



Cisco ASR 5000 Series Serving Gateway Administration Guide

Version 10.0

Last Updated June 30, 2010

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-22986-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco ASR 5000 Series Serving Gateway Administration Guide

© 2010 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

CONTENTS

About this Guide	vii
Conventions Used.....	viii
Contacting Customer Support	x
Serving Gateway Overview	11
eHRPD Network Summary	12
eHRPD Network Components.....	13
Evolved Access Network (eAN).....	13
Evolved Packet Control Function (ePCF).....	14
HRPD Serving Gateway (HSGW).....	14
SAE Network Summary	15
E-UTRAN EPC Network Components	16
eNodeB	17
Mobility Management Entity (MME).....	17
Serving Gateway (S-GW).....	17
PDN Gateway (P-GW)	18
Product Description	19
Product Specifications.....	22
Licenses	22
Hardware Requirements	22
Platforms	22
Components	22
Operating System Requirements	23
Network Deployment(s).....	24
Serving Gateway in the E-UTRAN/EPC Network.....	24
Supported Logical Network Interfaces (Reference Points).....	25
Features and Functionality - Base Software	29
Subscriber Session Management Features.....	29
IPv6 Capabilities.....	29
Lawful Intercept.....	30
Subscriber Level Trace	30
Session Recovery Support	31
Quality of Service Management Features.....	32
QoS Bearer Management.....	32
Network Access and Charging Management Features	33
Online/Offline Charging	33
Network Operation Management Functions.....	34
Support Interfaces (Reference Points)	34
Multiple PDN Support	35
Congestion Control.....	35
IP Access Control Lists.....	36
System Management Features	36
Management System Overview	37
Bulk Statistics Support.....	38
Threshold Crossing Alerts (TCA) Support	39
ANSI T1.276 Compliance	40
Features and Functionality - External Application Support	41

Web Element Management System.....	41
Features and Functionality - Optional Enhanced Feature Software	43
IP Security (IPSec) Encryption	43
Traffic Policing and Shaping.....	43
Layer 2 Traffic Management (VLANs).....	44
How the Serving Gateway Works.....	45
GTP Serving Gateway Call/Session Procedures in an LTE-SAE Network.....	45
Subscriber-initiated Attach (initial)	45
Subscriber-initiated Detach	48
Supported Standards.....	50
3GPP References.....	50
3GPP2 References.....	51
IETF References.....	51
Object Management Group (OMG) Standards.....	52
Serving Gateway Configuration	53
Configuring the System as a Standalone eGTP S-GW	54
Information Required	54
Required Local Context Configuration Information.....	54
Required S-GW Ingress Context Configuration Information	55
Required S-GW Egress Context Configuration Information.....	56
How This Configuration Works	57
eGTP S-GW Configuration	59
Initial Configuration	60
eGTP Configuration	63
Verifying and Saving the Configuration.....	65
Verifying and Saving Your Configuration	67
Verifying the Configuration.....	68
Feature Configuration.....	68
Service Configuration.....	69
Context Configuration.....	70
System Configuration.....	70
Finding Configuration Errors	70
Saving the Configuration	72
Saving the Configuration on the Chassis	73
Monitoring the Service	75
Monitoring System Status and Performance	76
Clearing Statistics and Counters	78
Configuring Subscriber Session Tracing.....	79
Introduction.....	80
Supported Functions.....	81
Supported Standards.....	83
Supported Networks and Platforms.....	84
Licenses.....	85
Subscriber Session Trace Functional Description	86
Operation.....	86
Trace Session.....	86
Trace Recording Session	86
Network Element (NE).....	86
Activation	86
Management Activation	87
Signaling Activation	87
Start Trigger	87
Deactivation	87





Stop Trigger	87
Data Collection and Reporting	87
Trace Depth.....	88
Trace Scope.....	88
Network Element Details.....	88
MME.....	88
S-GW	88
P-GW	89
Subscriber Session Trace Configuration	90
Enabling Subscriber Session Trace on EPC Network Element	90
Trace File Collection Configuration	91
Verifying Your Configuration.....	92
Sample Configuration Files	95
Standalone eGTP Serving Gateway	96
Configuration Sample.....	96
S-GW Engineering Rules.....	101
Interface and Port Rules	102
S1-U/S11 Interface Rules	102
S5/S8 Interface Rules	102
MAG to LMA Rules	102
S-GW Service Rules.....	104
S-GW Subscriber Rules.....	105

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 <code>screen display</code>	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 <i>variable</i> }	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 <i>variable</i>]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
	<p>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).</p> <p>Pipe filters can be used in conjunction with required or optional keywords or variables. For example:</p> <pre>{ nonce timestamp }</pre> <p>OR</p> <pre>[count <i>number_of_packets</i> size <i>number_of_bytes</i>]</pre>

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

Serving Gateway Overview

The ASR 5000 Core Platform provides wireless carriers with a flexible solution that functions as a Serving Gateway (S-GW) in Long Term Evolution-System Architecture Evolution (LTE-SAE) wireless data networks.

This overview provides general information about the S-GW including:

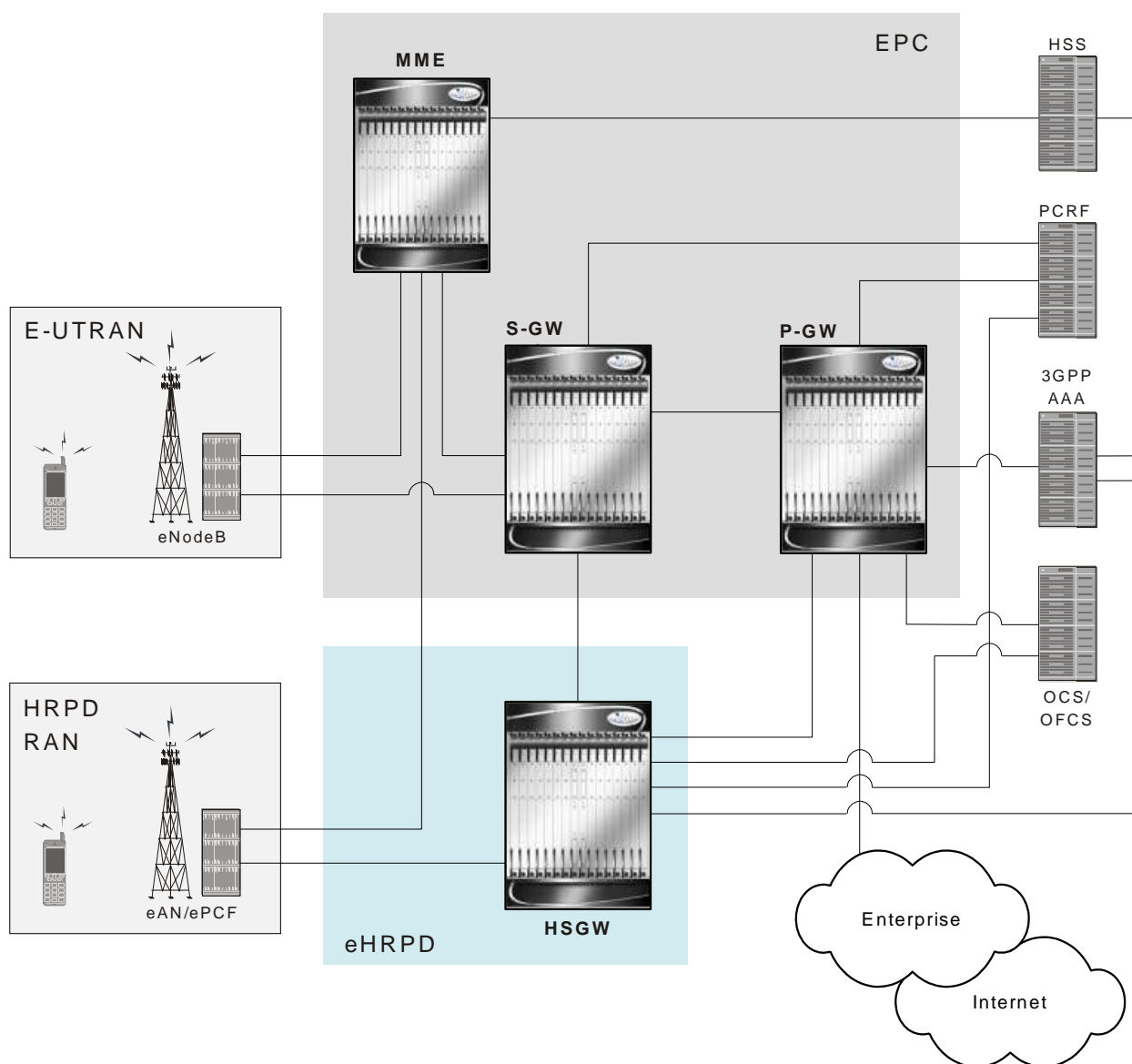
- [eHRPD Network Summary](#)
- [SAE Network Summary](#)
- [Product Description](#)
- [Product Specifications](#)
- [Network Deployment\(s\)](#)
- [Features and Functionality - Base Software](#)
- [Features and Functionality - External Application Support](#)
- [Features and Functionality - Optional Enhanced Feature Software](#)
- [How the Serving Gateway Works](#)
- [Supported Standards](#)

eHRPD Network Summary

In a High Rate Packet Data (HRPD) network, mobility is performed using client-based mobile IPv6 or Client Mobile IPv6 (CMIPv6). This involves the mobile node with an IPv6 stack maintaining a binding between its home address and its care-of address. The mobile node must also send mobility management signaling messages to a home agent.

The primary difference in an evolved HRPD (eHRPD) network is the use of network mobility (via proxy) allowing the network to perform mobility management, instead of the mobile node. This form of mobility is known as Proxy Mobile IPv6 (PMIPv6).

One of the eHRPD network's functions is to provide interworking of the mobile node with the 3GPP Evolved Packet Core (EPC). The EPC is a high-bandwidth, low-latency packet network also known as System Architecture Evolution (SAE), supporting the Long Term Evolution Radio Access Network (LTE RAN). The following figure shows the relationship of the eHRPD network with the EPC.



eHRPD Network Components

The eHRPD network is comprised of the following components:

Evolved Access Network (eAN)

The eAN is a logical entity in the radio access network used for radio communications with an access terminal (mobile device). The eAN is equivalent to a base station in 1x systems. The eAN supports operations for EPS – eHRPD RAN in addition to legacy access network capabilities.

Evolved Packet Control Function (ePCF)

The ePCF is an entity in the radio access network that manages the relay of packets between the eAN and the HSGW. The ePCF supports operations for the EPS – eHRPD RAN in addition to legacy packet control functions.

The ePCF supports the following:

- Main service connection over SO59
 - Uses PDN-MUX and allows multiplexing data belonging to multiple PDNs
- Signaling over Main A10
 - LCP messages for PPP link establishment
 - EAP messages used for authentication
 - VSNCP messages for establishment of PDNs
 - VSNP for establishment of EPS bearers and QoS mappings (RSVP)

HRPD Serving Gateway (HSGW)

The HSGW is the entity that terminates the HRPD access network interface from the eAN/PCF. The HSGW functionality provides interworking of the AT with the 3GPP EPS architecture and protocols specified in 23.402 (mobility, policy control (PCC), and roaming). The HSGW supports efficient (seamless) inter-technology mobility between LTE and HRPD with the following requirements:

- Sub 300ms bearer interruption
- Inter-technology handoff between 3GPP E-UTRAN and HRPD
- Intra-technology handoff between an HSGW and an existing PDSN
- Support for inter-HSGW fast handoff via PMIPv6 Binding Update

SAE Network Summary

The System Architecture Evolution was developed to provide a migration path for 3GPP systems and introduce higher data rates and lower latency for a variety of radio access technologies. SAE defines the packet network supporting the high-bandwidth radio network as the Evolved Packet Core (EPC). The EPC provides mobility between 3GPP (GSM, UMTS, and LTE) and non-3GPP radio access technologies, including CDMA, WiMAX, WiFi, High Rate Packet Data (HRPD), evolved HRPD, and ETSI defined TISPAN networks.

The following figure shows the interworking of the EPC with the different radio access technologies.



Cisco ASR 5000 Series Serving Gateway Administration Guide

eNodeB

The eNodeB is the LTE base station and is one of two nodes in the SAE Architecture user plane (the other is the S-GW). The eNodeB communicates with other eNodeBs via the X2 interface. The eNodeB communicates with the EPC via the S1 interface. The user plane interface is the S1-U connection to S-GW. The signaling plane interface is the S1-MME connection to MME.

Basic functions supported include:

- Radio resource management, radio bearer control, and scheduling
- IP header compression and encryption of user data stream
- Selection of MME at UE attachment (if not determined by information sent from the UE)
- Scheduling and transmission of paging messages (originated from the MME)
- Scheduling and transmission of broadcast information (originated from the MME or OA&M)
- Measurement & measurement reporting configuration for mobility and scheduling

Mobility Management Entity (MME)

The MME is the key control-node for the LTE access-network. The MME provides the following basic functions:

- NAS
 - signalling
 - signalling security
- UE access in ECM-IDLE state (including control and execution of paging retransmission)
- Tracking Area (TA) list management
- PGW and SGW selection
- MME selection for handovers with MME change
- SGSN selection for handovers to 2G or 3G 3GPP access networks
- Terminates interface to HSS (S6a)
- Authentication
- Bearer management functions including dedicated bearer establishment
- HRPD access node (terminating S101 reference point) selection for handovers to HRPD
- Transparent transfer of HRPD signalling messages and transfer of status information between E-UTRAN and HRPD access, as specified in the pre-registration and handover flows

Serving Gateway (S-GW)

For each UE associated with the EPS, there is a single S-GW at any given time providing the following basic functions:

- Terminates the interface towards E-UTRAN (S1-U)
- Functions (for both the GTP-based and the PMIP-based S5/S8) include:
 - local mobility anchor point for inter-eNodeB handover
 - mobility anchoring for inter-3GPP mobility (terminating S4 and relaying the traffic between 2G/3G system and P-GW)
 - ECM-IDLE mode downlink packet buffering and initiation of network triggered service request procedure
 - lawful intercept
 - packet routing and forwarding
 - transport level packet marking in the uplink and the downlink (e.g. setting the DiffServ Code Point)
 - Accounting
- Handling of Router Solicitation and Router Advertisement messages if PMIP based S5/S8 is used
- MAG for PMIP based S5 and S8

PDN Gateway (P-GW)

For each UE associated with the EPS, there is at least one P-GW providing access to the requested PDN. If a UE is accessing multiple PDNs, there may be more than one P-GW for that UE. The P-GW provides the following basic functions:

