Administering Avaya Aura® Communication Manager Server Options

Release 6.2
03-603479
Issue 3.0
December 2012

© 2012 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 reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

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

Concurrent User License

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.

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.

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

Avaya® , Avaya Aura®, Avaya™, and Avaya Aura™ are registered trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Hardware Support

For full hardware support, please see *Avaya Support Notices for Hardware Documentation*, document number 03–600759 on the Avaya Support Web site, 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 9
- Warranty 9

Chapter 2: Overview 11
- Overview 11
- Feature server 11
  - Half-call model 12
- Evolution server 12
  - Full-call model 13
- Trunk gateway 13
- Combination feature server and trunk gateway 13

Chapter 3: Communication Manager Server administration 15
- Prerequisites 15
- Application Sequencing (Evolution Server) 15
- Recommendations 16
- Feature server or evolution server administration checklist 16
- SAT Administration Commands 19
  - Changing dialplan analysis 19
  - Changing feature access codes 19
  - Changing an IP network region 20
  - Adding a node name 20
  - Adding a SIP signaling group 21
  - Adding a SIP trunk group 22
  - Administering a Route Pattern 23
  - Changing the uniform dial plan 24
  - Administering AAR 25
  - Administering ARS Analysis 25
  - Administering the Proxy Route 26
  - Administering Incoming Call Handling Treatment 26
  - Adding a Survivable Remote Server 27
  - Administering Public Unknown Numbering 27
  - Validating Minimum time of network stability 29
  - Validating Gateway recovery rule 29
  - Adding a privileged administrator 30
- System Manager Administration 30
  - Creating a Communication Manager managed element 30
  - Synchronizing Communication Manager data 31
  - Adding a Communication Manager server as a SIP Entity 32

Adding a survivable remote server as a SIP entity 33
Creating entity links 33
Checking the connections 34
Administering the Communication Manager server as an application 35
Administering Communication Manager in an application sequence 35
Adding users 36
Verifying a new SIP user 39
Testing Session Manager and Communication Manager calls 39
Chapter 4: Communication Manager as a trunk gateway 41
Trunk gateway administration checklist 41
Adding a non-IMS SIP signaling group 42
Changing dialplan analysis (trunk gateway) 42
Chapter 5: Communication Manager as feature server and trunk gateway 45
Feature server and trunk gateway administration checklist 45
Adding an IMS-enabled SIP signaling group 46
Adding a non-IMS SIP signaling group/allow Dialog Loopbacks 47
Routing from trunk gateway to feature server 48
Routing from feature server to trunk gateway 49
Administering public numbering 50
Administering routing for feature server and trunk gateway on System Manager 51
Chapter 6: Survivable Remote Session Manager Documentation Roadmap 53
Chapter 7: SIP Phone administration 55
Administering 96xx SIP telephones 55
Chapter 8: Feature Name Extension Administration 57
Administering feature name extensions on SAT 57
Administering feature name extensions on System Manager 57
Appendix A: Numbering configuration 59
Numbering 59
Numbering administration 59
Recommendations 61
Private short numbering 61
Private long numbering 62
Long private numbering and public signalling 64
Public numbering 66
Call to public extension (variation 1) 67
Call to public extension (variation 2) 69
Index 71

Chapter 1: Introduction

Purpose

This document provides administration information, procedures, and references to Avaya Partners and customer administrators who will configure Avaya Aura® Communication Manager as a feature server or evolution server. This document presents a sample configuration for a network that uses Avaya Aura® Session Manager to connect Communication Manager as a feature server or an evolution server.

Intended audience

The primary audience for this document is:

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

Document changes since last issue

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

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

Related Resources

Documentation

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

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

Avaya Mentor videos

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

Visit http://www.youtube.com/AvayaMentor and do one of the following:

- Enter a key word or key words in the Search channel to search for a specific product or topic.
- Click the name of a playlist to scroll through the posted videos.

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 notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to get answers to questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

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

Overview

You can configure Communication Manager 6.2 as any of the following servers or gateways:

- Feature server
- Evolution server
- Trunk gateway
- Combination feature server and trunk gateway

Avaya 96XX IP deskphones, which are configured as SIP stations, use the Session Manager User Registration feature and require Communication Manager configured as a feature server or an evolution server.

Communication Manager as a feature server only supports SIP stations. Communication Manager applies the half-call model, that is, it applies only origination features during the origination (imsorig) phase and only termination features during the termination (imsterm) phase.

