Administering Avaya Aura® Communication Manager Server Options

Release 6.3
03-603479
Issue 4
May 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

- Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
- Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.
- CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage

Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each virtual appliance has its own ordering code. Note that each instance of a virtual appliance must be ordered separately. If the end-user customer or Business Partner wants to install two of the same type of virtual appliances, then two virtual appliances of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya and Avaya Aura® are trademarks of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux is the registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for configuring Avaya Aura® Communication Manager as a feature server, an evolution server, a trunk gateway, or a combination feature server and trunk gateway. This document also provides a sample configuration for a network that uses Avaya Aura® Session Manager to connect Communication Manager as a feature server or an evolution server.

Intended audience

The primary audience for this document is:

- Avaya field technicians
- Avaya partners
- Technical support personnel
- Solution Architects
- Implementation Engineers
- Support Personnel
- Technical support representatives
- Authorized Business Partners

Document changes since last issue

The following change has been made to this document since the last issue:

- Updated Administering Public Unknown Numbering on page 27 to include the public unknown numbering table.

Related Resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Document number	Title	Description	Audience
Administration			
555-233-504	*Administering Network Connectivity on Avaya Aura® Communication Manager*	This document describes the network connectivity for Communication Manager.	Solution architects, Implementation engineers, Support personnel, Technical support representatives

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Overview

You can configure Communication Manager Release 6.0 and later as:

- A feature server
- An evolution server
- A trunk gateway
- A combination feature server and trunk gateway

Avaya 9600 series IP telephones that are configured as SIP endpoints use the User Registration feature of Avaya Aura® Session Manager and are supported by the feature server and the evolution server.

You cannot configure Communication Manager both as the feature server and the evolution server.

Feature server

A feature server provides the Communication Manager features to the SIP endpoints that are registered with Session Manager. The feature server uses the half-call model of IP Multimedia Subsystem (IMS). For more information about half-call model, see *Half-call model*. The feature server connects to Session Manager through an IMS-enabled SIP signaling group and an associated SIP trunk group.

The feature server supports full application sequencing.

The feature server has the following limitations:

- The dial plan for IMS users does not support routing of PSTN calls directly to ISDN trunks. Therefore, you must administer the dial plan to route all PSTN calls to Session Manager over the IMS trunk group.
- Traditional endpoints, such as DCP, H.323, ISDN, and analog are not supported.
- G650 gateway is not supported.

Related topics:

Half-call model on page 11

Half-call model

In the half-call model, a call request is processed in two following phases:

- Origination: The feature server applies services to the originator of the call.
- Termination: The feature server applies services to the recipient of the call.

The origination and termination phases are separate operations and are performed by different feature servers.

The half-call model supports full application sequencing. The number of originating sequenced applications can be different from the number of terminating sequenced applications.

For the half-call model, you must set the **IMS-enabled** field on the SIP Signaling Group screen to y.

Evolution server

An evolution server is equivalent to traditional Communication Manager. The evolution server provides the Communication Manager features to both SIP and non-SIP endpoints. The evolution server uses the full-call model. For more information about full-call model, see *Full-call model*. The evolution server connects to Session Manager through a non-IMS Signaling group. Session Manager handles call routing for SIP endpoints and enables SIP endpoints to communicate with all other endpoints that are connected to the evolution server.

To configure Communication Manager as the evolution server, disable **IMS** on the signaling group that is connected to Session Manager.

With Communication Manager configured as an evolution server:

- H.323, digital, and analog endpoints register with Communication Manager.
- SIP endpoints register with Session Manager.
- All endpoints receive service from Communication Manager.

Gateways provide connection-preserving failover and failback to survivable core processors and survivable remote processors. The evolution server supports IP-connected G650 gateways, but the gateways are not connection preserving.

The evolution server support limited form of application sequencing. For more information, see *Application sequencing in the evolution server*.

Related topics:

Full-call model on page 13
Application sequencing in the evolution server on page 13

Full-call model

In the full-call model, a call request is processed in a single step. The origination and termination phases of the call are performed without a break. Traditional Communication Manager follows the full-call model.

Application sequencing works only when all the servers support the half-call model. Therefore, no other sequenced application should be provisioned along with the evolution server.

For the full-call model, you must set the **IMS-enabled** field on the SIP Signaling Group screen to n.

Application sequencing in the evolution server

The evolution server supports a limited form of application sequencing:

- Non-SIP users receive implicit application sequencing.
- SIP users receive explicit application sequencing with the following conditions:
  - Origination sequencing: The sequenced applications must be before Communication Manager in the sequence vector.
  - Termination sequencing: The sequenced applications must be after Communication Manager in the sequence vector.

The evolution server operates in the full call model therefore, there is no flexibility in positioning the applications with respect to Communication Manager. Communication Manager must be last in the origination vector and first in the termination vector.

Trunk gateway

A trunk gateway provides an interface for trunk calls between SIP networks and non-SIP networks. The networks can be PSTN or private networks.

The trunk gateway supports only trunks. No other endpoints are supported.

The trunk gateway connects to Session Manager through a non-IMS SIP signaling group.

Combination feature server and trunk gateway

A combination feature server and trunk gateway allows only IMS to IMS and non-IMS to non-IMS traffic. The combination feature server and trunk gateway requires two SIP signaling

groups from Communication Manager to Session Manager: an IMS signaling group to support the feature server, and a non-IMS signaling group to support the trunk gateway.

All calls for the IMS users must route to Session Manager. Calls that come in on IMS trunks must route to an IMS trunk. Therefore, two sets of ARS route tables are required: one set for calls that come in on IMS trunks, and the other set for calls that come in on the non-IMS SIP trunks and non-SIP trunks.

For example, an incoming public trunk call to an IMS user must route to Session Manager through the non-IMS SIP signaling group. The non-IMS SIP signaling group routes the call to the trunk gateway through the IMS signaling group that is connected to the feature server.

Chapter 3: Communication Manager server administration

This section describes how to define the connection and routing between:

- Session Manager and Communication Manager configured as a feature server
- Session Manager and Communication Manager configured as an evolution server

Administering feature server or evolution server prerequisites

Procedure

1. Install Communication Manager on System Manager.
2. Install the patches as required.
3. Patch the Communication Manager feature server or evolution server through the System Platform Web Console. Use the **Server Management** > **Patch Management** option.
4. Configure the IP address of Processor Ethernet by using the **`add ip-interface procr`** command.
5. Add the required gateways by using the **`add media-gateway x`** command.

   The system updates the following two IP addresses in the mgc lists of the gateways: the IP address of Processor Ethernet of the Communication Manager feature server, and the IP address of Processor Ethernet of the Survivable Remote server.
6. Install the Communication Manager license file through System Platform Web Console by using the MAC address of the Communication Manager feature server or the Communication Manager evolution server.
7. Install theCommunication Manager authentication file through System Platform Web Console. The Communication Manager feature server and the simplex survivable remote server require separate authentication files.
8. Ensure that System Manager and Session Manager are active in the existing SIP routing deployment.

9. Configure the SSH client, such as PuTTY or Avaya Site Administrator (ASA), to gain access to the command line interface of the Communication Manager server.
10. Install and administer the Session Manager server.
11. Install the appropriate service packs, if applicable.

Recommendations

- Use adaptation modules only on the entry and exit points to and from Avaya Aura® network. Do not use them on the interface to sequenced applications.
- Use only real and existing public numbers. The number should always be Enterprise Canonical. Numbers without a public representation must be in the Private Long format to be Enterprise Canonical.
- Use Automatic Alternate Routing (AAR) or Automatic Routing Selection (ARS) to reach extensions on another Communication Manager.

Feature server or evolution server administration checklist

Use this checklist to administer Communication Manager as a feature server or an evolution server. Communication Manager is first administered using the System Administration Terminal (SAT) interface and then using the System Manager Web interface.

No.	Action	Link	✔
1	Log in to Communication Manager.		
2	Change the dial plan.	Changing dialplan analysis on page 19	
3	Add feature access codes for AAR and ARS.	Changing feature access codes on page 19	
4	Add the appropriate SIP domain in the network region that is used.	Changing an IP network region on page 20	
5	Administer a node name for the IP address of the Session Manager security module.	Adding a node name on page 20	

No.	Action	Link	✔
6	Administer a SIP signaling group.	Adding a SIP signaling group on page 21	
7	Add trunk groups for each Session Manager.	Adding a SIP trunk group on page 22	
8	Configure the appropriate route patterns.	Administering a route pattern on page 23	
9	Administer the uniform dial plan for non-SIP calls.	Changing the uniform dial plan on page 23	
10	Administer AAR.	Administering AAR analysis table on page 24	
11	Administer ARS for non-SIP calls.	Administering ARS analysis table on page 25	
12	Add the appropriate route pattern as the Proxy Route.	Administering the proxy route on page 26	
13	Administer the incoming call handling treatment.	Administering Incoming Call Handling Treatment on page 26	
14	If applicable, add a Survivable Remote server.	Adding a Survivable Remote server on page 27	
15	Change public unknown numbering so that the telephone displays a number in the E.164 format.	Administering Public Unknown Numbering on page 27	
16	If applicable, validate the minimum time of network stability for gateways to failback to Communication Manager when Communication Manager becomes available.	Validating the minimum time of network stability on page 29	
17	If applicable, validate the gateway recovery rule.	Validating gateway recovery rule on page 29	
18	Save translations by using the **`save translations`** command.		
19	Add a privileged administrator to be used by System Manager.	Adding a privileged administrator on page 30	
20	Log in to the System Manager Web interface.		