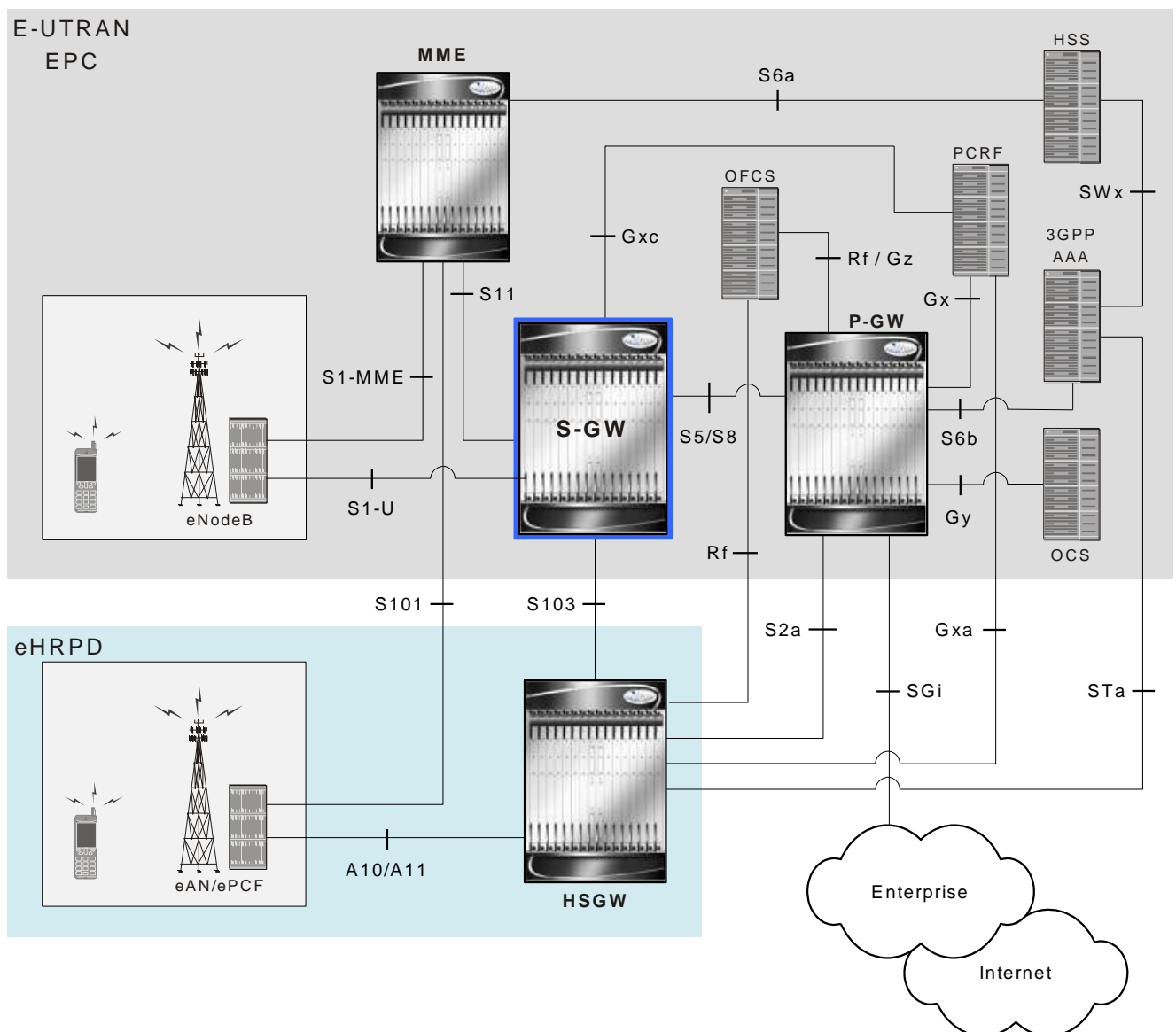
- Terminates the interface towards the PDN (SGi)
- P-GW functions (for both the GTP-based and the PMIP-based S5/S8) include:
 - per-user packet filtering (e.g. deep packet inspection)
 - lawful intercept
 - UE IP address allocation
 - UL and DL service level charging, gating control, and service level rate enforcement
 - DL rate enforcement based on AMBR (Aggregate Max Bit Rate) and based on the accumulated MBRs of the aggregate of SDFs with the same GBR QCI
 - DHCPv4 and DHCPv6 functions (client, relay and server)
- LMA for PMIP6

Product Description

The Serving Gateway routes and forwards data packets from the UE and acts as the mobility anchor during inter-eNodeB handovers. Signals controlling the data traffic are received on the S-GW from the MME which determines the S-GW that will best serve the UE for the session. Every UE accessing the EPC is associated with a single S-GW.

The S-GW is also involved in mobility by forwarding down link data during a handover from the E-UTRAN to the eHRPD network. An interface from the eAN/ePCF to an MME provides signaling that creates a GRE tunnel between the S-GW and the eHRPD Serving Gateway.

Figure 1. Basic E-UTRAN/EPC and eHRPD Network Topology



The functions of the S-GW for both GTP-based and PMIP-based network sessions include:

- packet routing and forwarding.
- providing the local mobility anchor point for inter-eNodeB handover and assisting the eNodeB reordering function by sending one or more “end marker” packets to the source eNodeB immediately after switching the path.
- mobility anchoring for inter-3GPP mobility (terminating the S4 interface from an SGSN and relaying the traffic between 2G/3G system and a PDN gateway).
- packet buffering for ECM-IDLE mode downlink and initiation of network triggered service request procedure.

- replicating user traffic in the event that Lawful Interception is required.
- transport level packet marking.
- user accounting and QCI granularity for charging.
- uplink and downlink charging per UE, PDN, and QCI.

Product Specifications

The following information is located in this section:

- [Licenses](#)
- [Hardware Requirements](#)
- [Operating System Requirements](#)

Licenses

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

The following licenses are available for this product:

- S-GW Software License, 10k Sessions - 600-00-7644
- S-GW Software License, 1k Sessions - 600-00-7645

Hardware Requirements

Information in this section describes the hardware required to enable S-GW services.

Platforms

The S-GW service operates on the ASR 5000 Series platforms:

Components

The following application and line cards are required to support S-GW 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):** Within the ASR 5000 platform, PSCs provide high-speed, multi-threaded PDP context processing capabilities for 4G S-GW 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 PSCs, these cards provide the physical interfaces to elements in the E-UTRAN EPC data network. Up to 26 line cards can be installed for a fully loaded system with 13 active PSCs,

13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant PSCs do not require line cards.

- Ethernet 10/100 and/or Ethernet 1000 line cards for IP connections to other network elements.
- **Redundancy Crossbar Cards (RCCs):** Installed in the lower-rear chassis slots directly behind the SPCs/SMCs, RCCs utilize 5 Gbps serial links to ensure connectivity between Ethernet 10/100 or Ethernet 1000 line cards and every PSC in the system for redundancy. Two RCCs can be installed to provide redundancy for all line cards and PSCs.



IMPORTANT: Additional information pertaining to each of the application and line cards required to support LTE-SAE services is located in the *Hardware Platform Overview* chapter of the *Product Overview Guide*.

Operating System Requirements

The S-GW is available for all Cisco ASR 5000 Platforms running StarOS Release 9.0 or later.

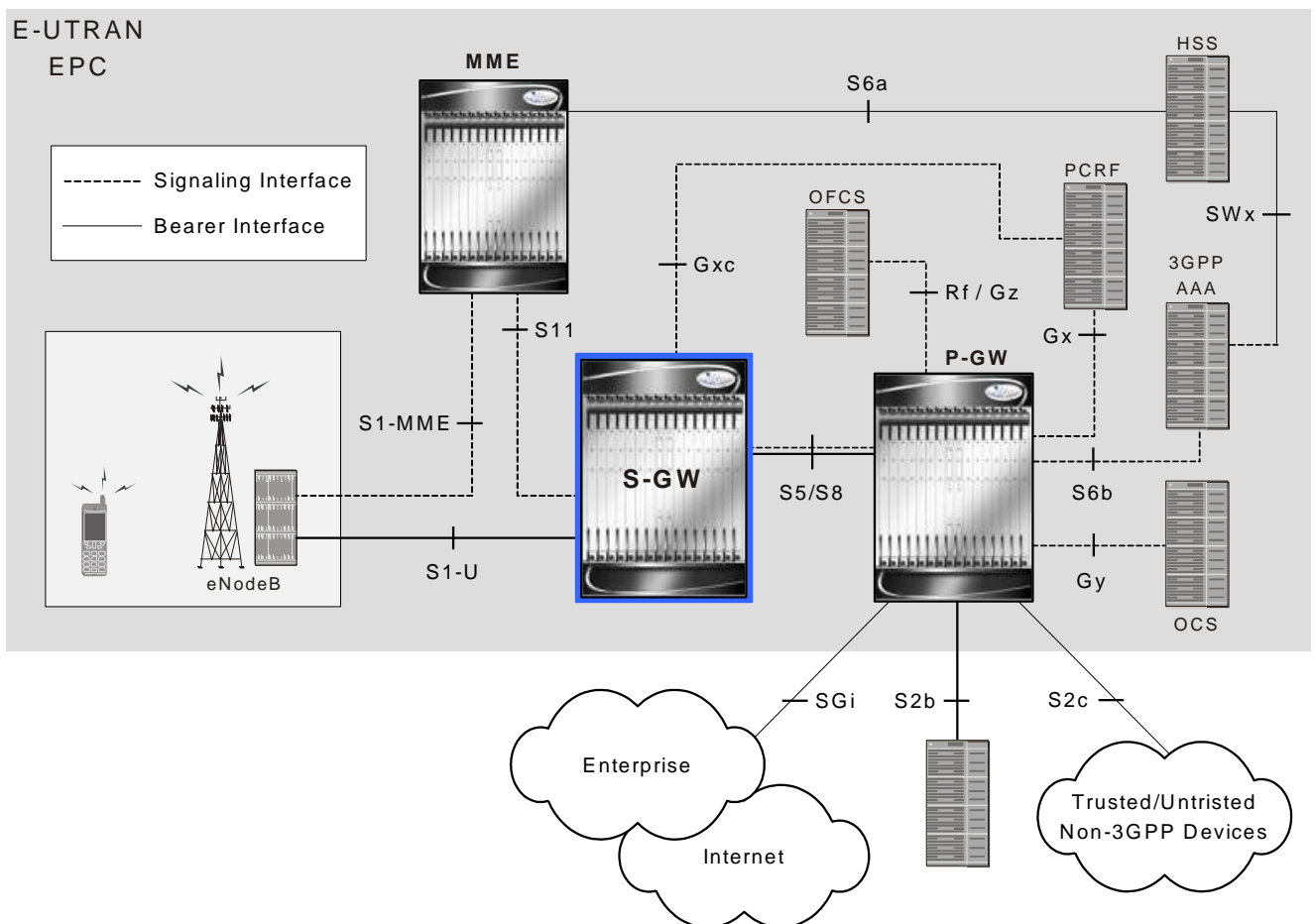
Network Deployment(s)

This section describes the supported interfaces and the deployment scenarios of a Serving Gateway.

Serving Gateway in the E-UTRAN/EPC Network

The following figure displays a simplified network view of the S-GW and how it interconnects with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

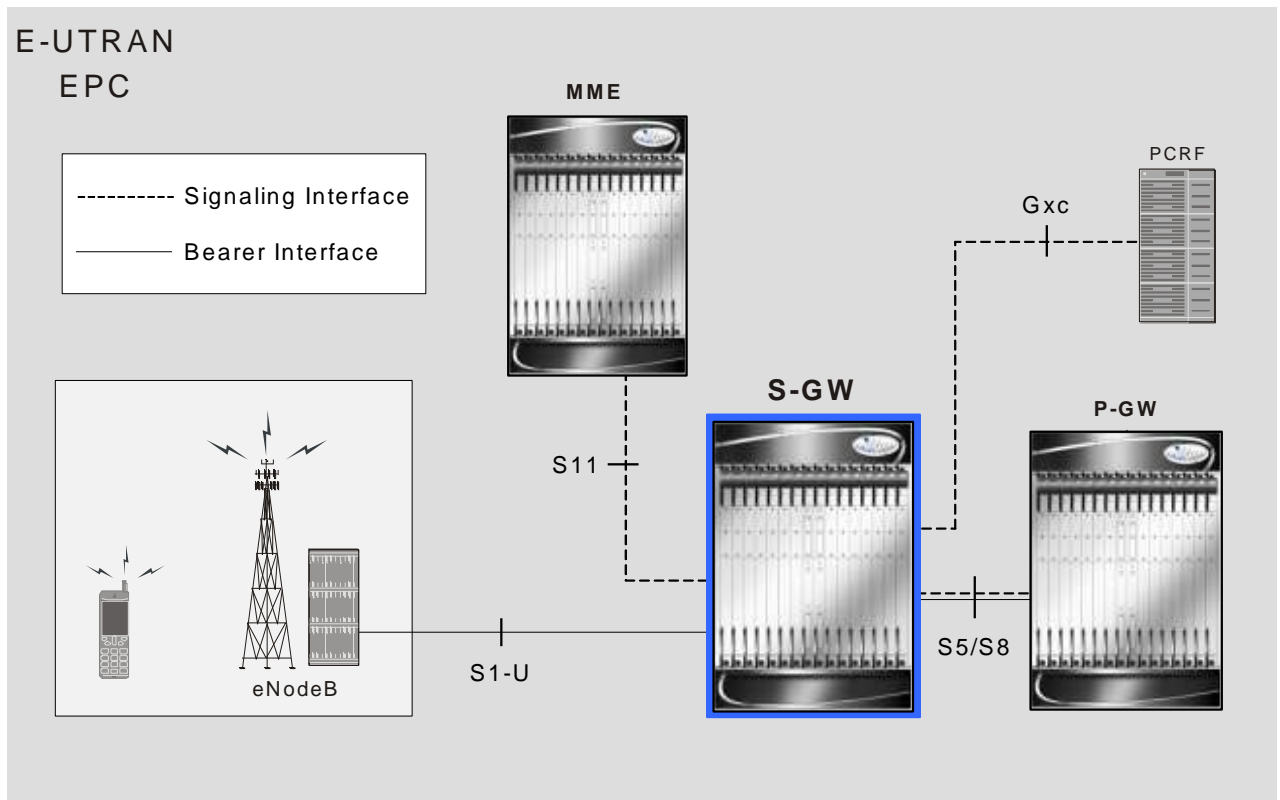
Figure 2. S-GW in the E-UTRAN/EPC Network



Supported Logical Network Interfaces (Reference Points)

The following figure displays the specific network interface between a Serving Gateway and other E-UTRAN network devices.

Figure 3. S-GW Interfaces in the E-UTRAN/EPC Network



The S-GW provides the following logical network interfaces in support of the E-UTRAN/EPC network:

S4 Interface

This reference point (not shown in the figure above) provides tunneling and management between the S-GW and an SGSN.

S5/S8 Interface

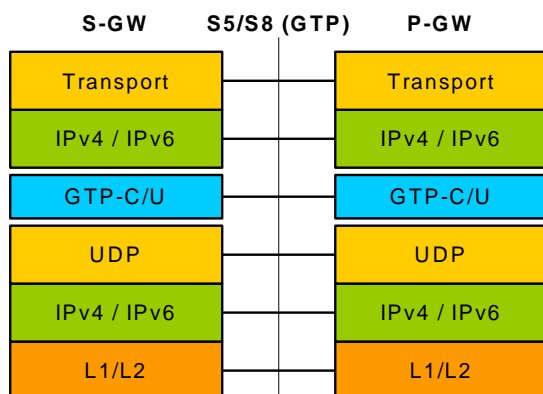
This reference point provides tunneling (bearer channel) and management (signaling channel) between the S-GW and the P-GW. The S8 interface is used for roaming scenarios. The S5 interface is used for non-roaming.

Supported protocols:

- Transport Layer: UDP, TCP

■ Network Deployment(s)

- Tunneling:
 - GTP: IPv4 or IPv6 GTP-C (signaling channel) and GTP-U (bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

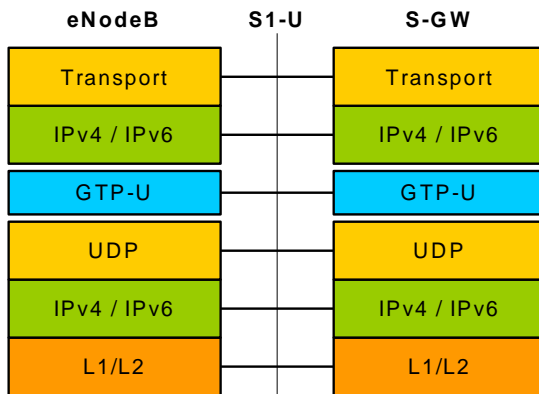


S1-U Interface

This reference point provides bearer channel tunneling between the eNodeB and the S-GW. It also supports eNodeB path switching during handovers.

