Oracle® Communications Service Broker

Signaling Server Units Configuration Guide

Release 6.1

E29457-01

February 2013

ORACLE®

Oracle Communications Service Broker Signaling Server Units Configuration Guide, Release 6.1

E29457-01

Contents

4 Configuring a Diameter Signaling Server Unit

5 Configuring a SIP Signaling Server Unit

6 Configuring a RADIUS Signaling Server Unit

7 Configuring a PCP Signaling Server Unit

8 Configuring a ECE Signaling Server Unit

9 Configuring an SMPP Signaling Server Unit

10 Configuring the Web Services Signaling Server Unit

Preface

This document provides reference information on configuring Oracle Communications Service Broker signaling server units (SSUs) using the Administration Console.

Audience

This document is intended for system administrators who are responsible for configuring Service Broker in their network.

This document assumes that the reader is already familiar with:

- Signaling System #7 (SS7) – both SIGTRAN and TDM
- Session Initiation Protocol (SIP)
- Diameter protocol
- RADIUS protocol
- Short Message Peer-to-Peer (SMPP) protocol
- Simple Object Access Protocol (SOAP)
- Representational state transfer (REST) protocol
- Java Management Extensions (JMX)

Related Documents

The following documents provide additional information about Service Broker and relevant standards.

- *Oracle Communications Service Broker Concepts Guide*
- *Oracle Communications Service Broker Installation Guide*
- *Oracle Communications Service Broker Orchestration User's Guide*
- *Oracle Communications Subscriber Store User's Guide*
- *Oracle Communications Service Broker System Administrator's Guide*
- *Oracle Communications Service Broker Modules Configuration Guide*
- *Oracle Communications Service Broker Security Guide*
- (Optional) *Oracle Communications Service Broker Online Mediation Controller Implementation Guide*
- (Optional) *Oracle Communications Service Broker Service Controller Implementation Guide*

- (Optional) *Oracle Communications Service Broker Policy Controller Implementation Guide*
- (Optional) *Oracle Communications Service Broker Online Mediation Controller Protocol Implementation Compliance Statement*

Downloading Oracle Communications Documentation

Oracle Communication Service Broker documentation is available from the Oracle software delivery Web site:

http://edelivery.oracle.com

Additional Oracle Communications documentation is available from Oracle Technology Network:

http://www.oracle.com/technetwork/index.html

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

About Signaling Domain Configuration

This chapter provides an overview of Oracle Communications Service Broker Signaling Domain configuration.

About the Signaling Domain

A Signaling Domain is a set of servers, known as Signaling Servers, on which you install Signaling Server Units (SSUs). Service Broker uses SSUs to communicate with a network.

Service Broker provides different types of SSUs. Each type supports a certain protocol that allows Service Broker to communicate with the following networks:

- SSU for SS7 networks in which traffic is carried out over SIGTRAN M3UA ("Configuring the SS7 Signaling Server Unit for SIGTRAN" for more information on SIGTRAN SSUs configuration)
- SSU for SS7 networks in which traffic is carried out over TDM (see "Configuring the SS7 Signaling Server Unit for TDM" for more information on TDM SSUs configuration)
- SSU for SIP networks (see "Configuring a SIP Signaling Server Unit" for more information on SIP SSU configuration)
- SSU for Diameter networks (see "Configuring a Diameter Signaling Server Unit" for more information on Diameter SSU configuration)
- SSU for RADIUS networks (see "Configuring a RADIUS Signaling Server Unit" for more information on RADIUS SSU configuration)
- SSU for communicating with Short Message System Centers (SMSCs) through the SMPP protocol (see "Configuring an SMPP Signaling Server Unit" for more information)
- SSU for communication with the Oracle Billing and Revenue Management (BRM) application through the Portal Communications Protocol (see "Configuring a PCP Signaling Server Unit" for more information on PCP SSU configuration)
- SSU for communication with the Oracle Elastic Charging Engine (ECE) application through the ECE API (see "Configuring a ECE Signaling Server Unit" for more information on ECE SSU configuration)
- SSU for communication with external entities using SOAP or REST over HTTP (see "Configuring the Web Services Signaling Server Unit" for more information)

Depending on your specific requirements, you can group Signaling Servers into groups and dedicate each server group to a specific type of the SSU. In this case, each group of Signaling Servers provides access to a different network. Alternatively, you

can deploy different SSUs—for example, SIP SSU and Diameter SSU—on Signaling Servers of the same group.

About the Configuration Process

During the configuration process, you define how an SSU handles traffic received from a network and to which interworking modules the SSU forwards this traffic for further processing. In addition, you specify how an SSU sends traffic from interworking modules to a network.

You need to configure each SSU deployed in the domain separately.

You configure SSUs using the Administration Console, which provides a graphical user interface.

Each chapter of this guide is dedicated to a specific type of an SSU.

2

Configuring the SS7 Signaling Server Unit for SIGTRAN

This chapter describes how to configure an Oracle Communications Service Broker SS7 Signaling Server Unit (SSU) in a network in which SS7 traffic is carried over SIGTRAN M3UA.

Accessing the SS7 SSU for SIGTRAN Configuration Pane

To access the SS7 SSU configuration pane:

1. In the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Select **SSU SS7 SIGTRAN**.

The SSU SS7 SIGTRAN configuration pane contains the tabs described in Table 2–1.

> **Note:** You must configure the parameters exactly in the order they are presented in Table 2–1.

Table 2–1 M3UA Configuration Tabs

Tab	Description
SSU SS7 SIGTRAN	Enables you to assign a point code to a Service Broker SSU and define the underlying SS7 stack. See "SSU SS7 SIGTRAN" for more information.
M3UA	Enables you to configure the M3UA layers of the SS7 stack. See "M3UA" for more information.
SCCP	Enables you to configure SCCP addresses: subsystems and global titling. See "SCCP" for more information.
Routing	Enables you to define how the SS7 SSU routes incoming SS7 messages to internal Service Broker IMs. See "Routing" for more information.
Monitoring	Enables you to configure Run-time MBeans and notifications for monitoring SS7 SSU for SIGTRAN. See "Monitoring" for more information.

SSU SS7 SIGTRAN

The SSU SS7 SIGTRAN tab enables you to assign a point code to a Service Broker SSU and configure the M3UA stack run-time options.

To access the SSU SS7 SIGTRAN tab:

- In the SSU SS7 SIGTRAN configuration pane, click the **SSU SS7 SIGTRAN** tab.

  The **General** subtab contains the parameters described in Table 2–2.

Table 2–2 SS7 SSU SIGTRAN Parameters

Name	Type	Description
Vendor	STRING	Specifies the SIGTRAN stack vendor. Possible options: ■ isigtran ■ dialogic
Standard	STRING	Specifies which standard to use to encode M3UA messages. Possible values: ■ ANSI ■ ETSI Default value: ETSI
SS7 Stack IP	INT	The IP address where the SS7 process (that is, the SS7 stack wrapper) is running.
SS7 Stack Port	INT	The port that the SS7 process is using to listen to messages from the SS7 SSU. This is the same port you specify to the SS7 process, in the command line, when you start it. See "Starting and Stopping the SS7 Process" in *Oracle Communications Service Broker System Administrator's Guide*.

Note: After you specified or updated these parameters, you need to restart the managed servers to make the changes to take effect.

M3UA

The M3UA tab enables you to configure the M3UA layers of the SS7 stack.

To access the M3UA tab:

1. In the SSU SS7 configuration pane, click the **M3UA** tab.

   The tab contains the following panes:

   - List of existing managed servers. This pane is located on the left.
   - Subtabs with configuration parameters of the managed server selected in the left of existing managed servers. This pane is located on the right.

2. Do one of the following:

   - To add a new managed server, on the bottom of the list of existing managed servers, click **Add**. Then in the **New** dialog box, enter the name of the managed server and click **Apply**.

- To configure M3UA for an existing managed server, in the list of existing managed servers, select the server for which you want to configure M3UA.

3. Select one of the subtabs described in Table 2–3.

Table 2–3 M3UA Subtabs

Subtab	Description
Local Point Code	Enables you to specify a point code for each SSU instance. See "Local Point Code" for more information.
Connectivity	Enables you to set up an IP connection between the Service Broker SSU instances and an SS7 network. See "Connectivity" for more information.
Network Mapping	Enables you to define SCTP associations and connect SSUs to adjacent signaling points. See "Network Mapping" for more information.
Network Routing	Enables you to configure routes to entities in an SS7 network. See "Network Routing" for more information.

Local Point Code

The Local Point Code subtab enables you to specify a point code of the SSU instance that you selected in the SSU Instance list, as described in Table 2–4.

Table 2–4 Point Code Field

Name	Type	Description
Local Point Code	INT	Specifies a local point code of the SSU instance that you selected in the SSU Instance list. A value of the parameter must be integer.

Note: After you specified or updated this parameter, you need to restart the managed servers to make the changes to take effect.

Connectivity

The Connectivity subtab enables you to set up an IP connection between the Service Broker SSU instances and an SS7 network. You configure SSU instances as local systems and other SS7 network entities that are directly connected to the SSU instance as remote systems.

Table 2–5 describes the subtabs on the SS7 SSU Connectivity subtab.

Table 2–5 SS7 Connectivity Subtab

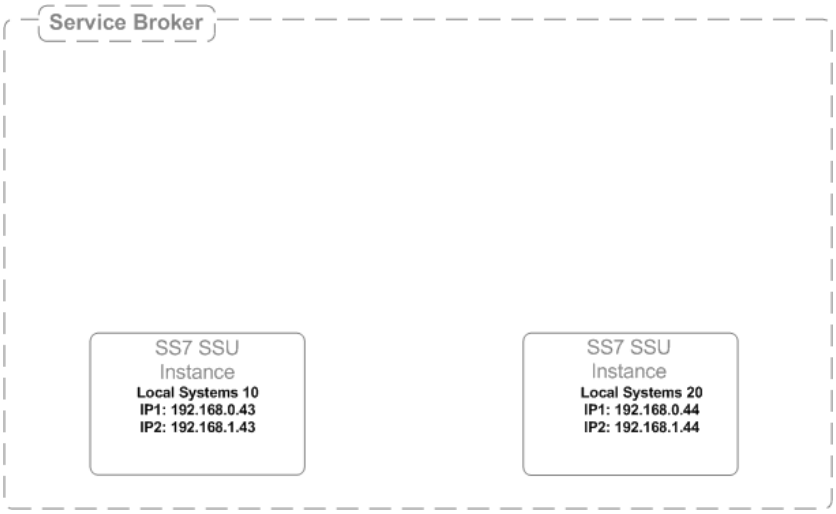
Subtab	Description
Local System	Enables you to configure the SS7 SSU instance as a local M3UA system. See "Configuring the Local System" for more information.
Remote Systems	Enables you to configure network entities. See "Configuring Remote Systems" for more information.

Configuring the Local System

The Local System subtab enables you to configure the SS7 SSU instance as a local M3UA system.

Figure 2–1 shows an example of configuration of the local systems components.

Figure 2–1 Configuration Example: M3UA Local Systems



The Local System subtab contains a table in which you configure one row that defines an SSU instance as a local system. When defining the SSU instance as a local system, you need to specify the fields described in Table 2–6.

Table 2–6 Local Systems Fields

Name	Type	Description
Name	STRING	Specifies a descriptive name for the local system
Routing Context	INT (11)	Specifies a unique identifier that logically identifies a local system when communicating with a traditional SS7 network through a signaling gateway. Routing Context can be set to any value between 0 and 2147483647. Default value: 0.
SS7 Mode	STRING	Specifies an SS7 signaling mode that determines the type of SS7 traffic. Possible options: ■ ITU14: ITU operation with 14 bit Point Code ■ ITU16: ITU operation with 16 bit Point Code ■ ITU24: ITU operation with 24 bit Point Code ■ ANSI: ANSI operation with 24 bit Point Code Default value: ITU14

Table 2–6 (Cont.) Local Systems Fields

Name	Type	Description
Traffic Mode	STRING	Specifies the traffic mode in which SSUs operate. Possible options: ■ Loadshare (LS): SSU shares traffic distribution with any other currently active SSUs. ■ Broadcast (BC): SSU receives the same messages as any other currently active SSUs ■ Override (OR): SSU takes over all traffic in Service Broker (that is, primary/backup operation) overriding any currently active SSUs in Service Broker Default value: Loadshare (LS)
IP Address1	STRING	Specifies an SSU IP. The IP address must have the following format: n.n.n.n. Default value: 0.0.0.0
IP Address2	STRING	Specifies an alternative SSU IP address. This address is used when the address defined in the IP Address1 parameter is unreachable. The IP address must have the following format: n.n.n.n.

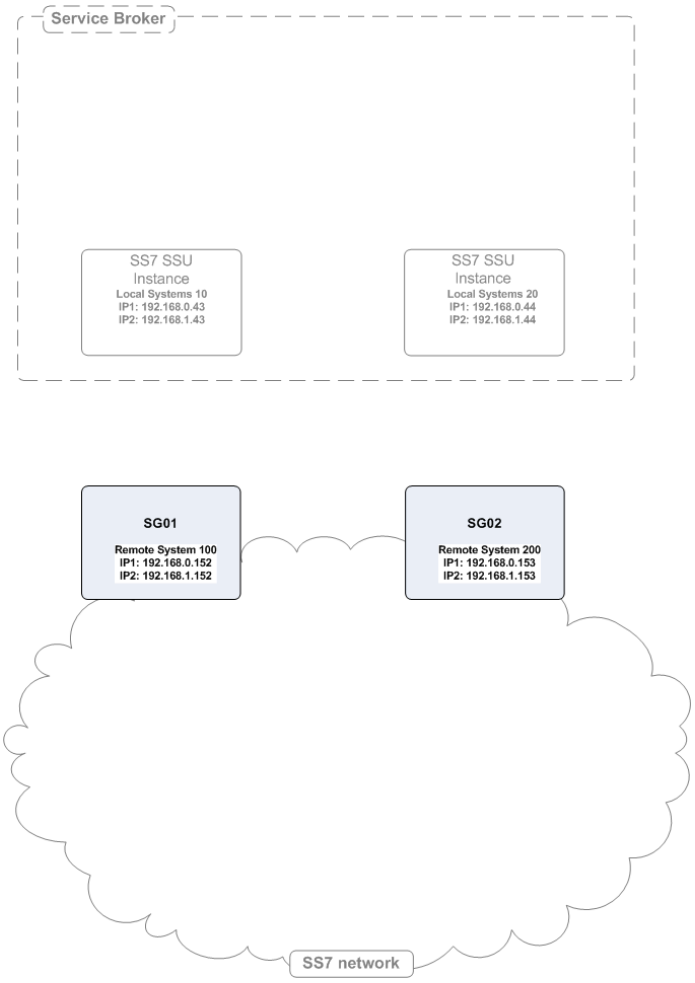
Note: After you specified or updated these parameters, you need to restart the managed servers to make the changes to take effect.

Configuring Remote Systems

The Remote Systems subtab enables you to configure other M3UA network entities to which the SSU instance is directly connected.

Figure 2–2 shows an example of configuration of the remote systems components.

Figure 2–2 Configuration Example: M3UA Remote Systems



The Remote Systems subtab contains a table in which each row represents a single entity that acts as a remote system. When defining a remote system, you need to specify the fields described in Table 2–7.

Table 2–7 Remote Systems Fields

Name	Type	Description
Name	STRING	Specifies a unique name for the Remote System
Type	STRING	Specifies the network entity type. The only available option is SG which stands for Signaling Gateway.
IP Address 1	STRING	Specifies a network entity IP address. The IP address must have the following format: n.n.n.n. Default value: 0.0.0.0.
IP Address 2	STRING	Specifies a network entity alternative IP address. This address is used when the address defined in the IP Address 1 parameter is unreachable. The IP address must have the following format: n.n.n.n.

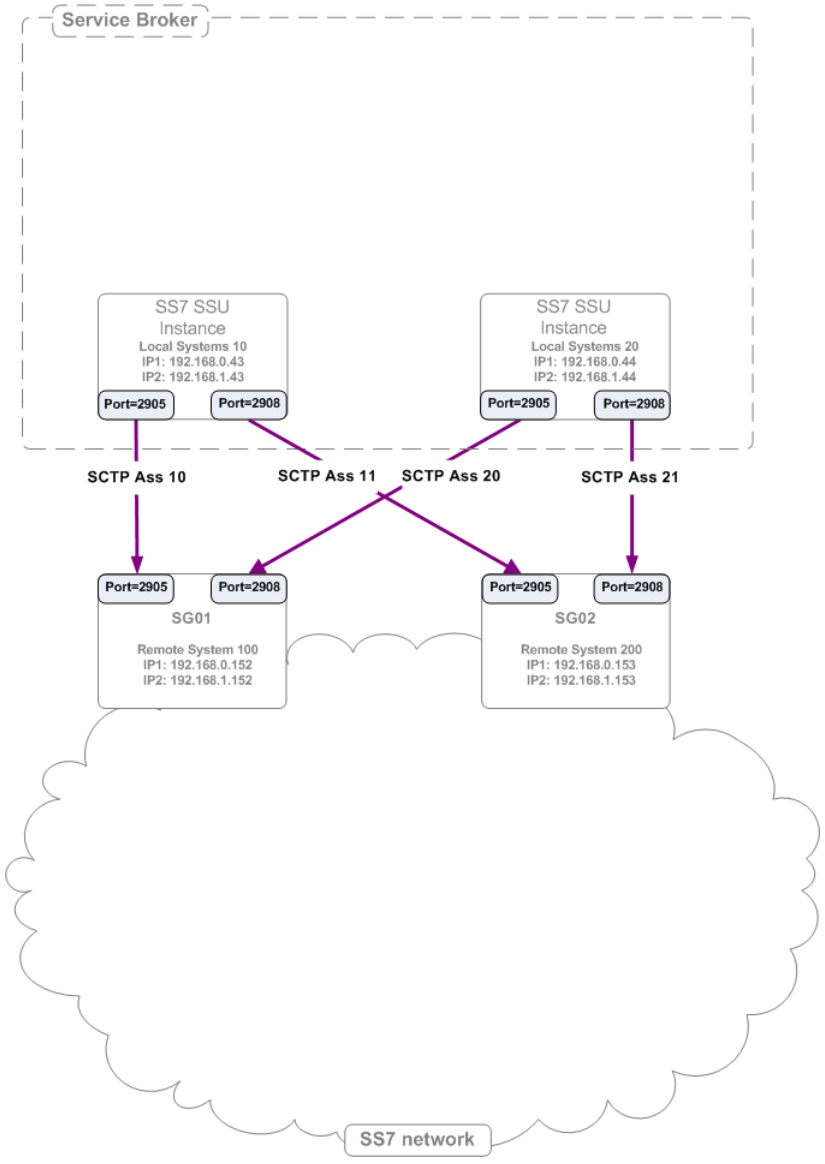
Note: After you specified or updated these parameters, you need to restart the managed servers to make the changes to take effect.

Network Mapping

The Network Mapping subtab enables you to define SCTP associations that connect a local system (an SSU instance) to remote systems.

Figure 2–3 shows an example of configuration of SCTP associations.

Figure 2–3 Configuration Example: M3UA SCTP Associations



The SCTP Associations subtab contains a table in which each row represents a single association. When defining an SCTP association, you need to specify the fields described in Table 2–8.

Table 2–8 SCTP Associations Fields

Name	Type	Description
Name	STRING	Specifies a descriptive name for the SCTP association
Side	STRING	Specifies the mode in which the local side operates. Possible options: ■ Client ■ Server Default value: Client. Setting this parameter requires coordination with the application on the remote side.
Type	STRING	Specifies the SIGTRAN mode. Set this parameter to M3UA.
Local Port	INT	Specifies an SCTP port on the local system side.
Remote Side	STRING	Specifies an entity on the association's network side. Select one of the remote systems that you have previously defined on the Remote Systems subtab in the Connectivity section. See "Configuring Remote Systems" for more information about configuring remote systems.
Remote Port	INT	Specifies an SCTP port on the remote system side

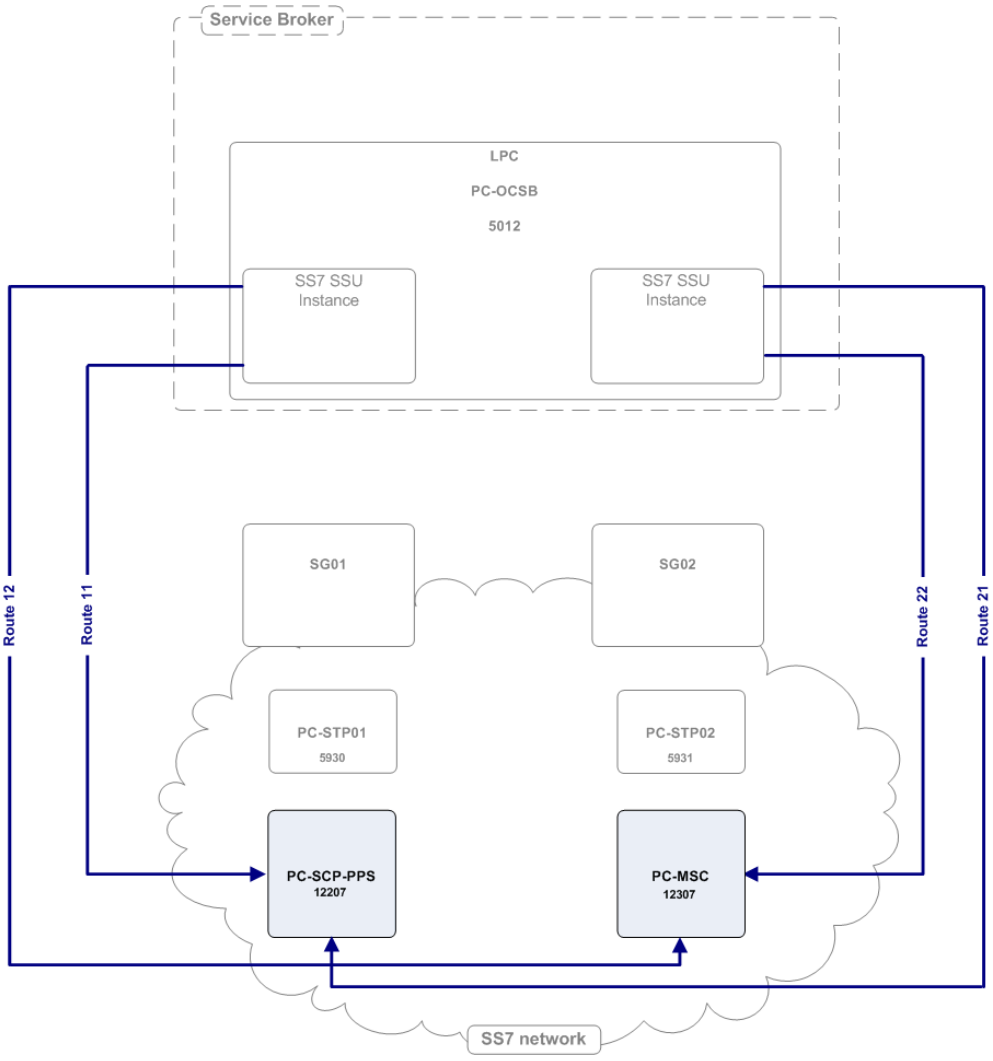
Note: After you specified or updated these parameters, you need to restart the managed servers to make the changes to take effect.

Network Routing

The Network Routing subtab enables you to configure routes to entities in an SS7 network.

Figure 2–4 shows an example of configuration of M3UA routes.

Figure 2–4 Configuration Example: M3UA Routes



The M3UA Routes subtab contains a table in which each row represents a route. When defining a route, you need to specify the fields described in Table 2–9.

Table 2–9 M3UA Routes Fields

Name	Type	Description
Name	STRING	Specifies a descriptive name for the route
Remote Point Code	INT (11)	Specifies an RPC that is available on the far end of the route. You can select one of the RPCs that you have previously defined on the Point Codes subtab in the Network Mapping section.
Primary Remote SIGTRAN System	STRING	Specifies the remote SIGTRAN system through which the SSU instance routes messages to the remote entity. Most likely, this is a Signaling Gateway.
Secondary Remote SIGTRAN System	STRING	Specifies an alternative SIGTRAN system through which the SSU instance routes messages to the remote entity

SCCP

The SCCP tab enables you to configure SCCP addresses for:

- Service Broker modules
- Remote entities in an SS7 network.

To access the SCCP tab:

- In the SS7 SSU SIGTRAN configuration pane, click the SCCP tab.

  The SCCP configuration screen contains the subtabs described in Table 2–10.

Table 2–10 SCCP Section Subtabs

Subtab	Description
General	Enables you to specify parameters, which are common for all SCCP addresses. See "General" for more information.
Local SSNs	Enables you to assign subsystem numbers for Service Broker module instances. See "Local SSNs" for more information.
Local GTs	Enables you to configure Global Title addresses for Service Broker module instances. See "Local GTs" for more information.
Remote PC and SSN Addresses	Enables you to configure addresses of remote entities in the SS7 network that can be reached using a point code and a subsystem number. See "Remote PC and SSN Addresses" for more information.
Remote Fixed GTs	Enables you to configure addresses of remote entities in the SS7 network that can be reached using a fixed Global Title. See "Remote Fixed GTs" for more information.
Remote Dynamic GTs	Enables you to configure addresses of remote entities in the SS7 network that can be reached using a dynamic Global Title. See "Remote Dynamic GTs" for more information.
Global Title Routing	Enables you to configure addresses of network entities that perform Global Title Translation. See "Global Title Routing" for more information.

General

The General subtab enables you to specify parameters, which are common for all SCCP addresses. Table 2–11 describes the parameter on the General subtab that you need to define.

Table 2–11 General Parameter

Name	Type	Description
Local Network Indicator	STRING	Specifies the network type of an SSU address, which is common for all SSU local SCCP addresses. Possible values: ■ International Network ■ International Network Extension ■ National Network ■ National Network Extension Default value: International Network The Local Network Indicator parameter of the M3UA stack is set to the same value as this parameter. However, because International Network Extension and National Network Extension are not supported in the M3UA stack, these two parameters are translated as follows in M3UA: ■ International Network Extension is translated to International Network ■ National Network Extension is translated to National Network
Remove Calling Party Point Code upon GT Routing	BOOL	Specifies whether the local SSU point code is to be added to the calling party address, when routing is done with a Global Title. Possible values: ■ True: the local point code is not added to the calling party address ■ False: the local point code is added to the calling party address
Remove Called Party Point Code upon GT Routing	BOOL	Specifies whether the remote point code is to be removed from the called party address, when routing is done with a Global Title. Possible values: ■ True: the remote point code is not added to the called party address ■ False: the remote point code is added to the called party address

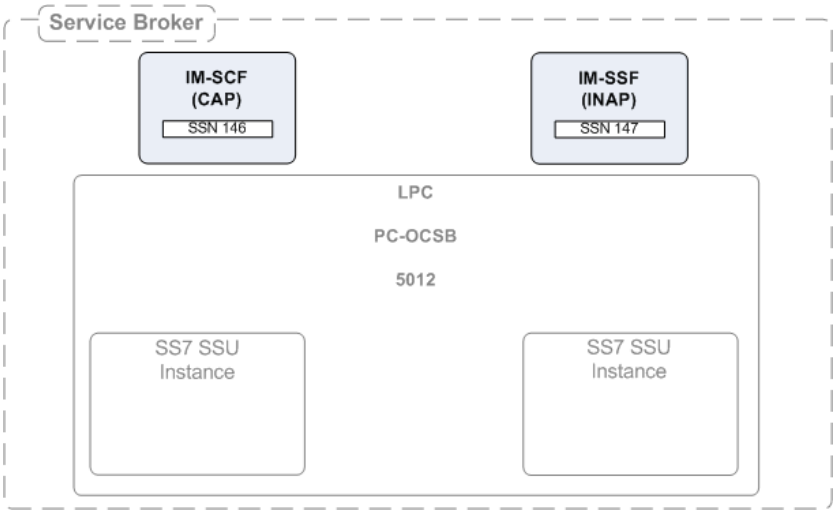
Note: After you specified or updated these parameters, you need to restart the managed servers to make the changes to take effect.

