STARSOLUTIONS™

All-IP GSM

Sonata® Core Voice Network

GSM-R4.5.2
Mobile Switching Center Server Provisioning Guide

Part Number D01140 Rev A0

All-IP GSM

Sonata® Core Voice Network

GSM-R4.5.2
Mobile Switching Center Server Provisioning Guide

Part Number D01140 Rev A0

STARSOLUTIONS™

Contents

About This Guide

Part I Getting Started

1 MSC Server Overview

2 Accounts and Tools Used in Provisioning

7 SS7 Signaling Connection Control Part

8 SS7 Transaction Capability Application Part

9 SS7 Mobility Application Part

10 CAMEL APPLICATION PART

PART V MOBILITY

11 CONFIGURING THE VISITOR LOCATION REGISTER

12 Adding a TDM-based Base Station Controller

Part VI Trunks

13 Adding and Removing ISUP Trunks

14 Adding and Removing CAS Trunks

21 Interfacing to Another MSC for IP Inter-MSC Trunking

22 Interfacing to an SMS-AS for Welcome SMS Messaging

Part VIII Call Processing

23 Call Processing Provisioning Overview

24 Classes of Service

25 Translations and Routing

26 Call Progress

27 Treatment

28 Tones and Announcements

About This Guide

This guide explains how to configure the Sonata Mobile Switching Center Server (MSC) to support a variety of network elements and services, including base station controllers, media gateways, trunk groups, and SS7 network elements such as Home Location Registers (HLRs) and Service Control Points (SCPs).

This guide is intended for people who design, provision, and configure telecommunications systems and services. It assumes background knowledge of wireless GSM networks, telephone network technologies, Internet Protocol (IP) telephony, and the Sun Solaris operating system. Readers also need knowledge of the target network topology and system administrator privileges.

About This Guide contains:

Release notes are issued with this product. If the information in the release notes differs from the information in this guide, follow the instructions in the release notes.

Guide Structure

This guide begins by presenting an MSC overview and provisioning fundamentals, then proceeds with adding a Media/Signaling Gateway (GW). Many of the following chapters require a GW to be installed. This is followed by details of the MSC's internal message routing structure and the SCCP and higher layers of the SS7 protocol stack. Mobility management is covered next, then Call Processing. This is followed by trunk groups and SIP network elements. The guide finishes with miscellaneous network elements and services. A detailed appendix is included that explains all the configuration database tables and their interrelationships.

CAMEL Pre-paid (page 357), CAP (page 127), IP Access BSC (page 78), and Handover support (page 147) are available only in GSM-R4.5.3 and later releases.

6 CONFIGURING SS7 AND SIGTRAN PROTOCOLS

This chapter provides an overview of the SS7 and SIGTRAN protocol configuration process. This chapter includes:

Overview

SS7 signaling is used to transport call/trunk control (ISUP) messages and transaction (INAP, MAP) messages within the Public Land Mobile Network (PLMN) and the Public Switched Telephone Network (PSTN).

The IETF Signaling Transport (SIGTRAN) class of protocols (such as SCTP, M3UA) provides for the transport of SS7 messages over IP networks.

SS7 Signaling Subsystem Components

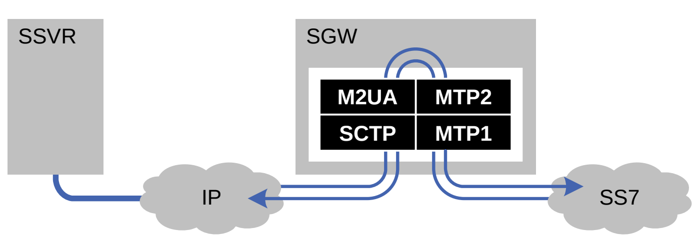
The MSC's SS7 Signaling Subsystem includes the Signaling Gateway and the Signaling Server. Both are shown in Figure 25.

Signaling Gateway

The Signaling Gateway (SGW) is required for communication between SS7 signaling endpoints when one is on an IP network and the other is on an MTP-based SS7 network. The MSC exchanges M2UA messages over SCTP with the Signaling Gateway, which converts them to MTP layer 2 messages and sends them to the SS7 network.

Refer to the *Signaling Server Guide* for further details.

Figure 25 Signaling Server and Signaling Gateway



Signaling Server Signaling Server (SSVR) refers to a group of protocol layers involved in SS7 signaling that are also part of the CONX subsystem. The protocols include:

- HI (TCP/UDP Convergence Layer): See Configuring the HI Layer (page 105).
- SCTP (SIGTRAN Stream Control Transmission Protocol): Covered in the *Signaling Server Guide*
- M2UA (SIGTRAN MTP2 User Adaptation): Covered in the *Signaling Server Guide*
- M3UA (SIGTRAN MTP3 User Adaptation): Covered in the *Signaling Server Guide*
- MTP3 (SS7 Message Transfer Part, Layer 3): Covered in the *Signaling Server Guide*
- SCCP: Chapter 7, SS7 Signaling Connection Control Part
- TCAP: Chapter 8, SS7 Transaction Capability Application Part
- GSM-MAP: Chapter 9, SS7 Mobility Application Part
- ISUP (ISDN User Part): Chapter 13, Adding and Removing ISUP Trunks

The lower layers of the SSVR can run either on the same platform with the MSC (co-located) or on a separate platform (distributed). In either case, the Signaling Server is the component that provides the M2UA/SCTP interface to the Signaling Gateway.

Refer to the *Signaling Server Guide* for further details.

Signaling Server Configurations

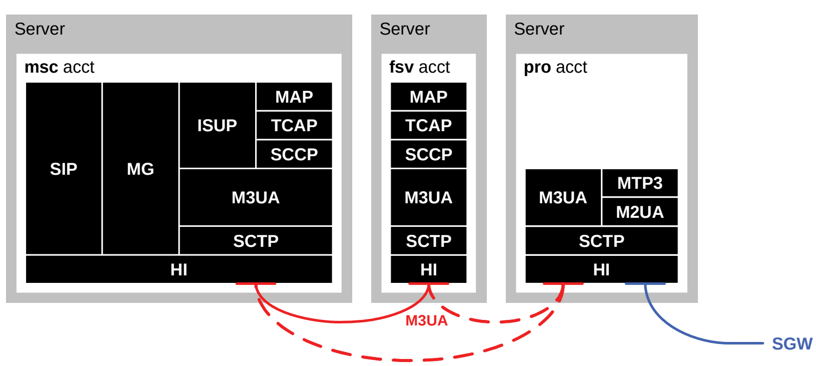
The Sonata system allows for great flexibility in SS7 signaling subsystem design.

