Administering Avaya Aura® Communication Manager Server Options

Release 6.3
03-603479
Issue 4
June 2015

© 2015, Avaya, Inc.
All Rights Reserved.

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 Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner 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 CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. 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 AVAYA CHANNEL PARTNER; 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, 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 7
- Purpose 7
- Intended audience 7
- Document changes since last issue 7
- Related resources 8
  - Documentation 8
  - Avaya Mentor videos 8
- Support 8
- Warranty 9

Chapter 2: Overview 10
- Feature server 10
  - Half-call model 11
- Evolution server 11
  - Full-call model 11
  - Application sequencing in the evolution server 12
- Trunk gateway 12
- Combination feature server and trunk gateway 12

Chapter 3: Communication Manager configured as a feature server or an evolution server 14
- Prerequisites for administering feature server or evolution server 14
- Recommendations 15
- Feature server or evolution server administration checklist 15

Chapter 4: Communication Manager configured as a trunk gateway 18
- Trunk gateway administration checklist 18

Chapter 5: Communication Manager configured as a feature server and trunk gateway 19
- Feature server and trunk gateway administration checklist 19
- Public numbering 20

Chapter 6: Administration procedures 22
- Administration procedures on Communication Manager 22
  - Administering the dial plan 22
  - Administering feature access codes 23
  - Administering an IP network region 23
  - Adding a node name 23
  - Adding a SIP signaling group 24
  - Adding a SIP trunk group 25
  - Administering a route pattern 26
  - Administering the uniform dial plan 27
  - Administering the AAR analysis table 27

Administering the ARS analysis table ... 28
Administering the proxy route ... 29
Administering the incoming call handling treatment ... 29
Adding a Communication Manager Survivable Remote Processor ... 30
Administering the public or unknown numbering format ... 30
Validating the minimum time of network stability ... 31
Validating the gateway recovery rule ... 32
Saving translations ... 32
Checklist for setting up routing from the trunk gateway to the feature server ... 32
Administering the ARS digit conversion table ... 33
Checklist for setting up routing from the feature server to the trunk gateway ... 33
Adding a privileged administrator account ... 34
Administration procedures on System Manager ... 35
Creating a Communication Manager managed element ... 35
Synchronizing Communication Manager data ... 36
Adding a Communication Manager server as a SIP entity ... 36
Adding a Branch Session Manager as a SIP entity ... 37
Creating entity links ... 37
Checking the connections ... 38
Administering Communication Manager as an application ... 39
Administering Communication Manager in an application sequence ... 39
Checklist for adding users ... 40
Verifying a new SIP user ... 43
Testing Session Manager and Communication Manager calls ... 44
Checklist for administering routing for the feature server and trunk gateway on System Manager ... 44
Chapter 7: Documentation road map for Survivable Remote Session Manager ... 47
Administering Communication Manager and Session Manager ... 47
Documentation roadmap ... 48
Chapter 8: SIP deskphone administration ... 50
Administering 96xx SIP deskphones ... 50
Chapter 9: Feature name extension administration ... 51
Administering feature name extensions on Communication Manager ... 51
Administering feature name extensions on System Manager ... 51
Appendix A: Numbering configuration ... 53
Numbering ... 53
Numbering administration ... 53
Administration settings for the numbering types ... 54
Private short numbering ... 55
Private long numbering ... 56
Long private numbering and public signaling ... 57
Public numbering ... 59
Call to public extension variation 1 ... 61

Call to public extension variation 2..... 62

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
- Technical support personnel
- Solution architects
- Implementation engineers
- Support personnel
- Technical support representatives
- Authorized BusinessPartners

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 30 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 how to administer network connectivity on	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:

Procedure

- 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

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

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

Related links

Trunk gateway on page 12
Combination feature server and trunk gateway on page 12

Feature server

A feature server provides Communication Manager features to the SIP endpoints registered with Session Manager. The feature server uses the half-call model of IP Multimedia Subsystem (IMS). 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:

- Does not support routing of PSTN calls directly to ISDN trunks for IMS users. You must administer the dial plan to route all PSTN calls to Session Manager over the IMS trunk group.
- Does not support traditional endpoints, such as DCP, H.323, ISDN, and analog.
- Does not support G650 Media Gateway.

Related links

Half-call model on page 11

Half-call model

The half-call model processes a call request in two 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 phase and the termination phase are separate operations that different feature servers perform.

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

Evolution server

An evolution server is similar to the traditional Communication Manager server. The evolution server provides Communication Manager features to both SIP and non-SIP endpoints. The evolution server uses the 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.

If you configure Communication Manager 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.

The evolution server supports a limited form of application sequencing.

Related links

Application sequencing in the evolution server on page 12
Full-call model on page 11

Full-call model

The full-call model processes a call request in a single step and performs the origination and the termination phase without a break. The traditional Communication Manager server follows the full-call model.

Application sequencing works only when all servers support the half-call model. Therefore, do not provision other sequenced applications with the evolution server.

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.

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 but not other endpoints.

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

Related links

Overview on page 10

Combination feature server and trunk gateway

Communication Manager configured as a combination feature server and trunk gateway processes only IMS to IMS and non-IMS to non-IMS traffic. This configuration requires two SIP signaling groups from Communication Manager to Session Manager:

- An IMS signaling group to support the feature server
- A non-IMS signaling group to support the trunk gateway

All calls for the IMS users route to Session Manager. Calls that arrive on IMS trunks route to an IMS trunk. Therefore, two sets of ARS route tables are required:

- One set for calls that come in on IMS trunks.
- The other set for calls that come in on non-IMS SIP trunks and non-SIP trunks.

For example, an incoming public trunk call to an IMS user routes 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.

Related links

Overview on page 10

Chapter 3: Communication Manager configured as a feature server or an evolution server

This section defines the connection and routing between Session Manager and Communication Manager configured as a:

- Feature server
- Evolution server

Prerequisites for administering feature server or evolution server

Procedure

1. Install Communication Manager on System Manager.
2. On System Platform web console, click **Server Management** > **Patch Management**.
3. Install patches for the Communication Manager feature server or evolution server.
4. Run the **`add ip-interface procr`** command to configure the IP address of Processor Ethernet.
5. Run the **`add media-gateway x`** command to add the gateways.

   The system updates the following two IP addresses in the mgc list of gateways:

   - The IP address of Processor Ethernet of the Communication Manager feature server
   - The IP address of Processor Ethernet of the Survivable Remote server
6. Use the System Platform web console to install the following files for Communication Manager:
   a. The license file. Use the MAC address of the Communication Manager feature server or the Communication Manager evolution server.
   b. The authentication file. The Communication Manager feature server and the simplex survivable remote server require separate authentication files.

7. Ensure that System Manager and Session Manager are active in the existing SIP routing deployment.
8. 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.
9. Install and administer the Session Manager server.
10. Install the appropriate service packs if applicable.