Supported protocols:

- Transport Layer: UDP, TCP
- Tunneling: IPv4 or IPv6 GTP-U (bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

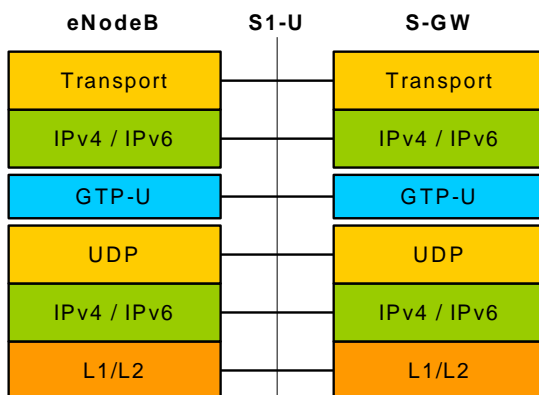


S11 Interface

This reference point provides GTP-C control signal tunneling between the MME and the S-GW.

Supported protocols:

- Transport Layer: UDP, TCP
- Tunneling: IPv4 or IPv6 GTP-C (control channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



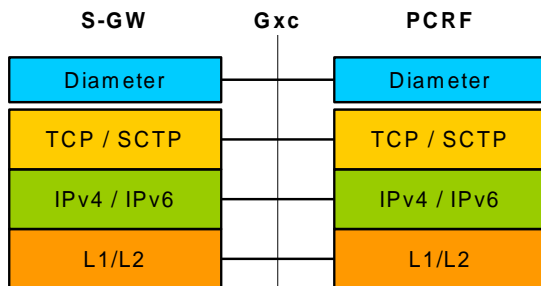
Gxc Interface

This signaling interface supports the transfer of policy control and charging rules information (QoS) between the Bearer Binding and Event Reporting Function (BBERF) on the S-GW and a Policy and Charging Rules Function (PCRF) server.

Supported protocols:

■ Network Deployment(s)

- Transport Layer: UDP, TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



Features and Functionality - Base Software

This section describes the features and functions supported by default in the base software for the S-GW service and do not require any additional licenses to implement the functionality.



IMPORTANT: To configure the basic service and functionality on the system for the S-GW service, refer to the configuration examples provided in the Serving Gateway Administration Guide.

The following features are supported and described in this section:

- [Subscriber Session Management Features](#)
- [Quality of Service Management Features](#)
- [Network Access and Charging Management Features](#)
- [Network Operation Management Functions](#)
- [System Management Features](#)

Subscriber Session Management Features

This section describes the following features:

- [IPv6 Capabilities](#)
- [Lawful Intercept](#)
- [Subscriber Level Trace](#)
- [Session Recovery Support](#)

IPv6 Capabilities

Enables increased address efficiency and relieves pressures caused by rapidly approaching IPv4 address exhaustion problem.

The S-GW platform offers the following IPv6 capabilities:

IPv6 Connections to Attached Elements

IPv6 transport and interfaces are supported on all of the following connections:

- Diameter Gxc policy signaling interface
- Diameter Rf offline charging interface
- Lawful Intercept (X1, X2 interfaces)

Routing and Miscellaneous Features

- OSPFv3
- MP-BGP v6 extensions
- IPv6 flows (Supported on all Diameter QoS and Charging interfaces as well as Inline Services (e.g. ECS, P2P detection, Stateful Firewall, etc))

Lawful Intercept

Provides a standardized architecture for lawful monitoring and interception of subscriber call content and control events as mandated by a court ordered warrant from a law enforcement agency.

In accordance with 3GPP TS 33.108 Release 8 requirements the Cisco S-GW supports the Lawful Intercept Access Function for intercepting control and data messages of mobile targets. Law Enforcement Agencies request the network operator to start the interception of a particular mobile user based on court ordered subpoenas.

The Cisco EPC gateways provide access to the intercepted Content of Communications (CC) and the Intercept Related Information (IRI) of the mobile target and services related to the target on behalf of Law Enforcement Agencies. In this release the S-GW supports the following three interfaces:

- X1 provisioning interface from Administrative Function (ADMf) using CLI over SSH: Intercept targets can be provisioned using subscriber information including MSISDN, IMSI and MEI. Interception of only events (IRI) or events and call content (IRI + CC) can be provisioned.
- X2 event delivery interface for transferring Intercept Related Information (IRI) to a Delivery Function/Mediation server: Intercepted events include QoS information (if available), bearer activation (Default and Dedicated bearer), start of intercept with bearer active, bearer modification, bearer deactivation, and UE requested bearer resource modification.
- X3 content delivery: Includes intercepted call content for all default and dedicated EPS bearers.

The intercepted call control data is encoded in a Cisco proprietary message header format using an optional TLV field to pack the IRI information. The message header also includes other identifying information including sequence numbers, timestamps and session & correlation numbers to correlate session and bearer related information with interception on other EPC elements. If provisioning is activated while the call is active for the target identity then the intercepted information is immediately forwarded to the mediation server. Otherwise camp-on monitoring is used and the system waits for the call to become active (ECM CONNECTED state) and compares the IMSI, MSISDN and MEI against the LI monitoring list as a trigger to begin the intercept.

A total of 20,000 simultaneous LI triggers can be provisioned on the Cisco P-GW, S-GW or MME. Our solution is currently interoperable with leading mediation solutions from partners such as SS8 and Utimaco.



IMPORTANT: For more information on Lawful Intercept support, refer to the *Lawful Intercept Configuration Guide*.

Subscriber Level Trace

Provides a 3GPP standards-based session level trace function for call debugging and testing new functions and access terminals in an LTE environment.

As a complement to Cisco's protocol monitoring function, the S-GW supports 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S1-U, S11, S5/S8, and Gxc. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at HSS with trace activation via authentication response messages over S6a reference interface
- Signaling based activation through signaling from subscriber access terminal

Note: Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

The session level trace function consists of trace activation followed by triggers. The time between the two events is treated much like Lawful Intercept where the EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the ASR 5000 platform. The Trace Depth defines the granularity of data to be traced. Six levels are defined including Maximum, Minimum and Medium with ability to configure additional levels based on vendor extensions.

All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a FTP or secure FTP (SFTP) connection. In the current release the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI. Once a subscriber level trace request is activated it can be propagated via the S5/S8 signaling to provision the corresponding trace for the same subscriber call on the P-GW. The trace configuration will only be propagated if the P-GW is specified in the list of configured Network Element types received by the S-GW. Trace configuration can be specified or transferred in any of the following message types:

- S11: Create Session Request
- S11: Trace Session Activation
- S11: Modify Bearer Request

Performance Goals:

As subscriber level trace is a CPU intensive activity the max number of concurrently monitored trace sessions per Cisco P-GW or S-GW is 32. Use in a production network should be restricted to minimize the impact on existing services.

Session Recovery Support

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.

In the telecommunications industry, over 90 percent of all equipment failures are software-related. With robust hardware failover and redundancy protection, any card-level hardware failures on the system can quickly be corrected. However, software failures can occur for numerous reasons, many times without prior indication. StarOS Release 9.0 adds the ability to support stateful intra-chassis session recovery for S-GW sessions.

When session recovery occurs, the system reconstructs the following subscriber information:

- Data and control state information required to maintain correct call behavior
- Subscriber data statistics that are required to ensure that accounting information is maintained
- A best-effort attempt to recover various timer values such as call duration, absolute time, and others

Session recovery is also useful for in-service software patch upgrade activities. If session recovery is enabled during the software patch upgrade, it helps to preserve existing sessions on the active PSC during the upgrade process.



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

Quality of Service Management Features

This section describes the following features:

- [QoS Bearer Management](#)

QoS Bearer Management

Provides a foundation for contributing towards improved Quality of User Experience (QoE) by enabling deterministic end-to-end forwarding and scheduling treatments for different services or classes of applications pursuant to their requirements for committed bandwidth resources, jitter and delay. In this way, each application receives the service treatment that users expect.

An EPS bearer is a logical aggregate of one or more Service Data Flows (SDFs), running between a UE and a P-GW in case of GTP-based S5/S8, and between a UE and HSGW in case of PMIP-based S2a connection. An EPS bearer is the level of granularity for bearer level QoS control in the EPC/E-UTRAN. The Cisco P-GW maintains one or more Traffic Flow Templates (TFTs) in the downlink direction for mapping inbound Service Data Flows (SDFs) to EPS bearers. The P-GW maps the traffic based on the downlink TFT to the S5/S8 bearer. The Cisco P-GW offers all of the following bearer-level aggregate constructs:

QoS Class Identifier (QCI): An operator provisioned value that controls bearer level packet forwarding treatments (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc). The Cisco EPC gateways also support the ability to map the QCI values to DiffServ codepoints in the outer GTP tunnel header of the S5/S8 connection. Additionally, the platform also provides configurable parameters to copy the DSCP marking from the encapsulated payload to the outer GTP tunnel header.

Guaranteed Bit Rate (GBR): A GBR bearer is associated with a dedicated EPS bearer and provides a guaranteed minimum transmission rate in order to offer constant bit rate services for applications such as interactive voice that require deterministic low delay service treatment.

Maximum Bit Rate (MBR): The MBR attribute provides a configurable burst rate that limits the bit rate that can be expected to be provided by a GBR bearer (e.g. excess traffic may get discarded by a rate shaping function). The MBR may be greater than or equal to the GBR for a given dedicated EPS bearer.

Aggregate Maximum Bit Rate (AMBR): AMBR denotes a bit rate of traffic for a group of bearers destined for a particular PDN. The Aggregate Maximum Bit Rate is typically assigned to a group of Best Effort service data flows over the Default EPS bearer. That is, each of those EPS bearers could potentially utilize the entire AMBR, e.g. when the other EPS bearers do not carry any traffic. The AMBR limits the aggregate bit rate that can be expected to be provided by the EPS bearers sharing the AMBR (e.g. excess traffic may get discarded by a rate shaping function). AMBR applies to all Non-GBR bearers belonging to the same PDN connection. GBR bearers are outside the scope of AMBR.

Policing & Shaping: The Cisco P-GW offers a variety of traffic conditioning and bandwidth management capabilities. These tools enable usage controls to be applied on a per-subscriber, per-EPS bearer or per-PDN/APN basis. It is also possible to apply bandwidth controls on a per-APN AMBR capacity. These applications provide the ability to inspect and maintain state for user sessions or Service Data Flows (SDF's) within them using shallow L3/L4 analysis or high touch deep packet inspection at L7. Metering of out-of-profile flows or sessions can result in packet discards or reducing the DSCP marking to Best Effort priority. When traffic shaping is enabled the P-GW enqueues the non-conforming session to the provisioned memory limit for the user session. When the allocated memory is exhausted, the inbound/outbound traffic for the user can be transmitted or policed in accordance with operator provisioned policy.

Network Access and Charging Management Features

This section describes the following features:

- [OnlineOffline Charging](#)

Online/Offline Charging

The Cisco EPC platforms offer support for offline charging interactions with external OCS and CGF/CDF servers.

Ga/Gz Reference Interfaces

The Cisco P-GW supports 3GPP Release 8 compliant offline charging as defined in TS 32.251, TS 32.297 and 32.298. Whereas the S-GW generates SGW-CDRs to record subscriber level access to PLMN resources, the P-GW creates PGW-CDRs to record user access to external networks. Additionally when Gn/Gp interworking with pre-release SGSNs is enabled, the GGSN service on the P-GW records G-CDRs to record user access to external networks.

To provide subscriber level accounting, the Cisco S-GW supports integrated Charging Transfer Functions (CTF) and Charging Data Functions (CDF). Each gateway uses Charging-ID's to distinguish between default and dedicated bearers within subscriber sessions. The Ga/Gz reference interface between the CDF and CGF is used to transfer charging records via the GTPP protocol. In a standards based implementation, the CGF consolidates the charging records and transfers them via an FTP/S-FTP connection over the Bm reference interface to a back-end billing mediation server. The Cisco EPC gateways also offer the ability to FTP/S-FTP charging records between the CDF and CGF server. CDR records include information such as Record Type, Served IMSI, ChargingID, APN Name, TimeStamp, Call Duration, Served MSISDN, PLMN-ID, etc. The ASR 5000 platform offers a local directory to enable temporary file storage and buffer charging records in persistent memory located on a pair of dual redundant RAID hard disks. Each drive includes 147GB of storage and up to 100GB of capacity is dedicated to storing charging records. For increased efficiency it is also possible to enable file compression using protocols such as GZIP. The Offline Charging implementation offers built-in heart beat monitoring of adjacent CGFs. If the Cisco P-GW have not heard from the neighbor CGF within the configurable polling interval, they will automatically buffer the charging records on the local drives until the CGF reactivates itself and is able to begin pulling the cached charging records.

The P-GW supports a Policy Charging Enforcement Function (PCEF) to enable Flow Based Bearer Charging (FBC) via the Gy reference interface to adjunct OCS servers (See Online Charging description above).

Network Operation Management Functions

This section describes the following features:

- [Support Interfaces \(Reference Points\)](#)
- [Multiple PDN Support](#)
- [Congestion Control](#)
- [IP Access Control Lists](#)

Support Interfaces (Reference Points)

S1-U (E-UTRAN EPC)

In an E-UTRAN network S1-U is the per-bearer user plane tunneling reference interface between the S-GW and eNodeB. The S-GW provides the local mobility anchor point for inter-eNodeB hand-overs. It provides inter-eNodeB path switching during hand-overs when the X2 handover interface between base stations cannot be used. The S1-U interface uses GPRS tunneling protocol for user plane (GTP-Uv1). GTP encapsulates all end user IP packets and it relies on UDP/IP transport.

In order to support S1-U hand-overs the source eNodeB initiates the hand-over by sending the hand-over required message over the S1-MME interface to the MME. The MME then determines if the S-GW needs to be relocated. The eNodeB decides which EPS bearers are subject to forwarding to the target base station. In the S1-U hand-over, the hand-off occurs indirectly from the source eNodeB to the target via the source and target S-GWs.

S11 (E-UTRAN EPC)

S11 is the reference interface that provides the control plane protocol (GTP-Cv2) between the MME and S-GW. As with all GTP-based interfaces S11 relies on UDP/IP transport. A GTP tunnel is identified in each node with a Tunnel Endpoint ID (TEID), IP address and UDP port number. The TEID values are exchanged between the tunnel endpoints using GTP-C. There is one GTP-C tunnel between the MME and S-GW for each mobile terminal. The GTP protocol provides the following functions:

- **Bearer management function:** This functionality is responsible for bearer management; setting up, modifying and releasing EPS bearers, which are triggered by the MME. The release of EPS bearers may be triggered by the P-GW or HSS as well. The messages include Create Session request, Create Bearer request, Create bearer response etc. Additionally GTP tunnel management messages may be sent for any of the following reasons:
 - Initial UE attachment
 - UE requests connection to an additional PDN
 - Tracking Area Update with S-GW change
 - S1/X2 handover with S-GW change
 - GERAN or UTRAN to E-UTRAN Inter-RAT handover with SGW change.
- **Path management function:** This functionality is responsible for managing the path between the tunnel endpoints. It includes messages like ECHO request, ECHO response and version not supported indication.

- **Mobility management functions:** This functionality consists of messages that are exchanged between GTP end points to manage UE mobility. Messages such as Forward Relocation request/response are sent between end points. These messages are not sent on the S11 interface.

