require the Authentication Vector to be generated in the HSS.

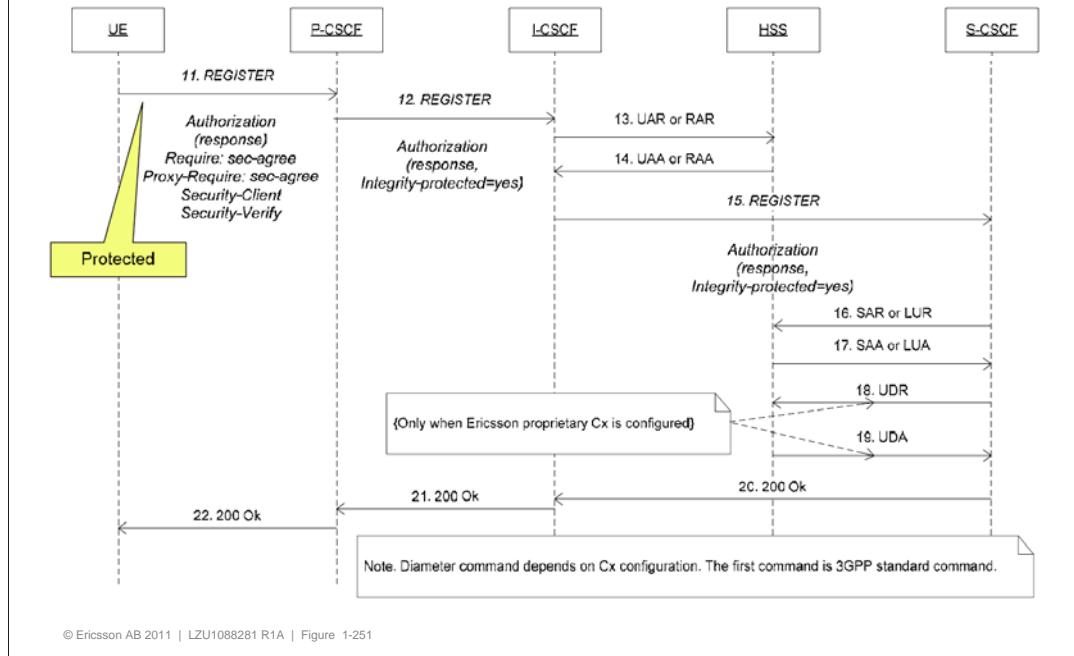
USIM users could retrieve an Authentication Vector from the HSS_AVG module or from the HLR.

For more details of the flow, please refer to the next two slides.



- At initial registration, the UE includes the *Authorization* header (username, uri, realm), the *Require: sec-agree* and *Proxy Require: sec-agree* headers and one or more *Security-Client* headers (for IPSec setup)
- P-CSCF selects encryption and integrity algorithms and forwards the REGISTER to the I-CSCF
- 4. I-CSCF sends a UAR/RAR to HSS to obtain the address of the requesting user's home S-CSCF. HSS responds with a UAA/RAA message
- I-CSCF forwards the REGISTER to S-CSCF
- S-CSCF requests an Authentication Vector (AV) by sending a MAR to the HSS
- HSS responds with a MAA containing an AV {RAND, AUTN, XRES, IK, CK}
- S-CSCF returns a 401 (Unauthorized) response to I-CSCF, including RAND, the challenge to be forwarded to the UE; AUTN, used to authenticate the network to the UE; and the two keys IK and CK for use by the P-CSCF to set up the security associations. XRES, the expected response to the challenge, is retained by S-CSCF and not included
- I-CSCF forwards the 401 (Unauthorized) response to P-CSCF
- P-CSCF sets up its end of the security associations using the keys and the algorithms selected in step 2, and forwards the challenge (without the keys) to the UE unprotected.

IMS AKA 2/2 (Protected)



- 11-15. The UE uses AUTN to authenticate the network, sets up its end of security associations, and calculates RES, the response to the challenge. The UE constructs a new REGISTER request, including an *Authorization* header with a *response* parameter that is calculated by a hash algorithm that takes as input RES, the *nonce* parameter sent by the S-CSCF and other parameters. The REGISTER request is sent over the new security associations to the P-CSCF and forwarded by the P-CSCF and the I-CSCF to the S-CSCF. In order to validate the *response* parameter, the S-CSCF constructs an expected *response* parameter value using the same hash algorithm as that used in the UE, but using XRES instead of RES. The received *response* value is compared to the expected *response* value and, if they are identical, then authentication has succeeded
- 16-17. S-CSCF sends a SAR or LUR message to HSS to confirm the authentication. HSS removes a "pending" flag from the assignment of the S-CSCF to the user's Public User Identity, allowing subsequent SIP requests to be delivered to this S-CSCF. If 3GPP standard Cx is used, the S-CSCF also obtains user profile information from the HSS.
- 18-19 (Only applicable when using Ericsson proprietary Cx) The S-CSCF obtains user profile information from the HSS with a UDR-UDA transaction
- 20-22 The S-CSCF sends a 200 OK message back to the UE, via the I-CSCF and the P-CSCF



AKA Allowed Algorithms in CSCF

JXplorer interface showing the configuration of AKA Allowed Algorithms in CSCF.

The left pane shows the LDAP tree structure under 'cn' with the following hierarchy:

- World
 - nodeName=al1tsp05
 - applicationName=CSCF
 - CscfAccessNetworkAssertionKey=0
 - CscfAuthenticationGroup=0
 - CscfAuthentication=ADSL
 - CscfAuthentication=default
 - CscfAuthentication=Digest
 - CscfAuthentication=SSO
 - CscfCharging=0
 - CscfConfigProfileMappingTableGroup=0
 - CscfEmergencyGroup=0
 - CscfGenericNumberPortabilityKey=0
 - CscfImsQuarantineKey=0
 - CscfLiKey=0
 - CscfMedia=0
 - CscfNumPortabilityKey=0
 - CscfNwIfContainerKey=0
 - CscfProfileGroup=0
 - CscfRegistrationGroup=0
 - CscfResourceBroker=0

attribute type	value
objectClass	CSCF-Application
applicationName	CSCF
BcfEnabled	FALSE
BcfOperationalState	0
CscfActiveUserMethod	
CscfAdministrativeState	1
CscfAkaAlgorithmEntry	1:hmac-md5-96,aes-cbc:enabled
CscfAkaAlgorithmEntry	2:hmac-sha-1-96,aes-cbc:enabled
CscfAkaAlgorithmEntry	3:hmac-md5-96,des-edc3-cbc:enabled
CscfAkaAlgorithmEntry	4:hmac-sha-1-96,des-edc3-cbc:enabled
CscfAkaAlgorithmEntry	5:hmac-md5-96,null:enabled
CscfAkaAlgorithmEntry	6:hmac-sha-1-96,null:enabled
CscfAkaStalenessTimer	1440
CscfASFallOverTimeInvite	5
CscfASFallOverTimeNonInvite	5
CscfAuthenticationPolicyEntry	Re-Registration:disabled
CscfAuthenticationPolicyEntry	User Initiated De-Registration:disabled

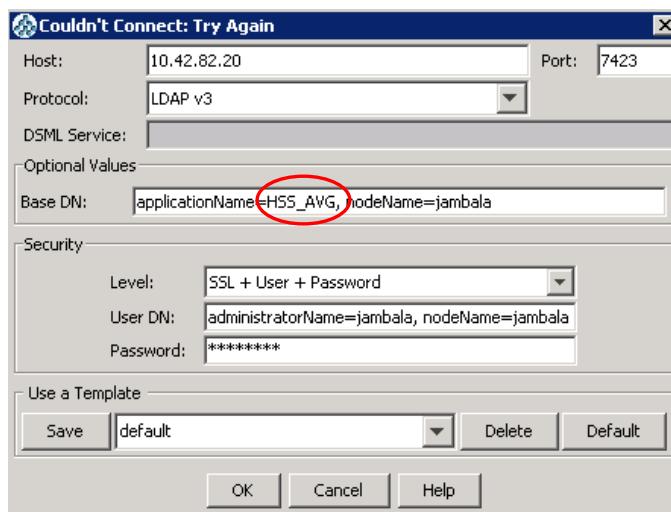
When the UE requests an IMS AKA authentication, the AKA algorithm is selected from the list specified by the parameter *CscfAkaAlgorithmEntry*, if a match is found with the algorithms supported by the UE and if the combination algorithm/encryption-algorithm is enabled.

CscfAkaAlgorithmEntry has the following syntax:

<priority-nr>:<algorithm>,<encryption-algorithm>:<enabled/disabled>



Login to the HSS_AVG application



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-253

The Application name for the AVG application is *HSS_AVG*.

AVG Configuration Object Class Model



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-254

This picture presents AVG Configuration Object Class Model.



AVG Configuration Parameters

Dxplorer interface showing the configuration of AVG parameters.

The left pane shows the LDAP tree structure under "cn" with nodes like "nodeName=jambala" and "applicationName=HSS_AVG".

The right pane displays the "HTML View" of the "Table Editor" for the object class "HSS-AvgGlobalConfiguration". The table contains the following data:

attribute type	value
HSS-AvgGlobalConfigurationName	HSS-AvgGlobalConfiguration
objectClass	HSS-AvgGlobalConfiguration
groupID	S15
HSS-AvgEpcDeployment	TRUE
HSS-AvgInstallationType	Monolithic
HSS-AvgOAMLogStatus	TRUE
HSS-AvgServicesLogStatus	TRUE
ownerId	S15
permissions	15
shareTree	nodeName=jambala
parent	

See also CPI "AVG LDAP Interface Description"

Connected To ldap://10.42.82.20:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-255

HSS-AvgEpcDeployment indicates that the AVG is configured to work in Evolved Packet Core (EPC) deployment .

HSS-AvgInstallationType identifies the HSS type of configuration (Monolithic,Front-End) . The visibility of some attributes/objects depends on the value of this attribute.

HSS-AvgOAMLogStatus is a flag that states whether OAM Log is active or not.

HSS-AvgServicesLogStatus is a flag that states whether Services Log is active or not.

The screenshot shows the JXplorer LDAP browser interface. On the left is a tree view of the LDAP structure under the 'World' node, including various application containers like DIA, FTU, and HSS_AVG. On the right is a table editor showing the attributes of the selected object, HSS-AvgA4KeyInd. The table has columns for attribute, type, and value. The highlighted rows are:

attribute	type	value
HSS-AvgA4KeyInd	object	I
objectClass	HSS-AvgA4Key	
oaid	S14	
HSS-AvgEncryptedA4Key	A1EE5608E33AF05470858608D1DE080F	
ownerId	S14	
permissions	9	
shareTree	nodeName=jambala	
HSS-AvgA4Key		
parent		

Below the table are buttons for Submit, Reset, Change Class, and Properties. A note on the right says "See also CPI 'AVG LDAP Interface Description'".

HSS-AvgA4KeyInd identifies the A4Key indication.

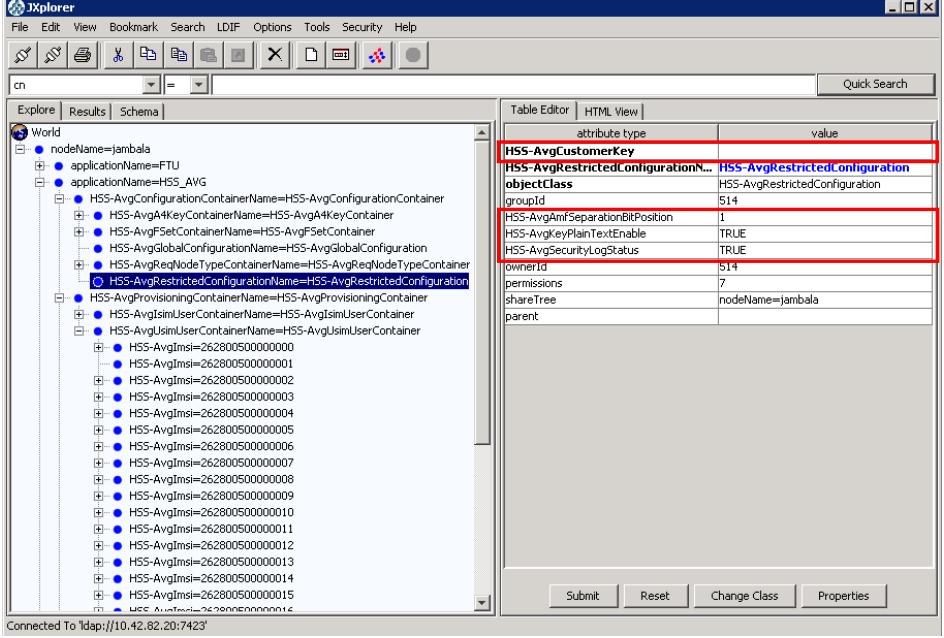
HSS-AvgEncryptedA4Key is the encrypted A4Key value.

See also CPI "AVG LDAP Interface Description"

HSS-AvgFSetInd is used to identify the function set identifier.

HSS-AvgSetName is used to identify the algorithm.

HSS-AvgFSetEncryptedOp is used to identify the encrypted Operator variant algorithm.



The screenshot shows the JXplorer LDAP browser interface. On the left is a tree view of the LDAP structure under 'World'. A selected node is expanded to show its sub-entries, including 'HSS-AvgCustomerKey', 'HSS-AvgRestrictedConfiguration...', 'objectClass', 'groupId', 'HSS-AvgAmfSeparationBitPosition', 'HSS-AvgKeyPlainTextEnable', 'HSS-AvgSecurityLogStatus', 'ownerId', 'permissions', 'shareTree', and 'parent'. The right panel displays a table editor for the selected entry, with columns for 'attribute type' and 'value'. The rows correspond to the expanded entries in the tree view. The 'HSS-AvgCustomerKey' row is highlighted with a red border. The entire configuration table is also highlighted with a red border. At the bottom of the table editor, there are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A note 'See also CPI "AVG LDAP Interface Description"' is visible on the right side of the table editor.

attribute type	value
HSS-AvgCustomerKey	
HSS-AvgRestrictedConfiguration...	HSS-AvgRestrictedConfiguration
objectClass	HSS-AvgRestrictedConfiguration
groupId	514
HSS-AvgAmfSeparationBitPosition	1
HSS-AvgKeyPlainTextEnable	TRUE
HSS-AvgSecurityLogStatus	TRUE
ownerId	514
permissions	7
shareTree	nodeName=jambala
parent	

HSS-AvgCustomerKey is the Customer Key value.

HSS-AvgAmfSeparationBitPosition is a separation bit position, starting from the Most Significant Bit and going up to the Least Significant Bit. More information can be found in *GPP System Architecture Evolution (SAE); Security architecture*, 3GPP TS 33.401.

HSS-AvgKeyPlainTextEnable indicates that the A4Key and the OP can be introduced in plain text.

HSS-AvgSecurityLogStatus is a flag that states whether Security Log is active or not.



AVG Requesting Node Type

See also CPI "AVG LDAP Interface Description"

attribute type	value
HSS-AvgEndIndValue	14
HSS-AvgInitialIndValue	11
HSS-AvgUsimReqNodeTypeName	MME
objectClass	HSS-AvgUsimReqNodeType
groupId	514
ownerId	514
permissions	9
shareTree	nodeName=jambala
parent	

Connected To 'ldap://10.42.82.20:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-259

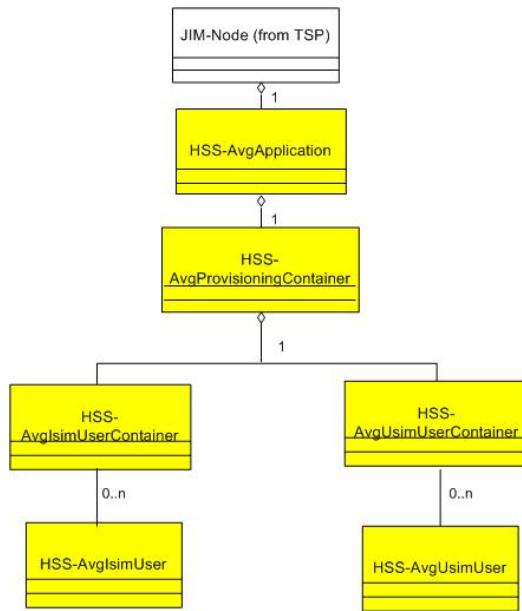
HSS-AvgEndIndValue is used to identify the end value for Requesting Node Type Index (IND) range.

HSS-AvgInitialIndValue is used to identify the initial value for IND range.

HSS-AvgUsimReqNodeTypeName is used to identify the requesting node type.



AVG Provisioning Object Class Model



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-260

This picture presents AVG Provisioning Object Class Model. It is only applicable to Monolithic deployment of HSS.

attribute type	value
HSS-AvgA4KeyInd	1
HSS-AvgEncryptedK	A09562241F632664A422D562F753AAA3
HSS-AvgFSetInd	0
HSS-AvgImsi	2628005000000001
objectClass	HSS-AvgUsmUser
group	S16
HSS-AvgAmf	0000
ownerId	S16
permissions	9
shareTree	nodeName=jambala
parent	

See also CPI "AVG LDAP Interface Description"

Connected To ldap://10.42.82.20:7423

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-261

HSS-AvgImsi identifies the International Mobile Subscriber Identity (IMSI) associated to the user.

HSS-AvgA4KeyInd contains the identifier of the key used for encrypting the key of the subscriber. It is a reference to *HSS-AvgA4KeyInd* of *HSS-AvgA4Key* Object Class.

HSS-AvgEncryptedK is used for store the encrypted K value for authentication service purposes.

HSS-AvgFSetInd is the key identifier of the object's *HSS-AvgFSet* that identifies the algorithm of generation of vectors associated with the user. It is a reference to *HSS-AvgFSetInd* of *HSS-AvgFSet* Object Class.