Communication Manager as an evolution server supports both SIP and non-SIP stations. Communication Manager applies the full-call model (applies both origination-side features and termination-side features in one step).

Using a Communication Manager as both a feature server and an evolution server is an unsupported and invalid configuration.

Avaya Aura® System Manager Release 6.1 and Avaya Aura® Session Manager Release 6.1 support Avaya Aura® Communication Manager Release 6.2.

Feature server

Communication Manager configured as a feature server provides features to SIP endpoints. It only supports SIP endpoints that are registered to an Avaya Aura® Session Manager. Communication Manager configured as a feature server uses the IP Multimedia Subsystem (IMS) half-call model for full application sequencing. It is connected to Session Manager via an IMS-enabled SIP signaling group and an associated SIP trunk group.

The Communication Manager feature server has the following constraints:

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

G430 and G450 gateways provide connection preserving failover and failback to Survivable Core and Survivable Remote processors.

Half-call model

The half-call model separates the processing of a call request into two phases:

- Origination, where services are applied to the originator of the call.
- Termination, where services are applied to the call recipient.

The origination and termination phases of the call are separate operations and can be performed by different feature servers.

Application sequencing works only when all the servers in a sequence support the half-call model. The number of originating sequenced applications may be different from the number of terminating sequenced applications.

Evolution server

Communication Manager configured as an evolution server is equivalent to the traditional Communication Manager. Evolution server provides Communication Manager features to both SIP and non-SIP endpoints. Evolution server uses the full-call model.

The connection from the evolution server to the Session Manager server is a non-IMS signaling group. Communication Manager is administered as an evolution server by disabling IMS on the signaling group to Session Manager. Session Manager handles call routing for SIP endpoints and enables the SIP endpoints to communicate with all other endpoints that are connected to the evolution server.

With Communication Manager configured as an evolution server:

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

Branch gateways provide connection preserving failover and failback to Survivable Core and Survivable Remote processors. Communication Manager as an evolution server can support IP-connected port networks, but they are not connection preserving.

Full-call model

In the full call model, the processing of a call request is done in one step. The origination and termination parts of the call are processed without a break. Classic Communication Manager adheres to the full-call model.

Because application sequencing expects the applications to follow the half-call model and because Communication Manager administered as an evolution server supports full-call model, no other sequenced application should be provisioned along with evolution server.

For the full-call model, the **IMS-enabled?** field on the SIP Signaling Group screen must be set to **n** (disabled).

Trunk gateway

Communication Manager as a trunk gateway provides an interface for trunk calls between Session Manager's SIP network and non-SIP networks, such as ISDN. These networks might be PSTN or private network calls.

Communication Manager as a trunk gateway only supports trunks. No other endpoints are supported.

The connection to Session Manager is a non-IMS SIP signaling group.

Combination feature server and trunk gateway

Communication Manager can function as a combination feature server and trunk gateway. Communication Manager only allows IMS to IMS and non-IMS to non-IMS traffic.

Two SIP signaling groups are required from Communication Manager to Session Manager. One is an IMS signaling group to support the feature server role of Communication Manager, the other is a non-IMS signaling group to support the trunk gateway role. The configuration must ensure that the two roles are not mixed internally.

All routing for IMS users must be to Session Manager.

Calls that come in on IMS trunks cannot route to anything except an IMS trunk. This means you need two sets of ARS route tables: one for calls that come in on IMS trunks, and the other for calls that come in on the non-IMS SIP trunks and the non-SIP trunks.

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

Chapter 3: Communication Manager Server administration

This section describes an example of how to define the connection and routing between Session Manager and Communication Manager as a feature server or evolution server.

Prerequisites

- Install Communication Manager on System Manager.
- Install the patches as required.
- Patch the Communication Manager feature server through the System Platform Web Console using the **Server Management** > **Patch Management** option.
- Configure Processor Ethernet IP using the add ip-interface *procr* SAT command.
- Add the required Gateways using the *add media-gateway x* SAT command.
- Install the Communication Manager license using System Platform Web Console using the MAC address of the Communication Manager feature server or evolution server.
- Install the Communication Manager authentication file using System Platform Web console. Both the Communication Manager feature server and the simplex survivable remote require their own authentication files.
- Ensure System Manager and Session Manager are active in the existing SIP routing deployment.
- In Gateways, the system updates the mgc lists with two IP addresses. The first address is the Main Communication Manager feature server Processor Ethernet IP address, and the second address is the Simplex Survivable Remote Processor Ethernet IP address.
- Configure SSH client, such as PuTTY or Avaya site administrator (ASA), on the system to access the server command line interface (CLI).