No.	Action	Link	✔
21	Administer Communication Manager as a managed element.	Creating a Communication Manager managed element on page 30	
22	Synchronize the Communication Manager data.	Synchronizing Communication Manager data on page 31	
23	Add the Communication Manager feature server or Communication Manager evolution server as a SIP Entity.	Adding a Communication Manager server as a SIP entity on page 32	
24	If adding Survivable Remote Session Manager, add as a SIP Entity.	Adding a Survivable Remote server as a SIP entity on page 33	
25	Create entity links between Session Manager and Communication Manager.	Creating entity links on page 33	
26	Verify the connections between Session Manager and Communication Manager.	Checking the connections on page 34	
27	Administer Communication Manager as an application.	Administering the Communication Manager server as an application on page 34	
28	Administer Communication Manager in an application sequence.	Administering Communication Manager in an application sequence on page 35	
29	Add users.	Adding users on page 36	
30	Verify users.	Verifying a new SIP user on page 38	
31	Test Session Manager and Communication Manager feature server or evolution server calls.	Testing Session Manager and Communication Manager calls on page 39	

SAT administration procedures

Changing dialplan analysis

Procedure

1. Type `change dialplan analysis`, and press Enter.
   The system displays the DIAL PLAN ANALYSIS TABLE screen.
2. Type the appropriate values in the fields.
   For example,

Dialed String	Total length	Call Type	Reason
9	1	fac	Feature Access Code (FAC) for ARS or PSTN calling
*	4	dac	Trunk access code
*	2	fac	Feature Access Code (FAC) for AAR feature
3	5	ext	SIP station extension
2, 4, 5, 6, 7	5	udp	Uniform Dial Plan (UDP) for Non-SIP extensions on a PBX connected to Session Manager

3. Save the changes.

Changing feature access codes

Procedure

1. Type `change feature-access-codes`, and press Enter.

The system displays the FEATURE ACCESS CODE (FAC) screen.

2. In the **Auto Alternate Routing (AAR) Access Code** field, type an access code.
   For example, `#83`
3. In the **Auto Route Selection (ARS) - Access Code 1** field, type an access code.
   For example, `9`
4. Save the changes.

Changing an IP network region

About this task

Use this procedure to add the appropriate IP addresses to the node names. For more information about the administration of IP network regions, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Procedure

1. Type `change ip-network-region x`, where *x* is an IP network region number, and press Enter.
   The system displays the IP NETWORK REGION screen.
2. In the **Authoritative Domain** field, type the domain name.
   For example, `MyCompany.com`
3. In the **Name** field, type a descriptive name.
   For example, `Main_SM_NR`
4. Save the changes.

Adding a node name

About this task

Use this procedure to define a node name for the IP address of the Session Manager security module. **procr** is the node name for the IP address of Communication Manager Processor Ethernet.

Procedure

1. Type `change node-names ip`, and press Enter.
   The system displays the IP NODE NAMES screen.

2. In the **Name** field, type a name for the IP address of the Session Manager security module.

   For example, `SM1HostName`

3. In the **IP Address** field, type the IP address of the Session Manager security module.
4. Save the changes.

Adding a SIP signaling group

About this task

Use this procedure to add a SIP signaling group for each Session Manager security module.

Procedure

1. Type `add signaling-group` *next*, and press Enter.

   The system displays the SIGNALING GROUP screen.

   Note the value of the **Group Number** field.
2. In the **Group Type** field, type `sip`.
3. In the **IMS Enabled** field, type one of the following:
   a. To configure Communication Manager as a feature server, type `y`.
   b. To configure Communication Manager as an evolution server, `n`.
4. In the **Transport Method** field, type `tls` or `tcp` depending on whether the calls that will run are secure calls.
5. In the **Peer Detection Enabled** field, type `y`.

   Note:

   This setting causes a message interchange between Communication Manager and the connected SIP server. The value for **Peer Server** changes to `SM` when the SIP signaling group is in service.

   For the trunks connected to Session Manager, set the **Peer Detection** field to `n` and the **Peer Server** field to `SM`.
6. In the **Near-end Node Name** field, type `procr`.
7. In the **Far-end Node Name** field, type the name of the Session Manager security module.
8. In the **Far-end Network Region** field, type the IP network region number used earlier in the *Changing an IP network region* procedure.

9. In the **Far-end Domain** field, type the domain name associated with Session Manager.
10. In the **Enable Layer 3 Test** field, type `y`.

    The system displays the **Enable Layer 3 Test** field only when you type a value in the **Far-end Node Name** field.

    Important:

    If the value of **Enable Layer 3 Test** field is `n`, Communication Manager does not monitor the links. This test is required for the trunks connected to Session Manager. Maintenance software takes the trunks out of service if this test is disabled.
11. In the **Initial IP-IP Direct Media** field, type `y` or `n` depending on the requirement of the **Direct Media** feature.
12. In the **H.323 Station Outgoing Direct Media** field, type `y` to configure Communication Manager as an evolution server.
13. Save the changes.

Adding a SIP trunk group

About this task

Use this procedure to add a SIP trunk group to the SIP signaling group for call routing from Communication Manager to Session Manager.

Procedure

1. Type `add trunk-group next`, and press Enter.

   The system displays the TRUNK GROUP screen.

   Note the value of the **Group Number** field.
2. In the **Group Type** field, type `sip`.
3. In the **Group Name** field, type a descriptive name for the trunk group.
4. In the **TAC** field, type a dial access code (DAC) added in the dial plan analysis table.

   For example, `*110`
5. In the **Direction** field, type `two-way`.
6. In the **Service Type** field, type `tie`.
7. In the **Signaling Group** field, type the SIP signaling group number that you added earlier in the *Adding a SIP signaling group* procedure.

8. In the **Number of Members** field, type the number of trunk group members.
   The required limit for the number of members is up to `255`.
9. In the **Numbering Format** field, type `unk-pvt` for a private network.
   Otherwise, type:
   - `public` for a trunk that receives ARS calls
   - `private` for a trunk that receives SIP calls
10. Save the changes.

Administering a route pattern

About this task

Use the following procedure to add a route pattern for non-enterprise calls.

Procedure

1. Enter `change route-pattern x`, where *x* is the route pattern number, and press Enter.
2. In the **Pattern Name** field, type a descriptive name for the route pattern.
3. In the **Grp No** field, type the trunk group number used earlier in the *Adding a SIP trunk group* procedure.
4. In the **FRL** field, type `0`.
5. In the **Inserted Digits** field, type `p` to allow Communication Manager to prepend a plus (+) sign to the number.
6. Save the changes.

Changing the uniform dial plan

About this task

Use the following procedure to modify digits in the number so that the non-enterprise call can be routed through the AAR table.

Procedure

1. Type `change uniform-dialplan x`, where *x* is the dial plan number, and press Enter.
   The system displays the UNIFORM DIAL PLAN TABLE screen.

2. Type the appropriate values in the fields.

   In the following example, when a five-digit number starting with the digits, 2, 4, 5, 6, or 7, is dialed, Communication Manager inserts digits to make the number a 11-digit number.

Matching Pattern	Len	Del	Inserted Digits	Net	Conv
2	5	0	120983	aar	n
4	5	0	120983	aar	n
5	5	0	120983	aar	n
6	5	0	120983	aar	n
7	5	0	120983	aar	n

Administering AAR analysis table

About this task

Use the following procedure to add appropriate entries for SIP and non-SIP station calls. AAR routes calls within a company over the private network of the company.

Procedure

1. Type `change aar analysis x`, where *x* is a digit string, and press Enter. For example, `change aar analysis 0`.

   The system displays the AAR DIGIT ANALYSIS TABLE screen.

2. Type the appropriate values in the fields.

   In the following example, two entries are used:

   - For non-SIP station calls, 11-digit numbers starting with 1 are sent to route pattern number 10 where Communication Manager prepends a plus (+) sign before routing the call to Session Manager.
   - For SIP station calls, five-digit numbers starting with 3 are sent to route pattern 11 where the call are sent to Session Manager directly without prepending a plus (+) sign.