Access Awareness

- › Access Awareness is used in an FMC (Fixed Mobile Convergent) network.
- › In some cases service delivery depends on the access
- › The Access Awareness function is realized by the following sub-functions:
 - PANI assertion
 - Selection of Authentication Policy
 - Selection of Nomadism Control or Roaming Restriction
 - Selection of Configuration Policy

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-262

Please note that if the PANI Assertion sub-function is enabled, the PANI header is asserted in the IMS Access nodes:

- P-CSCF
- A-ALG (e.g. A-SBG)

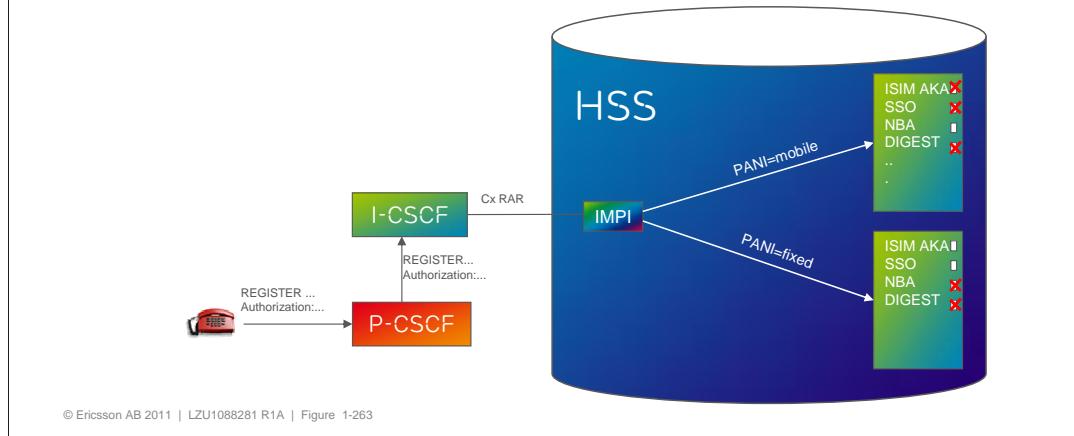
For broadband access, the CLF is queried by the A-ALG to get the correct access type.

For 3GPP access, the P-CSCF may receive one PANI generated by the UE that is validated against a configurable mapping of the IP-address to acceptable access types.

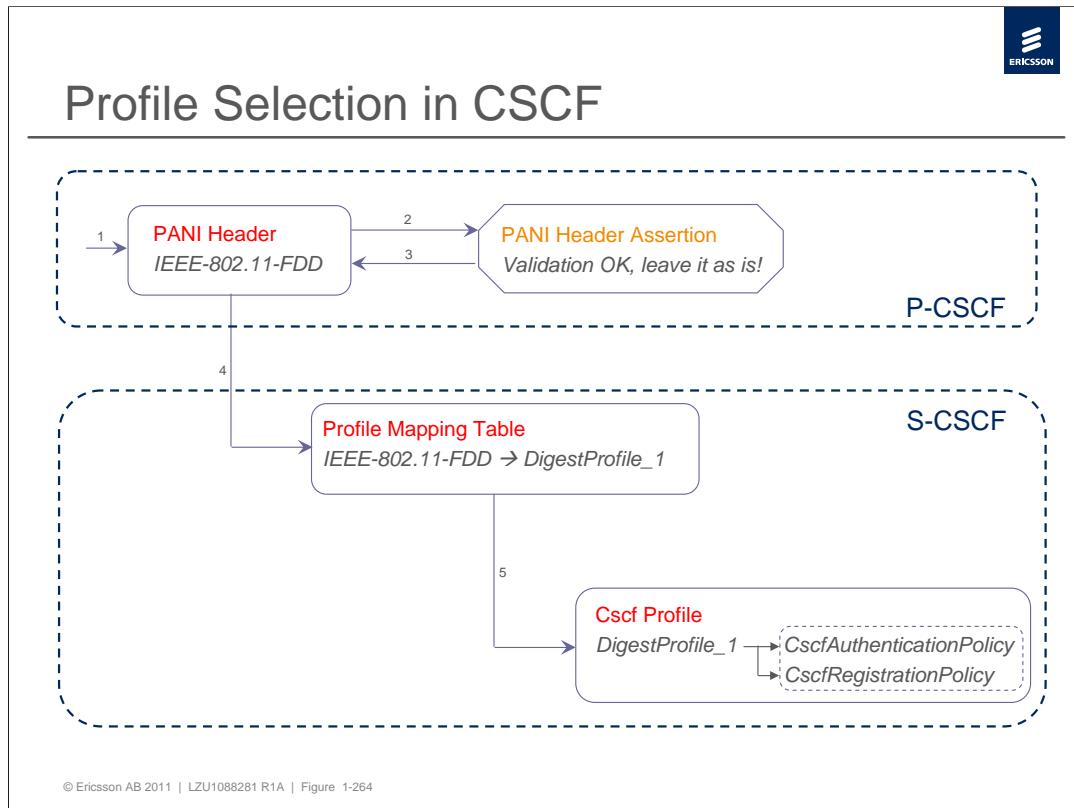
Selection of Authentication Method based on the Access Type

Selection of Authentication Method

- Different authentication methods are used for different access network types.
- Users are provisioned with different auth methods depending on the access.



By means of the Access Aware function, it is possible to differentiate the allowed authentication methods based on the access type. For instance, a user connecting from a fixed network could be authenticated using NBA or Digest, while a user connecting from a mobile network could be authenticated by using SSO or IMS AKA or Digest methods.



1. PANI Header is received in the SIP message specifying Broadband Access (*IEEE-802.11-FDD*)
2. If PANI Header Assertion is enabled, CSCF validates the received PANI Header. If validation is OK, the PANI Header is left unchanged, otherwise modifications might be required.
3. We assume that the SIP message has been sent by a trusted IP address, thus we can use the PANI Header "as is".
4. The value of the PANI Header is used to find a match towards a list specified by the parameter *CscfConfigProfileMappingTableEntry*.
5. The matching value will then point to a profile (*CscfProfile* in *CscfProfileGroup*). The profile specifies which Authentication and Registration Policies will be used. Several Authentication Policies can be created within the *CscfAuthenticationGroup*. In a similar way, several Registration Policies can be created within the *CscfRegistrationGroup*.



PANI Header Assertion Config

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn Quick Search

Explore Results Schema

World

- nodeName=al1tsp05
 - applicationName=CSCF
 - CscfAccessNetworkAssertionKey=0
 - CscfAuthenticationGroup=0
 - CscfCharging=0
 - CscfConfigProfileMappingTableGroup=0
 - CscfEmergencyGroup=0
 - CscfGenericNumberPortabilityKey=0
 - CscfHssQuarantineKey=0
 - CscfKey=0
 - CscfMedia=0
 - CscfNumPortabilityKey=0
 - CscfWifiContainerKey=0
 - CscfProfileGroup=0
 - CscfRegistrationGroup=0
 - CscfResourceBroker=0
 - CscfSipMsgPreProcessingKey=0
 - CscfUarRestrictionKey=0
 - CscfUnallocatedRoutingKey=0
 - Ecsckey=0
 - applicationName=DIA
 - applicationName=DNS
 - applicationName=ExtNetSelection

Connected To ldap://10.64.224.194:7423

HTML View Table Editor

attribute type	value
CscfAccessNetworkAssertionKey	0
objectClass	CscfAccessNetworkAssertion
groupId	0
ownerId	0
PcscfAccessTypeValidationEntry	192.168.100.0/24;IEEE-802.11:ADSL
PcscfPaniAssertionEnabled	TRUE
PcscfTrustedPaniGatewayEntry	10.64.229.132/32
permissions	9
shareTree	nodeName=al1tsp05
parent	

Submit Reset Change Class Properties

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-265

To turn on PANI Header Assertion, perform the followings steps:

- 1) Enable the function by setting the value of the parameter, *PcscfPaniAssertionEnabled*, to TRUE.
 - 2) If needed, define a list of IP addresses of trusted access gateways in parameter, *PcscfTrustedPaniGatewayEntry*. Each entry of the list is an IP address (subnet masked) of a trusted access gateway. PANI Headers of all messages coming from the trusted gateway would not need to be asserted. The PANI Headers of such messages are considered asserted and trustworthy.
 - 3) Define the parameter *PcscfAccessTypeValidationEntry*. This parameter is used to relate the IP address of a UE to its allowed access types. Each entry in this list contains valid access types and default access type of a given IP subnet. By default, the list is empty. Definition of default access type per subnet range is mandatory.
- PcscfTrustedPaniGatewayEntry: <IPaddress/netmask>*
PcscfAccessTypeValidationEntry:
<IPaddress/netmask>:<allowedAccessTypes>:<defaultAccessType>

Note: the default Access Type is used in case the source IP address is found in the list but the



Profile Mapping Tables

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn

Explore Results Schema

World

- nodeName=al1tsp05
 - applicationName=CSCF
 - CscfAccessNetworkAssertionKey=0
 - CscfAuthenticationGroup=0
 - CscfAuthentication=default
 - CscfAuthentication=Digest
 - CscfAuthentication=SSO
 - CscfCharging=0
 - CscfConfigProfileMappingTableGroup=0
 - CscfConfigProfileMappingTable=AccessType
 - CscfEmergencyGroup=0
 - CscfGenericNumberPortabilityKey=0
 - CscfHssQuarantineKey=0
 - CscfIkey=0
 - CscfMedia=0
 - CscfNumPortabilityKey=0
 - CscfNwifContainerKey=0
 - CscfProfileGroup=0
 - CscfProfile=DigestMin
 - CscfProfile=SSOMax
 - CscfRegistrationGroup=0
 - CscfRegistration=default
 - CscfRegistration=MaxRefresh
 - CscfRegistration=MinRefresh
 - CscfResourceBroker=0
 - CscfSipMsgPreProcessingKey=0
 - CscfUsRestrictionKey=0
 - CscfUnallocatedDroutingKey=0
 - CscfKey=0

Connected To ldap://10.64.224.194:7423*

attribute type	value
CscfConfigProfileMappingTable	<i>AccessType</i>
objectClass	CscfConfigProfileMappingTableClass
CscfConfigProfileMappingTableEntry	IEEE-802.11-FDD-DigestMin
CscfConfigProfileMappingTableEntry	3GPP-UTRAN-FDD:SSOMax
groupID	0
ownerId	0
permissions	9
shareTree	nodeName=al1tsp05
parent	

Submit Reset Change Class Properties

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-266

The value of the PANI Header is used to find a match towards a list specified by the parameter *CscfConfigProfileMappingTableEntry*.

It defines what configuration profile to be used for what access type. An access type can only exist once in the list but several access types can point to the same profile. A CscfProfile must have been configured in the LDAP interface before it can be pointed out to be used for a specific access type.

The syntax for this parameter is:

<AccessType>:<CscfProfile>

The screenshot shows the JXplorer LDAP browser interface. On the left is a tree view of the LDAP structure under 'cn=World'. A node named 'al1tsp05' is expanded, showing various attributes like 'applicationName=CSCF', 'CscfAccessNetworkAssertionKey=0', etc. On the right is a 'Table Editor' window for a 'CscfProfile' object. The table has two rows highlighted with red boxes: 'objectClass' with value 'CscfProfileClass' and 'DigestMin' selected in the dropdown, and 'CscfAuthenticationPolicy' with value 'Digest' and 'CscfRegistrationPolicy' with value 'MinRefresh'. Other visible columns include 'attribute type', 'value', and buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

Connected To 'ldap://10.64.224.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-267

The match found in the Profile Mapping Tables (please refer to previous slide) points to a profile (*CscfProfile* in *CscfProfileGroup*). The profile specifies which Authentication and Registration Policies will be used. Several Authentication Policies can be created within the *CscfAuthenticationGroup*. In a similar way, several Registration Policies can be created within the *CscfRegistrationGroup*.



Authentication Policies

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn =

Explore Results Schema

World

- nodeName=altsp05
 - applicationName=CSCF
 - CscAccessNetworkAssertionKey=0
 - CsdAuthenticationGroup=0
 - CsdAuthentication=default
 - CsdAuthentication=Digest
 - CsdCharging=0
 - CsdConfigProfileMappingTableGroup=0
 - CsdConfigProfileMappingTable=AccessType
 - CsdEmergencyGroup=0
 - CsdGenericNumberPortabilityKey=0
 - CsdHssQuarantineKey=0
 - CsdIkey=0
 - CsdMedia=0
 - CsdNumpPortabilityKey=0
 - CsdNwifContainerKey=0
 - CsdProfileGroup=0
 - CsdProfile=DigestMin
 - CsdProfile=SSOMax
 - CsdRegistrationGroup=0
 - CsdRegistration=default
 - CsdRegistration=MaxRefresh
 - CsdRegistration=MinRefresh
 - CsdResourceBroker=0
 - CsdSipMsgPreProcessingKey=0
 - CsdUaRestrictionKey=0
 - CsdUnallocatedRoutingKey=0
 - CscfKey=0

attribute type	value
CscAuthentication	Digest
objectClass	CscAuthenticationClass
CscAuthStalenessTimer	1440
CscAuthenticationPolicyEntry	Re-Registration:disabled
CscAuthenticationPolicyEntry	User Initiated De-Registration:disabled
CscAuthenticationPolicyEntry	INVITE:enabled
CscAuthenticationPolicyEntry	BYE:disabled
CscAuthenticationPolicyEntry	MESSAGE:disabled
CscAuthenticationPolicyEntry	SUBSCRIBE:disabled
CscAuthenticationPolicyEntry	NOTIFY:disabled
CscAuthenticationPolicyEntry	ACK:disabled
CscAuthenticationPolicyEntry	PRACK:disabled
CscAuthenticationPolicyEntry	INFO:disabled
CscAuthenticationPolicyEntry	REFER:disabled
CscAuthenticationPolicyEntry	CANCEL:disabled
CscAuthenticationPolicyEntry	OPTIONS:disabled
CscAuthenticationPolicyEntry	PUBLISH:disabled
CscAuthenticationProcedure	digest
CscNBAAccessNetworkType	
CscOverallAuthenticationPolicyEnabled	enabled
CscSipDigestAuthenticationNonceReusable...	10
CscSipDigestAuthenticationNonceTimeLength	900
CscSipDigestBlackListTimer	0
CscSipDigestMaxAuthenticationAttempt	3
CscSSOAuthenticationEnabled	FALSE
CscTrustedASEntry	10.64.227.198
CscTrustedASEntry	10.64.228.193
CscTrustedASEntry	10.64.228.195
CscTrustedGatewayEntry	10.64.227.192/32
CscTrustedGatewayEntry	10.64.229.164/32

Submit | Reset | Change Class | Properties |

Connected To ldap://10.64.224.194:7423'

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-268

Several Authentication Policies can be created within the *CscfAuthenticationGroup=0*. The *CscfAuthenticationClass* Object Class includes all the necessary parameters used for different authentication methods.

Note: It is important to understand that not all the parameters showed in the authentication policy are "access-aware". Parameters that are not "access-aware" can only be modified in the *CscfAuthentication=default* container.

In order to know if a particular parameter is "access-aware", please refer to CPI document "CSCF Common Configuration Management".

Registration Policies

attribute type	value
CscfRegistration	MinRefresh
objectClass	CscfRegistrationClass
CscfMaxContactsBehavior	2
CscfMaxNumberContactsPerUser	10
CscfRegistrationRefreshDefault	30
CscfRegistrationRefreshMax	60
CscfRegistrationRefreshMin	1
CscfUseUserContactIn3rdPartyReg	userContact
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=alitsp05
parent	

Connected To 'ldap://10.64.224.194:7423'

Several Registration policies can be defined under the *CscfRegistrationGroup=0*. The CscfRegistrationClass Object Class includes mainly parameters related to timers and max number of contacts.

CscfRegistrationRefreshMin specifies the minimum registration refresh time allowed by the CSCF (in minutes). Any registration request with a refresh time below this value is rejected.

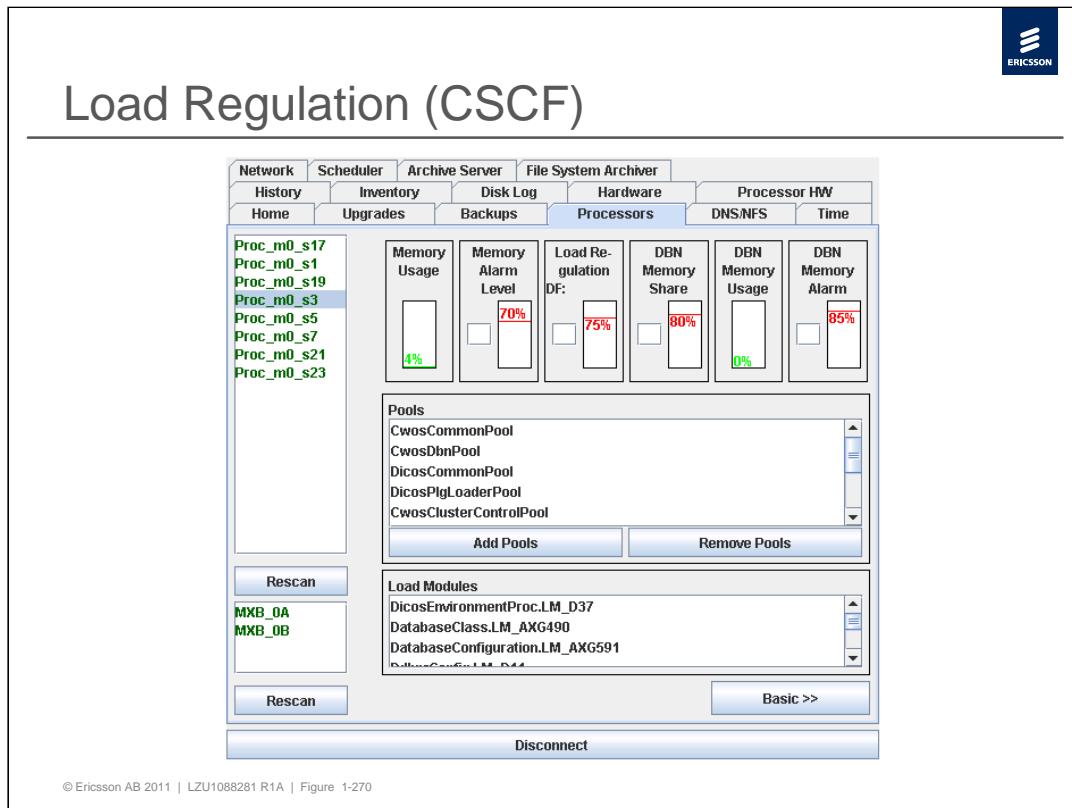
CscfRegistrationRefreshMax specifies the maximum registration refresh time allowed by the CSCF (in minutes). Any registration of refresh time specified greater than this value is reduced to this value.

