Cisco ASR 5000Series Session Control Manager Administration Guide

Version 11.0

Last Updated January 14, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-24217-01

Cisco ASR 5000Series Session Control Manager Administration Guide

CONTENTS

About this Guide

This document pertains to features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* slot_number is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

Command Syntax Conventions	Description
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

Important: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1
Session Control Manager Overview

This chapter contains general overview information about the Session Control Manager (SCM) including:

- Product Description
- Product Specifications
- Network Deployments and Interfaces
- Features and Functionality - Base Software
- Features and Functionality - Licensed Enhanced Feature Support
- How the SCM Works
- Supported Standards

Product Description

The Session Control Manager (SCM) delivers and controls a robust multimedia environment today, while preparing for the networks of tomorrow. SCM provides an easy on-ramp to deploying Session Initiation Protocol (SIP)-based services and a future-proof migration path to the IP Multimedia Subsystem/Multimedia Domain (IMS/MMD) architectures.

The SCM performs the following functions:

- SIP routing
- Translation and mobility
- Admission control
- Authentication
- Registration
- Emergency Registration
- Packet network access based on pre-established policies and procedures
- Localized policy selection and enforcement
- Multimedia Call Detail Records (CDRs)
- Per-subscriber service facilitation
- SIP Application-level Gateway (ALG)
- Media relay
- Mitigate SIP Denial of Service (DoS)
- Prevent registration hijacking
- Prevent theft of service

The SCM consists of multiple IMS components that can be integrated into a single ASR 5000 platform or distributed as standalone network elements:

- IETF-compliant SIP Proxy/Registrar
- 3GPP/3GPP2-compliant Proxy Call/Session Control Function (P-CSCF)
- 3GPP/3GPP2-compliant Serving Call/Session Control Function (S-CSCF)
    - 3GPP/3GPP2-compliant Interrogating Call/Session Control Function (I-CSCF)
    - 3GPP/3GPP2 Breakout Gateway Control Function (BGCF)
- 3GPP/3GPP2-compliant Emergency Call/Session Control Function (E-CSCF)
- 3GPP/IETF-compliant Access Border Gateway (A-BG)

As standards-based network elements, SCM components can be integrated with each other or with third-party IMS components.

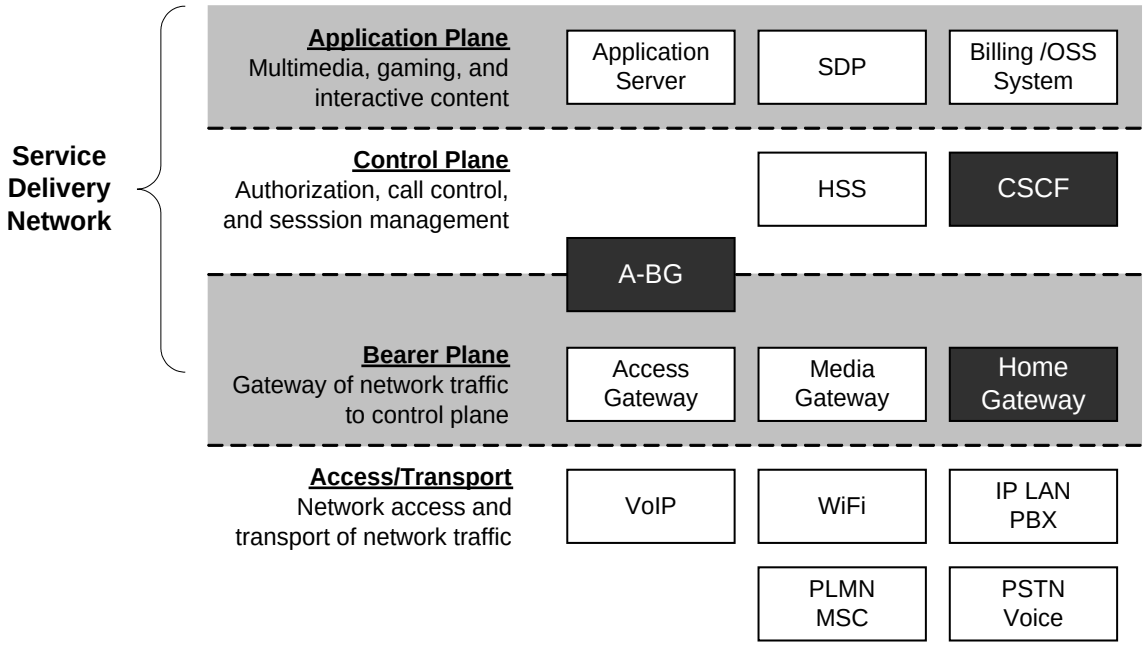
IMS Architecture

IP Multimedia Subsystem (IMS) specifies a standard architecture for providing combined IP services (voice, data, multimedia) over the existing public switched domain. IMS is an integral part of the 3GPP, 3GPP2, ETSI, and TISPAN network model standards that define circuit switched, packet switched, and IP multimedia domain environments. IMS also supports multiple access methods such as GSM, WCDMA, CDMA2000, WLAN, and wireless broadband access.

The call signaling protocol used in IMS is the Session Initiation Protocol (SIP). The primary component in the network for resolving and forwarding SIP messages is the Call/Session Control Function (CSCF). The CSCF provides the control and routing function for all IP sessions accessing the network. CSCFs are located in the control plane or layer of the Service Delivery Network as shown in the figure below.

When the SCM acts as an Access Border Gateway (A-BG), it uses the RFC3261/P-CSCF to provide a SIP/IMS control plane access border, as well as a bearer access border control function. Therefore, the A-BG provides all session border control functions for all SIP UEs attempting to access the mobile network from a network outside of the operator's control and operations.

Figure 1. IMS Service Delivery Networks Components

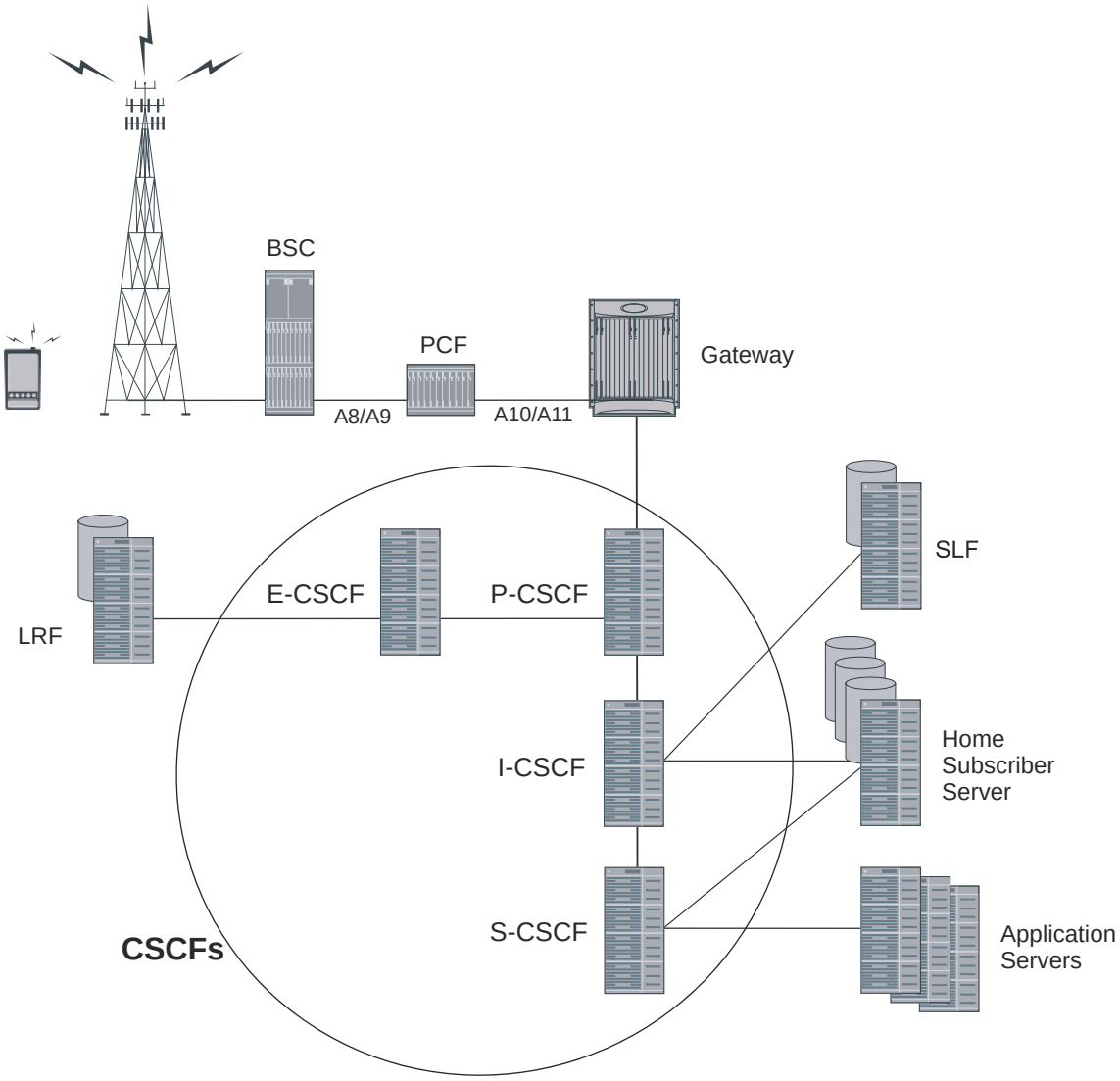


Collectively, CSCFs are responsible for managing an IMS session, including generating Call Detail Records (CDRs). Four functional behaviors are defined for the CSCF:

- Proxy
- Interrogating
- Serving
- Emergency

The following figure shows the general interaction between the CSCF components and the supporting servers.

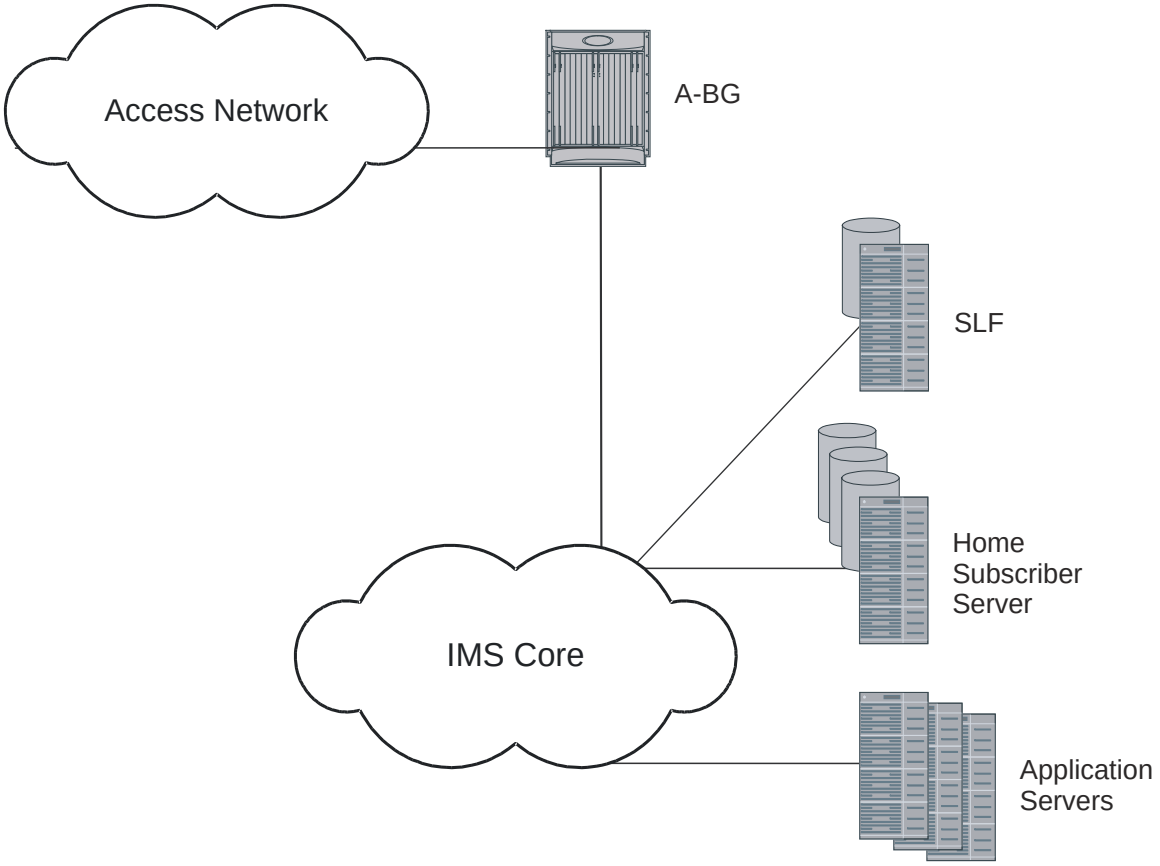
Figure 2. IMS CSCF Components



In addition, the SCM may act as an Access Border Gateway (A-BG).

The following figure shows the general interaction between the A-BG and the supporting servers.

Figure 3. Access Border Gateway



Proxy-CSCF

The primary point of entry into the IMS network is the Proxy-CSCF (P-CSCF). The P-CSCF is responsible for:

- providing message manipulation to allow for localized services (traffic/weather reports, news, directory services, etc.)
- initiating the breakout of emergency service calls
- Topology Hiding Inter-network Gateway (THIG)
- Quality of Service (QoS) authorization
- number conversions for local dialing plans
- terminate IPSec tunnels

The P-CSCF is the handset's first point of entry into the IMS and is also the outbound proxy for SIP. Once the P-CSCF has completed all of the functions for which it is responsible, the call setup is handed off to the Interrogating-CSCF (I-CSCF).

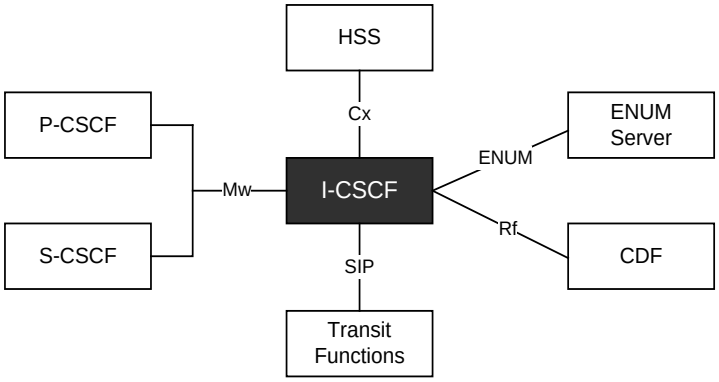
Interrogating-CSCF

The I-CSCF performs mostly as a load distribution device. The I-CSCF queries the Home Subscriber Server (HSS) to identify the appropriate Serving-CSCF (S-CSCF) to which the call is sent. Since the HSS maintains user profile information (much like the Home Location Register (HLR) in the Public Land Mobile Network (PLMN)), the I-CSCF can identify the proper S-CSCF for the call. The I-CSCF may also query a AAA server to determine subscriber profile information using DIAMETER.

Important: The I-CSCF is incorporated into the S-CSCF.

I-CSCF Interfaces

The following diagram shows the interfaces/reference points associated with the I-CSCF:



Serving-CSCF

The Serving-CSCF (S-CSCF) is the access point to services provided to the subscriber. Service examples include session control services, such as call features.

Other services include:

- VPN
- Centralized speed dialing lists
- Charging

The S-CSCF also interacts with the HSS for:

- User authentication
- Emergency registration
- Location management
- User data handling

A Breakout Gateway Control Function is integrated into the SCM's S-CSCF to support PSTN calls.