Dialed String	Total Min	Total Max	Route Pattern	Call Type	ANI Reqd
1	11	11	10	aar	n
3	5	5	11	aar	n

3. Save the changes

Administering ARS analysis table

Procedure

1. Type `change ars analysis x`, where *x* is a digit string, and press Enter.
   The system displays the ARS DIGIT ANALYSIS TABLE screen.
2. Type the appropriate values in the fields.
   For example,

Dialed String	Total Min	Total Max	Route Pattern	Call Type	ANI Reqd
1	11	11	10	natl	n
101xxxx0	8	8	deny	op	n
101xxxx0	18	18	deny	op	n
101xxxx01	16	24	deny	iop	n
101xxxx011	17	25	deny	intl	n
101xxxx1	18	18	deny	fnpa	n
10xxx0	6	6	deny	op	n
10xxx0	16	16	deny	op	n
10xxx01	14	22	deny	iop	n
10xxx011	15	23	deny	intl	n
10xxx1	16	16	deny	fnpa	n
1200	11	11	deny	fnpa	n
1209	11	11	10	natl	n
1300	11	11	deny	fnpa	n
1400	11	11	deny	fnpa	n

3. Save the changes.

Administering the proxy route

About this task

Use the following procedure to add a route pattern as the proxy route.

Procedure

1. Type `change locations`, and press Enter.
   The system displays the LOCATIONS screen.
2. In the **Name** field, type a descriptive name for the proxy route, for example, `main`.
3. In the **Proxy Sel Rte Pat** field, type the route pattern number.
4. Save the changes.

Administering Incoming Call Handling Treatment

About this task

Use this procedure to delete the number of digits to match the SIP extension length in the Communication Manager feature server or evolution server.

Procedure

1. Type `change inc-call-handling-trmt trunk-group` *n*, where *n* is the trunk group number, and press Enter. For example, `change inc-call-handling-trmt trunk-group` *10*.
   The system displays the INCOMING CALL HANDLING TREATMENT screen.
2. In the **Number Len** field, type the length of the extension, for example, `12`.
3. In the **Number Digits** field, type the digits, for example, `+1209833`.
4. In the **Del** field, type the number of digits to be deleted, for example, `7`.
5. Save the changes.

Adding a Survivable Remote server

Procedure

1. Type `add survivable-processor` *`node-name`*, where *node-name* is the name of the remote server, and press Enter. For example, `add survivable-processor` *`lsp6`*.

   The system displays the SURVIVABLE PROCESSOR screen.
2. In the **Type** field, type `lsp` for an LSP or a Survivable Remote server.
3. Ensure that the value of the **Cluster ID/MID** field matches with the value of the **MID number** field.

   The **MID number** field is on the **Server Role** page of the **Server Maintenance** section on the Communication Manager System Management Interface Web page.
4. Save the changes.

Administering Public Unknown Numbering

About this task

Use this task to add the appropriate information so that the telephone displays a number in the E.164 format.

Procedure

1. Type `change public-unknown-numbering` *`n`*, where *n* is the extension length, and press Enter. For example, `change public-unknown-numbering` *`10`*.

   The system displays the NUMBERING - PUBLIC/UNKNOWN FORMAT screen.
2. In the **Ext Len** field, type the number of digits of the extension.
3. In the **Ext Code** field, type one or more starting digits of the extension.
4. In the **CPN Prefix** field, type the digits to be attached as a prefix to the digit string.

Connection type	Server	Numbering format	Country code required?	Plus (+) sign required?	Action
`SIP`	`SM`	`Full internat`	Yes	Yes	Communication Manager

Connection type	Server	Numbering format	Country code required?	Plus (+) sign required?	Action
		ional E.164 number			automatically inserts the plus (+) sign
SIP	other	Full internat ional E.164 number	Yes	Yes	The system sets the **Prepend '+' to Calling Number** field on the Protocol Variation screen of the SIP trunk group to y
SIP	other	National E.164 number	No	No	Not applicable
Non-SIP	other	National E.164 number	No	No	Not applicable
Non-SIP	other	National E.164 number	Yes	No	The system sets the **Format** field on an ISDN trunk group to intl-pub

5. In the **Total CPN Len** field, type the total number of digits to be transmitted.

   Note:

   The value in the **CPN Prefix** field is combined with the extension that matches the entry on the NUMBERING - PUBLIC/UNKNOWN FORMAT screen. If the length of the number that is generated is longer than the length defined in the **Total CPN Len** field, then the system deletes the leading digits from the extension until the length of the number is equal to the length defined in the **Total CPN Len** field.

6. Save the changes.

Validating the minimum time of network stability

About this task

Use this procedure to set the minimum time of network stability to three minutes. With the three-minute timer, the gateway can failback to the Communication Manager feature server or evolution server when it becomes available. The three-minute timer also prevents unnecessary failback and failover when the network is unreliable.

Procedure

1. Type `change system-parameters mg-recovery-rule n`, where *n* is the rule number, and press Enter. For example, `change system-parameters mg-recovery-rule 1`.

   The system displays the SYSTEM PARAMETERS MEDIA GATEWAY AUTOMATIC RECOVERY RULE screen.
2. In the **Minimum time of network stability** field, type `3`.
3. Save the changes.

Validating gateway recovery rule

Procedure

1. Type `change media-gateway x`, where *x* is the gateway number, and press Enter.

   The system displays the MEDIA GATEWAY x screen.
2. In the **Recovery Rule** field, type the recovery rule number associated with the gateway or type `none` to disable the recovery rule.

   The value `none` indicates that the system does not accept any automatic fallback registrations.

   You can apply a single rule to all gateways, or each gateway can have its own rule and any permutation in between. You can administer the recovery rule by using the **system-parameters mg-recovery-rule** command.
3. Save the changes.

Adding a privileged administrator

About this task

Use the following procedure to add a privileged administrator account that is a member of the **suser** group. This account should be used only with System Manager.

Procedure

1. Log in to the Communication Manager server System Management Interface (SMI) Web page.
2. Click **Administration** > **Server (Maintenance)**.
3. In the navigation pane on the left-side of the page, in the **Security** section, click **Administrator Accounts**.
4. Select **Add Login**.
5. Select **Privileged Administrator**.
6. Click **Submit**.

   The system displays the Administrator Accounts -- Add Login: Privileged Administrator page.
7. In the **Login Name** field, type your login name.
8. In the **Password** field, type your password.
9. In the **Re-enter password** field, type the same password that you typed in the **Password** field.
10. In the **Force password/key change on next login** field, select `No`.
11. Click **Submit**.

System Manager Administration

Creating a Communication Manager managed element

Procedure

1. Log on to the System Manager Web interface.
2. Click **Services** > **Inventory**.

3. In the navigation pane on the left side of the page, click **Inventory** > **Manage Elements**.
4. Click **New**.
5. In the **Type** field, select **Communication Manager**.
6. In the **Name** field, type a descriptive name for the Communication Manager server.
7. In the **Hostname or IP Address** field, type the IP address of the Communication Manager server.
8. In the **Login** field, type the login name that you created earlier for the privileged administrator account.
9. In the **Password** field, type the password that you created earlier for the privileged administrator account.
10. In the **Confirm Password** field, type the same password that you typed in **Password** field.

    Note:

    Do not use services logins, such as craft, dadmin, and inads. To allow System Manager access to Communication Manager, in the **Login** and **Password** fields, you must type the same login information that you entered using the *Adding a privileged administrator* procedure. Synchronization does not occur unless the Communication Manager login administration is done.
11. Select the **SSH Connection** field.
12. In the **Port** field, type `5022`.
13. Click **Commit**.

Synchronizing Communication Manager data

About this task

After adding the Communication Managermanaged element, System Manager automatically attempts to synchronize with Communication Manager. Use the following procedure if synchronization has not started.

Procedure

1. Log on to the System Manager Web interface.
2. Click **Services** > **Inventory**.
3. In the navigation pane on the left side of the page, click **Inventory** > **Synchronization** > **Communication System**.

4. Select the appropriate Communication Manager server.
5. Scroll down and select the **Initialize data for selected devices** field.
6. Click **Now**.

   The system displays the status alert icon.

   The synchronization process might take several minutes. Click **Refresh** to show the current synchronization status. When synchronization is completed, the **Sync Status** field displays **Completed** .

Adding a Communication Manager server as a SIP entity

About this task

Use the following procedure to add the Communication Manager feature or evolution server as a SIP entity. Do not use adaptation on the Communication Manager server so that the SIP headers created by the Communication Manager server are maintained for proper application sequencing and routing.

Procedure

1. Log on to the System Manager Web interface.
2. Click **Elements** > **Routing** .
3. In the navigation pane on the left side of the page, click **Routing** > **SIP Entities**.
4. Click **New**.
5. In the **Name** field, type a descriptive name for the Communication Manager server.
6. In the **FQDN or IP Address** field, type the IP address of the Communication Manager server.
7. In the **Type** field, select **CM**.
8. In the **Notes** field, type a short description for the Communication Manager server.
9. In the **Location** field, select the location of the Communication Manager server.
10. In the **Time Zone** field, select the appropriate time zone.
11. Click **Commit**.