Recommendations

- Use the adaptation modules only on the entry and exit points of the Avaya Aura® network. Do not use the modules on the interface to the sequenced applications.
- Use only existing public numbers. The number must 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 call the 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.

No.	Task	Link	✔
1	Administer the dial plan.	Administering the dial plan on page 22	
2	Add the feature access codes for AAR and ARS.	Administering feature access codes on page 23	
3	Add the appropriate SIP domain in the network region.	Administering an IP network region on page 23	
4	Assign a node name to the IP address of the security module of Session Manager.	Adding a node name on page 23	
5	Add a SIP signaling group.	Adding a SIP signaling group on page 24	
6	Add trunk groups for each Session Manager.	Adding a SIP trunk group on page 25	
7	Configure the appropriate route patterns.	Administering a route pattern on page 26	

Table continues…

No.	Task	Link	✔
8	Administer the uniform dial plan for non-SIP calls.	Administering the uniform dial plan on page 27	
9	Administer AAR.	Administering the AAR analysis table on page 27	
10	Administer ARS for non-SIP calls.	Administering the ARS analysis table on page 28	
11	Add the appropriate route pattern as the proxy route.	Administering the proxy route on page 29	
12	Administer the incoming call handling treatment.	Administering the incoming call handling treatment on page 29	
13	If applicable, add a Survivable Remote server.	Adding a Communication Manager Survivable Remote Processor on page 30	
14	Modify the public unknown numbering so that a deskphone displays a number in the E.164 format.	Administering the public or unknown numbering format on page 30	
15	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 31	
16	If applicable, validate the gateway recovery rule.	Validating the gateway recovery rule on page 32	
17	Save translations.	Saving translations on page 32	
18	Add a privileged administrator for System Manager.	Adding a privileged administrator account on page 34	
19	Administer Communication Manager as a managed element.	Creating a Communication Manager managed element on page 35	
20	Synchronize the Communication Manager data.	Synchronizing Communication Manager data on page 36	
21	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 36	
22	If adding Survivable Remote Session Manager, add as a SIP entity.	Adding a Branch Session Manager as a SIP entity on page 37	
23	Create entity links between Session Manager and Communication Manager.	Creating entity links on page 37	
24	Verify the connection between Session Manager and Communication Manager.	Checking the connections on page 38	

Table continues…

No.	Task	Link	✔
25	Administer Communication Manager as an application.	Administering Communication Manager as an application on page 39	
26	Administer Communication Manager in an application sequence.	Administering Communication Manager in an application sequence on page 39	
27	Add users.	Checklist for adding users on page 40	
28	Verify the users.	Verifying a new SIP user on page 43	
29	Test the calls between Session Manager and the Communication Manager feature server or evolution server.	Testing Session Manager and Communication Manager calls on page 44	

Chapter 4: Communication Manager configured as a trunk gateway

This section defines the connection and routing between Session Manager and Communication Manager configured as a trunk gateway.

Trunk gateway administration checklist

No.	Task	Link	✔
!	Assign a node name to the IP address of the security module of Session Manager.	Adding a node name on page 23	
2	Administer an IP network region in the SIP signaling group connected to Session Manager.	Administering an IP network region on page 23	
3	Add a non-IMS SIP signaling group.	Adding a SIP signaling group on page 24	
4	Add a SIP trunk group to the SIP signaling group.	Adding a SIP trunk group on page 25	
5	Administer the dial plan.	Administering the dial plan on page 22	
6	Administer the AAR analysis table.	Administering the AAR analysis table on page 27	
7	Add Communication Manager as a SIP entity.	Adding a Communication Manager server as a SIP entity on page 36	
8	Administer a routing policy with the trunk gateway as the destination.		
9	Administer the dial pattern that uses the routing policy defined earlier.		

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

This section defines the connection and routing between Communication Manager and Session Manager.

You must configure two SIP signaling groups between Communication Manager and Session Manager:

- A non-IMS signaling group to gain access to the trunk gateway.
- An IMS-enabled signaling group for connection to the feature server.

For IMS users, Communication Manager must route all calls to Session Manager. For example, Communication Manager routes an incoming public trunk call to an IMS user to Session Manager on a non-IMS SIP signaling group. The signaling group 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

No.	Task	Link	✔
1	Assign a node name to the IP address of the security module of Session Manager.	Adding a node name on page 23	
2	Administer an IP network region in the SIP signaling group connected to Session Manager.	Administering an IP network region on page 23	
3	Add an IMS-enabled SIP signaling group from the Communication Manager procr server to the Session Manager security module.	Adding a SIP signaling group on page 24	

Table continues…

No.	Task	Link	✔
4	Add a SIP trunk group to the SIP signaling group.	Adding a SIP trunk group on page 25	
5	Administer the dial plan to route the external numbers through AAR to the non-IMS signaling group and trunk to Session Manager.		
6	Administer Communication Manager on System Manager.	Adding a Communication Manager server as a SIP entity on page 36	
7	Add a non-IMS SIP signaling group and allow Incoming Dialog Loopbacks.	Adding a SIP signaling group on page 24	
8	Set up routing from the trunk gateway to the feature server.	Checklist for setting up routing from the trunk gateway to the feature server on page 32	
9	Set up routing from the feature server to the trunk gateway.	Checklist for setting up routing from the feature server to the trunk gateway on page 33	
10	Administer public numbering.	Public numbering on page 20	
11	Set up routing on System Manager.	Checklist for administering routing for the feature server and trunk gateway on System Manager on page 44	

Public numbering

Calls to the public network:

The call from the endpoint routes to the Communication Manager feature server, Session Manager, Communication Manager trunk gateway, and then to the public network.

Even though the feature server is administered for Private Enterprise Canonical numbers, you can change the P-Asserted-Identity (PAI) header to a public long number. To change the PAI header, select a public call type in the respective Route Pattern. For example, pubu in the **Call Type** field on the ARS DIGIT ANALYSIS TABLE screen.

To adapt the PAI header, use Incoming Call Handling Treatment (ICHT) on the Communication Manager trunk gateway or the number adaptation module in Session Manager. Ensure that you do not have overlaps with the entries for the called number.

Calls from the public network:

The call from the public network routes to the Communication Manager trunk gateway, Session Manager, Communication Manager feature server, Session Manager, and then to the endpoint.

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

Chapter 6: Administration procedures

Administration procedures on Communication Manager

Administering the dial plan

Procedure

1. On the Communication Manager SAT interface, 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 for trunks.
3. In the **Total length** field, type the length of the digit string.
4. In the **Call Type** field, type the appropriate call type.

   For administering Communication Manager as a trunk gateway, type `aar`.
5. Save the changes.

   The following table specifies the values that you can enter in the fields.

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	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

Administering feature access codes

Procedure

1. On the Communication Manager SAT interface, 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 the AAR access code.

   For example, `#83`.

3. In the **Auto Route Selection (ARS) - Access Code 1** field, type the ARS access code.

   For example, `9`.