CscfMaxNumberContactsPerUser specifies the maximum number of contacts that a user may have registered. In case this threshold is already reached and a user is trying to register another contact, the behavior is decided by the parameter *CscfMaxContactsBehavior*. Three options are available:

0 -> there is no restriction and the parameter *CscfMaxNumberContactsPerUser* is ignored

1 -> the new registration will be rejected

2 -> the new registration will replace the oldest contact for that user



Load Regulation

The load regulation limit, both with regards to processor load and to memory consumption, should not be set higher than 80%.

The Telorb Manager is used to set the load regulation limits.

In the figure the first frame, Memory Usage, shows the current memory usage of the selected processor.

The second frame, Memory Alarm Level, shows the level at which an alarm is raised. A Memory Usage Limit Exceeded alarm is raised if the Memory Usage goes above the specified limit. The limit can be manually changed.

The third frame is called Load Regulation. Load regulation is typically called by an application on entry, to determine whether there is sufficient capacity available to perform a task. If the CPU load rises above the specified load regulation level, applications which use load regulation will start to reject calls.

The fourth frame, DBN Memory share, sets the percentage of the total memory available for use by the database.

The fifth frame, DBN Memory Usage, shows what percentage of the memory available to the Database is currently in use: this is for information only, but it can be used to see if the settings for the DBN Memory Share are too low.

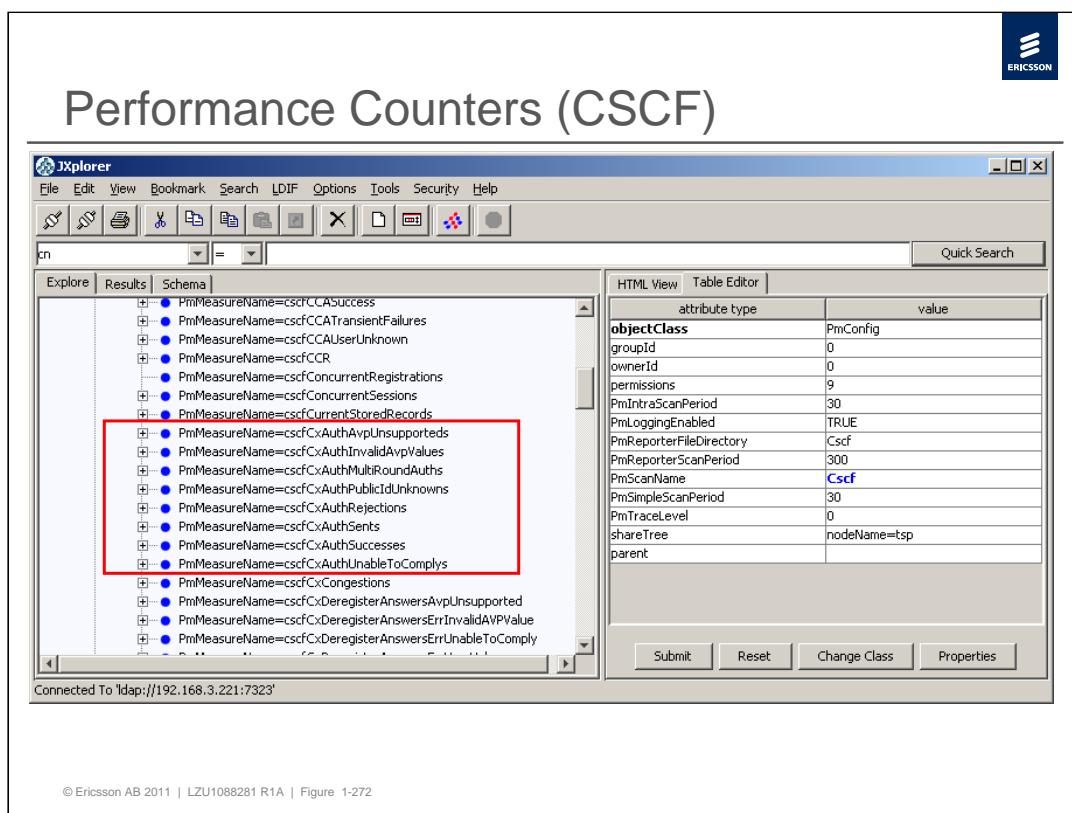
The sixth frame, DBN Memory Alarm, sets the level at which such an alarm is issued.

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view displays a node structure under 'World' with various entries like 'nodeName=al1tsp05', 'applicationName=CSCF', and several 'Cscf...' entries. On the right, the 'Table Editor' view shows a list of attributes and their values. The 'CscfSSOAuthenticationEnabled' attribute is set to 'FALSE'. Below it, four 'CscfTrustedASEntry' entries are listed with IP addresses: 10.64.228.193, 10.64.228.195, 137.58.246.150, and 10.64.227.198. These four entries are highlighted with a red border. Other visible attributes include 'CscfSipDigestAuthenticationNonceTimeLength' (900), 'CscfTrustedGatewayEntry' (10.64.227.192/32), 'CscfTrustedGatewayEntry' (10.64.229.164/32), 'CscfTrustedGatewayEntry' (10.64.229.232/32), 'CscfTrustedGatewayEntry' (10.66.32.97/32), 'groupId' (0), 'ownerId' (0), 'permissions' (9), 'shareTree' (nodeName=al1tsp05), and 'parent' (empty). At the bottom of the table editor are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A status bar at the bottom of the window indicates 'Connected To ldap://10.64.224.194:7423'.

Trusted Application Servers

CSCF has a list of configured trusted Application Servers. This list will be used when the Application Server initiates sending of SIP messages out of the blue (for example due to a wakeup call service) in order to verify if the Application Server is to be regarded as trusted network element and thereby allowed to send SIP messages to CSCF.

If the Application Server is not trusted, the SIP message will be rejected with the SIP response 403 User Agent not Authorized.



Performance Counters

In order to monitor the authentication function, if enabled, the counters in the figure should be monitored in order to see if unauthorized clients tries to access the IMS Core Network.



Default Security Configuration (HSS and SLF)

- › Installation of licensed modules only (HSS)
- › Secure protocols only (HSS and SLF)
- › Hiding of administrator and user passwords (HSS and SLF)

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-273

HSS includes the different SW elements IMS Subscription Manager (ISM), Subscription Data Access (SDA) modules, Packet Access Manager and Session Manager functions and SIM/USIM Authentication in WLAN function. All these elements are optional and one or several might not be part of the installation if not purchased. If this is the case, the software of the non purchased elements are delivered but it does not need to be loaded into the IOs. This avoids having extra software not used.

Ports likely to be attacked are not available at installation time. Standard ports defined for ftp (21), telnet (23) and http (8080) are not available in the system. Secure protocols are used instead, namely SSH and TLS.

The different passwords handled by the HSS are not visible through LDAP interface and not printed on the logs. This is the list of sensitive password parameters handled by the HSS: ISM and SDA Administrator password parameters, HSS-UserPassword parameters, HSS-XcapPassword parameters.

The SLF-Administrator Objects are: SLF-SystemAdministrator password, SLF-ConfigurationAdministrator password, SLF-ProvisioningAdministrator password, SLF-BrowserAdministrator password attribute.



HSS and SLF Security Recommendations

- › Updates of the HSS and SLF Software Version
- › Trusted Node Functionality in Session Manager Function (HSS)
- › Lock of SIP and XCAP for Users, Digest Authentication (HSS)
- › Change of Passwords for HSS and SLF Default Administrators
- › Secure Definition of Passwords in HSS and SLF
- › Barring of Service (HSS)
- › Data Access Control in SDA (HSS)

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-274

It is extremely recommended to get the latest version of HSS and SLF available. This secures that the latest security patches are added after initial delivery.

Session Manager function implements a mechanism to accept RADIUS requests only from those nodes provisioned as Network Access Server (NAS). The functionality is controlled by the *isTrustedNodeFunctionalityActivated* parameter.

ISM module keeps control of the number of consecutive failed Session Initiation Protocol (SIP) authentication attempts using digest authentication. If the number of consecutive failed authentication attempts reaches the limit, the private user identity is locked for authentication purposes. The state of the user for SIP authentication is visible via the parameter *HSS-SipLocked*.

The same functionality exists for XML Configuration Access Protocol (XCAP) authentication attempts. The state of the XCAP public identity is visible via the parameter *HSS-XcapLocked*.

This functionality is activated by default, by means of the parameter *HSS-AuthLock*. An alarm is also generated when the identity is locked, if parameter *HSS-AuthLockAlarm* is set. If the lock functionality is deactivated, a notification is generated instead.

Different administrators are created by HSS at installation time. It is recommended to change the default passwords defined in ISM (parameter *password*): *HSS-Ericsson-Administrator*, *HSS-SystemAdministrator* and *HSS-BrowserAdministrator*. Besides, it is recommended to change the passwords created in Session Manager function for a default administrator. It is also recommended to change the default passwords defined in SLF: *SLF-SystemAdministrator*, *SLF-ConfigurationAdministrator*, *SLF-ProvisioningAdministrator* and *SLF-BrowserAdministrator*.

It is recommended that all the passwords in the system conform to the following rules: they should not be the same as the username; minimum length of six letters, containing at least one non-alphabetical character as well as lower case and upper case letters too; passwords should be free of consecutive identical characters and should not be words or abbreviations that may be found in a dictionary.

In order to change the minimum length of the passwords used for SIP and XCAP authentication, *HSS-AuthMinPasswordLength* parameter should be set to a value equal or greater than six.

ISM provides the functionality of registration barring and session establishment barring. These functionalities might be used to prevent fraudulent use. Registration barring can be applied on subscriber and user level and it prevents the registration in the IMS domain. The barrings are set with the parameters *HSS-SubscriberBarringInd* and *HSS-UserBarringInd* for subscriber and user respectively. Session establishment barring can be applied on public identity level and it prevents the establishment of IMS sessions. The barring is set with the parameter *HSS-SessionBarringInd*.

SDA module provides mechanisms to control data access. A list of permissions is maintained for every defined Application Server where it is specified which Sh operations are allowed or rejected per Application Server.

SDA module also provides a mechanism to prevent Application Servers to get access to data of specific users. This policy is applied on user level by enabling the *HSS-PrivacyIndicator* parameter.

HSS and SLF Security Recommendations (cont.)

› Storage of the User Passwords (HSS)

attribute type	value
HSS-DigestAuthenticationDataName	HSS-DigestAuthenticationData
objectClass	HSS-DigestAuthenticationData
groupid	411
HSS-AuthDomain	isp.<HSS_AUTH_SERVER>@edu ims.se
HSS-AuthLock	TRUE
HSS-AuthLockAlarms	FALSE
HSS-AuthLockTimeWindow	5
HSS-AuthMaxPasswordLength	16
HSS-AuthMinPasswordLength	4
HSS-AuthNonceReusabilityLimit	10
HSS-AuthNonceTimeWindowLength	900
HSS-AuthNonceTimeWindowSize	6
HSS-AuthLogRequired	FALSE
HSS-AuthRealmName	edu.ims.se
HSS-AutRoundTripLimit	8
HSS-PwdEncrypt	TRUE
owner	4011
permissions	11
shareTree	nodeName=jambala
parent	

Connected To ldap://192.168.13.193:7429

ISM stores the User and XCAP passwords in plain text by default. The passwords are not visible through LDAP but are stored in the database in plain text. In order to store them in encrypted form the *HSS-PwdEncrypt* parameter needs to be enabled.



HSS and SLF Security Recommendations (cont.)

› Activation of Logging Functionality (HSS and SLF)

Screenshot of the JXplorer LDAP browser showing the configuration of the HSS-ISM-ConfigurationData object. The object has several attributes set to TRUE, indicating active logging.

attribute type	value
HSS-IsmConfigurationDataName	HSS-IsmConfigurationData
objectClass	HSS-IsmConfigurationData
ownerId	411
HSS-AuthenticationLogStatus	FALSE
HSS-DerouteMaxCallLegs	1
HSS-DerouteMaxSessions	1
HSS-LocationLogStatus	FALSE
HSS-MassiveUpdateAllowed	TRUE
HSS-MaxSimultaneousRequests	10
HSS-MaxNumPublicIpsPerUser	5
HSS-OAMLogStatus	FALSE
HSS-PerfEndScheduleTime	20080927T085857935
HSS-PerfInitialScheduleTime	20080927T085857935
HSS-PerfScheduleActive	FALSE
HSS-PerfStartStop	TRUE
HSS-RequestReattemptDelayTime	1000
HSS-RequestReattempts	5
ownerId	411
permissions	11
shareTree	nodeName=jambala
parent	

Logging function is essential to monitor the security and general operation of a node. They should be active in order to detect any fraudulent use.

Activation of ISM logs is done by setting the parameters: *HSS-LocationLogStatus*, *HSS-AuthenticationLogStatus* and *HSS-OAMLogStatus*. The following list shows the relevant security related events in ISM: User/Public Identity/Access Identifier unknown; Authorization denied; Message answered with Identity not registered; Public Identity unknown; Identity blocked; Unsuccessful authentication; Authentication attempted under suspicious circumstances.

Activation of SDA logs is done by setting the parameters: *HSS-SdaOamLogStatus* and *HSS-SdaServiceLogStatus*. The following list shows the relevant security related events in SDA: Operation not allowed; User data not available due to privacy restrictions; Subscription to notifications not allowed.

Activation of Packet Access Manager and Session Manager functions logs is done by setting the parameters: *isAppLogActive*, *isRadiusLogActive* and *isTracingLogActive*. The following list shows the relevant security related events in Packet Access Manager and Session Manager functions: Invalid RADIUS client; Invalid NAS; Invalid User; MSI Client Access Restriction Violation.

SLF has three different types of logging information, activation of ISM logs is done by setting the parameters: *SLF-SecurityLogStatus*, *SLF-OAMLogStatus* and *SLF-DiameterLogStatus*.



IPSec

- › HSS and CSCF is enabled to communicate securely with other core network elements based on the use of the Zb interface
- › Zb interface makes use of IPsec in order to achieve confidentiality, integrity, authentication and anti-replay protection.
- › This feature provides secure communication between IMS nodes on interfaces that has high security needs like Charging, O&M, and LI.

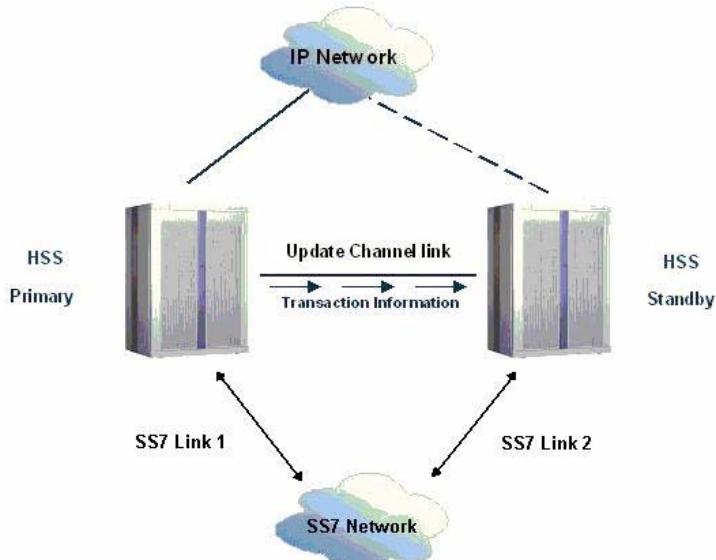
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-278

HSS and CSCF are enabled to communicate securely with core network elements based on the use of the Zb interface (specified in 3GPP TS 33.210, “IP network layer security”). This interface is intended for use between nodes residing within the same security domain, and it is based on the use of IPsec, with Encapsulating Security Payload (ESP) in tunnel mode and Internet Key Exchange (IKE).

In order to run traffic through the Zb interface, an IPsec tunnel must be configured. A tunnel is configured between a source end point (IP address and port) and a destination end point (IP address and port). For each tunnel, authentication methods and algorithms are also configured.

With an IPsec tunnel configured, all traffic between the end points are authenticated and encrypted.

HSS/SLF Geographical Redundancy general schema



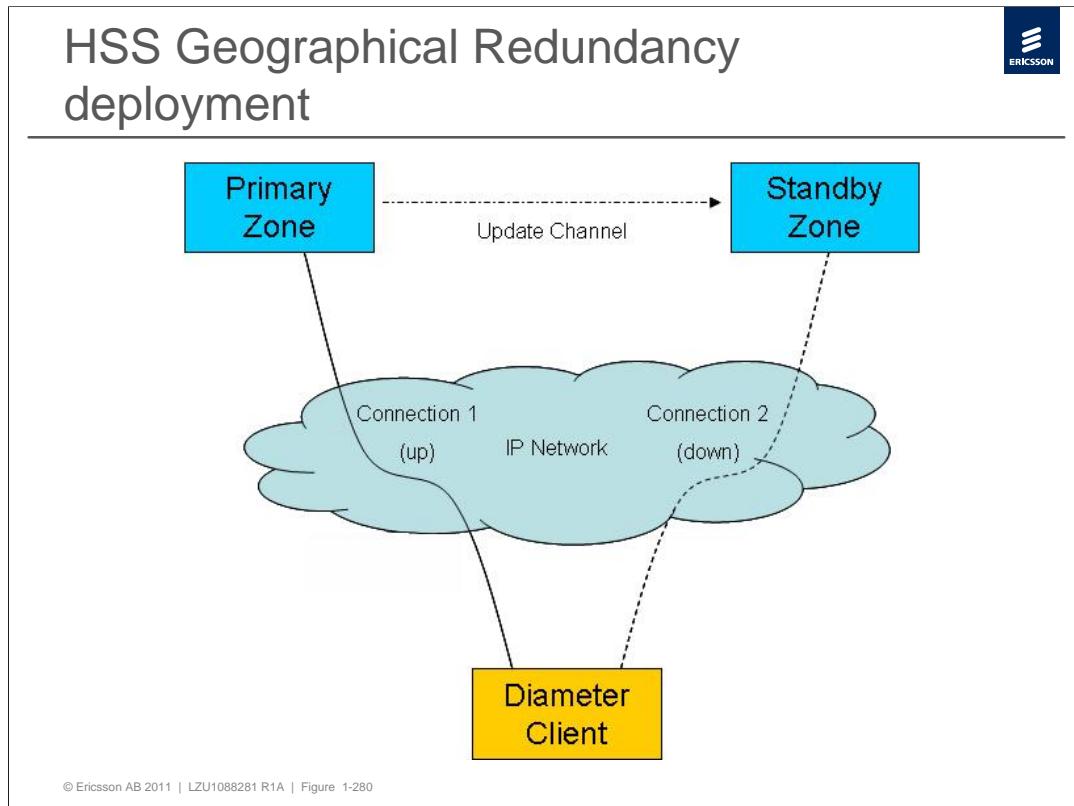
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-279

Geographical Redundancy provides protection against disaster situations such as fire or earthquakes and reduces non-availability caused by outages, which enhances the In Service Performance (ISP). Geographical Redundancy in HSS is supported for all the modules including SLF.