S5/S8 GTP (E-UTRAN EPC)

In accordance with 3GPP TS 23.401 the Cisco S-GW platform supports GTPv2-C and GTPv1-U call control and user plane tunnelling. A GTP tunnel is identified in each node with a Tunnel Endpoint ID (TEID), an IP address and a UDP port number. The S-GW and P-GW nodes provision separate GTP tunnels for each attached subscriber and for the individual PDN connections initiated by the UE. The StarOS distributed software architecture enables each function to run as independent stand-alone services on separate chassis or as simultaneous combination services running on the same platform.

The S5 reference interface provides user plane tunnelling and tunnel management between an S-GW and P-GW located within the same administrative domain. It is used for S-GW relocation due to UE mobility and if the S-GW needs to connect to a non-collocated P-GW for the required PDN connectivity.

The S8 reference interface is an inter-PLMN reference point providing user and control plane between the S-GW in the VPLMN and the P-GW in the HPLMN. It is based on the Gp reference point as defined between SGSN and GGSN. S8a is the inter PLMN variant of S5.

Multiple PDN Support

Enables an APN-based user experience that enables separate connections to be allocated for different services including IMS, Internet, walled garden services, or offdeck content services.

The MAG function on the S-GW can maintain multiple PDN or APN connections for the same user session. The MAG runs a single node level Proxy Mobile IPv6 tunnel for all user sessions toward the LMA function of the P-GW. When a user wants to establish multiple PDN connections, the MAG brings up the multiple PDN connections over the same PMIPv6 session to one or more P-GW LMAs. The P-GW in turn allocates separate IP addresses (Home Network Prefixes) for each PDN connection and each one can run one or multiple EPC default & dedicated bearers. To request the various PDN connections, the MAG includes a common MN-ID and separate Home Network Prefixes, APNs and a Handover Indication Value equal to one in the PMIPv6 Binding Updates.

Congestion Control

The congestion control feature allows you to set policies and thresholds and specify how the system reacts when faced with a heavy load condition.

Congestion control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may have an impact the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a

way similar to operation thresholds that are configured for the system as described in the Thresholding Configuration Guide. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, `starCongestion`, are generated.

A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, `starCongestionClear`, is then triggered.

- **Port Utilization Thresholds:** If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
- **Port-specific Thresholds:** If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.
- **Service Congestion Policies:** Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.



IMPORTANT: For more information on congestion control, refer to the *Congestion Control* chapter in the *System Enhanced Feature Configuration Guide*.

IP Access Control Lists

IP access control lists allow you to set up rules that control the flow of packets into and out of the system based on a variety of IP packet parameters.

IP access lists, or Access Control Lists (ACLs) as they are commonly referred to, 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



IMPORTANT: For more information on IP access control lists, refer to the *IP Access Control Lists* chapter in the *System Enhanced Feature Configuration Guide*.

System Management Features

This section describes following features:

- [Management System Overview](#)
- [Bulk Statistics Support](#)
- [Threshold Crossing Alerts \(TCA\) Support](#)

- [ANSI T1.276 Compliance](#)

Management System Overview

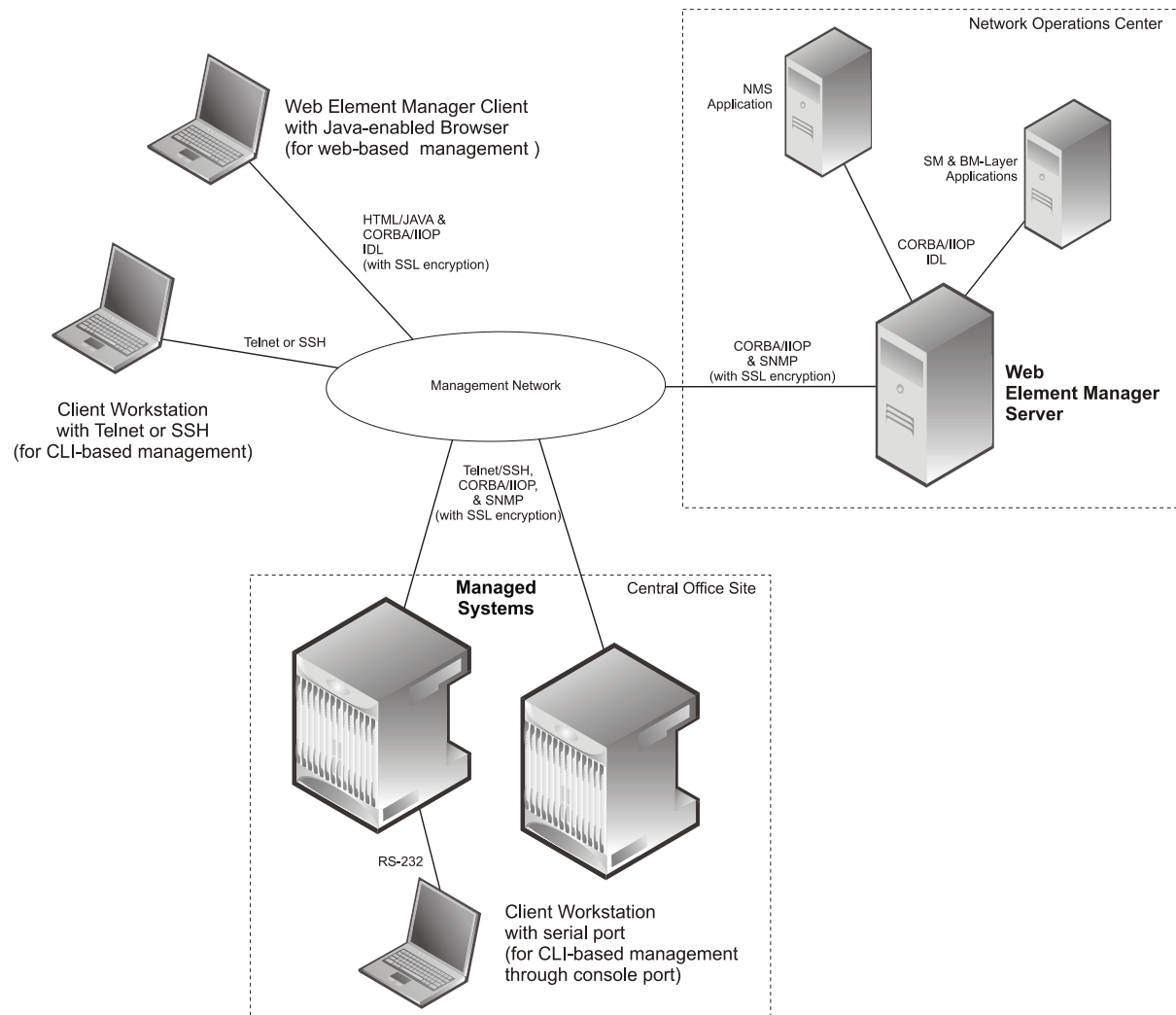
The system's management capabilities are designed around the Telecommunications Management Network (TMN) model for management - focusing on providing superior quality Network Element (NE) and element management system (Web Element Manager) functions. The system provides element management applications that can easily be integrated, using standards-based protocols (CORBA and SNMPv1, v2), into higher-level management systems - giving wireless operators the ability to integrate the system into their overall network, service, and business management systems. In addition, all management is performed out-of-band for security and to maintain system performance.

Cisco's O&M module offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces.

These include:

- Using the Command Line Interface (CLI)
- Remote login using Telnet, and Secure Shell (SSH) access to CLI through SPIO card's Ethernet management interfaces
- Local login through the console port on SPIO card using an RS-232 serial connection
- Using the Web Element Manager application
- Supports communications through 10 Base-T, 100 Base-TX, 1000 Base-TX, or 1000
- Base-SX (optical gigabit Ethernet) Ethernet management interfaces on the SPIO
- Client-Server model supports any browser (i.e. Microsoft Internet Explorer v5.0 and above or Netscape v4.7 or above, and others)
- Supports Common Object Request Broker Architecture (CORBA) protocol and Simple Network Management Protocol version 1 (SNMPv1) for fault management
- Provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) capabilities
- Can be easily integrated with higher-level network, service, and business layer applications using the Object Management Group's (OMG's) Interface Definition Language (IDL)

The following figure demonstrates these various element management options and how they can be utilized within the wireless carrier network.

Figure 4. Element Management Methods

IMPORTANT: P-GW management functionality is enabled by default for console-based access. For GUI-based management support, refer to the [Web Element Management System](#) section in this chapter.



IMPORTANT: For more information on command line interface based management, refer to the *Command Line Interface Reference* and *P-GW Administration Guide*.

Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with the Web Element Manager, the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema. Following is a partial list of supported schemas:

- **System:** Provides system-level statistics
- **Card:** Provides card-level statistics
- **Port:** Provides port-level statistics
- **MAG:** Provides MAG service statistics
- **S-GW:** Provides S-GW node-level service statistics
- **IP Pool:** Provides IP pool statistics
- **APN:** Provides Access Point Name statistics


The system supports the configuration of up to 4 sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the system or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, system host name, system uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

When the Web Element Manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of the Web Element Manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

 **IMPORTANT:** For more information on bulk statistic configuration, refer to the *Configuring and Maintaining Bulk Statistics* chapter in the *System Administration Guide*.

Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, IP pool addresses, etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

The following thresholding models are supported by the system:

- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.
- **Alarm:** Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values.

Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

Logs are supported in both the Alert and the Alarm models.

- **Alarm System:** High threshold alarms generated within the specified polling interval are considered “outstanding” until a the condition no longer exists or a condition clear alarm is generated. “Outstanding” alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in the Web Element Manager.

The Alarm System is used only in conjunction with the Alarm model.



IMPORTANT: For more information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide*.

ANSI T1.276 Compliance

ANSI T1.276 specifies security measures for Network Elements (NE). In particular it specifies guidelines for password strength, storage, and maintenance security measures.

ANSI T1.276 specifies several measures for password security. These measures include:

- Password strength guidelines
- Password storage guidelines for network elements
- Password maintenance, e.g. periodic forced password changes

These measures are applicable to the ASR 5000 Platform and the Web Element Manager since both require password authentication. A subset of these guidelines where applicable to each platform will be implemented. A known subset of guidelines, such as certificate authentication, are not applicable to either product. Furthermore, the platforms support a variety of authentication methods such as RADIUS and SSH which are dependent on external elements. ANSI T1.276 compliance in such cases will be the domain of the external element. ANSI T1.276 guidelines will only be implemented for locally configured operators.

Features and Functionality - External Application Support

This section describes the features and functions of external applications supported on the S-GW. These services require additional licenses to implement the functionality.

- [Web Element Management System](#)

Web Element Management System

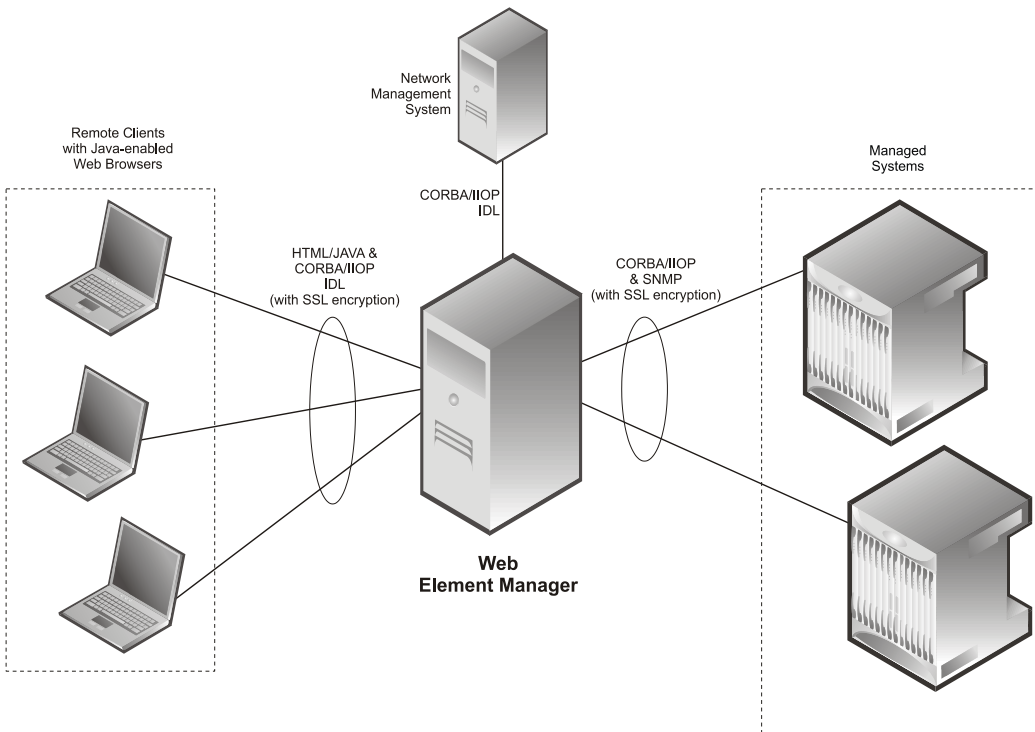
The Web Element Manager (WEM) provides a graphical user interface (GUI) for performing fault, configuration, accounting, performance, and security (FCAPS) management of the ASR 5000 Platform.

The Web Element Manager is a Common Object Request Broker Architecture (CORBA)-based application that provides complete fault, configuration, accounting, performance, and security (FCAPS) management capability for the system.

For maximum flexibility and scalability, the Web Element Manager application implements a client-server architecture. This architecture allows remote clients with Java-enabled web browsers to manage one or more systems via the server component which implements the CORBA interfaces. The server component is fully compatible with the fault-tolerant Sun® Solaris® operating system.

The following figure demonstrates various interfaces between the Cisco Web Element Manager and other network components.

Figure 5. Web Element Manager Network Interfaces



IMPORTANT: For more information on WEM support, refer to the *WEM Installation and Administration Guide*.

Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for the S-GW service.

Each of the following features require the purchase of an additional license to implement the functionality with the S-GW service.

This section describes following features:

- [IP Security \(IPSec\) Encryption](#)
- [Traffic Policing and Shaping](#)
- [Layer 2 Traffic Management \(VLANs\)](#)

IP Security (IPSec) Encryption

Enables network domain security for all IP packet switched LTE-EPC networks in order to provide confidentiality, integrity, authentication, and anti-replay protection. These capabilities are insured through use of cryptographic techniques.

The Cisco S-GW supports IKEv1 and IPSec encryption using IPv4 addressing. IPSec enables the following two use cases:

- Encryption of S8 sessions and EPS bearers in roaming applications where the P-GW is located in a separate administrative domain from the S-GW
- IPSec ESP security in accordance with 3GPP TS 33.210 is provided for S1 control plane, S1 bearer plane and S1 management plane traffic. Encryption of traffic over the S1 reference interface is desirable in cases where the EPC core operator leases radio capacity from a roaming partner's network.



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

Traffic Policing and Shaping

Traffic policing and shaping allows you to manage bandwidth usage on the network and limit bandwidth allowances to subscribers. Shaping allows you to buffer excesses to be delivered at a later time.

Traffic Policing

Traffic policing enables the configuring and enforcing of bandwidth limitations on individual subscribers and/or APNs of a particular traffic class in 3GPP/3GPP2 service.

Bandwidth enforcement is configured and enforced independently on the downlink and the uplink directions.