4. Save the changes.

Administering an IP network region

About this task

Use this procedure to assign 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. On the Communication Manager SAT interface, 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. On the Communication Manager SAT interface, 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

Procedure

1. On the Communication Manager SAT interface, 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 one of the following:
   - Type `y` to configure Communication Manager as a feature server.
   - Type `n` to configure Communication Manager as an evolution server.
5. In the **Transport Method** field, type one of the following:
   - Type `tls` if the calls are secure calls.
   - Type `tcp` if the calls are not secure calls.
6. In the **Peer Detection Enabled** field, type `y`.

   Note:

   This setting results in Communication Manager and the connected SIP server exchanging messages. The value for **Peer Server** changes to `SM` when the SIP signaling group is activated.
7. For the trunks connected to Session Manager, perform the following steps:
   a. Set the value of the **Peer Detection** field to `n`.
   b. Set the value of the **Peer Server** field to `SM`.
8. In the **Near-end Node Name** field, type `procr` or `CLAN`.
9. In the **Far-end Node Name** field, type the name of the Session Manager security module.

10. In the **Far-end Network Region** field, type the IP network region number used in the *Administering an IP network region* procedure.
11. 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`.
12. In the **Far-end Listen Port** field, type the port number that you typed in the **Far-end Listen Port** field on the IP NETWORK REGION screen.
13. In the **Far-end Domain** field, type the domain name associated with Session Manager.
14. To enable incoming dialog loopbacks, in the **Incoming Dialog Loopbacks** field, type `allow`.
15. 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. If you disable this test, maintenance software removes the trunks out of service.
16. In the **Initial IP-IP Direct Media** field, type `y` or `n`, depending on the requirement of the **Direct Media** feature.
17. To configure Communication Manager as an evolution server, in the **H.323 Station Outgoing Direct Media** field, type `y`.
18. 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. On the Communication Manager SAT interface, type `add trunk-group next`, and press `Enter`.

   The system displays the TRUNK GROUP screen.
2. Note the value of the **Group Number** field.
3. In the **Group Type** field, type `sip`.
4. In the **Group Name** field, type a name for the trunk group.

5. In the **TAC** field, type a dial access code (DAC).

   For example, `*110`.

6. In the **Direction** field, type `two-way`.
7. In the **Service Type** field, type `tie`.
8. In the **Signaling Group** field, type the SIP signaling group number that you added using the *Adding a SIP signaling group* procedure.
9. In the **Number of Members** field, type the number of trunk group members.

   The maximum number of members that you can add is 255.

10. In the **Numbering Format** field, type one of the following:
    - Type `unk-pvt` for a private network.
    - Type `public` for a trunk that receives ARS calls.
    - Type `private` for a trunk that receives SIP calls.
11. Save the changes.

Administering a route pattern

Procedure

1. On the Communication Manager SAT interface, type `change route-pattern x`, where *x* is the route pattern number, and press `Enter`.
2. In the **Pattern Name** field, type a name for the route pattern.
3. In the **Grp No** field, type the trunk group number used in the *Adding a SIP trunk group* procedure.

   For administering Communication Manager as a feature server and trunk gateway, type the group number of the non-IMS trunk group.

4. In the **FRL** field, type `0`.
5. In the **No. Del Dgts** field, type the number of digits that Communication Manager must delete in the non-IMS trunk.
6. To allow Communication Manager to prepend a plus (+) sign to the number, in the **Inserted Digits** field, type `p`.
7. Save the changes.

Administering the uniform dial plan

About this task

Use the following procedure to modify digits in the number so that Communication Manager can route non-enterprise calls through the AAR table.

Procedure

1. On the Communication Manager SAT interface, 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.

   The following table specifies the values that you can enter in the fields.

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 the AAR analysis table

About this task

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

Procedure

1. On the Communication Manager SAT interface, type `change aar analysis x`, where *x* is a digit string, and press `Enter`.

   The system displays the AAR DIGIT ANALYSIS TABLE screen.

2. 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.
3. In the **Min** field, type the minimum number of allowed digits.
4. In the **Max** field, type the maximum number of allowed digits.
5. In the **Route Pattern** field, type a route pattern number to the trunk group for the dialed string digits.

For administering Communication Manager as a feature server and trunk gateway, type a route pattern to the IMS-trunk group.

6. In the **Call Type** field, type `pubu`.
7. In the **ANI Req** field, type `n`.

   The following table specifies the values that you can enter in the fields.

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

   In the table, two entries are used:

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

Administering the ARS analysis table

Procedure

1. On the Communication Manager SAT interface, type `change ars analysis x`, where *x* is a digit string, and press `Enter`.

   The system displays the ARS DIGIT ANALYSIS TABLE screen.
2. In the **Dialed String** field, type the digits.
3. In the **Min** field, type the minimum number of allowed digits.
4. In the **Max** field, type the maximum number of allowed digits.
5. In the **Route Pattern** field, type the route pattern number.
6. In the **Call Type** field, type the appropriate call type.

   For administering Communication Manager as a feature server and trunk gateway, type `pubu`.
7. Save the changes.

   The following table specifies the values that you can enter in the fields.

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

Administering the proxy route

Procedure

1. On the Communication Manager SAT interface, type `change locations`, and press `Enter`.

   The system displays the LOCATIONS screen.

2. In the **Name** field, type a 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 the incoming call handling treatment

About this task

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

Procedure

1. On the Communication Manager SAT interface, 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 Communication Manager Survivable Remote Processor

Procedure

1. On the Communication Manager SAT interface, 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`.
3. Ensure that the value of the **Cluster ID/MID** field on the SURVIVABLE PROCESSOR screen matches with the value of the field on the Web page.
4. Record the value of Cluster ID/MID field. You will need this value during the *Configure the Communication Manager* step in the *Survivable remote installation checklist*.
5. Save the changes.

Administering the public or unknown numbering format

About this task

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

Procedure

1. On the Communication Manager SAT interface, 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 in the extension.
3. In the **Ext Code** field, type one or more starting digits in 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 international E.164 number	Yes	Yes	Communication Manager automatically inserts the plus (+) sign
SIP	other	Full international 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 that Communication Manager must transmit.

Note:

Communication Manager combines the value of the **CPN Prefix** field with the extension that matches the entry on the NUMBERING - PUBLIC/UNKNOWN FORMAT screen. If the length of the number is longer than the length defined in the **Total CPN Len** field, Communication Manager 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. On the Communication Manager SAT interface, 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.

Next steps

Refer to the *Communication Manager Survivable Remote Processor administration checklist*.

Validating the gateway recovery rule

Procedure

1. On the Communication Manager SAT interface, 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 of the gateway.
   - `none` to disable the recovery rule. The system does not accept any automatic fallback registrations.

   You can apply a single rule to all gateways, or each gateway can have a separate 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.

Saving translations

Procedure

On the Communication Manager SAT interface, type `save translations`, and press `Enter`.

Checklist for setting up routing from the trunk gateway to the feature server

Use the following checklist to set up the routing for an incoming trunk call to an IMS user. Communication Manager prepends 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.