Distributed Signaling Server

In the distributed configuration, the upper layers of the SSVR run in the `msc` account on one server and the lower layers of the SSVR run in the `pro` account on a different server, as shown in Figure 26.

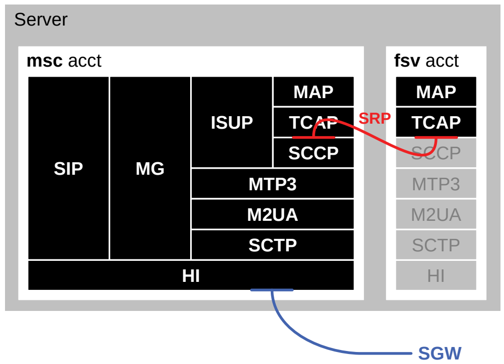
In the distributed configuration, M3UA is used for signaling between accounts.

Figure 26 Distributed SSVR



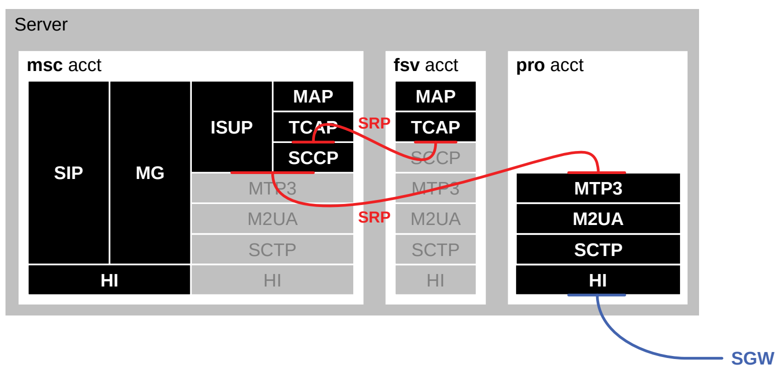
Co-located Signaling Server In the co-located configuration, all the SSVR layers run on the same server with the MSC. If there is no `pro` account, all the SSVR layers run in the `msc` account, as shown in Figure 27. If there is a `pro` account, the MTP3, M2UA, and SCTP layers run there, as shown in Figure 28.

Figure 27 Co-located SSVR without pro Account



In both co-located configurations, the Self-Reliant Protocol (SRP) is used to carry signaling between accounts.

Figure 28 Co-located SSVR with pro Account



The fsv account is present when an HLR/AuC is also co-located. In these cases, the TCAP layer in the fsv account interfaces to the SCCP layer in the msc account.

SS7 and SIGTRAN Configuration Sequence

Configure the SS7 and SIGTRAN layers in the order given in Table 34.

Table 34 SS7 and SIGRAN Configuration Sequence

Distributed SSVR	Co-located SSVR, no pro	Co-located SSVR, with pro
Signaling Server pro account: **1** HI **2** SCTP* **3** M2UA* **4** MTP3* **5** M3UA*	n/a	MSC Server pro account: **1** HI **2** SCTP* **3** M2UA* **4** MTP3* **5** SRP*
MSC Server msc account: **1** HI **2** SCTP* **3** M3UA* **4** SCCP **5** TCAP **6** GSM-MAP **7** ISUP	MSC Server msc account: **1** HI **2** SCTP* **3** M2UA* **4** MTP3* **5** SCCP **6** TCAP **7** GSM-MAP **8** ISUP	MSC Server msc account: **1** SCCP **2** TCAP **3** GSM-MAP **4** ISUP

** Refer to the Signaling Server Guide for instructions.*

Common SS7 Parameters

Several common parameters are needed to bridge together the SS7 and SIGTRAN tables. These include the SAPs covered in Chapter 5, Internal Message Routing. Other parameters include:

- OPC – originating SS7 point code
- DPC – destination SS7 point codes
- SSN – SS7 sub-system number
- IP address of the media/signaling gateway
- IP address of the MSC

7

SS7 SIGNALING CONNECTION CONTROL PART

This chapter describes how to provision the Signaling Connection Control Part of the SS7 protocol.

This chapter includes:

Overview

SCCP and MTP3 make up the Network Services Part (NSP) of SS7. While MTP3 routes messages to a point code, SCCP routes messages to a subsystem at a given point code. A subsystem is an application that uses SCCP, and each is addressed by a subsystem number (SSN). There may be several subsystems located at one node.

Depending on their function, subsystems use different protocols to access SCCP. For example, MSC-to-HLR communications use the Mobile Application Part (MAP), which uses the Transaction Capabilties Application Part (TCAP), which uses SCCP. MSC-to-(TDM) BSC communications use the Base Station Subsystem Application Part (BSSAP), which uses SCCP.

SCCP also enables global title translation (GTT), which allows SS7 network elements to route messages based on global title (GT) and spares each NE from knowing the point codes and SSNs of every signaling destination.

SCCP signaling network management functions are used to update routing and translation information based on input about point code and subsystem failures. This information enables a node to perform alternate routing for transaction services signaling.