Telephony Application Server (TAS) Basic Supported

The following describe the local basic call features implemented on the S-CSCF:

- Abbreviated Dialing (AD)
- Call Forward Busy Line (CFBL)
- Call Forward No Answer (CFNA)
- Call Forward Not Registered (CFNR)
- Call Forward Unconditional (CFU)
- Call Transfer
- Call Waiting
- Caller ID Display (CID)
- Caller ID Display Blocked (CIDB)
- Feature Code Activation/De-activation
- Follow Me/Find Me
- Locally Allowed Abbreviated Dialing
- Outbound Call Restrictions/Dialing Permissions
- Short Code Dialing

Integrated S/I-CSCF

The following Interrogating-CSCF features are supported for the integrated S/I-CSCF:

- **Assign an S-CSCF to a User Performing SIP Registration** - On a UE registration, the I-CSCF carries out a first step authorization and S-CSCF discovery. For this, the I-CSCF sends a Cx User-Authentication-Request (UAR) to the HSS by transferring the Public and Private User Identities and the visited network identifier (all extracted from the UE REGISTER message). The HSS answers with a Cx User-Authentication-Answer (UAA). The UAA includes the URI of the S-CSCF already allocated to the user. If there is no previously allocated S-CSCF, the HSS returns a set of S-CSCF capabilities that the I-CSCF uses to select the S-CSCF.
- **E.164 Address Translation** - Translates the E.164 address contained in all Request-URIs having the SIP URI with user=phone parameter format into the Tel: URI format before performing the HSS Location Query. In the event the user does not exist, and if configured by operator policy, the I-CSCF may invoke the portion of the transit functionality that translates the E.164 address contained in the Request-URI of the Tel: URI format to a routable SIP URI.
- **Obtain the S-CSCF Address from the HSS** - When the I-CSCF receives a SIP request from another network, it has to route the request to the called party. For this it obtains the S-CSCF address associated with the called party from the HSS by querying with a Cx Location-Information-Request (LIR) message. The Public-Identity AVP in the LIR is the Request-URI of the SIP request. The Location-Information-Answer (LIA) message contains the S-CSCF address in the Server-Name AVP. The request is then routed to the S-CSCF.
- **Route a SIP Request or Forward Response from Another Network** - When the I-CSCF receives a request from another network, it obtains the address of the S-CSCF from the HSS using the procedure detailed above and routes the request to the S-CSCF. Responses are also routed to the S-CSCF.

- **Perform Transit Routing Functions** - The I-CSCF may need to perform transit routing if, based on the HSS query, the destination of the session is not within the IMS. The IMS Transit Functions perform an analysis of the destination address and determine where to route the session. The session may be routed directly to an MGCF, BGCF, or to another IMS entity in the same network, to another IMS network, or to a CS domain or PSTN.
- **Generate CDRs** - The I-CSCF generates CDRs for its interactions. Upon completing a Cx query, the I-CSCF sends an Accounting Request with the Accounting-Record-Type set to EVENT. The CDF acknowledges the data received and creates an I-CSCF CDR.

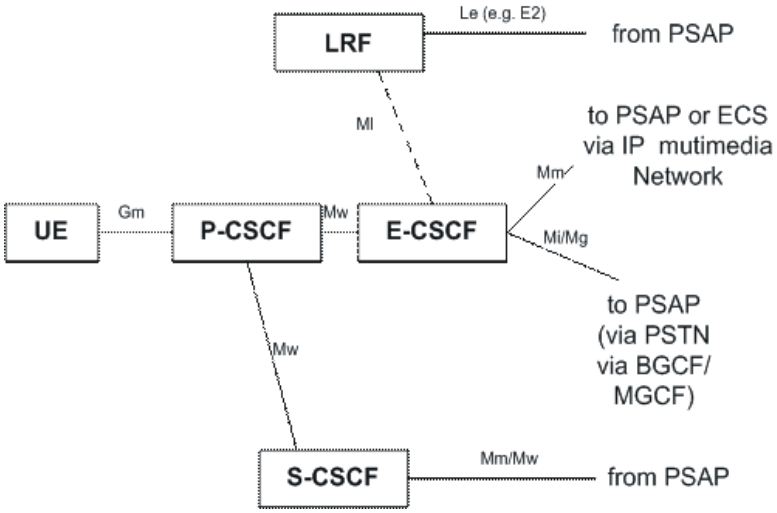
Emergency-CSCF

The Emergency-CSCF (E-CSCF) is a network element in IMS which is responsible for routing an emergency call to a Public Safety Answering Point (PSAP).

To identify the next hop PSAP, E-CSCF interacts with the Location Retrieval Function (LRF). LRF provides the necessary routing information so that E-CSCF can route the request to the appropriate PSAP.

E-CSCF Interfaces

The following diagram shows the interfaces/reference points associated with the E-CSCF:



A-BG

The A-BG is responsible for:

- Border Control for both Signaling and Bearer
- Intelligent Routing

    - Least Cost, Congestion Based, Call Type, Domain Based
    - As a SIP ALG, supports signaling and media routing with overlapping address ranges
- SIP Application-level Gateway (SIP-ALG)
    - SIP NAT Traversal
    - SIP NAT (IPv4 <–> IPv6 translation)
    - Media Relay (Header Manipulation): RTP, MSRP
- Call Admission and Access Control
    - Access Control based on IP, URL, SIP Identity, and Session Limits
- Topology Hiding Inter-network Gateway (THIG)
- CALEA Support
    - SIP and media taps
- SIP Security
    - Prevent Theft of Service
        - Prevent CSCF bypass
        - Robust authentication procedures
        - SIP message checking
    - Prevent Registration Hijacking
        - Authenticate Re-Register (S-CSCF)
        - Early IMS Security: DoS attack prevention, impersonating a server
        - UA authentication (prevent server impersonation)
        - AKA authentication mechanism (further protection)
    - Prevent Message Tampering (IPSec)
    - Prevent Early Session Tear Down
        - Early IMS Security prevents a different user releasing existing session
    - Mitigate SIP Denial of Service (DoS)
        - P-CSCF DoS Attack Prevention
        - Blocking of user/IP address
            - after repeated authentication and bad request failure in Register/INVITE
        - Dropping of Register
            - containing Contact header pointing to CSCF service ip:port
        - Limited number of contacts on which Forking is allowed
        - Dropping of Requests
            - coming from source address other than the Register request's source address

Product Specifications

Technical Specifications

The following table provides product specifications for the SCM.

Table 1. Session Control Manager Technical Specifications

	Description
Service Instances	Dual-mode proxy: simultaneously supports IETF & 3GPP/3GPP2 Proxies
SIP	• IETF SIP Proxy/Registrar • 3GPP/3GPP2 Proxy Call Session Control Function (P-CSCF) • Stateful session and subscriber aware control • Signaling Compression/Decompression (SIGCOMP) • Auto discovery, subscriber privacy, network security, call fraud prevention, thwarting network overload conditions
SIP Message Handling	Forking, error handling and discard, header stripping and insertion, Multiple public user identities
Logical Interfaces	• IETF: SIP Proxy/Registrar • 3GPP: Mw, Gm, Rx, Rf, Cx, Sh, Dx, MI • 3GPP2: Mw, Gm, Tx, Rf, Cx, Sh, Dx, MI

Licenses

The SCM is a licensed product. A session use license key must be acquired and installed to use the SCM service.

The following licenses are available for this product:

- SCM Software License
    - Serving-CSCF
    - Proxy-CSCF
    - A-BG

Apart from base software license, SCM requires feature licenses for various enhanced features supported on the ASR 5000 platform in SCM service.

Hardware Requirements

Information in this section describes the hardware required to properly enable SCM services.

Platforms

The SCM operates on the ASR 5000.

System Hardware Components

The following application and line cards are required to support SCM functionality on an ASR 5000 platform:

- **System Management Cards (SMCs)**: Provides full system control and management of all cards within the ASR 5000 platform. Up to two SMC can be installed; one active, one redundant.
- **Packet Services Cards (PSCs/PSC2s)**: Within the ASR 5000 platform, PSCs provide high-speed, multi-threaded PDP context processing capabilities for 2.5G SGSN, 3G SGSN, and GGSN services. Up to 14 PSCs can be installed, allowing for multiple active and/or redundant cards.
- **Switch Processor Input/Outputs (SPIOs)**: Installed in the upper-rear chassis slots directly behind the SMCs, SPIOs provide connectivity for local and remote management, Central Office (CO) alarms. Up to two SPIOs can be installed; one active, one redundant.
- **Line Cards:** Installed directly behind PSC/PSC2, these cards provide the physical interfaces to elements in the GPRS/UMTS data network. Up to 26 line cards can be installed for a fully loaded system with 13 active PSCs/PSC2s, 13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant PSCs/PSC2s do not require line cards.
    - Ethernet 10/100 and/or Ethernet 1000 line cards/Quad Gig-E Line Cards (QGLC) for IP connections to the GGSN, SGSN, or other network elements.
- **Redundancy Crossbar Cards (RCCs)**: Installed in the lower-rear chassis slots directly behind the SMCs, RCCs utilize 5 Gbps serial links to ensure connectivity between Ethernet 10/100 or Ethernet 1000 line cards/QGLCs and every PSC/PSC2 in the system for redundancy. Two RCCs can be installed to provide redundancy for all line cards and PSCs/PSC2s.

Additional information pertaining to each of the application and line cards required to support GPRS/UMTS wireless data services is located in the Hardware Platform Overview.

Operating System Requirements

The SCM is available for the ASR 5000 running StarOS Release 8.1 or later.

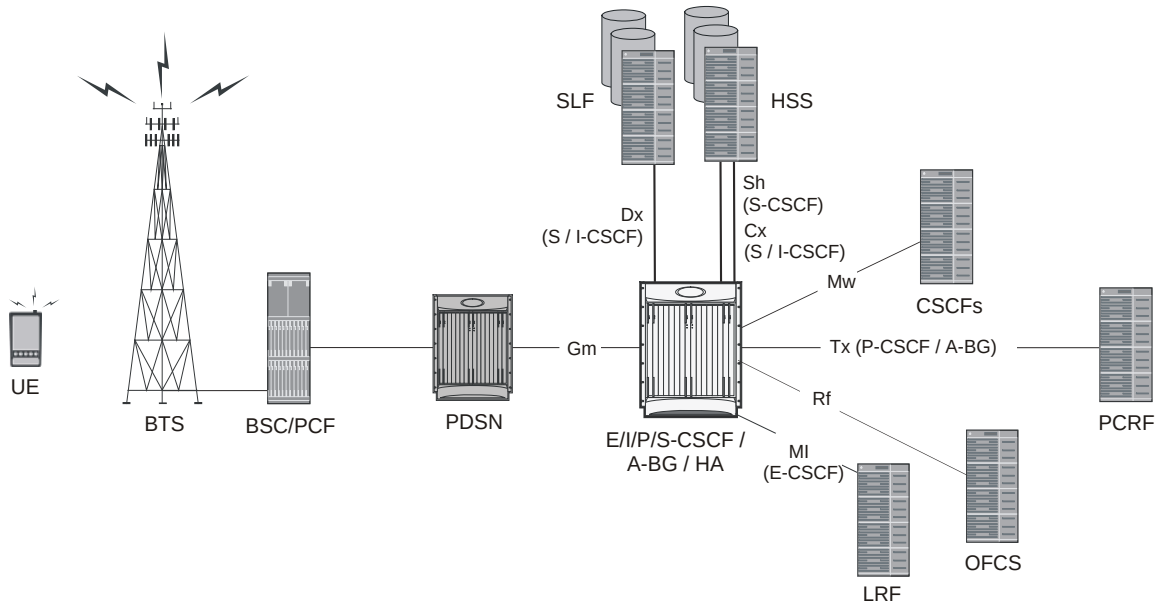
Network Deployments and Interfaces

SCM in a CDMA2000 Data Network Deployment

Integrated CSCF / A-BG / HA

The SCM is designed to function within a CDMA2000 PDSN network. By combining the SCM with a carrier-class Home Agent, a number of advantages emerge such as increased performance, distributed architecture, and high availability. As shown in the figure below, the SCM supports a number of interfaces used to communicate with other components in an IMS environment and supports the interface used to bridge the CDMA network.

Figure 4. CDMA2000 CSCF/A-BG/HA SCM Deployment Example



Logical Network Interfaces (Reference Points)

Interfaces, used to support IMS in a CDMA network, can be defined within two categories: SIP and DIAMETER. The SCM incorporates standards-based interfaces for both SIP and DIAMETER network architectures.

SIP Interfaces

The following table provides descriptions of SIP interfaces supported by the SCM in a CDMA2000 network deployment.

Table 2. SIP Interfaces in a CDMA Network

Interface	Description
Gm	The reference point between the P-CSCF and the User Equipment (UE).The Gm interface provides SIP signaling between the PDSN and the P-CSCF.
MI	The reference point between the E-CSCF and Location Retrieval Function (LRF). The MI interface is used for routing an emergency call to a Public Safety Answering Point (PSAP). The E-CSCF interacts with the Location Retrieval Function (LRF) to identify the next hop PSAP.
Mw	The reference point between the P/S-CSCF and other CSCFs.The Mw interface provides SIP signaling between two CSCFs.

DIAMETER Interfaces

The following table provides descriptions of DIAMETER interfaces supported by the SCM in a CDMA2000 network deployment.

Table 3. DIAMETER Interfaces in a CDMA Network

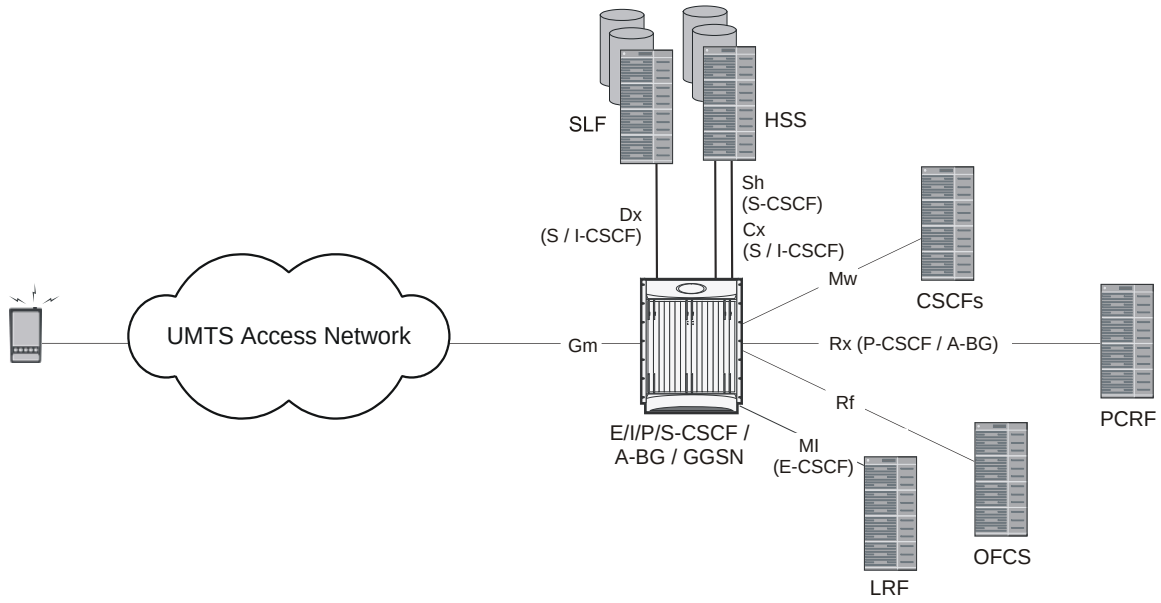
Interface	Description
Cx	The reference point between the S/I-CSCF and the Home Subscriber Server (HSS). The Cx interface is used to authenticate subscribers, provides server assignments, push user profile information from the HSS to the S-CSCF, and, when necessary, transmit a network initiated de-registration.
Dx	The reference point between the S/I-CSCF and Subscriber Location Function (SLF). The Dx interface is used to proxy queries to a subscriber data server (such as an HSS) in which subscription data for a user can be found. The SLF receives a query for the subscriber data server, looks up the address of appropriate subscriber data server, and proxies the query to the appropriate subscriber data server.
Rf	The reference point between the P-CSCF and the Offline Charging System (OFCS). The Rf interface is used to transfer charging information that will not affect, in real-time, the service being rendered. For more information, refer to the 3GPP2 specification X.S0013-007-A v1.0.
Sh	The reference point between the S-CSCF and Home Subscriber Server (HSS). The Sh interface is used for retrieval and update of call feature data parameters.
Tx	The reference point between the P-CSCF/A-BG and the Charging Rule Function (CRF)/Policy Decision Point (PDP) (PCRF) used for Service Based Bearer Control (SBBC). It identifies any P-CSCF/A-BG restrictions to be applied to the identified packet flows.