A Token Bucket Algorithm (a modified trTCM) [RFC2698] is used to implement the Traffic-Policing feature. The algorithm used measures the following criteria when determining how to mark a packet:

- Committed Data Rate (CDR): The guaranteed rate (in bits per second) at which packets can be transmitted/received for the subscriber during the sampling interval.
- Peak Data Rate (PDR): The maximum rate (in bits per second) that subscriber packets can be transmitted/received for the subscriber during the sampling interval.
- Burst-size: The maximum number of bytes that can be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber's "bucket". Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

The system can be configured to take any of the following actions on packets that are determined to be in excess or in violation:

- Drop: The offending packet is discarded.
- Transmit: The offending packet is passed.
- Lower the IP Precedence: The packet's ToS bit is set to "0", thus downgrading it to Best Effort, prior to passing the packet. Note that if the packet's ToS bit was already set to "0", this action is equivalent to "Transmit".

Traffic Shaping

Traffic Shaping is a rate limiting method similar to the Traffic Policing, but provides a buffer facility for packets exceeded the configured limit. Once the packet exceeds the data-rate, the packet queued inside the buffer to be delivered at a later time.

The bandwidth enforcement can be done in the downlink and the uplink direction independently. If there is no more buffer space available for subscriber data system can be configured to either drop the packets or kept for the next scheduled traffic session.



IMPORTANT: For more information on traffic policing and shaping, refer to the Traffic Policing and Shaping chapter in the *System Enhanced Feature Configuration Guide*.

Layer 2 Traffic Management (VLANs)

Virtual LANs (VLANs) provide greater flexibility in the configuration and use of contexts and services.

VLANs are configured as "tags" on a per-port basis and allow more complex configurations to be implemented. The VLAN tag allows a single physical port to be bound to multiple logical interfaces that can be configured in different contexts. Therefore, each Ethernet port can be viewed as containing many logical ports when VLAN tags are employed.



IMPORTANT: For more information on VLAN support, refer to the VLANs chapter in the *System Enhanced Feature Configuration Guide*.

How the Serving Gateway Works

This section provides information on the function of the S-GW in an EPC E-UTRAN network and presents call procedure flows for different stages of session setup and disconnect.

The S-GW supports the following network flows:

- [GTP Serving Gateway CallSession Procedures in an LTE-SAE Network](#)

GTP Serving Gateway Call/Session Procedures in an LTE-SAE Network

The following topics and procedure flows are included:

- [Subscriber-initiated Attach \(initial\)](#)
- [Subscriber-initiated Detach](#)

Subscriber-initiated Attach (initial)

This section describes the procedure of an initial attach to the EPC network by a subscriber.

Figure 6. Subscriber-initiated Attach (initial) Call Flow

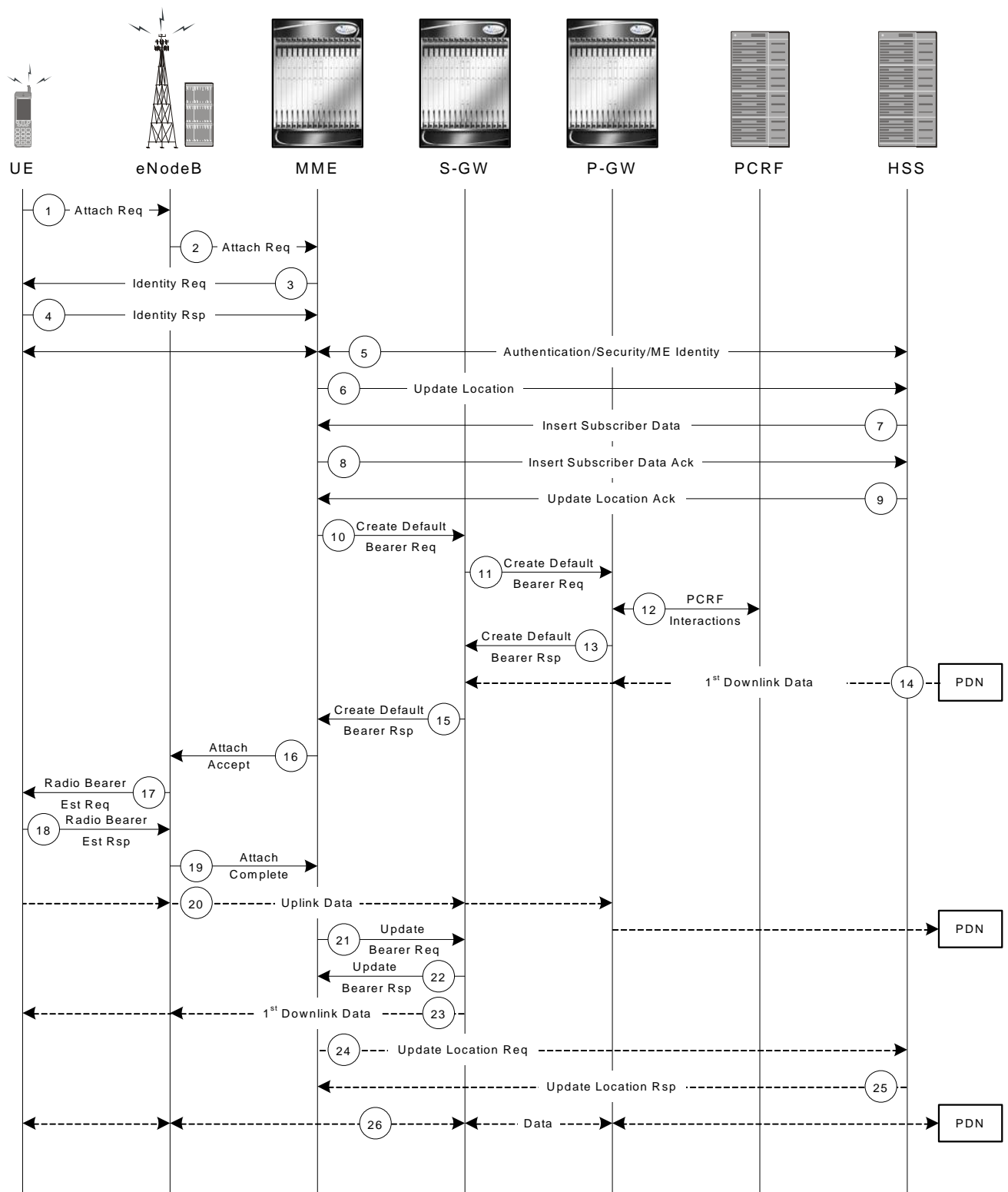


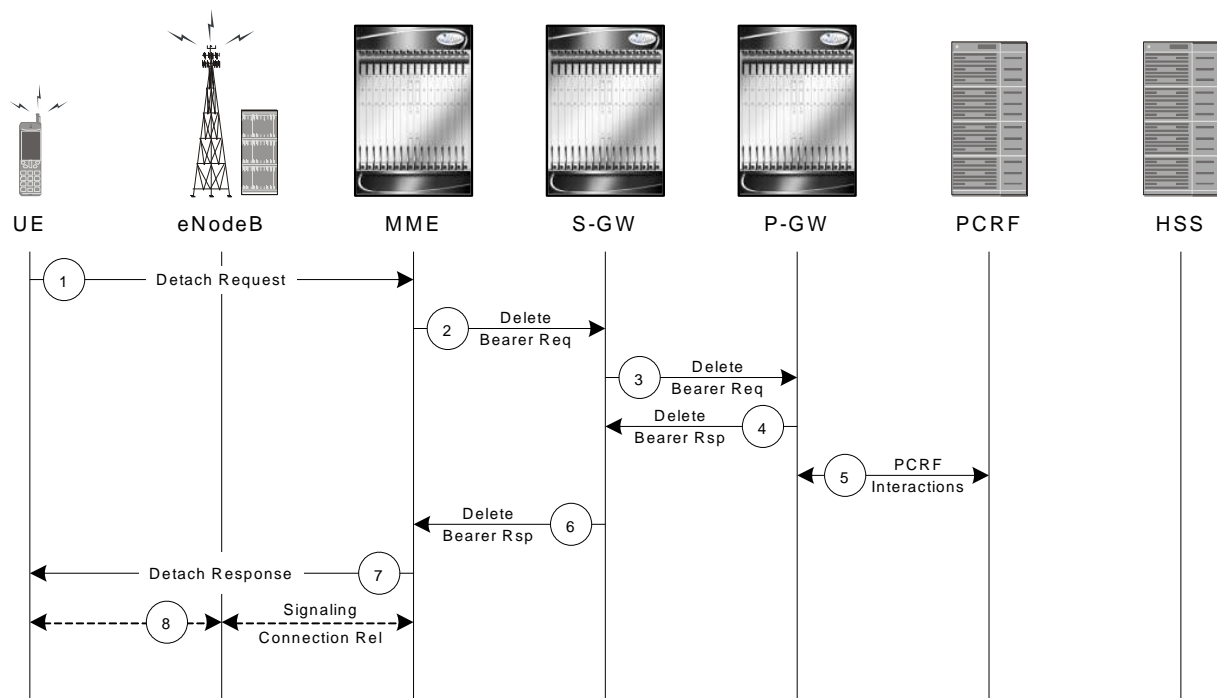
Table 1. Subscriber-initiated Attach (initial) Call Flow Description

Step	Description
1	The UE initiates the Attach procedure by the transmission of an Attach Request (IMSI or old GUTI, last visited TAI (if available), UE Network Capability, PDN Address Allocation, Protocol Configuration Options, Attach Type) message together with an indication of the Selected Network to the eNodeB. IMSI is included if the UE does not have a valid GUTI available. If the UE has a valid GUTI, it is included.
2	The eNodeB derives the MME from the GUTI and from the indicated Selected Network. If that MME is not associated with the eNodeB, the eNodeB selects an MME using an “MME selection function”. The eNodeB forwards the Attach Request message to the new MME contained in a S1-MME control message (Initial UE message) together with the Selected Network and an indication of the E-UTRAN Area identity, a globally unique E-UTRAN ID of the cell from where it received the message to the new MME.
3	If the UE is unknown in the MME, the MME sends an Identity Request to the UE to request the IMSI.
4	The UE responds with Identity Response (IMSI).
5	If no UE context for the UE exists anywhere in the network, authentication is mandatory. Otherwise this step is optional. However, at least integrity checking is started and the ME Identity is retrieved from the UE at Initial Attach. The authentication functions, if performed this step, involves AKA authentication and establishment of a NAS level security association with the UE in order to protect further NAS protocol messages.
6	The MME sends an Update Location (MME Identity, IMSI, ME Identity) to the HSS.
7	The HSS sends Insert Subscriber Data (IMSI, Subscription Data) message to the MME. The Subscription Data contains the list of all APNs that the UE is permitted to access, an indication about which of those APNs is the Default APN, and the 'EPS subscribed QoS profile' for each permitted APN.
8	The MME validates the UE's presence in the (new) TA. If due to regional subscription restrictions or access restrictions the UE is not allowed to attach in the TA, the MME rejects the Attach Request with an appropriate cause, and may return an Insert Subscriber Data Ack message to the HSS. If subscription checking fails for other reasons, the MME rejects the Attach Request with an appropriate cause and returns an Insert Subscriber Data Ack message to the HSS including an error cause. If all checks are successful then the MME constructs a context for the UE and returns an Insert Subscriber Data Ack message to the HSS. The Default APN shall be used for the remainder of this procedure.
9	The HSS acknowledges the Update Location message by sending an Update Location Ack to the MME. If the Update Location is rejected by the HSS; the MME rejects the Attach Request from the UE with an appropriate cause.
10	The MME selects an S-GW using “Serving GW selection function” and allocates an EPS Bearer Identity for the Default Bearer associated with the UE. If the PDN subscription context contains no P-GW address the MME selects a P-GW as described in clause “PDN GW selection function”. Then it sends a Create Default Bearer Request (IMSI, MME Context ID, APN, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the selected S-GW.
11	The S-GW creates a new entry in its EPS Bearer table and sends a Create Default Bearer Request (IMSI, APN, S-GW Address for the user plane, S-GW TEID of the user plane, S-GW TEID of the control plane, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the P-GW.
12	If dynamic PCC is deployed, the P-GW interacts with the PCRF to get the default PCC rules for the UE. The IMSI, UE IP address, User Location Information, RAT type, AMBR are provided to the PCRF by the P-GW if received by the previous message.

Step	Description
13	The P-GW returns a Create Default Bearer Response (P-GW Address for the user plane, P-GW TEID of the user plane, P-GW TEID of the control plane, PDN Address Information, EPS Bearer Identity, Protocol Configuration Options) message to the S-GW. PDN Address Information is included if the P-GW allocated a PDN address Based on PDN Address Allocation received in the Create Default Bearer Request. PDN Address Information contains an IPv4 address for IPv4 and/or an IPv6 prefix and an Interface Identifier for IPv6. The P-GW takes into account the UE IP version capability indicated in the PDN Address Allocation and the policies of operator when the P-GW allocates the PDN Address Information. Whether the IP address is negotiated by the UE after completion of the Attach procedure, this is indicated in the Create Default Bearer Response.
14	The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data.
15	The S-GW returns a Create Default Bearer Response (PDN Address Information, S-GW address for User Plane, S-GW TEID for User Plane, S-GW Context ID, EPS Bearer Identity, Protocol Configuration Options) message to the new MME. PDN Address Information is included if it was provided by the P-GW.
16	The new MME sends an Attach Accept (APN, GUTI, PDN Address Information, TAI List, EPS Bearer Identity, Session Management Configuration IE, Protocol Configuration Options) message to the eNodeB.
17	The eNodeB sends Radio Bearer Establishment Request including the EPS Radio Bearer Identity to the UE. The Attach Accept message is also sent along to the UE.
18	The UE sends the Radio Bearer Establishment Response to the eNodeB. In this message, the Attach Complete message (EPS Bearer Identity) is included.
19	The eNodeB forwards the Attach Complete (EPS Bearer Identity) message to the MME.
20	The Attach is complete and UE sends data over the default bearer. At this time the UE can send uplink packets towards the eNodeB which are then tunnelled to the S-GW and P-GW.
21	The MME sends an Update Bearer Request (eNodeB address, eNodeB TEID) message to the S-GW.
22	The S-GW acknowledges by sending Update Bearer Response (EPS Bearer Identity) message to the MME.
23	The S-GW sends its buffered downlink packets.
24	After the MME receives Update Bearer Response (EPS Bearer Identity) message, if an EPS bearer was established and the subscription data indicates that the user is allowed to perform handover to non-3GPP accesses, and if the MME selected a P-GW that is different from the P-GW address which was indicated by the HSS in the PDN subscription context, the MME sends an Update Location Request including the APN and P-GW address to the HSS for mobility with non-3GPP accesses.
25	The HSS stores the APN and P-GW address pair and sends an Update Location Response to the MME.
26	Bidirectional data is passed between the UE and PDN.

Subscriber-initiated Detach

This section describes the procedure of detachment from the EPC network by a subscriber.

Figure 7. Subscriber-initiated Detach Call Flow**Table 2. Subscriber-initiated Detach Call Flow Description**

Step	Description
1	The UE sends NAS message Detach Request (GUTI, Switch Off) to the MME. Switch Off indicates whether detach is due to a switch off situation or not.
2	The active EPS Bearers in the S-GW regarding this particular UE are deactivated by the MME sending a Delete Bearer Request (TEID) message to the S-GW.
3	The S-GW sends a Delete Bearer Request (TEID) message to the P-GW.
4	The P-GW acknowledges with a Delete Bearer Response (TEID) message.
5	The P-GW may interact with the PCRF to indicate to the PCRF that EPS Bearer is released if PCRF is applied in the network.
6	The S-GW acknowledges with a Delete Bearer Response (TEID) message.
7	If Switch Off indicates that the detach is not due to a switch off situation, the MME sends a Detach Accept message to the UE.
8	The MME releases the S1-MME signalling connection for the UE by sending an S1 Release command to the eNodeB with Cause = Detach.