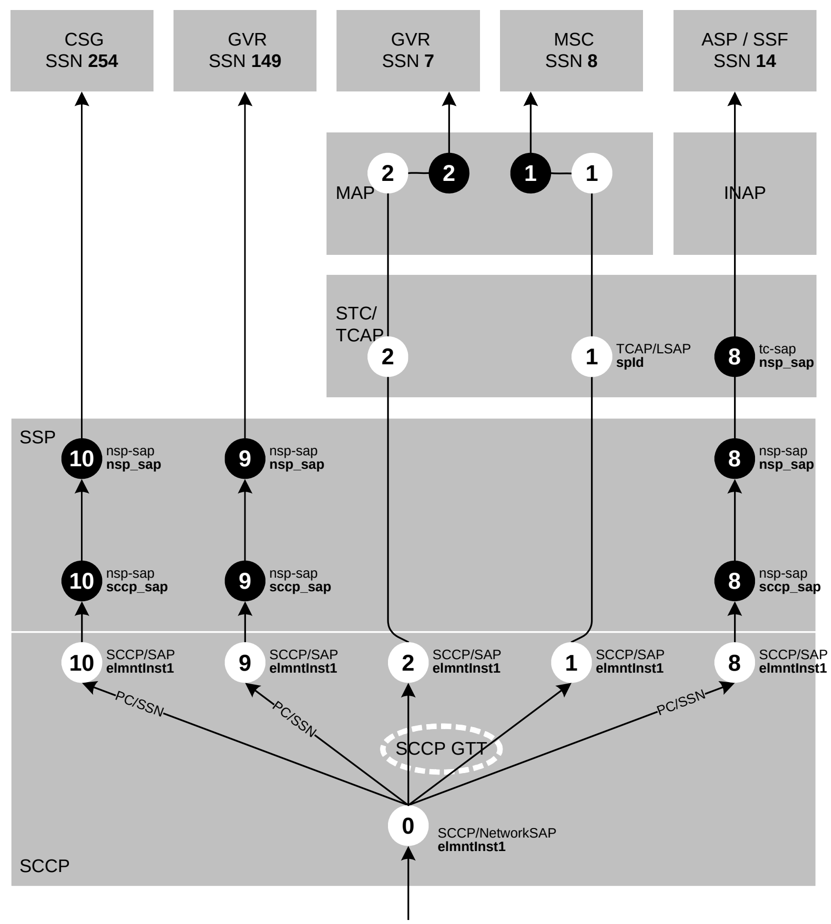
SCCP Architecture

In the Sonata implementation, the SCCP layer has two parts: SSP and CONX SCCP. SSP interfaces to STC above and CONX SCCP below. CONX SCCP interfaces with CONX TCAP above and to the MTP3 or M3UA layer below.

Incoming SCCP Message Processing

Incoming SCCP messages indicate whether they should be routed by point code and subsystem number (PC/SSN) or by the Global Title in the called party address. Figure 30 shows how the MSC processes incoming SCCP messages.

Figure 30 Incoming SCCP Message Processing



BSSAP messages come from BSCs and are destined for the CSG module in the Mobility functional application. BSSAP messages are always routed by PC/SSN. Global title translation is not performed.

BSSAP+ messages come from SGSNs and are destined for the GVR module (the VLR) in the Mobility functional application. BSSAP+ messages are also routed by PC/SSN.

INAP messages come from LNP SCPs and are destined for the SSF module in the Call Processing functional application. INAP messages are routed by PC/SSN.

MAP messages (except those exchanged between the VLR and MSC on the B-interface) come from network elements such as HLRs and SCPs. These messages require global title translation.

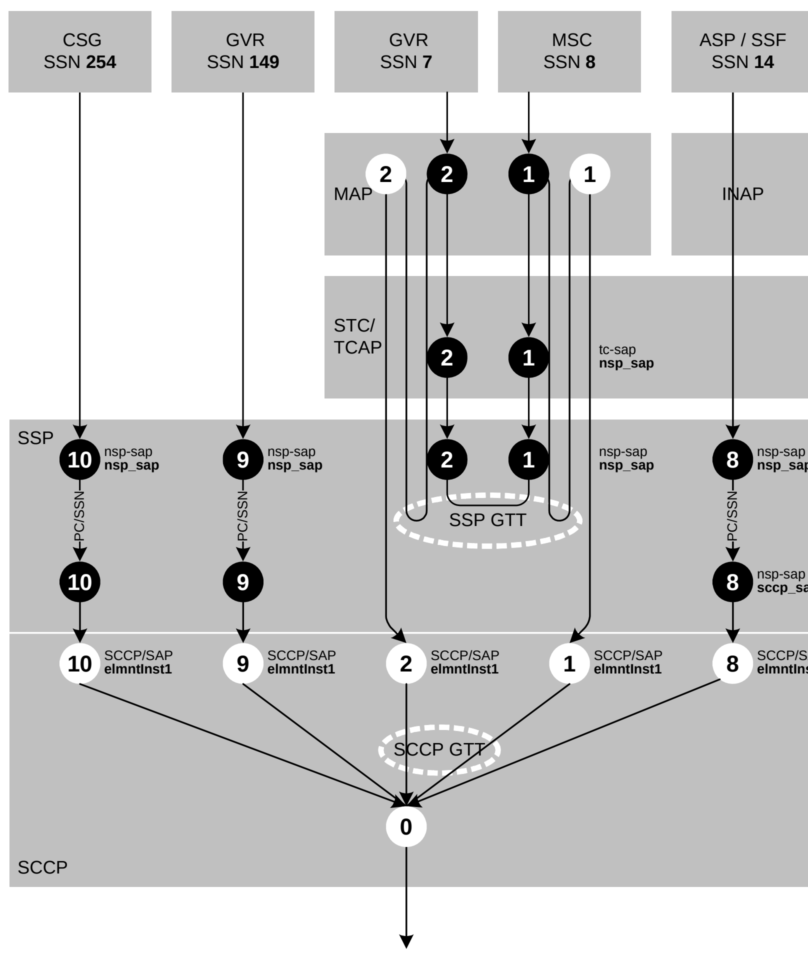
CONX SCCP carries out global title translation (GTT) for incoming SCCP messages. SSP is not involved in GTT for incoming messages - only for outgoing ones. Incoming GTT configuration requires changes to the SCCP/Association and SCCP/AddressMap tables.

Outgoing SCCP Message Processing

Outgoing SCCP messages originated by CSG (destined for a BSC), GVR (destined for an SGSN), and SSF (destined for an LNP SCP) are addressed to the PC/SSN of the destination network element. These messages require SCCP routing but not GTT.

Outgoing MAP messages are processed differently at the SCCP layer depending on whether they are destined internally (between MSC and VLR) or externally (to a remote NE such as an HLR). See Figure 31.

Figure 31 Outgoing SCCP Message Processing



Internal MAP messages go to STC, then SSP. SSP performs GTT on the internal messages. Because of this, two GTT rules must be provisioned in the `nsp-trans` configuration table - one for routing to the MCG module (the MSC) and one for routing to the GVR module (the VLR).