Local SSNs

The Local SSNs subtab enables you to assign Subsystem Numbers (SSNs) for Service Broker module instances. An SSU routes incoming messages to local subsystems based on these SSNs.

Figure 2–5 shows an example of configuration of local SSNs.

Figure 2–5 Configuration Example: Local SSNs



The Local SSNs subtab contains a table in which each row represents a single Service Broker subsystem. When configuring an SSN, you need to specify the fields described in Table 2–12.

Table 2–12 Local SSNs Fields

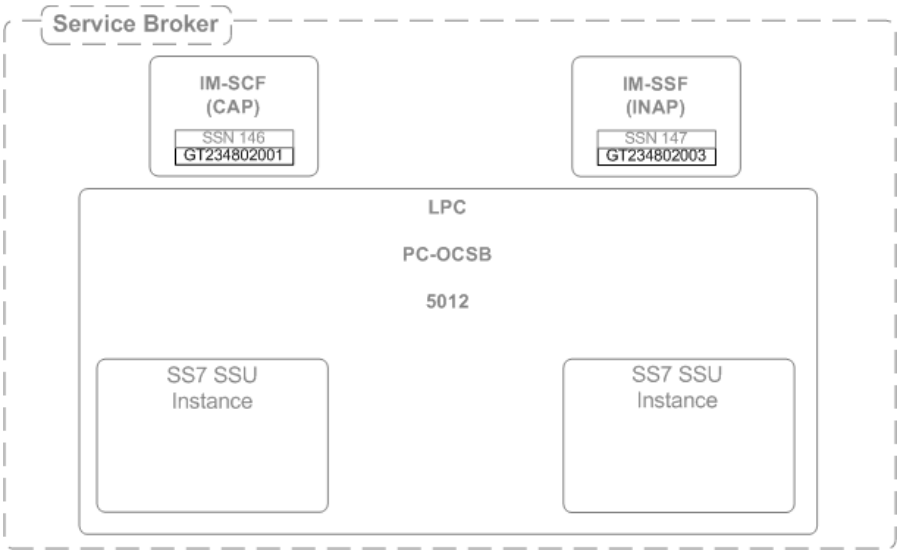
Name	Type	Description
Name	STRING	Specifies the subsystem name
SSN	INT	Specifies the subsystem number. Default value: 0.
Description	STRING	Specifies a subsystem description
Alias	STRING	Specifies an alias name given to a Service Broker subsystem. Applications that use Service Broker to connect to the SS7 network, use this alias to refer the specific subsystem.

Local GTs

The Local GTs subtab enables you to configure Global Title addresses for Service Broker module instances.

Figure 2–6 shows an example of configuration of local GTs.

Figure 2–6 Configuration Example: Local GT



The Local GTs subtab contains a table in which each row represents a single address. When defining an address, you need to specify the fields described in Table 2–13.

Table 2–13 Local GTs Fields

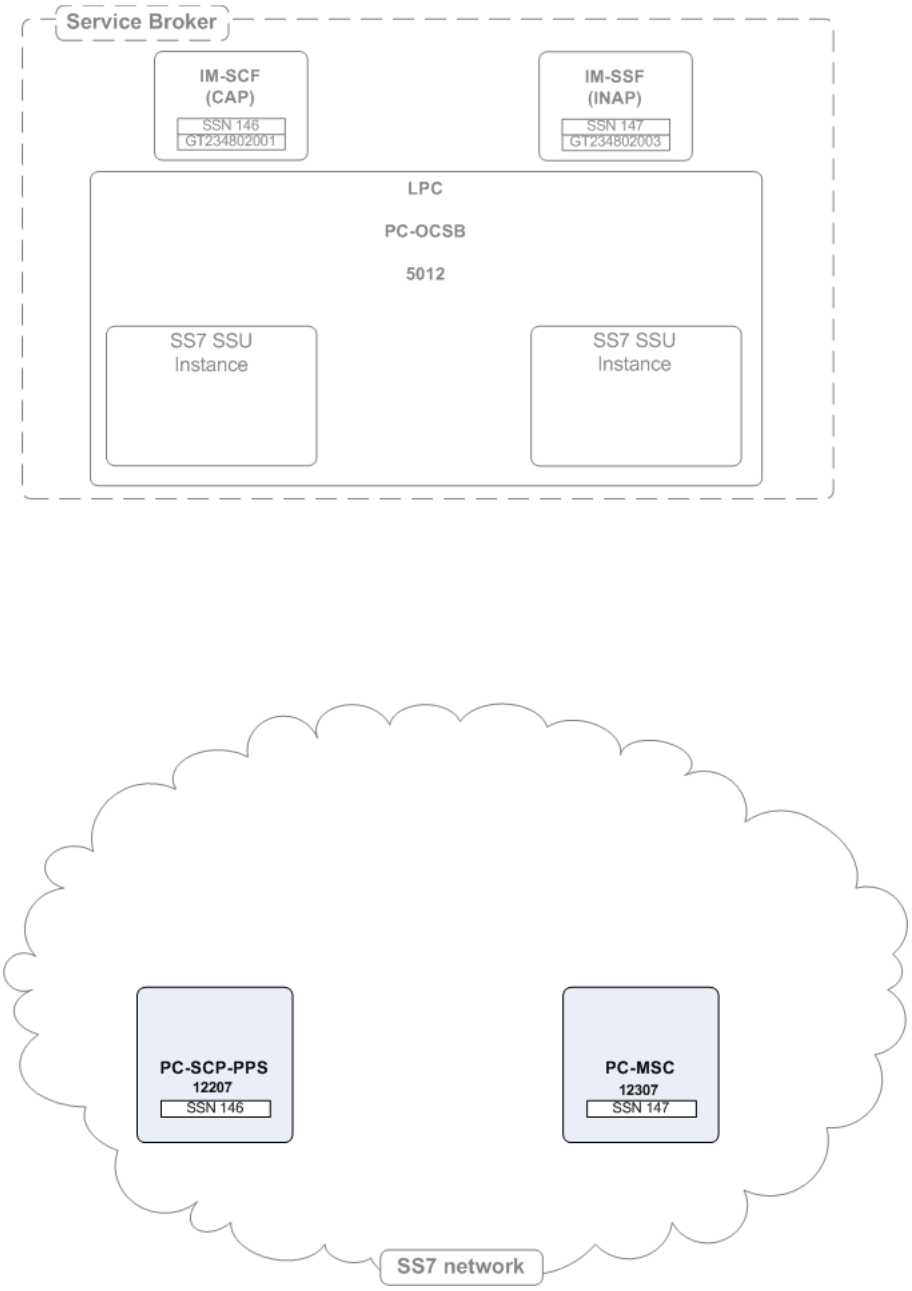
Name	Type	Description
Name	STRING	Specifies a unique name
Description	STRING	Specifies a description for the Service Broker GT address.
GT Address	STRING	Specifies the Global Title Address part of the SCCP address
SSN	INT	Specifies the SSN part of the SCCP address that identifies the user function
GT Indicator	INT	Specifies the Global Title Indicator part of the GT.
GT Nature of Address	INT	Specifies the Nature of Address Indicator part of the GT
GT Numbering Plan	INT	Specifies the Numbering Plan part of the GT
GT Translation Type	INT	Specifies the Translation Type part of the SCCP address
Alias	STRING	Specifies an alias name given to a Service Broker subsystem. Applications that use Service Broker to connect to the SS7 network use this alias to refer the specific GT address.

Remote PC and SSN Addresses

The Remote PC and SSN Addresses subtab enables you to configure addresses of remote entities in the SS7 network that can be reached using a point code and a subsystem number.

Figure 2–7 shows an example of configuration of a remote point code and an SSN.

Figure 2–7 Configuration Example: Remote PC and SSN



The SS7 SSU distributes messages among different SS7 network entities that share the same alias using the weighted load strategy. This strategy determines a network entity that receives a message based on the weight that you assign to the entity. The weight determines a relative share of the traffic that the network entity should receive. For example, you defined two entities whose weight is 100 and 200 correspondingly. The network entity with the weight of 100 receives 1/3 of the traffic, while the network entity with the weight of 200 receives the remaining 2/3 of the traffic.

If a network entity fails, the SS7 SSU redistributes the traffic among remaining networking entities according to their weight.

You can define a network entity that receives traffic if other network entities whose weight is greater than zero, fail. This entity is known as secondary network entity, and

its weight is always zero. If in the example above, you add one more entity whose weight is set to zero, the SS7 SSU sends messages to this network entity only if the network entities whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple network entities with secondary priority, the SS7 SSU distributes traffic equally among them.

The weighted load strategy enables you to control the traffic distribution depending on capabilities of network entities. For example, if a network entity runs a more powerful server, this entity can serve more traffic, then you would set its load weight relatively higher.

The Remote PC and SSN Addresses subtab contains a table in which each row represents a single SS7 network entity. When configuring a network entity, you need to specify the fields described in Table 2–14.

Table 2–14 Remote PC and SSN Fields

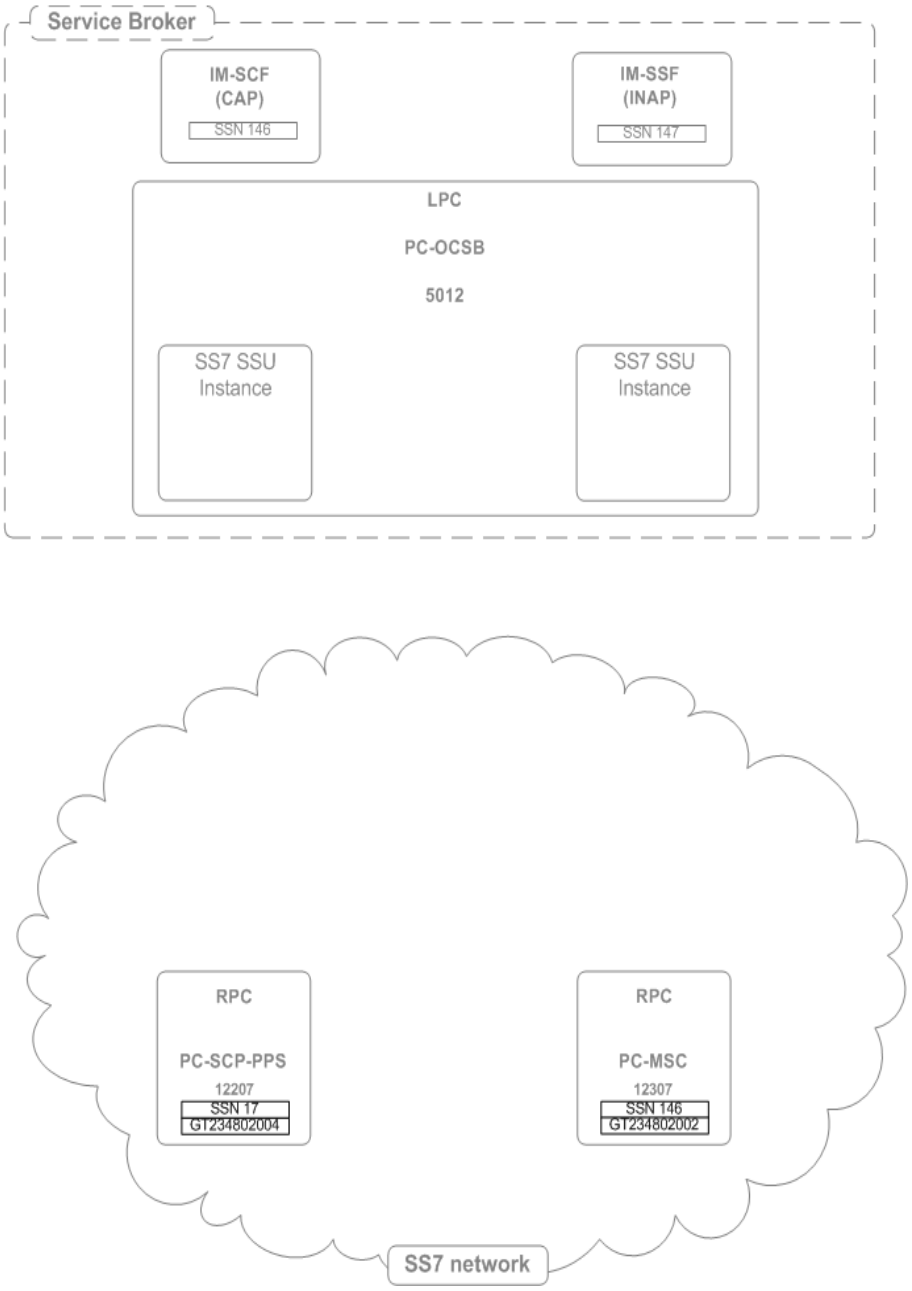
Name	Type	Description
Name	STRING	Specifies a unique name
Network Indicator	STRING	Specifies the network type. Possible values: ■ International Network ■ National Network Default value: International Network
SSN	INT	Specifies the SSN part of the SCCP address that identifies the user function.
Point Code	INT	Specifies the point code part of the SCCP address.
Description	STRING	Specifies a description for the remote SS7 network entity.
Alias	STRING	Specifies an alias name given to a remote network entity. Applications that use Service Broker to connect to the SS7 network use this alias to refer the specific network entity.
Weight	STRING	Specifies the relative load weight for the network entity. Default value: 0

Remote Fixed GTs

The Remote Fixed GTs subtab enables you to configure addresses of remote entities in the SS7 network that can be reached using a fixed Global Title.

Figure 2–8 shows an example of configuration of remote fixed GTs.

Figure 2–8 Configuration Example: Remote Fixed GTs



The SS7 SSU distributes messages among different SS7 network entities that share the same alias using the weighted load strategy. This strategy determines a network entity that receives a message based on the weight that you assign to the entity. The weight determines a relative share of the traffic that the network entity should receive. For example, you defined two entities whose weight is 100 and 200 correspondingly. The network entity with the weight of 100 receives 1/3 of the traffic, while the network entity with the weight of 200 receives the remaining 2/3 of the traffic.

If a network entity fails, the SS7 SSU redistributes the traffic among remaining networking entities according to their weight.

You can define a network entity that receives traffic if other network entities whose weight is greater than zero, fail. This entity is known as secondary network entity, and

its weight is always zero. If in the example above, you add one more entity whose weight is set to zero, the SS7 SSU sends messages to this network entity only if the network entities whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple network entities with secondary priority, the SS7 SSU distributes traffic equally among them.

The weighted load strategy allows you to control the traffic distribution depending on capabilities of network entities. For example, if a network entity runs a more powerful server, this entity can serve more traffic, then you would set its load weight relatively higher.

The Remote Fixed GTs subtab contains a table in which each row represents a single SS7 network entity. When configuring a network entity, you need to specify the fields described in Table 2–15.

Table 2–15 Remote Fixed GTs Fields

Name	Type	Description
Name	STRING	Specifies a unique name
Network Indicator	STRING	Specifies the network type. Possible options: ■ International Network ■ National Network Default option: International Network
Description	STRING	Specifies a description for the network entity and its address
GT Address	STRING	Specifies the Global Title Address part of the SCCP address
Point Code	INT	Optional: specifies the point code part of the SCCP address. When specified, the SSU routes messages to the specified point code, including a GT address.
SSN	INT	Specifies the SSN part of the SCCP address that identifies the user function
GT Indicator	INT	Specifies the Global Title Indicator part of the GT
GT Nature of Address	INT	Specifies the Nature of Address Indicator part of the GT
GT Numbering Plan	INT	Specifies the Numbering Plan part of the GT.
GT Translation Type	INT	Specifies the Translation Type part of the SCCP address
Weight	STRING	Specifies the relative load weight for the network entity. Default value: 0

Remote Dynamic GTs

The Remote Dynamic GTs subtab enables you to configure addresses of remote entities in the SS7 network that can be reached using a dynamic Global Title.

The SS7 SSU distributes messages among different SS7 network entities that share the same alias using the weighted load strategy. This strategy determines a network entity that receives a message based on the weight that you assign to the entity. The weight determines a relative share of the traffic that the network entity should receive. For

example, you defined two entities whose weight is 100 and 200 correspondingly. The network entity with the weight of 100 receives 1/3 of the traffic, while the network entity with the weight of 200 receives the remaining 2/3 of the traffic.

If a network entity fails, the SS7 SSU redistributes the traffic among remaining networking entities according to their weight.

You can define a network entity that receives traffic if other network entities whose weight is greater than zero, fail. This entity is known as secondary network entity, and its weight is always zero. If in the example above, you add one more entity whose weight is set to zero, the SS7 SSU sends messages to this network entity only if the network entities whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple network entities with secondary priority, the SS7 SSU distributes traffic equally among them.

The weighted load strategy enables you to control the traffic distribution depending on capabilities of network entities. For example, if a network entity runs a more powerful server, this entity can serve more traffic, then you would set its load weight relatively higher.

The Remote Dynamic GTs subtab contains a table in which each row represents a single SCCP address. When configuring an SCCP address, you need to specify the fields described in Table 2–16.

Table 2–16 Remote Dynamic GTs Fields

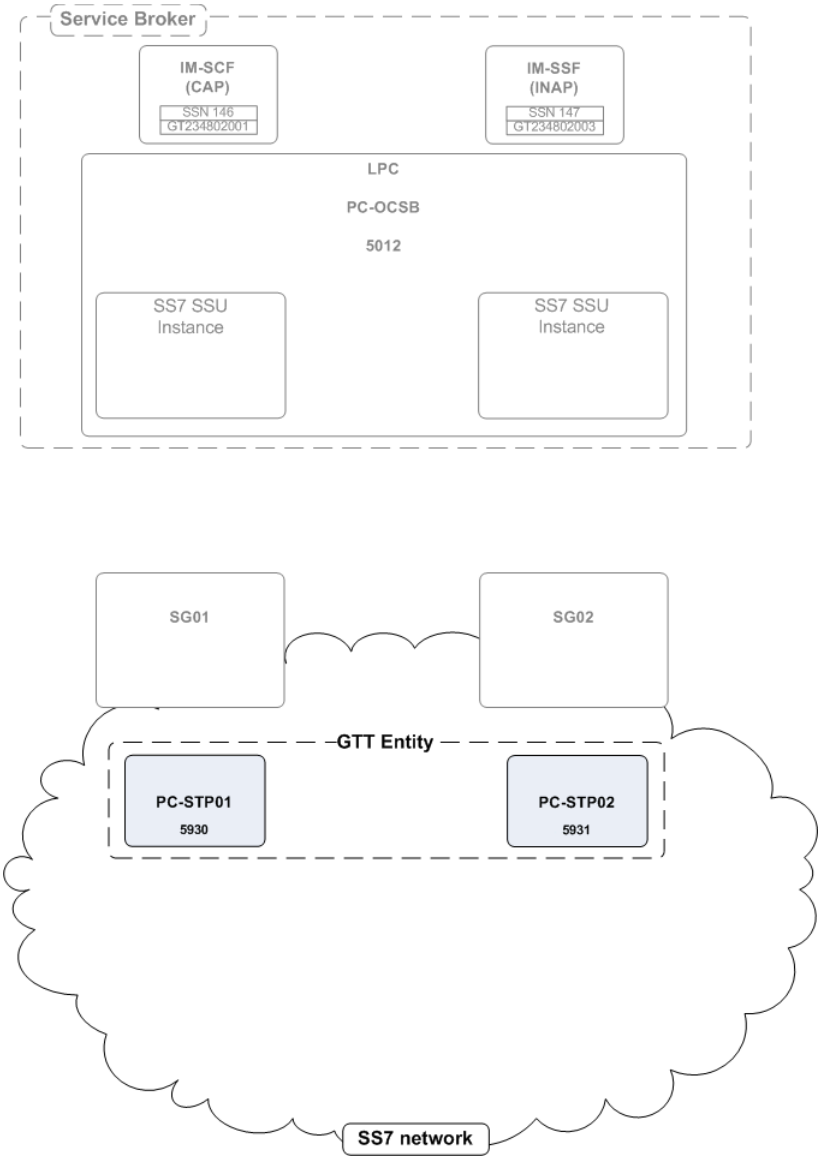
Name	Type	Description
Name	STRING	Specifies a unique name
Network Indicator	STRING	Specifies the network type. The following options are available: ■ International Network ■ National Network Default value: International Network
Description	STRING	Specifies a description for the dynamic GT address
Point Code	INT	Optional: specifies the point code part of the SCCP address. When specified, the SSU routes messages to the specified point code, including a GT address.
SSN	INT	Specifies the SSN part of the SCCP address that identifies the user function
GT Indicator	INT	Specifies the Global Title Indicator part of the GT
GT Nature of Address	INT	Specifies the Nature of Address Indicator part of the GT
GT Numbering Plan	INT	Specifies the Numbering Plan part of the GT.
GT Translation Type	INT	Specifies the Translation Type part of the SCCP address
Alias	STRING	Specifies an alias name given to an SCCP address. Applications that use Service Broker to connect to the SS7 network use this alias when they want route messages using this address.
Weight	STRING	Specifies the relative load weight for the network entity. Default value: 0

Global Title Routing

The Global Title Routing subtab enables you to configure addresses of network entities that perform Global Title Translation. Typically these point codes are Signal Transfer Points (STPs).

Figure 2–9 shows an example of configuration of point codes.

Figure 2–9 Configuration Example: Global Title Routing



The Global Title Routing subtab contains a table in which each row represents a point code that performs GTT. When defining a point code that performs GTT, you need to specify the fields described in Table 2–17.

Table 2–17 Global Title Routing Parameters

Name	Type	Description
Primary GTT Point Code	INT	Specifies a primary remote point code that performs GTT.

Table 2–17 (Cont.) Global Title Routing Parameters

Name	Type	Description
Secondary GTT Point Code	INT	Specifies an alternative remote point code that performs GTT.
Operation Mode	STRING	Specifies the mode in which the primary and secondary remote point codes operate. The following options are available: ■ LOAD_SHARING: the SSU sends messages to both primary and secondary point codes in a load sharing mode. ■ PRIMARY_SECONDARY: the SSU sends messages to the primary point code. If the primary point code is not available, the SSU routes messages to the secondary point code. Default value: PRIMARY_SECONDARY

Routing

The Routing tab enables you to define an IM to which the SS7 SSU routes an incoming session by specifying a set of parameters known as incoming routing rule. For each incoming routing rule, you need to configure the following parameters:

- IM to which the SS7 SSU routes an incoming session
- Criteria that an incoming session must meet to be routed to this IM
- Priority in which the SS7 SSU checks incoming routing rules to evaluate whether an incoming session fits the criteria defined in a rule. The SS7 SSU applies the first found rule which criteria are met by an incoming session.

  For example, if you created multiple rules for the same IM, SS7 SSU begins with the rule that has the highest priority. If an incoming session fits the criteria defined in this rule, the SS7 SSU applies the rule and do not check the rest of the rules. Otherwise, the SS7 SSU checks whether an incoming session fits the criteria of a rule with a lower priority. The SS7 SSU performs this check until the SS7 SSU finds a rule whose criteria are met by an incoming session.

You can define incoming routing rules using the Routing tab. The process of defining an incoming routing rule consists of the following steps:

1. You create a rule and define its name, priority, and an IM for which you create this rule. You perform these actions using the Incoming Routing Rules subtab.
2. You define criteria for each rule that you created on step 1.

Accessing the Routing Tab

The Routing tab enables you to define rules for routing incoming sessions to IMs.

To access the Routing tab:

1. In the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Select **SSU SS7 SIGTRAN**.
4. Click the **Routing** tab.

   This tab contains the following:

- List of existing routing rules. This pane is located on the left.
- Subtabs with configuration parameters of the routing rule selected in the left pane of existing routing rules. This pane is located on the right.

5. Do one of the following:
   - To create a routing rule, on the bottom of the list of existing routing rules, click **Add**. Then in the **New** dialog box, enter the name of the new routing rule and click **Apply**.
   - To configure an existing routing rule, in the list of existing routing rules, select the rule that you want to configure.
6. Select one of the subtabs described in Table 2–18.

Table 2–18 Routing Subtabs

Subtab	Description
Incoming Routing Rules	Enables you to define a name, priority, and an IM for which you create a rule. See "Configuring Incoming Routing Rules Parameters" for more information.
Incoming Routing Criteria	Enables you to define criteria for each routing rule created on the Incoming Routing Rules subtab. See "Configuring Incoming Routing Criteria Parameters" for more information.

Configuring Incoming Routing Rules Parameters

The Incoming Routing Rules subtab enables you to define a name, priority, and an IM for which you create a rule. The Incoming Routing Rules subtab contains a table in which each row represents an individual rule.

When you define a rule, you need to specify the fields defined in Table 2–19.

Table 2–19 Incoming Routing Rule Fields

Name	Type	Description
Name	STRING	Specifies a unique rule name
Priority	INT	Specifies an order in which the SS7 SSU checks routing rules to evaluate if an incoming session fits rule's criteria. The SS7 SSU applies the first found rule which criteria are met by an incoming session. The lower the number, the higher the priority. For example, if you created two rules and set Priority of one rule to" 1" and set Priority of another rule to "2", the SS7 SSU checks the rule with Priority set to "1" first. You can define an incoming routing rule that the SS7 SSU apply if no other rule can be applied by setting the Priority parameter of this rule to the highest number (that is, the number with the lowest priority). There is no need to specify incoming routing criteria for such a rule.

Table 2–19 (Cont.) Incoming Routing Rule Fields

Name	Type	Description
Module Instance	STRING	Specifies a URI of an IM to which the SS7 SSU routes an incoming session. The URI has the following format: *IM-instance-name.IM-type@domain-id* ■ *IM-instance-name*: The IM instance name that you specified when you added this IM in the IM Management Configuration screen. ■ *IM-type*: The type of the IM instance ■ *domain-id*: The name of a Processing Domain or a Processing Domain Group where the relevant IM is deployed. See "Setting Up the Service Broker Domain Name" in the *Oracle Communications Service Broker System Administrator's Guide* for more information on setting up a domain name. To set a Processing Domain, you must specify the name you configured for the domain during its creation. See "Setting a Service Broker Domain Name" in Oracle *Communications Service Broker Modules Configuration Guide* for more information. To set a Processing Domain Group, you must specify the group name. See Managing Processing Domain Groups in *Oracle Communications Service Broker Modules Configuration Guide* for more information about Processing Domain Groups. Example: `imscfcap4_instance.IMSCFCAP4@processing-domain-1`

Note: After you specified or updated these parameters, you need to restart the managed servers to make the changes to take effect.

Configuring Incoming Routing Criteria Parameters

The Incoming Routing Criteria subtab enables you to define criteria for rules that you created on the Incoming Routing Rules subtab. The Incoming Routing Criteria contains a table in which each row represents a routing rule.

When you define criteria, you need to specify the fields defined in Table 2–20.

Table 2–20 Incoming Routing Criteria Fields

Name	Type	Description
Name	STRING	Specifies a unique rule name

Table 2–20 (Cont.) Incoming Routing Criteria Fields

Name	Type	Description
Session Key	STRING	Specifies a parameter inside an SCCP message based on which the SS7 SSU performs routing. The SS7 SSU routes incoming messages to a specified module instance, if the value of this parameter matches the Value field. Possible values: ■ DEST_ADDRESS_ALIAS ■ SOURCE_ADDRESS_ALIAS ■ APPLICATION_CONTEXT ■ SERVICE_KEY ■ OPCODE
Value	STRING	Specifies a value that the Session Key parameter of an SCCP message must match, in order for the rule specified in the list of existing routing rules to apply. You can define one of the following in the Value parameter: ■ Single value ■ Range of dash-separated values ■ Comma-separated values

Note: After you specified or updated these parameters, you need to restart the managed servers to make the changes to take effect.