No.	Task	Link	✔
1	Administer the ARS digit conversion table.	Administering the ARS digit conversion table on page 33	
2	Administer the AAR analysis table.	Administering the AAR analysis table on page 27	
3	Administer the route pattern number that you entered in the **Route Pattern** field on the ARS DIGIT ANALYSIS TABLE screen.	Administering a route pattern on page 26	

Administering the ARS digit conversion table

Procedure

1. On the Communication Manager SAT interface, type `change ars digit-conversion x`, where *x* is a digit string, and press `Enter`.

   The system displays the ARS DIGIT CONVERSION TABLE screen.
2. In the **Matching Pattern** field, add an entry for the incoming trunk call number.
3. In the **Min** field, type the minimum number of digits that are allowed.
4. In the **Max** field, type the maximum number of digits that are allowed.
5. In the **Del** field, type the number of digits that Communication Manager must delete from the trunk call number.
6. In the **Replacement String** field, type the digits that Communication Manager prepends to the trunk call number.

   For example, `99`.
7. In the **Net** field, type `aar`.
8. In the **Conv** field, type `n`.
9. In the **ANI Req** field, type `n`.
10. Save the changes.

Checklist for setting up routing from the feature server to the trunk gateway

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.

No.	Task	Link	✔
1	Administer the AAR analysis table.	Administering the AAR analysis table on page 27	
2	Administer route pattern 1.	Administering a route pattern on page 26	
3	Administer route pattern 2.	Administering a route pattern on page 26	
4	Administer route pattern 3. You must administer this route pattern only for countries where customers can dial subscriber numbers, for example, Germany. A subscriber number is a public number without the country code and the national destination code or city code.	Administering a route pattern on page 26	
5	On the trunk gateway, administer Incoming Call Handling Treatment (ICHT) for each non-IMS trunk to insert digits for routing to the public trunk. Public numbers can be of different lengths and you must administer the numbers accordingly.	Administering the incoming call handling treatment on page 29	

Adding a privileged administrator account

About this task

Use the following procedure to add a privileged administrator account that is a member of the **suser** group. You must use this account with System Manager.

Procedure

1. Log on to the Communication Manager server System Management Interface (SMI) Web page.
2. Click **Administration** > **Server (Maintenance)**.

3. In the navigation pane, 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 a login name.
8. In the **Password** field, type a 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**.

Administration procedures on System Manager

Creating a Communication Manager managed element

Procedure

1. Log on to System Manager Web Console.
2. Click **Services** > **Inventory**.
3. In the navigation pane, click **Inventory** > **Manage Elements**.
4. Click **New**.
5. In the **Type** field, select **Communication Manager**.
6. In the **Name** field, type a 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 by using the *Adding a privileged administrator* procedure. System Manager and Communication Manager do not synchronize unless the Communication Manager login administration is complete.

11. Select the **SSH Connection** field.
12. In the **Port** field, type `5022`.
13. Click **Commit**.

Synchronizing Communication Manager data

About this task

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

Procedure

1. Log on to System Manager Web Console.
2. Click **Services** > **Inventory**.
3. In the navigation pane, click **Inventory** > **Synchronization** > **Communication System**.
4. Select the 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 to complete.
7. For the current synchronization status, click **Refresh**.

   When the synchronization is complete, the **Sync Status** field shows **Completed**.

Adding a Communication Manager server as a SIP entity

About this task

Use the following procedure to add the Communication Manager feature server or evolution server as a SIP entity. Do not use adaptation on the Communication Manager server, so that the system maintains proper application sequencing and routing for the SIP headers that the Communication Manager server creates.

Procedure

1. Log on to System Manager Web Console.

2. Click **Elements** > **Routing** .
3. In the navigation pane, click **Routing** > **SIP Entities**.
4. Click **New**.
5. In the **Name** field, type a name for the Communication Manager server.
6. In the **FQDN or IP Address** field, type the IP address of the Communication Manager server.

   For administering Communication Manager as a feature sever and trunk gateway, type the IP address for Processor Ethernet of Communication Manager. The IP address is the near end in the signaling group to Session Manager.
7. In the **Type** field, select **CM**.
8. In the **Notes** field, type a 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 time zone.
11. Click **Commit**.

Adding a Branch Session Manager as a SIP entity

Procedure

1. Log on to System Manager Web Console.
2. Click **Elements** > **Routing**.
3. In the navigation pane, 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 Branch 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:

- Each Session Manager server and the Communication Manager feature server or evolution server.
- The Branch Session Manager server and the Communication Manager feature server or evolution server.

If you use separate entities and entity links, such as for a 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 System Manager Web Console.
2. Click **Elements** > **Routing**.
3. In the navigation pane, click **Routing** > **Entity Links**.
4. Click **New**.
5. In the **Name** field, type a name for the entity link.
6. In the **SIP Entity 1** field, select the Branch Session Manager server.

   For administering Communication Manager as a feature server and trunk gateway, select the Session Manager entity.
7. In the **Protocol** field, select **tls**.
8. In the **Port** field, type the port number.
9. In the **SIP Entity 2** field, select the Communication Manager server.
10. In the **Port** field, type the port number.
11. In the **Connection policy** list box, select **Trusted**.
12. **(Optional)** In the **Notes** field, type a description for the entity link.
13. Click **Commit**.

Checking the connections

Procedure

1. On the Communication Manager SAT interface, type `list history`, and press `Enter`.

   The system displays the HISTORY screen.
2. Verify that you are logged in to Session Manager.
3. Verify that the initial data synchronization has begun.
4. On System Manager Web Console, click **Elements** > **Session Manager**.
5. Verify that the Session Manager server is active.
6. In the navigation pane, click **Session Manager** > **System Status** > **SIP Entity Monitoring**.
7. From the **All Monitored SIP Entities** list, select the Communication Manager server.
8. Verify that the value of the **Link Status** field is **Up**.

Administering Communication Manager as an application

Procedure

1. Log on to System Manager Web Console.
2. Click **Elements** > **Session Manager**.
3. In the navigation pane, click **Session Manager** > **Application Configuration** > **Applications**.
4. Click **New**.
5. In the **Name** field, type a name for the application.
6. In the **SIP Entity** field, select the Communication Manager server.
7. **(Optional)** In the **Description** field, type a 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. As an evolution server operates in the full-call model, you cannot change the position of the applications with regard to Communication Manager.

Procedure

1. Log on to System Manager Web Console.
2. Click **Elements** > **Session Manager**.
3. In the navigation pane, click **Session Manager** > **Application Configuration** > **Application Sequences**.
4. Click **New**.
5. In the **Name** field, type a name for the application sequence.
6. In the **Description** field, type a description for the application sequence.
7. In the **Available Applications** section, click the plus (+) icon beside the Communication Manager server.

The system selects the **Mandatory** field.

8. Click **Commit**.

Checklist for adding users

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

- A trunk associated with the primary Session Manager server.
- A trunk associated with the secondary Session Manager server.