External MAP messages undergo GTT at the SSP layer before being passed to the external MAP layer for transmission through TCAP to SCCP.

External MAP messages require GTT rules at the SSP and SCCP layers.

The SSP layer allows for global title digit reconstruction, which is not possible at the CONX SCCP layer.

Configuration Procedure

Follow these steps to configure the SCCP layer in the MSC. Each step refers to a section in this chapter that provides more detail.

1. Define general SCCP sublayer settings.
   See Defining Basic SCCP Information.
2. Configure SCCP sublayer binding to the lower layer (MTP3 or M3UA) by pointing SCCP/NetworkSAP:spId to either M3UA/NetworkSAP:sapId or MTP3/NetworkSAP:elmntInst1.
   See Adding an SCCP Lower Layer (Network) SAP).
3. Configure SCCP SAPs.
   See Adding an SCCP Upper Layer SAP.
4. Configure SSP SAPs.
   See Configuring SSP SAPs.
5. Define a network in SCCP/Network. Point SCCP/NetworkSAP:nwId to it.
   See Defining SCCP Network Parameters.
6. Define routes to destination point codes in SCCP/Route. The route indicates which SCCP/NetworkSAP:elmntInst1 to send the message through. Routes typically go to the point code of an STP acting as an SCCP gateway.
   See Adding an SCCP Route.
7. Configure Global Title Translation.
   See Global Title Translation.

The teleservice code must exactly match the one requested by the HLR. The following codes are supported:

- all-ts (allTeleservices)
- all-sts (allSpeechTransmissionServices)
- telephony
- emergency (emergencyCalls)
- all-sms (allShortMessageServices)
- sms-mt (shortMessageMT-PP)
- sms-mo (shortMessageMO-PP)
- null-ts (NULL)

Configuring Bearer Services and Teleservices

Follow these steps to indicate the bearer services and teleservices that the MSC/VLR supports:

1. From the OMC interface, double-click the MSC's **vlr-bs** folder.

   The *Configure* window appears.
2. Under Add/Delete, select a bearer service.
3. Click **Add**.
4. If you need to add another bearer service, repeat from step 2.
5. Click **Close**.
6. Double-click the MSC's **vlr-ts** folder.
7. Under Add/Delete, select a teleservice.
8. Click **Add**.
9. Repeat from step 7 until you have added all the teleservices the MSC/VLR supports.
10. Click **Close**.

Security

The VLR is involved in providing security through:

- Subscriber Identity Authentication
- Media/Signaling Stream Enciphering
- Subscriber Identity Confidentiality

Subscriber Identity Authentication

The Authentication Center (AuC), which is implemented along with the Sonata GSM HLR, stores the Individual Subscriber Authentication Key (Ki) for each subscriber and performs security-related calculations.

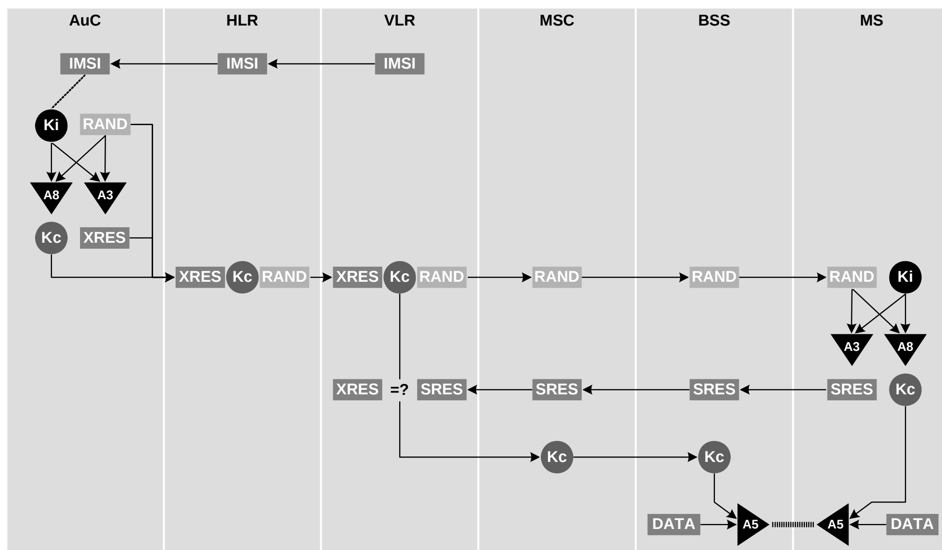
As shown in Figure 38, the VLR starts the authentication process by providing the IMSI to the HLR, which passes it to the AuC. The AuC uses the IMSI to look up the Ki in its database.

The AuC generates a Random Challenge (RAND) and applies the **A3** encryption algorithm to RAND + Ki to yield an Expected Result (**XRES**). The AuC also applies the A8 encryption algorithm to RAND + Ki to yield the Session Key (Kc) used in encrypting communications over the air interface.

The AuC passes the 'authentication triplet' (RAND, XRES, and Kc) to the HLR, which provides it to the serving VLR.

When the VLR decides to challenge a subscriber, it sends the RAND to the MS. The MS applies the A3 algorithm to the RAND and the Ki stored in its SIM to yield a Signed Result (SRES). The MS returns the Signed Result to the VLR. The VLR compares the SRES to the XRES and if they match the subscriber is authenticated.

Figure 38 Authentication and Encryption Process



Authentication Configuration Overview

You can set the percentage probability that the VLR will perform authentication on a given IMSI pattern during each of these MAP procedures:

- Normal call origination
- Emergency call origination
- Call termination
- Location update
- SMS access
- Supplementary Service access

Each set of percentage probabilities is keyed to an IMSI pattern and is applied to any MS with matching IMSI digits. The IMSI is parsed from the most significant bit, allowing, for example, a separate set of authentication criteria to be defined for MSs that have MCC and MNC in common.

You can also indicate whether the VLR should ignore errors during authentication and how many times authentication triplets can be reused, as well as set the authentication request timer.

Configuring Authentication

1 From the OMC interface, double-click the MSC's **vlr-auth** folder.

The *Configure* window appears.