Monitoring

The Monitoring tab enables you to configure Runtime MBeans and notifications for monitoring SS7 SSU for SIGTRAN. For more information about configuring monitoring, see the discussion on configuring Service Broker monitoring in *Oracle Communications Service Broker System Administrator's Guide*.

3

Configuring the SS7 Signaling Server Unit for TDM

This chapter describes how to configure an Oracle Communications Service Broker SS7 Signaling Server Unit (SSU) in a network in which SS7 traffic is carried over TDM.

Accessing the SS7 SSU TDM Configuration Pane

Because deployment of Service Broker involves configuration of two SSU instances, SS7 equipment connected to both instances must be configured as described in the following sections. The section provides graphical representations of deployment examples.

To access the SSU SS7 TDM configuration pane:

1. In the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Select **SSU SS7 TDM**.

   The SSU SS7 configuration pane contains the subtabs described in Table 3–1.

> **Note:** You must configure the parameters exactly in the same order as they are presented in Table 3–1.

Table 3–1 SSU SS7 TDM Tabs

Tab	Description
SS7 SSU TDM	Enables you to assign a point code to local SSU instances and configure the MTP stack run-time options. See "SSU SS7 TDM" for more information.
MTP3	Enables you to configure the MTP layers of the SS7 stack. See "MTP3" for more information.
SCCP	Enables you to configure SCCP addresses: subsystems and global titling. See "SCCP" for more information.
Routing	Enables you to define how the SS7 SSU routes incoming SS7 messages to internal Service Broker IMs. See "Routing" for more information.

Table 3–1 (Cont.) SSU SS7 TDM Tabs

Tab	Description
Monitoring	Enables you to configure Runtime MBeans and notifications for monitoring SS7 SSU for TDM. See "Monitoring" for more information.

SSU SS7 TDM

The SSU SS7 TDM tab enables you to assign a point code to a Service Broker SSU and configure the MTP stack run-time options.

To access the SSU SS7 TDM tab:

- In the SSU SS7 TDM configuration pane, click the **SSU SS7 TDM** tab.

  The SS7 SSU TDM configuration pane contains the parameters described in Table 3–2.

Table 3–2 SSU SS7 TDM Parameters

Name	Type	Description
Board Type	STRING	Specifies the board density. Possible values: ■ High: High density ■ Low: Low density Default value: High
Vendor	STRING	Specifies an MTP stack vendor. Possible values: ■ isigtran ■ dialogic
Standard	STRING	Specifies the standard that the MTP stack must use. Possible values: ■ ANSI ■ ETSI Default value: ETSI
MTP3RPO	STRING	Specifies the method of handling the Remote Processor Outage (RPO). Possible values: ■ Yes: Upon RPO, put the link in the Out of Service mode and select an alternative link. ■ No: Upon RPO, activate a timer first. Only if the failure remains by the time that the timer expires, move the link to the Out of Service mode and select an alternative link. The messages pulled up during time activation are discarded. Default value: Yes

Table 3–2 (Cont.) SSU SS7 TDM Parameters

Name	Type	Description
Routeset Test	STRING	Specifies whether the MTP RouteSetTest message must be sent when an RPC becomes unavailable. Possible values: ■ Yes – disable RouteSetTest ■ No – enable RouteSetTest Default value: Yes
SS7 Stack IP	INT	The IP address where the SS7 process is running. See "Starting and Stopping the SS7 Process" in *Service Broker System Administrator's Guide*.
SS7 Stack Port	INT	The port that the SS7 process is using to listen to messages from the SS7 SSU. This is the same port you specify to the SS7 process, in the command line, when you start it. See "Starting and Stopping the SS7 Process" in *Service Broker System Administrator's Guide*.

MTP3

The MTP3 tab enables you to configure the MTP layers of the SS7 stack.

To access the MTP3 tab:

1. In the SS7 SSU TDM configuration pane, click the **MTP3** tab.

   The tab contains the following:

   - List of existing managed servers. This pane is located on the left.
   - Subtabs with configuration parameters of the managed server selected in the left of existing managed servers. This pane is located on the right.

2. Do one of the following:

   - To add a new managed server, on the bottom of the list of existing managed servers, click **Add**. Then in the **New** dialog box, enter the name of the managed server and click **Apply**.
   - To configure M3UA for an existing managed server, in the list of existing managed servers, select the server for which you want to configure M3UA.

3. Select one of the subtabs described in Table 3–3.

Table 3–3 MTP Subtabs

Subtab	Description
Local Point Code	Enables you to specify a point code for each SSU instance. For more information, see "Local Point Code".
Connectivity	Enables you to configure boards and PCM interfaces (E1/T1). For more information, see "Connectivity".
Network Mapping	Enables you to configure SS7 Links and Linksets that connect SSU to adjacent signaling points. For more information, see "Network Mapping".

Table 3–3 (Cont.) MTP Subtabs

Subtab	Description
Network Routing	Enables you to configure how an SSU accesses SS7 network entities. For more information, see "Network Routing".

Local Point Code

The Local Point Code subtab enables you to specify a point code of the SSU instance that you selected in the SSU Instance list, as described in Table 3–4.

Table 3–4 Point Code Field

Name	Type	Description
Local Point Code	INT	Specifies a local point code of the SSU instance that you selected in the SSU Instance list. A value of the parameter must be integer.

Connectivity

The Connectivity subtab enables you to configure boards and PCM interfaces (E1/T1).

Table 3–5 describes subtabs in the SSU SS7 Connectivity section.

Table 3–5 SS7 Connectivity Sections

Subtab	Description
Boards	Enables you to configure SS7 boards plugged into the SS7 SSU system. For more information, see "Configuring SS7 Boards".
PCMs	Enables you to configure the PCMs that physically connect the SS7 SSU to the SS7 network. For more information, see "Configuring SS7 PCMs".

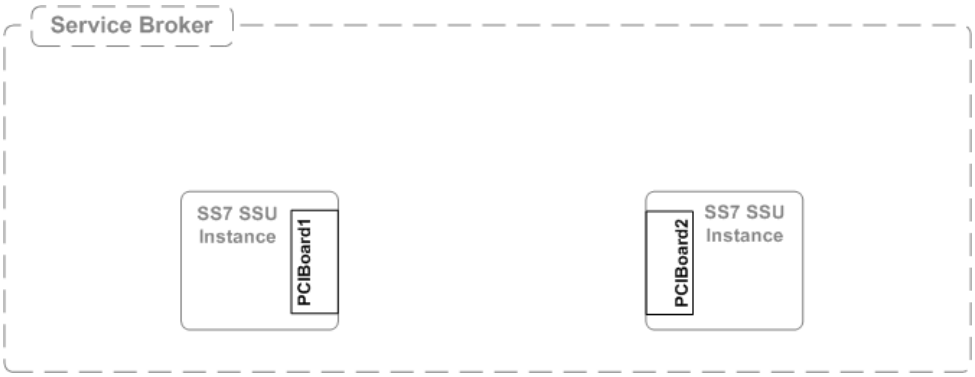
Configuring SS7 Boards

The Boards subtab enables you to configure SS7 boards plugged into the system chassis of the SSU instance.

An SS7 SSU instance can manage several SS7 PCI boards, depending on chassis and driver specifications.

Figure 3–1 shows an example of physical location of PCI boards.

Figure 3–1 Configuration Example: TDM Boards



The Boards subtab contains a table in which each row represents a single board. When defining a board, you need to specify the fields described in Table 3–6.

Table 3–6 SS7 Board Fields

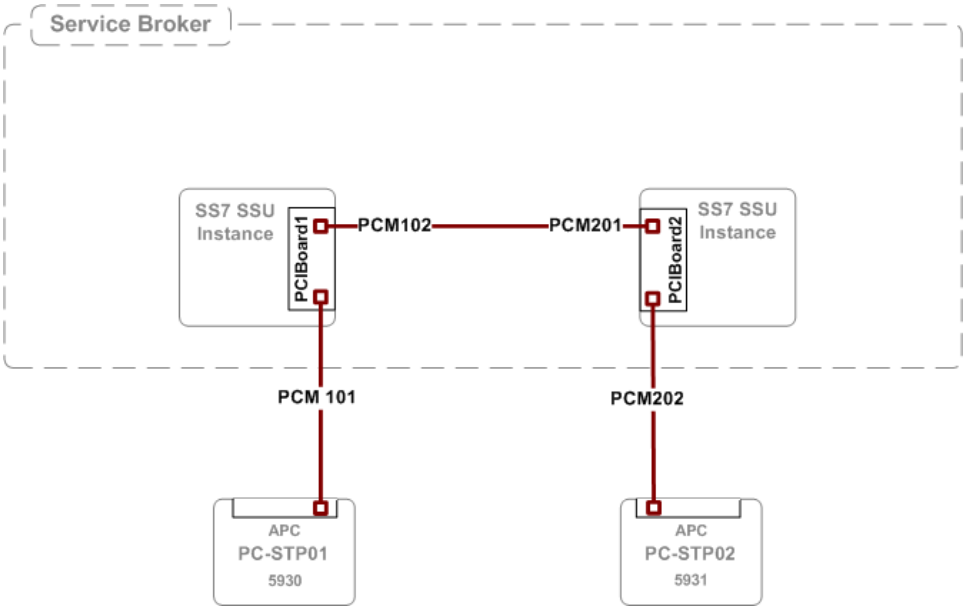
Name	Type	Description
Name	STRING	Specifies a short name for the board.
Slot	INT	Specifies an SSU chassis slot number into which the board is plugged. Default value: 0
Clock	STRING	Specifies how the board is synchronized. Possible options: ■ Master: The board uses an external clock from one of its link interfaces to drive the bus clock for other boards on the bus. ■ Slave: The board uses the bus clocks, which must be generated by another board on the bus. ■ Internal: The board uses the onboard clock oscillator to drive the bus clock for other boards on the bus. Default value: Master

Configuring SS7 PCMs

The SS7 boards are standard PCI boards. The PCMs subtab enables you to define PCMs that physically connect an SSU instance to an SS7 network.

Figure 3–2 shows an example of a physical connection between SSU and an SS7 network.

Figure 3–2 Configuration Example: PCM



The PCMs subtab contains a table in which each row represents one PCM. When defining a PCM, you need to specify the fields described in Table 3–7.

Table 3–7 SS7 PCM Fields

Name	Type	Description
Name	STRING	Specifies a unique PCM name.
Type	STRING	Specifies the type of the PCM hardware. Possible values: ▪ DISABLED ▪ E1-75ohm ▪ E1-120ohm ▪ T1, E1-75/120 ohm Default value: DISABLED
CRC	STRING	Specifies the CRC mode of operation. Possible values: ▪ DISABLED ▪ CRC4 ▪ CRC4 compatibility mode ▪ CRC6 enabled Default value: DISABLED

Table 3–7 (Cont.) SS7 PCM Fields

Name	Type	Description
Code	STRING	Specifies the line encoding format. Possible values: ■ HDB3 (E1 only) ■ AMI with no zero code ■ AMI with zero code (T1 only) ■ B8ZS (T1 only) Default value: HDB3 (E1 only). **Note:** Code must match the Type parameter, for example, if the code/frame value is E1 only, then type should be E1.
Frame	STRING	Specifies the framing format. Possible values: ■ E1 double frame ■ E1 CRC4 multi-frame ■ D3/D4 (T1 only) ■ ESF (T1 only) Default value: E1 double frame. **Note:** Frame must match the Type parameter, for example, if the code/frame value is E1 only, then type should be E1.
Port	INT	Specifies a port number of the SS7 board into which the PCM is plugged. Possible values: ■ 0 ■ 1 ■ 2 ■ 3 Default value: 0

Network Mapping

The Network Mapping subtab enables you to configure SS7 Links and Linksets that connect SSU to adjacent signaling points.

The Network Mapping Configuration screen contains the subtabs described in Table 3–8.

Table 3–8 Network Mapping Section Subtabs

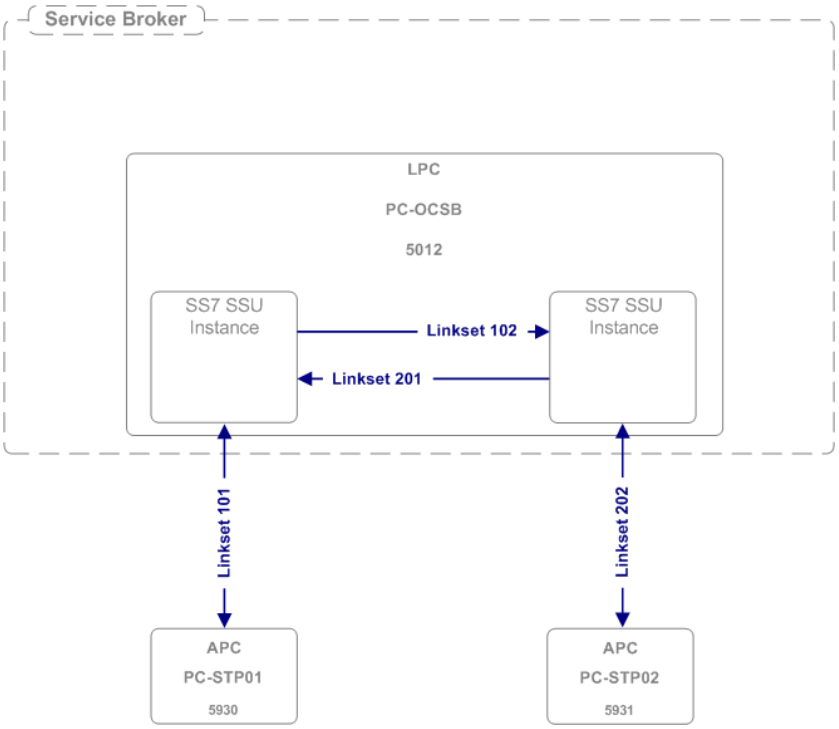
Subtab	Description
MtpLinkset	Enables you to configure MTP Linksets that connect SSU to adjacent signaling points. For more information, see "Configuring MTP Linksets".
MtpLink	Enables you to configure MTP links that connect SSU to adjacent signaling points. For more information, see "Configuring MTP Links".

Configuring MTP Linksets

The MtpLinkset subtab enables you to configure linksets for connecting an SSU to adjacent signaling points in an SS7 network.

Figure 3–3 shows an example of a linkset configuration.

Figure 3–3 Configuration Example: MTP Linkset



The MtpLinkset subtab contains a table in which each row represents one linkset. When defining a linkset, you need to specify the fields described in Table 3–9.

Table 3–9 MtpLinkset Fields

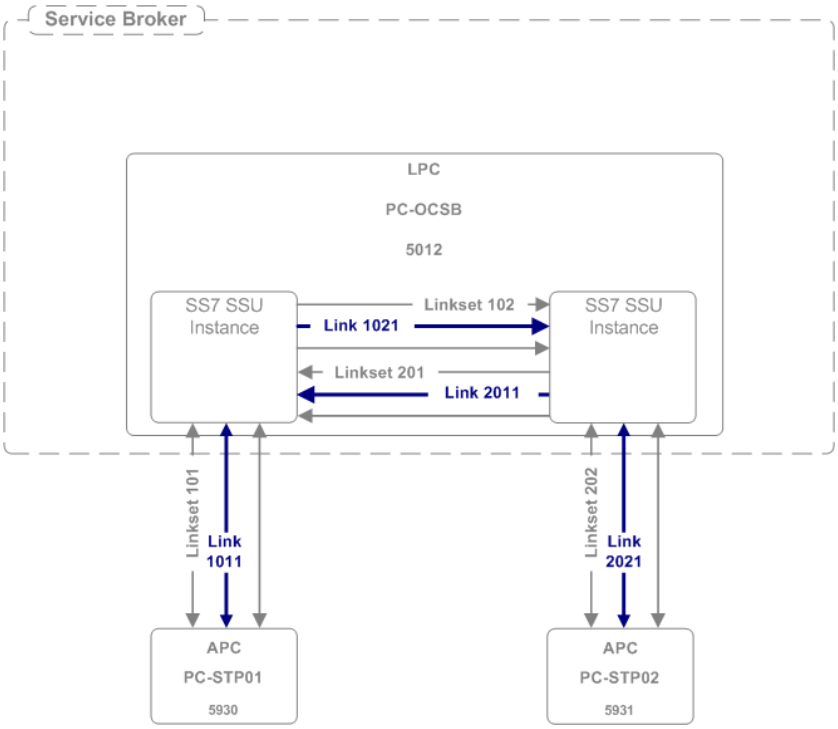
Name	Type	Description
Name	STRING	Specifies a unique linkset name.
Adjacent Point Code	INT	Specifies a point code on the far end of the linkset
Subservice	INT	Specifies a 4-bit value used in the Subservice field of all MTP3 messages that are passed over the linkset. This parameter can be set to any value from 0 to 16. Default value: 1

Configuring MTP Links

The MtpLink subtab enables you to configure links within linksets.

Figure 3–4 shows an example of a links configuration.

Figure 3–4 Configuration Example: MTP Links



The MtpLinks subtab contains a table in which each row represents one link. When defining a link, you need to specify the fields described in Table 3–10.

Table 3–10 MtpLink Fields

Name	Type	Description
Name	STRING	Specifies a unique link name.
PCM	STRING	Specifies a physical PCM cable with which a link is associated. You can select one of the PCMs that you have previously defined on the PCM subtab. (For more information on configuring PCMs, see "Configuring SS7 PCMs".)
Time Slot	STRING	Specifies the PCMs time slot used for a signaling link. The value that you can select depends on the protocol you use: ▪ E1: any value from 1 to 31 ▪ T1: any value from 1 to 24 Default value: 1
Signaling Link Code	INT	Specifies a unique identifier (signaling link code) of the link in the linkset. The value must be unique within the link set. Signaling Link Code can be set to any value from 0 to 15. Default value: 0
Operation Mode	STRING	Specifies the rate on which the link operates. Possible values: ▪ 56 kbits/s ▪ 64 kbits/s Default value: 56 kbits/s

Table 3–10 (Cont.) MtpLink Fields

Name	Type	Description
MTP2ECM	STRING	Specifies the MTP2 error correction mode. Possible values: ■ PCR: Preventive Cyclic Retransmission ■ BMEC: Basic Method of Error Correction Default value: BMEC

Network Routing

The Network Routing subtab enables you to configure how an SSU accesses SS7 network entities.

Table 3–11 describes subtabs in the Network Routing section.

Table 3–11 Network Routing Section Subtabs

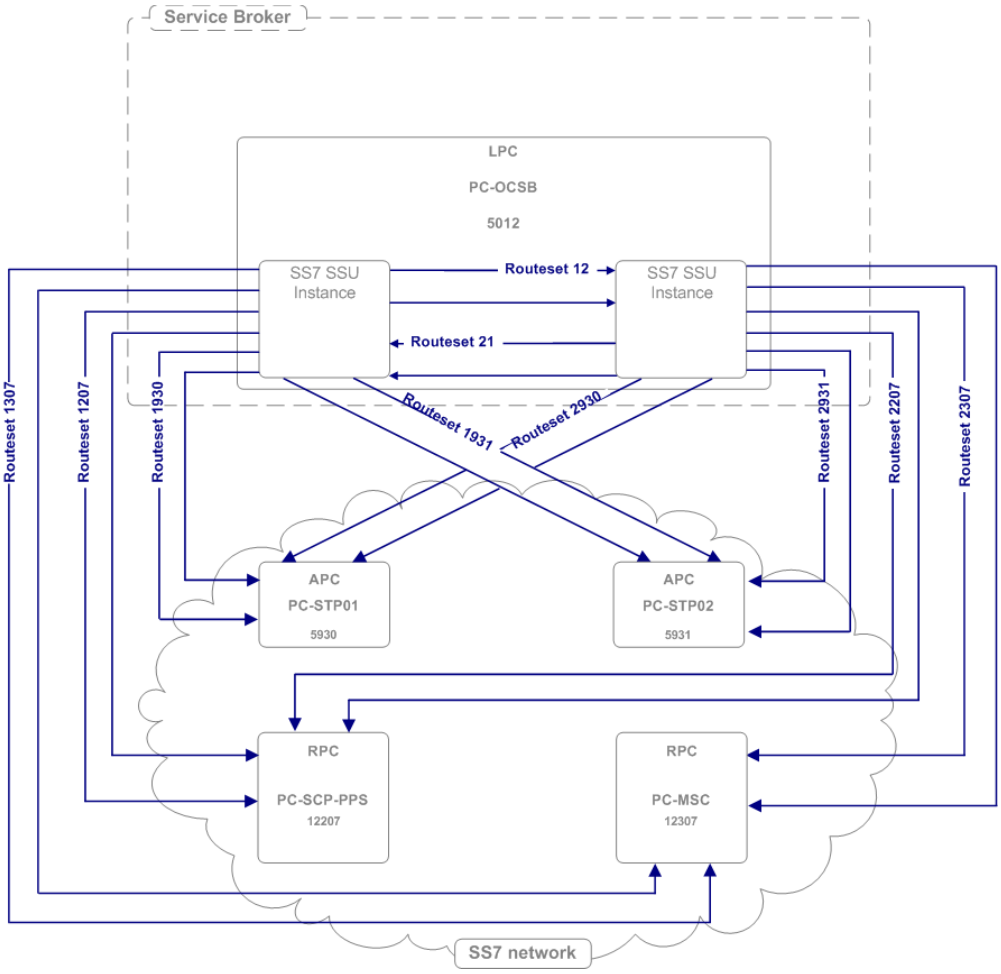
Subtab	Description
Routesets	Enables you to configure how an SSU instance accesses remote point codes in an SS7 network. For more information, see "Configuring Routesets".
Routes	Enables you to define the linkset that must be used to route a message to a remote point code. For more information, see "Configuring Routes".

Configuring Routesets

The Routesets subtab enables you to configure how an SSU instance accesses remote point codes in an SS7 network.

Figure 3–5 shows an example of a routesets configuration.

Figure 3–5 Configuration Example: MTP Routeset



The Routesets subtab contains a table in which each row represents a single routeset. When defining a routeset, you need to specify the fields described in Table 3–12.

Table 3–12 Routesets Fields

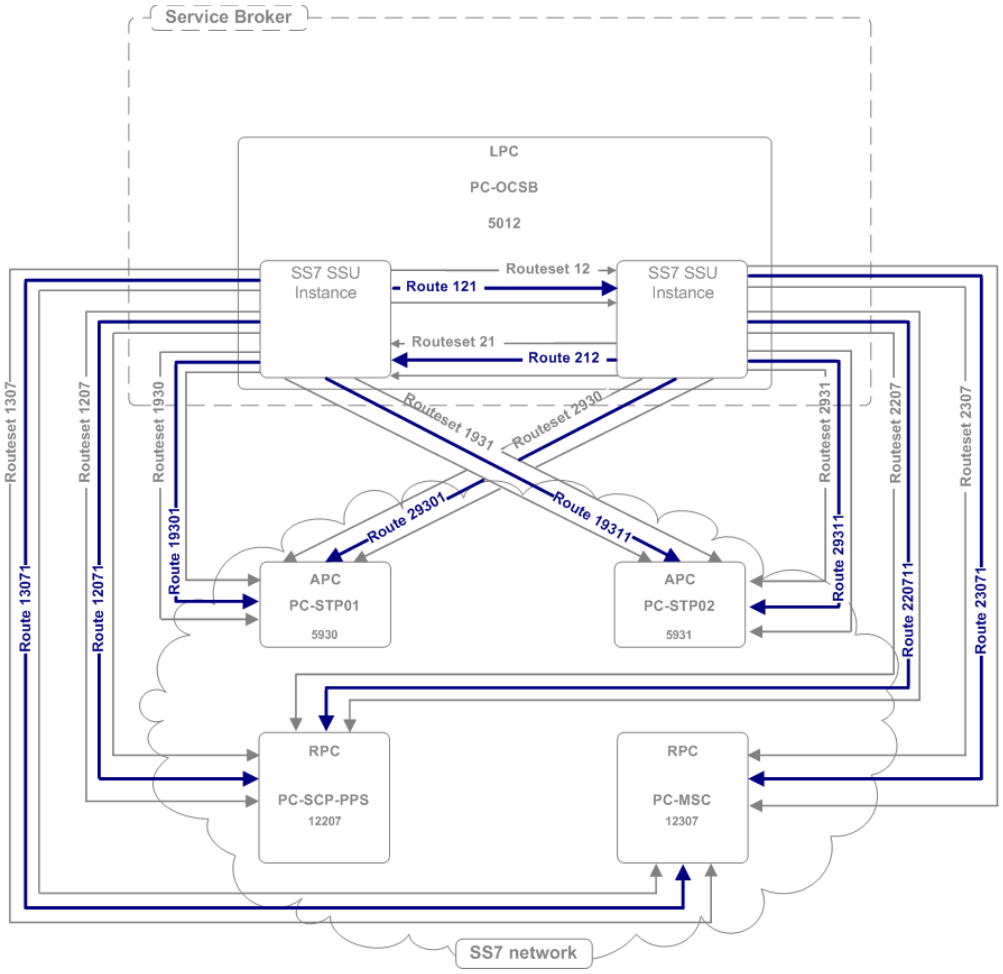
Name	Type	Description
Name	STRING	Specifies a unique routeset name.
Remote Point Code	INT	Specifies a point code or a remote SS7 entity
Default Route	STRING	Possible values: ▪ Yes ▪ No Default value: No
Description	STRING	Specifies a routeset description

Configuring Routes

The Routes subtab enables you to define routes within a routeset.

Figure 3–6 shows an example of a routes configuration.

Figure 3–6 Configuration Example: MTP Routes



The Routes subtab contains a table in which each row represents one route. When defining a route, you need to specify the fields described in Table 3–13.

Table 3–13 Routes Fields

Name	Type	Description
Name	STRING	Specifies a unique route name.
Primary Linkset	INT	Specifies a linkset over which messages are sent to a remote point code. You can select one of the linksets that you have previously defined on the MTP Linksets subtab. (For more information on configuring linksets, see "Configuring MTP Linksets".)
Secondary Linkset	INT	Specifies an alternative linkset over which messages can be sent to a remote point code. You can select one of the linksets that you have previously defined on the MTP Linksets subtab in the Network Mapping section. (For more information on configuring linksets, see "Configuring MTP Linksets".)

Table 3–13 (Cont.) Routes Fields

Name	Type	Description
Type	STRING	Specifies a route type. Possible values: ■ Standalone: An SSU sends messages to the RPC over the linkset specified in the Linkset parameter. The Standalone type cannot have an alternative linkset. ■ Preferred: An SSU sends messages to the RPC over the linkset specified in the Linkset parameter. If the sending messages over this fails, the SSU routes messages to the alternative linkset as defined in the SecondLinkset parameter. The Preferred type must have the Second Linkset defined. ■ Combined: An SSU sends messages to the RPC over both the linkset and alternative linkset as defined in the Linkset and Second Linkset parameters. The Combine type must have Second Linkset defined. Default value: Standalone

SCCP

The SCCP tab enables you to configure SCCP addresses for:

- Service Broker modules
- Remote entities in an SS7 network.

To access the SCCP tab:

- In the SSU SS7 TDM Configuration screen, click the SCCP tab.

  The SCCP configuration pane contains the subtabs described in Table 3–14.

Table 3–14 SCCP Section Subtabs

Subtab	Description
General	Enables you to specify parameters, which are common for all SCCP addresses. For more information, see "General".
Local SSNs	Enables you to assign subsystem numbers for Service Broker module instances. For more information, see "Local SSNs".
Local GTs	Enables you to configure Global Title addresses for Service Broker module instances. For more information, see "Local GTs".
Remote PC and SSN Addresses	Enables you to configure addresses of remote entities in the SS7 network that can be reached using a point code and a subsystem number. For more information, see "Remote PC and SSN Addresses".
Remote Fixed GTs	Enables you to configure addresses of remote entities in the SS7 network that can be reached using a fixed Global Title. For more information, see "Remote Fixed GTs".