SCM in a GSM/UMTS Data Network Deployment

CSCF / A-BG / GGSN Deployment

The SCM is designed to function within a UMTS GGSN network. As shown in following figure, the SCM supports a number of interfaces used to communicate with other components in an IMS environment and supports the interface used to bridge the GGSN network.

Figure 5. GSM/UMTS CSCF/A-BG/GGSN SCM Deployment Example



Logical Network Interfaces (Reference Points)

Interfaces, used to support IMS in a UMTS network, can be defined within two categories: SIP and DIAMETER. The SCM incorporates standards-based interfaces for both SIP and DIAMETER network architectures.

SIP Interfaces

The following table provides descriptions of SIP interfaces supported by the SCM in a GSM/UMTS network deployment.

Table 4. SIP Interfaces in a GSM/UMTS Network

Interface	Description

Interface	Description
Gm	The reference point between the P-CSCF and the User Equipment (UE). The Gm interface provides SIP signaling between the GGSN and the P-CSCF.
MI	The reference point between the E-CSCF and Location Retrieval Function (LRF). The MI interface is used for routing an emergency call to a Public Safety Answering Point (PSAP). The E-CSCF interacts with the Location Retrieval Function (LRF) to identify the next hop PSAP.
Mw	The reference point between the P/S-CSCF and other CSCFs. The Mw interface provides SIP signaling between two CSCFs.

DIAMETER Interfaces

The following table provides descriptions of DIAMETER interfaces supported by the SCM in a GSM/UMTS network deployment.

Table 5. DIAMETER Interfaces in a GSM/UMTS Network

Interface	Description
Cx	The reference point between the S/I-CSCF and the Home Subscriber Server (HSS). The Cx interface is used to authenticate subscribers, provides server assignments, push user profile information from the HSS to the S-CSCF, and, when necessary, transmit a network initiated de-registration.
Dx	The reference point between the S/I-CSCF and Subscriber Location Function (SLF). The Dx interface is used to proxy queries to a subscriber data server (such as an HSS) in which subscription data for a user can be found. The SLF receives a query for the subscriber data server, looks up the address of appropriate subscriber data server, and proxies the query to the appropriate subscriber data server.
Rf	The reference point between the P-CSCF and the Offline Charging System (OFCS). The Rf interface is used to transfer charging information that will not affect, in real-time, the service being rendered. For more information, refer to the 3GPP2 specification X.S0013-007-A v1.0.
Rx	The reference point between the P-CSCF/A-BG and the Charging Rule Function (CRF)/Policy Decision Point (PDP) (PCRF). The Rx interface (3GPP 29.211) is used to exchange Flow Based Charging (FBC) control information between the PCRF and the P-CSCF/A-BG. The CRF uses the information to make FBC decisions that are then exchanged with the Traffic Plane Function (TPF). This interface is used in a 3GPP2 Release 7 implementation.
Sh	The reference point between the S-CSCF and Home Subscriber Server (HSS). The Sh interface is used for retrieval and update of call feature data parameters.

Features and Functionality - Base Software

The following is a list containing a variety of features found in the SCM and the benefits they provide.

Call Abort Handling

Call abort handling provides resource cleanup in error scenarios and makes sure resources that are not being used can be used for new calls. This feature is managed gracefully for a P-CSCF failure and CLI-initiated subscriber and session clean up.

Call Forking

Call forking allows subscribers to receive calls wherever they are by enabling multi-location UE registration.

Call Types Supported

In the IMS architecture, telephony features are normally provided by an external application server. Providing these features with the S-CSCF:

- Reduces the need for an additional SIP AS
- Simplifies the network architecture
- Improves latency for call setup and feature invocation

The following call types are supported:

- **Directory service, toll-free, long distance, international, and operator-assisted calls** - are supported through translation lists.
- **Emergency calls -** are managed through the addition of an Emergency Call/Session Control Function (E-CSCF) that routes emergency calls to a Public Safety Answering Point (PSAP).
- **Mobile-to-Mobile SIP calls** - supports SIP-based VoIP calls between mobile data users.
- **Public Switched Telephone Network (PSTN) calls** - can be routed through a 3GPP/2 compliant BGCF located in the S-CSCF.

Early IMS Security

Early IMS security allows authenticating the UE without IMS protocols and clients. Based on the 3GPP TR 33.978 specification, the SCM supports security inter-operation with 2G and non-IPSec user devices.

Emergency Call Support

P-CSCF gives priority to emergency calls, especially in a congested network. In addition, P-CSCF rejects new calls to any user who is in an emergency call.

Error Handling

The SCM supports consistent management of errors in a framework that considers existing and future standards and specifications.

Future-proof Solution

The SCM eliminates the capital and operational barriers associated with deploying traditional, server-based SIP proxies that lack carrier-class characteristics, occupy valuable rack space, and require numerous network interfaces, while also introducing additional control hops in the network that add call setup latency.

When operators deploy IMS/MMD, profitability will improve because a seamless on-ramp will be provided by simultaneously supporting 3GPP/3GPP2-based standards, P-CSCF functionality, and IETF SIP standards.

Intelligent Integration

For deployed platforms, no new hardware is necessary to install or manage. Functionality is enabled with a simple software download.

Intelligent integration lowers operational expenditure and reduces the number of network elements, network interfaces, and call setup latency.

Interworking Function

The SCM allows non-IMS UEs (pre IMS or RFC3261-compliant UEs) to work with the IMS core. When UEs are not IMS compliant, having this protocol interworking function at the edge allows the IMS core to be IMS compliant. After the interworking function inserts all necessary IMS headers toward the IMs core, the call appears to the IMS core network elements as if it is coming from an IMS-compliant UE.

The feature allows simultaneous support of IETF SIP and 3GPP/3GPP2 IMS/MMD clients.

MSRP Support

The SCM supports Message Session Relay Protocol (MSRP) session and page modes.

Presence Enabled

With its high transaction setup rate, this is an ideal solution to handle a large number of messages generated by presence signaling. CSCF supports all the presence RFC extensions and signaling and interoperates with several presence servers.

Redirection

The SCM supports response to 3xx redirect messages. In addition to supporting redirection as per 3GPP, it supports call redirection to other chassis in the network (based on configuration) in case of system overload.

Redundancy and Session Recovery

When enabled, provides automatic failover of existing CSCF sessions due to hardware or software faults.

The system recovers from a single hardware or software fault with minimal interruption to the subscriber's service and maintains session information to rebuild sessions if multiple faults occur.

Registration Event Package

A set of event notifications used to inform SIP node of changes made to a registration.

Signaling Compression (SigComp)

SigComp compresses SIP call setup messages and is supported on the P-CSCF component. This reduces bandwidth demands on the RAN and reduces setup times.

SIP Denial of Service (DoS) Attack Prevention

The A-BG provides a scalable proxy network and a distributed Network Address Translation (NAT) network which effectively mitigates DoS attacks.

Prevents a variety of DoS attacks specific to CSCF and SIP technology.

SIP Intelligence at the Core

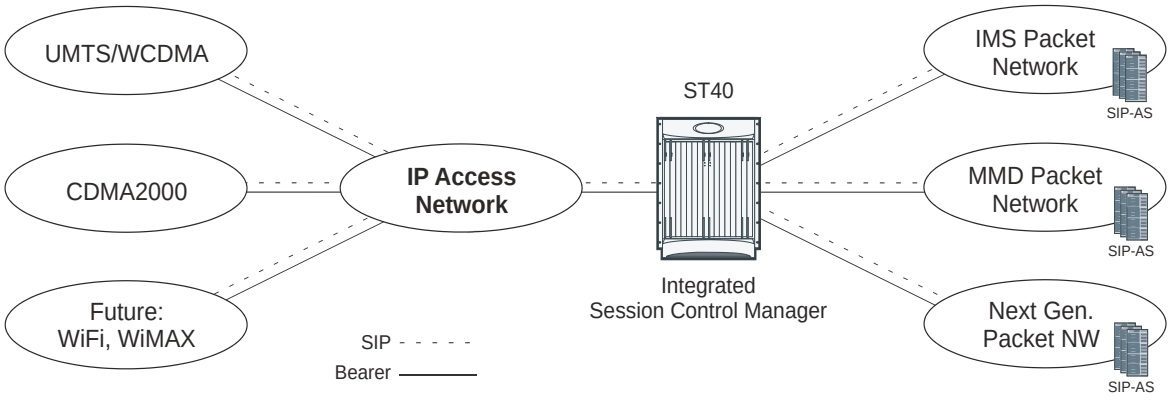
The SCM provides operators with an easy on-ramp for deploying SIP-based subscriber services while supporting various network control operations that provide the necessary intelligent control to insure a robust, carrier-class subscriber experience is achieved in this always changing multimedia environment.

When integrated into Cisco's session-aware Home Agent or GGSN platform, the SCM becomes the first SIP hop in the network, allowing operators to monitor and control all SIP-based sessions and execute additional value-added functions.

As the logical anchor point within the packet core, the SCM improves the user experience with device and location independence, and enhances subscriber control and policy enforcement with faster, more intelligent decisions for multimedia services.

Furthermore, as Fixed Mobile Convergence takes hold, it will be especially important to incorporate the SCM in the packet core in order to achieve mobility and voice continuity between multiple access networks (3G, WiFi, WiMAX, etc.).

Figure 6. Cisco Integrated Session Control Manager



SIP Large Message Support

Large notify contains information about multiple users in one message, which reduces the number of SIP messages in the network. Large SIP messages can be sent on UDP if the endpoint can support fragmentation; otherwise, UDP to TCP switching can be used to transport large messages intact.

If a request is within 200 bytes of the path MTU, or if it is larger than 1300 bytes and the path MTU is unknown, the request MUST be sent using TCP. This prevents fragmentation of messages over UDP and provides congestion control for larger messages. P-CSCF/A-BG is also able to handle messages up to the maximum datagram packet size. For UDP, this size is 65,535 bytes, including IP and UDP headers.

Large message support is needed for handling presence signaling traffic as the size of messages could be as large as 50K.

SIP Routing Engine

The SIP routing engine deploys SIP in a secure and controlled fashion.

Provides auto discovery of SIP elements, subscriber privacy, call fraud prevention, network security, and thwarting of network overload conditions.

Shared Initial Filter Criteria (SiFC)

If both the HSS and the S-CSCF support this feature, subsets of iFC may be shared by several service profiles. The HSS downloads the unique identifiers of the shared iFC sets to the S-CSCF. The S-CSCF uses a locally administered database to map the downloaded identifiers onto the shared iFC sets.

If the S-CSCF does not support this feature, the HSS will not download identifiers of shared iFC sets.

Telephony Application Server (TAS) Basic Supported

The following describe the local basic call features implemented on the S-CSCF:

- Abbreviated Dialing (AD)
- Call Forward Busy Line (CFBL)
- Call Forward No Answer (CFNA)
- Call Forward Not Registered (CFNR)
- Call Forward Unconditional (CFU)
- Call Transfer
- Call Waiting
- Caller ID Display (CID)
- Caller ID Display Blocked (CIDB)
- Feature Code Activation/De-activation
- Follow Me/Find Me
- Locally Allowed Abbreviated Dialing
- Outbound Call Restrictions/Dialing Permissions

- Short Code Dialing

TAS Basic provides basic voice call feature support in the SCM. In the IMS architecture, these telephony features are normally provided by an external application server. Providing these features with the S-CSCF:

- Reduces the need for an additional SIP AS
- Simplifies the network architecture
- Improves latency for call setup and feature invocation

The following describe the local basic call features implemented on the S-CSCF:

- **Abbreviated Dialing (AD)** - This feature allows the subscriber to call a Directory Number by entering less than the usual ten digits.Usually, the subscriber has four digit dialing to mimic PBX dialing privileges but these must be set up prior to use. When the SCM receives these numbers, it translates them and routes the call.
- **Call Forward Busy Line (CFBL)** - This feature forwards the call if busy line indication is received from the UE. If CFBL is enabled on both the AS and the S-CSCF, the call is forwarded by the S-CSCF on Busy Line indication. The feature detects and eliminates call forward loops if the History-Info header is present. It also terminates forwarding if forwarding causes the forward attempts to be more than the number specified in the Max-Forwards header.
- **Call Forward No Answer (CFNA)** - This feature forwards the call if no answer is received from the UE. If CFNA is enabled on both the AS and the S-CSCF, the call is forwarded by the S-CSCF on No Answer indication. The feature detects and eliminates call forward loops if the History-Info header is present. It also terminates forwarding if forwarding causes the forward attempts to be more than the number specified in the Max-Forwards header.
- **Call Forward Not Registered (CFNR)** - This feature forwards the call if the subscriber is not registered. If CFNR is enabled on both the AS and the S-CSCF, the call is forwarded by the S-CSCF on Not Registered indication. The feature detects and eliminates call forward loops if the History-Info header is present. It also terminates forwarding if forwarding causes the forward attempts to be more than the number specified in the Max-Forwards header.
- **Call Forward Unconditional (CFU)** - This feature unconditionally forwards the call. The check for local CFU is done prior to the filter criteria and before any AS interaction. Thus CFU is enabled on both the S-CSCF and the destination AS, the local CFU occurs and there is no AS interaction. The feature eliminates basic loop detection (A calls B which is forwarded to A) and if the History-Info header is present, enhanced loop detection is performed based on the contents of this header. It also terminates forwarding if forwarding causes the forward attempts to be more than the number specified in the Max-Forwards header.
- **Call Transfer** - This feature allows the subscriber to transfer a call.
- **Call Waiting** - This feature allows the subscriber to receive a second call while on the first call.
- **Caller ID Display (CID)** - This feature inserts P-Preferred-Identity which communicates the identity of the user within the trust domain. If this header is already present, the feature may not do anything different.
- **Caller ID Display Blocked (CIDB)** - This feature removes P-Preferred-Identity and P-Preferred-Asserted-Identity headers and inserts a Privacy header with the privacy value set to “id”.
- **Feature Code Activation/De-activation** - This feature allows for activating and de-activating certain features using a star (*) - number sequence (star code). Registered subscribers have the option of activating or deactivated call features using specified star codes. The SCM translates these codes and routes the call.
- **Follow Me/Find Me** - This feature invokes the incoming call to several configured destinations in parallel and connects the call to the first destination that responds, “tearing down” all the other calls. There are two possible implementations of this feature; one a sequential implementation in which each destination is attempted in

sequence till a successful connection. The other is a parallel approach in which several destinations are tried simultaneously. The advantage of the parallel approach is a faster set up.