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

No.	Task	Link	✔
1	Log on to System Manager Web Console.		
2	Administer the **Identity** section.	Administering the Identity section of a user on page 40	
3	Administer the **Communication Profile** section.	Administering the Communication Profile section of a user on page 41	
4	Verify that the data synchronization is complete.	Checking the synchronization status on page 42	
5	Assign the user to a Communication Manager station.	Assigning the user to a Communication Manager station on page 43	

Administering the Identity section of a user

Procedure

1. On System Manager Web Console, click **Users** > **User Management**.
2. In the navigation pane, click **User Management** > **Manage Users**.
3. Click **New**.

   The system displays the New User Profile page.
4. Click the **Identity** tab.
5. In the **Last Name** field, type the last name of the user.
6. In the **First Name** field, type the first name of the user.
7. In the **Middle Name** field, type the middle name of the user.
8. **(Optional)** In the **Description** field, type a description for the user.
9. In the **Login Name** field, type the login name using the SIP domain in Session Manager.

The login name must be in the following format: `name@domain.com`.

10. In the **Authentication Type** field, type `Basic`.
11. In the **Password** field, type a password that starts with a lower case or an upper case alphabet.
12. In the **Confirm Password** text box, type the password that you entered in the **Password** field.
13. In the **Localized Display Name** field, type a name that the system must display to the calling party.
14. In the **Endpoint Display Name** field, type the full text name of the user.
15. In the **Language Preference** field, select a language.
16. In the **Time Zone** field, select a time zone.

Next steps

Administer the **Communication Profile** section. See *Administering the Communication Profile section of a user*.

Administering the Communication Profile section of a user

Before you begin

Administer the **Identity** section. See *Administering the Identity section of a user*.

About this task

A user can have more than one communication profile.

Procedure

1. On the New User Profile page of System Manager Web Console, click the **Communication Profile** tab.
2. In the **Communication Profile Password** field, type a communication profile password that contains only numbers.

   Note:

   You must use this password in the Endpoint Profile security code and to log in to a deskphone.
3. In the **Confirm Communication Profile Password** text box, type the same password that you typed in the **Communication Profile Password** field.
4. Click **New**.
5. In the **Type** field, select **Avaya SIP**.
6. In the **Fully Qualified Address** field, type the extension number of the SIP deskphone.
7. Select the correct domain from the drop-down list that follows the **@** sign.
8. Click **Add**.

9. Select the added entry.
10. Click **New**.
11. In the **Type** field, select **Avaya E.164**.
12. If you are using private numbering, administer **Fully Qualified Address**, which is a private handle.

    The private handle depends on the numbering format.
13. Select the appropriate domain from the drop-down list that follows the **@** sign.
14. Click **Add**.
15. Click the **Session Manager Profile** arrow.
16. Select **Session Manager Profile**.
17. If applicable, in the **Secondary Session Manager** field, select the 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.
18. **(Optional)** In the **Origination Application Sequence** field, select the appropriate application sequence name that the system must use when calls are routed from the user.
19. **(Optional)** In the **Termination Application Sequence** field, select the appropriate application sequence name that the system must use when calls are routed to the user.
20. **(Optional)** In the **Survivability Server** field, select the entity that the system must use for survivability.

    For a Survivable Remote Session Manager, select the Survivable Remote Session Manager SIP entity.
21. In the **Home Location** field, select the Communication Manager server SIP entity that the system must use as the home location for call routing.

Next steps

Check the synchronization status. See *Checking the synchronization status*.

Checking the synchronization status

Before you begin

Administer the **Communication Profile** section. See *Administering the **Communication Profile** section of a user*.

Procedure

1. On System Manager Web Console, click **Services** > **Inventory**.
2. In the navigation pane, click **Inventory** > **Synchronization** > **Communication System**.
3. The system displays the synchronization status in the **Sync Status** column of the table.

Next steps

Assign the user to a Communication Manager station. See *Assigning the user to a Communication Manager station*.

Assigning the user to a Communication Manager station

Before you begin

Check the synchronization status. See *Checking the synchronization status*.

Procedure

1. On the New User Profile page of System Manager Web Console, click the **Communication Profile** tab.
2. Click the **CM Endpoint Profile** arrow.
3. Select **Endpoint Profile**.
4. In the **System** field, select the Communication Manager server.
5. In the **Profile Type** field, select the profile type.
6. Do not select the **Use Existing Endpoints** field.
7. In the **Extension** field, type the extension that is administered on the Communication Manager server for the existing or new station.
8. 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`
9. In the **Set Type** field, type the deskphone set type.
10. You can leave the **Security Code** field blank.

    The value in the **Security Code** is not used to log in to the deskphone.
11. In the **Port** field, select **IP**.
12. In the **Voice Mail Number** field, type the voice mail number.
13. Select the **Delete Endpoint on Unassign of Endpoint from User** field.
14. Select the **Override Endpoint Name** field.

Verifying a new SIP user

Procedure

1. Log in to the SIP deskphone with the values in the **Extension** and **Password** fields of Endpoint Profile.
2. Log on to System Manager Web Console.
3. Click **Elements** > **Session Manager**.

4. In the navigation pane, click **Session Manager** > **System Status** > **User Registrations**.
5. In the **User Registrations** table, in the row that displays the details of the user, click **Show**.
6. Click the **Registration Detail** tab, and verify that the information is correct.
7. On Communication Manager SAT interface, type `display station n`, where *n* is the deskphone extension of the user, and press `Enter`.

   The system displays the STATION screen.
8. Verify that the value of the **Type** field is SIP.
9. Verify that the value of the **SIP Trunk** is **aar**.
10. Press `CANCEL` to return to the command prompt.
11. Type `display off-pbx-telephone station-mapping n`, where *n* is the deskphone extension of the user, and press `Enter`.

    The system displays the STATIONS WITH OFF-PBX TELEPHONE INTEGRATION screen.
12. For the deskphone 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 deskphone to another.
2. Place 20-digit calls from one SIP deskphone to another.
3. To validate routing, place five-digit calls to a non-SIP deskphone on another Private Branch Exchange (PBX) on the Session Manager server.
4. To validate routing, place 20-digit calls to a non-SIP deskphone on another PBX on the Session Manager server.

Checklist for administering routing for the feature server and trunk gateway on System Manager

Although the feature server functionality and the trunk gateway functionality are within the same Communication Manager server, you must configure both as separate SIP entities by using the System Manager routing .