Application Sequencing (Evolution Server)

Communication Manager as an evolution server supports a limited form of application sequencing:

- Non-SIP users get implicit application sequencing only
- SIP users get explicit application sequencing with the following caveats:
  - Origination-side sequencing: Sequenced applications *must be placed BEFORE* Communication Manager in the sequence vector. Any application sequenced before Communication Manager will not see a normalized number. Communication Manager applies its dial plan transformation rules to normalize the Request URI.
  - Termination-side sequencing: Sequenced applications *must be placed AFTER* Communication Manager in the sequence vector.

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

Recommendations

The following are administration recommendations:

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

Feature server or evolution server administration checklist

Use this checklist to administer Communication Manager as a main feature server or evolution server.

Communication Manager as a feature server or evolution server is first administered on Communication Manager using system administration terminal (SAT) screens, then administered using System Manager.

Prerequisites:

- Install and administer Session Manager.
- Install the appropriate service packs, as applicable.
- Install Communication Manager with the license.

Table 1: Feature server and evolution server administration checklist

#	Steps	Link	✔
1	Log in to the main Communication Manager server.		
2	Change the dial plan analysis.	Changing dialplan analysis on page 19	
3	Add the feature access codes for AAR and ARS.	Changing feature access codes on page 19	
4	Add the appropriate SIP domain in the Network Region that will be used.	Changing an IP network region on page 20	
5	Administer a node name for the IP address of the Session Manager Security Module.	Adding a node name on page 20	
6	Administer a SIP signaling group.	Adding a SIP signaling group on page 21	
7	Add trunk groups for each Session Manager.	Adding a SIP trunk group on page 22	
8	Configure the appropriate Route Patterns.	Administering a Route Pattern on page 23	
9	Administer the Uniform Dial Plan for non-SIP calls.	Changing the uniform dial plan on page 24	
10	Administer AAR analysis.	Administering AAR on page 25	
11	Administer ARS Analysis for non-SIP calls.	Administering ARS Analysis on page 25	
12	Add the appropriate Route Pattern as the Proxy Route.	Administering the Proxy Route on page 26	
13	Administer incoming call handling treatment.	Administering Incoming Call Handling Treatment on page 26	
14	Add a Survivable Remote server, if applicable.	Adding a Survivable Remote Server on page 27	
15	Change public unknown numbering so that the caller-id will appear as E.164.	Administering Public Unknown Numbering on page 27	
16	If applicable, validate the minimum time of network stability for Gateways to failback to the main Communication Manager when it becomes available.	Validating Minimum time of network stability on page 29	

#	Steps	Link	✔
17	If applicable, validate the Gateway recovery rule.	Validating Gateway recovery rule on page 29	
18	Save translations with the **save translations** SAT command.		
19	Add a privileged administrator to be used only by System Manager.	Adding a privileged administrator on page 30	
20	Log in to the System Manager Web console if you are not logged in already.		
21	Administer the Communication Manager server as a managed element.	Creating a Communication Manager managed element on page 30	
22	Synchronize Communication Manager data.	Synchronizing Communication Manager data on page 31	
23	Add the Communication Manager feature or evolution server as a SIP Entity.	Adding a Communication Manager server as a SIP Entity on page 32	
24	If adding a Survivable Remote Session Manager, add it as a SIP Entity.	Adding a survivable remote server as a SIP entity on page 33	
25	Create entity links between Session Manager and Communication Manager.	Creating entity links on page 33	
26	Verify the connections between Communication Manager and Session Manager.	Checking the connections on page 34	
27	Administer the Communication Manager server as an application.	Administering the Communication Manager server as an application on page 35	
28	Administer the Communication Manager server in an Application Sequence.	Administering Communication Manager in an application sequence on page 35	
29	Add users.	Adding users on page 36	
30	Verify users.	Verifying a new SIP user on page 39	
31	Test Session Manager and Main Communication Manager feature server or evolution server calls.	Testing Session Manager and Communication Manager calls on page 39	

SAT Administration Commands

Changing dialplan analysis

1. On Communication Manager interface, enter the SAT command: **change dialplan analysis**.

2. Enter the appropriate dial plan digits as required.

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

3. Submit the form.

Changing feature access codes

About this task

Use the **change feature-access-codes** command to add the feature access codes for AAR and ARS.

Note:

- #83 – Used for AAR access code.
- 9 – Used for ARS access code.