Table 3–14 (Cont.) SCCP Section Subtabs

Subtab	Description
Remote Dynamic GTs	Enables you to configure addresses of remote entities in the SS7 network that can be reached using a dynamic Global Title. For more information, see "Remote Dynamic GTs".
Global Title Routing	Enables you to configure addresses of network entities that perform Global Title Translation. For more information, see "Global Title Routing".

General

The General subtab enables you to specify parameters, which are common for all SCCP addresses. Table 3–15 describes the parameters on the General subtab that you need to define.

Table 3–15 General Parameters

Name	Type	Description
Local Network Indicator	STRING	Specifies the network type of an SSU address, which is common for all SSU local SCCP addresses. Possible values: ■ International Network ■ International Network Extension ■ National Network ■ National Network Extension Default value: International Network The Local Network Indicator parameter of the M3UA stack is set to the same value as this parameter. However, because International Network Extension and National Network Extension are not supported in the M3UA stack, these two parameters are translated as follows in M3UA: ■ International Network Extension is translated to International Network ■ National Network Extension is translated to National Network
Remove Calling Party Point Code upon GT Routing	BOOL	Specifies whether the local SSU point code is to be added to the calling party address, when routing is done with a Global Title. Possible values: ■ True: the local point code is not added to the calling party address ■ False: the local point code is added to the calling party address

Table 3–15 (Cont.) General Parameters

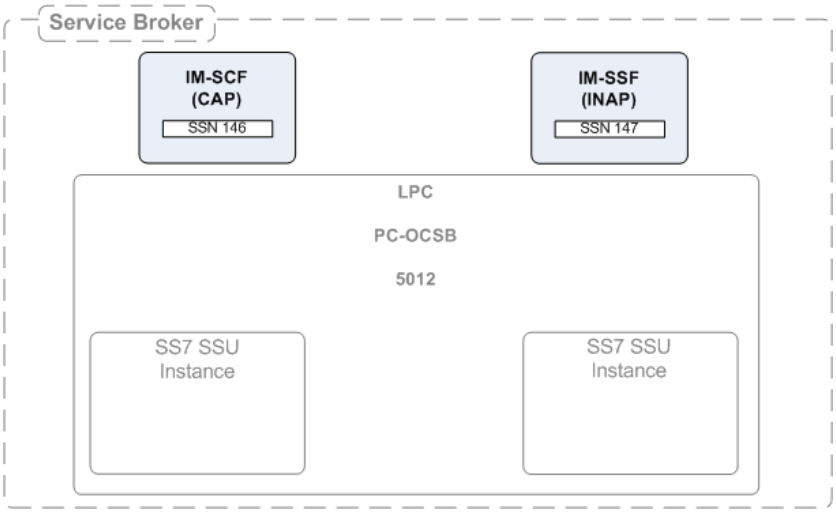
Name	Type	Description
Remove Called Party Point Code upon GT Routing	BOOL	Specifies whether the remote point code is to be removed from the called party address, when routing is done with a Global Title. Possible values: ■ True: the remote point code is not added to the called party address ■ False: the remote point code is added to the called party address

Local SSNs

The Local SSNs subtab enables you to assign Subsystem Numbers (SSNs) for Service Broker module instances. An SSU routes incoming messages to local subsystems based on these SSNs.

Figure 3–7 shows an example of a configuration of local SSNs.

Figure 3–7 Configuration Example: Local SSNs



The Local SSNs subtab contains a table in which each row represents a single Service Broker subsystem. When configuring an SSN, you need to specify the fields described in Table 3–16.

Table 3–16 Local SSNs Fields

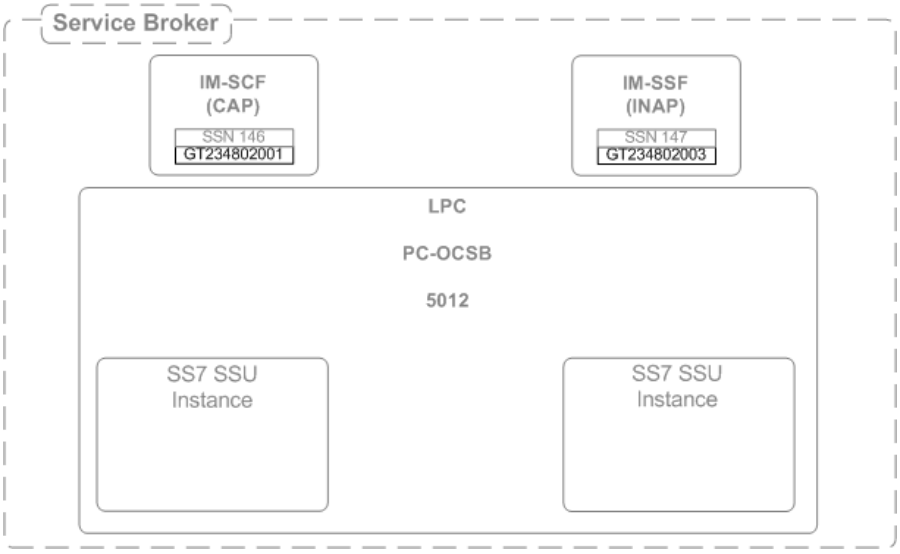
Name	Type	Description
Name	STRING	Specifies the subsystem name
SSN	INT	Specifies the subsystem number. Default value: 0.
Description	STRING	Specifies a subsystem description
Alias	STRING	Specifies an alias name given to a Service Broker subsystem. Applications that use Service Broker to connect to the SS7 network, use this alias to refer the specific subsystem.

Local GTs

The Local GTs subtab enables you to configure Global Title addresses for Service Broker module instances.

Figure 3–8 shows an example of a local GT configuration.

Figure 3–8 Configuration Example: Local GT



The Local GTs subtab contains a table in which each row represents a single address. When defining an address, you need to specify the fields described in Table 3–17.

Table 3–17 Local GTs Fields

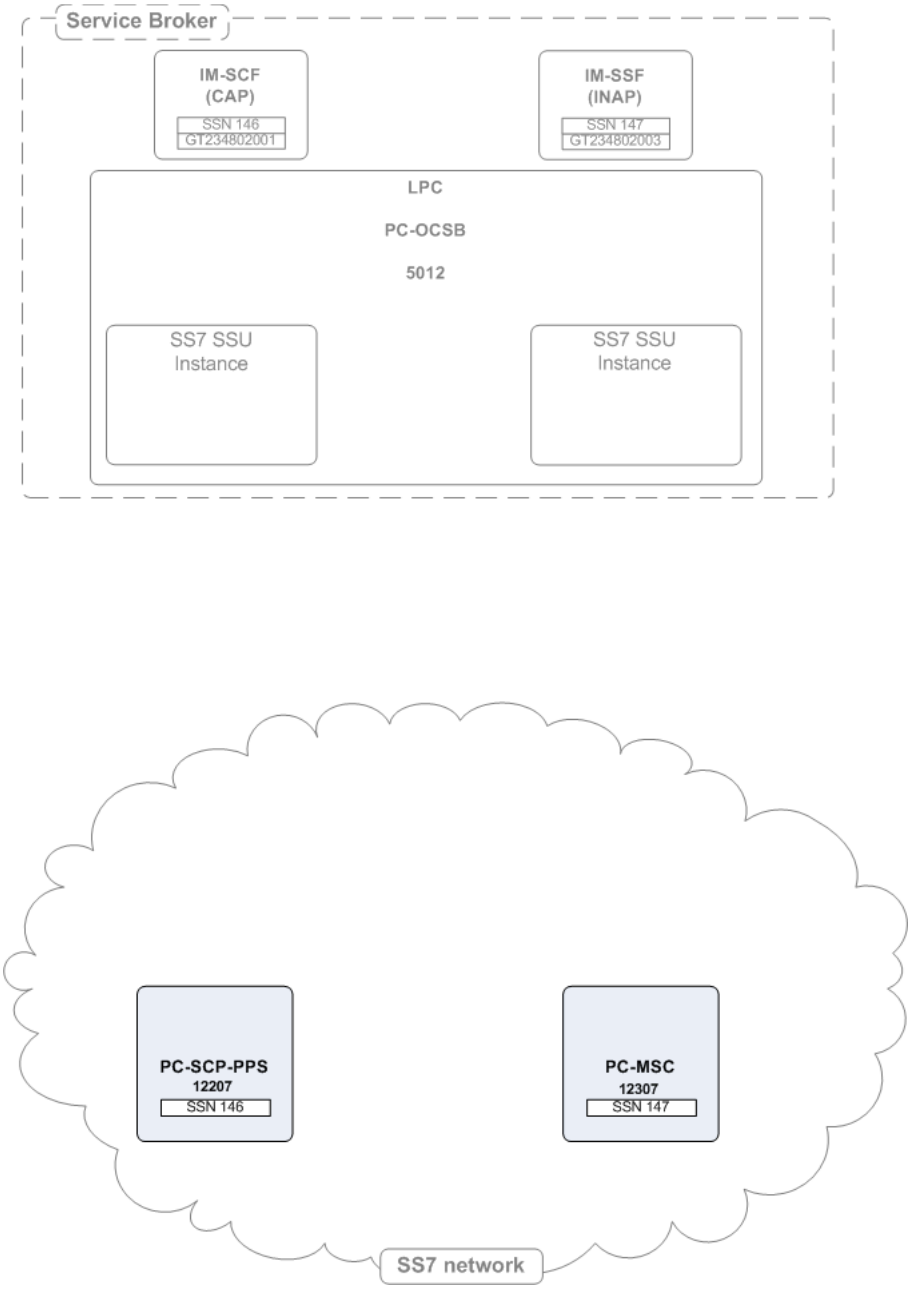
Name	Type	Description
Name	STRING	Specifies a unique name
Description	STRING	Specifies a description for the Service Broker GT address.
GT Address	STRING	Specifies the Global Title Address part of the SCCP address
SSN	INT	Specifies the SSN part of the SCCP address that identifies the user function
GT Indicator	INT	Specifies the Global Title Indicator part of the GT.
GT Nature of Address	INT	Specifies the Nature of Address Indicator part of the GT
GT Numbering Plan	INT	Specifies the Numbering Plan part of the GT
GT Translation Type	INT	Specifies the Translation Type part of the SCCP address
Alias	STRING	Specifies an alias name given to a Service Broker subsystem. Applications that use Service Broker to connect to the SS7 network, use this alias to refer the specific GT address.

Remote PC and SSN Addresses

The Remote PC and SSN Addresses subtab enables you to configure addresses of remote entities in the SS7 network that can be reached using a point code and a subsystem number.

Figure 3–9 shows an example of a remote point code and SSN configuration.

Figure 3–9 Configuration Example: Remote PC and SSN



The SS7 SSU distributes messages among different SS7 network entities that share the same alias using the weighted load strategy. This strategy determines a network entity that receives a message based on the weight that you assign to the entity. The weight determines a relative share of the traffic that the network entity should receive. For example, you defined two entities whose weight is 100 and 200 correspondingly. The

network entity with the weight of 100 receives 1/3 of the traffic, while the network entity with the weight of 200 receives the remaining 2/3 of the traffic.

If a network entity fails, the SS7 SSU redistributes the traffic among remaining networking entities according to their weight.

You can define a network entity that receives traffic if other network entities whose weight is greater than zero, fail. This entity is known as secondary network entity, and its weight is always zero. If in the example above, you add one more entity whose weight is set to zero, the SS7 SSU sends messages to this network entity only if the network entities whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple network entities with secondary priority, the SS7 SSU distributes traffic equally among them.

The weighted load strategy enables you to control the traffic distribution depending on capabilities of network entities. For example, if a network entity runs a more powerful server, this entity can serve more traffic, then you would set its load weight relatively higher.

The Remote PC and SSN Addresses subtab contains a table in which each row represents a single SS7 network entity. When configuring a network entity, you need to specify the fields described in Table 3–18.

Table 3–18 Remote PC and SSN Fields

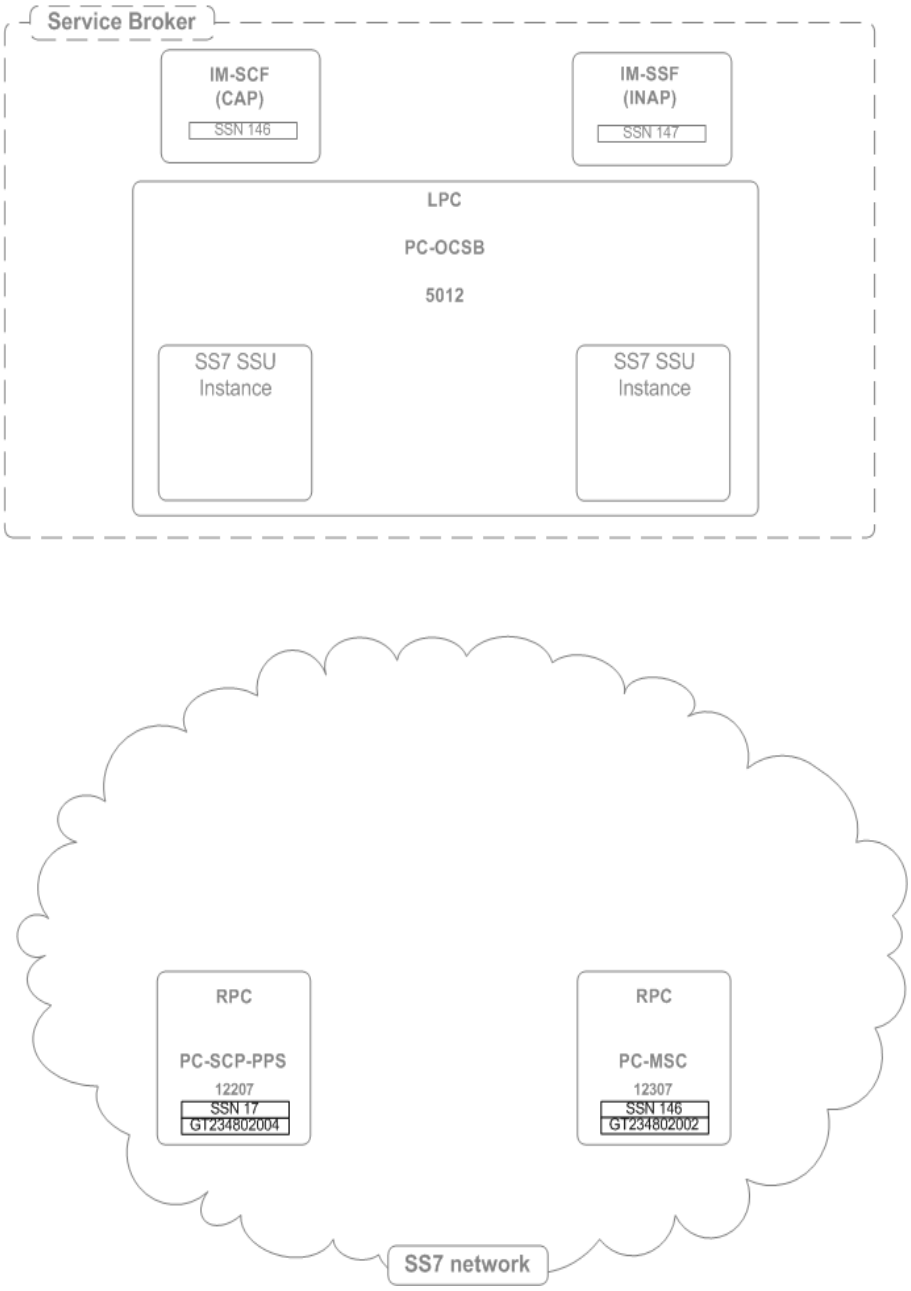
Name	Type	Description
Name	STRING	Specifies a unique name
Network Indicator	STRING	Specifies the network type. Possible values: ■ International Network ■ National Network Default value: International Network
SSN	INT	Specifies the SSN part of the SCCP address that identifies the user function.
Point Code	INT	Specifies the point code part of the SCCP address.
Description	STRING	Specifies a description for the remote SS7 network entity.
Alias	STRING	Specifies an alias name given to a remote network entity. Applications that use Service Broker to connect to the SS7 network, use this alias to refer the specific network entity.
Weight	STRING	Specifies the relative load weight for the network entity. Default value: 0

Remote Fixed GTs

The Remote Fixed GTs subtab enables you to configure addresses of remote entities in the SS7 network that can be reached using a fixed Global Title.

Figure 3–10 shows an example of a remote fixed GTs configuration.

Figure 3–10 Configuration Example: Remote Fixed GTs



The SS7 SSU distributes messages among different SS7 network entities that share the same alias using the weighted load strategy. This strategy determines a network entity that receives a message based on the weight that you assign to the entity. The weight determines a relative share of the traffic that the network entity should receive. For example, you defined two entities whose weight is 100 and 200 correspondingly. The network entity with the weight of 100 receives 1/3 of the traffic, while the network entity with the weight of 200 receives the remaining 2/3 of the traffic.

If a network entity fails, the SS7 SSU redistributes the traffic among remaining networking entities according to their weight.

You can define a network entity that receives traffic if other network entities whose weight is greater than zero, fail. This entity is known as secondary network entity, and

its weight is always zero. If in the example above, you add one more entity whose weight is set to zero, the SS7 SSU sends messages to this network entity only if the network entities whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple network entities with secondary priority, the SS7 SSU distributes traffic equally among them.

The weighted load strategy enables you to control the traffic distribution depending on capabilities of network entities. For example, if a network entity runs a more powerful server, this entity can serve more traffic, then you would set its load weight relatively higher.

The Remote Fixed GTs subtab contains a table in which each row represents a single SS7 network entity. When configuring a network entity, you need to specify the fields described in Table 3–19.

Table 3–19 Remote Fixed GTs Fields

Name	Type	Description
Name	STRING	Specifies a unique name
Network Indicator	STRING	Specifies the network type. Possible options: ■ International Network ■ National Network Default option: International Network
Description	STRING	Specifies a description for the network entity and its address
GT Address	STRING	Specifies the Global Title Address part of the SCCP address
Point Code	INT	Optional: specifies the point code part of the SCCP address. When specified, the SSU routes messages to the specified point code, including a GT address.
SSN	INT	Specifies the SSN part of the SCCP address that identifies the user function
GT Indicator	INT	Specifies the Global Title Indicator part of the GT
GT Nature of Address	INT	Specifies the Nature of Address Indicator part of the GT
GT Numbering Plan	INT	Specifies the Numbering Plan part of the GT.
GT Translation Type	INT	Specifies the Translation Type part of the SCCP address
Alias	STRING	Specifies an alias name given to a remote network entity. Applications that use Service Broker to connect to the SS7 network, use this alias to refer the specific network entity.
Weight	STRING	Specifies the relative load weight for the network entity. Default value: 0

Remote Dynamic GTs

The Remote Dynamic GTs subtab enables you to configure addresses of remote entities in the SS7 network that can be reached using a dynamic Global Title.

The SS7 SSU distributes messages among different SS7 network entities that share the same alias using the weighted load strategy. This strategy determines a network entity that receives a message based on the weight that you assign to the entity. The weight determines a relative share of the traffic that the network entity should receive. For example, you defined two entities whose weight is 100 and 200 correspondingly. The network entity with the weight of 100 receives 1/3 of the traffic, while the network entity with the weight of 200 receives the remaining 2/3 of the traffic.

If a network entity fails, the SS7 SSU redistributes the traffic among remaining networking entities according to their weight.

You can define a network entity that receives traffic if other network entities whose weight is greater than zero, fail. This entity is known as secondary network entity, and its weight is always zero. If in the example above, you add one more entity whose weight is set to zero, the SS7 SSU sends messages to this network entity only if the network entities whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple network entities with secondary priority, the SS7 SSU distributes traffic equally among them.

The weighted load strategy enables you to control the traffic distribution depending on capabilities of network entities. For example, if a network entity runs a more powerful server, this entity can serve more traffic, then you would set its load weight relatively higher.

The Remote Dynamic GTs subtab contains a table in which each row represents a single SCCP address. When configuring an SCCP address, you need to specify the fields described in Table 3–20.

Table 3–20 Remote Dynamic GTs Fields

Name	Type	Description
Name	STRING	Specifies a unique name
Network Indicator	STRING	Specifies the network type. The following options are available: ■ International Network ■ National Network Default value: International Network
Description	STRING	Specifies a description for the dynamic GT address
Point Code	INT	Optional: specifies the point code part of the SCCP address. When specified, the SSU routes messages to the specified point code, including a GT address.
SSN	INT	Specifies the SSN part of the SCCP address that identifies the user function
GT Indicator	INT	Specifies the Global Title Indicator part of the GT
GT Nature of Address	INT	Specifies the Nature of Address Indicator part of the GT
GT Numbering Plan	INT	Specifies the Numbering Plan part of the GT.
GT Translation Type	INT	Specifies the Translation Type part of the SCCP address
Alias	STRING	Specifies an alias name given to an SCCP address. Applications that use Service Broker to connect to the SS7 network, use this alias when they want route messages using this address.

Table 3–20 (Cont.) Remote Dynamic GTs Fields

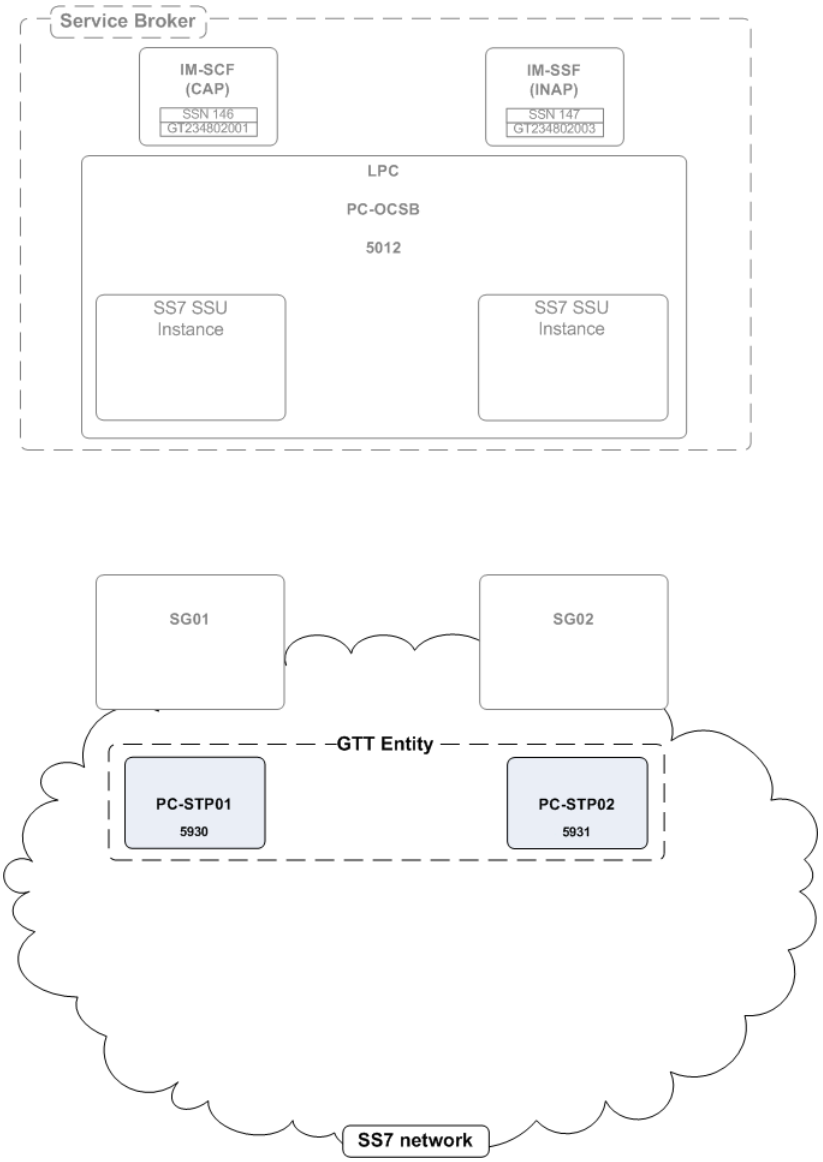
Name	Type	Description
Weight	STRING	Specifies the relative load weight for the network entity. Default value: 0

Global Title Routing

The Global Title Routing subtab enables you to configure addresses of network entities that perform Global Title Translation. Typically these point codes are Signal Transfer Points (STPs).

Figure 3–11 shows an example of a point code configuration.

Figure 3–11 Configuration Example: Global Title Routing



The Global Title Routing subtab contains a table in which each row represents a point code that performs GTT. When defining a point code that performs GTT, you need to specify the fields described in Table 3–21.

Table 3–21 Global Title Routing Parameters

Name	Type	Description
Primary GTT Point Code	INT	Specifies a primary remote point code that performs GTT.
Secondary GTT Point Code	INT	Specifies an alternative remote point code that performs GTT.
Operation Mode	STRING	Specifies the mode in which the primary and secondary remote point codes operate. The following options are available: ■ LOAD_SHARING: the SSU sends messages to both primary and secondary point codes in a load sharing mode. ■ PRIMARY_SECONDARY: the SSU sends messages to the primary point code. If the primary point code is not available, the SSU routes messages to the secondary point code. Default value: PRIMARY_SECONDARY

Routing

The Routing tab enables you to define an IM to which SS7 SSU routes an incoming session by specifying a set of parameters known as incoming routing rules. For each incoming routing rule, you need to configure the following parameters:

- IM to which SS7 SSU routes an incoming session
- Criteria that an incoming session must meet to be routed to this IM
- Priority in which SS7 SSU checks incoming routing rules to evaluate whether an incoming session fits the criteria defined in a rule. SS7 SSU applies the first found rule which criteria are met by an incoming session.

  For example, if you created multiple rules for the same IM, SS7 SSU begins with the rule that has the highest priority. If an incoming session fits the criteria defined in this rule, SS7 SSU applies the rule and do not check the rest of the rules. Otherwise, SS7 SSU checks whether an incoming session fits the criteria of a rule with a lower priority. SS7 SSU performs this check until SS7 SSU finds a rule whose criteria are met by an incoming session.

You can define incoming routing rules using the Routing tab. The process of defining an incoming routing rule consists of the following steps:

1. You create a rule and define its name, priority, and the IM for which you are creating the rule. You perform these actions using the Incoming Routing Rules subtab.
2. You define criteria for each rule that you created in step 1.

Accessing the Routing Tab

The Routing tab enables you to define rules for routing incoming sessions to IMs.

To access the Routing tab:

1. In the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Select **SSU SS7 TDM**.
4. In the configuration pane, click the **Routing** tab.

   The tab contains the following:

   - List of existing routing rules. This pane is located on the left.
   - Subtabs with configuration parameters of the routing rule selected in the left pane of existing routing rules. This pane is located on the right.
5. Do one of the following:
   - To create a new routing rule, on the bottom of the list of existing routing rules, click **Add**. Then in the **New** dialog box, enter the name of the new routing rule and click **Apply**.
   - To configure an existing routing rule, in the list of existing routing rules, select the rule that you want to configure.
6. Select one of the subtabs described in Table 3–22.

Table 3–22 Routing Subtabs

Subtab	Description
Incoming Routing Rules	Enables you to define a name, priority, and an IM for which you create a rule. For more information, see "Configuring Incoming Routing Rules Parameters".
Incoming Routing Criteria	Enables you to define criteria for each routing rule created on the Incoming Routing Rules subtab. For more information, see "Configuring Incoming Routing Criteria Parameters".

Configuring Incoming Routing Rules Parameters

The Incoming Routing Rules subtab enables you to define a name, priority, and an IM for which you create a rule. The Incoming Routing Rules subtab contains a table in which each row represents an individual rule.

When you define a rule, you need to specify the fields defined in Table 3–23.