No.	Task	Link	✔
1	Define the entity and the entity link for the feature server and the trunk gateway as a TCP connection with		

Table continues…

No.	Task	Link	✔
	the ports defined in the Communication Manager signaling groups. For example, TCP port 5060 for the feature server and TCP port 5070 for the trunk gateway.		
2	For routing calls from the feature server to the trunk gateway, define a dial pattern and a routing policy to route an incoming plus (+) sign to the trunk gateway. For more information, see the Routing Policy Details screen of System Manager.		
3	Add the SIP domains of the Communication Manager server.	Adding a Communication Manager SIP domain on page 45	
4	Administer Communication Manager as a SIP entity.	Adding a Communication Manager server as a SIP entity on page 36	
5	Create an entity link from the Session Manager entity to the Communication Manager entity.	Creating entity links on page 37	
6	Administer Communication Manager as an application.	Adding a Communication Manager application on page 46	

Adding a Communication Manager SIP domain

Procedure

1. Log on to System Manager Web Console.
2. Click **Elements** > **Routing**.
3. In the navigation pane, click **Routing** > **Domains**.
4. Click **New**.
5. In the **Name** field, type the domain name for Communication Manager.
6. In the **Type** field, select **CM**.
7. Click **Commit**.
8. Click **New**.
9. In the **Name** field, type the domain name for Session Manager.
10. In the **Type** field, select **sip**.

11. Click **Commit**.

Adding a Communication Manager application

Procedure

1. Log on to System Manager Web Console.
2. Click **Elements** > **Inventory**.
3. In the navigation pane, click **Inventory** > **Manage Elements**.
4. Click **New**.
5. In the **Type** field, select **CM**.
6. 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**.
7. In the **Node** field, type the management IP address to gain access to the Communication Manager SAT interface.
8. In the **Attributes** section, in the **Login** field, type the SSH SAT login name.
9. In the **Attributes** section, in the **Password** field, type the SSH SAT password.
10. Select the **Is SSH Connection** field.
11. In the **Port** field, type `5022`.
12. Click **Commit**.

    The system schedules the Communication Manager entity for data synchronization on an hourly basis initially and by an increment of one hour later.

Chapter 7: Documentation road map for Survivable Remote Session Manager

The documentation road map provides information about the books to refer to install, configure, administer, and test a Survivable Remote Session Manager server and the book to refer for each task. You need to use more than one book to install and administer the Survivable Remote Session Manager server.

You must administer Communication Manager and Session Manager before you install and administer the Survivable Remote Session Manager server.

Related links

Administering Communication Manager and Session Manager on page 47
Documentation roadmap on page 48

Administering Communication Manager and Session Manager

Procedure

1. Install Communication Manager.
2. Install the license file for Communication Manager.
3. Configure Communication Manager as a feature server or an evolution server.
4. Ensure that the server is operational.
5. Administer Communication Manager as a SIP entity on Session Manager.

Related links

Documentation road map for Survivable Remote Session Manager on page 47

Documentation roadmap

Task	Books 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 System Manager Web Console.	*Implementing Avaya Aura® Communication Manager*, 03-603558	
Administer the Survivable Remote Session Manager server on Communication Manager.	*Deploying 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 S8800 Server, install S8800 Server.	*Upgrading to Avaya Aura® Communication Manager Release 6.3*	
If installing the simplex Survivable Remote template on S8510 Server, install or upgrade S8510 Server.	*Upgrading to Avaya Aura® Communication Manager Release 6.3*	If S8510 Server does not have 8GB of memory, upgrade the server. S8510 Server requires the Communication Manager migration kit.
If installing the embedded Survivable Remote template, install S8300E or 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	
Install System Platform on the server.	*Implementing Avaya Aura® Communication Manager*, 03-603558	
Install the license file and the authentication file.	*Implementing Avaya Aura® Communication Manager*, 03-603558	
Install the Communication Manager template by using System Manager Web Console.	*Implementing Avaya Aura® Communication Manager*, 03-603558	

Table continues…

Task	Books to use	Notes
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 by using System Manager Web Console.	*Deploying Avaya Aura® Session Manager*, 03-603473	See the *Survivable Remote Session Manager administration checklist* section.
Verify the registration.	*Deploying Avaya Aura® Session Manager*, 03-603473	
Test the installation.	*Deploying Avaya Aura® Session Manager*, 03-603473	

Related links

Documentation road map for Survivable Remote Session Manager on page 47

Chapter 8: SIP deskphone administration

Administering 96xx SIP deskphones

About this task

A deskphone can use settings from a file server if you set up the environment for the deskphone.

Procedure

1. To go to the **Configuration** menu, perform one of the following steps:
   - On the physical deskphone, press the **Mute** button, and type `CRAFT#` by using the keypad.
   - On the soft telephone, type `admin options`, and press `Enter`.
2. In the **SIP Global Settings** section, perform the following steps:
   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 **simultaneous**.
   d. Leave the **Avaya Config Server:** field blank.
3. In the **SIP Proxy Settings** section, perform the following steps:
   a. In the **SIP Proxy Server** field, type the IP address of the primary Session Manager server.
   b. If applicable, type the IP address of the secondary Session Manager server.
   c. In the **Transport** field, select **TCP** or **TLS**.
   d. In the **SIP Port** field, type the port number defined in the Session Manager SIP entity.

      For example, type `5060` for TCP.
4. In the **SSON** field, type the appropriate SSON number for the deskphone to gain access to the file server.

Note:

For more information on administering 96xx SIP deskphones, see *Administering Avaya 9601/9608/ 9608G/9611G/9621G/9641G IP Deskphones SIP* .

Chapter 9: Feature name extension administration

This section describes how to administer feature name extensions. You must administer feature name extensions first on Communication Manager by using the Communication Manager SAT interface and then on Session Manager by using System Manager Web Console.

Administering feature name extensions on Communication Manager

Procedure

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

   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`, and press `Enter`.

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

Administering feature name extensions on System Manager

Procedure

1. Log on to System Manager Web Console.

2. Click **Elements** > **Session Manager**.
3. In the navigation pane, click **Session Manager** > **Application Configuration** > **Implicit Users**.
4. Click **New**.
5. In the **Pattern** field, type the deskphone 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 description.

   For example, `Turn on EC500`.
9. In the **SIP Domain** field, select the SIP domain.
10. In the **Origination Application Sequence** field, select the originating feature server name.
11. In the **Termination Application Sequence** field, select the terminating feature server name.
12. Click **Commit**.

Appendix A: Numbering configuration

Numbering

The following are the types of numbering:

- **Enterprise Canonical Number (ECN)**: ECN is unique to Session Manager and can be a public long number, a private long number, or a short or internal number.
- **Public number**: A public number must begin with a plus (+) sign.
- **Private alias**: A private alias is required for public numbering when telephones, such as Avaya deskphones, are unable to register with a plus (+) sign.
- **Off-PBX Telephony Integration and Mobility (OPTIM) table**: This table converts a registration number to a short number. The registration number can be an ECN.
- **Public numbering table**: This table converts a short number to a public long number. Communication Manager adds the short number as an avext parameter to the PAI header and the Contact header for messages to the deskphone.
- **Private numbering table**: This table converts a short number to a private long number. Communication Manager adds the short number as an avext parameter to the PAI header and the Contact header for messages to the deskphone.
- **Incoming Call Handling Treatment (ICHT)**; ICHT converts a public or a private long number to a short number.