2 Under Add/Delete, enter an IMSI pattern.

3 Enter the percentage probability that the VLR will send a MAP_ AUTHENTICATE toward the MS when the VLR performs each procedure:

Table 37 Authentication Percentage Fields in vlr-auth

Parameter	Definition
normal_call_pct	Percentage probability of performing authentication on mobile-originated calls.
emergency_call_pct	Percentage probability of performing authentication on emergency calls.
call_termination_pct	Percentage probability of performing authentication on mobile-terminated calls.
location_update_pct	Percentage probability of performing authentication during location updates.
sms_access_pct	Percentage probability of performing authentication at SMS access.
ss_access_pct	Percentage probability of performing authentication at supplementary services access.

4 Also from **vlr-auth**, select `y` or `n` for `auth_silent_mode`. If `y`, the VLR ignores errors during authentication and proceeds normally.

5 Click **Add**.

6 Click **Close**.

7 Double-click the MSC's **vlr-config** folder.

8 Click the **Modify** tab.

For `auth_reuse`, enter the number of times the VLR may re-use an authentication triplet (if it is necessary).

9 Click **Apply to selected entries**.

10 Click **Close**.

11 Double-click the MSC's **msc-map-timers** folder.

12 For `t_auth_cnf`, enter the timeout for the authentication request sent to the BSS (the T3260 A_AUTHENTICATE request timer), in seconds.

13 Click **Add**.

14 Click **Close**.

The Session Initiation Protocol (SIP) is used between the MRF and MSC. The Access Server is in compliance with IETF draft document draft-burger-sipping-netann-03 (November 2, 2002). The MSC is always the SIP client and the Access Server is always the SIP server.

The MSC uses SIP to create a voice (RTP) connection between the MRF and an IP-based BSC when the MSC needs to play announcements or tones to a mobile station (MS). The MRF sends the RTP stream, which comes from a stored media file, to the BSC, which delivers it to the MS.

The MSC also uses SIP to create an RTP connection between the MRF and a Media Gateway when the MSC needs to play announcements or tones to a PSTN user. The MRF sends the RTP stream from the stored media file to the Media Gateway, which delivers it to the PSTN.

Adding an MRF To add an MRF for Tone and Announcement Playback:

1. Prepare the MRF. See Preparing the MRF.
2. Add the MRF hostname to `/etc/hosts`. See Adding the MRF Hostname.
3. Bind the MSC application to the SIP SAP. See Binding the SAPs.
4. Add routes from the MSC to each MRF. See Adding Routes to MRFs.

Preparing the MRF

To set up and operate the MRF itself, refer to the *Sonata GSM/CDMA R4.5.2 Core Voice Network Access Server (MRF) Guide*.

Adding the MRF Hostname

Verify that there is an entry in `/etc/hosts` for the MSC and add an entry for the Access Server (MRF).

1. Log in to the MSC as `root`.
2. Open the `/etc/hosts` file for editing.
3. Add a line for the MRF.

   For example:

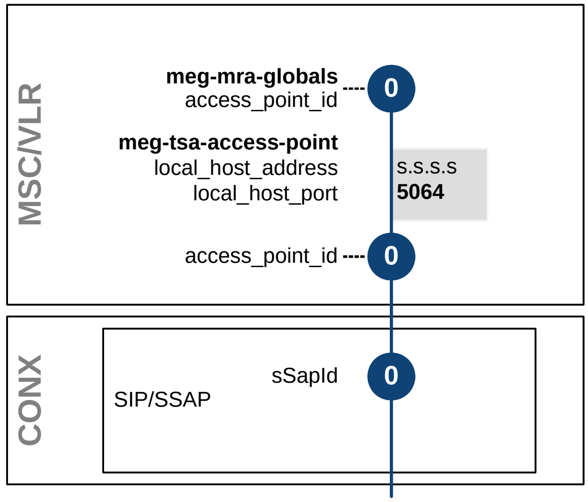
   ```
   149.112.34.48     mrf1
   ```

4. Save and close the file.
5. Log out of the MSC.

Binding the SAPs

The MSC application interfaces with the SIP stack at five points. The `access_point_id` field in `meg-tsa-access-point` indicates the SIP SSAP (0) intended for applications in which the MSC controls tone and announcement playback by an MRF. See Figure 72.

Figure 72 SAP Bindings for Tone and Announcement Playback



To configure the bindings for Tone and Announcement Playback:

1 Configure the SIP stack. See Configuring the SIP Stack on page 219.

2 Start the OMC user interface and expand the element tree for the MSC.

3 Right-click the **`meg-tsa-access-point`** table.

The `meg-tsa-access-point` window appears.

4 Enter values as recommended in Table 61.

Table 61 meg-tsa-access-point Field Descriptions

Field Name	Description
access_point_id	[key, unique] Identifier of the SIP stack access point (SIP/SSAP: sSapId). Use 0 for Tone and Announcement Playback.
access_point_type	Defines role of the access point. USER_AGENT or NETWORK_SERVER. Use USER_AGENT.
local_host_address	MSC IP address.
local_host_port	MSC listening port for Tone and Announcement Playback. Use 5064.
use_call_control	Relevant only if access_point_type is NETWORK_SERVER. Typically n.
transport_protocol_type	UDP or TCP. Use UDP.

5 Click **Add**.

6 Click **Close**.

7 Right-click the **`meg-mra-globals`** table.

The `meg-mra-globals` window appears. This table provides the global settings for controlling MRFs.

8 Enter values as recommended in Table 62.

Table 62 meg-mra-globals Field Descriptions

Field Name	Description
tsa_ua_access_point_id	[key, unique] Refers to an access_point_id in meg-tsa-access-point. Use 0.
tsa_coupling_type	Type of coupling with the Trillium SIP Adapter (TSA) – use TIGHT.
sip_session_timer	SIP session audit time for call-progress tone sessions between the MSC and the MRF. Every sip_session_timer/2 seconds the session will be audited. 0 is disabled.
routing_policy	Refer to meg-tsa-routes. If multiple routes are defined, use LOAD_SHARING.
dynamic_registration_enabled	[Future] Set to n.
tsa_ns_access_point_id	[Future] Same as meg-tsa-access-point: access_point_id.