Supported Standards

The S-GW service complies with the following standards.

- [3GPP References](#)
- [3GPP2 References](#)
- [IETF References](#)
- [Object Management Group \(OMG\) Standards](#)

3GPP References

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.107: Quality of Service (QoS) concept and architecture
- 3GPP TS 23.203: Policy and charging control architecture
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture Enhancements for non-3GPP accesses
- 3GPP TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 24.229: IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3
- 3GPP TS 29.210: Gx application
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.213: Policy and Charging Control signaling flows and QoS
- 3GPP TS 29.214: Policy and Charging Control over Rx reference point
- 3GPP TS 29.274: Evolved GPRS Tunnelling Protocol for Control plane (GTPv2-C), version 8.1.1
- 3GPP TS 29.274: Evolved GPRS Tunnelling Protocol for Control plane (GTPv2-C), version 8.2.0 (both versions are intentional)
- 3GPP TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols, version 8.1.0
- 3GPP TS 29.281: GPRS Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging
- 3GPP TS 32.295: Charging management; Charging Data Record (CDR) transfer

- 3GPP TS 32.298: Telecommunication management; Charging management; Charging Data Record (CDR) encoding rules description
- 3GPP TS 32.299: Charging management; Diameter charging applications
- 3GPP TS 33.106: 3G Security; Lawful Interception Requirements
- 3GPP TS 36.107: 3G security; Lawful interception architecture and functions
- 3GPP TS 36.300: Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description
- 3GPP TS 36.412: EUTRAN S1 signaling transport
- 3GPP TS 36.413: Evolved Universal Terrestrial Radio Access (E-UTRA); S1 Application Protocol (S1AP)
- 3GPP TS 36.414: Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 data transport

3GPP2 References

- X.P0057-0 v0.11.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

IETF References

- RFC 768: User Datagram Protocol (STD 6).
- RFC 791: Internet Protocol (STD 5).
- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2698: A Two Rate Three Color Marker
- RFC 2784: Generic Routing Encapsulation (GRE)
- RFC 2890: Key and Sequence Number Extensions to GRE
- RFC 3319: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
- RFC 3588: Diameter Base Protocol
- RFC 3775: Mobility Support in IPv6
- RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4006: Diameter Credit-Control Application
- RFC 4282: The Network Access Identifier
- RFC 4283: Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4861: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration

Supported Standards

- RFC 5094: Mobile IPv6 Vendor Specific Option
- RFC 5213: Proxy Mobile IPv6
- Internet-Draft (draft-ietf-netlmm-proxymip6-07.txt): Proxy Mobile IPv6
- Internet-Draft (draft-ietf-netlmm-grekey-option-01.txt): GRE Key Option for Proxy Mobile IPv6, work in progress
- Internet-Draft (draft-ietf-mext-binding-revocation-02.txt): Binding Revocation for IPv6 Mobility, work in progress

Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group

Chapter 2

Serving Gateway Configuration

This chapter provides configuration information for the Serving Gateway (S-GW).



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 S-GW product are located in the *Command Line Interface Reference*.

The following procedures are located in this chapter:

- [Configuring the System as a Standalone eGTP S-GW](#)

Configuring the System as a Standalone eGTP S-GW

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as a eGTP S-GW in a test environment. For a more robust configuration example, refer to the *Sample Configuration Files* appendix. Information provided in this section includes the following:

- [Information Required](#)
- [How This Configuration Works](#)
- [eGTP S-GW Configuration](#)

Information Required

The following sections describe the minimum amount of information required to configure and make the S-GW operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the S-GW in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an eGTP S-GW.

Table 3. Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

Required Information	Description
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access that will be used to access the system such as telnetd, sshd, and/or ftpd.

Required S-GW Ingress Context Configuration Information

The following table lists the information that is required to configure the S-GW ingress context on an eGTP S-GW.

Table 4. Required Information for S-GW Ingress Context Configuration

Required Information	Description
S-GW ingress context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the S-GW ingress context is recognized by the system.
Accounting policy name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy is recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.
S1-U/S11 Interface Configuration (To/from eNodeB/MME)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
GTP-U Service Configuration	
GTP-U service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service will be recognized by the system.

Required Information	Description
IP address	S1-U/S11 interface IPv4 or IPv6 address.
S-GW Service Configuration	
S-GW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the S-GW service is recognized by the system. Multiple names are needed if multiple S-GW services will be used.
eGTP Ingress Service Configuration	
eGTP Ingress Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP ingress service is recognized by the system.

Required S-GW Egress Context Configuration Information

The following table lists the information that is required to configure the S-GW egress context on an eGTP S-GW.

Table 5. Required Information for S-GW Egress Context Configuration

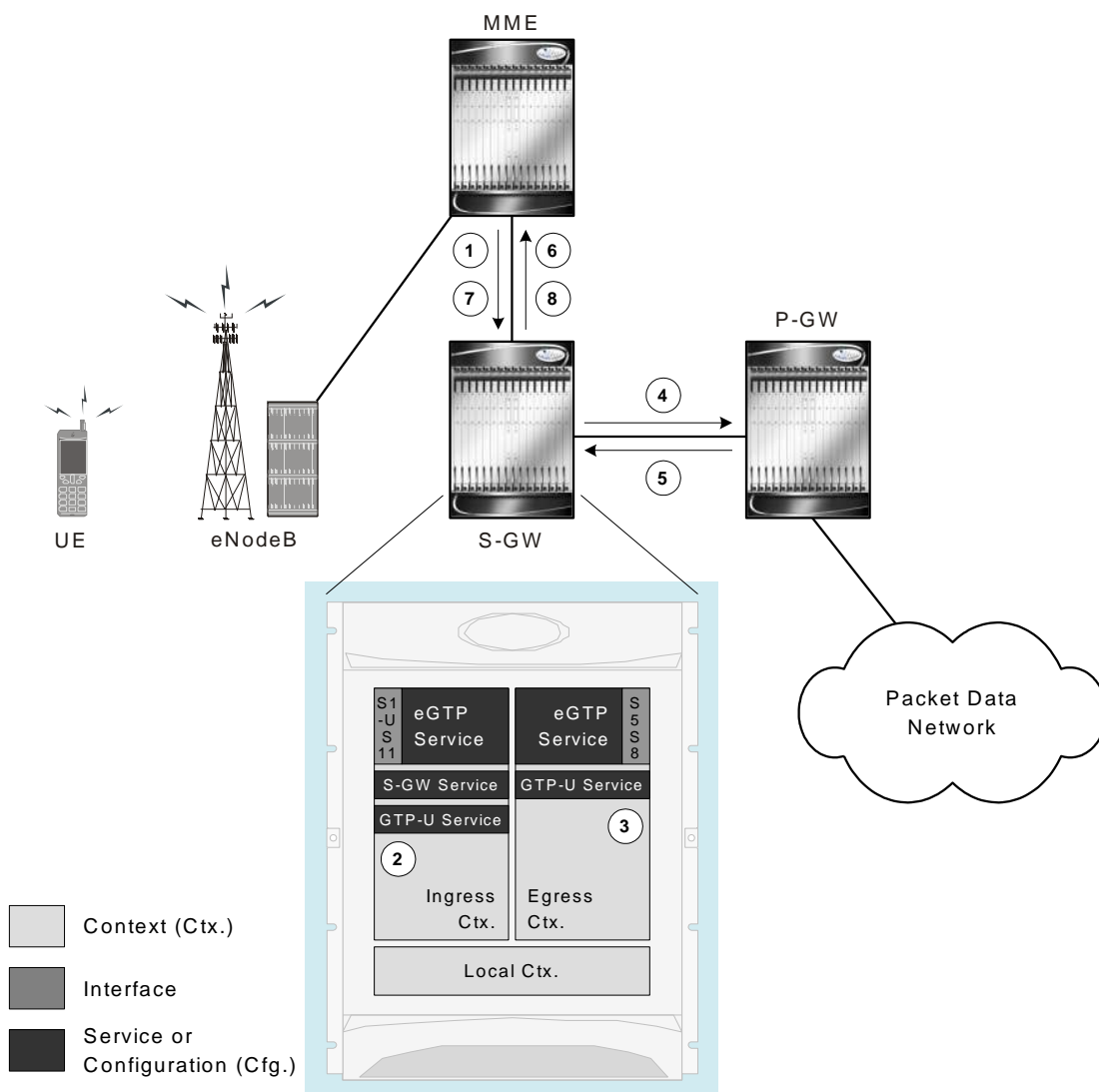
Required Information	Description
S-GW egress context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the S-GW egress context is recognized by the system.
S5/S8 Interface Configuration (To/from P-GW)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
GTP-U Service Configuration	
GTP-U service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service will be recognized by the system.
IP address	S5/S8 interface IPv4 or IPv6 address.
eGTP Egress Service Configuration	

Required Information	Description
eGTP Egress Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP egress service is recognized by the system.

How This Configuration Works

The following figure and supporting text describe how this configuration with a single ingress and egress context is used by the system to process a subscriber call.

Figure 8. eGTP S-GW Call Processing Using a Single Ingress and Egress Context

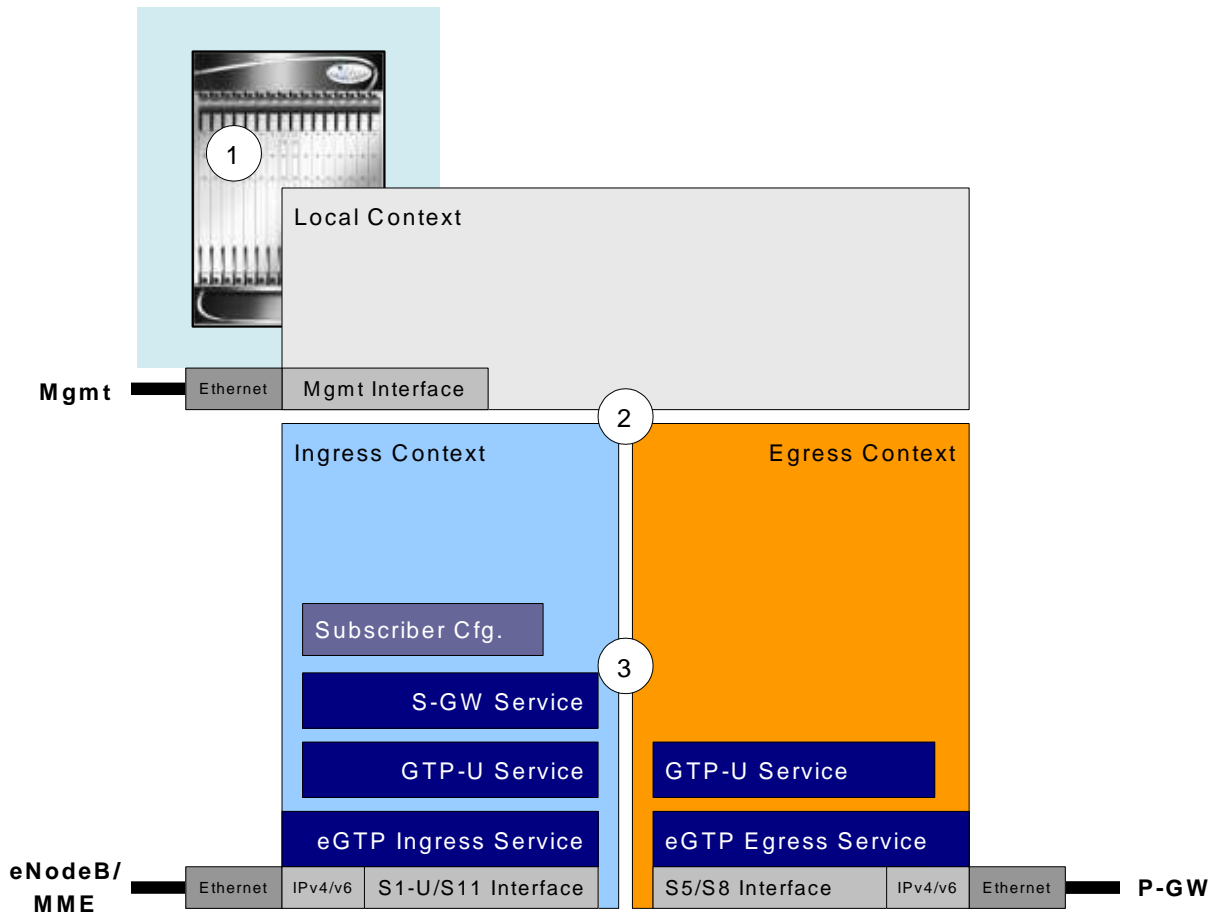


1. A subscriber session from the MME is received by the S-GW service over the S11 interface.
2. The S-GW service determines which context to use to access PDN services for the session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the System Administration Guide.
3. S-GW uses the configured egress context to determine the eGTP service to use for the outgoing S5/S8 connection.
4. The S-GW establishes the S5/S8 connection by sending a create session request message to the P-GW.
5. The P-GW responds with a Create Session Response message that includes the PGW S5/S8 Address for control plane and bearer information.
6. The S-GW conveys the control plane and bearer information to the MME in a Create Session Response message.

7. The MME responds with a Create Bearer Response and Modify Bearer Request message.
8. The S-GW sends a Modify Bearer Response message to the MME.

eGTP S-GW Configuration

To configure the system to perform as a standalone eGTP S-GW, review the following graphic and subsequent steps.



- 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 contexts and services by applying the example configurations found in the [Initial Configuration](#) section of this chapter.
- Step 3** Configure the system to perform as an eGTP S-GW and set basic S-GW parameters such as eGTP interfaces and an IP route by applying the example configurations presented in the [eGTP Configuration](#) section.
- Step 4** Verify and save the configuration by following the instruction in the [Verifying and Saving 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 an ingress context where the S-GW and eGTP ingress service will reside by applying the example configuration in the [Creating an S-GW Ingress Context](#) section.
- Step 3** Create an eGTP ingress service within the newly created ingress context by applying the example configuration in the [Creating an eGTP Ingress Service](#) section.
- Step 4** Create an S-GW egress context where the eGTP egress services will reside by applying the example configuration in the [Creating an S-GW Egress Context](#) section.
- Step 5** Create an eGTP egress service within the newly created egress context by applying the example configuration in the [Creating an eGTP Egress Service](#) section.
- Step 6** Create a S-GW service within the newly created ingress context by applying the example configuration in the [Creating an S-GW 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 <lcl_cntxt_intrfc_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 <lcl_cntxt_intrfc_name> local

end
```

Creating an S-GW Ingress Context

Use the following example to create an S-GW ingress context and Ethernet interfaces to an MME and eNodeB, and bind the interfaces to configured Ethernet ports.

```
configure

context <ingress_context_name> -noconfirm

  subscriber default

  exit

  interface <slu-s11_interface_name>

    ip address <ipv4_address_primary>

    ip address <ipv4_address_secondary>

    exit

    ip route 0.0.0.0 0.0.0.0 <next_hop_address> <sgw_interface_name>

    exit

  port ethernet <slot_number/port_number>

    no shutdown

    bind interface <slu-s11_interface_name> <ingress_context_name>

  end
```

Notes:

- This example presents the S1-U/S11 connections as a shared interface. These interfaces can be separated to support a different network architecture.
- The S1-U/S11 interface IP address(es) can also be specified as IPv6 addresses using the **ipv6 address** command.

Creating an eGTP Ingress Service

Use the following configuration example to create an eGTP ingress service:

```
configure
```

```

context <ingress_context_name>

  egtp-service <egtp_ingress_service_name> -noconfirm

end

```

Creating an S-GW Egress Context

Use the following example to create an S-GW egress context and Ethernet interface to a P-GW and bind the interface to configured Ethernet ports.