Table 3–23 Incoming Routing Rule Fields

Name	Type	Description
Name	STRING	Specifies a unique rule name

Table 3–23 (Cont.) Incoming Routing Rule Fields

Name	Type	Description
Priority	INT	Specifies an order in which SS7 SSU checks routing rules to evaluate if an incoming session fits rule's criteria. SS7 SSU applies the first found rule which criteria are met by an incoming session. The lower the number, the higher the priority. For example, if you created two rules and set Priority of one rule to" 1" and set Priority of another rule to "2", SS7 SSU checks the rule with Priority set to "1" first. You can define an incoming routing rule that SS7 SSU applies if no other rule can be applied, by setting the Priority parameter of this rule to the largest number (that is lowest priority). There is no need to specify incoming routing criteria for such a rule.
Module Instance	STRING	Specifies the URI of an IM to which the SS7 SSU routes an incoming session. The URI has the following format: *IM-instance-name.IM-type@domain-id* ■ *IM-instance-name*: The IM instance name that you specified when you added this IM in the IM Management Configuration screen. ■ *IM-type*: The type of the IM instance ■ *domain-id*: The name of a Processing Domain or a Processing Domain Group where the relevant IM is deployed. Example: `imscfcap4_instance.IMSCFCAP4@processing-domain-1`

Configuring Incoming Routing Criteria Parameters

The Incoming Routing Criteria subtab enables you to define criteria for rules that you created on the Incoming Routing Rules subtab. The Incoming Routing Criteria contains a table in which each row represents a routing rule.

When you define criteria, you need to specify the fields defined in Table 3–24.

Table 3–24 Incoming Routing Criteria Fields

Name	Type	Description
Name	STRING	Specifies a unique rule name
Session Key	STRING	Specifies a parameter inside an SCCP message based on which the SS7 SSU performs routing. The SS7 SSU will route incoming messages to a specified module instance, if the value of this parameter matches the Value field. Possible values: ■ DEST_ADDRESS_ALIAS ■ SOURCE_ADDRESS_ALIAS ■ APPLICATION_CONTEXT ■ SERVICE_KEY ■ OPCODE

Table 3–24 (Cont.) Incoming Routing Criteria Fields

Name	Type	Description
Value	STRING	Specifies a value that the Session Key parameter of an SCCP message must match, in order for the rule specified in the list of existing routing rules to apply. You can define one of the following in the Value parameter: ■ Single value ■ Range of dash-separated values ■ Comma-separated values

Monitoring

The Monitoring tab enables you to configure Runtime MBeans and notifications for monitoring SS7 SSU for TDM. For more information about configuring monitoring, see the discussion on configuring Service Broker monitoring in *Oracle Communications Service Broker System Administrator's Guide*.

4

Configuring a Diameter Signaling Server Unit

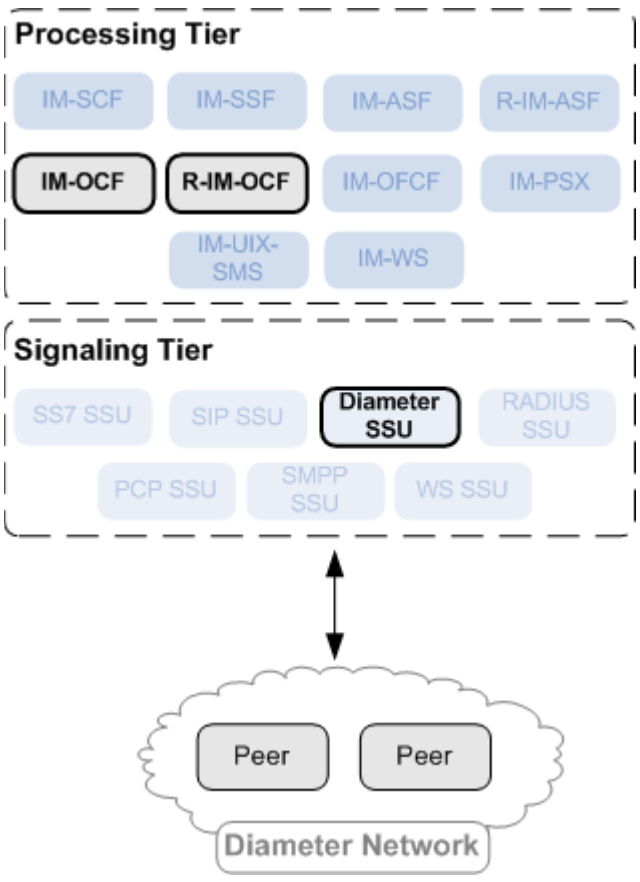
This chapter describes how to configure an Oracle Communications Service Broker Diameter Signaling Server Unit (SSU) using the Administration Console.

About the Diameter SSU

The Diameter SSU provides connectivity between Diameter network entities and those internal Service Broker components that communicate through Diameter, such as IM-OCF and R-IM-OCF.

Figure 4–1 shows the Diameter SSU in the Signaling Tier. The Diameter SSU provides IM-OCF and R-IM-OCF with Diameter connectivity.

Figure 4–1 Diameter SSU in the Service Broker Architecture



About Diameter Nodes and Peers

The Diameter SSU is a process that implements the Diameter protocol. You define the Diameter SSU as a Diameter node.

By default, the Diameter SSU is configured as one Diameter node, where all signaling servers provide a Diameter network channel on the same port. If you deploy the Diameter SSU on multiple signaling servers running on the same physical system, you must configure each signaling server to listen on a different port, otherwise the ports collide. In this case, you define a Diameter node for each signaling server. In general, when you need to define a different address, host or port to Diameter SSU deployments running on different Signaling Servers, you create a Diameter node for each Signaling Server.

A Diameter node communicates with Diameter network entities known as peers. Each Diameter node can communicate with multiple peers. To define peers with which the Diameter node can communicate, you can use the following methods:

- Explicitly define each peer with which the Diameter node can communicate.
- Enable dynamic peer discovery in combination with TLS transport to allow the Diameter SSU to recognize peers automatically. Oracle recommends enabling dynamic peers only when using the TLS transport, because no access control mechanism is available to restrict hosts from becoming peers.

When a Diameter node receives a message from a peer, the Diameter node routes the message to a server that you define based on the realm of the peer. Depending on the configuration, the Diameter node can process the message locally without routing to another server, include additional AVPs to the message before routing, or route the message to the specified server.

A message that the Diameter node receives might not match any realm-based criteria. To allow the Diameter SSU to still handle such a message, you can define a route known as a default route. For the default route, you need to specify the server to which the Diameter SSU routes the message and the action the Diameter node should perform before the routing.

About Routing Messages to Service Broker Components

After the Diameter SSU received a message, the Diameter SSU routes the message to a Processing Tier component (R-IM-OCF or IM-OCF) that process Diameter messages. The Diameter SSU decides to which component to route the message based on criteria known as routing rules. A routing rule defines the destination component based on the value of a specified AVP. For example, you can create a rule based on the ORIGIN_REALM AVP. This rule routes messages from the specified realm to a certain instance of R-IM-OCF.

A routing rule consists of the following parts:

- Incoming routing rule

  This defines an instance of the IM to which the Diameter SSU routes the message. You can create multiple rules for the same IM. The Diameter SSU checks these rules in the order determined by the priority of the rule.

  The lower the number, the higher the priority. For example, if you created two rules and set Priority of one rule to "1" and set Priority of another rule to "2", the Diameter SSU checks the rule with Priority set to "1" first.

  The Diameter SSU begins with the rule that has the highest priority. If an incoming session fits the criteria defined in this rule, the Diameter SSU applies the rule and

does not check the rest of the rules. Otherwise, the Diameter SSU checks whether an incoming session fits the criteria of a rule with a lower priority. The Diameter SSU performs this check until the Diameter SSU finds a rule whose criteria are met by an incoming session.

- Incoming routing criteria

  The criteria define conditions for incoming routing rules. If these conditions are met, the Diameter SSU routes the incoming message to the IM specified in the incoming routing rule.

  The conditions are based on AVPs. You specify the AVP that the Diameter SSU should check. If the AVP specified by you and the AVP set in the incoming message match, then the Diameter SSU routes the message to the IM that you defined in the incoming routing rule associated with the incoming routing criteria.

  You can specify the AVP using one of the following methods:

  - Selecting one of the pre-defined attributes and specifying its value
  - Specifying a custom AVP by entering the AVP's code, vendor ID (if necessary), and value

About Routing Messages to Diameter Peers

You can specify a destination Diameter peer to which the Diameter SSU routes a message based on the alias of the peer. Several peers can share the same alias. If the Diameter SSU fails to send a message to a peer (for example, when the peer is inactive), the Diameter SSU sends the message to another peer that has the same alias.

You specify the alias of the peer in the Destination-Realm AVP parameter when configuring IM-OCF. The Diameter SSU refers to the outbound destinations table to map the alias to the destination host and destination realm.

If the value in the Destination-Realm AVP of the outbound message does not match the alias you set in the outbound destinations table, the Diameter SSU routes the message to the destination specified in the Destination-Host AVP field.

The Diameter SSU distributes messages among different peers that share the same alias using the weighted load strategy. This strategy determines a peer that receives a message based on the weight that you assign to the peer. The weight determines a relative share of the traffic that the peer should receive. For example, you defined two peers whose weight is 100 and 200 correspondingly. The peer with the weight of 100 receives 1/3 of the traffic, while the peer with the weight of 200 receives the remaining 2/3 of the traffic.

If a peer fails, the Diameter SSU redistributes the traffic among remaining peers according to their weight.

You can define a peer that receives traffic if other peers whose weight is greater than zero, fail. This peer is known as secondary peer, and its weight is always zero. If in the example above, you add one more peer whose weight is set to zero, the Diameter SSU sends messages to this peer only if the peers whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple peers with secondary priority, the Diameter SSU distributes traffic equally among them.

The weighted load strategy enables you to control the traffic distribution depending on capabilities of peers. For example, if a peer runs a more powerful server, this peer can serve more traffic, then you would set its load weight relatively higher.

Configuring Diameter Nodes

Configuration of a Diameter node requires the following:

- Creating a new node. See "Setting Up a Diameter Node" for more information.
- Setting up the default route. See "Configuring the Default Route" for more information.
- Setting up routes. See "Configuring Routes" for more information.
- Setting up peers. See "Configuring Peers" for more information.

Setting Up a Diameter Node

To set up a Diameter node:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SSU Diameter** node.
4. In the SSU Diameter configuration pane, click the **DIAMETER** tab.
5. Click the **Diameter Configuration** subtab.

   This subtab contains the following panes:

   - List of existing Diameter nodes. This pane is located on the left.
   - Subtabs with configuration parameters of the Diameter node selected in the left of existing Diameter nodes. This pane is located on the right.
6. Do one of the following:

   - To create a new Diameter node, on the bottom of the list of existing Diameter nodes, click **Add**. Then in the **New** dialog box, enter the name of the new Diameter node and click **Apply**.
   - To configure an existing Diameter node, in the list of existing Diameter nodes, select the node that you want to configure.
7. In the **General** subtab, specify values for the parameters described in Table 4–1.

Table 4–1 Diameter Node Parameters

Field	Description
Name	Specifies the name of the Diameter node.

Table 4–1 (Cont.) Diameter Node Parameters

Field	Description
Target	Specifies the name of the server on which the Diameter SSU runs. Leaving this field blank indicates that the configuration applies to all servers. The Target field includes the following additional options: ■ **Include Origin State ID**: Specifies that the Origin State ID AVP is included in each request, which allows for the rapid detection of terminated sessions. Diameter AVPs carry specific authentication, accounting, authorization routing and security information, and configuration details for request and reply. ■ **SCTP**: Indicates that the Diameter node is configured with support for SCTP. ■ **TLS**: Indicates that the Diameter node is configured with support of Transport Layer Security (TLS). This field advertises TLS capabilities when the node is interrogated by another Diameter node.
Host	Specifies the host name of the Diameter node. The host identity might or might not match the DNS name.
Realm	Specifies the realm name of the Diameter node. For example: **host@oracle.com** Multiple Diameter nodes can be run on a single host using different realms and listen port numbers.
Address	Specifies the listen address for this Diameter node, using either the DNS name or the IP address. The host identity is used as the listen address when this field is blank. The host identity might or might not match the DNS name. Oracle recommends configuring the **Address** property with an explicit DNS name or IP address to avoid configuration errors.
Port	Specifies the network port number to use with the listen address.
TLS Enabled	Specifies whether the Transfer Layer Security (TLS) mechanism is enabled. Possible values: ■ TRUE ■ FALSE
SCTP Enabled	Specifies whether the Stream Control Transmission Protocol is enabled. Possible values: ■ TRUE ■ FALSE
Peer Retry Delay	Specifies the time, in seconds. This node waits before retrying a request to a Diameter peer. The default wait value is 30 seconds.

Table 4–1 (Cont.) Diameter Node Parameters

Field	Description
Allow Dynamic Peers	Enables dynamic discovery of Diameter peers. Dynamic peer support is disabled by default. If you enabled dynamic peers, you can set two additional parameters: ■ **diameter.watchdog.for.dynamic.peers** This parameter defines whether the Diameter SSU should send Device-Watchdog-Request (DWR) commands to dynamic Diameter peers. ■ **diameter.tcp.keepalive.for.client.peers** This parameter defines whether the TCP socket option SO_KEEPALIVE for Diameter dynamic peers is set to true. You define these parameters in the **start.sh** file of the server on which the Diameter SSU runs. See the "System Properties" section in the "System Administrator's Reference" chapter in *Oracle Communications Service Broker System Administrator's Guide*.
Request Timeout	Specifies the amount of time, from 0 milliseconds, this node waits for an answer message before timing out.
Watchdog Timeout	Specifies the amount of time, from 0 seconds, this node uses for the value of the Diameter Tw watchdog timer interval.
Include Origin-State-Id	Specifies whether the Diameter SSU includes an Origin-State-Id AVP into each request. Possible values: ■ TRUE ■ FALSE
Keystore Id	Specifies the ID of the keystore as you configured it in the Credential Store. Notice that the **Keystore Id** parameter is applicable only when you set the **TLS Enabled** parameter to **TRUE**.
Truststore Id	Specifies the ID of the truststore as you configured it in the Credential Store. Notice that the **Truststore Id** parameter is applicable only when you set the **TLS Enabled** parameter to **TRUE**.

8. Click **Apply**.

Configuring the Default Route

To configure the default route:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SSU Diameter** node.
4. In the SSU Diameter configuration pane, click the **DIAMETER** tab.
5. In the list of existing Diameter nodes, select the node for which you set up the default route.
6. Click the **Default Route** subtab.

7. Specify values for the parameters described in Table 4–2.

Table 4–2 Diameter Default Route Parameters

Field	Description
Name	Specifies an administrative name for the route.
Action	Specifies an action that this node performs when using the default route. Select **relay**. The Diameter SSU routes the message to the server without adding or modifying AVPs.

8. Click **Apply**.
9. Underneath the configuration parameters of the default route, click **New**.
10. In the **New** dialog box, enter the host name of the target server.
11. Click **Apply**.

Configuring Routes

To configure a new Diameter route:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SSU Diameter** node.
4. In the SSU Diameter configuration pane, click the **DIAMETER** tab.
5. In the list of existing Diameter nodes, select the node for which you set up the routes.
6. Click the **Routes** subtab.

   This subtab contains the following panes:

   - List of existing routes. This pane is located on the left.
   - Configuration parameters of the route selected in the list of existing routes. This pane is located on the right.
7. Do one of the following:
   - To create a new route, on the bottom of the list of existing routes, click **Add**. In the **New** dialog box, enter the name of the new route and click **Apply**.
   - To modify an existing route, in the list of existing routes, select the route that you want to modify.
8. Specify values of the parameters described in Table 4–3.

Table 4–3 Routes Parameters

Field	Description
Name	Specifies an administrative name for the route.
Realm	Specifies the target realm for this route.

Table 4–3 (Cont.) Routes Parameters

Field	Description
Application ID	Specifies the type of Diameter billing to use. Possible values ■ **3** Specifies Diameter Rf charging. ■ **4** Specifies Diameter Ro charging.
Action	Specifies an action that this node performs when using the route. Select **relay**. The Diameter SSU routes the message to the server without adding or modifying AVPs.

9. Click **Apply**.
10. Underneath the configuration parameters of the route, click **New**.
11. In the **New** dialog box, in the **Host** field, enter the host name of the target server.
12. Click **Apply**.

Configuring Peers

To configure a Diameter peer:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SSU Diameter** node.
4. In the SSU Diameter configuration pane, click the **DIAMETER** tab.
5. In the list of existing Diameter nodes, select the node for which you set up the peers.
6. Click the **Peers** subtab.
7. On the bottom of the **Peers** subtab, click the **New** button.
8. In the **New** window, fill in the fields described in Table 4–4.

Table 4–4 Peer Recognition Parameters

Field	Description
Host	Specifies the peer's host identity.
Address	Specifies the peer's address, using either the DNS name or IP address.
Port	Specifies the listen port number of the peer.

Table 4–4 (Cont.) Peer Recognition Parameters

Field	Description
Protocol	Specifies the protocol used to communicate with the peer. Possible values: ■ tcp ■ sctp Default value: tcp Note that Service Broker attempts to connect to the peer using *only* the protocol you specify. The other protocol is not used, even if a connection fails using the selected protocol.
Watchdog Enabled	Indicates whether the peer supports the Diameter Tw watchdog timer interval. Possible values: ■ TRUE ■ FALSE

Routing Incoming Messages to Service Broker's Components

Configuration of incoming routing rules requires the following:

- Configuring routing rules. See "Configuring Routing Rules" for more information.
- Configuring routing criteria. See "Configuring Routing Criteria" for more information.

Configuring Routing Rules

To set up incoming routing rules:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SSU Diameter** node.
4. In the SSU Diameter configuration pane, click the **SSU Diameter** tab.
5. Click the **Routing** subtab.

   This subtab contains the following panes:

   - List of existing routes. This pane is located on the left.
   - Subtabs with configuration parameters of the route selected in the list of existing routes. This pane is located on the right.
6. Do one of the following:

   - To create a new route, on the bottom of the list of existing routes, click **Add**. Then in the **New** dialog box, enter the name of the new route and click **Apply**.
   - To modify an existing route, in the left of existing routes, select the route you want to modify.
7. On the **Incoming Routing Rules** subtab, specify values for the parameters described in Table 4–5.

Table 4–5 Diameter SSU Incoming Routing Rule Fields

Name	Type	Description
Name	STRING	Specifies a unique rule name.
Priority	INT	Specifies an order in which the Diameter SSU checks routing rules to evaluate if an incoming session fits rule's criteria. The Diameter SSU applies the first found rule which criteria are met by an incoming session. The lower the number, the higher the priority. For example, if you created two rules and set Priority of one rule to" 1" and set Priority of another rule to "2", the Diameter SSU checks the rule with Priority set to "1" first. You can define an incoming routing rule that the Diameter SSU applies if no other rule can be applied, by setting the Priority parameter of this rule to the largest number (that is lowest priority). There is no need to specify incoming routing criteria for such a rule.
Module Instance	STRING	Specifies the URI of the destination Service Broker component to which the Diameter SSU routes incoming sessions. The URI has the following format: SSU:*IM-instance-name*.*IM-type*@*domain-id* ■ *IM-instance-name*: The IM instance name that you specified when you added this IM in the IM Management Configuration screen. ■ *IM-type*: The type of the IM instance ■ *domain-id*: Name of the Processing Domain or Processing Domain Group where the relevant IM or application is deployed. This parameter is required only when your Service Broker deployment includes two or more Processing Domains. Use the name given to the domain when it was created. This name is specified by the axia.domain.id property. *domain-id* is required only if your deployment includes two or more Processing Domains. For example: `ssu:imocf_instance.IMOCF@processing-domain-1`

8. Click **OK**.

Configuring Routing Criteria

To set up incoming routing criteria:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SSU Diameter** node.
4. In the SSU Diameter configuration pane, click the **SSU Diameter** tab.
5. Click the **Routing** subtab.
6. Click the **Incoming Routing Criteria** subtab.

   The Incoming Routing Criteria configuration pane appears. This pane displays a table. The table contains criteria that define the conditions to be met in order the

incoming message to be sent to the Service Broker component that you defined in the incoming routing rules. Each row in the table represents a single rule.

7. Click **New** at the bottom of the Incoming Routing Criteria pane.

   The New dialog box appears.

8. Specify values of the parameters described in Table 4–6.

Table 4–6 Diameter SSU Incoming Routing Criteria Fields

Name	Type	Description
Name	STRING	Specifies a unique rule name.
Attribute	STRING	Specifies a Diameter AVP based on which the Diameter SSU performs routing. Possible values: ▪ APPLICATION_ID ▪ ORIGIN_REALM ▪ ORIGIN_HOST ▪ CUSTOM_AVP Default value: APPLICATION_ID
Value	STRING	Specifies a value of the AVP. When the Attribute parameter is not set to CUSTOM_AVP, you can define one of the following in the Value parameter: ▪ Single value ▪ Range of dash-separated values ▪ Comma-separated values If you set the Attribute parameter to CUSTOM_AVP, specify the code, vendor ID, and value of the AVP using the following format: `code=AVP_code;[vendorId=vendor_ID]?;[code=AVP_code;[vendorId=vendor_ID];]*; value=AVP_value` For example: `code=296;value=seagull_client` The absence of a Vendor-ID or a Vendor-ID value of zero (0) identifies the IETF IANA controlled AVP Codes namespace. For more information on adding custom Diameter AVPs to the Service Broker Diameter stack, see the discussion on adding custom AVPs in *Oracle Communication Service Broker Online Mediation Controller Implementation Guide*.

Routing Message Routing to Diameter Peers

To add outbound destinations:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SSU Diameter** node.
4. In the SSU Diameter configuration pane, click the **SSU Diameter** tab.
5. Click the **Outbound Destinations** subtab.

   The Outbound Destinations configuration pane appears. This pane displays a table. The table contains rules that define the destination Diameter peer to which

the Diameter SSU routes an outgoing message. Each row in the table represents a single rule.

6. Click the **New** button at the bottom of the Outbound Destinations pane.

   The New dialog box appears.

7. Fill in the fields described in Table 4–7.

Table 4–7 Diameter SSU Outbound Destinations Parameters

Field	Descriptions
Name	Specifies a unique destination identifier.
Alias	Specifies the alias of a Diameter peer that must be set in the Destination-Realm AVP of the message sent by a Service Broker's component (such as IM-OCF) to the Diameter SSU. See the "Configuring AVPs" in "Configuring Diameter Credit Control Application Parameters" in "Setting Up IM-OCF Ro" in *Oracle Communications Service Broker Modules Configuration Guide* for more information on specifying the Destination-Realm AVP in outbound messages. If the alias set in the message and the value of the Alias parameter match, the Diameter SSU forwards the message to the peer whose host and realm are defined in the Destination Host and Destination Realm parameters.
Destination Host	Specifies the host of the destination Diameter peer.
Destination Realm	Specifies the realm to which the destination Diameter peer belongs.
Weight	Specifies the relative load weight for the Diameter peer. Default value: 0

8. Click **OK**.

   The Diameter SSU dispatches messages to destination Diameter peers in the realm according to a preconfigured strategy.

Configuring the Credential Store

You use the Credential Store to securely store, encrypt, and validate the credentials that Service Broker uses to communicate with Diameter peers. For more information about how the Credential Store works and how you configure credentials, see a discussion on administering Credential Stores in *Oracle Communications Service Broker Security Guide*.

5

Configuring a SIP Signaling Server Unit

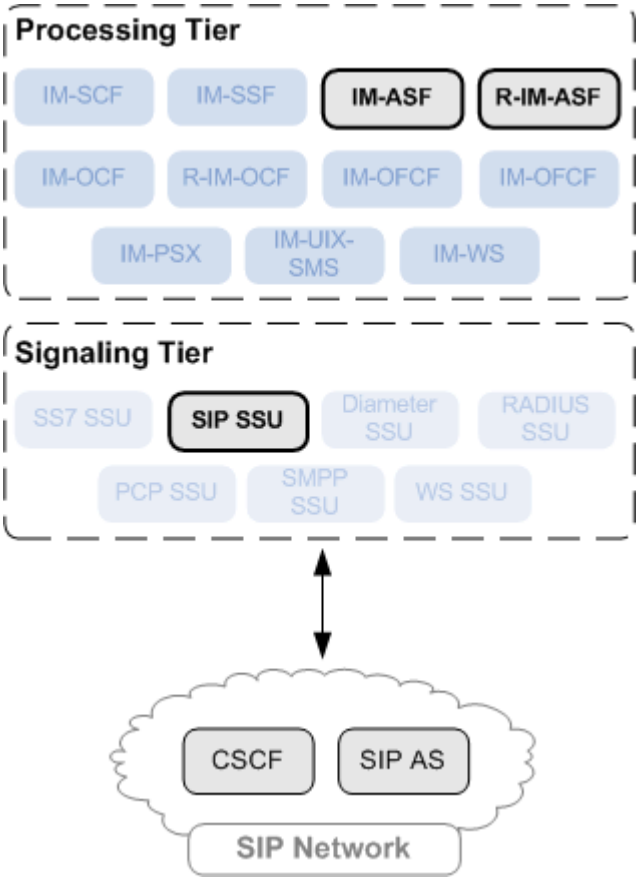
This chapter describes how to configure an Oracle Communications Service Broker SIP Signaling Server Unit (SSU) using the Administration Console.

About the SIP SSU

The SIP SSU provides SIP connectivity between network entities, such as CSCFs and application servers, and those internal Service Broker components that communicate through SIP, such as IM-ASF-SIP and R-IM-ASF-SIP.

Figure 5–1 shows the SIP SSU in the Signaling Tier. The SIP SSU provides IM-ASF and R-IM-ASF with SIP connectivity.

Figure 5–1 Role and Position of the SIP SSU in the Overall Architecture of Service Broker

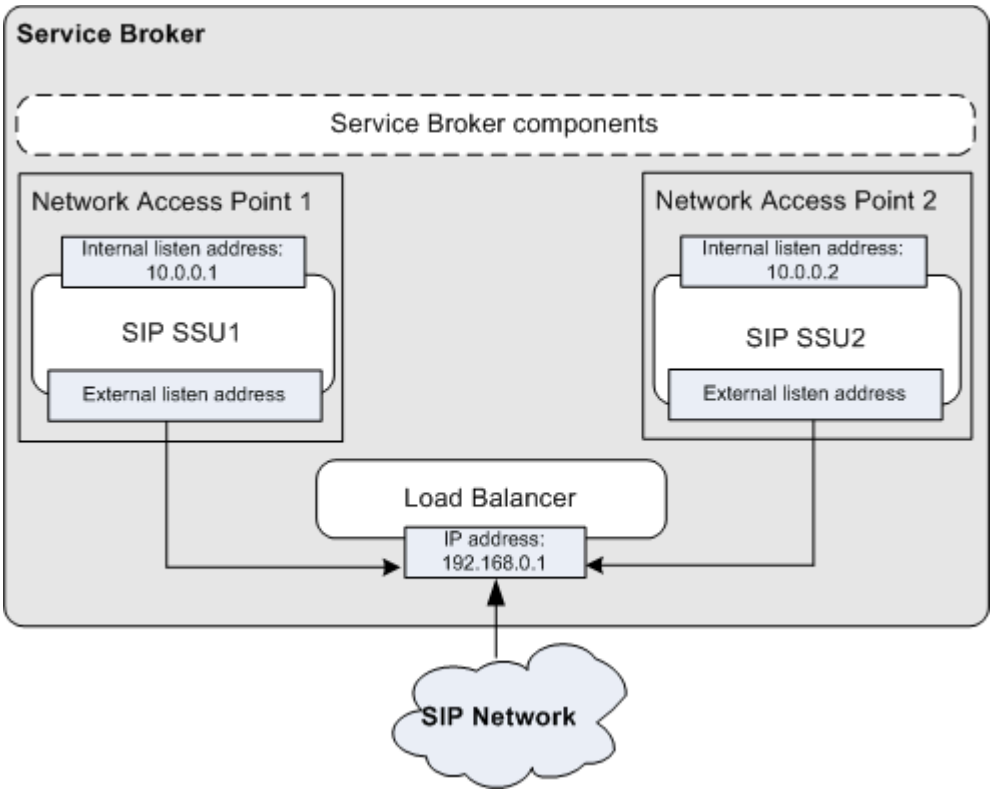


About Network Access Points

The SIP SSU runs on servers in the signaling tier. Each server provides a listen address, that is IP and port, called network access point, that entities in the network use to connect Service Broker. If you use a Load Balancer in your system, entities in the network connect Service Broker through the Load Balancer. In this case you also specify the address of the Load Balancer as the external listen address of each network access point. When you do not use a Load Balancer in your system, you set the external listen address of a network access point to be the same as the network access point's listen address.