9 Click **Add**.

10 Click **Close**.

Adding Routes to MRFs

Define each MRF that the MSC uses for Tone and Announcement Playback in the `meg-tsa-routes` table:

1 Start the OMC user interface and expand the element tree for the MSC.

2 Right-click the **`meg-tsa-routes`** table.

The `meg-tsa-routes` window appears. This table defines static routes to the MRFs.

Table 63 meg-tsa-routes Field Descriptions

Field Name	Description
route_id	[key, unique] Identifies a route to an MRF.
route	IP address and port number of the SIP signaling destination. Typically <mrf_ip_addr>:5061. This field is inserted into the REQUEST URI of the SIP INVITE message sent to the MRF.
q_value	Route weight. Q value – used when routing_policy in meg-mra-globals is set to Q_VALUE.
appl_id	SIMPLE_TONE or CRBT. Set to SIMPLE_TONE for routes to MRFs.
enabled	Whether the route is enabled.

3 Click **Add**.

4 Click **Close**.

Early Media Playback

The Early Media feature (on the IP Inter-MSC Trunking interface) enables the calling party to hear call-progress tones from the far-end switch, whether the call is terminated at the remote MSC or at another switch in the PSTN.

The MSC supports the SIP Early Media feature on the IP Inter-MSC Trunking interface. This enables the calling party to hear call-progress tones from the far-end switch, whether the call is terminated at the remote MSC or at another switch in the PSTN.

The SIP Early Media feature can be enabled and disabled online, without restarting the MSC, by changing the MSC's `callprogress` configuration table.

Adding an MRF

To add an MRF for Early Media Playback:

1. Prepare the MRF. See Preparing the MRF.
2. Add the MRF hostname to `/etc/hosts`. See Adding the MRF Hostname.
3. Bind the MSC application to the SIP SAP. See Binding the SAPs.
4. Add routes from the MSC to each MRF. See Adding Routes to MRFs.
5. Configure `callprogress`. See Configuring callprogress.

Preparing the MRF

To set up and operate the MRF itself, refer to the *Sonata GSM/CDMA R4.5.2 Core Voice Network Access Server (MRF) Guide*.

Adding the MRF Hostname

Verify that there is an entry in `/etc/hosts` for the MSC and add an entry for the Access Server (MRF).

1. Log in to the MSC as `root`.
2. Open the `/etc/hosts` file for editing.
3. Add a line for the MRF.

   For example:

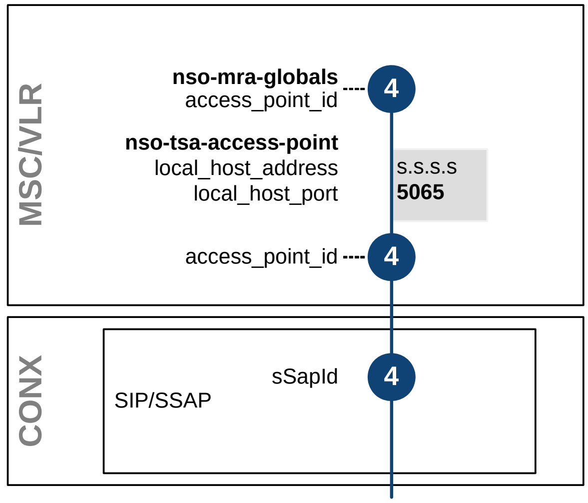
   ```
   149.112.34.48    mrf1
   ```

4. Save and close the file.
5. Log out of the MSC.

Binding the SAPs

The MSC application interfaces with the SIP stack at five points. The `access_point_id` field in `nso-tsa-access-point` indicates the SIP SSAP (4) intended for applications in which the MSC controls early media playback by an MRF. See Figure 72.

Figure 73 SAP Bindings for Early Media Playback



To configure the bindings for Early Media Playback:

1 Configure the SIP stack. See Configuring the SIP Stack on page 219.

2 Start the OMC user interface and expand the element tree for the MSC.

3 Right-click the **`nso-tsa-access-point`** table.

The `nso-tsa-access-point` window appears.

4 Enter values as recommended in Table 61.

Table 64 nso-tsa-access-point Field Descriptions

Field Name	Description
access_point_id	[key, unique] Identifier of the SIP stack access point (SIP/SSAP: sSapId). Use 4 for Early Media Playback.
access_point_type	Defines role of the access point. USER_AGENT or NETWORK_SERVER. Use USER_AGENT.
local_host_address	MSC IP address.
local_host_port	MSC listening port for Tone and Announcement Playback. Use 5065.
use_call_control	Relevant only if access_point_type is NETWORK_SERVER. Typically n.
transport_protocol_type	UDP or TCP. Use UDP.

5 Click **Add**.

6 Click **Close**.

7 Right-click the **`nso-mra-globals`** table.

The `nso-mra-globals` window appears. This table provides the global settings for controlling MRFs.

8 Enter values as recommended in Table 62.

Table 65 nso-mra-globals Field Descriptions

Field Name	Description
tsa_ua_access_point_id	[key, unique] Refers to an access_point_id in nso-tsa-access-point. Use 4.
tsa_coupling_type	Type of coupling with the Trillium SIP Adapter (TSA) – use TIGHT.
sip_session_timer	SIP session audit time for call-progress tone sessions between the MSC and the MRF. Every sip_session_timer/2 seconds the session will be audited. 0 is disabled.
routing_policy	Refer to nso-tsa-routes. If multiple routes are defined, use LOAD_SHARING.
dynamic_registration_enabled	[Future] Set to n.
tsa_ns_access_point_id	[Future] Same as nso-tsa-access-point: access_point_id.

9 Click **Add**.

10 Click **Close**.

Adding Routes to MRFs

Define each MRF that the MSC uses for Tone and Announcement Playback in the `nso-mra-routes` table:

1 Start the OMC user interface and expand the element tree for the MSC.

2 Right-click the **`nso-mra-routes`** table.

The `nso-mra-routes` window appears. This table defines static routes to the MRFs.