Adding a Survivable Remote server as a SIP entity

Procedure

1. Log on to the System Manager Web interface.
2. Click **Elements** > **Routing**.
3. In the navigation pane on the left side of the page, click **Routing** > **SIP Entities**.
4. Click **New**.
5. In the **FQDN or IP Address** field, type the IP address of the security module of the Survivable Remote Session Manager server.
6. In the **Type** field, select **Session Manager**.
7. Click **Commit**.

Creating entity links

About this task

When applicable, create the entity links between the following:

- Each Session Manager server and Communication Manager feature server or evolution server.
- Survivable Remote Session Manager server and Communication Manager feature server or evolution server.

If you use separate entities and entity links, such as for an feature server and trunk gateway configuration, you must administer two entity links for each entity on the Survivable Remote server. However, if you use only one entity and entity link, such as for an evolution server configuration, you must administer only one entity link on the Survivable Remote server.

Procedure

1. Log on to the System Manager Web interface.
2. Click **Elements** > **Routing**.
3. In the navigation pane on the left side of the page, click **Routing** > **Entity Links**.
4. Click **New**.
5. In the **Name** field, type a descriptive name for the entity link.
6. In the **SIP Entity 1** field, select the Survivable Remote Session Manager server.
7. In the **Protocol** field, select `tls`.

8. In the **Port** field, type `5061`.
9. In the **SIP Entity 2** field, select the Communication Manager server.
10. In the **Port** field, type `5061`.
11. In the **Connection policy** list box, select `Trusted`.
12. **(Optional)** In the **Notes** field, type a short description about the entity link.
13. Click **Commit**.

Checking the connections

Procedure

1. On the Communication Manager SAT interface, perform the following steps:
   a. Type the `list history` command.
   b. Verify that you are logged in to Session Manager.
   c. Verify that the initial data synchronization has begun.
2. On the System Manager Web interface, perform the following steps:
   a. Click **Elements** > **Session Manager**.
   b. Verify that the Session Manager server is active.
   c. In the navigation pane on the left side of the page, click **Session Manager** > **System Status** > **SIP Entity Monitoring**.
   d. From the **All Monitored SIP Entities** list, select the Communication Manager server.
   e. Verify that the value of the **Link Status** field is Up.

Administering the Communication Manager server as an application

Procedure

1. Log on to the System Manager Web interface.
2. Click **Elements** > **Session Manager**.
3. In the navigation pane on the left side of the page, click **Session Manager** > **Application Configuration** > **Applications**.
4. Click **New**.

5. In the **Name** field, type a descriptive name for the application.
6. In the **SIP Entity** field, select the Communication Manager server.
7. **(Optional)** In the **Description** field, type a short description for the application.
8. Leave the **Application Handle** and **URI Parameters** fields blank.
9. Click **Commit**.

Administering Communication Manager in an application sequence

About this task

Use the following procedure to create an application sequence for the Communication Manager server.

Important:

If you have configured Communication Manager as an evolution server, Communication Manager must be the last application in the origination vector and must be the first application in the termination vector. Communication Manager as an evolution server operates in the full-call model. Therefore, there is no flexibility in the position of the applications with respect to Communication Manager.

Procedure

1. Log on to the System Manager Web interface.
2. Click **Elements** > **Session Manager**.
3. In the navigation pane on the left side of the page, click **Session Manager** > **Application Configuration** > **Application Sequences**.
4. Click **New**.
5. In the **Name** field, type a descriptive name for the application sequence.
6. In the **Description** field, type a short description for the application sequence.
7. Under the **Available Applications** section, click the plus (+) icon beside the appropriate Communication Manager server.
   On refreshing, the system selects the **Mandatory** field.
8. Click **Commit**.

Adding users

About this task

You can ignore the fields that are not mentioned in the following procedure.

A user can have more than one communication profile.

If there is a secondary Session Manager for a user, the route pattern in Communication Manager must have the following two trunks:

- The first trunk associated with the primary Session Manager
- The second trunk associated with the secondary Session Manager

  The second signaling group must be connected to the secondary Session Manager.

Procedure

1. Log on to the System Manager Web interface.
2. Click **Users** > **User Management**.
3. In the navigation pane on the left side of the page, click **User Management** > **Manage Users**.
4. Click **New**.
5. In the **Identity** section, perform the following steps:
   a. In the **Last Name** field, type the last name of the user.
   b. In the **First Name** field, type the first name of the user.
   c. In the **Middle Name** field, type the middle name of the user.
   d. **(Optional)** In the **Description** field, type a short description for the user.
   e. In the **Login Name** field, type the login name using the appropriate SIP domain in Session Manager.

      The login name must be in the following format: `name@domain.com`.
   f. In the **Authentication Type** field, type `Basic`.
   g. In the **Password** field, type a password that starts with a lower case or an upper case alphabet.
   h. In the **Confirm Password** text box, type the password that you entered in the **Password** field.
   i. In the **Localized Display Name** field, type a name that should be displayed to the calling party.
   j. In the **Endpoint Display Name** field, type the full text name of the user.
   k. In the **Language Preference** field, select a language.
   l. In the **Time Zone** field, select a time zone.
6. In the **Communication Profile** section, perform the following steps:

a. In the **Communication Profile Password** field, type a communication profile password that contains only numeric characters.

Note:

You must use this password in the Endpoint Profile security code and to log in to a telephone.

b. In the **Confirm Communication Profile Password** text box, type the same password that you typed in the **Communication Profile Password** field.
c. Click **New**.
d. In the **Type** field, select **Avaya SIP**.
e. In the **Fully Qualified Address** field, type the extension number of the SIP telephone.
f. Select the correct domain from the drop-down list that follows the **@** sign.
g. Click **Add**.
h. Select the added entry.
i. Click **New**.
j. In the **Type** field, select `Avaya E.164`.
k. If you are using private numbering, administer **Fully Qualified Address**, which is a private handle.

The private handle depends on the numbering format.

l. Select the appropriate domain from the drop-down list that follows the **@** sign.
m. Click **Add**.
n. Click the **Session Manager Profile** arrow.
o. Select **Session Manager Profile**.
p. If applicable, in the **Secondary Session Manager** field, select the appropriate Session Manager server as the backup server.

As soon as you select primary Session Manager and secondary Session Manager, the system displays the count in a table, which is on the right side of the fields.

q. **(Optional)** In the **Origination Application Sequence** field, select the appropriate application sequence name that should be used when calls are routed from the user.
r. **(Optional)** In the **Termination Application Sequence** field, select the appropriate application sequence name that should be used when calls are routed to the user.
s. **(Optional)** In the **Survivability Server** field, select the entity that should be used for survivability.

For a Survivable Remote Session Manager, select the Survivable Remote Session Manager SIP entity.

t. In the **Home Location** field, select the Communication Manager server SIP entity that should be used as the home location for call routing.

7. To verify that the data synchronization is completed, perform the following steps:

a. On the right side of the page, click the **Home** tab.
b. Click **Services** > **Inventory**.
c. In the navigation pane on the left side of the page, click **Inventory** > **Synchronization** > **Communication System**.
d. The system displays the synchronization status in the **Sync Status** column of the table.

8. To assign the user to a Communication Manager station, perform the following steps:

Note:

Do not perform this step until synchronization of the data is completed.

a. Click the **Endpoint Profile** arrow.
b. Select **Endpoint Profile**.
c. In the **System** field, select the Communication Manager server.
d. In the **Profile Type** field, select the profile type.
e. Do not select the **Use Existing Stations** field.
f. In the **Extension** field, type the extension that is administered on the Communication Manager server for the existing or new station.
g. In the **Template** field, select the appropriate template.

For a Session Manager server, use the SIP version of the template, for example, `DEFAULT_9640SIP_CM_6_0`

h. In the **Set Type** field, type the telephone set.
i. The **Security Code** field can be left blank.

The value in the **Security Code** is not used to log in to the telephone.

j. In the **Port** field, select `IP`.
k. In the **Voice Mail Number** field, type the voice mail number.
l. Select the **Delete Endpoint on Unassign of Endpoint from User** field.
m. Select the **Override Endpoint Name** field.

9. Click **Commit**.

Verifying a new SIP user

Procedure

1. Log in to the SIP telephone with the values in the **Extension** and **Password** fields of Endpoint Profile.
2. To verify the registration information, perform the following steps:
   a. Log on to the System Manager Web interface.
   b. Click **Elements** > **Session Manager**.

c. In the navigation pane on the left side of the page, click **Session Manager** > **System Status** > **User Registrations**.
d. In the **User Registrations** table, in the row that displays the details of the user, click **Show**.
e. Click the **Registration Detail** tab, and verify that the information is correct.

3. To verify the station information, perform the following steps:
   a. On Communication Manager SAT interface, type `display station n`, where *n* is the telephone extension of the user.

      The system displays the STATION screen.
   b. Verify that the value of the **Type** field is SIP.
   c. Verify that the value of the **SIP Trunk** is **aar**.
   d. Press **CANCEL** to return to the command prompt.
   e. Type `display off-pbx-telephone station-mapping n`, where *n* is the telephone extension of the user.