Figure 5–2 shows a Service Broker deployment with two network access points and a Load Balancer. Each network access point has its own listen address. The external listen address of each network access point is set to the same address that the Load Balancer has. SIP entities in the network use the external listen address to send SIP messages to the SIP SSUs.

Figure 5–2 Deployment with Two Network Access Points and the Load Balancer



The SIP SSU monitors connections between a network access point and network entities. You can specify the maximum number of network entities that can connect to the network access point. Once the SIP SSU detects the maximum number of connection attempts, it declines any additional attempts.

You can specify a timeout that the network access point waits for a complete message to be received by a network entity. In addition, you can define the amount of time that a connection is allowed to be idle before the network access point closes it.

About Connection Pools

To minimize communication overhead with SIP network entities, the SIP SSU provides a connection pooling mechanism. You can configure multiple fixed pools of connections to different addresses.

The SIP SSU opens new connections from the connection pool on demand as the server makes requests to a configured address. The server then multiplexes new SIP requests to the address using the already opened connections, rather than repeatedly terminating and recreating new connections. The SIP SSU uses opened connections in a round-robin fashion. The SIP SSU leaves these existing connections open until they are explicitly closed by the network entity.

Notice that the SIP SSU uses connection pools only for those connections that the SIP SSU initiates. If a network entity originates a request, this network entity establishes a connection with the SIP SSU. The SIP SSU does not force such an entity to use a new connection with the SIP SSU, and closes it when the session ends.

Receiving and Sending SIP Messages

From the perspective of SIP network entities, Service Broker acts as a SIP user agent. To receive SIP messages from other network entities, Service Broker requires a user agent identifier that uniquely identifies Service Broker within the SIP network. This identifier is called a Globally Routable User Agent URI (GRUU).

You define the GRUU as a part of the SIP SSU configuration process. The SIP SSU distributes the GRUU in the Contact and Routeset headers of SIP messages that the SIP SSU sends to network entities.

Receiving SIP Messages from Network Entities

The SIP SSU routes incoming SIP messages to a Processing Tier component (R-IM-ASF or IM-ASF) for processing. The SIP SSU selects a target component to route the message to based on criteria that you specify in the form of incoming routing rules. Incoming routing rules specify SIP message destinations using the messages's origination address.

For example, a SIP network might have two CSCFs whose IP addresses are 192.168.0.220 and 192.168.0.240. In your Service Broker deployment, you might have two instances of R-IM-ASF whose names are R-IM-ASF1 and R-IM-ASF2 accordingly. To specify to which of the two IMs the SIP SSU should route a SIP message, you can create two incoming routing rules.

In one rule, you specify that if the IP address of the sending network entity is 192.168.0.220, the SIP SSU routes the message to R-IM-ASF1. In the second rule, you specify that if the IP address of the network entity which sent the message is 192.168.0.240, the SIP SSU routes the message to R-IM-ASF2.

Sending SIP Messages to Network Entities

For outgoing SIP traffic, you define SIP network entities to which the SIP SSU route outgoing requests. You define the address of a network entity in the form of a SIP URI. This is the SIP URI that internal Service Broker components use to specify the destination of outgoing traffic. If several network entities act as one logical destination entity, you can assign one alias to those network entities. When Service Broker components send SIP messages to network entities, the Service Broker components can use the alias to specify the message destination.

The SIP SSU distributes messages among different SIP network entities that share the same alias using the weighted load strategy. This strategy determines a network entity that receives a message based on the weight that you assign to the entity. The weight determines a relative share of the traffic that the network entity should receive. For example, you defined two entities whose weight is 100 and 200 correspondingly. The network entity with the weight of 100 receives 1/3 of the traffic, while the network entity with the weight of 200 receives the remaining 2/3 of the traffic.

If a network entity fails, the SIP SSU redistributes the traffic among remaining networking entities according to their weight.

You can define a network entity that receives traffic if other network entities whose weight is greater than zero, fail. This entity is known as secondary network entity, and its weight is always zero. If in the example above, you add one more entity whose weight is set to zero, the SIP SSU sends messages to this network entity only if the network entities whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple network entities with secondary priority, the SIP SSU distributes traffic equally among them.

The weighted load strategy enables you to control the traffic distribution depending on capabilities of network entities. For example, if a network entity runs a more powerful server, this entity can serve more traffic, then you would set its load weight relatively higher.

To provide a stable connection with network entities, the SIP SSU implements a heartbeat mechanism. This mechanism allows the SIP SSU check availability of network entities by periodically sending requests to SIP network entities. If the SIP SSU does not receive a response within the specified period, the SIP SSU considers the network entity inactive, and stop sending requests to it. However, the SIP SSU continues to periodically check availability of inactive network entities.

You configure the heartbeat mechanism for each SIP network entity separately when you define the network entity.

Specifying SIP Headers Insertion

To specify how the SIP SSU handles SIP headers:

1. In the navigation tree in the domain navigation pane, expand the **Signaling Tier** node.
2. Select **SSU SIP**.
3. In the SSU SIP configuration pane, click the **SIP** tab.
4. In the **SIP Configuration** area, specify values for the parameters described in Table 5–1.

Table 5–1 SIP Header Insertion Parameters

Field	Description
Server Header Insertion	Specifies when the SIP SSU inserts a Server header with the signaling server name into outgoing SIP messages. You can use this functionality to limit or eliminate Server headers to reduce the message size for wireless networks, or to increase security. Possible values: ■ **None** The SIP SSU does not insert a Server header. ■ **Request** The SIP SSU inserts the Server header only for SIP requests generated by the SIP SSU. ■ **Response** The SIP SSU inserts the Server header only for SIP responses generated by the SIP SSU. ■ **All** The SIP SSU inserts the Server header for all SIP requests and responses. Default value: **None**
Server Header Value	Specifies the value of the Server header that the SIP SSU inserts into SIP messages.

Table 5–1 (Cont.) SIP Header Insertion Parameters

Field	Description
Default Form For Header Insertion	Specifies how the SIP SSU applies rules for compacting SIP message headers. Possible values: ■ **Compact** The SIP SSU uses the compact form for all system-generated headers. However, any headers that are copied from an originating message use their original form. ■ **Force compact** The SIP SSU uses the compact form for all headers, converting long headers in existing messages into compact headers. ■ **Long** The SIP SSU uses the long form for all system-generated headers. However, any headers that are copied from an originating message (rather than generated) use their original form. ■ **Force long** The SIP SSU uses the long form for all headers, converting compact headers in existing messages into long headers.

5. Click **Apply**.

Configuring SIP Network Access Points

To configure a SIP network access point:

1. In the navigation tree in the domain navigation pane, expand the **Signaling Tier** node.
2. Select **SSU SIP**.
3. In the SSU SIP configuration pane, click the **SIP** tab.
4. Click the **Network Access Point** subtab.

   This subtab consists of the following panes:

   - List of existing network access points. This pane is located on the left.
   - Subtabs with configuration parameters of the network access point selected in the list of existing network access points. This pane is located on the right.
5. Do one of the following:
   - To create a new network access point, on the bottom of the list of existing network access points, click **Add**. Then in the **New** dialog box, enter the name of the new access network point and click **Apply**.
   - To modify an existing network access point, in the list of existing network access points, select the network access point that you want to modify.
6. On the **General** subtab, specify values for the parameters described in Table 5–2.

Table 5–2 SIP Network Access Point General Parameters

Field	Description
Target	The name of the server on which the SIP SSU runs. Leaving this field blank indicates that the configuration applies to all servers.
Name	A unique SIP network channel name.
Protocol	The protocol used for connections through the network channel. Set this field to **SIP**.
Complete Message Timeout	Specifies the amount of time in seconds that the network access point waits for a complete message to be received. A value of **0** disables the network access point complete message timeout. Valid values range from **0** to **480** seconds.
Idle Connection Timeout	Specifies the amount of time in seconds that a connection is allowed to be idle before it is closed by the network access point. The minimum value is **0** seconds.
Maximum Connected Clients	Specifies the maximum number of SIP network entities that can connect to the network access point.

7. Click the **Listen Address** subtab.
8. Specify values for the parameters described in Table 5–3.

Table 5–3 Listen Address Parameters

Field	Description
Network Type	Specifies the network type of the internal listen address. Set this field to: **internet**
Address Type	Specifies the address type of the internal listen address. Set this field to: **IP4**
Host	Specifies the IP address or DNS name that Service Broker's components use to communicate with the network access point. Setting the value to **0.0.0.0** resolves to the IP of the local computer.
Port	Specifies the port that Service Broker's components use to communicate with the network access point.

9. Click the **External Listen Address** subtab.
10. Specify values for the parameters described in Table 5–4.

Table 5–4 External Listen Address Parameters

Field	Description
Network Type	Specifies the network type of the external listen address. Set this field to **internet**
Address Type	Specifies the address type of the external listen address. Set this field to **IP4**
Host	Specifies the IP address or DNS name that SIP network entities use to communicate with the network access entity. If you use the Load Balancer, enter the IP address of the Load Balancer.
Port	Specifies the port that SIP network entities use to communicate with the network access entity. If you use the Load Balancer, enter the port of the Load Balancer.

Configuring SIP Connection Pools

To configure a connection pool:

1. In the navigation tree in the domain navigation pane, expand the **Signaling Tier** node.
2. Select **SSU SIP**.
3. In the **SSU SIP** configuration pane, click the **SIP** tab.
4. Click the **Connection Pools** subtab.

   This subtab contains a table in which each row represents a pool of connections to one destination host.
5. On the bottom of the **Connection Pool** subtab, click the **New** button.
6. Fill in the fields described in Table 5–5.

Table 5–5 Connection Pool Parameters

Field	Description
Name	Specifies a string value that identifies the name of the pool. All configured names must be unique in the domain.
Destination Host	Specifies the IP address or host name of the destination.
Destination Port	Specifies the destination port number.
Maximum Connections	Specifies the maximum number of opened connections to maintain in the pool.

7. Click **OK**.

   The values you enter are displayed in the table.

Configuring SIP Network Entities

To configure SIP network entities:

1. In the navigation tree in the domain navigation pane, expand the **Signaling Tier** node.
2. Select **SSU SIP**.
3. In the SSU SIP configuration pane, click the **SSU SIP** tab and then the **SIP Network Entities** subtab.
4. Click the **New** button at the bottom of the **SIP Network Entities** pane.

   The New dialog box appears.
5. Fill in the fields described in Table 5–6.

Table 5–6 SIP Network Entities Parameters

Field	Description
Name	Specifies a unique network entity name.

Table 5–6 (Cont.) SIP Network Entities Parameters

Field	Description
Alias	Specifies the alias of a SIP network entity that must be set in the message sent by a Service Broker's component (such an IM-ASF) to the SIP SSU. If the alias set in the message and the value of the Alias parameter match, the SIP SSU forwards the message to the IP address defined in the SipUri parameter. The alias has a format of a SIP URI. For example: `sip:simple_b2b@example.com`
Heartbeat	Specifies whether to use a heartbeat mechanism over the connection with the SIP network entity. Possible values: ■ ON ■ OFF Default value: ON
SipUri	Specifies the SIP URI of the SIP network entity to which the SIP SSU should forward the message. For example: `sip:simple_b2b@192.168.0.219:6060`
Weight	Specifies the relative load weight for the network entity. Default value: 0
Heartbeat Method	Specifies the SIP method that the SIP SSU uses to test the connection with the SIP network entity. Default value: OPTIONS
Response Timeout	Specifies the time interval in seconds during which the SIP SSU waits for a response from the SIP network entity. The heartbeat mechanism uses this field.
Active Interval	Specifies the time interval in seconds for sending heartbeat requests from the SIP SSU to the SIP network entity. This field is used if the previous heartbeat test showed that the SIP network entity is active.
Inactive Interval	Specifies the time interval in seconds for sending heartbeat requests from the SIP SSU to the SIP network entity. This field is used if the previous heartbeat test showed that the SIP network entity is inactive.

6. Click **OK**.

   The values you enter are displayed in the table.

Specifying a Globally Routable User Agent URI

To configure a Globally Routable User Agent URI:

1. In the navigation tree in the domain navigation pane, expand the **Signaling Tier** node.
2. Select **SSU SIP**.
3. In the SSU SIP configuration pane, click the **SSU SIP** tab and then the **SIP Server** subtab.

4. In the **Globally Routable User Agent URI** field, specify a SIP URI that the SIP SSU automatically inserts into **Contact** and **Routeset** headers when communicating with network elements.

   For example: `sip:sb@209.95.109.191:5060`.

5. Click **Apply**.

Configuring Incoming Routing Rules

To configure incoming routing rules:

1. In the navigation tree in the domain navigation pane, expand the **Signaling Tier** node.
2. Select **SSU SIP**.
3. In the SSU SIP configuration pane, click the **SSU SIP** tab and then the **Incoming Routing Rules** subtab.

   The Incoming Routing Rules pane contains a table in which each row represents one routing rule.

4. Click the **New** button, located at the bottom of the Incoming Routing Rules pane.

   The New dialog box appears.

5. Fill in the fields in the dialog box described in Table 5–7.

Table 5–7 SIP Incoming Routing Rules Parameters

Field	Description
Name	Specifies a unique routing rule name
IP Address	Specifies the IP address of the network entity that sends the message to the SIP SSU. If the actual IP address of the network entity and the value of the **IP Address** parameter match, the SIP SSU routes the message to a Service Broker's component with the alias defined in the **Alias** parameter. Setting this field to **any** applies the routing rule to any incoming SIP message, regardless of the IP address of the network entity that sends the message. **Note**: When typing **any** into the IP Address field, you must use only lowercase, as follows: any. Do not type Any or ANY.

Table 5–7 (Cont.) SIP Incoming Routing Rules Parameters

Field	Description
Alias	Specifies the SIP URI of the IM to which the SIP SSU routes an incoming session. The alias has the following format: `ssu:`*IM-instance-name.IM-type@domain-id* ■ *IM-instance-name*: IM instance name you specified when you added this IM in the IM configuration pane. ■ *IM-type*: Type of IM instance. ■ *domain-id*: Name of the Processing Domain or Processing Domain Group where the relevant IM is deployed. This parameter is required only when your Service Broker deployment includes two or more Processing Domains. Use the name given to the domain when it was created. This name is specified by the axia.domain.id property. Example: `ssu:r-imocf_instance.RIMOCF@processing-domain.1` You can also specify the SIP URI of an application external to OCSB to which the SIP SSU routes an incoming message. The alias has the following format: `ssu:`*parameter*`@processing-domain.1/`*application* ■ *parameter*: Developer-specfied parameters that are configured to forward the incoming message to the specified application ■ *application*: The destination application registered to the specified ID to which the incoming event is dispatched.

6. Click **OK**.

   The values you enter are displayed in the table.

6

Configuring a RADIUS Signaling Server Unit

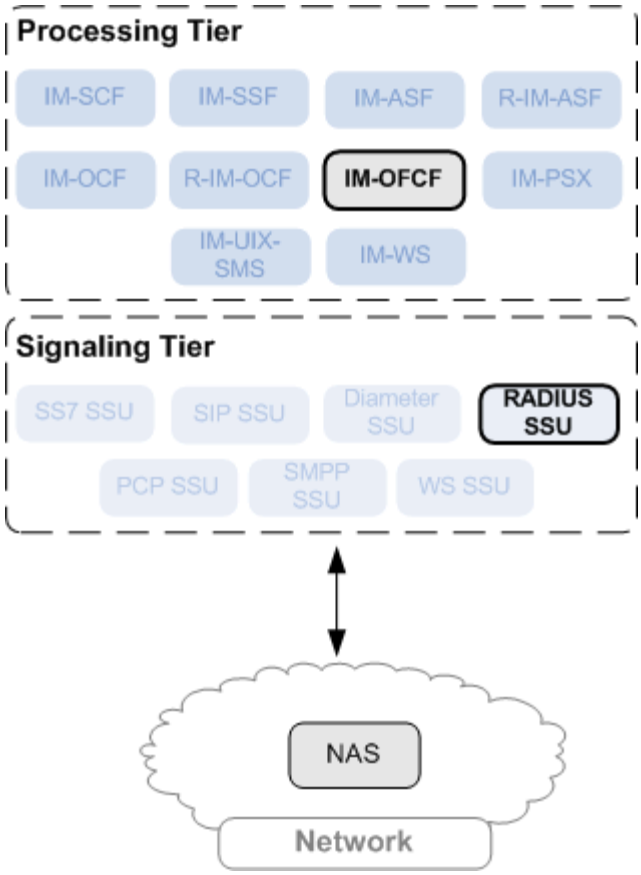
This chapter describes how to configure an Oracle Communications Service Broker RADIUS Signaling Server Unit (SSU) using the Service Broker Administration Console.

About the RADIUS SSU

Service Broker uses the RADIUS SSU to receive RADIUS accounting and access requests from the network. The RADIUS SSU forwards these messages to appropriate components of the Processing Tier.

Figure 6–1 shows the RADIUS SSU in the Signaling Tier. The RADIUS SSU provides IM-OFCF with RADIUS connectivity.

Figure 6–1 Place of RADIUS SSU in the Overall Architecture of Service Broker



About RADIUS Authentication

A RADIUS authentication request contains an Attribute-Value Pair (AVP) called Nas-Identifier AVP. This AVP contains the identity of the Network Access Server (NAS) that provides service to the user. The NAS can be either Oracle BRM or Oracle ECE.

You can specify whether you want to perform authentication against Oracle BRM or Oracle ECE by defining a regular expression that Service Broker compares with the Nas-Identifier AVP.

If your regular expression matches the Nas-Identifier AVP, then Service Broker performs the authentication against the BRM. Otherwise, Service Broker performs the authentication against the ECE.

About Proxy and Local Realms

You can configure the RADIUS SSU to act as one of the following:

- RADIUS server. In this configuration, the RADIUS SSU forwards accounting and authorization requests to Oracle BRM through IMs. The realm in which Oracle BRM is located is called local realm.
- RADIUS proxy. In this configuration, the RADIUS SSU to bypass IMs and send requests directly to an external charging server known as proxy server. The realm in which such a proxy server is located is called proxy realm.

If you want the RADIUS SSU to forward requests to a server in a proxy realm rather than to Oracle BRM, you need to configure the table of realms and table of servers. The table of realms contains different realms to which the RADIUS SSU can forward the request based on the value of the User-Name attribute. The table of servers defines the servers in each of these realms. When the RADIUS SSU finds a match between the value of User-Name defined in the request and the value specified in the tables of realms, the RADIUS SSU forwards the requests to the first available server in the found realm.

About Communication with RADIUS Network Entities

The RADIUS SSU receives requests from NASs. To allow the RADIUS SSU to receive requests from NASs, you need to specify criteria that NASs must meet. A set of these criteria is known as client profile.

A client profile consists of the following:

- Address information criteria. These criteria define the requirements for the address of NASs whose messages the RADIUS SSU can receive. For example, you can define that the RADIUS SSU can receive messages from any NAS whose IP address starts from 10.148.
- AVPs that the RADIUS SSU should copy from a request sent by the NAS to the response generated by Service Broker.

You can create as many client profiles as you need. The RADIUS SSU applies the first profile found whose criteria fit the parameters of the NAS which attempts to connect to the RADIUS SSU.

Online Mediation Controller is provided with a default client profile already set up. This client profile defines that the RADIUS SSU copies User-Name and Acct-Session-Id attributes from a request to the response.

In addition, you can configure the RADIUS SSU to receive messages only from those NASs whose port is in a specified range.

About Receiving and Forwarding RADIUS Requests

When the RADIUS SSU receives a request from a NAS, the RADIUS SSU forwards the request to a Service Broker component. The RADIUS SSU decides to which component to route the request based on criteria known incoming routing rules.

The RADIUS SSU handles accounting and authorization requests differently. When the RADIUS receives an accounting request, the RADIUS SSU forwards it to an appropriate Service Broker component based on the realm from which the request is sent. This realm is called local realm.

The RADIUS SSU forwards all authorization requests to the component that you defined.

About RADIUS Dictionary

A dictionary is a set of attribute-value pairs that Service Broker uses to perform authorization and accounting operations. See the **Customizing the RADIUS data dictionary** section in **Service Integration Components** in *Oracle Communications Billing and Revenue Management (BRM) 7.3.1 Documentation* for more information about the format and syntax of RADIUS dictionaries.

By default, Service Broker uses the standard RADIUS dictionary defined in the RFC 2865 (see `http://www.ietf.org/rfc/rfc2865.txt` for more information). If you need

Service Broker to recognize additional vendor-specific AVPs, you can provide Service Broker with a file that contains a custom dictionary. If any AVP defined in the custom dictionary conflict with the AVPs in any existing AVPs with the product, the custom dictionary one overrides the existing one.

Setting Up RADIUS Authentication

To specify whether Service Broker performs the authentication against the BRM or ECE:

1. In the navigation tree in the domain navigation pane, expand the **OCSB** node.
2. Expand the **Signaling Tier** node.
3. Select the **SSU RADIUS** node.
4. Click the **OCS Authentication** tab.
5. In the **Nas Identifier pattern for BRM** field, enter the string that Service Broker should compare with the Nas-Identifier AVP in the authentication request.
6. Click **Apply**.

Configuring Incoming Routing Rules

You configure rules for the following types of requests:

- Accounting requests. See "Configuring Incoming Routing Rules for Accounting Requests" for more information.
- Access requests. See "Specifying the Service Broker Component for Dispatching Access Requests" for more information.

Configuring Incoming Routing Rules for Accounting Requests

To configure RADIUS SSU Accounting parameters:

1. In the navigation tree in the domain navigation pane, expand the **OCSB** node.
2. Expand the **Signaling Tier** node.
3. Select the **SSU RADIUS** node.
4. In the **SSU RADIUS** tab, click the **Accounting** subtab.
5. At the bottom of the Incoming Routing Rules pane, click the **New** button.

   The New dialog box appears.
6. Fill in the fields of the New dialog box described in Table 6–1.

Table 6–1 RADIUS Accounting Incoming Routing Parameters

Field	Descriptions
Name	Specifies a unique routing rule name.

Table 6–1 (Cont.) RADIUS Accounting Incoming Routing Parameters

Field	Descriptions
Local Realm	Specifies the value to match against the Local Realm. Example: *user-name*`@isp.net` If a RADIUS accounting request arrives containing only a user name but without a Local Realm, the RADIUS SSU discards the request. To prevent the request from being discarded when no Local Realm is specified, set this field to **any**. The RADIUS SSU then forwards the request to the destination specified in the Alias field. Important: When typing **any** into the Local Realm field, you must use only lowercase, as follows: **any**. Do not type **Any** or **ANY**.
Alias	Specifies the URL of the destination IM to which the RADIUS message is dispatched. The alias has the following format: `SSU:`*IM-instance-name.IM-type@domain-id* ■ *IM-instance-name*: IM instance name you specified when you added this IM in the IM configuration pane. ■ *IM-type*: Type of IM instance. ■ *domain-id*: Name of the Processing Domain or Processing Domain Group where the relevant IM or application is deployed. This parameter is required only when your Service Broker deployment includes two or more Processing Domains. Use the name given to the domain when it was created. This name is specified by the axia.domain.id property. Example: `SSU:imocf.IMOCF@ocsb`.1

7. Click **OK**.

Specifying the Service Broker Component for Dispatching Access Requests

To specify the Service Broker component:

1. In the navigation tree in the domain navigation pane, expand the **OCSB** node.
2. Expand the **Signaling Tier** node.
3. Select the **SSU RADIUS** node.
4. In the **SSU RADIUS** tab, click the **Access** subtab.
5. In the **Radius Access Inbound Destination** field, enter the address of the Service Broker component to which you want to dispatch the RADIUS Access request.

   The address has the following format: `ssu:`*domain*

   domain: The name of the domain to which the request is despatched.

   For example: `ssu:ocsb`

   If you leave this field empty, the request is not routed through Service Broker.
6. Click **Apply**.

Specifying a Custom Dictionary

To specify a custom dictionary file:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **RADIUS SSU** node.
4. Click the **RADIUS Custom Dictionary** tab.
5. In the **Custom dictionary file** field, enter the path of the custom dictionary file located on your local file system.

Configuring Server Parameters

To receive RADIUS authentication and accounting requests from the network, you configure the following:

- Server parameters, which define how the RADIUS SSU receives RADIUS requests. See "Configuring Server Parameters" for more information.
- NAS port range, which defines the range of NASs ports from which the RADIUS SSU can receive accounting authentication and accounting requests. See "Specifying the NAS Port Range" for more information.

Configuring Server Parameters

To configure server parameters:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **RADIUS SSU** node.
4. Click the **RADIUS** tab.
5. Click the **Server** subtab and then the **Server** tab.
6. Click **New**.

   The New dialog box appears.
7. Fill in the fields described in Table 6–2.

Table 6–2 Server Parameters

Field	Description
Target managed server	Specifies the target managed server.
IP Address	Specifies the IP address that the RADIUS SSU uses to listen for RADIUS messages.
Authentication Port	Specifies the port that the RADIUS SSU uses to receive RADIUS authentication messages.
Accounting Port	Specifies the port that the RADIUS SSU uses to receive RADIUS accounting messages.
UDP Connection timeout	Specifies the UDP connection timeout in seconds.

Table 6–2 (Cont.) Server Parameters

Field	Description
Retransmission detection time	Specifies the period during which the RADIUS SSU considers incoming RADIUS messages retransmissions if these messages have the same ID received and are sent by the same peer. The RADIUS SSU ignores these messages. If you set the retransmissionTime parameter to 0, the RADIUS SSU does not recognize these messages as retransmissions.
Root CA Store key	Specifies the root CA keystore key. You provide this key to the credential store that contains root CA certificates.
Server Key Store key	Specifies the server keystore. You provide this key to the credential store that contains server certificates.

Specifying the NAS Port Range

To specify the port range:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **RADIUS SSU** node.
4. Click the **RADIUS** tab and then the **Server** subtab.
5. In the **Valid NAS Port Range** tab, fill in the fields as described in Table 6–3.

Table 6–3 Valid NAS Port Range Parameters

Field	Description
Min Value of NAS Port	Specifies the lower limit of the range.
Max Value of NAS Port	Specifies the upper limit of the range.

Setting Up Client Profiles

This set of settings consists of the following:

- Client profiles. See "Setting Up a Client Profile" for more information.
- AVPs that the RADIUS SSU needs to copy from a request to a response. See "Specifying AVPs to Be Copied from a Request to a Response" for more information.

Setting Up a Client Profile

To set up a client profile:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **RADIUS SSU** node.
4. Click the **RADIUS** tab and then the **Client Profile** tab.
5. Click the **Client Profile** tab.
6. Click **New**.

   The New dialog box appears.