Procedure

1. On the Communication Manager interface, enter **change feature-access-codes** command.
2. In the **Auto Alternate Routing (AAR) Access Code** field, enter an access code (for example, **#83)**.

3. In the **Auto Route Selection (ARS) - Access Code 1** field, enter an access code (for example, **9**).
4. Submit the form.
   The system displays the feature access code.

Changing an IP network region

About this task

Use the **change ip-network-region** command to add all appropriate IP address to node-name mappings. Administer the IP network region that are referred to in the SIP signaling group to Session Manager (defined later).

Procedure

1. On the Communication Manager interface, enter `change ip-network-region` *x*, where *x* is an IP network region number.
2. In the **Authoritative Domain** field, enter the name of the domain that the network region is responsible for. For example, MyCompany.com.
3. In the **Name** field, enter a descriptive name. For example, Main_SM_NR.
4. Submit the form.
   The system updates the changes to IP network region.

Note:

For detailed information on administration of IP network regions, see the 'Administering IP network regions' section of the *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Adding a node name

About this task

Define a node name for the IP address of the Session Manager Security Module.

procr is the main Communication Manager server Processor Ethernet IP address.

Procedure

1. On the Communication Manager nterface, enter **change node-names ip** command.

2. In the **Name** field, enter the name associated with the IP address of the Session Manager Security Module, that is, SM1HostName.
3. In the **IP Address** field, enter the IP address of the Session Manager Security Module.
4. Submit the form.
   The system adds the node name.

Adding a SIP signaling group

About this task

Add a SIP signaling group for each Session Manager Security Module in the system configuration. Use the **add signaling-group *x*** command to add an IMS enabled signaling group for each Session Manager SM100 in deployment. The **IMS Enabled?** field on this form determines whether the Communication Manager server operates as a feature server or evolution server.

Procedure

1. On the Communication Manager interface, enter **add signaling-group *next*** command.
2. Note the value of the **Group Number**.
3. In the **Group Type** field, select `sip`. By default, the value of **Group Type** is `ISDN-PRI`. If the system does not display `sip` in the **Group Type** field, select `sip` from the drop-down menu and right-click to display the associated fields on the screen.
4. Do one of the following for **IMS Enabled?** field:
   a. To configure Communication Manager as a feature server, in the **IMS Enabled?** field, select `y`.
   b. To configure Communication Manager as an evolution server, in the **IMS Enabled?** field, select `n`.
5. In the **Transport Method** field, select `tls` or `tcp` depending on whether the calls to be run are secure calls.
6. In the **Peer Detection Enabled?** field, select `y`.

   Note:

   Selecting the value of **Peer Detection Enabled** as y causes a message interchange between Communication Manager and the connected SIP server. The value for **Peer Server** changes to `SM` when the SIP signaling group is put into service.

   For ASM trunks, perform the following steps:

   a. Set the **Peer Detection** field to `n`.

b. Set the **Peer Server** field to `SM`.

7. In the **Near-end Node Name** field, select `procr`.
8. In the **Far-end Node Name** field, enter the name of the Session Manager Security Module.
9. In the **Far-end Network Region** field, enter the same Network Region number that you used on the **change ip-network-region**.
10. In the **Far-end Domain** field, enter the domain name associated with Session Manager.
11. In the **Enable Layer 3 Test?** field, select `y`. The system displays the **Enable Layer 3 Test?** field when you enter the value in **Far-end Node Name** field.

    Important:

    If the value of **Enable Layer 3 Test?** field is selected as `n`, the Communication Manager does not monitor the links. This test is required for trunks connected to Session Manager. Maintenance software takes the trunks out of service if this test is disabled.
12. In the **Initial IP-IP Direct Media** field, select `y` or `n` depending on the requirement of the **Direct Media** feature.
13. To configure the Communication Manager as an evolution Server, in the **H.323 Station Outgoing Direct Media** field, select `y`.
14. Submit the form.
    The system adds the SIP signaling group.

Adding a SIP trunk group

About this task

Add a SIP trunk group to the SIP signaling group using the **trunk-group** *x* command for call routing from the Communication Manager server to Session Manager.

For the **Numbering Format** field in Step 10:

- Use **public** numbering for a trunk that gets ARS calls.
- Use **private** numbering for a trunk that gets SIP calls.

Procedure

1. On the Communication Manager interface, enter **add trunk-group *next***.
2. In the **Group Type** field, enter `sip`.