      The system displays the STATIONS WITH OFF-PBX TELEPHONE INTEGRATION screen.
   f. For the telephone extension, verify that the value of the **Trunk Selection** field is aar.

Testing Session Manager and Communication Manager calls

Procedure

1. Place five-digit calls from one SIP extension to another.
2. Place 9+11-digit calls from one SIP extension to another.
3. To validate routing, place five-digit calls to a non-SIP telephone on another Private Branch Exchange (PBX) on the Session Manager server.
4. To validate routing, place 9+11-digit calls to a non-SIP telephone on another PBX on the Session Manager server.

Chapter 4: Communication Manager as a trunk gateway

This section describes how to define the connection and routing between Session Manager and Communication Manager configured as a trunk gateway.

Trunk gateway administration checklist

#	Task	Link to description	✔
1	Log in to Communication Manager.		
2	Administer a node name for the IP address of the Session Manager security module.	Adding a node name on page 20	
3	Administer an IP network region to be used in the SIP signaling group connected to Session Manager.	Changing an IP network region on page 20	
4	Administer a non-IMS SIP signaling group.	Adding a non-IMS SIP signaling group on page 42	
5	Administer a SIP trunk group connected to the SIP signaling group.	Adding a SIP trunk group on page 22	
6	Administer the dial plan.	Changing dialplan analysis on page 42	
7	Log in to the System Manager Web interface.		
8	Add the Communication Manager server as a SIP entity.	Adding a Communication Manager server as a SIP entity on page 32	
9	For routing, administer a routing policy with the trunk gateway as the destination.		

#	Task	Link to description	✔
10	Administer the dial pattern that uses the routing policy defined earlier.		

Adding a non-IMS SIP signaling group

Procedure

1. Type `add signaling-group` *next*, and press Enter.
   The system displays the SIGNALING GROUP screen.
2. In the **Group Type** field, type `sip`.
3. In the **IMS Enabled** field, type `n`.
4. In the **Peer Detection Enabled** field, type **y**.
5. In the **Near-end Node Name** field, type `procr`.
6. In the **Far-end Node Name** field, type the name of the Session Manager security module.
7. In the **Far-end Domain** field, type the domain name.
8. In the **Enable Layer 3 Test** field, type `y`.
   If you set the value of this field to `n`, Communication Manager does not monitor the links.
9. Save the changes.

Changing dialplan analysis

About this task

Use the following procedure to administer the dial plan analysis table to route the external numbers through AAR to the non-IMS signaling group and trunk to Session Manager.

Procedure

1. Type `change dialplan analysis`, and press Enter.
   The system displays the DIAL PLAN ANALYSIS TABLE screen.

2. In the **Dialed String** field, type a digit string to be used for trunks.
3. In the **Call Type** field, type `aar`.
4. Save the changes and go to the command prompt.
5. Type `change aar analysis` *xx*, where *xx* is the first two digits of the dialed string.

   The system displays the AAR DIGIT ANALYSIS TABLE screen.
6. For each dialed string on the DIAL PLAN ANALYSIS TABLE screen:
   a. In the **Dialed String** field, type the digit string.
   b. In the **Total Min** field, type the minimum number of digits.
   c. In the **Total Max** field, type the maximum number of digits.
   d. In the **Route Pattern** field, type the route pattern number.
   e. In the **Call Type** field, type `pubu`.
7. Save the changes.

Chapter 5: Communication Manager configured as a feature server and trunk gateway

This section describes how to define the connection and routing between Communication Manager and Session Manager.

Two SIP signaling groups are required between Communication Manager and Session Manager:

- A non-IMS signaling group to gain access to the trunk gateway part of Communication Manager
- An IMS-enabled signaling group for connection to the feature server

For IMS users, all calls must route to Session Manager. For example, an incoming public trunk call to an IMS user must route to Session Manager on a non-IMS SIP signaling group which in turn routes the call back to the Communication Manager trunk gateway by using the IMS-enabled signaling group connected to the feature server part of Communication Manager.

Feature server and trunk gateway administration checklist

#	Administration action	Link to action	✔
1	Log in to the Communication Manager SAT interface.		
2	Add a node name for the IP address to the Session Manager security module.	Adding a node name on page 20	
3	Define an IP network region to be used in the signaling group connected to Session Manager.	Changing an IP network region on page 20	
4	Add an IMS-enabled SIP signaling group.	Adding an IMS-enabled SIP signaling group on page 46	
5	Add a SIP trunk group to the SIP signaling group.	Adding a SIP trunk group on page 22	

#	Administration action	Link to action	✔
6	Administer the dial plan to route the external numbers through AAR to the non-IMS signaling group and trunk to Session Manager.		
7	Administer Communication Manager on System Manager.	Adding a Communication Manager server as a SIP entity on page 32	
8	Add a non-IMS SIP signaling group and allow Incoming Dialog Loopbacks.	Adding a non-IMS SIP signaling group and allowing dialog loopbacks on page 47	
9	Set up routing from the trunk gateway to the feature server.	Setting up routing from the trunk gateway to the feature server on page 48	
10	Set up routing from the feature server to the trunk gateway.	Setting up routing from the feature server to the trunk gateway on page 49	
11	Administer public numbering.	Public numbering on page 50	
12	Set up routing on System Manager.	Administering routing for feature server and trunk gateway on System Manager on page 51	

Adding an IMS-enabled SIP signaling group

About this task

Use the following procedure to add an IMS-enabled SIP signaling group from the Communication Manager PROCR feature server to the Session Manager security module.

Procedure

1. Type `add signaling-group next`, and press Enter.
   The system displays the SIGNALING GROUP screen.
2. Note the value of the **Group Number** field.
3. In the **Group Type** field, type `sip`.
4. In the **IMS Enabled** field, type `y`.
5. In the **Transport Method** field, type `tls`.

6. In the **Peer Detection Enabled**, type `y`.

   If you set the value the **Peer Detection Enabled** field to `y`, a message interchange takes place between Communication Manager and the connected SIP server. When the SIP signaling group is put into service, the system sets the value of the **Peer server Type** field to `SM`.

7. In the **Near-end Node Name** field, type `procr`.
8. In the **Far-end Node Name** field, type the name of the Session Manager security module.
9. In the **Far-end Domain** field, type the domain name that you typed in the **Authoritative Domain** field on the IP NETWORK REGION screen.
10. In the **Enable Layer 3 Test** field, type `y`.

    If you set the value of this field to `n`, Session Manager does not monitor the links.

11. Save the changes.

Adding a non-IMS SIP signaling group and allowing dialog loopbacks

Procedure

1. Type `add signaling-group` *`next`*, and press Enter.

   The system displays the SIGNALING GROUP screen.

2. In the **Group Type** field, type `sip`.
3. In the **Transport Method**, type `tcp`.
4. In the **IMS Enabled** field, type `n`.
5. In the **Near-end Node Name** field, type `CLAN`.
6. In the **Far-end Node Name** field, type the name of the Session Manager SM100 board.
7. In the **Near-end Listen Port** field, type a port number other than the port number defined in the IMS signaling group. For example, `5070`.
8. In the **Far-end Listen Port** field, type the port number that you typed in the **Far-end Listen Port** field.
9. In the **Far-end Domain** field, type the domain name that you typed in the **Authoritative Domain** field on the IP NETWORK REGION screen.
10. In the **Incoming Dialog Loopbacks** field, type `allow`.

11. In the **Enable Layer 3 Test** field, type `y`.

    If you set the value of this field to `n`, Communication Manager does not monitor the links.

12. Save the changes.

Setting up routing from the trunk gateway to the feature server

About this task

Use the following procedure to set up routing for an incoming trunk call to an IMS user. Communication Manager must prepend digits to the extension of the IMS user to route the call through a non-IMS trunk to Session Manager. Communication Manager deletes the prepended digits in the route pattern entry.

Procedure

1. For the ARS digit conversion, perform the following steps:
   a. Type `change ars digit-conversion x`, where *x* is a digit string, and press Enter.

      The system displays the ARS DIGIT CONVERSION TABLE screen.
   b. In the **Matching Pattern** field, add an entry for the incoming trunk call number.
   c. In the **Min** field, type the minimum number of digits.
   d. In the **Max** field, type the maximum number of digits.
   e. In the **Del** field, type the number of digits that Communication Manager must delete from the trunk call number.
   f. In the **Replacement String** field, type the digits that Communication Manager must prepend to the trunk call number. For example, `99`.
   g. In the **Net** field, type `aar`.
   h. In the **Conv** field, type `n`.
   i. In the **ANI Req** field, type `n`.
   j. Save the changes.
2. For the AAR analysis, perform the following steps:
   a. Type `change aar analysis x`, where *x* is a digit string, and press Enter.