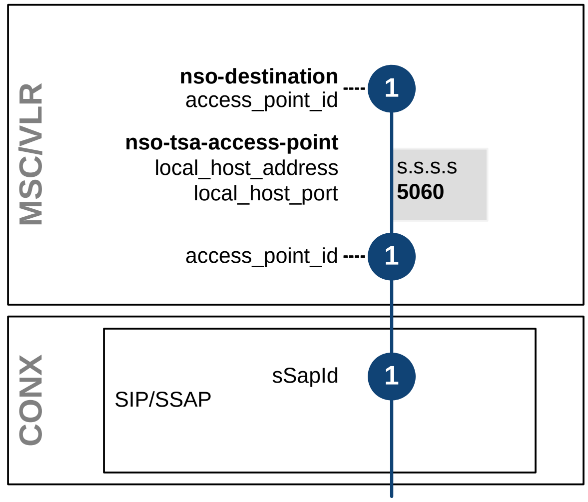
Table 66 nso-mra-routes Field Descriptions

Field Name	Description
route_id	[key, unique] Identifies a route to an MRF.
route	IP address and port number of the SIP signaling destination. Typically <mrf_ip_addr>:5061. This field is inserted into the REQUEST URI of the SIP INVITE message sent to the MRF.
q_value	Route weight. Q value – used when routing_policy in nso-mra-globals is set to Q_VALUE.
appl_id	SIMPLE_TONE or CRBT. Set to SIMPLE_TONE for routes to MRFs.
enabled	Whether the route is enabled.

3 Click **Add**.

4 Click **Close**.

Figure 74 SAP Bindings for Three-Way Calling



To configure the bindings for Three-Way Calling:

1. Configure the SIP stack. See Configuring the SIP Stack on page 219.
2. Start the OMC user interface and expand the element tree for the MSC.
3. Right-click the **`nso-tsa-access-point`** table.

   The `nso-tsa-access-point` window appears.
4. Enter values as recommended in Table 67.

Table 67 nso-tsa-access-point Field Descriptions

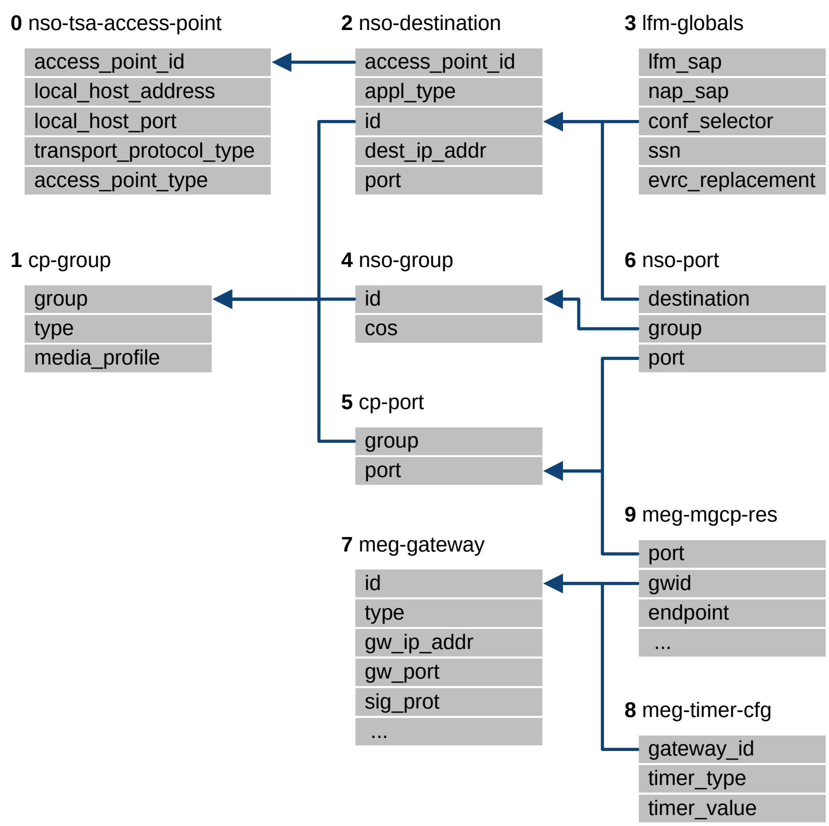
Field Name	Description
access_point_id	[key, unique] Identifier of the SIP stack access point (SIP/SSAP: sSapId). Use 1 for Three-Way Calling. This SAP can be shared by other applications.
access_point_type	Defines role of the access point. USER_AGENT or NETWORK_SERVER. Use USER_AGENT.
local_host_address	MSC IP address.
local_host_port	MSC listening port for SIP trunking. Use 5060.
use_call_control	Relevant only if access_point_type is NETWORK_SERVER. Typically n.
transport_protocol_type	UDP or TCP. Use UDP.

5. Click **Add**.
6. Click **Close**.

Integrating MSC-CCS Signaling with Call Processing

First a point-to-point MSC-CCS signaling link must be set up, then the link must be integrated with the MSC's Call Processing system. Figure 75 shows how the configuration database tables relate to one another to accomplish this. The numbers in the diagram correspond to the steps in the following procedure.

Figure 75 MSC Configuration Database for Three-Way Calling



1 In `cp-group`, create a SIP trunk group. The class of service (cos) assigned in `cp-group` is not used, instead, the cos is picked up from `nso-group`.

   a Start the OMC Console and expand the element list for the MSC.

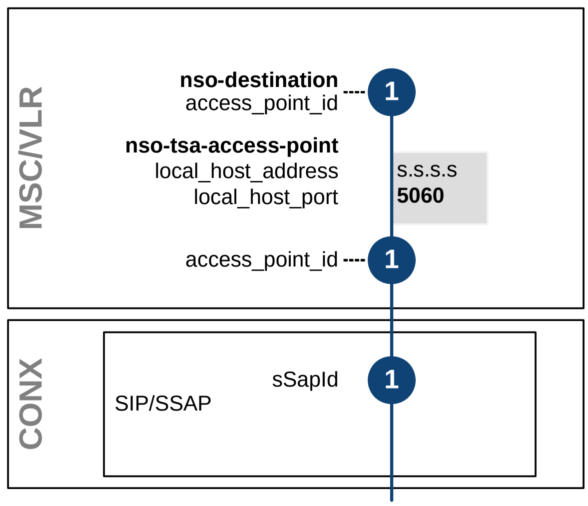
   b Right-click the **`cp-group`** table.