- **Locally Allowed Abbreviated Dialing** - This feature allows the subscriber to dial a local-only, legacy, short code such as *CG or *POL. The SCM translates these codes to a ten-digit directory number and routes the call.
- **Outbound Call Restrictions/Dialing Permissions** - This feature restricts subscribers from initiating certain outbound calls. For example, if a subscriber attempts to make an international call and is not permitted to, the S-CSCF rejects the call.
- **Short Code Dialing** - This feature allows the subscriber to dial a short code such as #PAYor #MIN. The SCM translates these codes and routes the call.

Trust Domain

Enables the identification of trusted network entities. This keeps subscriber information confidential when it is received.

Features and Functionality - Licensed Enhanced Feature Support

This section describes optional enhanced features and functions.

Each of the following optional enhanced features require the purchase of an additional license to implement the functionality with the SCM.

Important: For more information about enhanced features in this section, refer to the *System Enhanced Feature Configuration Guide*.

Interchassis Session Recovery

The ASR 5000 provides industry leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operational state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

- Under normal N+1 PSC/PSC2 hardware redundancy, if a catastrophic packet processing card failure occurs all affected calls are migrated to the standby packet processing card if possible. Calls which cannot be migrated are gracefully terminated with proper call-termination signaling and accounting records are generated with statistics accurate to the last internal checkpoint
- If the Session Recovery feature is enabled, any total packet processing card failure will cause a packet processing card switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though Cisco Systems provides excellent intra-chassis redundancy with these two schemes, certain catastrophic failures which can cause total chassis outages, such as IP routing failures, line-cuts, loss of power, or physical destruction of the chassis, cannot be protected by this scheme. In such cases, the Interchassis Session Recovery feature provides geographic redundancy between sites. This has the benefit of not only providing enhanced subscriber experience even during catastrophic outages, but can also protect other systems such as the RAN from subscriber re-activation storms.

The Interchassis Session Recovery feature allows for continuous call processing without interrupting subscriber services. This is accomplished through the use of redundant chassis. The chassis are configured as primary and backup with one being active and one in recovery mode. A checkpoint duration timer is used to control when subscriber data is sent from the active chassis to the inactive chassis. If the active chassis handling the call traffic goes out of service, the inactive chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a propriety TCP-based connection called a redundancy link. This link is used to exchange Hello messages between the primary and backup chassis and must be maintained for proper system operation.

- **Interchassis Communication**

Chassis configured to support Interchassis Session Recovery communicate using periodic Hello messages. These messages are sent by each chassis to notify the peer of its current state. The Hello message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a Hello message to be received from the chassis' peer. If the standby chassis does not receive a Hello message from the active chassis within the dead interval, the standby chassis transitions to the active state. In situations where the redundancy link goes out of service, a priority scheme is used to determine which chassis processes the session. The following priority scheme is used:

- router identifier
- chassis priority
- SPIO MAC address

- **Checkpoint Messages**

  Checkpoint messages are sent from the active chassis to the inactive chassis. Checkpoint messages are sent at specific intervals and contain all the information needed to recreate the sessions on the standby chassis, if that chassis were to become active. Once a session exceeds the checkpoint duration, checkpoint data is collected on the session. The checkpoint parameter determines the amount of time a session must be active before it is included in the checkpoint message.

Important: For more information on interchassis session recovery support, refer to the *Interchassis Session Recovery* chapter in the *System Enhanced Feature Configuration Guide*.

IPSec Support

Encrypted IPSec tunnels are terminated and decrypted so that traffic coming from untrusted networks are secured before entering the secure operator network. This prevents eavesdropping, hijacking, and other intrusive behavior from occurring.

IP Security (IPSec) is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways.

Important: IPSec implementation is a mandatory part of IPv6, but it is optional to secure IPv4 traffic.

Important: For more information on IPSec support, refer to the *IP Security* chapter in the *System Enhanced Feature Configuration Guide*.

IPv4-IPv6 Interworking

This feature allows the P-CSCF to provide IPv4-IPv6 interworking in the following scenarios:

- When UEs are IPv6-only and the IMS core network is IPv4-only

- When UEs are IPv4-only and the IMS core network is IPv6-only

In addition, IPv4-IPv6 interworking helps an IPv4 IMS network transition to an all-IPv6 IMS network.

The following interworking requirements are currently supported:

- MSRP support when IPv4-IPv6 interworking is enabled
- IPv4 TCP and IPv6 TCP
- Transport switching allowed based on size for both v4 and v6 network
- UDP fragmentation allowed for both v4 and v6 networks
- P-CSCF supports Mw and Gm interfaces on both v4 and v6
- KPIs for Mw and Gm interfaces are supported on both v4 and v6
- DNS supported for v4 and v6 networks
- Interworking supported for IM and presence
- Both v4 and v6 handsets are supported simultaneously on the same P-CSCF node

P-CSCF will provide IPv4-IPv6 interworking functionality between IPv6-only UEs and IPv4-only core network elements (I/S-CSCF) by acting as a dual stack. To achieve the dual-stack behavior, P-CSCF will be configured in two services with the first service (V6-SVC) listening on an IPv6 address and the second service (V4-SVC) listening on an IPv4 address. SIP messages coming from IPv6 UEs will come to V6-SVC and will be forwarded to the IPv4 core network through V4-SVC. Similarly, messages from the IPv4 core network come to V4-SVC and will be forwarded to IPv6 UEs via V6-SVC. P-CSCF also provides interworking functionality between IPV4-only UEs and IPv6-only core network elements.

P-CSCF handling different v4-v6 interworking scenarios is shown below.

Figure 7. Interworking Between IPv6 UE and IPv4 IMS Core Network

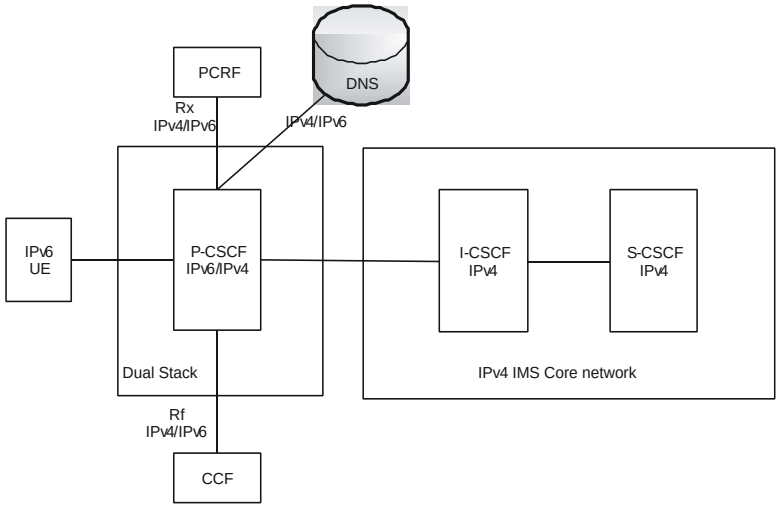
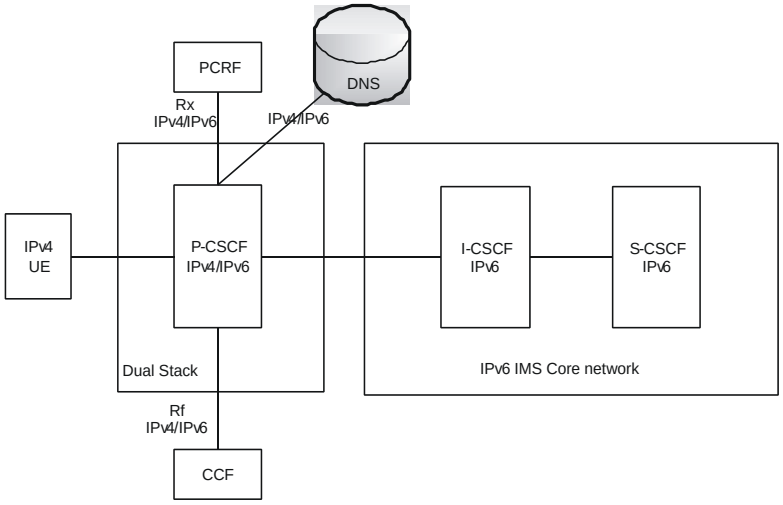


Figure 8. Interworking Between IPv4 UE and IPv6 IMS Core Network



To identify the need for IPv4-IPv6 interworking for a new incoming IPv6 REGISTER arriving at V6-SVC, a route lookup is performed based on the request-uri, first in V4-SVC context and then in V6-SVC context if the first lookup does not return any matching route entry. If a matching IPv4 next-hop route entry is found, then this indicates that interworking needs to be done. If no route entry is found, then a DNS query on request-uri domain is done for both A and AAAA type records. If DNS response yields only an IPv4 address, then this is also the case for performing IPv4-IPv6 interworking.

Headers (such as Via, Path, etc.) are automatically set to IPv4 bind address of P-CSCF V4-SVC. Remaining headers will be not be altered and sent as is toward the S-CSCF. The IPv4 address in a Path header received from S-CSCF in 200Ok of REGISTER will be replaced with V6-SVC's IPv6 address before forwarding to UE.

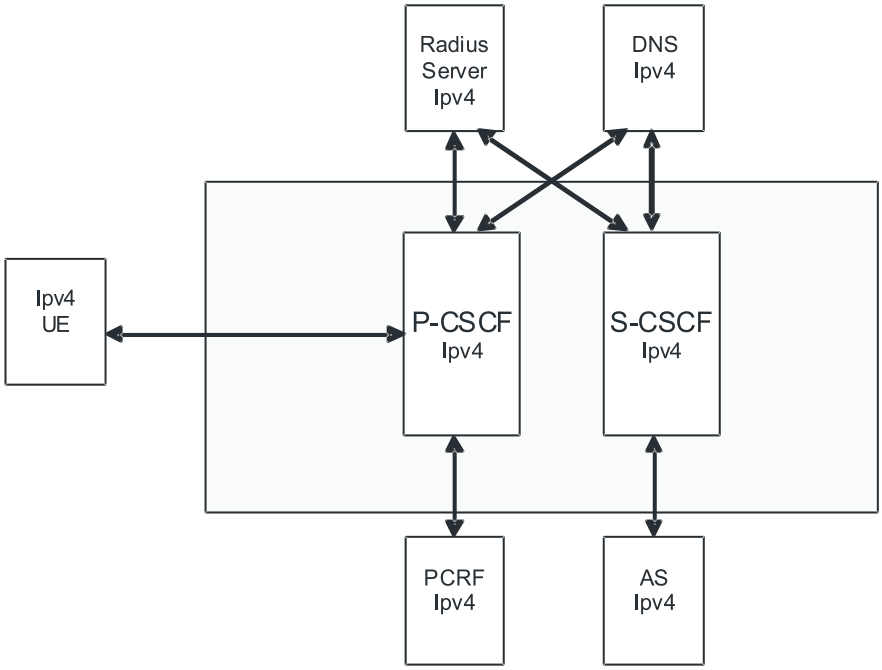
IPv6 Support

In addition to supporting IPv4, the SCM supports IPv6 addressing. A CSCF service can be configured with v6 addresses to support an all v6 network.

Important: For this feature, you may bind a CSCF service to either an IPv4 address or to an IPv6 address, but not both simultaneously.

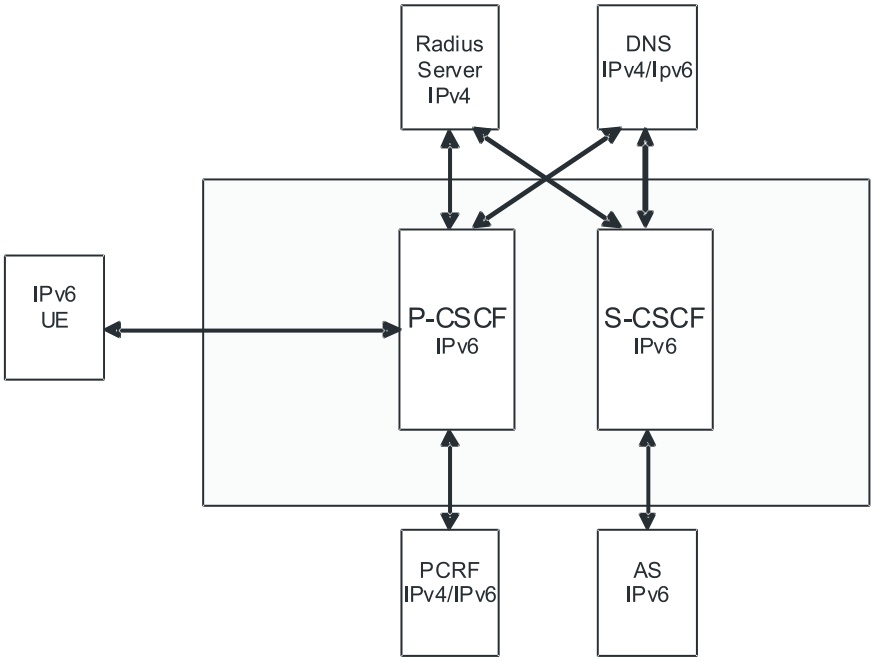
The following diagram shows the implementation where CSCF supports only IPv4.

Figure 9. IPv4 Configuration



With IPv6 support, the configuration supported would look like the following diagram. The DNS server could be either IPv4 or IPv6.

Figure 10. IPv6 Configuration



Important: The policy interface to PCRF will be IPv6 based when DIAMETER supports IPv6.

Session Recovery Support

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

Session recovery is performed by mirroring key software processes (e.g. session manager and AAA manager) within the system. These mirrored processes remain in an idle state (in standby-mode), wherein they perform no processing, until they may be needed in the case of a software failure (e.g. a session manager task aborts). The system spawns new instances of “standby mode” session and AAA managers for each active Control Processor (CP) being used.

Additionally, other key system-level software tasks, such as VPN manager, are performed on a physically separate Packet Services Card (PSC/PSC2) to ensure that a double software fault (e.g. session manager and VPN manager fails at same time on same card) cannot occur. The PSC/PSC2 used to host the VPN manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

The additional hardware resources required for session recovery include a standby System Management Card (SMC) and a standby PSC/PSC2.

There are two modes for Session Recovery.

- **Task recovery mode**: Wherein one or more session manager failures occur and are recovered without the need to use resources on a standby PSC. In this mode, recovery is performed by using the mirrored “standby-mode” session manager task(s) running on active PSCs. The “standby-mode” task is renamed, made active, and is then populated using information from other tasks such as AAA manager.

- **Full PSC/PSC2 recovery mode**: Used when a PSC hardware failure occurs, or when a PSC migration failure happens. In this mode, the standby PSC is made active and the “standby-mode” session manager and AAA manager tasks on the newly activated PSC perform session recovery.

Session/Call state information is saved in the peer AAA manager task because each AAA manager and session manager task is paired together. These pairs are started on physically different PSCs/PSC2s to ensure task recovery.

Important: Session Recovery is supported for either IPv4 or IPv6 traffic.

Important: For more information on session recovery support, refer to the *Session Recovery* chapter in the *System Enhanced Feature Configuration Guide*.