HSS in a Geographical Redundancy configuration is composed of two HSS single nodes, or zones, interconnected by point to point or dedicated connection, called Update Channel link.

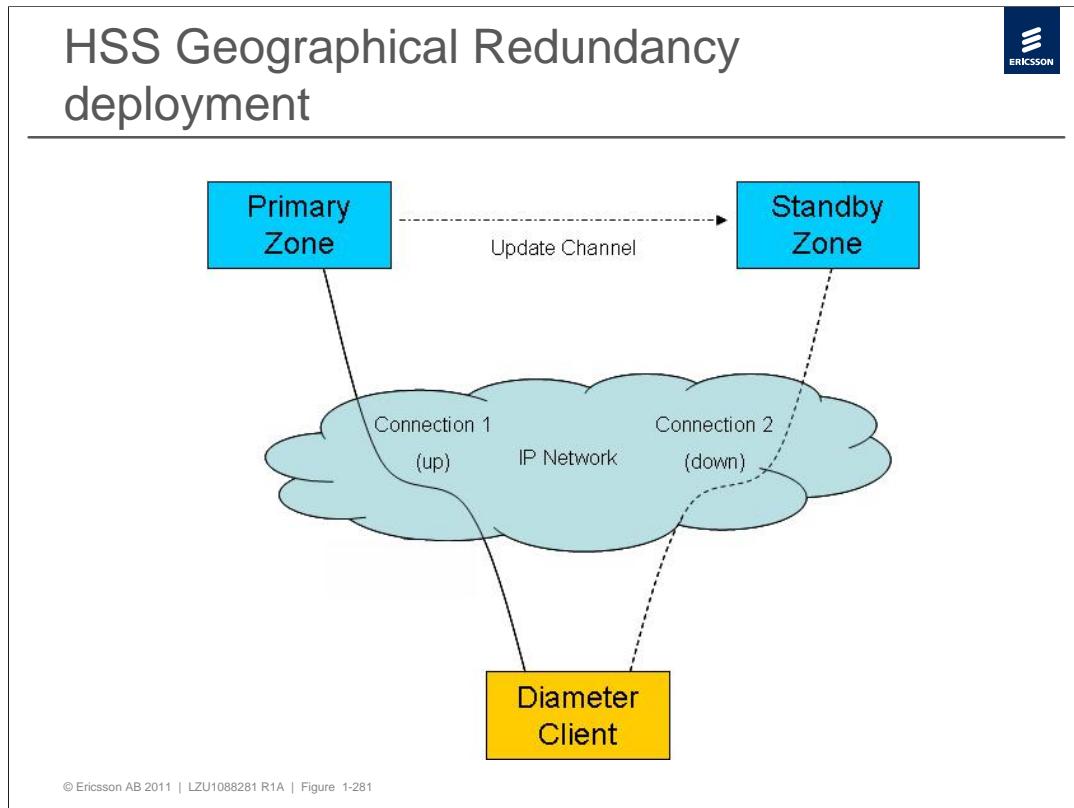
The Update Channel link is used to transfer changes in database information done in the Primary zone to the Standby zone. Standby zone processes it, and updates its state.

During normal operation, both nodes work in a Primary/Standby model, where the primary HSS processes the incoming traffic and the standby keeps the state of the primary to be ready to process the incoming traffic when the primary one can not handle it.



The HSS Geographical Redundancy solution is based on using local addresses. Diameter connections from the client nodes need to be set up to both the preferred primary and the preferred standby zones, using the local address of each zone (using the Multiple TCP connection function or SCTP). A connection to the zone that is currently standby is refused by Diameter, meaning that all communication will go to the primary zone over another connection. At a zone transfer, the connection to the previously primary zone is lost, and a new connection is automatically established to the zone becoming the new acting primary zone.

When SLF is deployed using the Primary/Standby model, it works the same way as the rest of the HSS modules.



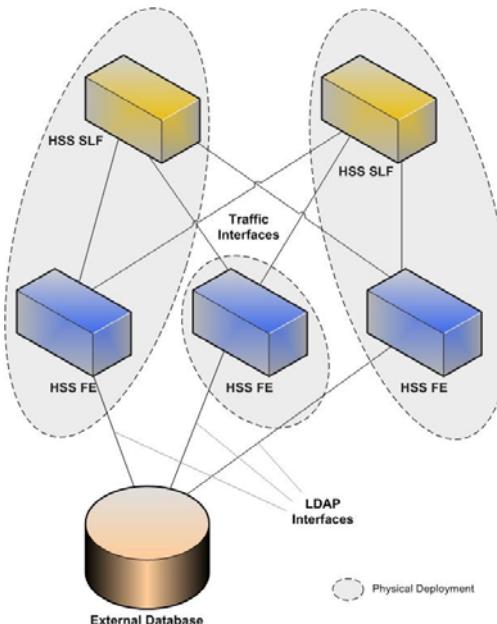
Two aspects are considered: **Database replication** (which data are replicated) and **Database Consistency** (how the HSS assures the database consistency in case of unpredictable crash).

Database replication: In order to make a transparent switching in case of failure between primary and standby HSS, the following information is replicated by automatic mechanisms in both nodes:

- The HSS Configuration information except SS7 configuration, is replicated.
- The HSS Provisioning information, that is, information related to Subscribers, Users and Public Identifications is replicated.
- The HSS Dynamic Traffic data can be:
 - Replicated such as IMS registration information, IMS localization data, transparent data, GPRS Location Information.
 - Non replicated such as the temporary authentication information (nonce and authentication vectors).
 - Non replicated, but kept synchronized such as Authentication Vector Generator (AVG) Sequence Number (SQN).

Database Consistency: The database synchronization mechanism is automatically performed as configured, but if something wrong occurs, HSS guarantees the execution of the pending database updating that was already performed in the primary before the failure and not synchronized in the standby.

SLF High Availability



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-282

High availability in the network can be achieved by deploying multiple active geographically distributed SLF entities, all actively sharing the traffic load.

From the HSS Diameter Clients perspective, routing towards multiple active SLF nodes is based on standard Diameter Realm-based Routing, using a static round-robin load distribution mechanism across all deployed SLF instances.

When SLF is configured as DbManager, in order to equally share the traffic load across all deployed SLF instances, all SLFs need to have the same provisioning data, and the Provisioning System needs to multicast the same service orders to all SLFs deployed.

When SLF is configured as Load Balancer, no provisioning is required.

A dimensioning exercise is required to deploy the active load-sharing SLF cluster in high availability configuration. In practice, if any of the SLF entities becomes unavailable, the related traffic will be implicitly and equally distributed across the remaining SLF entities in the network.

From the HSS RADIUS Clients perspective, all SLF entities are deployed as an active load-sharing cluster of RADIUS Proxy entities.



Chapter 8 – Session Establishment

1. Introduction
2. Architecture
3. User Interface
4. Fault Management
5. Configuration Management
6. Performance Management
7. Security, Authentication and Redundancy
- 8. Session Establishment**
9. Configuration Examples

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-283





IMS Address Types

Address Type	Example	Usage
Private User Identity	Xyz123@domain.com	Master identity, used for authentication/authorization, etc.
Public User Identity	SIP:john.smith@domain.com	The public SIP address that can be used for addressing of terminating SIP sessions towards the user.
Contact Address	468123456@138.85.84.61:5060	IP address used to address the User Agent where currently registered (dynamic address).
E.164 Number	+46 8 123456	A public, international phone number associated with the user, which can be used for addressing of terminating SIP sessions towards the user.
Extension Number	3456	The user's extension number within a group.
Tel URI	tel:+46709123456	The Tel URI is a public, international phone number (E.164 number) that can be used for addressing of terminating SIP sessions towards the user.

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-284

IMS addressing is a combination of two technologies - Telephony and Internet. A SIP URI contains a host and optionally a user name, similar to an e-mail address. E.164 numbers, used in telephony systems, can be included in URIs instead of user name.

Domains

The Public & Private user IDs identify the user's home domain (e.g. 'domain.com' above).

Private User ID

A private user identity identifies a subscriber and is used for authentication when HTTP digest is used as the authentication method. The UE includes the private user identity in the REGISTER message.

Public User ID

The public user identity is defined in the document 'Numbering, addressing and identification (Release 6)' 3GPP TS 23.003. It is used to establish sessions between users.

- A public user identity with the SIP URI format (example **sip:ronald.underwood@example.com**)
- A public user identity with the TEL URI format (example **tel:+46709860422**).

E.164 number

The E.164/MSISDN number can be transported as a Tel URI or as telephone digits in a SIP URI.

An example of an E.164/MSISDN number transported in a Tel URI is: **tel:+4687197378**

An example of an E.164/MSISDN number transported as telephone digits in a SIP URI is:

sip:4687197378@my-operator.net;user=phone



Information Storage (before, during and after registration)

Node	Before Registration	During Registration	After Registration
UE – In local Network	Home domain Proxy or SBG name/address	Same as before registration	Same as before registration
P-CSCF in local network	-	UE IP address (or SBG) Public user ID	UE IP address (or SBG) Public user ID S-CSCF name/address
I-CSCF in home network	HSS name/address S-CSCF preferences	S-CSCF name/address P-CSCF network ID	Same as before registration
HSS in home Network	User service profile	User service profile P-CSCF network ID S-CSCF name/address	User service profile S-CSCF name/address
S-CSCF in home network	No presence state information	HSS address User service profile P-CSCF name/address P-CSCF network ID Public user ID UE IP address & port	Same as during registration May have presence state information

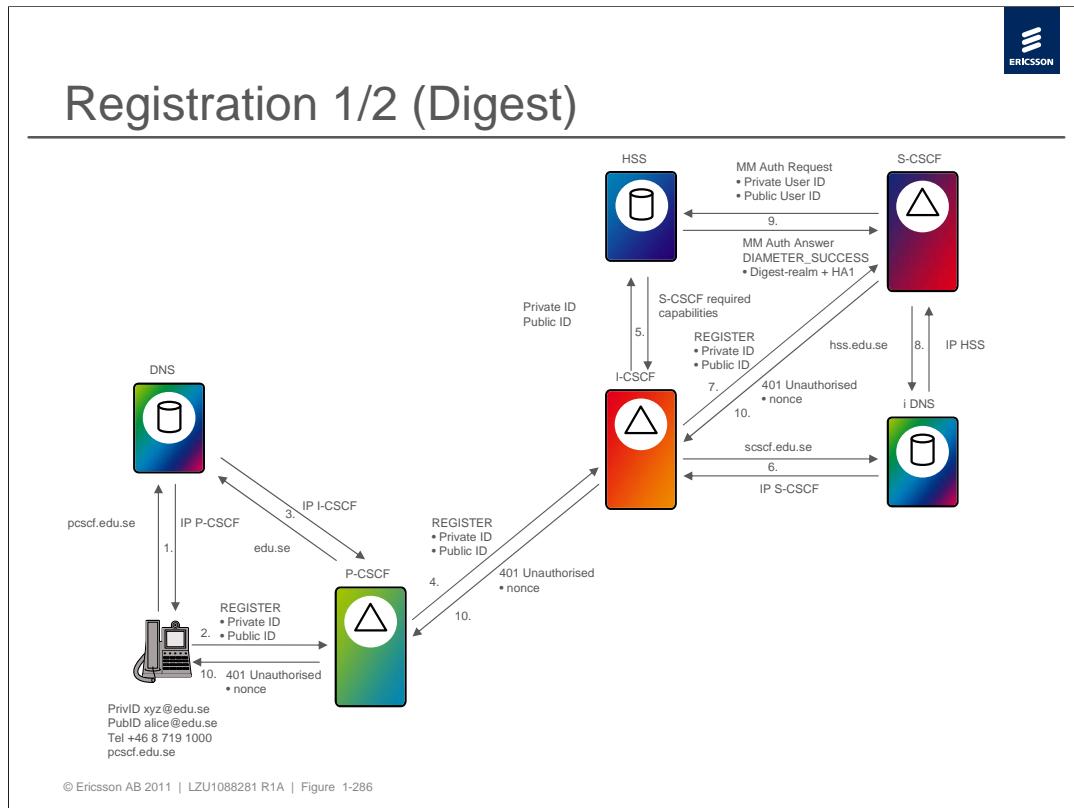
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-285

A prerequisite for all end user services is that the user is registered on an S-CSCF in the home network. A user registers from the UE by sending a SIP REGISTER request to the network.

This REGISTER request includes an IP address with the user's current location and the Public and Private User Identities. On receipt of the REGISTER message the IMS network:

- Checks if the user belongs to the home domain, i.e. that the user has a subscription.
- Authenticates the user, if required.
- Allows the user to register in the system.

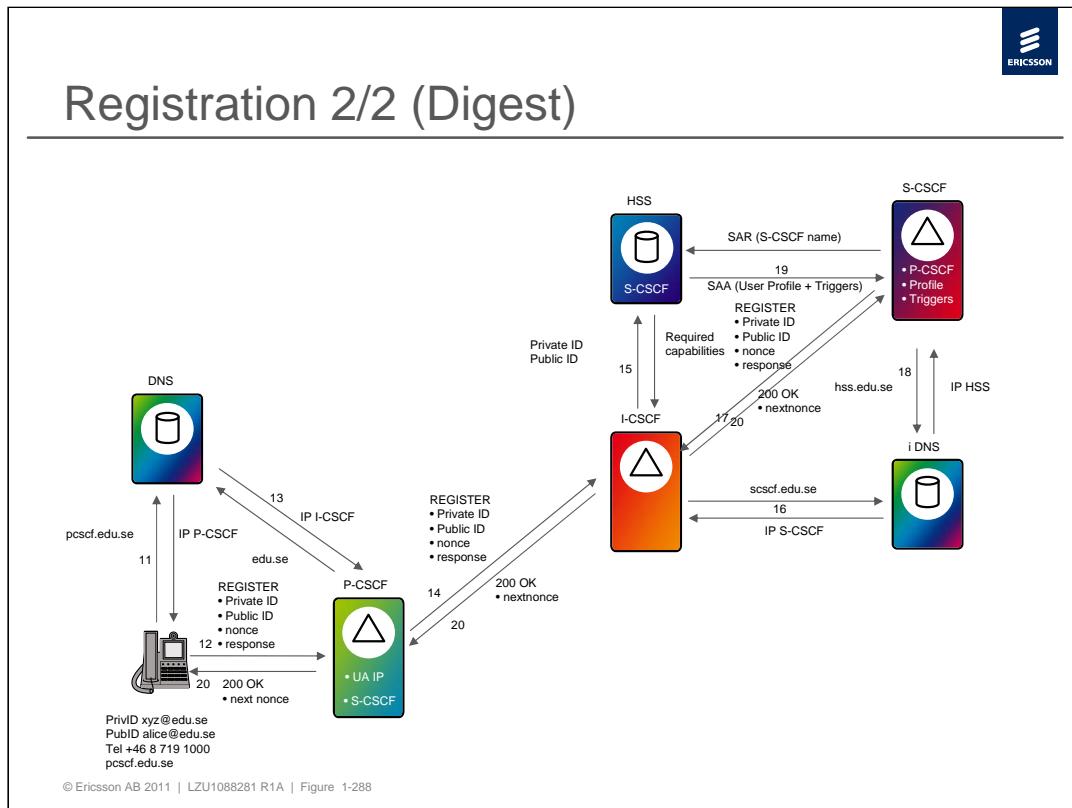
The figure shows some of the main information stored in the different nodes before, during, and after registration



The figure shows a *simplified* signal flow for registration. Note that for clarity, the A-SBG is not shown and not all DNS queries are shown. In reality, most nodes will query DNS to find the IP address of the node to which the SIP and Diameter messages must be sent.

1. Alice initiates registration. The IP address of her P-CSCF is obtained from DNS using the proxy address that is pre-configured in the UE (pcscf.edu.se in the figure).
2. The SIP Client sends a SIP REGISTER message to the P-CSCF, routed towards her home network domain 'edu.se' (pre-configured in the User Equipment). The REGISTER includes Alice's public ID to be registered (alice@edu.se) as well as her private user ID for authentication and the IP address/port of the UE-A. The REGISTER is routed via an A-SBG if present.
3. The P-CSCF stores the UE-A contact (IP) address and requests the IP address of the server for Alice's home domain (edu.se). DNS returns the IP address of the I-CSCF in the domain edu.se.
4. The P-CSCF proxies the REGISTER to the I-CSCF, first adding a Path header containing the P-CSCF-URI to inform the S-CSCF where to route future terminating requests for the user.
5. The I-CSCF sends a Diameter Cx USER AUTHORIZATION REQUEST (UAR) containing the user's private and public address to the Home Subscriber Server (HSS). If the private and public user IDs exist on the HSS, the HSS returns the required S-CSCF capabilities to the I-CSCF.
6. Based on the received information (and locally configured data), the I-CSCF selects a suitable S-CSCF and obtains the S-CSCF's IP address from the internal iDNS.