   The window shown in Figure 76 appears.

Binding to the SAP The MSC application interfaces with the SIP stack at five points, as shown in Figure 67. The `access_point_id` field in `nso-tsa-access-point` indicates the SIP SSAP (**1**) intended for SIP trunking applications. See Figure 86. Multiple destinations can share the `access_point_id` – that is, they can 'listen' for incoming SIP traffic on the same port.

If `access_point_id` ***1*** *in* `nso-tsa-access-point` *is already configured, skip this section.*

Figure 86 SAP Bindings for IP Inter-MSC Trunking



To configure the bindings for IP Inter-MSC Trunking:

1 Configure the SIP stack. See Configuring the SIP Stack on page 219.

2 Start the OMC user interface and expand the element tree for the MSC.

3 Right-click the **`nso-tsa-access-point`** table.

The `nso-tsa-access-point` window appears.

4 Enter values as recommended in Table 71.

Table 71 nso-tsa-access-point Field Descriptions

Field Name	Description
access_point_id	[key, unique] Identifier of the SIP stack access point (SIP/SSAP: sSapId). Use 1 for IP Inter-MSC Trunking. This SAP can be shared by other applications.
access_point_type	Defines role of the access point. USER_AGENT or NETWORK_SERVER. Use USER_AGENT.
local_host_address	MSC IP address.
local_host_port	MSC listening port for SIP trunking. Use 5060.
use_call_control	Relevant only if access_point_type is NETWORK_SERVER. Typically n.
transport_protocol_type	UDP or TCP. Use UDP.

5 Click **Add**.

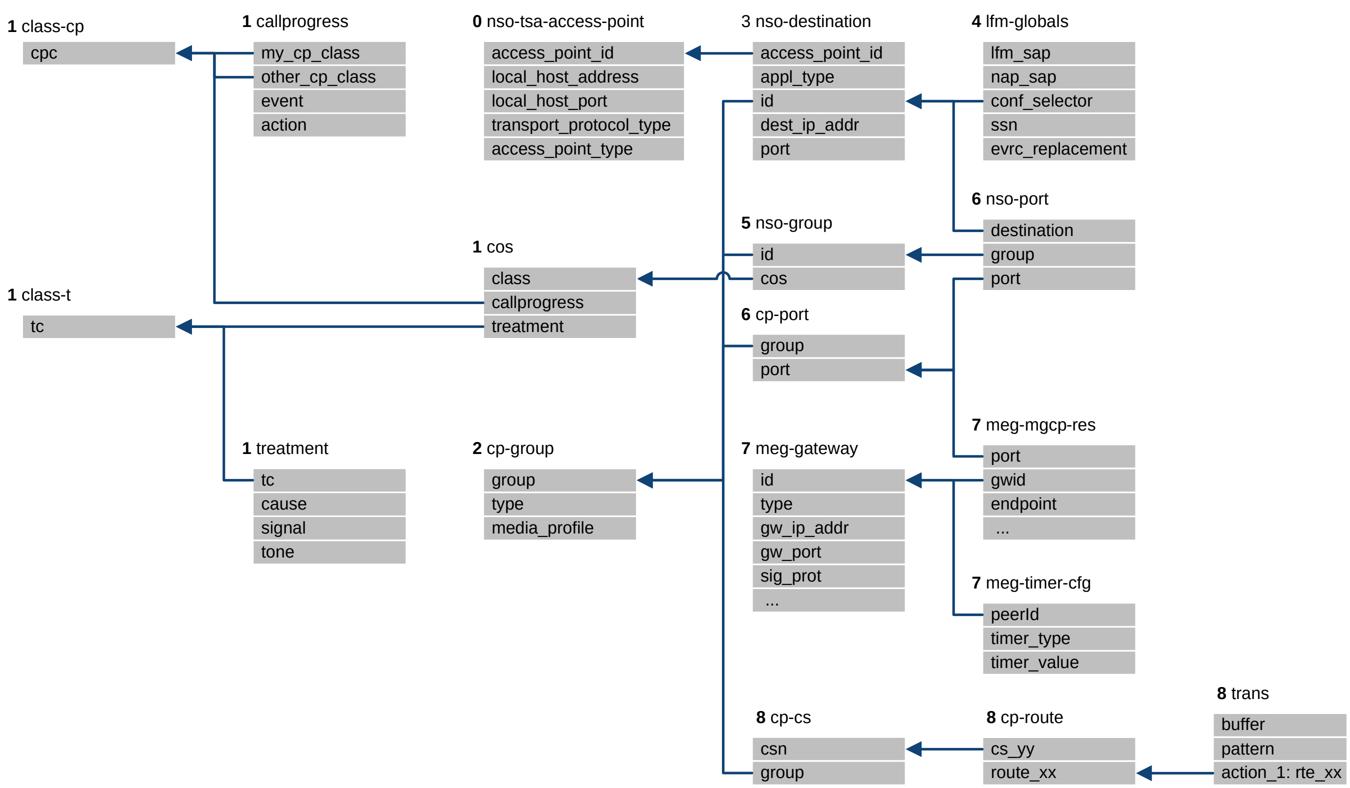
6 Click **Close**.

Configuring IP Inter-MSC Trunking

To configure IP Inter-MSC trunking, add specialized classes of service for IP Inter-MSC Trunking calls, add a call-processing trunk group, add the peer MSC as a SIP signaling destination, and integrate the SIP signaling destination with the MSC's Call Processing subsystem.

The numbers in Figure 87 refer to step numbers in the procedure below.

Figure 87 Overview of the IP Trunking Provisioning Procedure



1 In the `class-cp` table, add a unique call-progress class (`cpc`) for IP inter-MSC trunking calls. In the `class-t` table, add a unique treatment class (`tc`) for IP Inter-MSC Trunking calls.

In the `treatment` table, copy treatment class 0 to the new class for IP Inter-MSC Trunking calls, mapping every cause to `tone_null`. In the `callprogress` table, for the new IP Inter-MSC Trunking class to all classes (including the IP Inter-MSC Trunking class), set queuing and alerting to `ignore`. For all other classes to the IP Inter-MSC Trunking class, set queuing and alerting to `tone`.