How the SCM Works

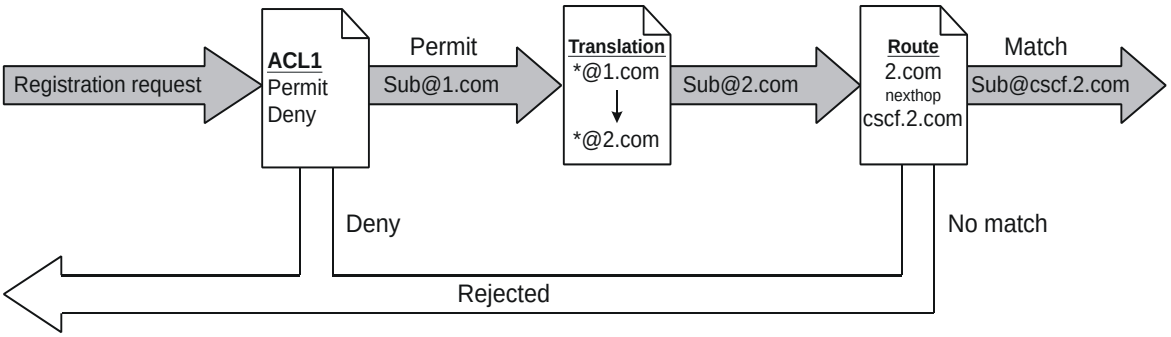
This section provides information on the function of the SCM in a CDMA2000 PDSN or UMTS GGSN network and presents call procedure flows for different stages of session setup.

Admission and Routing

Admission and routing of subscriber URIs is performed through a number of configurable lists in the SCM.

The following sections describe the main admission and routing techniques used in the SCM. The following figure presents the method and order for admitting and routing sessions within the SCM.

Figure 11. Admission and Routing Method



CSCF Access Control Lists

Access Control Lists (ACLs) are a set of rules that are applied during CSCF session establishment. A typical use of these rules is to accept or deny registration or session establishment requests. ACLs may be tied to subscribers and/or the whole service. Subscriber based ACLs can also be imported from an external ACL/policy server. In that event, the external policy server address would be configured with the service.

A complete explanation of the ACL configuration method is located in Access Control Lists Appendix of the Session Control Manager Configuration Guide.

Translation Lists

Translation lists help modify request-uri (i.e. addressing of a CSCF session). One example is that E.164 numbers could be altered by adding prefixes and suffixes or the request-uri could be modified based on the registration database.

Route Lists

Route lists are service level lists that assist in finding the next CSCF/UA hop. These are static routes and will override any dynamic routes (based on DNS queries for FQDNs).

Signaling Compression

The Session Initiation Protocol (SIP) is a text-based protocol designed for higher bandwidth networks. As such, it is inherently less suited for lower bandwidth environments such as wireless networks. If a wireless handset uses SIP to set up a call, the setup time is significantly increased due to the high overhead of text-based signaling messages.

Signaling Compression (SigComp) is a solution for compressing/decompressing messages generated by application protocols such as SIP. The P-CSCF component of the SCM uses SigComp to reduce call setup times on the access network, typically between the P-CSCF and the UE. The following features are supported:

- **SigComp Detection** - P-CSCF detects if the UE supports SigComp and compresses messages it sends to the UE. The P-CSCF also detects if messages it receives are compressed and decompresses them.
- **SigComp Parameter Configuration** - P-CSCF allows the configuration of Decompression Memory Size (DMS), State Memory Size (SMS), and Cycles Per Bit (CPB).
- **Failure Acknowledgement** - P-CSCF replies with NACK on decompression failure.
- **SIP/SDP Static Dictionaries** - P-CSCF supports the Session Initiation Protocol/Session Description Protocol Static Dictionary for Signaling Compression.

Supported Standards

The SCM service complies with the following standards for CDMA2000 PDSN and UMTS GGSN network wireless data services.

Release 8 3GPP References

Important: The SCM currently supports the following Release 8 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 would be listed under Release 8 3GPP2 References.

- TS 23.167 IP Multimedia Subsystem (IMS) emergency sessions
- TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
- TS 29.214 Policy and charging control over Rx reference point
- TS 33.178 Security aspects of early IP Multimedia Subsystem (IMS)
- TS 33.978 Security aspects of early IP Multimedia Subsystem (IMS)

Release 7 3GPP References

Important: The SCM currently supports the following Release 7 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under Release 7 3GPP2 References.

- TR 23.806 Voice call continuity between Circuit Switched (CS) and IP Multimedia Subsystem (IMS) Study
- TR 23.808 Supporting Globally Routable User Agent URI (GRUU) in IMS; Report and conclusions
- TR 23.816 Identification of Communication Services in IMS
- TR 24.930 IP Multimedia core network Subsystem (IMS) based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
- TR 29.847 Conferencing based on SIP, SDP, and other protocols; Functional models, information flows and protocol details
- TR 33.978 Security aspects of early IP Multimedia Subsystem (IMS)
- TS 22.101 Service principles

- TS 23.003 Numbering, addressing and identification
- TS 23.107 Quality of Service (QoS) concept and architecture
- TS 23.125 Overall high level functionality and architecture impacts of flow based charging; Stage 2
- TS 23.141 Presence service; Architecture and functional description; Stage 2
- TS 23.167 IP Multimedia Subsystem (IMS) emergency sessions
- TS 23.203 Policy and charging control architecture
- TS 23.204 Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access; Stage 2
- TS 23.207 End-to-end Quality of Service (QoS) concept and architecture
- TS 23.218 IP Multimedia (IM) session handling; IM call model; Stage 2
- TS 23.221 Architectural Requirements
- TS 23.228 IP Multimedia Subsystem (IMS); Stage 2
- TS 23.271 Functional description of Location Services (LCS)
- TS 23.981 Interworking aspects and migration scenarios for IPv4 based IMS Implementations
- TS 24.141 Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3
- TS 24.228 Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
- TS 24.229 Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
- TS 24.341 Support of SMS over IP networks; Stage 3
- TS 26.114 IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction
- TS 26.141 IP Multimedia System (IMS) Messaging and Presence; Media formats and codecs
- TS 26.234 Transparent end-to-end Packet-switched Streaming Service (PSS); Protocols and codecs
- TS 26.235 Packet switched conversational multimedia applications; Default codecs
- TS 26.236 Packet switched conversational multimedia applications; Transport protocols
- TS 29.207 Policy control over Go interface
- TS 29.208 End-to-end Quality of Service (QoS) signalling flows
- TS 29.209 Policy control over Gq interface
- TS 29.214 Policy and charging control over Rx reference point
- TS 29.228 IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents
- TS 29.229 IMS Cx and Dx interfaces based on the Diameter protocol; Protocol details
- TS 29.328 IMS Sh interface: signalling flows and message content
- TS 29.329 IMS Sh interface based on the Diameter protocol; Protocol details
- TS 31.103 Characteristics of the IMS Identity Module (ISIM) application
- TS 32.225 Telecommunication management; Charging management; Charging data description for the IP Multimedia Subsystem (IMS)
- TS 32.240 Telecommunication management; Charging management; Charging architecture and principles
- TS 32.260 Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging
- TS 33.102 3G security; Security architecture

- TS 33.203 3G security; Access security for IP-based services

Release 7 3GPP2 References

- S.R0079-A v1.0 Support for End-to-End QoS - Stage 1 Requirements
- S.R0086-A v1.0 IMS Security Framework
- X.S0013-000-A v1.0 All-IP Core Network Multimedia Domain - Overview
- X.S0013-002-A v1.0 All-IP Core Network Multimedia Domain - IP Multimedia Subsystem Stage 2
- X.S0013-003-0 v2.0 All-IP Core Network Multimedia Domain - IP Multimedia (IMS) Session Handling; IP Multimedia (IM) Call Model - Stage 2
- X.S0013-004-A v1.0 All-IP Core Network Multimedia Domain - IP Multimedia Call Control Protocol Based on SIP and SDP Stage 3
- X.S0013-005-0 All-IP Core Network Multimedia Domain: IP Multimedia Subsystem Cx Interface Signaling Flows and Message Contents
- X.S0013-006-0 All-IP Core Network Multimedia Domain - Cx Interface Based on the Diameter Protocol; Protocol Details
- X.S0013-007-0 All-IP Core Network Multimedia Domain: IP Multimedia Subsystem - Charging Architecture
- X.S0013-007-A v1.0 All-IP Core Network Multimedia Domain - IP Multimedia Subsystem - Charging Architecture
- X.S0013-008-0 All-IP Core Network Multimedia Domain: IP Multimedia Subsystem - Accounting Information Flows and Protocol
- X.S0013-008-A All-IP Core Network Multimedia Domain - IP Multimedia Subsystem - Offline Accounting Information Flows and Protocol
- X.S0013-010-0 v1.0 All-IP Core Network Multimedia Domain: IP Multimedia Subsystem Sh Interface; Signaling Flows and Message Contents - Stage 2
- X.S0013-011-0 v1.0 All-IP Core Network Multimedia Domain: Sh Interface Based on Diameter Protocols Protocol Details - Stage 3
- X.S0013-012-0 v1.0 All-IP Core Network Multimedia Domain - Service Based Bearer Control - Stage 2
- X.S0013-014-0 v1.0 All-IP Core Network Multimedia Domain - Service Based Bearer Control - Tx Interface Stage 3
- X.S0016-000-A v1.0 3GPP2 Multimedia Messaging System MMS Specification Overview, Revision A
- X.S0027-002-0 v1.0 Presence Security
- X.S0027-003-0 v1.0 Presence Stage 3
- X.S0029-0 v1.0 Conferencing Using the IP Multimedia (IM) Core Network (CN) Subsystem
- X.S0049-0 v1.0 All-IP Network Emergency Call Support

IETF References

- RFC 1594 (March 1994): “FYI on Questions and Answers to Commonly Asked “New Internet User” Questions”
- RFC 1889 (January 1996): “RTP: A Transport Protocol for Real-Time Applications”
- RFC 2327 (April 1998) SDP: Session Description Protocol
- RFC 2401 (November 1998): “Security Architecture for the Internet Protocol (IPSec)”
- RFC 2403 (November 1998): “The Use of HMAC-MD5-96 within ESP and AH”
- RFC 2404 (November 1998): “The Use of HMAC-SHA-1-96 within ESP and AH”
- RFC 2462 (December 1998): “IPv6 Address Autoconfiguration”
- RFC 2617 (June 1999): “HTTP Authentication: Basic and Digest Access Authentication”
- RFC 2753 (January 2000): “A Framework for Policy-based Admission Control”
- RFC 2833 (May 2000): “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”
- RFC 2915 (September 2000) The Naming Authority Pointer (NAPTR) DNS Resource Record
- RFC 2976 (October 2000): “The SIP INFO Method”
- RFC 3041 (January 2001): “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”
- RFC 3261 (June 2002): “SIP: Session Initiation Protocol”
- RFC 3262 (June 2002): “Reliability of provisional responses in Session Initiation Protocol (SIP)”
- RFC 3263 (June 2002): “Session Initiation Protocol (SIP): Locating SIP Servers”
- RFC 3264 (June 2002): “An Offer/Answer Model with Session Description Protocol (SDP)”
- RFC 3265 (June 2002): “Session Initiation Protocol (SIP) - Specific Event Notification”
- RFC 3310 (September 2002): “Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)”
- RFC 3311 (September 2002): “The Session Initiation Protocol (SIP) UPDATE Method”.
- RFC 3312 (October 2002): “Integration of Resource Management and Session Initiation Protocol (SIP)”
- RFC 3313 (January 2003): “Private Session Initiation Protocol (SIP) Extensions for Media Authorization”
- RFC 3315 (July 2003): “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”
- RFC 3320 (January 2003): “Signaling Compression (SigComp)”
- RFC 3321 (January 2003): “Signaling Compression (SigComp) - Extended Operations”
- RFC 3323 (November 2002): “A Privacy Mechanism for the Session Initiation Protocol (SIP)”
- RFC 3325 (November 2002): “Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks”
- RFC 3326 (December 2002): “The Reason Header Field for the Session Initiation Protocol (SIP)”
- RFC 3327 (December 2002): “Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts”
- RFC 3329 (January 2003): “Security Mechanism Agreement for the Session Initiation Protocol (SIP)”
- RFC 3388 (December 2002): “Grouping of Media Lines in the Session Description Protocol (SDP)”

- RFC 3428 (December 2002): “Session Initiation Protocol (SIP) Extension for Instant Messaging”
- RFC 3455 (January 2003): “Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)”
- RFC 3485 (February 2003): “The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp)”
- RFC 3486 (February 2003): “Compressing the Session Initiation Protocol (SIP)”
- RFC 3515 (April 2003): “The Session Initiation Protocol (SIP) Refer method”
- RFC 3556 (July 2003): “Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth”
- RFC 3581 (August 2003): “An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing”
- RFC 3588 (September 2003): “Diameter Base Protocol”
- RFC 3608 (October 2003): “Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration”
- RFC 3665 (December 2003): “Session Initiation Protocol (SIP) Basic Call Flow Examples”
- RFC 3680 (March 2004): “A Session Initiation Protocol (SIP) Event Package for Registrations”
- RFC 3761 (April 2004): “The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)”
- RFC 3824 (June 2004): “Using E.164 numbers with the Session Initiation Protocol (SIP)”
- RFC 3840 (August 2004): “Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)”
- RFC 3841 (August 2004): “Caller Preferences for the Session Initiation Protocol (SIP)”
- RFC 3842 (August 2004): “A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)”
- RFC 3856 (August 2004): “A Presence Event Package for the Session Initiation Protocol (SIP)”
- RFC 3857 (August 2004): “A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)”
- RFC 3858 (August 2004): “An Extensible Markup Language (XML) Based Format for Watcher Information”
- RFC 3861 (August 2004): “Address Resolution for Instant Messaging and Presence”
- RFC 3891 (September 2004): “The Session Initiation Protocol (SIP) “Replaces” Header”
- RFC 3892 (September 2004): “The Session Initiation Protocol (SIP) Referred-By Mechanism”
- RFC 3903 (October 2004): “Session Initiation Protocol (SIP) Extension for Event State Publication”
- RFC 3911 (October 2004): “The Session Initiation Protocol (SIP) “Join” Header”
- RFC 3966 (December 2004): “The tel URI for Telephone Numbers”
- RFC 3986 (January 2005): “Uniform Resource Identifier (URI): Generic Syntax”
- RFC 4028 (April 2005): “Session Timers in the Session Initiation Protocol (SIP)”
- RFC 4032 (March 2005): “Update to the Session Initiation Protocol (SIP) Preconditions Framework”
- RFC 4077 (May 2005): “A Negative Acknowledgement Mechanism for Signaling Compression”
- RFC 4244 (November 2005): “An Extension to the Session Initiation Protocol (SIP) for Request History Information”
- RFC 4317 (December 2005): “Session Description Protocol (SDP) Offer/Answer Examples”

- RFC 4353 (February 2006): “A Framework for Conferencing with the Session Initiation Protocol (SIP)”
- RFC 4475 (May 2006): “Session Initiation Protocol (SIP) Torture Test Messages”
- RFC 4566 (July 2006): “SDP: Session Description Protocol”
- RFC 4975 (September 2007): “Message Session Relay Protocol (MSRP)”
- RFC 5031 (January 2008): “A Uniform Resource Name (URN) for Emergency and Other Well-Known Services”
- RFC 5049 (December 2007): “Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)”
- RFC 5112 (January 2008): “The Presence-Specific Static Dictionary for Signaling Compression (Sigcomp)”
- draft-ietf-sip-outbound-11 (November 2007): “Managing Client Initiated Connections in the Session Initiation Protocol (SIP)”

Other

- Packet-Cable spec (PKT-TR-SEC-V02-061013)

Chapter 2
Configuration

This chapter provides configuration information for the SCM.