```

configure

context <egress_context_name> -noconfirm

  interface <s5s8_interface_name> tunnel

    ipv6 address <address>

    tunnel-mode ipv6ip

    source interface <name>

    destination address <ipv4 or ipv6 address>

  end

configure

port ethernet <slot_number/port_number>

  no shutdown

  bind interface <s5s8_interface_name> <egress_context_name>

end

```

Notes:

- The S5/S8 interface IP address can also be specified as an IPv4 address using the **ip address** command.

Creating an eGTP Egress Service

Use the following configuration example to create an eGTP egress service in the S-GW egress context:

```

configure

context <egress_context_name>

  egtp-service <egtp_egress_service_name> -noconfirm

end

```

Creating an S-GW Service

Use the following configuration example to create the S-GW service in the ingress context:

```
configure
    context <ingress_context_name>
        sgw-service <sgw_service_name> -noconfirm
    end
```

eGTP Configuration

- Step 1** Set the system's role as an eGTP S-GW and configure eGTP service settings by applying the example configuration in the [Setting the Systems Role as an eGTP S-GW and Configuring GTP-U and eGTP Service Settings](#) section.
- Step 2** Configure the S-GW service by applying the example configuration in the [Configuring the S-GW Service](#) section.
- Step 3** Specify an IP route to the eGTP Serving Gateway by applying the example configuration in the [Configuring an IP Route](#) section.

Setting the System's Role as an eGTP S-GW and Configuring GTP-U and eGTP Service Settings

Use the following configuration example to set the system to perform as an eGTP S-GW and configure the GTP-U and eGTP services:

```
configure
    context <sgw_ingress_context_name>
        gtp group default
        exit
        gtpu-service <gtpu_ingress_service_name>
            bind ipv4-address <s1-us11_interface_ip_address>
            exit
        egtp-service <egtp_ingress_service_name>
            interface-type interface-sgw-ingress
            validation-mode default
            associate gtpu-service <gtpu_ingress_service_name>
            gtpc bind address <s1u-s11_interface_ip_address>
```

```

    exit
  exit
  context <sgw_egress_context_name>
    gtpu-service <gtpu_egress_service_name>
      bind ipv4-address <s5s8_interface_ip_address>
    exit
    egtp-service <egtp_egress_service_name>
      interface-type interface-sgw-egress
      validation-mode default
      associate gtpu-service <gtpu_egress_service_name>
      gtpc bind address <s5s8_interface_ip_address>
    end
  end

```

Notes:

- The **bind** command in the GTP-U ingress and egress service configuration can also be specified as an IPv6 address using the **ipv6-address** command.

Configuring the S-GW Service

Use the following example to configure the S-GW service:

```

configure
  context <ingress_context_name>
    sgw-servers <sgw_service_name> -noconfirm
      associate ingress egtp-service <egtp_ingress_service_name>
      associate egress-proto gtp egress-context <egress_context_name>
      qci-qos-mapping <map_name>
    end
  end

```

Configuring an IP Route

Use the following example to configure an IP Route for control and user plane data communication with an eGTP PDN Gateway:

```

configure

```



```
context <egress_context_name>
    ip route <pgw_ip_addr/mask> <sgw_next_hop_addr> <sgw_intrfc_name>
end
```

Verifying and Saving the Configuration

Refer to the [Verifying and Saving the Configuration](#) chapter to verify and save your S-GW configuration.

Chapter 3

Verifying and Saving Your Configuration

This chapter describes how to save the system configuration.

Verifying the Configuration

You can use a number of command 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, specific features are set and need to be verified. 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: gtpv 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))
||||
||||+--Busout: (B) - Busout 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: Many features can be configured on the system. There are show commands specifically for these features. Refer to the *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 SPC's/SMC's CompactFlash or on an installed PCMCIA memory card on the SPC/SMC. Files that are saved to a remote network node can be transmitted using either 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
<i>url</i>	<p>Specifies the path and name to which the configuration file is to be stored. <i>url</i> may refer to a local or a remote file. <i>url</i> must be entered using one of the following formats:</p> <ul style="list-style-type: none"> • <code>{ /flash /pcmcia1 /pcmcia2 } [/dir] /file_name</code> • <code>file://{ /flash /pcmcia1 /pcmcia2 } [/dir] /file_name</code> • <code>tftp://{ ipaddress host_name [:port#] } [/directory] /file_name</code> • <code>ftp://{ username [:pwd] @ } { ipaddress host_name } [:port#] [/directory] /file_name</code> • <code>sftp://{ username [:pwd] @ } { ipaddress host_name } [:port#] [/directory] /file_name</code> <p>/flash corresponds to the CompactFlash on the SPC/SMC. /pcmcia1 corresponds to PCMCIA slot 1. /pcmcia2 corresponds to PCMCIA slot 2. <i>ipaddress</i> is the IP address of the network server. <i>host_name</i> is the network server's <i>hostname</i>. <i>port#</i> is the network server's logical port number. Defaults are:</p> <ul style="list-style-type: none"> • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data <p>Note: <i>host_name</i> can only be used if the networkconfig parameter is configured for DHCP and the DHCP server returns a valid nameserver. <i>username</i> is the username required to gain access to the server if necessary. <i>password</i> is the password for the specified username if required. <i>/directory</i> specifies the directory where the file is located if one exists. <i>/file_name</i> specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.</p>
-redundant	<p>Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the <i>url</i> variable, and then automatically copy that same file to the like device on the Standby SPC/SMC, if available.</p> <p>Note: This keyword will only work for like local devices that are located on both the active and standby SPCs/SMCs. For example, if you save the file to the /pcmcia1 device on the active SPC/SMC, that same type of device (a PC-Card in Slot 1 of the standby SPC/SMC) must be available. Otherwise, a failure message is displayed.</p> <p>Note: If saving the file to an external network (non-local) device, the system disregards this keyword.</p>

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



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 SPC/SMC, then you must synchronize the local file system on both SPCs/SMCs.

To save a configuration file called `system.cfg` to a directory that was previously created called `cfgfiles` on the SPC's/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
```

Chapter 4

Monitoring the Service

This chapter provides information for monitoring service status and performance using the **show** commands found in the Command Line Interface (CLI). These command have many related keywords that allow them to provide useful information on all aspects of the system ranging from current software configuration through call activity and status.

The selection of keywords described in this chapter is intended to provided the most useful and in-depth information for monitoring the system. For additional information on these and other **show** command keywords, refer to the *Command Line Interface Reference*.


In addition to the CLI, the system supports the sending of Simple Network Management Protocol (SNMP) traps that indicate status and alarm conditions. Refer to the *SNMP MIB Reference* for a detailed listing of these traps.

Monitoring System Status and Performance

This section contains commands used to monitor the status of tasks, managers, applications and other software components in the system. Output descriptions for most of the commands are located in the *Statistics and Counters Reference*.

Table 6. System Status and Performance Monitoring Commands

To do this:	Enter this command:
View Congestion-Control Information	
View Congestion-Control Statistics	
View Congestion-Control Statistics	<code>show congestion-control statistics { allmgr ipsecmgr }</code>
View Subscriber Information	
Display Session Resource Status	
View session resource status	<code>show resources session</code>
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	<code>show subscribers configuration username subscriber_name</code>
View remotely configured subscriber profile settings	<code>show subscribers aaa-configuration username subscriber_name</code>
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the system	<code>show subscribers all</code>
View Statistics for Subscribers using S-GW Services on the System	
View statistics for subscribers using any S-GW service on the system	<code>show subscribers sgw-only full</code>
View statistics for subscribers using a specific S-GW service on the system	<code>show subscribers sgw-service service_name</code>
View Statistics for Subscribers using MAG Services on the System	
View statistics for subscribers using any MAG service on the system	<code>show subscribers mag-only full</code>
View statistics for subscribers using a specific MAG service on the system	<code>show subscribers mag-service service_name</code>
View Session Subsystem and Task Information	

To do this:	Enter this command:
Display Session Subsystem and Task Statistics	
 IMPORTANT: Refer to the System Software Task and Subsystem Descriptions appendix in the <i>System Administration Guide</i> for additional information on the Session subsystem and its various manager tasks.	
View AAA Manager statistics	<code>show session subsystem facility aaamgr all</code>
View AAA Proxy statistics	<code>show session subsystem facility aaaproxy all</code>
View Session Manager statistics	<code>show session subsystem facility sessmgr all</code>
View MAG Manager statistics	<code>show session subsystem facility magmgr all</code>
View Session Recovery Information	
View session recovery status	<code>show session recovery status [verbose]</code>
View Session Disconnect Reasons	
View session disconnect reasons with verbose output	<code>show session disconnect-reasons</code>
View S-GW Service Information	
View S-GW service statistics	<code>show sgw-service statistics all</code>
View MAG Service Information	
View MAG service statistics for a specific service	<code>show mag-service statistics name <i>service_name</i></code>
View GTP Information	
View eGTP-C service statistics for a specific service	<code>show egtpc statistics egtpc-service <i>name</i></code>
View GTP-U service statistics for all GTP-U data traffic on the system	<code>show gtpu statistics</code>
View QoS/QCI Information	
View QoS Class Index to QoS mapping tables	<code>show qci-qos-mapping table all</code>

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping (PPP, MIPHA, MIPFA, etc.).

Statistics and counters can be cleared using the CLI **clear** command. Refer to *Command Line Reference* for detailed information on using this command.

Chapter 5

Configuring Subscriber Session Tracing

This chapter provides information on subscriber session trace functionality to allow an operator to trace subscriber activity at various points in the network and at various level of details in EPS network. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.



IMPORTANT: The features described in this chapter is an enhanced feature and need enhanced feature license. This support is only available if you have purchased and installed particular feature support license on your chassis.

This chapter discusses following topics for feature support of Subscriber Session Tracing in LTE service:

- [Introduction](#)
- [Supported Standards](#)
- [Supported Networks and Platforms](#)
- [Licenses](#)
- [Subscriber Session Tracing Functional Description](#)
- [Subscriber Session Trace Configuration](#)
- [Verifying Your Configuration](#)

Introduction

The Subscriber Level Trace provides a 3GPP standards-based session-level trace function for call debugging and testing new functions and access terminals in an LTE environment.

In general, the Session Trace capability records and forwards all control activity for the monitored subscriber on the monitored interfaces. This is typically all the signaling and authentication/subscriber services messages that flow when a UE connects to the access network.

The EPC network entities like MME, S-GW, P-GW support 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S6a, S1-MME and S11 on MME, S5, S8, S11 at S-GW and S5 and S8 on P-GW. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at HSS with trace activation via authentication response messages over S6a reference interface
- Signaling based activation through signaling from subscriber access terminal



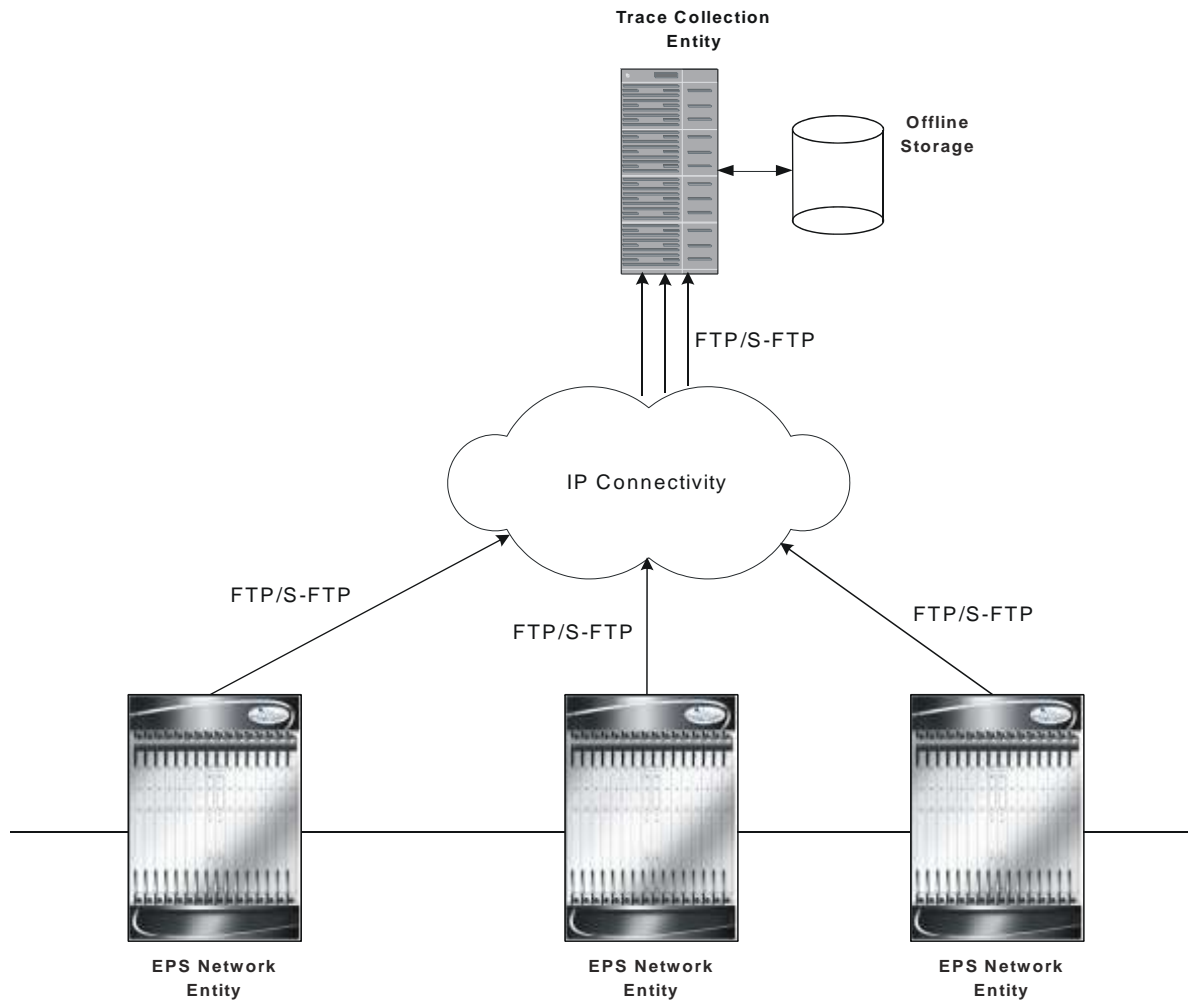
IMPORTANT: Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

The session level trace function consists of trace activation followed by triggers. The time between the two events is treated much like Lawful Intercept where the EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the ASR 5000 platforms. The Trace Depth defines the granularity of data to be traced. Six levels are defined including Maximum, Minimum and Medium with ability to configure additional levels based on vendor extensions.



IMPORTANT: Only Maximum Trace Depth is supported in the current release.

The following figure shows a high-level overview of the session-trace functionality and deployment scenario:

Figure 9. Session Trace Function and Interfaces

All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a FTP or secure FTP (SFTP) connection.

Note: In the current release the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI.