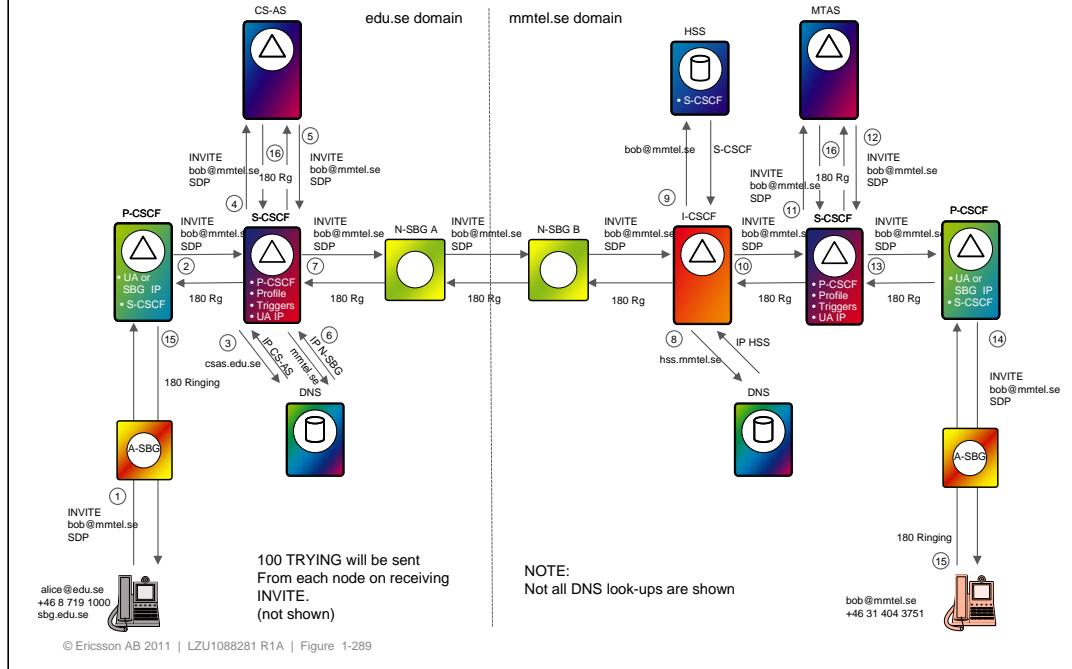
7. The I-CSCF forwards the REGISTER to the selected S-CSCF. The S-CSCF stores the contents of the REGISTER Path header (the P-CSCF address; to be used for routing terminated requests towards this public address) and the UE-A IP address (received in REGISTER Contact header). If optimized authentication is enabled in the S-CSCF, the Optimized Digest function will store a state (authentication IP Address) with the Served User's IP address and all IP addresses of the intermediate nodes.
8. The S-CSCF obtains the IP address of the HSS from DNS.
9. S-CSCF sends a MULTIMEDIA AUTHENTICATION REQUEST (MAR) to HSS in order to obtain an Authentication Vector, consisting of Digest-realm and HA1 password.
The S-CSCF stores the values received in the MULTIMEDIA AUTHENTICATION ANSWER, generates a “nonce” (a unique randomly generated challenge) and, together with the user password, calculates the expected response.
10. The S-CSCF returns 401 UNAUTHORISED towards the UE-A. The message includes the challenge to the user (the “nonce” value).



11. The UE takes the “nonce” and the user’s password and applies the MD5 algorithm to compute a “response”. It then obtains the IP address of the P-CSCF from DNS.
- 12 – 18. The UE sends a new REGISTER message which includes the “nonce” and “response” values to the P-CSCF and the process described above (points 2 to 9) is repeated.
19. The S-CSCF checks that the received “nonce” and expected “response” values are correct. If so, the S-CSCF informs the HSS that the user has been registered by sending a SERVER ASSIGNMENT REQUEST (SAR) containing the S-CSCF name to be used for routing terminating requests towards the user.
The S-CSCF obtains the User’s Profile from the HSS included in the SERVER ASSIGNMENT ANSWER (SAA). The returned information includes CS-AS trigger filtering criteria, CS-AS address information and all public user identities associated with the subscription (to be implicitly registered).
20. The S-CSCF sends a 200 OK response to the P-CSCF indicating that the registration was successful. The 200 OK contains the “nextnonce” (to be used for authentication of a subsequent SIP Request) that was created by the S-CSCF, as well as a Service Route header containing the S-CSCF URI (to be used for routing of subsequent originating SIP requests from the P-CSCF to the S-CSCF). In addition, the 200 OK contains a P-Associated-Id header containing a list of all the Public User Identities that have been registered (explicitly and implicitly).

The P-CSCF saves the S-CSCF URI and the Public User IDs and associates them with the UE-A. The P-CSCF then forwards the 200 OK response to the UE-A.

SIP to SIP Session part 1



An example of the signalling flow for a call between two IMT users in different domains is described in the figure. Alice wishes to invite Bob to an audio or video call and uses Bob's public SIP:URI 'bob@mmtel.se'.

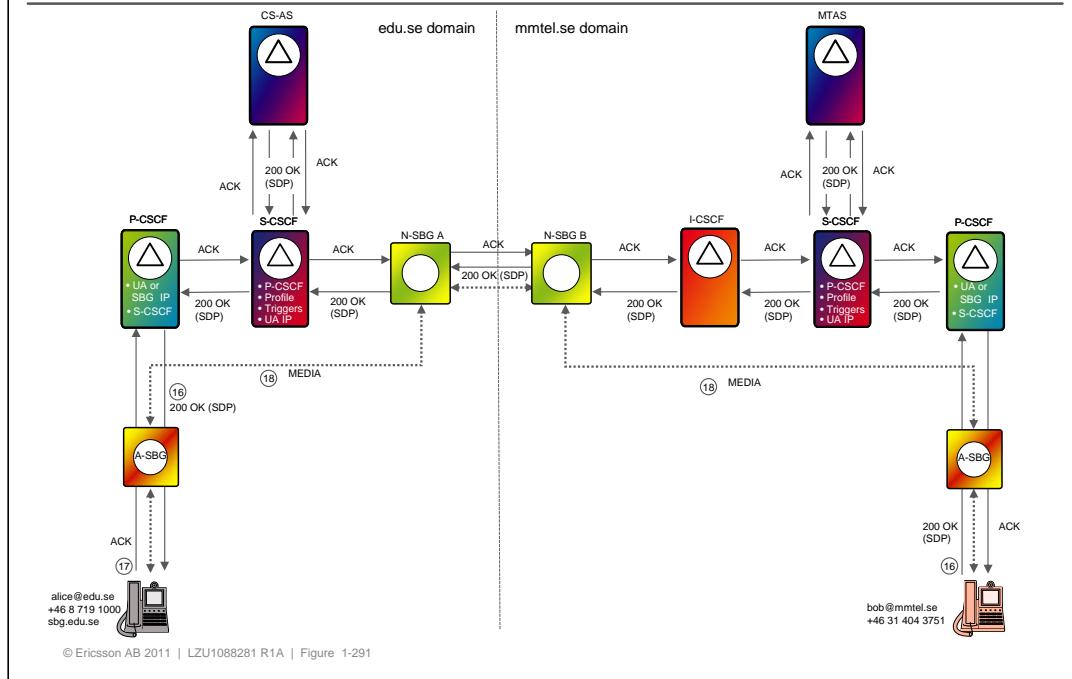
The flow diagrams show the position and function of the Session Border Gateways on the Access network (A-SBG) and between networks (N-SBG).

INVITE

1. Alice selects Bob's Public SIP identity and requests an audio call (for example). Her UA sends the SIP INVITE to the A-SBG. The A-SBG analyses the content of the INVITE, replaces Alice's IP address and RTP port with its own (NAT) for firewalling and forwards the INVITE to the Proxy CSCF. The INVITE includes details of the session requested in the SDP including – type of session ('audio'), a list of audio Codecs supported by Alice's UA, and the IP address for RTP.
2. The P-CSCF forwards the INVITE to the S-CSCF.
3. The S-CSCF checks Alice's Triggers. Originating INVITEs trigger the Centrex Application Server, CS-AS. S-CSCF obtains the IP Address for CS-AS by querying the internal iDNS.
4. The INVITE is sent to CS-AS.
5. CS-AS checks Alice's profile data to see if the call is allowed and executes Alice's outgoing services, if any. The INVITE is then returned to the S-CSCF.
(An example of an outgoing service – if Alice and Bob are members of a Group and Alice had dialled Bob's extension, CS-AS would insert Bob's full E.164 number in the INVITE).

6. S-CSCF needs to find where to route the INVITE. It sends the FQDN for Bob (mmtel.se) to DNS which returns the IP address to the N-SBG A, indicating the call needs to go outside Alice's home domain.
7. S-CSCF sends the INVITE to N-SBG A. N-SBG A will be configured to send messages for mmTEL.se to the N-SBG for that domain 'N-SBG B'.
N-SBG A replaces the IP address & RTP port in the message with its own values (for firewalling) and forwards the INVITE to N-SBG B.
N-SBG B does the same – replaces the IP address and RTP port with its own and forwards the INVITE to the I-CSCF for mmTEL.se (after a DNS look-up).
8. I-DNS needs to find the S-CSCF where Bob is registered. It obtains the IP address for the HSS.
9. I-CSCF sends a Diameter request to HSS with 'bob@mmtel.se'. HSS responds with the name of the S-CSCF where Bob is registered.
10. I-CSCF forwards the INVITE to the S-CSCF.
11. S-CSCF examines Bob's incoming INVITE Triggers. A 'terminating' INVITE triggers Bob's CS-AS.
12. The CS-AS examines Bob's profile and incoming services. It then returns the INVITE to the S-CSCF. The CS-As may modify the INVITE based on Bob's services and profile. For example if Bob has Call Forwarding Always' active, CS-AS will replace Bob's SIP URI with the address indicated in Bob's services data (previously provisioned by Bob using the Web interface). The INVITE will be returned to S-CSCF and will then be routed to this new address.
13. S-CSCF forwards the INVITE to the P-CSCF for Bob. Stored during Registration.
14. P-CSCF forwards the INVITE to Bob's A-SBG, also stored during Registration. A-SBG replaces the IP address and RTP port with one of its own and sends the INVITE to Bob's UA.

SIP to SIP Session part 2



180 Ringing

15. Bob's UA alerts Bob and returns a Provisional Response, '180 Ringing' which is routed via all of the relevant nodes to Alice. Alice's UA informs Alice that Bob is being alerted.

ANSWER and 200 OK

16. Bob answers the call and his UA SIP Client sends a Final Response, '200 OK', which is routed through all relevant nodes back to Alice. The 200 OK advises the nodes that the call has been answered. The S-CSCF, CS-AS and N-SBG in each domain can all generate Diameter Charging Requests to the Multi Mediation node to start changing for the call. The 200 OK includes Bob's SDP – indicating acceptance of the session type, listing Codecs supported by Bob's UA and advising Bob's IP Address and RTP port for media. Each SBG will replace the IP address and port received in the 200 OK with its own, before forwarding on.

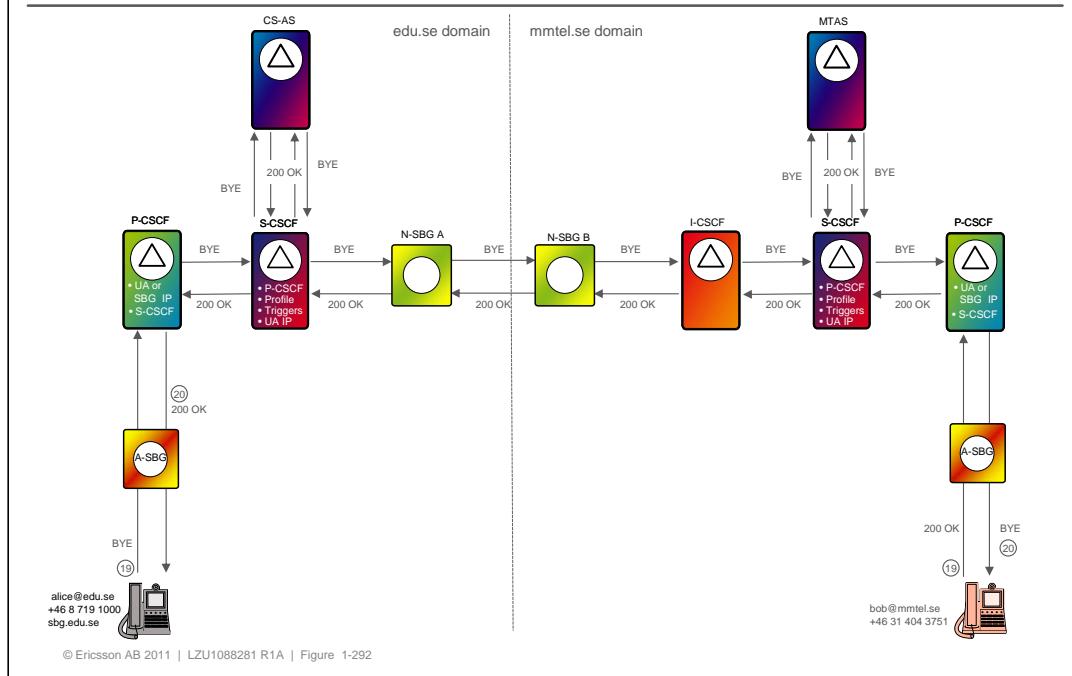
ACK

17. Alice's UA sends a SIP ACK to acknowledge the final response to the INVITE.

Media Established

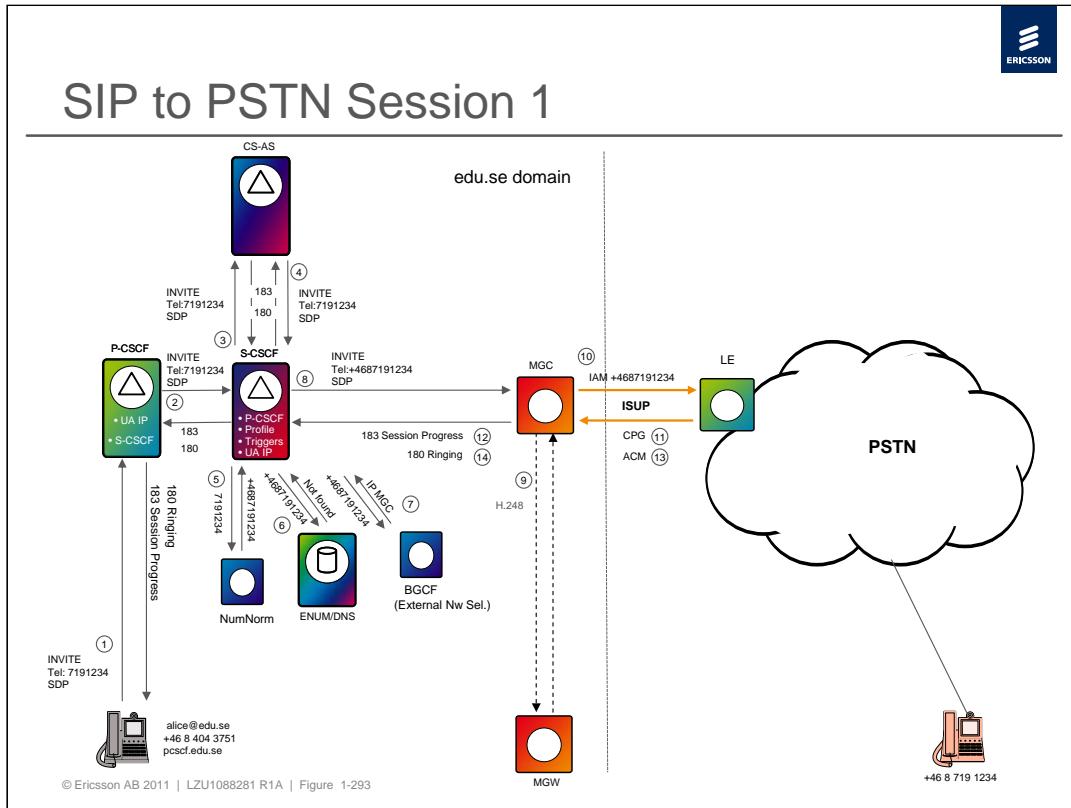
18. Media (speech) can now be sent and received by the two UAs. Alice's UA sends the RTP media packets to the A-SBG IP address & port received in the 200 OK. The A-SBG opens a 'pinhole' through its firewall, between the incoming RTP port and the outgoing port, which forwards the IP packets to the N-SBG. The N-SBG A opens a similar pinhole and so on to Bob's UA. In this way the SBGs firewall the media stream from Alice to Bob. In the backward direction, Bob's UA sends Bob's RTP packets to the A-SBG IP address and port received in the INVITE. The A-SBG pinhole for this session forwards this on to the N-SBG B IP address and port it received in the INVITE and so on. In this way the SBGs firewall the media stream from Bob to Alice.

SIP to SIP Session part 3



Session Release

19. Either user can clear the call. Here Alice hangs up and her UA sends SIP **BYE** to Bob via all the relevant nodes, so that they also know the call has ended and can for example, reset data and send final Diameter charging requests to Multi Mediation to stop charging. The SBGs close the firewall ‘pinholes’ they opened for the RTP media packets.
20. Bob’s UA acknowledges the **BYE** with success – ‘200 OK’



An example of the signalling flow for a call from an IMT user to a PSTN user is described in the figure. Alice wishes to invite user with E.164 number +46 8 719 1234. It is assumed the users are in the same area, so Alice keys the number without country code and area code i.e. '719 1234'.

In this example, A-SBG is not used.

INVITE

1. Alice makes a 'telephone' call and keys the local phone number '7191234'. After querying DNS, her UA sends a SIP INVITE to Tel:7191234 towards the P-CSCF.

The INVITE includes details of the session requested in the SDP including – type of session ('audio'), a list of audio codecs supported by Alice's UA, and the IP address for RTP.

2. The P-CSCF forwards the INVITE to the S-CSCF.
3. The S-CSCF checks Alice's Triggers. Originating INVITEs trigger the Centrex Application Server, CS-AS. S-CSCF obtains the IP Address for CS-AS by querying the internal iDNS and the INVITE is sent to CS-AS.
4. CS-AS checks Alice's profile data to see if the call is allowed and executes Alice's outgoing services, if any. The INVITE is then returned to the S-CSCF.

Number Normalization

5. The S-CSCF sees that the INVITE is addressed to a telephone number and sends the number to Number Normalization (NumNorm), which converts it to a full E.164 number.