Important: Information about all commands in this chapter can be found in the *Command Line Interface Reference*.

Because each wireless network is unique, the system is designed with a variety of parameters allowing it to perform in various wireless network environments. In this chapter, only the minimum set of parameters are provided to make the system operational. Optional configuration commands specific to the SCM product are located in the *Command Line Interface Reference*.

The following procedures are located in this chapter:

- Configuring the System to Perform as a Proxy-CSCF
- Configuring the System to Perform as a Serving-CSCF
- Configuring the System to Perform as an Emergency-CSCF
- Configuring the System to Perform as an A-BG

Configuring the System to Perform as a Proxy-CSCF

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as a Proxy-CSCF in a test environment. For a more robust configuration example, refer to the *Sample Configuration Files*appendix.

To configure the system to perform as a Proxy-CSCF:

Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Set initial configuration parameters such as creating the VPN context and CSCF service by applying the example configurations found in the Initial Configuration section.

Step 3 Configure the system to perform as a Proxy-CSCF and set basic CSCF parameters such as service configuration, session limits, default AoR domain, CSCF peer servers, access control, translation and route lists, CSCF policy, and session template by applying the example configurations presented in the Proxy-CSCF Configuration section.

Step 4 Configure additional P-CSCF context parameters by applying the example configuration found in the P-CSCF Context Configuration section.

Step 5 Log system activity by applying the example configuration found in the CSCF Logging Configuration section.

Step 6 Save the configuration by following the steps found in the Save the Configuration section.

Initial Configuration

Step 1 Set local system management parameters by applying the example configuration in the Modifying the Local Context section.

Step 2 Create the context where the P-CSCF service will reside by applying the example configuration in the Creating a P-CSCF VPN Context section.

Step 3 Create the P-CSCF service within the newly created context by applying the example configuration in the Creating the CSCF Service section.

Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
   context local
            interface <interface_name>
               ip address <ip_address> <ip_mask>
```

```
            exit
         server ftpd
            exit
         server telnetd
            exit
         subscriber default
            exit
         administrator <name> encrypted password <password> ftp
         ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
         exit
      port ethernet <slot#/port#>
         no shutdown
         bind interface <local_context_interface_name> local
         exit
      end
```

Creating a P-CSCF VPN Context

Use the following example to create a P-CSCF VPN context and interface, and bind the VPN interface to a configured Ethernet port.

```
configure
      context <p-cscf_context_name> -noconfirm
         interface <p-cscf_interface_name>
            ip address <address>
            exit
         ip route 0.0.0.0 0.0.0.0 <next_hop_address> <s-cscf_interface_name>
         exit
      port ethernet <slot_number/port_number>
         no shutdown
         bind interface <p-cscf_interface_name> <p-cscf_context_name>
```

```
        end
```

Creating the CSCF Service

Use the following configuration example to create the CSCF service:

```
configure
    context <p-cscf_context_name>
        cscf service <p-cscf_service_name> -noconfirm
            end
```

Proxy-CSCF Configuration

- Set the system's role as a Proxy-CSCF and configure service settings by applying the example configuration in the Setting the Systems Role as a Proxy-CSCF and Configuring Service Settings section.
- Configure communication with CSCF peer servers by applying the example configuration in the Identifying CSCF Peer Servers section.
- Specify ACLs and route lists by applying the example configuration in the Configuring Access Control and Route Lists section.
- Configure the CSCF policy and session template by applying the example configuration in the Setting the CSCF Policy and CSCF Session Template section.

Setting the System's Role as a Proxy-CSCF and Configuring Service Settings

Use the following configuration example to set the system to perform as a Proxy-CSCF and configure the CSCF service:

```
configure
    context <p-cscf_context_name>
        cscf service <p-cscf_service_name>
            bind address <ip_address> port <port_num>
            session-timer session-expires <value>
            session-timer min-se <value>
            keepalive method crlf max-retry <value> expire-timer <value>
```

```
            keepalive method stun max-retry <value> expire-timer <value>
            recurse-on-redirect-resp
            subscription package reg
            default-aor-domain <name>
            subscriber-policy-override
            proxy-cscf
               allow rfc3261-ua-interworking
               end
```

Identifying CSCF Peer Servers

Use the following example to identify peer servers to the P-CSCF:

```
configure
         context <p-cscf_context_name>
            cscf peer-servers <name> type <type> -noconfirm
               server <name> address <ip_address> port <number>
               hunting-method sequential-on-failure
               end
```

Configuring Access Control and Route Lists

Use the following example to configure CSCF access control lists (ACLs), CSCF translation lists, and CSCF route lists:

```
configure
         context <p-cscf_context_name>
            cscf acl default
               permit source aor $.
               exit
            cscf routes default
               end
```

Setting the CSCF Policy and CSCF Session Template

Use the following example to configure CSCF policy and session templates:

```
configure
         context <p-cscf_context_name>
            cscf policy default
               exit
            cscf session-template name <name>
               inbound-cscf-acl default
               outbound-cscf-acl default
               route-list default
               translation-list default
               cscf-policy-profile default
               cscf-urn-service-list default
               end
```

P-CSCF Context Configuration

Use the following example to configure additional P-CSCF context parameters such as local subscribers for SIP UAs, AAA groups, and IP network settings:

```
configure
         context <p-cscf_context_name>
            subscriber default
               exit
            aaa group default
               exit
            domain <name>
            ip domain-lookup
```

```
ip name-servers <ip_addr>
dns-client <name>
   bind address <ip_addr>
   cache ttl positive <sec>
   cache ttl negative <sec>
   end
```

CSCF Logging Configuration

Use the following example to configure logging for the CSCF application:

```
logging filter active facility sessmgr level critical
logging filter active facility cscfmgr level critical
logging filter active facility cscf level critical
logging active
```

Save the Configuration

Refer to *Verifying and Saving Your Configuration* to save changes made to the Proxy-CSCF configuration.

Configuring the System to Perform as a Serving-CSCF

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as a Serving-CSCF in a test environment. For a more robust configuration example, refer to the *Sample Configuration Files*appendix.

To configure the system to perform as a Serving-CSCF:

Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Set initial configuration parameters such as creating the VPN context and CSCF service by applying the example configurations found in the Initial Configuration section.

Step 3 Configure S-CSCF context parameters by applying the example configuration found in the S-CSCF Context Configuration section.

Step 4 Configure the system to perform as a Serving-CSCF and set basic CSCF parameters such as service configuration, default AoR domain configuration, CSCF peer servers, access control, translation and route lists, and session template by applying the example configurations presented in the Serving-CSCF Configuration section.

Step 5 *Optional:* Configure the S-CSCF to also perform as an Interrogating-CSCF by applying the example configurations presented in the Optional Interrogating-CSCF Configuration section.

Step 6 Configure accounting service by applying the example configuration found in the CDR Accounting Service Configuration section.

Step 7 Log system activity by applying the example configuration found in the CSCF Logging Configuration section.

Step 8 Save the configuration by following the steps found in the Save the Configuration section.

Initial Configuration

Step 1 Set local system management parameters by applying the example configuration in the Modifying the Local Context section.

Step 2 Create the context where the S-CSCF service will reside by applying the example configuration in the Creating an S-CSCF VPN Context section.

Step 3 Create the S-CSCF service within the newly created context by applying the example configuration in the Creating the CSCF Service section.

Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
```

```
context local
         interface <interface_name>
            ip address <ip_address> <ip_mask>
            exit
         server ftpd
            exit
         server telnetd
            exit
         subscriber default
            exit
         administrator <name> encrypted password <password> ftp
         ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
         exit
      port ethernet <slot#/port#>
         no shutdown
         bind interface <local_context_interface_name> local
         exit
      end
```

Creating an S-CSCF VPN Context

Use the following example to create an S-CSCF VPN context and interface, and bind the VPN interface to a configured Ethernet port.

```
configure
      context <s-cscf_context_name> -noconfirm
         interface <s-cscf_interface_name>
            ip address <address>
            exit
         ip route 0.0.0.0 0.0.0.0 <next_hop_address> <s-cscf_interface_name>
         exit
```

```
        port ethernet <slot_number/port_number>
           no shutdown
           bind interface <s-cscf_interface_name> <s-cscf_context_name>
           end
```

Creating the CSCF Service

Use the following configuration example to create the CSCF service:

```
configure
        context <s-cscf_context_name>
           cscf service <s-cscf_service_name> -noconfirm
              end
```

S-CSCF Context Configuration

Use the following example to configure additional S-CSCF context parameters such as local subscribers for SIP UAs, AAA groups, and IP network settings:

```
configure
        context <s-cscf_context_name>
           ims-sh-service <name>
              diameter dictionary standard
              diameter endpoint <hss_host_name>
              exit
           subscriber default
              exit
           aaa group default
              radius dictionary custom2
              diameter authentication dictionary aaa-custom4
              diameter authentication endpoint <hss_host_name>
              diameter authentication server <host_name> priority 1
```

```
    exit
domain <name>
ip domain-lookup
ip name-servers <ip_addr>
diameter endpoint <hss_host_name>
    origin realm <realm_name>
    origin host <host_name> address <host_ip_addr>
    connection retry-timeout <duration>
    peer <name> realm <realm_name> address <peer_pee_ip_addr>
dns-client <name>
    bind address <ip_addr>
    cache ttl positive <sec>
    cache ttl negative <sec>
    end
```

Serving-CSCF Configuration

Step 1 Set the system's role as a Serving-CSCF and configure service settings by applying the example configuration in the Setting the Systems Role as a Serving-CSCF and Configuring Service Settings section.

Step 2 Configure communication with CSCF peer servers by applying the example configuration in the Identifying CSCF Peer Servers section.

Step 3 Specify ACL, translation, and route lists by applying the example configuration in the Configuring Access Control, Translation, and Route Lists section.

Step 4 Configure the CSCF policy and session template by applying the example configuration in the Setting the CSCF Session Template section.

Step 5 Configure communication with Domain Name Servers by applying the example configuration in the Configuring DNS Connectivity section.

Setting the System's Role as a Serving-CSCF and Configuring Service Settings

Use the following configuration example to set the system to perform as a Serving-CSCF and configure the service:

```
configure
```

```
context <s-cscf_context_name>
   cscf service <s-cscf_service_name>
      bind address <ip_address> port <port_num>
      serving-cscf
         authentication allow-noauth invite
         authentication allow-noipauth
         registration lifetime min <sec> max <sec> default <sec>
         allow rfc3261-ua-interworking
         exit
      session-timer session-expires <value>
      session-timer min-se <value>
      default-aor-domain <name>
      subscription package reg
      trusted-domain-entity <domain_name>
      policy-name <s-cscf_policy_name>
      tas
      tas-service <ims-sh-service_name>
      end
```

Identifying CSCF Peer Servers

Use the following example to identify peer servers to the S-CSCF:

```
configure
         context <s-cscf_context_name>
            cscf peer-servers <name> type <type> -noconfirm
               server <name> address <ip_address> port <number>
               hunting-method sequential-on-failure
               end
```

Configuring Access Control, Translation, and Route Lists

Use the following example to configure CSCF access control lists (ACLs), CSCF translation lists, and CSCF route lists:

```
configure
        context <s-cscf_context_name>
           cscf acl default
              permit any
              permit source aor $.
              exit
           cscf translation default
              uri-readdress type <tag> base-criteria destination aor <aor>
              exit
           cscf routes default
              end
```

Setting the CSCF Session Template

Use the following example to configure CSCF policy and session templates:

```
configure
        context <s-cscf_context_name>
           cscf session-template <name>
              inbound-cscf-acl default
              outbound-cscf-acl default
              route-list default
              translation-list default
              cscf-policy-profile default
              end
```

Configuring DNS Connectivity

Use the following example to configure communication with a DNS and bind an interface to the server:

```
configure
         context <context_name>
            ip domain-lookup
            ip name-server <ip_address>
            dns-client <name>
               bind address <ip_address>
```

Optional Interrogating-CSCF Configuration

Use the following example to configure the S-CSCF service to also perform Interrogating-CSCF task including communicating with the HSS via a Diameter Cx interface:

```
configuration
         context <s-cscf_context_name>
            cscf service <s-cscf_service_name>
               serving-cscf
                  interrogating-cscf-role
                  allow rfc3261-ua-interworking
                  exit
                  diameter policy-control <hss_host_name>
                     origin endpoint <hss_host_name>
                     peer-select peer <auth_srv_host> peer-realm
<origin_realm_name>
                     dictionary Rx-standard
                  exit
               exit
            aaa group default
               radius dictionary custom2
```

```
            diameter authentication dictionary aaa-custom4
            diameter authentication endpoint <hss_host_name>
            diameter authentication server <host_name> priority 1
            exit
         diameter endpoint <hss_host_name>
            origin realm <realm_name>
            origin host <host_name> address <ip_address>
            connection retry-timeout 1
            peer <auth_srv_host> realm <origin_realm_name> address <ip_addr>
```

CDR Accounting Service Configuration

Use the following example to configure CDR accounting access for the CSCF application:

```
configure
      context <context_name>
         radius group default
            radius attribute nas-ip-address address <primary_address>
            radius dictionary <db>
            radius server <ip_address key <value> port <number>
            radius accounting server <ip_address> key <value> port <number>
            end
```

CSCF Logging Configuration

Use the following example to configure logging for the CSCF application:

```
logging filter active facility sessmgr level critical
logging filter active facility cscfmgr level critical
logging filter active facility cscf level critical
logging active
```

Save the Configuration

Refer to *Verifying and Saving Your Configuration* to save changes made to the Serving-CSCF configuration.

Configuring the System to Perform as an Emergency-CSCF

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an Emergency-CSCF in a test environment. For a more robust configuration example, refer to the *Sample Configuration Files*appendix.

To configure the system to perform as an Emergency-CSCF:

Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Configure the system to perform as a Proxy-CSCF and set basic CSCF parameters by applying the example configurations presented in the Configuring the System to Perform as a Proxy-CSCF section.

Step 3 Set the system's role as an Emergency-CSCF and configure service settings by applying the example configuration in the section.

Step 4 *Optional:* Configure the system to perform as a Serving-CSCF and set basic CSCF parameters by applying the example configurations presented in the Configuring the System to Perform as a Serving-CSCF section.

Step 5 Log system activity by applying the example configuration found in the CSCF Logging Configuration section.

Step 6 Save the configuration by following the steps found in the Save the Configuration section.

Setting the System's Role as an Emergency-CSCF and Configuring Service Settings

Use the following configuration example to set the system to perform as an Emergency-CSCF and configure the CSCF service:

```
configure
        context <emergency_context_name>
           cscf service <emergency_service_name>
              emergency-cscf
                 privacy
                 exit
              default-aor-domain <name>
              keepalive method crlf max-retry <value> expire-timer <value>
              keepalive method stun max-retry <value> expire-timer <value>
              policy-name <emergency_policy_name>
```

```
bind address <ip_address> port <port_num>
   end
```

CSCF Logging Configuration

Use the following example to configure logging for the CSCF application:

```
logging filter active facility sessmgr level critical
logging filter active facility cscfmgr level critical
logging filter active facility cscf level critical
logging active
```

Save the Configuration

Refer to *Verifying and Saving Your Configuration* to save changes made to the Emergency-CSCF configuration.

Configuring the System to Perform as an A-BG

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an A-BG in a test environment. For a more robust configuration example, refer to the *Sample Configuration Files*appendix.

To configure the system to perform as an A-BG:

Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Configure the system to perform as a Proxy-CSCF and set basic CSCF parameters by applying the example configurations presented in the Configuring the System to Perform as a Proxy-CSCF section.