Supported Functions

This section provides the list of supported functionality of this feature support:

- Support to trace the control flow through the access network.
 - Trace of specific subscriber identified by IMSI
 - Trace of UE identified by IMEI(SV)

- Ability to specify specific functional entities and interfaces where tracing should occur.
- Scalability and capacity
 - Support up to 32 simultaneous session traces per NE
 - Capacity to activate/deactivate TBD trace sessions per second
 - Each NE can buffer TBD bytes of trace data locally
- Statistics and State Support
- Session Trace Details
- Management and Signaling-based activation models
- Trace Parameter Propagation
- Trace Scope (EPS Only)
 - MME: S1, S3, S6a, S10, S11
 - S-GW: S4, S5, S8, S11, Gxc
 - PDN-GW: S2a, S2b, S2c, S5, S6b, Gx, S8, SGi
- Trace Depth: Maximum, Minimum, Medium (with or without vendor extension)
- XML Encoding of Data as per 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09)
- Trace Collection Entity (TCE) Support
 - Active pushing of files to the TCE
 - Passive pulling of files by the TCE
- 1 TCE support per context
- Trace Session Recovery after Failure of Session Manager

Supported Standards

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- 3GPP TS 32.421 V8.5.0 (2009-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace concepts and requirements (Release 8)
- 3GPP TS 32.422 V8.6.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace; Trace control and configuration management (Release 8)
- 3GPP TS 32.423 V8.2.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace data definition and management (Release 8)

Supported Networks and Platforms

This feature supports all ASR 5000 Series Platforms with StarOS Release 9.0 or later running MME/S-GW/P-GW service(s) for the core LTE network functions.

Licenses

This is a base feature and available for configuration with default LTE component license(s) on the system:

Subscriber Session Trace Functional Description

This section describes the various functionality involved in tracing of subscriber session on EPC nodes:

Operation

The session trace functionality is separated into two steps - activation and trigger.

Before tracing can begin, it must be activated. Activation is done either via management request or when a UE initiates a signaled connection. After activation, tracing actually begins when it is triggered (defined by a set of trigger events).

Trace Session

A trace session is the time between trace activation and trace de-activation. It defines the state of a trace session, including all user profile configuration, monitoring points, and start/stop triggers. It is uniquely identified by a Trace Reference.

The Trace Reference id is composed of the MCC (3 digits) + the MNC (3 digits) + the trace Id (3 byte octet string).

Trace Recording Session

A trace recording session is a time period in which activity is actually being recorded and traceable data is being forwarded to the TCE. A trace recording session is initiated when a start trigger event occurs and continues until the stop trigger event occurs and is uniquely identified by a Trace Recording Session Reference.

Network Element (NE)

Network elements are the functional component to facilitate subscriber session trace in mobile network.

The term network element refers to a functional component that has standard interfaces in and out of it. It is typically shown as a stand-alone AGW. Examples of NEs are the MME, S-GW, and P-GW.

Currently subscriber session trace is not supported for co-located network elements in EPC network.

Activation

Activation of a trace is similar whether it be via the management interface or via a signaling interface. In both cases, a trace session state block is allocated which stores all configuration and state information for the trace session. In addition, a (S)FTP connection to the TCE is established if one does not already exist (if this is the first trace session established, odds are there will not be a (S)FTP connection already established to the TCE).

If the session to be traced is already active, tracing may begin immediately. Otherwise, tracing activity concludes until the start trigger occurs (typically when the subscriber/UE under trace initiates a connection). A failure to activate a trace (due to max exceeded or some other failure reason) results in a notification being sent to the TCE indicating the failure.

Management Activation

With a management-initiated activation, the WEM sends an activation request directly to the NE where the trace is to be initiated. The NE establishes the trace session and waits for a triggering event to start actively tracing. Depending upon the configuration of the trace session, the trace activation may be propagated to other NEs.

Signaling Activation

With a signaling based activation, the trace session is indicated to the NE across a signaling interface via a trace invocation message. This message can either be piggybacked with an existing bearer setup message (in order to trace all control messages) or by sending a separate trace invocation message (if the user is already active).

Start Trigger

A trace recording session starts upon reception of one of the configured start triggers. Once the start trigger is received, the NE generates a Trace Recording Session Reference (unique to the NE) and begins to collect and forward trace information on the session to the TCE.

List of trigger events are listed in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

Deactivation

Deactivation of a Trace Session is similar whether it was management or signaling activated. In either case, a deactivation request is received by the NE that contains a valid trace reference results in the de-allocation of the trace session state block and a flushing of any pending trace data. In addition, if this is the last trace session to a particular TCE, the (S)FTP connection to the TCE is released after the last trace file is successfully transferred to the TCE.

Stop Trigger

A trace recording session ends upon the reception of one of the configured stop triggers. Once the stop trigger is received, the NE will terminate the active recording session and attempt to send any pending trace data to the TCE. The list of triggering events can be found in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

Data Collection and Reporting

Subscriber session trace functionality supports data collection and reporting system to provide historical usage and event analysis.

All data collected by the NE is formatted into standard XML file format and forwarded to the TCE via (S)FTP. The specific format of the data is defined in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09).

Trace Depth

The Trace Depth defines what data is to be traced. There are six depths defined: Maximum, Minimum, and Medium all having with and without vendor extension flavors. The maximum level of detail results in the entire control message getting traced and forwarded to the TCE. The medium and minimum define varying subsets of the control messages (specific decoded IEs) to be traced and forwarded. The contents and definition of the medium and minimum trace can be found in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09).

Note: Only Maximum Trace Depth is supported in the current release.

Trace Scope

The Trace Scope defines what NEs and what interfaces have the tracing capabilities enabled on them. This is actually a specific list of NE types and interfaces provided in the trace session configuration by the operator (either directly via a management interface or indirectly via a signaling interface).

Network Element Details

Trace functionality for each of the specific network elements supported by this functionality are described in this section.

This section includes the trace monitoring points applicable to them as well as the interfaces over which they can send and/or receive trace configuration.

MME

The MME support tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S1a	eNodeB	N	Y
S3	SGSN	Y	Y
S6a	HSS	Y	N
S10	MME	Y	Y
S11	S-GW	N	Y

S-GW

The S-GW support tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
----------------	---------------	-----------------------------------	-----------------------------------

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S4	SGSN	N	N
S3	P-GW (Intra-PLMN)	N	Y
S6a	P-GW (Inter-PLMN)	N	N
S11	MME	Y	N

P-GW

The PDN-GW support tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S2abc	Various NEs	N	N
S5	S-GW (Intra-PLMN)	Y	N
S6b	AAA Server/Proxy	Y	N
S8	S-GW (Inter-PLMN)	N	N
Gx	Policy Server	Y	N
SGi	IMS	Y	N

Subscriber Session Trace Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system to enable the Subscriber Session Trace collection and monitoring function on network elements in LTE/EPC networks.



IMPORTANT: This section provides the minimum instruction set to enable the Subscriber Session Trace functionality to collect session traces on network elements on EPC networks. Commands that configure additional function for this feature are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in the *System Administration Guide* and specific product Administration Guide.

To configure the system to support subscriber session trace collection and trace file transport on a system:

- Step 1** Enable the subscriber session trace functionality with NE interface and TCE address at the Exec Mode level on an EPC network element by applying the example configurations presented in the *Enabling Subscriber Session Trace on EPC Network Element* section.
- Step 2** Configure the network and trace file transportation parameters by applying the example configurations presented in the *Trace File Collection Configuration* section.
- Step 3** Save the changes to system configuration by applying the example configuration found in *Verifying and Saving Your Configuration* chapter.
- Step 4** Verify the configuration of Subscriber Session Trace related parameters by applying the commands provided in the *Verifying Your Configuration* section of this chapter.

Enabling Subscriber Session Trace on EPC Network Element

This section provides the configuration example to enable the subscriber session trace on a system at the Exec mode:

```
session trace subscriber network-element {mme | pgw | sgw} {imei
<imei_id> {imsi <imsi_id>} {interface {all | <interface>}} trace-ref
<trace_ref_id> collection-entity <ip_address>
```

Notes:

- *<interface>* is the name of the interfaces applicable for specific NE on which subscriber session traces have to be collected. For more information, refer **session trace subscriber** command in the *Command Line Interface Reference*.
- *<trace_ref_id>* is the configured Trace Id to be used for this trace collection instance. It is composed of MCC (3 digit)+MNC (3 digit)+Trace Id (3 byte octet string).
- *<ip_address>* is the IP address of Trace collection Entity in IPv4 notation.

Trace File Collection Configuration

This section provides the configuration example to configure the trace file collection parameters and protocols to be used to store trace files on TCE through FTP/S-FTP:

```
configure

    session trace [ collection-timer <dur> ] [ network-element { all | mme
| pgw | sgw } ] [ retry-timer <dur> ] [ tce-mode { none | push transport
{ ftp | sftp } path <string> username <name> { encrypted password
<enc_pw> | password <password> } } ]

end
```

Notes:

- <string> is the location/path on the trace collection entity (TCE) where trace files will be stored on TCE. For more information, refer **session trace** command in the *Command Line Interface Reference*.

Verifying Your Configuration

This section explains how to display and review the configurations after saving them in a .cfg file as described in Saving Your Configuration chapter of this guide and also to retrieve errors and warnings within an active configuration for a service.



IMPORTANT: All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the Subscriber Session Trace configuration.

Step 1 Verify that your subscriber session support is configured properly by entering the following command in Exec Mode:

```
show session trace statistics
```

The output of this command displays the statistics of the session trace instance.

```
Num current trace sessions: 5
Total trace sessions activated: 15
Total Number of trace session activation failures: 2
Total Number of trace recording sessions triggered: 15
Total Number of messages traced: 123
Number of current TCE connections: 2
Total number of TCE connections: 3
Total number of files uploaded to all TCEs: 34
```

Step 2 View the session trace references active for various network elements in an EPC network by entering the following command in Exec Mode:

```
show session trace trace-summary
```

The output of this command displays the summary of trace references for all network elements:

```
MME
    Trace Reference: 310012012345
    Trace Reference: 310012012346
SGW
    Trace Reference: 310012012345
```

Trace Reference: 310012012346

PGW

Trace Reference: 310012012347

Appendix A

Sample Configuration Files

This appendix contains sample configuration files for the S-GW. The following configurations are supported:

- [Standalone eGTP Serving Gateway](#)

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

Standalone eGTP Serving Gateway

Configuration Sample

```
# Configuration file for an ASR 5000 in an eGTP S-GW role
#
# Send S-GW licenses
configure /flash/flashconfig/<sgw_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
end
#
```



```
# Modify the local context for local system management
configure
  context local
    interface <name>
      ip address <address> <mask>
    exit
  server ftpd
    exit
  ssh key <key> length <bytes>
  server sshd
    subsystem sftp
    exit
  server telnetd
    exit
  subscriber default
    exit
  administrator <name> encrypted password <password> ftp
  aaa group 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 <lcl_cntxt_intrfc_name> local
  exit
ntp
  enable
  server 10.2.10.2
```

```
    exit

snmp engine-id local <id>

snmp notif-threshold <count> low <low_count> period <seconds>

snmp authentication-failure-trap

snmp heartbeat interval <minutes>

snmp community <string> read-write

snmp target <name> <ip_address>

system contact <string>

system location <string>

# Ingress context configuration

context <sgw_context_name> -noconfirm

    subscriber default

        exit

    interface <s1u-s11_interface_name>

        ip address <ipv4_address_primary>

        ip address <ipv4_address_secondary>

# note alternative IPv6 address:

        ipv6 address <address>

        exit

    gtp group default

        exit

    gtpu-service <gtpu_ingress_service_name>

        bind ipv4-address <s1-us11_interface_ip_address>

# note alternative IPv6 address:

        bind ipv6-address <s1-us11_interface_ip_address>

        exit

    egtp-service <egtp_ingress_service_name>

        interface-type interface-sgw-ingress

        validation-mode default
```

```
    associate gtpu-service <gtpu_ingress_service_name>
    gtpc bind address <slu-s11_interface_ip_address>
    exit

sgw-servers <sgw_service_name> -noconfirm

    associate ingress egtp-service <egtp_ingress_service_name>
    associate egress-proto gtp egress-context <egress_context_name>
    qci-qos-mapping <map_name>
    exit

ip route <pgw_ip_addr/mask> <sgw_next_hop_addr> <sgw_intrfc_name>
exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <slu-s11_interface_name> <sgw_context_name>
    exit

# Egress context configuration
context <egress_context_name> -noconfirm

    interface <s5s8_interface_name>

        ipv6 address <address>

        tunnel-mode ipv6ip

        source interface <name>

        destination address <ipv4_or_ipv6_address>
        exit
    exit

# note alternative IPv4 address:

    ip address <ipv4_address>
    exit

    gtpu-service <gtpu_egress_service_name>

        bind ipv4-address <s5s8_interface_ip_address>

# note alternative IPv6 address:
```

```
    bind ipv6-address <s5s8_interface_ip_address>
    exit

    egtp-service <egtp_egress_service_name>

    interface-type interface-sgw-egress

    validation-mode default

    associate gtpu-service <gtpu_egress_service_name>

    gtpc bind address <s5s8_interface_ip_address>

    exit

    ip route <pgw_ip_addr/mask> <sgw_next_hop_addr> <sgw_intrfc_name>

    exit

    port ethernet <slot_number/port_number>

    no shutdown

    bind interface <s5s8_interface_name> <sgw_context_name>

    exit

# QCI-QoS mapping

qci-qos-mapping <name>

    qci 1 user-datagram dscp-marking <hex>

    qci 3 user-datagram dscp-marking <hex>

    qci 9 user-datagram dscp-marking <hex>

end
```

Appendix B

S-GW Engineering Rules

This appendix provides Serving Gateway-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 Guide* for the specific network type.

The following rules are covered in this appendix:

- [Interface and Port Rules](#)
- [S-GW Service Rules](#)
- [S-GW Subscriber Rules](#)

Interface and Port Rules

The rules discussed in this section pertain to the Ethernet 10/100 line card, the Ethernet 1000 line card and the four-port Quad Gig-E line card and the type of interfaces they facilitate, regardless of the application.

S1-U/S11 Interface Rules

The following engineering rules apply to the S1-U0/S11 interface:

- An S1-U0/S11 interface is created once the IP address of a logical interface is bound to an S-GW service.
- The logical interface(s) that will be used to facilitate the S1-U0/S11 interface(s) must be configured within an “ingress” context.
- S-GW services must be configured within an “ingress” context.
- At least one S-GW service must be bound to each interface, however, multiple S-GW services can be bound to a single interface if secondary addresses are assigned to the interface.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the S1-U0/S11 interface can be limited.

S5/S8 Interface Rules

This section describes the engineering rules for the S5 interface for communications between the Mobility Access Gateway (MAG) service residing on the S-GW and the Local Mobility Anchor (LMA) service residing on the P-GW.

MAG to LMA Rules

The following engineering rules apply to the S5/S8 interface from the MAG service to the LMA service residing on the P-GW:

- An S5/S8 interface is created once the IP address of a logical interface is bound to an MAG service.
- The logical interface(s) that will be used to facilitate the S5/S8 interface(s) must be configured within the egress context.
- MAG services must be configured within the egress context.
- MAG services must be associated with an S-GW service.

- Depending on the services offered to the subscriber, the number of sessions facilitated by the S5/S8 interface can be limited.

S-GW Service Rules

The following engineering rules apply to services configured within the system:

- A maximum of 256 services (regardless of type) can be configured per system.



CAUTION: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

- The system maintains statistics for a maximum of 4096 peer LMAs per MAG service.
- The total number of entries per table and per chassis is limited to 256.
- Even though service names can be identical to those configured in different contexts on the same system, this is not a good practice. Having services with the same name can lead to confusion, difficulty troubleshooting problems, and make it difficult understanding outputs of show commands.

S-GW Subscriber Rules

The following engineering rule applies to subscribers configured within the system:

- A maximum of 2,048 local subscribers can be configured per context.
- Default subscriber templates may be configured on a per S-GW or MAG service.