ENUM

6. The S-CSCF needs to check if the telephone number relates to a SIP user in the domain. It sends the number to ENUM to analyze. If there is a match then the ENUM returns the user's SIP:URI, if not then ENUM indicates 'not found'. The telephone number must exist in another network (assuming it is a valid number).

External Network Selection

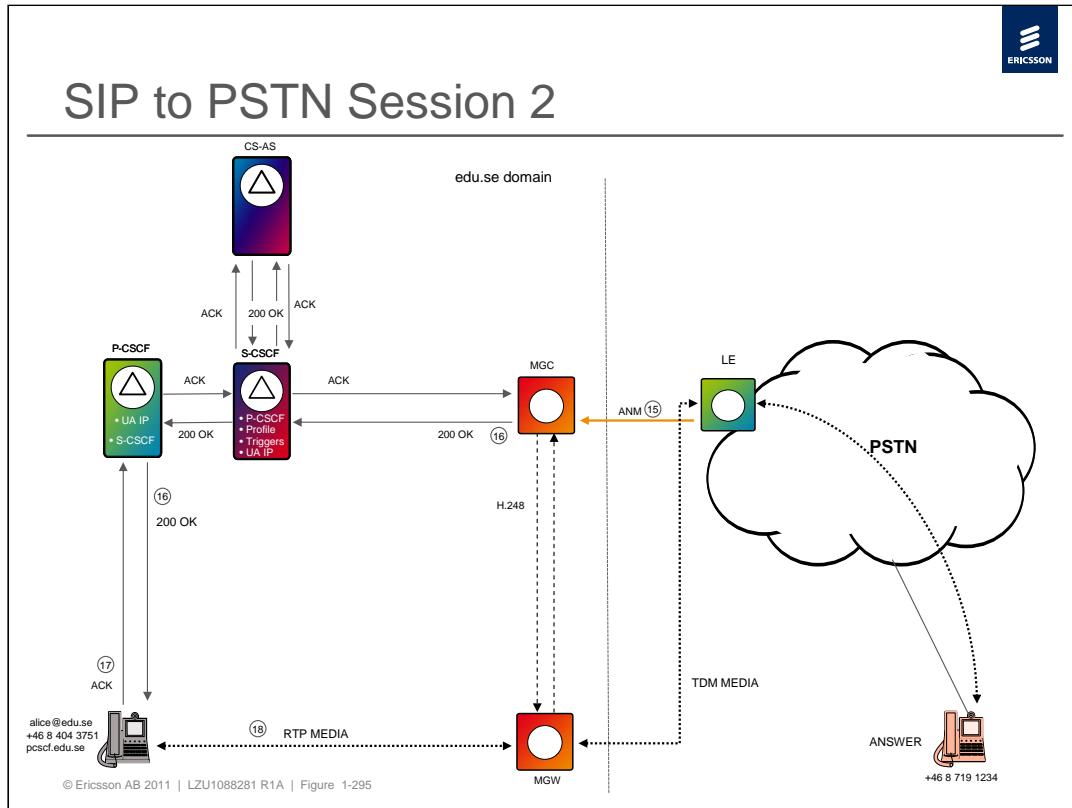
7. The S-CSCF now needs to find where to route the INVITE. It queries the External Network Selection function (Called 'Breakout Gateway Control Function 'BGCF' in 3GPP). The BGCF returns the identity of the gateway with access to the external network hosting the telephone number. This could be a N-SBG if the number exists in another VoIP network or a Media Gateway Controller 'MGC' if the user is a PSTN or Mobile subscriber. In this example it is assumed the user is in the PSTN.
8. The S-CSCF queries DNS and sends the INVITE to the MGC.
9. MGC requests an IP address and RTP port from MGW using H.248.
10. MGC selects a free outgoing trunk circuit (timeslot in an e1) on the TDM side, maps the SIP INVITE to an ISUP Initial Address Message 'IAM', inserts the Telephone number and TDM circuit identity and sends the IAM to the PSTN Local or Transit exchange.
11. The PSTN node returns ISUP Address Complete Message 'ACM' to MGC and proceeds to route the call through the PSTN to User B.

SIP 183 Session Progress

12. MGC maps the CPG to a SIP 183 Session Progress message and sends it to Alice via the relevant nodes .

180 Ringing

13. User B's telephone rings and the PSTN returns ISUP ACM with alerting indication to MGC.
14. MGC maps the ACM to a SIP 180 Ringing message and sends it to Alice via the relevant nodes. Alice's UA indicates that the called party is being alerted.



Answer & 200 OK

15. The called party answers and an ISUP Answer Message 'ANM' is sent from PSTN to MGC.
16. MGC maps the ISUP ANM to a SIP 200 OK message, inserts the selected MGW IP Address and RTP port in the SDP and sends it to Alice via the relevant nodes.

ACK

17. Alice's UA returns a SIP ACK to acknowledge the final response to the INVITE.

Media Established

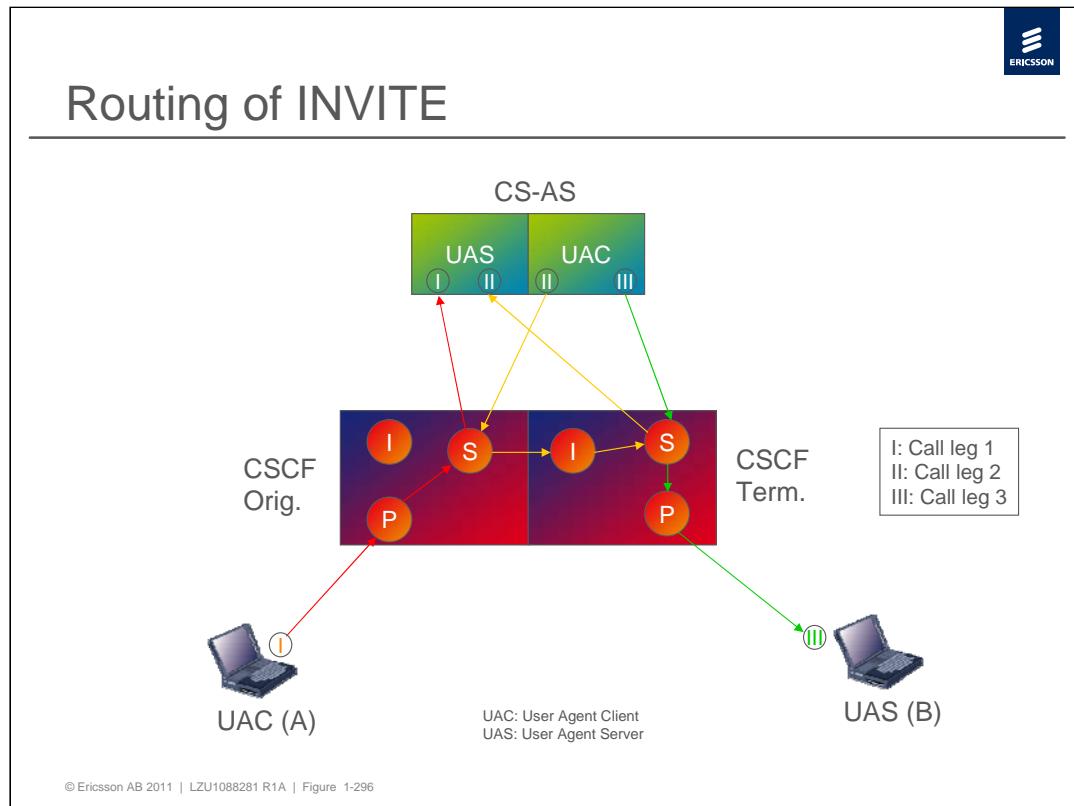
18. When the MGC receives the ACK, it requests the MGW to establish a media connection between the allocated IP address and port on the IMT side, and the e1 & timeslot on the PSTN side. The MGW performs the transcoding between the two networks, mapping the RTP media to TDM and vice-versa.

The media stream is now established.

Clearing - BYE

When Alice hangs up, her UA sends a SIP BYE message to the MGC. The MGC

- Returns a SIP 200 OK to Alice;
- Maps the BYE to an ISUP Release Message 'REL' to the PSTN;
- Signals to the MGW to tear down the media connection.



The figure shows how the INVITE messages are routed when the P, I, and S-CSCF functions are co-located within the same TSP platform. The routing of INVITE will be the same as when the functions are distributed on different TSP platforms because the CSCF functions will be divided into originating and terminating sides.

A session will always consist of three call legs which will have unique Call IDs.

The picture shows the typical behaviour of a B2B-UA (Back-to-Back User Agent). The AS works as a B2B-UA in the example above, thus it initiates a new call leg (with unique Call ID).



Chapter 9 – Configuration Examples

1. Introduction
2. Architecture
3. User Interface
4. Fault Management
5. Configuration Management
6. Performance Management
7. Security, Authentication and Redundancy
8. Session Establishment
9. Configuration Examples

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-297





CSCF CPI Documents

- › Configuring Diameter
- › Diameter Parameter List
- › CSCF Common Configuration Management Parameters
- › CSCF Charging Configuration Management Parameters
- › DNS Configuration Management Parameters
- › Number Normalization Management Data
- › External Network Selection Configuration Management Parameters

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-298

The figure lists the CPI documents to be used for the different CSCF configuration tasks.



HSS and SLF CPI Documents

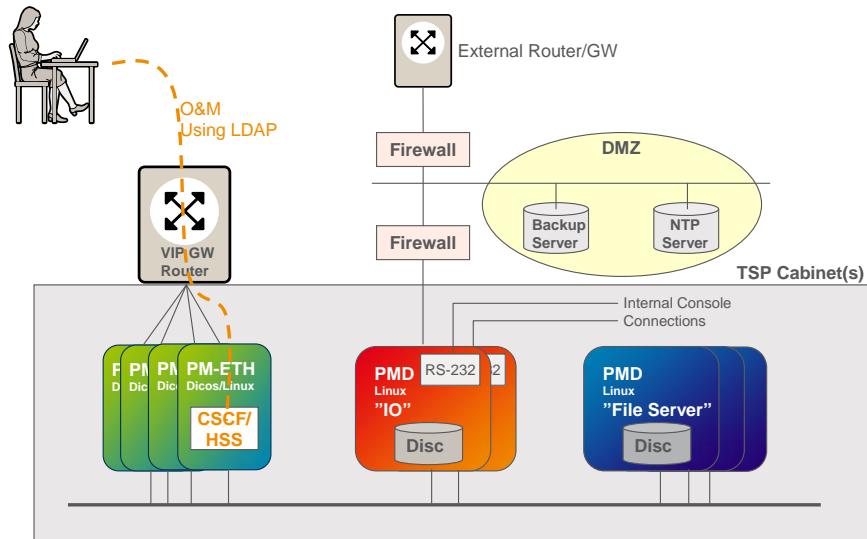
- › Administration of User Data in ISM
- › ISM LDAP Interface Description
- › SDA LDAP Interface Description
- › Configuring Diameter
- › Diameter Parameter List
- › LDAP Interface Description for Packet Access Manager & Session Manager in HSS
- › Configuration Guide for Session Manager in ISM
- › MAP LDAP Interface Description
- › Administration of User Entries in SLF
- › SLF LDAP Interface Description
- › Handling of Service Profiles in ISM
- › Handling of Charging Data in ISM

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-299

The figure lists the CPI documents to be used for the different HSS and SLF configuration tasks.



CSCF/HSS Data Management



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-300

LDAP is used to manage configuration data (parameters and values) for a number of TSP applications such as HSS & CSCF.

The TSP O&M VIP address will be used for the LDAP communication.



What is LDAP?

- › Lightweight Directory Access Protocol (LDAP)
- › Protocol for querying and modifying *Directory Services* over TCP/IP
- › Directory is a set of information with similar attributes organized in a hierarchical manner
- › Current Version is LDAPv3 (RFC4510)
- › LDAP is specified in ASN.1 and encoded in BER
 - LDIF is commonly used for ASCII representation

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-301

What is a directory service?

- Software application that stores and organizes information
- Not a relational database, but usually stores data in a database
- Optimized for fast read access
- Uses open LDAP protocol

When is LDAP useful?

- For storing data that you wish to read from many locations, but update infrequently
- Typical use: Address books

Lightweight Directory Access Protocol (LDAP):

It is a protocol for accessing information directories such as organizations, individuals, phone numbers, and addresses. It is based on the X.500 directory protocols, but it is simpler, and unlike X.500, it supports TCP/IP for Internet usage. The standards are specified in RFC 1777.

What is different between a directory and a database?

A database is optimized for transactions, it can handle updates, searches, relations and lots of other things at the same time. A Directory service is instead primarily optimized for fast searches on objects in a very standardized way. The Directory Server is in many cases based on a database. The LDAP standard defines only how searches are performed, but not how the directory is categorized. A Directory is quite static, entries are not changed so frequently even if new entries are added from time to time.



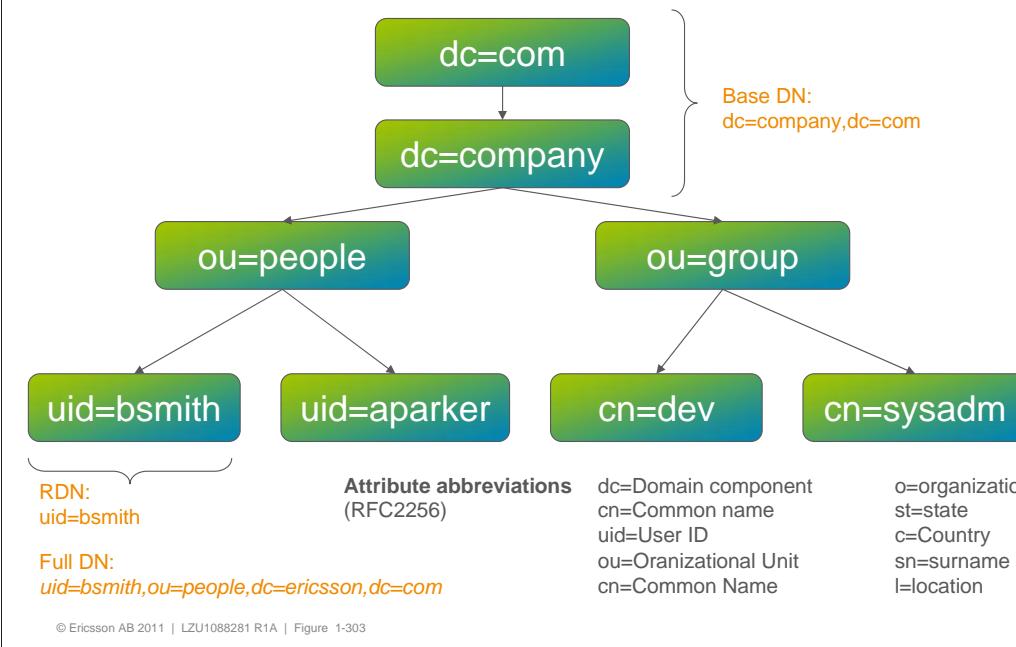
Architecture

- › The protocol accesses LDAP *directories*
- › A directory is a tree of directory *entries*
- › Each entry has a unique identifier, *Relative Distinguished Name (RDN)*
- › A RDN is part of the DN (path) of the entry
- › An entry is categorized with *Object Classes*
- › For each Object Class a *schema* exists
- › An entry consists of a set of *attributes*
- › Allowed and mandatory attributes are defined in the *Schema*

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-302

LDAP is based on entries in a directory. Each entry has a unique ID called the RDN, Relative Distinguished Name (RDN), this is the central id for an entry. RDN is used as part of the address to the entry that is called Distinguished Name (DN). A DN is constructed on many posts. Each entry is part of one or several categories (objectClass) and for each object class, a schema exist that specifies which attributes that are allowed and shall be used for this specific category of entry.

Hierarchical structure



Each entry in a LDAP directory has a unique distinguished name (DN). The dn is composed of two parts, the Relative Distinguished Name (RDN) and the location within the directory where the record resides.

The RDN is the part of your DN that is unrelated to the directory tree structure. Most items that you'll store in an LDAP directory will have a name, and the name is frequently stored in the `cn` (Common Name) or `uid` (User ID) attribute. Since nearly everything has a name, most objects you'll store in LDAP will use their `cn` or `uid` values as the basis for their RDN.

The full DN for Bob Smith at company.com could look like this:
`uid=bsmith,ou=people,dc=company,dc=com`

The base dn of the directory is `dc=company,dc=com`

All people at company.com is organized under `ou=people`

The RDN of an employee is in this example `uid=bsmith`



Entry example (LDIF)

```
version: 1
dn: uid=bsmith,ou=people,dc=company, dc=com
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: companyPerson
uid: bsmith
sn: Smith
cn: Bobby
cn: Bob Smith
telephonenumber: +4687131001
roomnumber: 122G
o: Company, AB
mailRoutingAddress: bob.smith@company.com
mailhost: mail.company.com
userpassword: {crypt}3x1231v76T89N
uidnumber: 123456
homedirectory: /home/bsmith
loginshell: /usr/local/bin/bash
```

The objectclass categorizes an entry and defines the attributes according to the schema

Attributes and values

attributeType:attributeValue

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-304

The LDAP Data Interchange Format (LDIF) is a standard data interchange format for representing (LDAP) directory content as well as directory update (Add, Modify, Delete, Rename) requests. LDAP itself is a binary protocol.

DN

The first row is the full dn of the entry. The other lines show the attributes in the entry. Attribute names are typically mnemonic strings, like "cn" for common name and "dc" for domain component.

Attributes:

All other parameters in the entries are defined as attributes, defined as an attributetype with one or several values attached.

Note that there are multiple entries for the CN. LDAP allows some attributes to have multiple values, with the number of values being arbitrary.

Object Classes:

Each entry belongs to object classes that identify the type of data represented by the entry, the object class specifies the mandatory and optional attributes that may be associated with an entry of that class.

The object classes for all objects in the directory form a class hierarchy. The classes "top" and "alias" are at the root of the hierarchy. For example, the "organizationalPerson" object class is a subclass of the "Person" object class, which in turn is a subclass of "top".

If the schema is examined for the objectclass *person* it is seen that the mandatory parameters are *objectclass,sn,cn* and several others are marked as optional.