      The system displays the ARS DIGIT ANALYSIS TABLE screen.
   b. In the **Dialed String** field, type `xxyy`, where `xx` are the digits that you entered for the **Replacement String** field on the ARS DIGIT CONVERSION TABLE screen, and `yy` are the first two digits of the extension of the IMS user.

c. In the **Min** field, type the minimum number of digits.
d. In the **Max** field, type the maximum number of digits.
e. In the **Route Pattern** field, type a route pattern number to the non-IMS trunk group for the dialed string digits.
f. In the **Call Type** field, type `pubu`.
g. In the **ANI Req** field, type `n`.
h. Save the changes.

3. To administer the route pattern, perform the following steps:
   a. Type `change route-pattern x`, where `x` is the route pattern number that you entered in the **Route Pattern** field on the ARS DIGIT ANALYSIS TABLE screen.
   b. In the **Grp No** field, type the group number of the non-IMS trunk group.
   c. In the **No. Del Dgts** field, type the number of digits that Communication Manager must delete in the non-IMS trunk.
   d. Save the changes.

Setting up routing from the feature server to the trunk gateway

About this task

For calls from the feature server to the public network, you must administer routing for:

- Outgoing calls from the feature server to Session Manager through the IMS trunk
- Incoming calls to the trunk gateway through the non-IMS trunk

Procedure

1. To administer the ARS analysis, perform the following steps:
   a. Type `change ars analysis x`, where *x* is a digit string.
      The system displays the ARS DIGIT ANALYSIS TABLE screen.
   b. In the **Dialed String** field, type the digits.
   c. In the **Min** field, type the minimum number of digits.
   d. In the **Max** field, type the maximum number of digits.
   e. In the **Route Pattern** field, type the route pattern number.
   f. In the **Call Type** field, type `pubu`
   g. Save the changes.
2. To administer Route Pattern 1, perform the following steps:
   a. Type `change route–pattern 1`.

b. In the **No. Del Dgts** field, type the number of digits that are a part of the international dialing prefix and that Communication Manager must delete.

   For example, in the U.S., the prefix is 011. Therefore, the number of digits to delete is `3`.

c. In the **Inserted Digits** field, type **p** to allow Communication Manager to add a plus (+) sign to the beginning of the number.

d. Save the changes.

3. To administer Route Pattern 2, perform the following steps:

   a. Type `change route–pattern 2`.

   b. In the **No. Del Dgts** field, type the number of digits that are a part of the international dialing prefix and that Communication Manager must delete.

      For example, in Germany, the national prefix is 0, so the number of digits to delete is `1`.

   c. In the **Inserted Digits** field, type `p##` , where `p##` is the country code.

   d. Save the changes.

4. To administer Route Pattern 2, perform the following steps.

   This route pattern is only needed for countries where dialing of subscriber numbers is allowed, for example, Germany. A subscriber number is a public number without the country code and the national destination code or city code.

   a. Type `change route–pattern 3`.

   b. In the **Inserted Digits** field, type `p##`, where `p##` is the combination of the country code and the national destination code or city code.

   c. Save the changes.

5. On the trunk gateway, administer the Incoming Call Handling Treatment (ICHT) for each non-IMS trunk to insert digits for routing to the public trunk.

   a. Type `change inc-call-handingling-trmt trunk-group x`, where *x* is the non-IMS trunk group number.

   b. Type ICHT entries with different lengths.

      Public numbers can be of different lengths and must be handled accordingly.

   c. Save the changes.

Public numbering

The following sections describes the handling for public numbering.

Calls to the public network:

Endpoint > Communication Manager feature server > Session Manager > Communication Manager trunk gateway > public network

Even if the Communication Manager feature server is administered for Private Enterprise Canonical numbers, the PAI for a call to the public network can be changed to a Public Long Number by choosing a public call type in the respective Route Pattern, for example, pubu in the **Call Type** field on the ARS DIGIT ANALYSIS TABLE screen.

The PAI can then be adapted by the ICHT on the Communication Manager trunk gateway or by the number adaptation module in Session Manager. Be careful to have no overlaps with the entries for the called number.

Calls from the public network:

Public network > Communication Manager trunk gateway > Session Manager > Communication Manager feature server > Session Manager > endpoint

In Session Manager, all public numbers should be international with the leading plus (+) sign. The number adaptation module in Session Manager adapts the national numbers, which are received from the public network, to international numbers on the SIP trunk.

Administering routing for feature server and trunk gateway on System Manager

About this task

Although the feature server functionality and the trunk gateway functionality are within the same Communication Manager, both need to be configured using the System Manager routing as separate SIP entities.

Procedure

1. Define the entity and entity link for the feature server and the trunk gateway as a TCP connection with the ports defined in the Communication Manager signaling groups.

   For example, TCP port 5060 for feature server, TCP port 5070 for trunk gateway.

2. For the routing from the feature server to the trunk gateway, define a dial pattern and routing policy to route an incoming plus (+) sign to the trunk gateway.

   For more information, see the Routing Policy Details screen on System Manager.

3. To add the SIP domains of the Communication Manager server, perform the following steps:

   a. Log on to the System Manager Web interface.
   b. Click **Elements** > **Routing**.
   c. In the navigation pane on the left side of the page, click **Routing** > **Domains**.

d. Click **New**.
e. In the **Name** field, type the domain name for Communication Manager.
f. In the **Type** field, select **cm**.
g. Click **Commit**.
h. Click **New**.
i. In the **Name** field, type the domain name for Session Manager.
j. In the **Type** field, select **sip**.
k. Click **Commit**.

4. To administer Communication Manager as a SIP entity, perform the following steps:
   a. On the right side of the System Manager Web interface, click the **Home** tab.
   b. Click **Elements** > **Routing**.
   c. In the navigation pane on the left side of the page, click **Routing** > **SIP Entities**.
   d. Click **New**.
   e. In the **Name** field, type the name of Communication Manager.
   f. In the **FQDN or IP Address** field, type the IP address for Processor Ethernet of Communication Manager.

      The IP address is the near end in the signaling group to Session Manager.
   g. In the **Type** field, select **CM**.
   h. Click **Commit**.
5. To create an entity link from the Session Manager entity to the Communication Manager entity, perform the following steps:
   a. On the right side of the System Manager Web interface, click the **Home** tab.
   b. Click **Elements** > **Routing**.
   c. In the navigation pane on the left side of the page, click **Routing** > **Entity Links**.
   d. Click **New**.
   e. In the **Name** field, type a descriptive name for the entity link.
   f. For **SIP Entity 1**, select the Session Manager entity.
   g. In the **Port** field, type the port number.
   h. For **SIP Entity 2**, select the Communication Manager entity.
   i. In the **Port** field, type the port number.
   j. Click **Commit**.
6. To administer Communication Manager as an application, perform the following steps:
   a. On the right side of the System Manager Web interface, click the **Home** tab.
   b. Click **Elements** > **Inventory**.
   c. In the navigation pane on the left side of the page, click **Inventory** > **Manage Elements**.
   d. Click **New**.
   e. In the **Type** field, select **CM**.

f. In the **Application** section, type the name of the Communication Manager server.
   The system deactivates the selected type.

   To change the value of the **Type** field, click **Reset**.
g. In the **Node** field, type the management IP address that is used to gain access to the Communication Manager SAT interface.
h. In the **Attributes** section, in **Login** field, type the SSH SAT login name.
i. In the **Attributes** section, in **Password** field, type the SSH SAT password.
j. Select the **Is SSH Connection** field.
k. In the **Port** field, type `5022`.
l. Click **Commit**.
   The system schedules the Communication Manager entity for an initial incremental hourly data synchronization.

Chapter 6: Survivable Remote Session Manager documentation roadmap

Installation and administration of the Survivable Remote Session Manager server requires using more than one book. The following table contains the tasks in order for installing, configuring, administering, and testing a Survivable Remote Session Manager server and which book to use for the task.

You must complete the following tasks on the Communication Manager and Session Manager servers and these tasks are not a part of the roadmap:

- Install Communication Manager and install the license file. Configure Communication Manager either as a feature server or an evolution server and ensure that the server is operational.
- Administer Communication Manager as a SIP entity on Session Manager.

Table 1: Survivable Remote Session Manager documentation roadmap

Task	Book to use	Notes
Administer the survivability options on the Communication Manager server.	*Implementing Avaya Aura® Communication Manager*, 03-603558	
Administer the Survivable Communication Manager server by using the System Manager Web interface.	*Implementing Avaya Aura® Communication Manager*, 03-603558	
Administer the Survivable Remote Session Manager server on Communication Manager.	*Implementing Avaya Aura® Session Manager*, 03-603473	See the *Administering Survivable Remote Session Manager SAT administration checklist* section.
If installing the simplex Survivable Remote template on an Avaya S8800 server, install the S8800 server.	*Installing the Avaya S8800 Server for Avaya Aura® Communication Manager*, 03-603444	
If installing the simplex Survivable Remote template on an Avaya S8510 server, install or upgrade the S8510 server.	*Upgrading to Avaya Aura® Communication Manager,* 03–603560	If the S8510 server does not have 8GB of memory, upgrade the server. The S8510 server requires Communication Manager Migration kit.