7. Fill in the fields described in Table 6–4.

Table 6–4 Client Profile Parameters

Field	Description
Client Address	Specifies the IP address of the RADIUS client from which the RADIUS SSU receives requests. To define a range of addresses to receive requests from a group of RADIUS clients, you can use a regular expression. For example, to define that the RADIUS SSU receives requests from the clients whose IP addresses start from 10.148, you can set the clientAddress parameter to 10.148.*.*
Client NAS Identifier	Specified the ID of the Network Access Server (NAS) from which the RADIUS SSU receives accounting and access requests. To define a range of IDs to receive requests from a group of NASs, you can use a regular expression. For example, to define that the RADIUS SSU receives requests from the NASs whose IDs is in the oracle.com domain, you can set the clientNasId to *.oracle.com.
Authentication Shared Secret Key	Specifies the key that you associated with the password that the RADIUS SSU uses for authentication requests. You associate keys and passwords using the Credential Store tab.
Accounting Shared Secret Key	Specifies the key that you associated with the password that the RADIUS SSU uses for accounting requests. You associate keys and passwords using the Credential Store tab.

Specifying AVPs to Be Copied from a Request to a Response

To specify the AVPs:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **RADIUS SSU** node.
4. Click the **RADIUS** tab and then the **Client Profile** tab.
5. Click the **Avps to copy from Request to Response** tab.
6. Click **New**.

   The New dialog box appears.
7. In the **New** dialog box, in the **Attribute Name** field, enter the name of the AVP that the RADIUS SSU needs to copy.
8. Click **OK**.

   The new AVP appears in the configuration screen.

Configuring Proxy Realm

When you configure a proxy server, you define the following:

- Proxy realm, which defines a realm to which the RADIUS SSU routes a request based on the User-Name AVP. See "Configuring a Proxy Realm" for more information.

- Target server, which defines the server address and ports in the specified realm. See "Configuring Target Servers" for more information.

Configuring a Proxy Realm

To configure a proxy realm:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **RADIUS SSU** node.
4. Click the **RADIUS** tab.
5. Click the **Proxy Realm** subtab and then the **Proxy Realm** tab.
6. Click **New**.

   The New dialog box appears.
7. Fill in the fields described in Table 6–5.

Table 6–5 Proxy Realm Parameters

Field	Description
Name	Specifies the name of the proxy realm.
Username Match Criteria	Specifies the User-Name AVP to be set in the incoming request. If this AVP matches the value of the userNameMatchCriteria parameter, the RADIUS SSU routes the request to the realm specified in the name parameter. To define a range of possible names, you can use regular expressions.
Authentication Shared Secret Key	Specifies the key that you associated with the password that the RADIUS SSU uses for authentication requests. You associate keys and passwords using the Credential Store tab.
Accounting Shared Secret Key	Specifies the key that you associated with the password that the RADIUS SSU uses for accounting requests. You associate keys and passwords using the Credential Store tab.
Request Timeout	Specifies the period, in seconds, that the RADIUS SSU waits for a response from the target RADIUS server.
Number Of Retries	Specifies the number of attempts that the RADIUS SSU tries to send a RADIUS request to the target RADIUS server.

Configuring Target Servers

To configure a target server:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **RADIUS SSU** node.
4. Click the **RADIUS** tab.
5. Click the **Proxy Realm Configuration** subtab and then the **Target Servers** tab.
6. In the **Parent** list, select the proxy realm for which you set up the server. The list displays the proxy realms that you configured using the ProxyRealm tab. See "Configuring Proxy Realm" for more information.

7. Click **New**.

   The New dialog box appears.

8. Fill in the fields described in Table 6–6.

Table 6–6 TargetServers Parameters

Field	Description
Server Address	Specifies the IP address of the proxy server.
Authentication port	Specifies the port that the RADIUS SSU uses to receive RADIUS authentication messages.
Accounting port	Specifies the port that the RADIUS SSU uses to receive RADIUS access messages.

Configuring the Credential Store

You use the Credential Store to securely store, encrypt, and validate the credentials that Service Broker uses to communicate with RADIUS clients and servers. For more information about how the Credential Store works and how you configure credentials, see a discussion on administering Credential Stores in *Oracle Communications Service Broker Security Guide*.

7

Configuring a PCP Signaling Server Unit

This chapter describes how to configure an Oracle Communications Service Broker Portal Communications Protocol (PCP) Signaling Server Unit (SSU) using the Administration Console.

About the PCP SSU

Service Broker acts as an Oracle Communications BRM client application and uses the PCP SSU to communicate with it. The communication is done through a proprietary Oracle Communications BRM protocol, the PCP.

The PCP SSU receives charging requests from internal Service Broker components, such as IM-OFCF PCP and IM-OCF PCP, and routes these request to BRM applications through PCP.

To access Oracle Communications BRM, the PCP SSU must use a BRM client application account. The PCP SSU uses the default root account created when BRM is installed, and its password. See the discussion on configuring login names and passwords for BRM access in *Oracle Communications Billing and Revenue Management System Administrator's Guide*.

The PCP SSU uses connection pools to communicate with BRM. A connection pool is a set of connections maintained between the PCP SSU and the BRM Connection Manager (CM). Each Oracle Communications BRM CM is running on a different physical address and listens for a PCP request on a different port. See the discussion about connection pooling in *Oracle Communications Billing and Revenue Management System Administrator's Guide*, for more information. On the BRM side, an incoming request is assigned a connection from the connection pool and uses the connection to perform operations. When the operation completes, the connection is returned to the pool.

When configuring the PCP SSU connectivity with BRM, you define a number of connection pools, each communicates with one CM. Oracle recommends that you define two or more connection pools, for redundancy and high availability.

Connection pools need to be secured with passwords. You set a password in both the PCP SSU and Oracle Communications BRM. You have to configure the same password for a connection pool that you define in the PCP SSU, and the related CM that you configure on Oracle Communications BRM.

Each connection pool is considered a PCP network entity. If one or more PCP network entities act as one logical Oracle Communications BRM application, you assign one alias to those network entities. Service Broker IMs sending PCP requests to an Oracle Communications BRM application, use the alias to specify the destination BRM application. The PCP SSU routing the requests to their destination, provides a measure

of redundancy, distributing the PCP requests among the different PCP network entities belonging to the same destination BRM application.

The PCP SSU distributes messages among different network entities that share the same alias using the weighted load strategy. This strategy determines a network entity that receives a message based on the weight that you assign to the entity. The weight determines a relative share of the traffic that the network entity should receive. For example, you defined two entities whose weight is 100 and 200 correspondingly. The network entity with the weight of 100 receives 1/3 of the traffic, while the network entity with the weight of 200 receives the remaining 2/3 of the traffic.

If a network entity fails, the PCP SSU redistributes the traffic among remaining networking entities according to their weight.

You can define a network entity that receives traffic if other network entities whose weight is greater than zero, fail. This entity is known as secondary network entity, and its weight is always zero. If in the example above, you add one more entity whose weight is set to zero, the PCP SSU sends messages to this network entity only if the network entities whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple network entities with secondary priority, the PCP SSU distributes traffic equally among them.

The weighted load strategy enables you to control the traffic distribution depending on capabilities of network entities. For example, if a network entity runs a more powerful server, this entity can serve more traffic, then you would set its load weight relatively higher.

The PCP SSU implements a heartbeat mechanism, regularly sending requests to PCP network entities to check their availability. Not receiving a response within a configured time interval denotes that the PCP network entity is inactive. The PCP SSU stops sending requests to inactive network entities, but continues checking their availability every few seconds. You configure the heartbeat mechanism for each PCP network entity separately, when you define the network entity.

After configuring connection pools and destination Oracle Communications BRM applications, you can also optionally change the default configuration of PCP transactions.

Defining Operation Codes

To define operation codes (opcodes):

1. In the navigation tree in the domain navigation pane, expand the **OCSB** node.
2. Expand the **Signaling Tier** node.
3. Select the **SSU PCP** node.
4. Click the **PCP** tab.
5. On the Opcode subtab, configure the fields described in Table Table 7–1.

Table 7–1 Opcode Configuration Parameters

Field	Description
Opcode retry attempts	Specifies how many times the PCP SSU sends the opcode to the BRM if the connection attempt fails. Default value: 2

Table 7–1 (Cont.) Opcode Configuration Parameters

Field	Description
Opcode default timeout	This timeout is used when the opcode timeout attribute is not included into a PCP outbound request event. Default value: 5000
PCP transaction timeout	Specifies the timeout, in milliseconds, on PCP transactions (when PCP transaction opcodes executed, e.g., TRANS_OPEN, TRANS_CLOSED) Default value: 10000

Configuring PCP Transactions

To configure PCP Transaction:

1. In the navigation tree in the domain navigation pane, expand the **OCSB** node.
2. Expand the **Signaling Tier** node.
3. Select the **SSU PCP** node.
4. In the **PCP Network Entities** tab, configure the fields described in Table 7–2.

Table 7–2 SSU PCP Configuration Parameters

Field	Description
Name	A unique identifier for the SSU PCP instance.
Alias	Specifies a name that Service Broker uses to refer the PCP network entity. The alias is a simple string.
Weight	Defines the relative amount of traffic sent to the SSU PCP destination. See the discussion on Weight in "About the PCP SSU".
Heartbeat	Specifies whether to use a heartbeat mechanism over the connection with the PCP network entity to check the connection status.
PcpPoolId	Specifies the pool id to map to this alias. The PcpPoolId is a simple string.
Response Timeout	Specifies the time interval, in seconds, during which the PCP SSU waits for a response from the PCP network entity. The heartbeat mechanism uses this field.
Active Interval	Specifies the periodicity, in seconds, for sending heartbeat requests from the SSU PCP to the PCP network entity. This field is used if the previous heartbeat test results in an active PCP connection.
Inactive Interval	Specifies the periodicity, in seconds, for sending heartbeat requests from the SSU PCP to the PCP network entity. This field is used if the previous heartbeat test results in a inactive PCP connection.

Defining Connection Pools

To define a connection pool:

1. In the navigation tree in the domain navigation pane, expand the **OCSB** node.
2. Expand the **Signaling Tier** node.

3. Select the **SSU PCP** node.
4. In the **PCP** tab, select the **Connection Pools** tab.
5. Click the **New** button. The New dialog box appears.
6. Enter the fields described in Table 7–3.

Table 7–3 Connection Pool Parameters

Field	Descriptions
Pool ID	A unique connection pool identifier.
BRM CM Host	The name or IP address of the system running the Oracle Communications BRM CM. See "Using Configuration Files to Connect and Configure Components" in *Oracle Communications Billing and Revenue Management System Administrator's Guide*.
BRM CM Port	The port number of the Oracle Communications BRM CM on the host system. See "Using Configuration Files to Connect and Configure Components" in *Oracle Communications Billing and Revenue Management System Administrator's Guide*.
BRM CM Login ID	*account-name.database-number* Where: *account-name* is the name of the BRM client application account that Service Broker uses to access Oracle Communications BRM. See "Configuring Login Names and Passwords for BRM Access" in the chapter "Implementing System Security" in *Oracle Communications Billing and Revenue Management System Administrator's Guide*. *database-number* is the database number that you configured when you installed the BRM application. Default value: root.0.0.0.1 See "Installing BRM" in Oracle Communications Billing and Revenue Management Installation Guide.
Max Connections	Specifies the maximum number of connections in the pool. Default value: 8
Min Connections	Specifies the minimum number of connections in the pool. Default value: 4
Request Timeout	Specifies the time that the PCP SSU waits for establishing a connection.
Max Idle Time	Specifies the maximum idle time for a connection. When the specified time expires, the PSP SSU closes the connection.
Request Queue Size	Specifies the maximum size of the queue. When the maximum size is reached, the PCP SSU drops all further requests.

Table 7–3 (Cont.) Connection Pool Parameters

Field	Descriptions
Enabled	Specifies whether the connection is enabled. You can use this field to disable a connection pool, for example, for maintenance. Possible values: ■ true ■ false Default value: true

Securing Connection Pools

To set up a connection pool password:

1. In the navigation tree in the domain navigation pane, expand the **OCSB** node.
2. Expand the **Signaling Tier** node.
3. Select the **SSU PCP** node.
4. In the **PCP** tab, select the **Credential Store** tab.
5. In the Password area, enter in the fields described in Table 7–4:

Table 7–4 Connection Pool Password

Field	Descriptions
Key	A connection pool identifier. The identifier that you assigned to the connection pool, in the field Pool ID, when you initially defined the connection pool.
Password	The password of the BRM client application account used by the connection pool to access the BRM. This is the password of the account that you configured in the BRM CM Login ID, when you initially defined the connection pool.
One-way	Always uncheck this box. The PCP SSU should be able retrieve the connection pool password from the Credential Store and use it when sending requests to Oracle Communications BRM.

6. Click the **Set Password** button.

Managing Connection Pool Credentials

To check whether a key exists in the credential store:

1. In the navigation tree in the domain navigation pane, expand the **OCSB** node.
2. Expand the **Signaling Tier** node.
3. Select **SSU PCP** node.
4. In the **PCP** tab, click the **Credential Store** tab.
5. In the **General** area, in the **Key** field, enter the key whose existence you want to check.

6. Click **Contains Key?**.

   The message which informs you whether the key exists, appears.

7. To close the message, click **OK**.

To delete a a specified key from the credential store:

- In the **Credential Store** tab, in the General area, in the Key field, enter the key and then click **Delete Key**.

To delete a all keys from the credential store:

- In the **Credential Store** tab, in the General area, click **Delete All Keys**.

Defining PCP Network

To define a PCP network entity:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SSU PCP** node.

   The PCP SSU configuration pane appears. This pane displays a table listing PCP network entities. Each row represents one PCP network entity.

4. To define a new PCP network, at the bottom of the PCP SSU configuration pane, click the **New** button.

   The New dialog box appears.

5. Fill in the fields described in Table 7–5.

Table 7–5 PCP SSU Parameters

Field	Description
Name	A unique name that you give to the PCP network entity.
Alias	An alias that you assign to the PCP network entity. IMs use this alias to specify the destination of PCP requests. If two or more PCP network entities belong to the same BRM application, you assign the same alias to all of them. The PCP SSU distributes requests among network entities having the same alias. For information on how to use the alias in IMs, see ■ The discussion on setting up IM-OCF PCP in *Oracle Communications Service Broker Modules Configuration Guide* ■ The discussion on setting up IM-OFCF PCP in *Oracle Communications Service Broker Modules Configuration Guide*
Weight	Specifies the relative load weight for the network entity. Default value: 0
Connection Pool ID	The identifier of the connection pool used to communicate with the remote PCP network entity. This should be one of the connection pools that you have previously defined. See "Defining Connection Pools"
Heartbeat	Specifies whether the PCP SSU activates the heartbeat mechanism over the connection with the network entity.

Table 7–5 (Cont.) PCP SSU Parameters

Field	Description
Response Timeout	The time interval, in seconds, during which the PCP SSU waits for a response from the network entity. If the PCP SSU does not receive a response within this time interval, then it considers the network entity inactive.
Active Interval	The time interval, in seconds, between two consecutive heartbeat requests sent to the network entity. This time interval is valid so long the network entity is considered active.
Inactive Interval	The time interval, in seconds, between two consecutive heartbeat requests sent to the network entity. This time interval is valid so long the network entity is considered inactive.

8

Configuring a ECE Signaling Server Unit

This chapter describes how to configure an Oracle Communications Service Broker Elastic Charging Engine (ECE) Signaling Server Unit (SSU) using the Administration Console.

About the ECE SSU

Service Broker acts as a client application using the ECE SSU to communicate with the ECE client API. The ECE SSU relays charging requests from internal Service Broker components, such as IM-OFCF ECE and IM-OCF ECE, and routes these request to ECE using the API.

The ECE SSU distributes messages among different network entities that share the same alias using the weighted load strategy. This strategy determines a network entity that receives a message based on the weight that you assign to the entity. The weight determines a relative share of the traffic that the network entity should receive.

For example, you defined two entities whose weight is 100 and 200 correspondingly. The network entity with the weight of 100 receives 1/3 of the traffic, while the network entity with the weight of 200 receives the remaining 2/3 of the traffic. If a network entity fails, the ECE SSU redistributes the traffic among remaining networking entities according to their weight.

You can define a network entity that receives traffic if other network entities whose weight is greater than zero, fail. This entity is known as secondary network entity, and its weight is always zero. If in the example above, you add one more entity whose weight is set to zero, the ECE SSU sends messages to this network entity only if the network entities whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple network entities with secondary priority, the ECE SSU distributes traffic equally among them.

The weighted load strategy enables you to control the traffic distribution depending on capabilities of network entities. For example, if a network entity runs a more powerful server, this entity can serve more traffic, then you would set its load weight relatively higher.

The ECE SSU implements a heartbeat mechanism, regularly sending requests to ECE network entities to check their availability. Not receiving a response within a configured time interval denotes that the ECE network entity is inactive. The ECE SSU stops sending requests to inactive network entities, but continues checking their availability every few seconds. You configure the heartbeat mechanism for each ECE network entity separately, when you define the network entity.

Configuring ECE Transactions

To connect Service Broker to ECE:

1. In the Administration Console:
   a. In the navigation tree, expand the **OCSB** node, and then the **Signaling Tier** node.
   b. Select the **SSU ECE** node.
   c. In the **ECE** tab, select the **Coherence** tab.
2. Populate the ECE Protocol Adapter values listed in Table 8–1 used to connect to the ECE OCS:

Table 8–1 ECE OCS Configuration Parameters

Name	Type	Description
Coherence Cluster Name	String	Specifies the name for the ECE cluster to join.
JMX Management read-only	Boolean	Specifies whether the MBeans exposed by this cluster node allow operations that modify run-time attributes.
Coherence Log File Name	String	Specifies the name of the Coherence log file.
Coherence Log Level	Integer	Specifies which logged messages will be output to the log destination.
Use ECE Well Known Address	Boolean	Specifies whether to use the ECE OCS Well Known Address.
Well Known Address 1 (ip:port)	String	Specifies the first Well Known Address of the ECE cluster if Multicast networking is not in use.
Well Known Address 2 (ip:port)	String	Specifies the second Well Known Address of the ECE cluster if Multicast networking is not in use.
Multicast Address (ip:port)	String	The multicast address and port of the ECE OCS.
Multicast TTL	Integer	Specifies the time to live for multicast packets.

For information about the ECE Coherence configuration values, see *Oracle Communications Elastic Charging Engine Administrator's Guide*.

For information about Oracle Coherence, see the Oracle Coherence Knowledge Base Home at:

`http://coherence.oracle.com/display/COH/Oracle+Coherence+Knowledge+Base+Home`

3. Select the **General** tab to set the general parameters listed inTable 8–2:

Table 8–2 ECE OCS General Parameters

Name	Type	Description
Request Default Timeout	Integer	Specifies the default request timeout in milliseconds when no value is supplied by the outbound request. The default value is 2000 milliseconds.
ECE Request Batch Size	Integer	Specifies the number of ECE requests to send per request. The default value is 1.
ECE Request Batch Timeout	Integer	Specifies the ECE batch request timeout in milliseconds.

Table 8–2 (Cont.) ECE OCS General Parameters

Name	Type	Description
ECE Thread Pool Size	Integer	Specifies the number of ECE threads to use in the connection pool.
ECE Request Specification Override File	String	Specifies the path and file name of an override ECE request specification File. If the value is set, the specified file will be loaded instead of the default ECE request specification.

4. Click **Apply** to save the configuration.

Defining ECE Network Entities

To define a ECE network entity:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SSU ECE** node.

   The SSU ECE configuration pane appears.
4. To define a new ECE network, at the bottom of the **SSU ECE** configuration tab, click the **New** button.

   The New dialog box appears.
5. Fill in the fields described in Table 8–3.

Table 8–3 SSU PCP Configuration Parameters

Field	Description
Name	A unique identifier for the SSU ECE instance.
Alias	Specifies a name that Service Broker uses to refer the ECE network entity. The alias is a simple string.
ClusterName	The Oracle Coherence cluster name where ECE is hosted.
Weight	Defines the relative amount of traffic sent to the SSU ECE destination. See the discussion on Weight in "About the ECE SSU".
Heartbeat	Specifies whether to use a heartbeat mechanism over the connection with the ECE network entity to check the connection status.
Response Timeout	Specifies the time interval, in seconds, during which the ECE SSU waits for a response from the ECE network entity. The heartbeat mechanism uses this field.
Active Interval	Specifies the periodicity, in seconds, for sending heartbeat requests from the SSU ECE to the ECE network entity. This field is used if the previous heartbeat test results in an active ECE connection.
Inactive Interval	Specifies the periodicity, in seconds, for sending heartbeat requests from the SSU ECE to the ECE network entity. This field is used if the previous heartbeat test results in a inactive ECE connection.

Securing the ECE Connection with SSL

In production environments, Oracle recommends that you secure the Service Broker connection to ECE. Service Broker supports SSL connections to the ECE Coherence cluster when both systems are configured for secure communications. Consult your ECE Administrator for additional assistance in configuring SSL including host IP address(es) and port number(s).

To configure the Service Broker SSL connection to ECE:

1. Enable SSL on ECE setting the following property in the **ece.properties** file located in *ECE_Home*/**ocecеserver/config** on the ECE server host:

   ```
   tangosol.coherence.override=charging-coherence-override-secure-prod.xml
   ```

2. Oracle Coherence does not support the use of multicast addresses when using SSL for communication. A list of well known addresses (WKA) for ECE is configured during ECE installation.

   Add the Service Broker server host(s) IP address(es) to the list of well known addresses (WKA) in the **charging-coherence-override-secure-prod.xml file** within the appropriate authorized hosts lists section as shown:

   ```
   <!-- authorized hosts list -->
           <authorized-hosts>
               <host-address>192.168.0.111</host-address>
           </authorized-hosts>
   ```

3. Copy the **server.jks** file located in *ECE_Home*/**ocecеserver/config** from the ECE server into the *OCSB_Home*/**managed_server** directory of your Service Broker server. This file contains the encrypted ECE credentials specified during ECE installation used by Service Broker to authenticate with the ECE Coherence cluster.
4. Rename the **server.jks** file to **ece_server.jks** on the Service Broker server.
5. Configure the Service Broker Protocol Adapter to use the SSL-enabled ECE host(s) and port(s). See "Configuring ECE Transactions", for more information.
6. Add the ECE store and key passwords to the ECE Protocol Adapter Credential Store. See "Configuring the SSU ECE Credential Store", for more information.
7. Restart the Service Broker managed server configured for SSL communications with ECE.

Configuring the SSU ECE Credential Store

The SSU ECE must be configured with the ECE **Keystore** and **Certificate Store** passwords. Service Broker uses these credentials to securely connect to ECE over SSL. The passwords are created during ECE installation. Obtain the necessary credentials by consulting your ECE administrator and configure the SSU ECE Credential Store using the following instructions:

1. In the navigation tree in the domain navigation pane, expand the **OCSB** node.
2. Expand the **Signaling Tier** node.
3. Select the **SSU ECE** node.
4. In the **ECE** tab, select the **Credential Store** tab.
5. Create password entries for both the ECE Keystore and Certificate Store in the Password area using the fields and values described in Table 8–4:

Table 8–4 ECE Credential Store Passwords

Field	Descriptions
Key	Use the following Service Broker Key values: ■ **storepassword** ■ **keypassword**
Password	Use the following Password values: ■ Enter the **ECE Certificate store** password used during ECE installation for the **storepassword** credential. ■ Enter the ECE **Keystore Password** used during ECE installation for the **keypassword** credential. Consult your ECE Administrator for password information.
One-way	Always uncheck this box. The ECE SSU should be able retrieve the ECE passwords from the Credential Store and use it when sending requests to Oracle Communications ECE.

6. Click the **Set Password** button for each entry.

9

Configuring an SMPP Signaling Server Unit

This chapter describes how to configure an Oracle Communications Service Broker SMPP Signaling Server Unit (SSU) using the Administration Console.

About the SMPP SSU

Service Broker uses the SMPP SSU to communicate with Short Message System Centers (SMSCs) through the Short Message Peer-to-Peer protocol.

When configuring the SMPP SSU, you set up the following:

- SMPP network entities. See "About SMPP Network Entities" for more information.
- Incoming routing rules. See "About Incoming Routing Rules" for more information.
- SMSC connections. See "About SMSC Connections" for more information.
- Secure settings of SMSC connections. See "About Securing SMSC Connections" for more information.
- Password for the credential store. See "About Securing the Credential Store" for more information.

About SMPP Network Entities

SMPP network entities are SMSCs to which the SMPP SSU routes **submit_sm** messages generated by IM-UIX-SMS.

You set up rules that define the following:

- ID of the SMSCs to which the SMPP SSU routes the message
- Alias to be set in the IM-UIX-SMS configuration to route the message to the SMSC with a specified ID. To provide continuous operation in situations when an SMSC fails, you can map the same alias to multiple SMSCs. If one of the specified SMSCs fails, the SMPP SSU routes the message to another SMSC mapped to the same alias.
- Parameters of the heartbeat mechanism. Using this mechanism, the SMPP SSU regularly sends requests to an SMSC. If the SMPP SSU does not receive a response from the SMSC within the specified period, the SMPP SSU considers this SMSC inactive. The SMPP SSU does not send any further requests to this SMSC.

The SMPP SSU distributes messages among different SMPP network entities that share the same alias using the weighted load strategy. This strategy determines a network entity that receives a message based on the weight that you assign to the entity. The weight determines a relative share of the traffic that the network entity should receive.

For example, you defined two entities whose weight is 100 and 200 correspondingly. The network entity with the weight of 100 receives 1/3 of the traffic, while the network entity with the weight of 200 receives the remaining 2/3 of the traffic.

If a network entity fails, the SMPP SSU redistributes the traffic among remaining networking entities according to their weight.

You can define a network entity that receives traffic if other network entities whose weight is greater than zero, fail. This entity is known as secondary network entity, and its weight is always zero. If in the example above, you add one more entity whose weight is set to zero, the SMPP SSU sends messages to this network entity only if the network entities whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple network entities with secondary priority, the SMPP SSU distributes traffic equally among them.

The weighted load strategy enables you to control the traffic distribution depending on capabilities of network entities. For example, if a network entity runs a more powerful server, this entity can serve more traffic, then you would set its load weight relatively higher.

See "Configuring SMPP Network Entities" for more information.

About Incoming Routing Rules

Incoming routing rules define the IM-UIX-SMS instance to which the SMPP SSU routes a **deliver_sm** message received from the SMSC. For each rule, you define the following parameters:

- Conditions:
  - Destination address
  - Service Type
- Alias of the IM-UIX-SMS instance to which the SMPP SSU routes the message if both conditions are met

See "Configuring Incoming Routing Rules" for more information.

About SMSC Connections

To route a **submit_sm** message to an SMSC, you set up connection between the SMPP SSU and SMSCs. Setting up a connection requires configuration of the following parameters:

- General parameters, which define parameters which are common for all connections to SMSCs.
- SMSC connection parameters, which define settings required for each connection. When setting up a connection, you map SMSC IDs specified in SMPP Network Entities, to physical addresses of SMSCs.

See "Configuring SMSC Connections" for more information.

About Securing SMSC Connections

When communicating with SMSCs, Service Broker acts as an External Short Messaging Entity (ESME). A connection between an ESME and SMSC can be established if the ESME provides a proper password. To specify a password for a connection, you need to define the following:

- In the credential store, you specify a password for the connection between Service Broker and SMSC. In addition, you specify a key under which Service Broker stores this password in the credential store.
- When you set up a connection with an SMSC, you do not specify a password directly. Instead, in the **ESME Credential Key** parameter, you provide the credential store's key that you associated with the required password. See "Setting Up Connection Pools" for more information.

About Securing the Credential Store

You use the Credential Store to securely store, encrypt, and validate the credentials that Service Broker uses to communicate with SMSCs. For more information about how the Credential Store works and how you configure credentials, see a discussion on administering Credential Stores in *Oracle Communications Service Broker Security Guide*.

Configuring SMPP Network Entities

To configure SMPP network entities:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SMPP SSU** node.
4. In the SMPP SSU configuration pane, click the **SSU SMPP** tab and then the **SMPP Network Entities** subtab.

   The SMPP Network Entity configuration pane appears. This pane displays a table. The table contains rules that define to which SMSC the short message is routed. Each row in the table represents a single rule.
5. To create a new rule, at the bottom of the SMPP Network Entities configuration pane, click **New**.