LDAP rarely defines any ordering: The server may return the values in an attribute, the attributes in an entry, and the entries found by a search operation in any order. This follows from the formal definitions - an entry is defined as a set of attributes, and an attribute is a set of values, and sets are inherently unordered.



Entry (LDIF) from the External NW Selection

Base DN

```
version: 1
dn: ExtNetSelPoolTableEntry=test,ExtNetSelPools=0,applicationName=ExtNetSelection,nodeName=tsp
objectClass: ExtNetSelPoolTableEntryClass
ExtNetSelPoolTableEntry: test
ExtNetSelPoolTimeout: 2000
ExtNetSelPoolURI: sip:mgc1.edu.mmtel.se;lr
ExtNetSelTrunkGroupAndContext:: PEdycE5hbWU+OjxDb250ZXh0Pg==
groupId: 0
ownerId: 0
permissions: 9
shareTree: nodeName=tsp
```

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-305

The figure shows an example of a LDIF representation of the RDN *ExtNetSelPoolTableEntry=test* exported from the TSP based External Network Selection Application.

The first row shows the full DN.



JXplorer

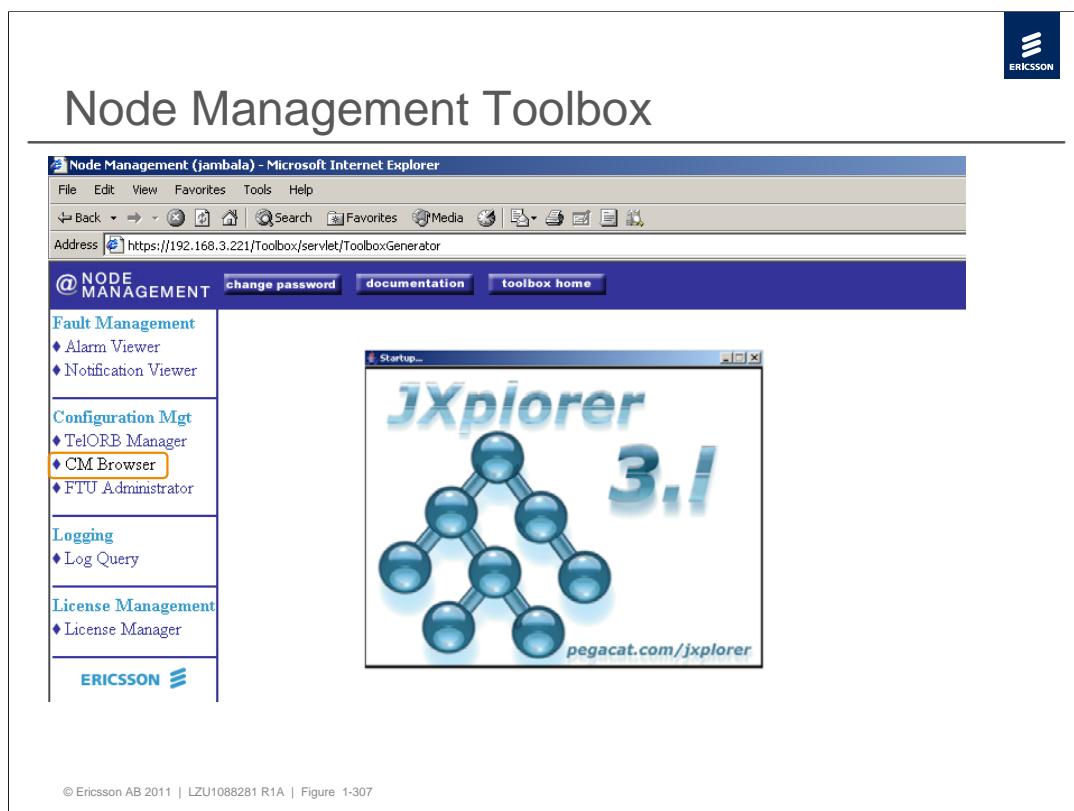
- › One browser for LDAP directory access
- › Important tool to set parameters in various nodes
- › Used in among others the following nodes:
 - HSS (Home Subscriber Server)
 - CSCF (Call Session Control Function)
 - SLF (Subscription Locator Function)

© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-306

Ericsson recommends to use the JXplorer when managing data for the different TSP applications like CSCF, HSS and SLF. JXplorer is part of the Node Management toolbox used for TSP.

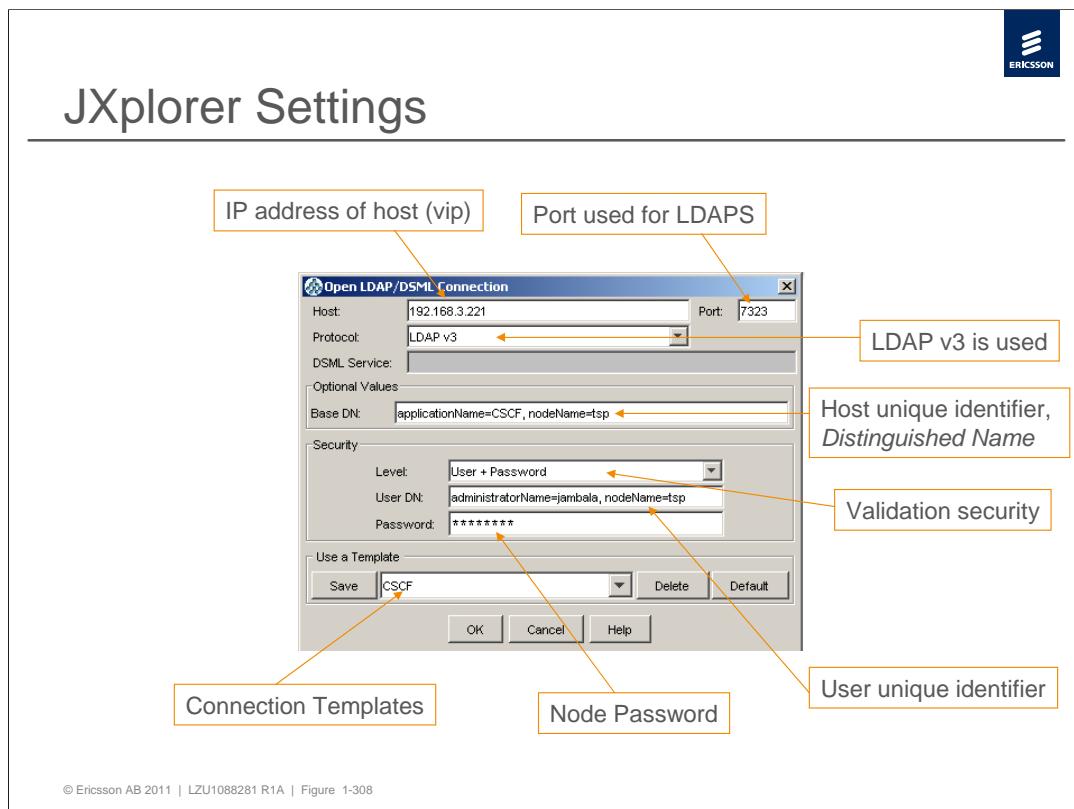
JXplorer is a LDAP browser that provides access to directory services. It allows you to connect to any directory that supports LDAP Version 3.0. Once connected, you can:

- Navigate, search, view, and modify the directory
- Read the directory's schema
- Cut, paste, and edit subtrees within the directory
- Import and export LDAP Data Interchange Format



JXplorer is only one tool to access LDAP directory services, and it is part of Node Management toolbox of TSP as the configuration management browser (CM Browser).

The figure shows the Java applet starting...



To connect to an application on the TSP, its attributes must be specified.

Host: The IP address of the machine that hosts the node (normally the platform VIP of the TSP)

Port: The port number for secure LDAP in IMS (7323)

Protocol: Which protocol to use. (LDAP v3 is used and DSML Service is obsolete)

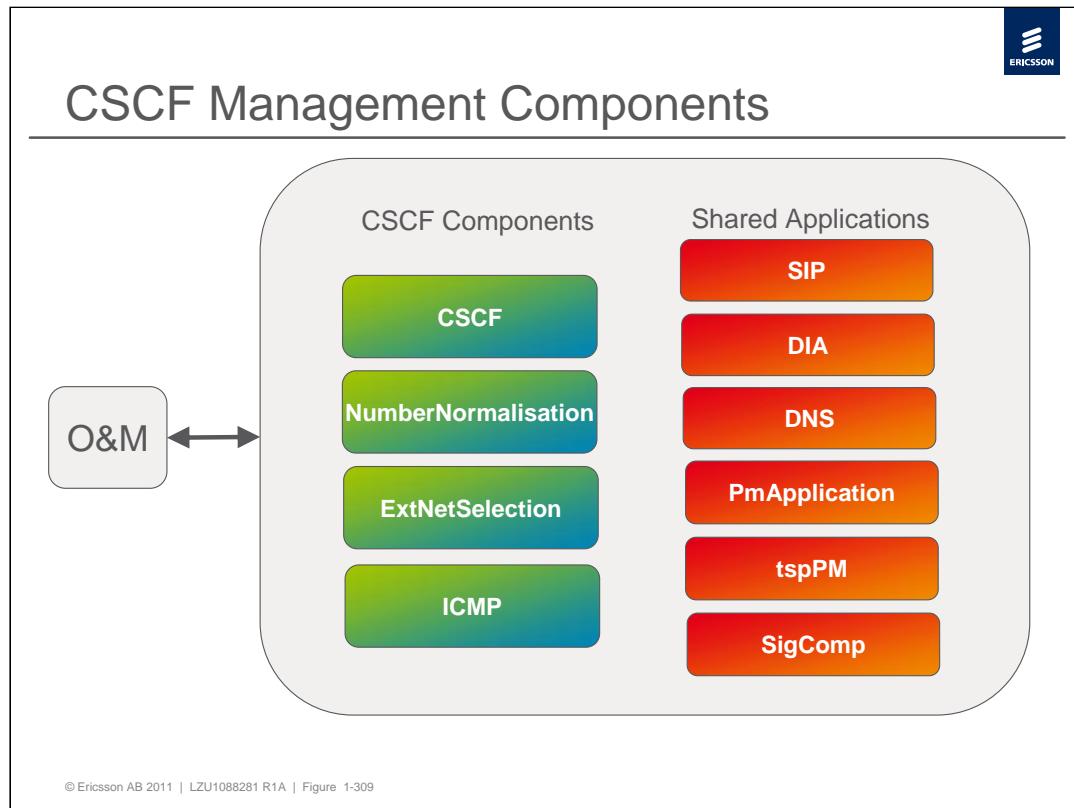
Base DN: The Base Distinguished Name of the host, consisting of an *application name* and *nodeName*. Application name is the name used in the database for the application e.g. HSS, CSCF, platform, DIA.

Level: Specify how a user is validated on connection

User DN: The distinguished name of the user, consisting of an *administratorName* and *nodeName*.

Password: The password for the user specified in User DN.

Save: Connection templates for the different applications can be saved for faster access.



NumberNormalisation implements the Number Normalization function which converts local telephone numbers and national numbers to fully internationalized numbers.

ExtNetSelection implements a simplified BGCF function in order to route a session to an external network (PSTN or H.323) based on the A-number, B-number, RN or CIC parameter.

SIP implements the SIP stack as specified by RFC 3261.

SigComp specifies a signaling compression mechanism of requests and responses specified in RFC 3320.

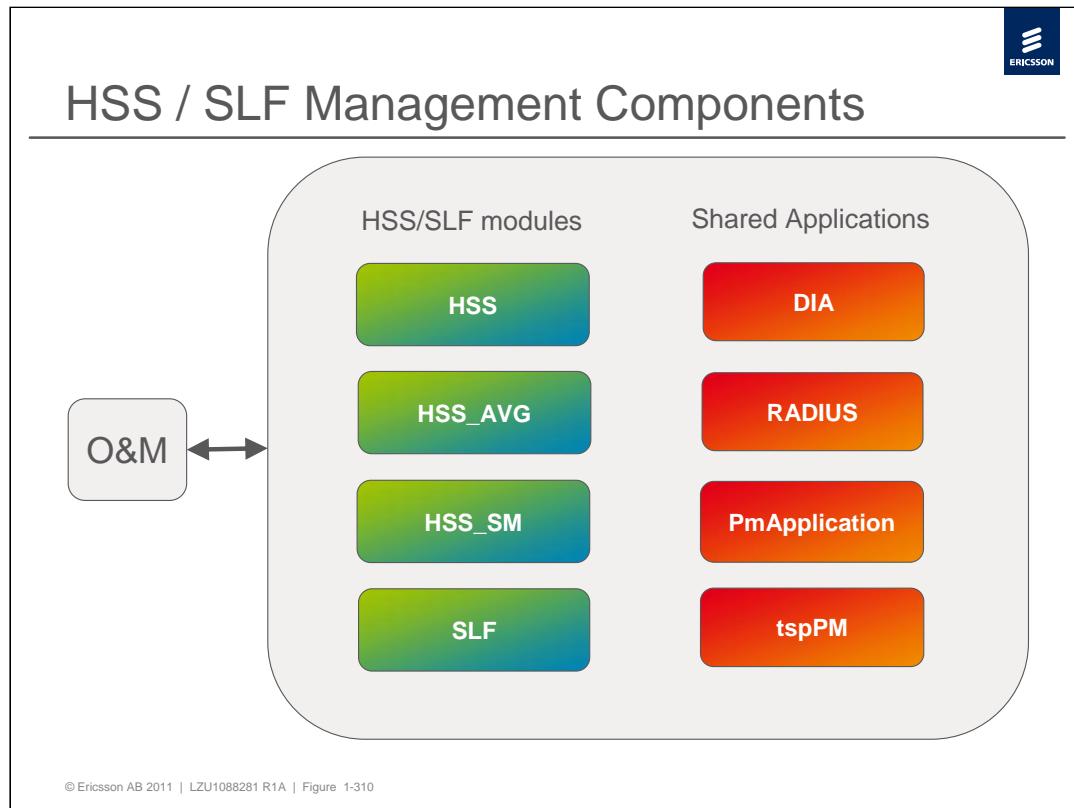
DIA implements the Diameter stack used for HSS (Cx), SLF (Dx) and charging (Rf) communication.

DNS implements the interface towards ENUM/DNS.

PmApplication provides applications/components with a single framework to report and manage performance measurements.

tspPM provides applications/components with an improved framework to report and manage performance measurements.

ICMP provides the possibility to handle communication problems with gateways/hosts.



The figure shows the simplified internal interworking architecture between the HSS (or SLF) component and other TSP based components.

The names in the figure are the same as the system defined names (ApplicationName) used when accessing the components via LDAP browser for configuration management.

The **HSS** and **SLF** components implement the 3GPP and 3GPP2 specific functionality of the respective logical entities.

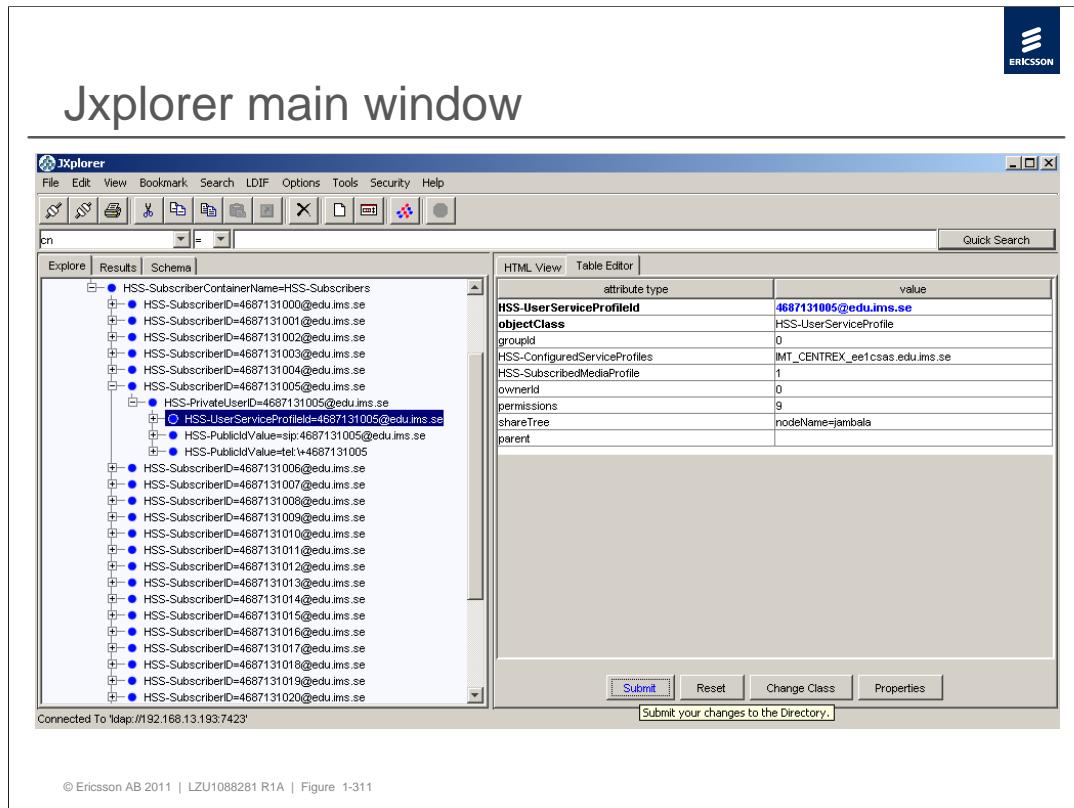
DIA implements the Diameter stack used for HSS (Cx), SLF (Dx) and charging (Rf) communication.

PmApplication provides applications/components with a single framework to report and manage performance measurements.

HSS_SM implements an ISM Session Manager module that provides a support for Single-Sign-On authentication mechanism in HSS

RADIUS implements the RADIUS stack and configurations for communication with a Network Access Server (e.g. GGSN)

All the components interact with the O&M component.



In the main window there are three tabs; Explore, Results and Schema.

Explore is the window for examining the directory entries or modifying.

Results show search hits.

Schema:

The contents of the entries in a subtree are governed by a schema.