Numbering administration

You can administer numbering in Communication Manager by using different tables to adapt the calling number and the called number. The numbering type settings, such as AAR, route pattern, and trunk, have an assigned priority. Ensure that you administer the users and handles in Session Manager by matching the numbering form in Communication Manager.

Communication Manager Release 6.0 and later uses the trunk numbering setting to adapt the calling party number. The entries in AAR, Route Pattern, and ARS adapt the called party number. Communication Manager uses the following fields for the numbering adaptation:

- **Numbering Format** field on the TRUNK GROUP screen:
  - public: The calling number adapts to the entry in the **public-unknown-numbering** table.
  - unk-pvt: The calling number adapts to the entry in the **private-numbering** table.

Although the trunk is set to private, the calling number adapts to a public number when the settings of the AAR and route pattern determine the called number as public. For this adaptation, you must administer a matching entry 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 as a public number. The calling number adapts to a public number.
  - pubu: The called number is determined as a public number. The calling number adapts to a public number.
  - unku: The called number is determined as a private number.

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

  The value of the **Numbering Format** field has a higher priority than the value of the **Call type** field. When the calling party number adapts to a public number, you must administer a matching entry in the **public-unknown-numbering** table.

Administration settings for the numbering types

The numbering type used for registration must be different from the numbering type signaled to the network.

The settings on the routing and the numbering forms depend on the numbering type.

Registration numbering type	Signaled numbering type	Administration
private short	private short	Private short numbering on page 55.
private long	private long	Private long numbering on page 56.
private long	public	Long private numbering and public signaling on page 57.
public plus (+) sign	public	Public numbering on page 59.
private short or long (variation 1)	call to public number	Call to public extension variation 1 on page 61.
private short or long (variation 2)	call to public number	Call to public extension variation 2 on page 62.

Private short numbering

Private short numbering uses the private extension. In Session Manager, you need to administer only the private short number. In Communication Manager, the administration does not change the internal extension.

The configuration for private short numbering is for the following numbering types:

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

The following table describes the administration settings for private short numbering.

SAT screen	Page number	Field	Value	Notes
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION	1	**Phone Number**	Extension number	
	1	**Trunk Selection**	aar	For 90xx SIP station types, the **Trunk Selection** field is provided on the last page of the STATION screen.
TRUNK GROUP	3	**Numbering Format**	private	
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Extension number	
NUMBERING - PRIVATE FORMAT	1	**Ext Code**	Extension number or pattern for extension numbers	
	1	**Trk Grp (s)**	blank	Blank means the setting 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	Lists trunk groups with trunks to primary Session Manager listed first.
	1	**FRL**	0	
	1	**Numbering format**	blank	

Table continues…

SAT screen	Page number	Field	Value	Notes
INCOMING CALL HANDLING TREATMENT				No entries.

Private long numbering

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

The configuration for private long numbering is for the following numbering types:

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

The following table describes the administration settings for private long numbering.

SAT screen	Page number	Field	Value	Notes
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION	1	**Phone Number**	Long private extension number	
	1	**Trunk Selection**	aar	For 90xx SIP station types, set the value of the **Trunk Selection** field on the STATION screen.
TRUNK GROUP	3	**Numbering Format**	private	
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Long private extension number	The value of the **Dialed String** field is an 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.	

Table continues…

SAT screen	Page number	Field	Value	Notes
	1	**Trk Grp (s)**	blank	Blank means the setting applies to all trunks.
	1	**Private Prefix**	Private prefix	
	1	**Total Len**	Extension length and prefix	
NUMBERING - PUBLIC/UNKNOWN FORMAT				No entries.
ROUTE PATTERN	1	**Grp Num**	Trunk group number	Lists trunk groups with the 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 uses the private extension with a prefix. In Session Manager, you must administer the private long number and the public number are administered. In Communication Manager, the administration changes the private long number to the extension and changes the outgoing direction to the public number.

The configuration for long private numbering and public signaling is for the following numbering types:

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

The following table describes the administration settings for the long private numbering.

SAT screen	Page number	Field	Value	Notes
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION	1	**Phone Number**	Long private extension number	
	1	**Trunk Selection**	aar	For 90xxSIP station types, set the value of the **Trunk Selection** field is on the STATION screen.
TRUNK GROUP	3	**Numbering Format**	public	
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Long private extension number	The value of the **Dialed String** field is an 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 the setting applies to all trunks.
	1	**CPN Prefix**	Public prefix to the extension without the plus (+) sign. The system adds the plus (+) sign.	
	1	**Total Len**	Extension length and CPN prefix	
ROUTE PATTERN	1	**Grp Num**	Trunk group	Lists trunk groups with the trunks to primary Session Manager listed first.
	1	**FRL**	0	
	1	**Numbering format**	unk-unk	

Table continues…

SAT screen	Page number	Field	Value	Notes
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

The public numbering format requires a plus (+) sign as a login character. Therefore, only soft telephones can use the public numbering format. For all other telephones, this numbering is realized with a private alias by using the private long and the public signalling configuration.

In Session Manager, you can only the public number is administered.

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

The configuration for the public numbering format is for the following numbering types:

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

The following table describes the administration settings for public numbering.

SAT screen	Page number	Field	Value	Notes
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION	1	**Phone Number**	Public number without a leading plus (+) sign	
	1	**Trunk Selection**	aar	For 90xx SIP station types, set the value of the **Trunk Selection** field on the STATION screen.

Table continues…

SAT screen	Page number	Field	Value	Notes
TRUNK GROUP	3	**Numbering Format**	public	
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Public number without a leading plus (+) sign	The value of the **Dialed String** field is an 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 pattern for extension numbers	
	1	**Trk Grp (s)**	Trunk number or blank.	Blank means the setting applies to all trunks.
	1	**CPN Prefix**	Public prefix to the extension without the plus (+) sign. The system adds the plus (+) sign.	
	1	**Total Len**	Extension length and CPN prefix	
ROUTE PATTERN	1	**Grp Num**	Trunk group number	Lists trunk groups with the 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 adapts to a public number when the called number is identified as a public number. For example, a call to a public network.

In Communication Manager, you must perform the additional administration for the private numbering. You must administer the public number as a secondary Session Manager server.

The configuration is for the following numbering types:

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

The following table describes the administration settings for Call to public extension variation 1.

SAT screen	Page number	Field	Value	Notes
TRUNK GROUP	3	**Numbering Format**	private	
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Private long or short number	The value of the **Dialed String** field is an 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 the setting 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 the setting applies to all trunks.

Table continues…

SAT screen	Page number	Field	Value	Notes
	1	**CPN Prefix**	Public prefix to the extension without the plus (+) sign. The system adds the plus (+) sign.	
	1	**Total Len**	Extension length and CPN prefix	
ROUTE PATTERN	1	**Grp Num**	Trunk group number	Lists trunk groups with the 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 adapts to a public number when the called number is identified as a public number. For example, a call to a public network.

In Communication Manager, you must perform the additional administration for the private numbering.