Task	Book to use	Notes
If installing the embedded Survivable Remote template, install the Avaya S8300D server on the gateway.	• *Quick Start for Hardware Installation: Avaya G250 Branch Gateway*, 03-300433 • *Quick Start for Hardware Installation: Avaya G350 Branch Gateway*, 03-300148 • *Quick Start for Hardware Installation: Avaya G430 Branch Gateway*, 03-603236 • *Quick Start for Hardware Installation: Avaya G450 Branch Gateway*, 03-602053 • *Quick Start for Hardware Installation: Avaya G700 Branch Gateway*, 555-233-150	Refer to the book for your particular Gxxx gateway.
Install System Platform on the server.	*Implementing Avaya Aura® Communication Manager*, 03-603558	
Install the license and the authentication files	*Implementing Avaya Aura® Communication Manager*, 03-603558	
Install the appropriate Communication Manager template through the System Platform Web console.	*Implementing Avaya Aura® Communication Manager*, 03-603558	
Administer the IP address of the Survivable Remote Session Manager security module for Network Configuration of System Platform.	*Implementing Avaya Aura® Communication Manager*, 03-603558	In the SIP signaling groups, the far-end node names with the core Session Manager instance are replaced with the IP address of the Survivable Remote Session Manager security module.
Administer the Survivable Remote Session Manager server through the System Manager Web interface.	*Implementing Avaya Aura® Session Manager*, 03-603473	See the *Survivable Remote Session Manager administration checklist* section.
Verify the registration.	*Implementing Avaya Aura® Session Manager*, 03-603473	
Test the installation.	*Implementing Avaya Aura® Session Manager*, 03-603473	

Chapter 7: SIP telephone administration

Administering 96xx SIP telephones

About this task

A telephone can download settings from a file server if the environment is set up for the telephone.

Procedure

1. Go to the configuration menu:
   a. On the physical telephone: Press the **Mute** button on the telephone and use the keypad to type **CRAFT#**.
   b. On the soft telephone: Type `admin options`
2. In the **SIP Global Settings** menu:
   a. In the **SIP Domain** field, type the domain name of the Session Manager server.
   b. In the **Avaya Environment** field, select `auto`.
   c. In the **Reg. Policy** field, select `simulateous`.
   d. Leave the **Avaya Config Server:** field blank.
3. In the **SIP Proxy Settings** menu:
   a. In the **SIP Proxy Server** field, type the IP address of the primary Session Manager server that the telephone should register to, and if applicable, type the IP address of the secondary Session Manager server as the second entry.
   b. In the **Transport** field, select `TCP` or `TLS`.
   c. In the **SIP Port** field, type the port number as defined in the Session Manager SIP entity, for example, `5060` for TCP.
4. To access the correct file server, in the **SSON** menu, type the SSON number.

Chapter 8: Feature name extension administration

The following steps describe how to administer feature name extensions. Feature name extensions must first be administered on the Communication Manager SAT interface, and then administered for Session Manager on the System Manager Web interface.

Administering feature name extensions on Communication Manager

Procedure

1. On the Communication Manager SAT interface, type `change feature-access-codes`.

   The system displays the FEATURE ACCESS CODE (FAC) screen.
2. Type the appropriate codes for the features that you want to enable.
3. Save the changes and go to the command prompt.
4. Type `change off-pbx-telephone feature-name-extensions set 1`.

   The system displays the EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME screen.
5. Type the extension that you want to use for a particular feature.
6. Save the changes.

Administering feature name extensions on System Manager

Procedure

1. Log on to the System Manager Web interface.

2. Click **Elements** > **Session Manager**.
3. In the navigation pane on the left side of the page, click **Session Manager** > **Application Configuration** > **Implicit Users**.
4. Click **New**.
5. In the **Pattern** field, type the telephone extension.
6. In the **Min** field, type the minimum number of digits to be matched.
7. In the **Max** field, type the maximum number of digits to be matched.
8. In the **Description** field, type a short description. For example, Turn on EC500.
9. In the **SIP Domain** field, select the appropriate SIP domain.
10. In the **Origination Application Sequence** field, select the appropriate originating feature server name.
11. In the **Termination Application Sequence** field, select the appropriate terminating feature server name.
12. Click **Commit**.

Appendix A: Numbering configuration

Numbering

Enterprise Canonical Number (ECN) is a number that is unique to Session Manager. The number can be a public long number, a private long number, or a short or internal number.

Public Number must begin with a plus (+) sign.

Private Alias for public numbering is needed when telephones are unable to register with the plus (+) sign, such as Avaya physical telephones.

OPTIM Table converts a registration number, which might be an ECN, to a short number.

Public Numbering Table converts a short number to a public long number (called party or Request-URI and calling party or PAI). The short number is added as an avext parameter to the PAI and the Contact headers for messages to the telephone.

Private Numbering Table converts a short number to a private long number (called party or Request-URI and calling party or PAI). The short number is added as an avext parameter to the PAI and the Contact headers for messages to the telephone.

ICHT (Incoming Call Handling Treatment) converts a public or private long number to a short number (called party or Request-URI and calling party or PAI).

Numbering administration

In general, the numbering administration in Communication Manager is a bit complicated due to various tables that are used to adapt the calling and called numbers. Furthermore, the numbering type settings, such as AAR, Route Pattern, and Trunk, have an assigned priority. The administration of the users and handles in Session Manager must match the numbering form used in Communication Manager.

For Communication Manager Release 6.0, the trunk numbering setting is used to adapt the calling party number. The entries in AAR, Route Pattern, and ARS adapt the called party number.

Following fields are evaluated for the numbering adaptation:

- **Numbering Format** field on the TRUNK GROUP screen:

- public: calling number is adapted to the entry in the **public-unknown-numbering** table.
- unk-pvt: calling number is adapted to the entry in the **private-numbering** table.

Although the trunk is set to private, the calling number is adapted to a public number when the called number is determined to be public by the settings of the AAR and Route Pattern for the called number. For this adaptation, a matching entry is required for the calling number in the **public-unknown-numbering** table.

- **Call type** field on the AAR DIGIT ANALYSIS TABLE screen:
  - aar: the called number is determined to be a public number. The calling number is also adapted to a public number.
  - pubu: the called number is determined to be a public number. The calling number is also adapted to a public number.
  - unku: the called number is determined to be a private number.

  The **Call type** setting in AAR has a higher priority than **Numbering Format** in the trunk group. When the calling party number is adapted to public, a matching entry is required in the **public-unknown-numbering** table.
- **Numbering Format** field on the ROUTE PATTERN screen:
  - pub-unk: the called number is determined to be a public number. The calling number is also adapted to a public number.
  - unk-unk: the called number is determined to be a private number.
  - blank: the numbering setting from AAR and trunk group are used.

  The **Numbering Format** setting in Route Pattern has a higher priority than **Call type** in AAR. When the calling party number is adapted to public, a matching entry is required in the **public-unknown-numbering** table.

For more information about administration settings for the different numbering types, see the following table.

The numbering type used for registration needs to be differentiated from the numbering type that is signaled to the network.

Table 2: Administration settings for different numbering types

Registration numbering type	Signaled numbering type	Administration
private short	private short	Private short numbering on page 63.
private long	private long	Private long numbering on page 64.
private long	public	Long private numbering and public signaling on page 66.
public plus (+) sign	public	Public numbering on page 68.

private short or long (variation 1)	call to public number	Call to public extension (variation 1) on page 70.
private short or long (variation 2)	call to public number	Call to public extension (variation 2) on page 72.

The settings in the different routing and numbering forms depend on the numbering format that is used. What is correct for private numbering may not be correct for public numbering.

Recommendations

- Use adaptation modules only on the entry and exit points to and from Avaya Aura® network. Do not use them on the interface to sequenced applications.
- Use only real and existing public numbers. The number should always be Enterprise Canonical. Numbers without a public representation must be in the Private Long format to be Enterprise Canonical.
- Use Automatic Alternate Routing (AAR) or Automatic Routing Selection (ARS) to reach extensions on another Communication Manager.

Private short numbering

Private short numbering format uses the private extension. In Session Manager, only the private short number is administered. In Communication Manager, the described administration does not change the internal extension.

The configuration is for the following numbering types:

- Registration numbering type: private short
- Signaled numbering type: private short

SAT screen	Page number	Field	Value	Comment
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION	1	**Phone Number**	Extension number	
	1	**Trunk Selection**	aar	For station types 90xxSIP, the **Trunk Selection** field is set on the last page of the STATION screen.

SAT screen	Page number	Field	Value	Comment
TRUNK GROUP	3	**Numbering Format**	private	
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Extension number	
NUMBERING - PRIVATE FORMAT	1	**Ext Code**	Extension number or patter for extension numbers	
	1	**Trk Grp (s)**	blank	blank means it applies to all trunks.
	1	**Private Prefix**	blank	
	1	**Total Len**	Extension length	
NUMBERING - PUBLIC/ UNKNOWN FORMAT				No entries.
ROUTE PATTERN	1	**Grp Num**	Trunk group number	List trunk groups with trunks to primary Session Manager listed first.
	1	**FRL**	0	
	1	**Numbering format**	blank	
INCOMING CALL HANDLING TREATMENT				No entries.