The schema defines the *attribute types* that directory entries can contain. An attribute definition includes a *syntax*, and most non-binary values in LDAPv3 use UTF-8 string syntax. For example, a "mail" attribute might contain the value "user@example.com". A "jpegPhoto" attribute would contain photograph(s) in binary JPEG/JFIF format. A "member" attribute contains DNs of other directory entries. Attribute definitions also specify whether the attribute is single-valued or multi-valued, how to search/compare the attribute (e.g. case-sensitive vs. case-insensitive and whether substring matching is supported), etc.

The schema defines *object classes*. Each entry must have an *objectClass* attribute, containing named classes defined in the schema. The schema definition of the classes of an entry defines what kind of object the entry may represent - e.g. a person, organization or domain. The object class definitions also list which attributes the entry MAY and MUST contain. For example, an entry representing a person might belong to the classes "top" and "person". Membership in the "person" class would require the entry to contain the "sn" and "cn" attributes, and allow the entry also to contain "userPassword", "telephoneNumber", and other attributes. Since entries may belong to multiple classes, each entry has a complex of optional and mandatory attribute sets formed from the union of the object classes it represents.

The schema also includes various other information controlling directory entries.

Most schema elements have a name and a globally unique Object Identifier (OID).

Definitions

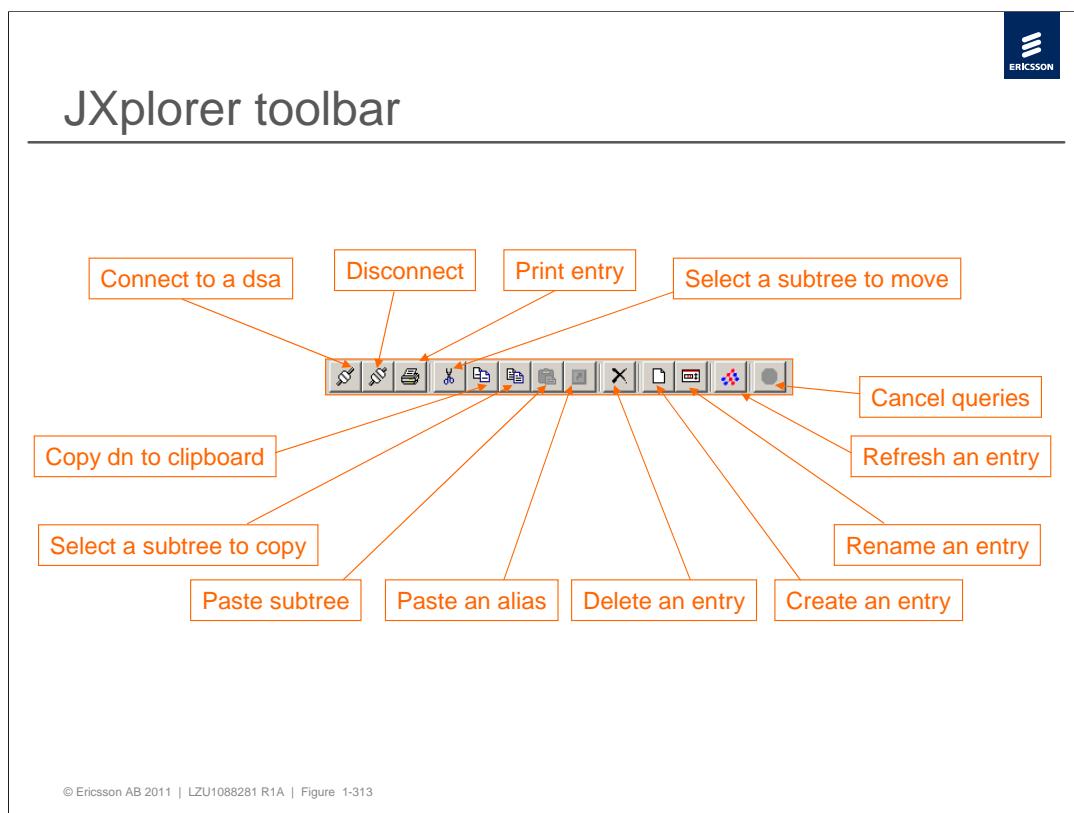
- › Base DN = applicationName=CSCF,nodeName=tsp
 - Top entry in the directory
- › RDN = a unique id for an entry

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view shows the directory structure under 'World'. An entry for 'applicationName=hss' is selected and highlighted with a red box, labeled 'RDN'. Above it, another entry is labeled 'Base DN'. To the right, the 'HTML View' panel displays the attributes of the selected entry. The attributes listed are:

attribute type	value
HSS-IsmConfigurationDataName	HSS-IsmConfigurationData
objectClass	HSS-IsmConfigurationData
groupId	411
HSS-AuthenticationLogStatus	FALSE
HSS-DefaultMaxCallLegs	1
HSS-DefaultMaxSessions	1
HSS-LocationLogStatus	FALSE
HSS-MassiveUpdateAllowed	TRUE
HSS-MaxSimultaneousRequests	10
HSS-NumMaxPublicIdsPerUser	5
HSS-OAMLogStatus	FALSE
HSS-PerfEndScheduleTime	20080827T085857935
HSS-PerfInitialScheduleTime	20080827T085857935

At the bottom of the interface, there are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'.

Each entry has a unique identifier: its *Distinguished Name* (DN). This consists of its *Relative Distinguished Name* (RDN) constructed from some attribute(s) in the entry, followed by the parent entry's DN. DN is constructed on RDNs.

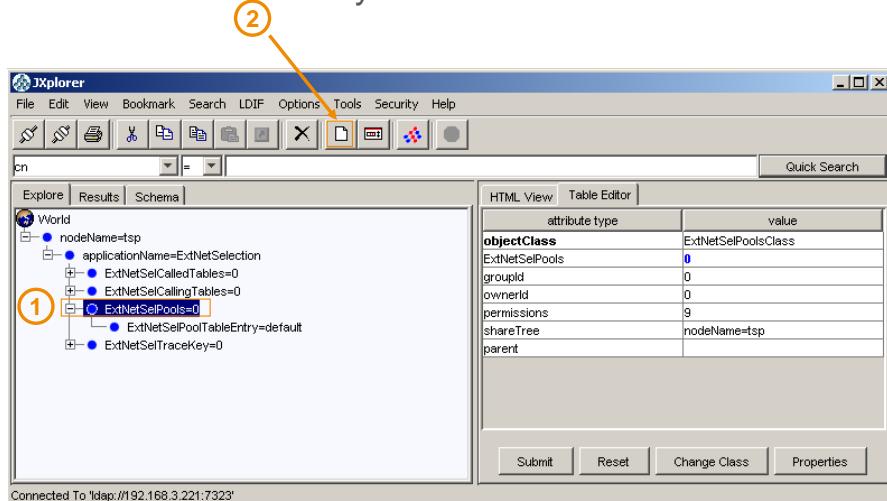


The figure shows the JXplorer tool bar.

dsa=Directory Service Agent=LDAP Server

Example: Adding new MGC Address

- › Click the branch to modify and Edit > New



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-314

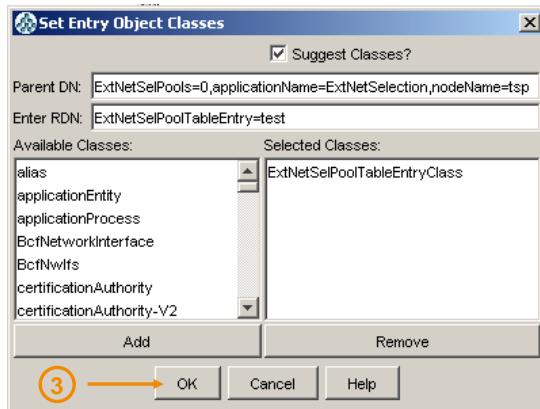
A new ExtNetSelPoolTableEntry containing a new MGC SIP address for PSTN breakout is defined in the example.

1. Mark the parent DN.
 2. Click on the "create an entry button" on the toolbar.
- A pop up window will appear as seen on the next slide.



Setting Object Classes

- › RDN is the unique id.
- › Object Classes defines (according to schema) which attributes an entry shall have



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-315

3. Enter a new unique value for the entry (RDN) and select the correct object class. The object class will according to the schema define what attributes the entry will have.

Which object class to use is described in the CPI documentation.



Editing attribute values and Submit

- Mandatory and optional attributes according to objectClass can be found under the schema tab

The screenshot shows the JXplorer LDAP browser interface. The 'Schema' tab is selected in the top navigation bar. On the left, the LDAP tree shows a node named 'ExtNetSelPoolTableEntry'. In the 'Table Editor' on the right, there is a table with columns 'attribute type' and 'value'. The table contains several entries, with the last one, 'ExtNetSelPoolURI', highlighted. A yellow circle labeled '4' is drawn around the value 'sip:mgc1.edu.int.se;lr'. An orange arrow labeled '5' points from the bottom-left towards the 'Submit' button at the bottom right of the editor. The status bar at the bottom indicates a connection to 'ldap://192.168.3.221:7323'.

attribute type	value
objectClass	ExtNetSelPoolTableEntryClass
objectClass	JIM-ManagedObject
objectClass	top
ExtNetSelPoolTableEntry	test
ExtNetSelPoolTimeout	
ExtNetSelPoolURI	sip:mgc1.edu.int.se;lr
ExtNetSelTrunkGroupAndContext	
groupId	
ownerId	
parent	
permissions	
shareTree	

4. Add a attribute value for the new MGC SIP address.

5. Submit your new values.

Mandatory and optional attributes can be found under the schema tab.

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view under 'cn' shows a node named 'nodeName=tsp'. This node has several children, including 'applicationName=ExtNetSelection', 'ExtNetSelCalledTables=0', 'ExtNetSelCallingTables=0', 'ExtNetSelPools=0', and 'ExtNetSelPoolTableEntry=default'. The 'ExtNetSelPoolTableEntry=default' node has a child 'ExtNetSelPoolTableEntry=test' which is highlighted with a yellow circle containing the number '6'. On the right, the 'Table Editor' tab is selected, displaying a table of attributes and their values:

attribute type	value
objectClass	ExtNetSelPoolTableEntryClass
ExtNetSelPoolTableEntry	test
ExtNetSelPoolTimeout	0
ExtNetSelPoolURI	sip:mgc1.edu.int.se;lr
ExtNetSelTrunkGroupAndContext	<GrpName><Context>
groupId	0
ownerId	0
permissions	9
shareTree	nodeName=tsp
parent	

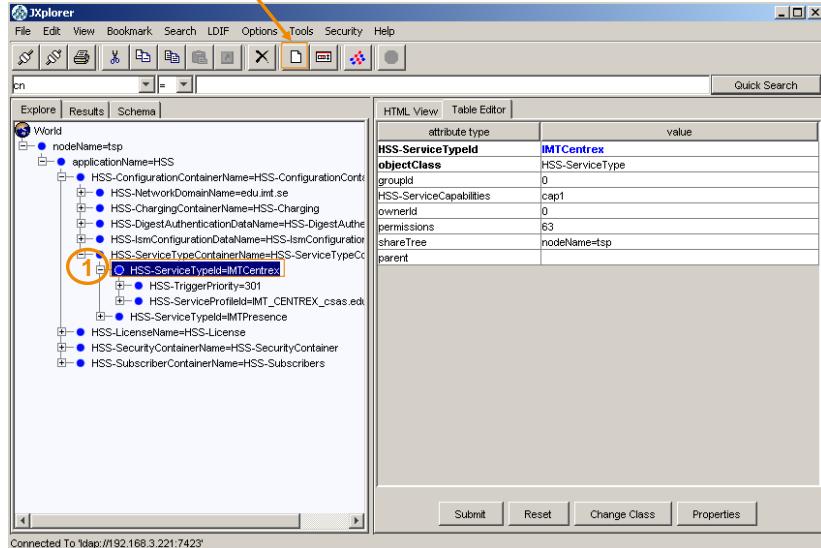
At the bottom of the interface, there are buttons for 'Submit', 'Reset', 'Change Class', and 'Properties'. A status message at the bottom left says 'Connected To ldap://192.168.3.221:7323'.

6. Verify the new entry.

Default values will be allocated by the system to attributes without values.

Example: Adding a New Trigger

- › Click the branch to modify and Edit > New



© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-318

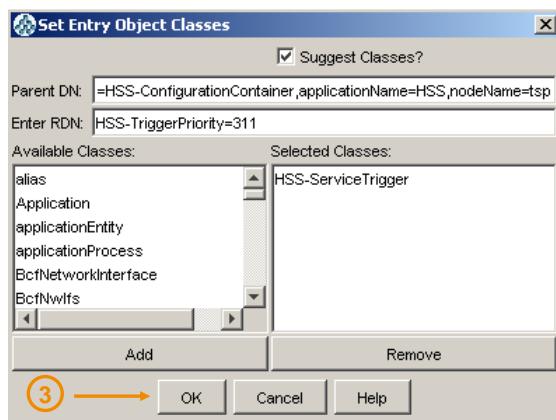
A new HSS-TriggerPriority containing a new trigger description is defined in the example.

1. Mark the parent DN.
 2. Click on the "create an entry button" on the toolbar.
- A pop up window will appear as seen on the next slide.



Setting Object Classes

- › RDN is the unique id.
- › Object Classes defines (according to schema) which attributes an entry shall have



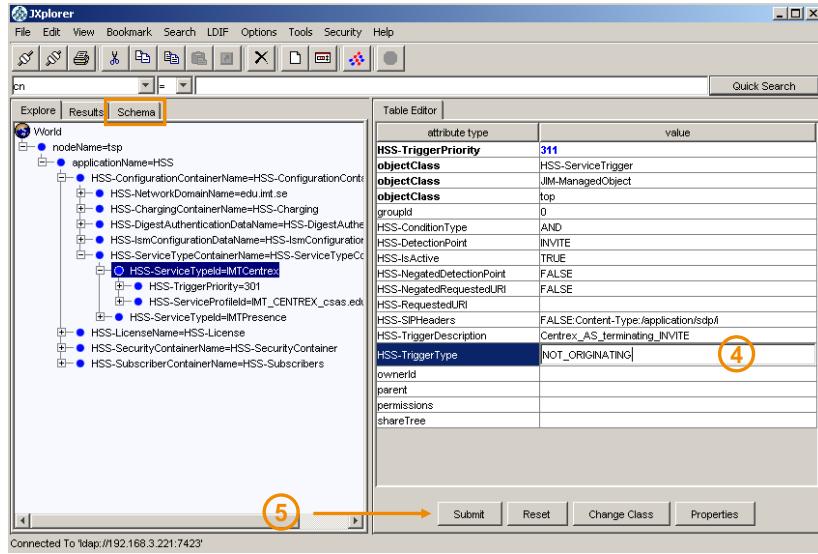
© Ericsson AB 2011 | LZU1088281 R1A | Figure 1-319

3. Enter a new unique value for the entry (RDN) and select the correct object class. The object class will according to the schema define what attributes the entry will have.

Which object class to use is described in the CPI documentation.

Editing attribute values and Submit

- Mandatory and optional attributes according to objectClass can be found under the schema tab



The screenshot shows the JXplorer LDAP browser interface. The title bar says "JXplorer". The menu bar includes File, Edit, View, Bookmark, Search, LDIF, Options, Tools, Security, Help. The toolbar has icons for search, filter, export, and import. The left pane is titled "cn" and shows a tree structure of LDAP objects under "World" and "nodeName=hss". The "Schema" tab is selected in the top navigation bar. The right pane is titled "Table Editor" and displays a table of attributes and their values. The table includes:

attribute type	value
HSS-TriggerPriority	311
objectClass	HSS-ServiceTrigger
objectClass	JIM-ManagedObject
objectClass	top
groupId	0
HSS-ConditionType	AND
HSS-DetectionPoint	INVITE
HSS-IsActive	TRUE
HSS-NegatedDetectionPoint	FALSE
HSS-NegatedRequestedURI	FALSE
HSS-RequestedURI	
HSS-SIPHeaders	FALSE-Content-Type:application/sdp/
HSS-TriggerDescription	Centrex_AS_terminating_INVITE
HSS-TriggerType	NOT_ORIGINATING (4)
ownerId	
parent	
permissions	
shareTree	

At the bottom of the table editor, there are buttons for Submit, Reset, Change Class, and Properties. An orange arrow labeled "5" points from the "Submit" button to the "HSS-TriggerType" row. Another orange circle labeled "4" highlights the value "NOT_ORIGINATING" in the "HSS-TriggerType" row.

4. Add a attribute value for all the attributes required.

5. Submit your new values.

Mandatory and optional attributes can be found under the schema tab.

The screenshot shows the JXplorer LDAP browser interface. On the left, the tree view displays the structure under 'nodeName=tsp'. A node labeled 'HSS-TriggerPriority=311' is highlighted with a red circle containing the number '6'. On the right, the 'Table Editor' tab is active, showing a table of attributes and their values. The 'attribute type' column includes 'HSS-TriggerPriority', 'objectClass', 'groupID', 'HSS-ConditionType', 'HSS-DetectionPoint', 'HSS-IsActive', 'HSS-NegatedDetectionPoint', 'HSS-NegatedRequestedURI', 'HSS-RequestedURI', 'HSS-SIPHeaders', 'HSS-TriggerDescription', 'HSS-TriggerType', 'ownerID', 'permissions', 'shareTree', and 'parent'. The 'value' column contains corresponding values such as '311', 'HSS-ServiceTrigger', '0', 'AND', 'INVITE', 'TRUE', 'FALSE', 'FALSE', 'HSS-ServiceProfiled=IMT_CENTREX_casas.edu', '0', '63', 'nodeName=tsp', and ''.

attribute type	value
HSS-TriggerPriority	311
objectClass	HSS-ServiceTrigger
groupID	0
HSS-ConditionType	AND
HSS-DetectionPoint	INVITE
HSS-IsActive	TRUE
HSS-NegatedDetectionPoint	FALSE
HSS-NegatedRequestedURI	FALSE
HSS-RequestedURI	
HSS-SIPHeaders	FALSE Content-Type:/application/sdpf
HSS-TriggerDescription	Centrex_AS_terminating_INVITE
HSS-TriggerType	NOT_ORIGINATING
ownerID	0
permissions	63
shareTree	nodeName=tsp
parent	

6. Verify the new entry.

Default values will be allocated by the system to attributes without values.



ERICSSON