> ***Important:*** The following commands must be added to the Proxy-CSCF Service: nat-pool name `<core_pool_name>` access-service name `<access_proxy_name>`

Step 3 Configure access context parameters by applying the example configuration found in the Access Context Configuration section.

Step 4 Set the system's role as an access-proxy and configure service settings by applying the example configuration in the Setting the Systems Role as an Access-Proxy and Configuring Service Settings section.

Step 5 *Optional:* Configure the system to perform as a Serving-CSCF and set basic CSCF parameters by applying the example configurations presented in the Configuring the System to Perform as a Serving-CSCF section.

Step 6 Log system activity by applying the example configuration found in the CSCF Logging Configuration section.

Step 7 Save the configuration by following the steps found in theSave the Configuration section.

Access Context Configuration

Use the following example to configure additional access context parameters, such as local subscribers for SIP UAs, AAA groups, and IP network settings:

```
configure
        context <access_context_name>
           ip pool <nat_pool> range <start_address> <end_address> nat 0
           interface <interface_name>
              ip address <ip_address> <ip_mask>
              exit
           cscf policy name <access_policy_name>
```

```
            service-policy-rules
               video-sessions
               exit
            exit
         subscriber default
            exit
         aaa group default
            exit
         gtpp group default
            end
```

Setting the System's Role as an Access-Proxy and Configuring Service Settings

Use the following configuration example to set the system to perform as an access-proxy and configure the CSCF service:

```
configure
         context <access-proxy_context_name>
            cscf service <access-proxy_service_name>
               proxy-cscf
                  allow rfc3261-ua-interworking
                  exit
               core-service name <proxy_cscf>
               nat-pool name <nat_pool>
               default-aor-domain <name>
               keepalive method crlf max-retry <value> expire-timer <value>
               keepalive method stun max-retry <value> expire-timer <value>
               policy-name <access_policy_name>
               bind address <ip_address> port <port_num>
```

```
end
```

CSCF Logging Configuration

Use the following example to configure logging for the CSCF application:

```
logging filter active facility sessmgr level critical
logging filter active facility cscfmgr level critical
logging filter active facility cscf level critical
logging active
```

Save the Configuration

Refer to *Verifying and Saving Your Configuration* to save changes made to the A-BG configuration.

Chapter 3
Verifying and Saving Your Configuration

This chapter describes how to save your system configuration.

Verifying the Configuration

You can use a number of commands to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of, or specific lines in, the configuration file.

Feature Configuration

In many configurations, you have to set and verify specific features. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

show apn all

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn1

authentication context: test

pdp type: ipv4

Selection Mode: subscribed

ip source violation: Checked drop limit: 10

accounting mode: gtpp No early PDUs: Disabled

max-primary-pdp-contexts: 1000000 total-pdp-contexts: 1000000

primary contexts: not available total contexts: not available

local ip: 0.0.0.0

primary dns: 0.0.0.0 secondary dns: 0.0.0.0

ppp keep alive period : 0 ppp mtu : 1500

absolute timeout : 0 idle timeout : 0

long duration timeout: 0 long duration action: Detection

ip header compression: vj

data compression: stac mppc deflate compression mode: normal

min compression size: 128

ip output access-group: ip input access-group:

ppp authentication:

allow noauthentication: Enabled imsi
```

```
 authentication:Disabled
```

Enter the following command to display the IP address pool configuration:

show ip pool

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:

+-----Type: (P) - Public (R) - Private

 | (S) - Static (E) - Resource

 |

 |+----State: (G) - Good (D) - Pending Delete (R)-Resizing

 ||

 ||++--Priority: 0..10 (Highest (0) .. Lowest (10))

 ||||

 ||||+-Busyout: (B) - Busyout configured

 |||| |||||| vvvvv Pool Name Start Address Mask/End Address Used Avail

 ----- --------- --------------- --------------- -------- --------

PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00

pool1 10.10.0.0 255.255.0.0 0 65534 SG00

vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

Important: To configure features on the system, use the *show* commands specifically for these features. Refer to the *Cisco Systems ASR 5000 Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

show *<service_type> <service_name>*

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called pgw is configured.

```
Service name : pgw1

Service-Id : 1
```

```
Context : test1

Status : STARTED

Restart Counter : 8

EGTP Service : egtp1

LMA Service : Not defined

Session-Delete-Delay Timer : Enabled

Session-Delete-Delay timeout : 10000(msecs)

PLMN ID List : MCC: 100, MNC: 99

Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

show context name *<name>*

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

```
Context Name     ContextID     State

------------     ---------     -----

test1            2          Active
```

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

show configuration

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

show configuration errors

This command displays errors it finds within the configuration. For example, if you have created a service named "service1", but entered it as "srv1" in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

If the configuration contains no errors, an output similar to the following is displayed:

```
##############################################################################

Displaying Global
AAA-configuration errors
##############################################################################

Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the SMC's CompactFlash or on an installed PCMCIA memory card on the SMC. Files that are saved to a remote network node can be transmitted through FTP, or TFTP.

Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

To save your current configuration, enter the following command:

save configuration *url* **[-redundant] [-noconfirm] [showsecrets] [verbose]**

Keyword/Variable	Description
url	Specifies the path and name to which the configuration file is to be stored. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats: • **{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **file:/{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **tftp://**{ *ipaddress*|*host_name* [*:port#*] } [*/directory*] */file_name* • **ftp://**[*username* [*:pwd*] *@*] { *ipaddress*|*host_name* } [*:port#*] [*/directory*] */file_name* • **sftp://**[*username* [:*pwd*] *@*] { *ipaddress*|*host_name* } [*:port#*] [*/directory*] */file_name* **/flash** corresponds to the CompactFlash on the SMC. **/pcmcia1** corresponds to PCMCIA slot 1. **/pcmcia2** corresponds to PCMCIA slot 2. *ipaddress* is the IP address of the network server. *host_name* is the network server's *hostname*. *port#* is the network server's logical port number. Defaults are: • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data Note: *host_name* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx *username* is the username required to gain access to the server if necessary. *password* is the password for the specified username if required. */directory* specifies the directory where the file is located if one exists. */file_name* specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.
-redundant	Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the Standby SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SMCs. For example, if you save the file to the /pcmcia1 device on the active SMC, that same type of device (a PC-Card in Slot 1 of the standby SMC) must be available. Otherwise, a failure message is displayed. Note: If saving the file to an external network (non-local) device, the system disregards this keyword.
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).

Keyword/Variable	Description
showsecrets	Optional: This keyword saves the CLI configuration file with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies to display every parameter that is being saved to the new configuration file.

Important: The **-redundant** keyword is only applicable when saving a configuration file to local devices. This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SMC, you must synchronize the local file system on both SMCs.

To save a configuration file called system.cfg to a directory that was previously created called cfgfiles on the SMC's CompactFlash, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called simple_ip.cfg to a directory called host_name_configs, using an FTP server with an IP address of 192.168.34.156, on which you have an account with a username of administrator and a password of secure, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called init_config.cfg to the root directory of a TFTP server with a hostname of config_server, enter the following command:

save configuration *tftp://config_server/init_config.cfg*

Appendix A
Access Control Lists

Access Control Lists (ACLs) are used to control the flow of packets into and out of the system. They are configured on a per-context basis and consist of “rules” (ACL rules) or filters that control the action taken on packets that match the filter criteria. Once configured, an ACL can be applied to any of the following:

- An individual interface
- All traffic facilitated by a context (known as a policy ACL)
- An individual subscriber
- All subscriber sessions facilitated by a specific context

Understanding ACLs

This section discusses concepts about how ACLs are created, ordered, and viewed on the system. The two main aspects to consider when creating an ACL are:

- Rule(s)
- Rule Order

Rule(s)

A single ACL consists of one or more ACL rules. As discussed earlier, the rule is a filter configured to take a specific action on packets matching specific criteria. Up to 128 rules can be configured per ACL.

Important: Configured ACLs consisting of no rules imply a "permit any" rule. The **deny** action and **any** criteria are discussed later in this section.

Each rule specifies the action to take when a packet matches the specifies criteria. This section discusses the rule actions and criteria supported by the system.

Actions

ACLs specify that one of the following actions can be taken on a packet that matches the specified criteria:

- **Deny:** The packet is rejected.
- **Permit:** The packet is accepted and processed.
- **Log:** Enables logging for packets meeting the criteria specified in the ACL. The logs can be viewed by executing the **logging filter active facility acl-log** command in the system's Execute mode.

Important: Packet logging is not supported for context-level (policy) ACLs. Subscriber-level ACL logging can be performed using the Session Manager task (sessmgr) logging facility.

Permit and Deny use the following syntax:

```
{ permit | deny } [ log ] { <criteria> }
```

Keyword/Variable	Description

Keyword/Variable	Description
log	Enables logging for packets meeting the criteria specified in the ACL. *Important:* Logging is not supported for Policy ACLs (those applied to contexts).
criteria	The criteria to compare packets against as described in the section that follows.

Criteria

Each ACL consists of one or more rules specifying the criteria that packets will be compared against. The following criteria are supported:

- **Any:** Filters all packets
- **Source Address:** Filter packets based on one or more source IP addresses
- **Source AoR:** Filters packets based on the source address of record
- **Destination AoR:** Filters packets based on the destination address of record

Each of the above criteria are described in detail in the sections that follow.

Important: The following sections contain basic ACL rule syntax information. Refer to the *ACL Configuration Mode Commands* chapter of the *Command Line Interface Reference* for the full command syntax.

Any

The rule applies to all packets.

The following syntax is used when configuring rule criteria that applies to all packets:

```
any
```

Source Address

The rule applies to specific packets originating from a specific source IP address or a group of source IP addresses.

The following syntax is used when configuring rule criteria that apply to one or more source IP addresses:

```
source address <ip_address> <wildcard>
```

Keyword/Variable	Description

Keyword/Variable	Description
ip_address	The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *wildcard* parameter.
wildcard	This option is used in conjunction with the *ip_address* option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:Zero-bits in this parameter mean that the corresponding bits configured for the *ip_address* parameter must be identical. One-bits in this parameter mean that the corresponding bits configured for the *ip_address* parameter must be ignored. *Important:* The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Source AoR

The rule applies to specific packets originating from a specific source address of record.

The following syntax is used when configuring rule criteria that apply to source AoRs:

source aor *<aor> <wildcard>*

Keyword/Variable	Description
aor	The address of record from which the packet originated.This option is used to filter all packets from a specific address of record or a group of AoRs. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *wildcard* parameter.
wildcard	This option is used in conjunction with the *aor* option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:Zero-bits in this parameter mean that the corresponding bits configured for the *aor* parameter must be identical. One-bits in this parameter mean that the corresponding bits configured for the *aor* parameter must be ignored. *Important:* The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Destination AoR

The rule applies to specific packets sent to a specific destination address of record.

The following syntax is used when configuring rule criteria that apply to destination AoRs:

destination aor *<aor> <wildcard>*

Keyword/Variable	Description
aor	The address of record to which the packet is being sent.This option is used to filter all packets being sent to a specific address of record or a group of AoRs. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *wildcard* parameter.
wildcard	This option is used in conjunction with the *aor* option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:Zero-bits in this parameter mean that the corresponding bits configured for the *aor* parameter must be identical. One-bits in this parameter mean that the corresponding bits configured for the *aor* parameter must be ignored. *Important:* The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Rule Order

A single ACL can consist of multiple rules. Each packet is compared against each of the ACL rules, in the order in which they were entered, until a match is found. Once a match is identified, all subsequent rules are ignored.

Additional rules can be added to an existing ACL and properly ordered using either of the following options:

- Before
- After

Using these placement options requires the specification of an existing rule in the ACL and the configuration of the new rule as demonstrated by the following flow:

[**before** | **after**] { *<existing_rule>* }

{ *<new_rule>* }

An example of an ACL is shown in the following section.

Viewing ACLs

ACLs can be viewed through the **show configuration** command executed from the context where the ACL resides. The following example was taken from the output of the **show configuration context** *<name>* command:

```
[test1]st40# show configuration context test1
config
 context test1
 subscriber default
 exit
 radius group default
 #exit
cscf acl name acl1
after permit criteria source address 1.2.3.4
after deny criteria destination aor *.bad.com
after permit criteria source aor *@test.com
after deny criteria source address 0.0.0.255
after deny criteria source aor user@test.com
 #exit
 #exit
end
```

Appendix B
Sample Configuration Files

This appendix contains sample configuration files for the following SCM configurations:

- Proxy-CSCF Configuration
- Serving-CSCF Configuration
- A-BG Configuration

In each configuration example, commented lines are labeled with the number symbol (#) and variables are identified using italics within brackets (<*variable*>).

Proxy-CSCF Configuration

```
# Complete Configuration file for ASR 5000 in Proxy-CSCF role

#

# Send IMS licenses

configure /flash/flashconfig/<license_name>.cfg

end

#

# Set system to not require confirmation when creating new contexts and/or
services. Config file must end with “no autoconfirm” to return the CLI to its
default setting.

#

configure

         autoconfirm

#

# Configure ASR 5000 cards

#

# Activate the PSCs

         card <slot_number>

            mode active psc

            exit

         card <slot_number>

            mode active psc

            exit

# Repeat for the number of PSCs in the system

#

# Modify the local context for local system management

         context local
```

```
            interface <interface_name>
               ip address <address> <mask>
               exit
            server ftpd
               exit
            server telnetd
               exit
            subscriber default
               exit
            administrator <name> encrypted password <password> ftp
#
#Set default IP route for local context
            ip route <ip_addr ip_mask> <next_hop_addr>
<local_context_interface_name>
            exit
#
# Configure Ethernet port for local context
         port ethernet <slot_number/port_number>
            no shutdown
            bind interface <local_context_interface_name> local
            exit
         end
#
# Create VPN context for P-CSCF service
configure
         context <p-cscf_context_name>
            interface <p-cscf_interface_name>
               ip address <address>
               exit
```

```
#
#Set the default subscriber for the P-CSCF context
            subscriber default
               exit
#
# Set default IP route for VPN context
            ip route 0.0.0.0 0.0.0.0 <next_hop_address> <vpn_interface_name>
            exit
#
# Configure Ethernet port for the VPN context
         port ethernet <slot_number/port_number>
            no shutdown
            bind interface <vpn_interface_name> <p-cscf_context_name>
            end
#
# Create the P-CSCF service in the P-CSCF VPN context
configure
         context <p-cscf_context_name>
            cscf service <p-cscf_service_name>
#
# Set the role of the service to P-CSCF
               proxy-cscf
                  allow rfc3261-ua-interworking
                  exit
#
# Bind an interface to the CSCF service
               bind address <ip_address> port <port_num>
#
# Enable Subscription package reg (reg-event package)
```

```
                subscription package reg
                exit
#
# Enable the session timers and set session-expires
                session-timer session-expires <sec>
#
# Set min-se
                session-timer min-se <sec>
#
# Set keepalive methods
                keepalive method crlf max-retry <value> expire-timer <value>
                keepalive method stun max-retry <value> expire-timer <value>
#
# Set default AoR domain
                default-aor-domain <alias>
#
# Set redirection recurse
                recurse-on-redirect-response
                exit
#
# Configure peer server list
            cscf peer-servers <name> type <type>
#
# Add a server to this list
                server <name> domain <domain_name> port <port_num>
                exit
#
# CSCF ACLs to permit or deny a CSCF session
            cscf acl default
```

```
                permit source aor $.
                exit
#
# CSCF route lists to define next-hop server address for a CSCF session
            cscf routes default
                exit
#
# CSCF policy to classify AoR policies
            cscf policy default
                exit
#
# CSCF session template to classify users/domains
            cscf session-template <name>
                inbound-cscf-acl default
                outbound-cscf-acl default
                route-list default
                translation-list default
                cscf-policy-profile default
                exit
#
#Configure additional P-CSCF Context parameters
#
# Configure domain name
            domain <name>
            end
#
# DNS client config
configure
         context <p-cscf_context_name>
```

```
            ip domain-lookup
            ip name-servers <ip_address>
            dns-client <name>
               bind address <ip_address>
               cache ttl positive <sec>
               cache ttl negative <sec>
               exit
            end
#
# Create local subscribers for SIP UAs
configure
         context <p-cscf_context_name>
            subscriber name <user_name>
               password <password>
               end
#
# Create AAA Group
configure
         context <p-cscf_context_name>
            aaa group default
               exit
#
# CDR Accounting service for calls over P-CSCF
            radius attribute nas-ip-address address <address>
            radius dictionary <dictionary_id>
            radius server <address> key <key> port <port_num>
            radius accounting server <address> key <key> port <port_num>
            end
#
```

```
# Configure Logging

logging filter active facility sessmgr level critical

logging filter active facility cscfmgr level critical

logging filter active facility cscf level critical

logging active

#

# Return system CLI to default setting of requiring confirmation when creating
new contexts and/or services.

#

configure

         no autoconfirm

         end

#
```

Serving-CSCF Configuration

```
# Complete Configuration file for ASR 5000 in Serving-CSCF role

#

# Send IMS licenses

configure /flash/flashconfig/<license_name>.cfg

end

#

# Set system to not require confirmation when creating new contexts and/or
services. Config file must end with “no autoconfirm” to return the CLI to its
default setting.