Private long numbering

Private long numbering format uses the private extension extended by a prefix. In Session Manager, only the private long number is administered. In Communication Manager, the described administration shortens and extends the long number to the Communication Manager internal extension.

The configuration is for the following numbering types:

- Registration numbering type: private long
- Signaled numbering type: private long

SAT screen	Page number	Field	Value	Comment
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION	1	**Phone Number**	Long private extension number	
	1	**Trunk Selection**	aar	For station types 90xxSIP, the **Trunk Selection** field is set on the last page of the STATION screen.
TRUNK GROUP	3	**Numbering Format**	private	
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Long private extension number	**Dialed String** is the extension or a pattern of extensions.
	1	**Route Pattern**	Pattern to route to Session Manager	
	1	**Call Type**	unku	
NUMBERING - PRIVATE FORMAT	1	**Ext Len**	Extension length	
	1	**Ext Code**	Extension number or patter for extension numbers.	
	1	**Trk Grp (s)**	blank	blank means it applies to all trunks.
	1	**Private Prefix**	Private prefix	
	1	**Total Len**	Extension length and prefix	
NUMBERING - PUBLIC/				No entries.

SAT screen	Page number	Field	Value	Comment
UNKNOWN FORMAT				
ROUTE PATTERN	1	**Grp Num**	Trunk group number	List trunk groups with trunks to primary Session Manager listed first.
	1	**FRL**	0	
	1	**Numbering format**	blank	
INCOMING CALL HANDLING TREATMENT	1	**Len**	Length of private long number.	
	1	**Number Digits**	Private prefix	
	1	**Del**	Length of private prefix	
	1	**Insert**	blank	

Long private numbering and public signaling

Long private numbering format uses the private extension extended by a prefix. In Session Manager, the private long number and the public number is administered. In Communication Manager, the described administration changes the private long number to the extension and the outgoing direction to the public number.

The configuration is for the following numbering types:

- Registration numbering type: private long
- Signaled numbering type: public

SAT screen	Page number	Field	Value	Comment
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION	1	**Phone Number**	Long private extension number	

SAT screen	Page number	Field	Value	Comment
	1	**Trunk Selection**	aar	For station types 90xxSIP, the **Trunk Selection** field is set on the last page of the STATION screen.
TRUNK GROUP	3	**Numbering Format**	public	
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Long private extension number	**Dialed String** is the extension or a pattern of extensions.
	1	**Route Pattern**	Pattern to route to Session Manager	
	1	**Call Type**	unku	
NUMBERING - PRIVATE FORMAT	1			No entries.
NUMBERING - PUBLIC/ UNKNOWN FORMAT	1	**Ext Len**	Extension length	
	1	**Ext Code**	Extension number or pattern for extension numbers	
	1	**Trk Grp (s)**	Trunk number or blank	blank means it applies to all trunks.
	1	**CPN Prefix**	Public prefix to the extension without the plus (+) sign. The plus (+) sign is added automatically.	
	1	**Total Len**	Extension length and CPN prefix	

SAT screen	Page number	Field	Value	Comment
ROUTE PATTERN	1	**Grp Num**	Trunk group	List trunk groups with trunks to primary Session Manager listed first.
	1	**FRL**	0	
	1	**Numbering format**	unk-unk	
INCOMING CALL HANDLING TREATMENT	1	**Len**	Length of public long number	
	1	**Number Digits**	Public prefix	
	1	**Del**	Length of public prefix	
	1	**Insert**	blank	
INCOMING CALL HANDLING TREATMENT	1	**Len**	Length of private long number	
	1	**Number Digits**	Private prefix	
	1	**Del**	Length of private prefix	
	1	**Insert**	blank	

Public numbering

A plus (+i) sign is required as a login character in public numbering format. Therefore, only softphones can use this numbering format. For all other telephones, this numbering is realized with a private alias using the private long and public signalling configuration.

In Session Manager, only the public number is administered.

In Communication Manager, the described administration shortens and extends the public number to the Communication Manager internal extension.

The configuration is for the following numbering types:

- Registration numbering type: public (+)
- Signaled numbering type: public

SAT screen	Page number	Field	Value	Comment
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION	1	**Phone Number**	Public number without the leading plus (+) sign	
	1	**Trunk Selection**	aar	For station types 90xxSIP, the **Trunk Selection** field is set on the last page of the STATION screen.
TRUNK GROUP	3	**Numbering Format**	public	
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Public number without the leading plus (+) sign	**Dialed String** is the extension or a pattern of extensions.
	1	**Route Pattern**	Pattern to route to Session Manager	
	1	**Call Type**	pubu	
NUMBERING - PRIVATE FORMAT				No entries.
NUMBERING - PUBLIC/ UNKNOWN FORMAT	1	**Ext Len**	Extension length	
	1	**Ext Code**	Extension number or patter for extension numbers	
	1	**Trk Grp (s)**	Trunk number or blank.	blank means it applies to all trunks.
	1	**CPN Prefix**	Public prefix to the extension without the plus (+) sign. The plus (+)	

SAT screen	Page number	Field	Value	Comment
			sign is added automatically.	
	1	**Total Len**	Extension length and CPN prefix	
ROUTE PATTERN	1	**Grp Num**	Trunk group number	List trunk groups with trunks to primary Session Manager listed first.
	1	**FRL**	0	
	1	**Numbering format**	unk-unk	
INCOMING CALL HANDLING TREATMENT	1	**Len**	Length of public long number.	
	1	**Number Digits**	Public prefix	
	1	**Del**	Length of public prefix	
	1	**Insert**	blank	

Call to public extension (variation 1)

Although private numbering is used for registration and signaling, the calling private number is adopted to a public number when the called used is identified as a public number. For example, call to a public network.

In Communication Manager, additional administration is required for the private numbering.

The administration for this version requires the public number to be administered as a secondary Session Manager.

The configuration is for the following numbering types:

- Registration numbering type: private short or long
- Signaled numbering type: call to public number

SAT screen	Page number	Field	Value	Comment
TRUNK GROUP	3	**Numbering Format**	private	
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Private long or short number	**Dialed String** is the extension or a pattern of extensions.
	1	**Route Pattern**	Pattern to route to Session Manager	
	1	**Call Type**	unku	
NUMBERING - PRIVATE FORMAT	1	**Ext Code**	Extension number or pattern for extension numbers	
	1	**Trk Grp (s)**	blank	blank means it applies to all trunks.
	1	**Private Prefix**	blank	
	1	**Total Len**	Extension length	
NUMBERING - PUBLIC/ UNKNOWN FORMAT	1	**Ext Len**	Extension length	
	1	**Ext Code**	Extension number or pattern for extension numbers	
	1	**Trk Grp (s)**	Trunk number or blank	blank means it applies to all trunks.
	1	**CPN Prefix**	Public prefix to the extension without the plus (+) sign. The plus (+) sign is added automatically.	

SAT screen	Page number	Field	Value	Comment
	1	**Total Len**	Extension length and CPN prefix	
ROUTE PATTERN	1	**Grp Num**	Trunk group number	List trunk groups with trunks to primary Session Manager listed first.
	1	**FRL**	0	
	1	**Numbering format**	pub-unk	
INCOMING CALL HANDLING TREATMENT				No entries.

Call to public extension (variation 2)

Although private numbering is used for registration and signaling, the calling private number is adopted to a public number when the called used is identified as a public number. For example, call to a public network.

In Communication Manager, additional administration is required for the private numbering.

The administration for this version requires an adaptation in Session Manager for the public number of a user.

The configuration is for the following numbering types:

- Registration numbering type: private short or long
- Signaled numbering type: call to public number

SAT screen	Page number	Field	Value	Comment
TRUNK GROUP	3	**Numbering Format**	private	
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Private long or short number	**Dialed String** is the extension or a pattern of extensions.

SAT screen	Page number	Field	Value	Comment
	1	**Route Pattern**	Pattern to route to Session Manager	
	1	**Call Type**	unku	
NUMBERING - PRIVATE FORMAT	1	**Ext Code**	Extension number or pattern for extension numbers	
	1	**Trk Grp (s)**	blank	blank means it applies to all trunks.
	1	**Private Prefix**	blank	
	1	**Total Len**	Extension length	
NUMBERING - PUBLIC/ UNKNOWN FORMAT				No entries. The adaptation to public is done in Session Manager.
ROUTE PATTERN	1	**Grp Num**	Trunk group number	List trunk groups with trunks to primary Session Manager listed first.
	1	**FRL**	0	
	1	**Numbering format**	unk-unk	
INCOMING CALL HANDLING TREATMENT				No entries.

Index

Numerics

A

C

D

E

F

G

I

L

M

N

O

P

R

S

T

U

V

W