The administration for this numbering 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

The following table describes the administration settings for Call to public extension variation 2.

SAT screen	Page number	Field	Value	Notes
TRUNK GROUP	3	**Numbering Format**	private	

Table continues…

SAT screen	Page number	Field	Value	Notes
AAR DIGIT ANALYSIS TABLE	1	**Dialed String**	Private long or short number	The value of the **Dialed String** field is an 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 the setting applies to all trunks.
	1	**Private Prefix**	blank	
	1	**Total Len**	Extension length	
NUMBERING - PUBLIC/UNKNOWN FORMAT				No entries. The adaptation to public numbering is performed in Session Manager.
ROUTE PATTERN	1	**Grp Num**	Trunk group number	Lists trunk groups with the trunks to primary Session Manager listed first.
	1	**FRL**	0	
	1	**Numbering format**	unk-unk	
INCOMING CALL HANDLING TREATMENT				No entries.

Index

Numerics

96xx SIP deskphone administration 50

A

AAR analysis table 27
adding users 40
    assigning user to station 43
    checklist 40
    Communication Profile 41
    Identity 40
    synchronization status 42
administering evolution server prerequisites 14
administering feature server or evolution server prerequisites 14
administering feature server prerequisites 14
administering routing for feature server and trunk gateway on System Manager
    checklist 44
application sequencing 12
    administration 39
ARS analysis table 28
ARS digit conversion 33
assigning user to station 43

C

call to public extension - variation 1 61
call to public extension - variation 2 62
checking connections 38
combination feature server and trunk gateway 12
Communication Manager evolution server 11
Communication Manager feature server 10
Communication Manager feature server and trunk gateway 19
Communication Manager in application sequence 39
Communication Manager managed element administration 35
Communication Manager server application administration 39
Communication Manager SIP entity 36
Communication Manager trunk gateway 12, 18
Communication Profile 41
configuring evolution server 14
configuring feature server 14
creating entity links 37

D

dialplan analysis 22
documentation roadmap 47
    Survivable Remote Session Manager 47
document changes 7
document purpose 7

E

ECN 53
enterprise canonical number 53
entity link administration 37
evolution server 11
    application sequencing 12
    full-call model 11
evolution server administration 15
    AAR analysis table 27
    ARS analysis table 28
    checking connections 38
    checklist 15
    Communication Manager in application sequence 39
    Communication Manager managed element administration 35
    Communication Manager server application administration 39
    Communication Manager SIP entity 36
    dialplan analysis 22
    entity links 37
    feature access codes 23
    gateway recovery rule 32
    incoming call handling treatment 29
    IP network region 23
    minimum time of network stability 31
    node name 23
    privileged administrator account 34
    proxy route 29
    public unknown numbering 30
    recommendations 15
    route pattern 26
    SIP signaling group 24
    SIP trunk group 25
    SIP user verification 43
    Survivable Remote server 30
    Survivable Remote SIP entity 37
    synchronizing Communication Manager data 36
    testing calls 44
    uniform dial plan 27
evolution server configuration 14

F

feature access codes 23
feature name extension 51
feature name extension administration
    Communication Manager SAT interface 51
    System Manager Web Console 51
feature server 10

feature server *(continued)*
half-call model ... 11
feature server administration ... 15
AAR analysis table ... 27
ARS analysis table ... 28
checking connections ... 38
checklist ... 15
Communication Manager in application sequence ... 39
Communication Manager managed element administration ... 35
Communication Manager server application administration ... 39
Communication Manager SIP entity ... 36
dialplan analysis ... 22
entity links ... 37
feature access codes ... 23
gateway recovery rule ... 32
incoming call handling treatment ... 29
IP network region ... 23
minimum time of network stability ... 31
node name ... 23
privileged administrator account ... 34
proxy route ... 29
public unknown numbering ... 30
recommendations ... 15
route pattern ... 26
SIP signaling group ... 24
SIP trunk group ... 25
SIP user verification ... 43
Survivable Remote server ... 30
Survivable Remote SIP entity ... 37
synchronizing Communication Manager data ... 36
testing calls ... 44
uniform dial plan ... 27
feature server and trunk gateway ... 12, 19
feature server configuration ... 14
feature server trunk gateway administration
checklist ... 19
Communication Manager SIP entity ... 36
IP network region ... 23
node name ... 23
public numbering ... 20
routing from feature server to trunk gateway ... 33
routing from trunk gateway to feature server ... 32
SIP signaling group ... 24
SIP trunk group ... 25
System Manager ... 44
full-call model ... 11

G

gateway recovery rule ... 32

H

half-call model ... 11

I

ICHT ... 53
Identity ... 40
incoming call handling treatment ... 29, 53
IP network region ... 23

L

legal notice ...
long private numbering ... 57

M

managed element ... 35
minimum time of network stability ... 31

N

node name ... 23
numbering ... 53
administration ... 53
administration settings ... 54
numbering administration
call to public extension - variation 1 ... 61
call to public extension - variation 2 ... 62
long private numbering ... 57
private long numbering ... 56
private short numbering ... 55
public numbering ... 59
public signaling ... 57

O

OPTIM table ... 53
overview ... 10

P

private alias ... 53
private long numbering ... 56
private numbering table ... 53
private short numbering ... 55
privileged administrator account ... 34
proxy route ... 29
public number ... 53
public numbering ... 20, 59
public numbering table ... 53
public signaling ... 57
public unknown numbering ... 30
purpose of document ... 7

R

related documentation ... 8
roadmap ... 48

route pattern 26
routing feature server trunk gateway
Communication Manager application 46
Communication Manager SIP domain 45
Communication Manager SIP entity 36
entity links 37
routing from feature server to trunk gateway 33
ARS analysis table 28
checklist 33
incoming call handling treatment 29
route pattern 26
routing from trunk gateway to feature server 32
AAR analysis table 27
ARS digit conversion 33
checklist 32
route pattern 26

S

SIP deskphone administration 50
96xx 50
SIP signaling group 24
SIP trunk group 25
SIP user verification 43
support
contact 8
Survivable Remote server 30
Survivable Remote Session Manager documentation 47
Survivable Remote SIP entity administration 37
synchronization status 42
synchronizing Communication Manager data 36
synchronizing data 36

T

testing calls 44
translation 32
trunk gateway 12, 18
trunk gateway administration 18
AAR analysis table 27
Communication Manager SIP entity 36
dialplan analysis 22
IP network region 23
node name 23
SIP signaling group 24
SIP trunk group 25
trunk gateway administration checklist 18
trunk gateway and feature server 12, 19
trunk gateway feature server administration
checklist 19
Communication Manager SIP entity 36
IP network region 23
node name 23
public numbering 20
routing feature server trunk gateway
System Manager 44
routing from feature server to trunk gateway 33
routing from trunk gateway to feature server 32
SIP signaling group 24
SIP trunk group 25
System Manager 44

U

uniform dial plan 27

V

verifying a new SIP user 43
videos 8

W

Warranty 9