#

configure

         autoconfirm

#

# Configure ASR 5000 cards

#

# Activate the PSCs

         card <slot_number>

            mode active psc

            exit

         card <slot_number>

            mode active psc

            exit

# Repeat for the number of PSCs in the system

#

# Modify the local context for local system management

         context local

            interface <interface_name>
```

```
                ip address <address> <mask>
                exit
            server ftpd
                exit
            server telnetd
                exit
            subscriber default
                exit
            administrator <name> encrypted password <password> ftp
#
# Set default IP route for local context
            ip route <ip_addr ip_mask> <next_hop_addr> <lcl_context_intfc_name>
            exit
#
# Configure Ethernet port for local context
         port ethernet <slot_number/port_number>
            no shutdown
            bind interface <local_context_interface_name> local
            exit
         end
#
# Create VPN context for S-CSCF service
configure
         context <s-cscf_context_name>
            interface <s-cscf_interface_name>
                ip address <address>
                exit
#
# Configure system access to an HSS
```

```
            ims-sh-service <name>
               diameter dictionary standard
               diameter endpoint <hss_host_name>
               exit
#
# Set the default subscriber for the S-CSCF context
            subscriber default
               exit
#
# Set default IP route for VPN context
            ip route 0.0.0.0 0.0.0.0 <next_hop_address> <vpn_interface_name>
            exit
#
# Configure Ethernet port for the VPN context
         port ethernet <slot_number/port_number>
            no shutdown
            bind interface <vpn_interface_name> <s-cscf_context_name>
            end
#
# Create the S-CSCF service in the S-CSCF VPN context
configure
         context <s-cscf_context_name>
            cscf service <s-cscf_service_name>
#
# Set the role of the service to S-CSCF
               serving-cscf
                  authentication allow-noauth invite
                  authentication allow-noipauth
                  registration lifetime min <sec> max <sec> default <sec>
```

```
                  allow rfc3261-ua-interworking
                  exit
#
# Bind an interface to the CSCF service
               bind address <ip_address> port <port_num>
#
# Enable Subscription package reg (reg-event package)
               subscription package reg
#
# Set default AoR domain
               default-aor-domain <alias>
               exit
#
# Identify trusted network entities to the S-CSCF
               trusted-domain-entity <domain_name>
               trusted-domain-entity <domain_name>
                  exit
#
# Configure CSCF Service access to the HSS for Call Features
               tas
               tas-service <ims-sh-service_name>
               exit
#
# Configure peer server list
            cscf peer-servers <name> type <type>
# Add a server to this list
               server <name> domain <domain_name> port <port_num>
               exit
#
```

```
# CSCF ACLs to permit or deny a CSCF session
            cscf acl default
               permit any
               permit source aor $.
               exit
#
# CSCF translation lists to re-address CSCF sessions
            cscf translation default
               uri-readdress type <tag> base-criteria destination aor <aor>
               exit
#
# CSCF route lists to define next-hop server address for a CSCF session
            cscf routes default
               exit
#
# CSCF session template to classify users/domains
            cscf session-template <name>
               inbound-cscf-acl default
               outbound-cscf-acl default
               route-list default
               translation-list default
               cscf-policy-profile default
               exit
#
# Optional: Configure integrated I-CSCF
            cscf service <s-cscf_service_name>
               proxy-cscf
                  interrogating-cscf-role
                  allow rfc3261-ua-interworking
```

```
                exit
            exit
        aaa group default
            radius dictionary custom2
            diameter authentication dictionary aaa-custom4
            diameter authentication endpoint <hss_host_name>
            diameter authentication server <host_name> priority 1
            exit
        diameter endpoint <hss_host_name>
            origin realm <realm_name>
            origin host <host_name> address <ip_address>
            connection retry-timeout 1
            peer <auth_srv_host> realm <origin_realm_name> address <ip_addr>
#
# Configure additional S-CSCF Context parameters
#
# DNS client config
configure
        context <s-cscf_context_name>
        ip domain-lookup
        ip name-servers <ip_address>
        dns-client <name>
            bind address <ip_address>
            exit
        end
#
# Create AAA Group
configure
        context <s-cscf_context_name>
```

```
            aaa group default
               radius dictionary custom2
               diameter authentication dictionary aaa-custom4
               diameter authentication endpoint <hss_host_name>
               diameter authentication server <host_name> priority 1
               exit
#
# CDR Accounting service for calls over S-CSCF
            radius attribute nas-ip-address address <address>
            radius dictionary <dictionary_id>
            radius server <address> key <key> port <port_num>
            radius accounting server <address> key <key> port <port_num>
            end
#
# Configure Logging
logging filter active facility sessmgr level critical
logging filter active facility cscfmgr level critical
logging filter active facility cscf level critical
logging active
#
# Return system CLI to default setting of requiring confirmation when creating
new contexts and/or services.
#
configure
         no autoconfirm
         end
#
```

A-BG Configuration

```
# Complete Configuration file for ASR 5000 in Access-Proxy-CSCF role

#

# Send IMS licenses

configure /flash/flashconfig/<license_name>.cfg

end

#

# Set system to not require confirmation when creating new contexts and/or
services. Config file must end with “no autoconfirm” to return the CLI to its
default setting.

#

configure

         autoconfirm

#

# Configure ASR 5000 cards

#

# Activate the PSCs

         card <slot_number>

            mode active psc

            exit

         card <slot_number>

            mode active psc

            exit

# Repeat for the number of PSCs in the system

#

# Modify the local context for local system management

         context local
```

```
            interface <interface_name>
               ip address <address> <mask>
               exit
            server ftpd
               exit
            server telnetd
               exit
            subscriber default
               exit
            administrator <name> encrypted password <password> ftp
#
#Set default IP route for local context
            ip route <ip_addr ip_mask> <next_hop_addr>
<local_context_interface_name>
            exit
#
# Configure Ethernet port for local context
         port ethernet <slot_number/port_number>
            no shutdown
            bind interface <local_context_interface_name> local
            exit
         end
#
# Create VPN context for P-CSCF service
configure
         context <p-cscf_context_name>
            interface <p-cscf_interface_name>
               ip address <address>
               exit
```

```
#
#Set the default subscriber for the P-CSCF context
            subscriber default
               exit
#
# Set default IP route for VPN context
            ip route 0.0.0.0 0.0.0.0 <next_hop_address> <vpn_interface_name>
            exit
#
# Configure Ethernet port for the VPN context
         port ethernet <slot_number/port_number>
            no shutdown
            bind interface <vpn_interface_name> <p-cscf_context_name>
            end
#
# Create the P-CSCF service in the P-CSCF VPN context
configure
         context <p-cscf_context_name>
            cscf service <p-cscf_service_name>
#
# Set the role of the service to P-CSCF
               proxy-cscf
                  allow rfc3261-ua-interworking
                  exit
## Bind an interface to the CSCF service
               bind address <ip_address> port <port_num>
#
# Enable Subscription package reg (reg-event package)
               subscription package reg
```

```
                exit
#
# Enable the session timers and set session-expires
                session-timer session-expires <sec>
#
# Set min-se
                session-timer min-se <sec>
#
# Configure nat-pool
                nat-pool name <core_pool_name>
#
# Set default AoR domain
                default-aor-domain <alias>
#
# Set redirection recurse
                recurse-on-redirect-response
#
# Configure access service
                access-service name <access_proxy_name>
                exit
#
# Configure peer server list
            cscf peer-servers <name> type <type>
#
# Add a server to this list
                server <name> domain <domain_name> port <port_num>
                exit
#
# CSCF ACLs to permit or deny a CSCF session
```

```
            cscf acl default
               permit source aor $.
               exit
#
# CSCF route lists to define next-hop server address for a CSCF session
            cscf routes default
               exit
#
# CSCF policy to classify AoR policies
            cscf policy default
               exit
#
# CSCF session template to classify users/domains
            cscf session-template <name>
               inbound-cscf-acl default
               outbound-cscf-acl default
               route-list default
               translation-list default
               cscf-policy-profile default
               exit
#
#Configure additional P-CSCF Context parameters
#
# Configure domain name
            domain <name>
            end
#
# DNS client config
configure
```

```
        context <p-cscf_context_name>
           ip domain-lookup
           ip name-servers <ip_address>
           dns-client <name>
              bind address <ip_address>
              cache ttl positive <sec>
              cache ttl negative <sec>
              exit
           end
#
# Create local subscribers for SIP UAs
configure
        context <p-cscf_context_name>
           subscriber name <user_name>
              password <password>
              end
#
# Create AAA Group
configure
        context <p-cscf_context_name>
           aaa group default
              exit
#
# CDR Accounting service for calls over P-CSCF
           radius attribute nas-ip-address address <address>
           radius dictionary <dictionary_id>
           radius server <address> key <key> port <port_num>
           radius accounting server <address> key <key> port <port_num>
           end
```

```
#
# Create context for access_proxy service
configure
         context <access_pcscf_context_name>
            ip pool <nat_pool> range <start_address> <end_address> napt-users-
per-ip-address <num_users> port-chunk-size <ports_per_user> nat-binding-timer
<seconds>
            interface <p-cscf_interface_name>
               ip address <address>
               exit
#
#Set the default subscriber for the access-pcscf context
            subscriber default
               exit
#
# Set default IP route for access-pcscf context
            ip route 0.0.0.0 0.0.0.0 <next_hop_address> <vpn_interface_name>
            exit
#
# Configure Ethernet port for the access_pcscf context
         port ethernet <slot_number/port_number>
            no shutdown
            bind interface <access-pcscf_interface_name> <access-
pcscf_context_name>
            end
#
# Create the access_proxy service in the access-pcscf context
configure
         context <access_pcscf_context_name>
            cscf service <access_proxy_service_name>
```

```
#
# Set the role of the service to access_proxy
               proxy-cscf
                  allow rfc3261-ua-interworking
                  exit
#
# Bind an interface to the access_proxy service
               bind address <ip_address> port <port_num>
#
# Configure core service
               core-service name <proxy_cscf>
#
# Configure nat-pool
               nat-pool name <access_pool_name>
#
# Set default AoR domain
               default-aor-domain <alias>
#
# Set keepalive methods
               keepalive method crlf max-retry <value> expire-timer <value>
               keepalive method stun max-retry <value> expire-timer <value>
#
# CSCF policy to classify AoR policies
            cscf policy <access_policy>
               exit
#
# Configure Logging
logging filter active facility sessmgr level critical
logging filter active facility cscfmgr level critical
```

```
logging filter active facility cscf level critical

logging active

#

# Return system CLI to default setting of requiring confirmation when creating
new contexts and/or services.

#

configure

        no autoconfirm

        end

#
```

Appendix C
SCM Engineering Rules

This appendix provides SCM-specific engineering rules or guidelines that must be considered prior to configuring the ASR 5000 for your network deployment. General and network-specific rules are located in the appendix of the *System Administration and Configuration Guide* for the specific network type.

The following rules are covered in this appendix:

- SCM Context and Service Rules
- SCM Subscriber Rules
- AoR Regular Expression Rules
- Session Recovery Rules

SCM Context and Service Rules

- Multiple SCM services can be configured in the same context (the general rules of 256 maximum services per system and 64 maximum contexts per system apply)
- SCM services configured within the same context cannot communicate with each other
- When running collapsed with an access service such as the HA, the CSCF service correlates its call-line with the corresponding HA service call-line. If the HA service call goes down, the CSCF service aborts its call.

SCM Subscriber Rules

- When running collapsed with an access service such as the HA, the CSCF service correlates its call-line with the corresponding HA service call-line. If the HA service call goes down, the CSCF service aborts its call.

AoR Regular Expression Rules

Regular expressions can be used in **`source aor`** and **`destination aor`** keywords. Individual characters, sometimes referred to as wildcards or meta characters, can be used to create AoR ranges or broader groups to which rules or policies can be applied.

Meta Characters

Currently, the following meta characters are supported:

- "$." (dollar period): can be used in the username, domain, or sub-domain portion of the AoR. The following examples show how this character can be used:
  - $.@Provider.com - matches all users from the "Provider" domain
  - $.@$..com - matches all users with a ".com" domain only
  - mobile$.@Provider.com - matches "Provider" users who have an AoR starting with "mobile"
- "$" (dollar sign): use to substitute any single character. Example:
  - $11 matches 911, 411, etc.
- "%" (percent symbol): use to signify the start of a pattern such as add/delete/substitute for translations.

AoR Regular Expression Patterns

The **`uri-readdress aor`** keyword found in the Translation Configuration mode, supports the use of regular expression patterns. Individual characters, sometimes referred to as wildcards or meta characters, can be used to create AoR ranges or broader groups to which rules or policies can be applied. In a regular expression pattern, the meta character "%" is used to signify the beginning of an add, delete, or substitute command used for translations.

The syntax of a pattern is:

- **%-***num***p**
- **%+***num***s***sub*
- **%***num***t**
- **%+p***sub*

Character/Variable	Description
-	Delete
+	Add
num	Numeric character up to 32.
p	Prefix
s	Suffix

Character/Variable	Description
t	Truncate
sub	Substitute alpha and/or numeric string or "-" (hyphen) or "." (dot)

Syntax examples:

- **%-***num***p**: Removes (**-**) specified number (*num*) of characters from the prefix (**p**) of the username.
- **%+***num***s***sub*: Adds (**+**) specified number (*num*) of characters (*sub*) to suffix (**s**) of the username.
- **%***num***t**: Truncates (**t**) the username to a specified number (*num*) of characters.
- **%+p***sub*: Adds (+) specified number (*num*) to prefix of a dial number.

Practical examples:

- **%-***3***p**: Deletes first three characters from the prefix
- **%+***3***s***111*: Adds 111 as the suffix
- **%***10***t**: Truncates the username to 10 characters
- **%+p***sub*: Translation from number 23XY to 155588823XY using the following command:

```
uri-readdress user %+p1555888 base-criteria destination aor 23$.
```

Session Recovery Rules

RFC 3261 Proxy

- Only one call context in the call leg can be recovered. If the call leg is in multiple calls, only the active primary call context will be recovered after a sessmgr task failure.
- Session recovery should be enabled before the CSCF service creation.