   The New dialog box appears.
6. Fill in the fields described in Table 9–1.

Table 9–1 SMPP Network Entities Parameters

Field	Descriptions
Name	Specifies the name of the rule.

Table 9–1 (Cont.) SMPP Network Entities Parameters

Field	Descriptions
Alias	Specifies the SIP URI of the IM to which the SMPP SSU routes an incoming session. The alias has the following format: `SSU:`*IM-instance-name*.*IM-type*@*domain-id* ■ *IM-instance-name*: IM instance name you specified when you added this IM in the IM configuration pane. ■ *IM-type*: Type of IM instance. ■ *domain-id*: Name of the Processing Domain or Processing Domain Group where the relevant IM or application is deployed. This parameter is required only when your Service Broker deployment includes two or more Processing Domains. Use the name given to the domain when it was created. This name is specified by the axia.domain.id property. Example: `ssu:im_uix-sms.IMUIXSMS@processing-domain.1` *domain-id* is required only if your deployment includes two or more Processing Domains. To provide continuous operation in situations when an SMSC fails, you can map the same alias to multiple SMSCs. If one of the specified SMSCs fails, the SMPP SSU routes the message to another SMSC mapped to the same alias.
Weight	Specifies the relative load weight for the network entity. Default value: 0
Heartbeat	Specifies whether the SMPP SSU uses the heartbeat mechanism to regularly check whether the SMSC is active. Possible values: ■ ON ■ OFF Default value: ON
SMSC Identifier	Specifies the ID of the SMSC to which the SMPP SSU routes the **submit_sm** message if the value of the Default SMSC Alias parameter set in the IM-UIX-SMS configuration and the value of the Alias parameter match.
Response Timeout	Specifies the time interval, in seconds, during which the SMPP SSU waits for a response from the SMSC. If the response timeout expires, and the SMPP SSU still does not receive a response, the SMPP SSU considers the SMSC inactive.
Active Interval	Specifies the time interval, in seconds, for sending heartbeat requests from the SMPP SSU to the SMSC. This field is used if the previous heartbeat test showed that the SMSC is active.
Inactive Interval	Specifies the time interval, in seconds, for sending heartbeat requests from the SMPP SSU to the SMSC. This field is used if the previous heartbeat test showed that the SMSC is inactive.

7. Click **Apply**.

Configuring Incoming Routing Rules

To configure incoming routing rules:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SMPP SSU** node.

   The SMPP SSU configuration pane appears.
4. In the SMPP SSU configuration pane, click the **SSU SMPP** tab and then the **Incoming Routing Rules** subtab.

   The Incoming Routing Rules configuration pane appears. This pane displays a table. The table contains rules that define to which instance of IM-UIX-SMS the **deliver_sm** message is routed. Each row in the table represents a single rule.
5. To create a new rule, at the bottom of the Incoming Routing Rules configuration pane, click **New**.

   The New dialog box appears.
6. Fill in the fields described in Table 9–2.

Table 9–2 Incoming Routing Rules Parameters

Field	Descriptions
Name	Specifies the name of the rule.
SMPP Destination Address	Specifies the destination address to be set in the **deliver_sm** message.
Service Type	Specifies the service type to be set in the **deliver_sm** message.
Alias	Specifies the alias of the IM-UIX-SMS instance. The SMPP SSU routes the **deliver_sm** message to this instance if the destination address and service type set in the **deliver_sm** message match the values set in SMPP Destination Address and Service Type parameters.

7. Click **Apply**.

Configuring SMSC Connections

You need to configure the following:

- General parameters. See "Configuring General Parameters" for more information.
- Connection pools. See "Setting Up Connection Pools" for more information.

Configuring General Parameters

To configure general parameters:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SMPP** node.
4. In the SMPP configuration pane, click the **SMPP** tab and then the **General** subtab.
5. Fill in the fields described in Table 9–3.

Table 9–3 General Parameters

Field	Descriptions
protocolVersion	Specifies the version of the SMPP protocol that the SMPP SSU uses to communicate with SMSCs.
eventTimeoutMs	Specifies the timeout for an incoming event in milliseconds. Default value: 10000

6. Click **Apply**.

Setting Up Connection Pools

To configure connection parameters:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand the **Signaling Tier** node.
3. Select the **SMPP** node.
4. In the SMPP configuration pane, click the **SMPP** tab and then the **SMSC** subtab.
5. Fill in the fields described in Table 9–4.

Table 9–4 SMSc Connections Parameters

Field	Descriptions
SMSC Identifier	Specifies the ID of the SMSC for which you set up a connection. The value that you specify in this parameter must correspond to the SmscId parameter which you set in the SMPP Network Entities configuration.
SMSC Address	Specifies the host name or IP address of the SMSC to which the SMPP SSU routes a **submit_sm** message.
SMSC Port	Specifies the port of the SMSC to which the SMPP SSU routes a **submit_sm** message.
ESME System ID	Specifies the ID of the External Short Messaging Entity (ESME) that the SMPP SSU uses to bind to the SMSC.
ESME Credential Key	Specifies the key that the SMPP SSU uses to retrieve the ESME password from the credential store.
ESME System Type	Specifies the type of the ESME system that the SMPP SSU uses to bind to the SMSC.
ESME Address Ton	Specifies the Type Of Number of the ESME address that the SMPP SSU uses to bind to the SMSC.
ESME Address NPI	Specifies the Numbering Plan Indicator of the ESME address that the SMPP SSU uses to bind to the SMSC.
ESME Address Range	Specifies the range of the ESME address that SMPP SSU uses to bind to the SMSC. Default value: .*
Local Address	Specifies the local address (hostname or IP) used to connect to the SMSC. To use any address, leave this parameter empty.

Table 9–4 (Cont.) SMSc Connections Parameters

Field	Descriptions
ESME Port	Specifies the local TCP port used to connect to the SMSC. Use -1 for any port. Default value: -1
Bind Type	Specifies the type of connection to the SMSC. Possible values: ■ TRANSCEIVER ■ TRANSMITTER ■ RECEIVER Default value: TRANSCEIVER
Connection Pool Size	Specifies the size of the connection pool. Default value: 1
Connection Timer (sec)	Specifies the time, in seconds, that the SMPP SSU waits between connection attempts to the SMSC. Default value: 30
Request Timeout (ms)	Specifies the period, in milliseconds, that the SMPP SSU waits to consider the request timed out. Default value: 10000
Enquire Link Timer (sec)	Specifies the frequency, in seconds, with which the SMPP SSU sends a Enquire Link PDU on each SMSC connection. To disable sending a Enquire Link PDU, enter 0. Default value: 30
Window Size	Specifies the maximum number of pending requests for each TCP connection. To disable limitation, enter 0. Default value: 0
Connection Acquire Timeout (ms)	Specifies the timeout, in milliseconds, that the SMPP SSU waits for an available connection when no connections are currently available. This parameter is applicable only when the value of the windowSize parameter is greater than 0. Default value: 1000
Target	Specifies the name of the managed server to which this configuration applies. If you leave this parameter empty, the configuration applies to all managed servers.

10

Configuring the Web Services Signaling Server Unit

This chapter describes how to configure an Oracle Communications Service Broker Web Services Signaling Server Unit (SSU) using the Administration Console.

About the Web Service SSU

The Web Services SSU enables Service Broker Processing Tier components to communicate with external entities using SOAP or REST over HTTP. Service Broker can act as a Web services server or client to external entities through the Web Services SSU.

In general, you control Web service traffic through the Service Broker Signaling Tier using the following Web Services SSU components:

- Incoming routing rules, which map a request URL addressed by an incoming request to an internal service or IM.
- Outgoing routing rules, which specify external Web services to which Service Broker sends service requests.
- HTTP network access points, which specify connection-level settings for the Web services communications, such as the port on which Service Broker listens for HTTP traffic and security settings for connections.
- Specific settings for SOAP-based or REST-based HTTP connections.

The Processing Tier components that rely on the Web Services SSU are the Web Services IM (WS-IM) and Service Broker applications, such as Top Up or Subscriber Provisioning. These applications expose SOAP APIs that clients use to configure and manage their services.

Enabling access to the SOAP APIs involves the following general configuration steps:

1. Opening an HTTP listening port in the Web Services SSU configuration.
2. Configuring SSL security or authentication requirements for the connection.
3. Configuring an incoming routing rule that directs incoming client requests to the Web Service endpoint within Service Broker.

This chapter provides information about configuring the Web Services SSU. For more information about a particular SOAP API, see the implementation guide applicable to the Service Broker application, such as *Service Broker Subscriber Store User's Guide*.

The following procedures describe how to perform a task in the Administration Console.

Configuring Incoming Routing Rules

You use the **Incoming Routing Rules** tab to define how the Web Services SSU routes incoming Web service messages to internal Service Broker IMs and other applications.

To configure incoming routing rules for Web service messages:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Expand the **SSU Web Services** node.
4. Click the **General** item.
5. In the **SSU WS** tab, click the **Incoming Routing Rules** tab.

   The Incoming Routing Rules pane contains a table in which each row represents one Web services endpoint.
6. Click the **New** button.

   The New dialog box appears.
7. In the dialog box, provide values for the fields listed in Table 10–1.

Table 10–1 Web Services Incoming Routing Rules Parameters

Field	Description
Name	A unique name for the routing rule.
Service Name	The service name of the Service Broker Web service endpoint. Setting this field to **Any** causes all incoming web service messages to be routed to the specified module instance. This value is generally used to create a rule that routes incoming Web services messages to a default IM in the absence of a more specific routing rule. For the incoming routing rules for Service Broker applications that expose SOAP APIs, use the following service names: ▪ **BalanceManagerService**: Use for the routing rule for the Top Up and Balance Manager API service. ▪ **SubscriberProvisioning**: Use for the routing rule for the Subscriber Provisioning API service.

Table 10–1 (Cont.) Web Services Incoming Routing Rules Parameters

Field	Description
Alias	A logical name that specifies the Service Broker IM or application to which the Web Services SSU routes an incoming Web services message. The format differs depending upon whether you are routing to an internal service or an IM. The alias has the following format for IMs: **ssu:***IM_instance_name.IM_type@domain_id* The alias has the following format for internal service: **ssu:***domain_Id/application_id* Where: ■ *IM_instance_name*: Name of the destination IM instance. This is the IM name you specified when you added this IM in the IM configuration pane. ■ *IM_type*: Type of the destination IM instance. ■ *domain-id*: Name of the Processing Domain or Processing Domain Group where the relevant IM or application is deployed. This parameter is required only when your Service Broker deployment includes two or more Processing Domains. Use the name given to the domain when it was created. This name is specified by the axia.domain.id property. ■ *application_id*: Name of the destination Service Broker application. This is a static name assigned to each Service Broker application. This is **topup** for the Balance Manager API service and **provisioning** for the Subscriber Provisioning API service. For the Service Broker SOAP API services, use the following alias values (given the default domain ID of **ocsb**): ■ **ssu:ocsb/topup**: The alias for the Balance Manager API service. ■ **ssu:ocsb/provisioning**: The alias for the Subscriber Provisioning API service.

8. Click **OK** to save the new incoming routing rule configuration.

Configuring Outgoing Routing Rules

You use the **Outgoing Routing Rules** tab to define how the Web Services SSU routes outgoing Web service messages to external Web service endpoints.

In the rule, you specify the address of each external Web service endpoint and assign an alias to each endpoint. IMs and Service Broker applications use the alias to refer to an external Web service destination.

The Web Services SSU distributes messages among different Web service endpoints that share the same alias using the weighted load strategy. This strategy determines a Web service endpoint that receives a message based on the weight that you assign to the endpoint. The weight determines a relative share of the traffic that the Web service endpoint should receive. For example, you defined two endpoints whose weight is 100 and 200 correspondingly. The endpoint with the weight of 100 receives 1/3 of the traffic, while the endpoint with the weight of 200 receives the remaining 2/3 of the traffic.

If a Web service endpoint fails, the Web Services SSU redistributes the traffic among remaining Web service endpoints according to their weight.

You can define a Web service endpoint that receives traffic if other endpoints whose weight is greater than zero, fail. This endpoint is known as secondary Web service endpoint, and its weight is always zero. If in the example above, you add one more endpoint whose weight is set to zero, the Web Services SSU sends messages to this endpoint only if the endpoints whose weight is set to 100 and 200 correspondingly, fail.

If you define multiple Web service endpoints with secondary priority, the Web Services SSU distributes traffic equally among them.

The weighted load strategy enables you to control the traffic distribution depending on capabilities of Web service endpoints. For example, if a Web service endpoint runs a more powerful server, this endpoint can serve more traffic, then you would set its load weight relatively higher.

To configure outgoing routing rules for Web service messages:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Expand the **SSU Web Services** node.
4. Click the **General** tab.
5. In the **SSU WS** tab, click the **Outgoing Routing Rules** tab.

   The Outgoing Routing Rules pane contains a table in which each row represents one Web services endpoint.
6. Click the **New** button.

   The New dialog box appears.
7. In the dialog box, provide values for the fields listed in Table 10–2.

Table 10–2 Web Services Outgoing Routing Rules Parameters

Field	Description
Name	A unique routing rule name.
Alias	A logical name that you assign to the Web services endpoint.
Web Service URI	The Uniform Resource Identifiers (URI) used to address the Web services endpoint. The format of the address is similar to Web Uniform Resource Locators (URLs). For example: **http://webservices.example.com/eventnotification**
Weight	Specifies the relative load weight for the Web service endpoint. Default value: 0
Heartbeat	Whether the Web Services SSU periodically checks the Web services endpoint availability. Select **ON** to activate periodic availability check, or **OFF** to disable it.
Hearbeat Method	The HTTP method used to check endpoint availability. Service Broker supports the **GET** only. If the Heartbeat field to **OFF** this field is ignored.
Response Timeout	The amount of time, in seconds, Service Broker waits for a response from the Web services endpoint before the endpoint is considered unavailable. If the Heartbeat field to **OFF** this field is ignored.

Table 10–2 (Cont.) Web Services Outgoing Routing Rules Parameters

Field	Description
Active Interval	The amount of time, in seconds, between consecutive endpoint availability checks if the last availability check showed that the endpoint was available.
Inactive Interval	The amount of time, in seconds, between consecutive endpoint availability checks if the last availability check showed that the endpoint was unavailable.

8. Click **OK** to save the new outgoing rule configuration.

Configuring HTTP Access Settings

To enable HTTP connections between Service Broker and external entities, you must configure the HTTP connection settings in the Web Services SSU.

The HTTP connection settings specify the port on which Service Broker listens for HTTP requests, timeout settings, security requirements, and general connection settings.

Configuring HTTP Server General Settings

The general HTTP server settings apply to connections to Service Broker through the Web Services SSU that are initiated by an external client.

To specify general timeout settings:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Expand the **SSU Web Services** node.
4. Click the **General** item.
5. Click the **HTTP** tab.

   The General configuration pane under the Server subtab appears.
6. Set the value of the **Timeout** field to the maximum number of milliseconds that Service Broker can use to process a request. If this time expires, Service Broker returns an error response to the client.

   Set to any value from 1000 and 60000. The default is 30000.
7. Click **Apply** to save your change.

Configuring HTTP Server Network Access Settings

The network access point specifies the port on which the Web Services SSU listens for HTTP traffic, including HTTP traffic in the form of SOAP and REST messages.

To configure HTTP server network access settings:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Expand the **SSU Web Services** node.
4. Click the **General** item.

5. Click the **HTTP** tab.
6. In the **Server** subtab, click the **Network Access** subtab.
7. Click the **New** button.

   The New dialog box appears.
8. In the dialog box, provide values for the fields listed in Table 10–3.

Table 10–3 HTTP Network Access Parameters

Field	Description
Server Address	The local IP address or hostname bound to this HTTP listener.
Server Port	An available port number on which the Signaling Server listens for HTTP traffic. Be sure to avoid entering a port number already in use by the system.
Protocol	The protocol used for the port, either **HTTP** or **HTTPS** for Secure HTTP.
SSL Client Auth	Whether to enable SSL client authentication for this access point. Set to **true** to enable SSL client authentication. Enable SSL client authentication only if this network access point uses HTTPS protocol. If enabled, clients attempting to connect to this access point must present a client certificate that matches one in the truststore. Set to **false** to disable SSL client authentication. For more information on security, see *Service Broker Security Guide*.
Keystore ID	The identifier of the security keystore for the connection in the Credential Store. Only applicable if this network access point uses HTTPS. See *Service Broker Security Guide* for more information on using the Credential Store.
Truststore ID	The identifier of the security truststore in the Credential Store. Only applicable if this network access point uses HTTPS. See *Service Broker Security Guide* for more information on using the Credential Store.
Target	The target Signaling Server to which this configuration applies. If empty, it applies to all servers.

9. Click **OK** to save the new HTTP access configuration.

Creating or Modifying HTTP Server Security Contexts

You use the Security Context tab to apply authentication requirements to the resources exposed by Service Broker through the Web Services SSU. When authentication is required, Service Broker validates the credentials provided in incoming requests.

Note: The HTTP server security context applies HTTP Basic Authentication or HTPP Digest Authentication requirements to requests. Alternatively, you can require credentials in the form of Web Service Security (WSSE) UsernameToken credentials. See "Authenticating SOAP Requests with WSSE UsernameToken Credentials" for more information.

You associate a security requirement to a resource by configuring a security context by URI path.

For instance, the default REST root URI context is exposed at **/rest**. If HTTP Basic Auth is enabled for this address, any resource available under the REST root URI (such as **/rest/subscriber**) has the same requirement, unless a more specific security context applies to it.

To configure a security context for HTTP access:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Expand the **SSU Web Services** node.
4. Click the **General** item.
5. Click the **HTTP** tab.
6. In the **Server** subtab, click the **Security Context** subtab.
7. In the Security Context pane, you can either:
   - Click **New** to create a new context.
   - Select an existing context in the list and click **Update** to modify its values.
8. In the dialog box, provide values for the fields listed in Table 10–4.

Table 10–4 HTTP Security Context Parameters

Field	Description
Context URI	The URI to which the security requirement applies.
Auth Method	The authentication method applied to the resource. Options are: ■ **NONE**: No authentication is required. ■ **BASIC**: HTTP Basic Authentication is required to access the resource. ■ **DIGEST**: HTTP Digest Authentication is required to access the resource.
Realm	The security realm value to be presented to clients who do not provide credentials.
Username	The required user name to be included in the requests.
Credential Key	A key that identifies the credential in the Credential Store. This key is a name for the credential provided when loading the password associated with the user in the Credential Store. See *Service Broker Security Guide* for more information on the Credential Store.

9. Click **OK** to save the new security context configuration.

Configuring HTTP Client Settings

The HTTP client settings apply to outgoing connections. In this case, Service Broker acts as a client to external HTTP servers through the Web Services SSU.

To configure HTTP client settings:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.

3. Expand the **SSU Web Services** node.
4. Click the **General** item.
5. Click the **HTTP** tab.
6. Click the **Client** tab.
7. Modify, if required, the default settings for the outgoing connection listed in Table 10–5.

Table 10–5 HTTP Client Parameters

Field	Description
Connect Timeout	The amount of time, in milliseconds, Service Broker allows for establishing an HTTP connection to a remote server. If the timeout expires before receiving data, the connect attempt is abandoned. The default value is 50000 milliseconds. Value must be from 1000 to 60000.
Read Timeout	The amount of time, in milliseconds, Service Broker allows for reading data from a remote server on the established connection. If the timeout expires, the read attempt is aborted. The default value is 30000 milliseconds. Value must be from 1000 to 60000.

8. Click **Apply** to save your changes to the configuration.

Configuring SOAP Web Service Access

As an HTTP-based protocol, SOAP is subject to the common HTTP connection settings configured in the HTTP tab. These include, for example, the port on which Service Broker listens for HTTP traffic, Basic Authentication security, and so on. See "Configuring HTTP Access Settings" for information on configuring common HTTP access settings.

In addition, you can configure specific settings that apply to SOAP-based communication with external SOAP clients or servers.

Configuring SOAP Server Settings

The SOAP server settings apply to client connections to Service Broker in which Service Broker acts as the Web Service provider or server front-end. These include connections made to the Subscriber Profile API and Balance Manager API services.

To enable the SOAP services, you must configure HTTP access settings. You can then configure specific settings for SOAP access as described in this section.

Configuring Common SOAP Server Settings

To configure general SOAP access settings:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Expand the **SSU Web Services** node.
4. Click the **General** item.
5. Click the **SOAP** tab.

The Server settings pane appears.

6. Verify and, if required, modify the default settings listed in Table 10–6.

Table 10–6 SOAP Server Parameters

Field	Description
Root URI	The path root for the SOAP API services provided by Service Broker. The default is **/soap**. Together with the service location, this root path forms the complete URI for accessing the SOAP resource at the Service Broker Signaling Domain. For example, given the default path for the root URI and Subscriber Provisioning service, the full path would be: https://*hostname*:*port*/soap/SubscriberProvisioning
Timeout	The maximum amount of time, in milliseconds, Service Broker may take to generate a response before returning an error response to the client. The default value is 10000 milliseconds. Values can be from 1000 to 60000.

7. Click **Apply** to save your changes to the configuration.

Configuring the URI Path for a Specific SOAP Service

To view or change the URI path of a SOAP service, follow these steps:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Expand the **SSU Web Services** node.
4. Select the name of the service for which you want to modify the existing URI path, either **Subscriber Provisioning** or **Balance Manager**.
5. In the **End Point** tab, click the URI context for the service.
6. Click the **Update** button.
7. Set the **URI** field to the value of the new path. The path value should be preceded by a slash character, as in the default value.

   By default, this is **/SubscriberProvisioning** for the Subscriber Provisioning SOAP service, and **/BalanceManagerService** for the Balance Manager SOAP service. Together with the root URI path, this path makes up the URI at which clients address the SOAP service.
8. Click **OK**.

See "Authenticating SOAP Requests with WSSE UsernameToken Credentials" for information on configuring the authentication fields for the SOAP service.

Configuring SOAP Client Parameters

The SOAP client settings apply to outgoing connections. In this case, Service Broker acts as a client to external SOAP Web service providers.

To configure SOAP client settings:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.

2. Expand **Signaling Tier**.
3. Expand the **SSU Web Services** node.
4. Click the **General** item.
5. Click the **SOAP** tab.
6. Click the **Client** subtab.
7. Enter values for the fields listed in Table 10–7.

Table 10–7 SOAP Client Parameters

Field	Description
Connect Timeout	The amount of time, in milliseconds, Service Broker allows for establishing a connection to a remote server. If the timeout expires before Service Broker establishes the connection, the connect attempt is abandoned. The default value is **5000**. Values can be from 1000 to 60000. To disable time outs, set this value to **0**.
Read Timeout	The amount of time, in milliseconds, Service Broker allows for reading data from a remote server on an established connection. If the timeout expires, the read attempt is aborted. The default value is **30000**. Values can be from 1000 to 60000. To disable time outs, set the value to **0**.

8. Click **Apply** to save your changes to the configuration.

Authenticating SOAP Requests with WSSE UsernameToken Credentials

Service Broker can authenticate incoming SOAP requests that contain WSSE UsernameToken credentials, as specified by OASIS UsernameToken Profile 1.0. For general information on WSSE UsernameToken, see the OASIS Web Service Security specifications at:

`http://www.oasis-open.org/`

You enable WSSE UsernameToken credential requirement by SOAP service. That is, it can be enabled for the Subscriber Provisioning service and disabled for the Balance Manager service, for example.

A service that requires WSSE UsernameToken authentication should not be configured to require an HTTP Basic Authentication credential as well. See "Creating or Modifying HTTP Server Security Contexts" for more information about HTTP Basic Authentication security contexts.

Service Broker validates the WSSE UsernameToken credential against credentials stored in the Service Broker Credential Store. Before configuring service authentication as described below, add the credential to be authenticated to the Credential Store. See *Service Broker Security Guide* for information about the Credential Store.

To apply WSSE UsernameToken credential authentication to incoming SOAP service requests, follow these steps:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Expand the **SSU Web Services** node.
4. Click the **General** item.

5. Click the **SOAP** tab.
6. Click the **Credential Store** subtab.
7. In the **Key** field, enter an alias for the credential.
8. In the **Password** field, enter the password value for the credential.
9. Verify that HTTP Basic Authentication is disabled for the underlying HTTP security context for the SOAP service as follows:
   a. Click the **HTTP** tab under the SSU Web Services node.
   b. In the **Server** subtab, click the **Security Context** subtab.
   c. Verify that the **Auth Method** value is **NONE** for the Context URI path applicable to the Web service. By default, the context path for all SOAP Web services exposed by Service Broker is **/soap**.
   d. If necessary, select the security context item and click the **Update** button to change the Auth Method.
10. Under the **OCSB** navigation tree, expand, if necessary, the **Signaling Tier** node and then the **SSU Web Services** node.
11. Click the name of the service for which you want to require WSSE UsernameToken authentication, either **BALANCE MANAGER** or **SUBSCRIBER PROVISIONING**.
12. In the End Point tab, click the URI context for the service.
13. Click the **Update** button.
14. For the **Authentication Method** value, choose **USERNAME_TOKEN**.
15. For the **Username** value, enter the user name portion of the credential to be authenticated by WSSE UsernameToken authentication.
16. For the **Credential Key** value, enter the credential alias you used when storing the password to be validated into the Credential Store.
17. Click **OK** to save your changes to the configuration.

Clients of the service must submit valid WSSE UsernameToken credentials with their service requests.

Configuring REST Web Service Access

As an HTTP-based protocol, REST-based communication is subject to the common HTTP connection settings configured in the HTTP tab. These include, for example, the port on which Service Broker listens for HTTP traffic, Basic Authentication security, and so on. See "Configuring HTTP Access Settings" for information on configuring common HTTP access settings.

In addition, you can configure specific settings that apply to REST-based communication with external REST clients or servers.

Configuring REST Server Parameters

The REST server settings apply to client connections made to Service Broker in which Service Broker acts as the server or server front-end for a REST API service.

To configure REST server settings:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.

2. Expand **Signaling Tier**.
3. Expand the **SSU Web Services** node.
4. Click the **General** item.
5. Click the **REST** tab.
6. In the **Server** tab, verify and, if required, modify the default settings listed in Table 10–8.

Table 10–8 REST Server Parameters

Field	Description
Root URI	The URI path at which Service Broker exposes REST APIs. This path value forms the root of the address that clients use to access REST resources. For example, given the default path of **/rest**, the full address of a REST resource would be: https://*hostname*:*port*/rest/subscriber/carol
Timeout	The amount of idle time, in milliseconds, after which Service Broker releases a client connection on which it is awaiting data. The default value is 10000 milliseconds. Values can be from 1000 to 60000. To disable timeout, set the timeout to **0**.

7. Click **Apply** to save your changes to the configuration.

Configuring REST Client Parameters

The REST client settings apply to outgoing connections. In this case, Service Broker acts as a client to external REST Web service providers.

To configure REST client settings:

1. In the navigation tree in the domain navigation pane, expand **OCSB**.
2. Expand **Signaling Tier**.
3. Expand the **SSU Web Services** node.
4. Click the **General** item.
5. Click the **REST** tab.
6. Click the **Client** subtab.
7. Verify and, if required, modify the default settings listed in Table 10–9.

Table 10–9 REST Client Parameters

Field	Description
Connect Timeout	The amount of time, in milliseconds, Service Broker allows to establish a connection to a remote server. If the timeout expires before receiving data, the connection attempt is abandoned. The default value is **5000**. Values can be from 1000 to 60000. To disable timeout, set the timeout to **0**.
Read Timeout	The amount of time, in milliseconds, Service Broker allows for reading data from a remote server on an established connection. If the timeout expires, the read attempt is abandoned. The default value is 30000 milliseconds. Values can be from 1000 to 60000. To disable timeout, set the timeout to **0**.

8. Click **Apply** to save your changes to the configuration.