3. In the **Group Name** field, enter the name of the Session Manager Security Module.
4. Enter a **TAC** as per the dac added in the dial plan analysis table, that is, *110.
5. In the **Direction** field, enter `two-way`.
6. In the **Service Type** field, enter `tie`.
7. In the **Signaling Group** field, enter the SIP signaling group number that you added earlier.
8. In the **Number of Members** field, enter the number of trunk group members. The required limit of the number of members is up to 255.
9. Go to Page 3 of the trunk-group form.
10. If you will be using a private network, enter **unk-pvt** in the **Numbering Format** field. Otherwise, enter **Public**.
11. Submit the form.
    The system adds the SIP trunk group.

Administering a Route Pattern

About this task

Nonenterprise number route patterns are used for calls going to non-SIP telephones. This type of Route Pattern prepends a plus (+) to 11-digit calls from UDP/AAR and ARS to be routed to Session Manager as 12-digit E.164.

Enterprise number route patterns are used for SIP telephones only. This type of route pattern does not insert any digits or a plus.

If multiple Session Managers exist in a deployment, multiple trunk groups can be specified in the **Grp No** column. Use the **next** option in each LAR row corresponding to the trunk group row numbers. This option allows calls to fail over to multiple trunk groups in the event of a trunk failure.

Procedure

1. For nonenterprise number routing, on the Communication Manager interface, do as follows:
   a. In the **change route-pattern *x*** field, enter the value of *x* where *x* is the number of the route pattern.
   b. In the **Pattern Name** field, enter a Route Pattern Name (for example, **TO_SM6**).
   c. In the **Grp No** field, enter the trunk group number for Session Manager which you added earlier.
   d. In the **FRL** field, enter **0**

e. In the **Inserted Digits** field, enter **p** so that a plus (+) is prepended to the digits.
f. Submit the form.
The system adds a route pattern for nonenterprise number routing.

2. For enterprise number routing, on the Communication Manager interface, do as follows:
   a. In the **change route-pattern *x*** field, enter the value of *x*, where *x* is the number of route pattern.
   b. In the **Pattern Name** field, enter a Route Pattern Name (for example, **SIP_PHONE_ONLY**).
   c. In the **Grp No** field, enter the trunk group for the Session Manager which you added earlier.
   d. In the **FRL** field, enter **0**.
   e. Submit the form.
   The system adds a route pattern for enterprise number routing.

Changing the uniform dial plan

Use the **change uniform-dialplan *x*** command to add entries in the Uniform Dial Plan to prepare digits to be routed through the AAR table.

In the following example for nonenterprise station calls, when 5-digit calls starting with 2, 4, 5, 6, or 7 are dialed, the Uniform Dial Plan inserts digits to build them up to 11-digit numbers to be routed through AAR. In this example, the inserted digit string is **120983**.

1. Enter **change uniform-dialplan *x*** where *x* is the number of the dial plan.
2. Enter the date in the Uniform Dial Plan table.

   Refer to the following example on how to enter values in the Uniform Dial Plan table.

   Table 2: Example – Changing the uniform dial plan

Matching Pattern	Len	Del	Insert 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

3. Submit the form.

The system updates the uniform dial plan.

Administering AAR

Use the **change aar analysis *x*** command to add appropriate entries for SIP station and non-SIP station calls. AAR routes calls within a company over the company's private network.

In the following example, two entries are used:

- 11-digit numbers starting with 1 (non-SIP station calls) are sent to Route Pattern 10 to have a plus (+) inserted before being routed to Session Manager.
- 5-digit numbers starting with 3 (SIP station extensions) are sent to Route Pattern 11 where they are sent to Session Manager untouched.

1. On SAT, enter **change aar analysis *x*** command where *x* is an AAR table number. In this example, the value of *x* is 0.
2. Enter information in the AAR table, as displayed in the following table:

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

3. Submit the form.

   The system saves the information for SIP station and non-SIP station calls.

Administering ARS Analysis

Use the **change ars analysis *x*** command to send the appropriate 9+11– digit calls to route pattern 10.

1. Enter **change ars analysis *x*** where *x* is the number of the ARS Analysis table.
2. Enter data in the table, as shown in the following example:

Dialed String	Total Min	Total Max	Route Pattern	Call Type	ANI Reqd
1	11	11	10	natl	n
101xxxx0	8	8	deny	op	n
101xxxx0	18	18	deny	op	n
101xxxx01	16	24	deny	iop	n
101xxxx011	17	25	deny	intl	n
101xxxx1	18	18	deny	fnpa	n

Dialed String	Total Min	Total Max	Route Pattern	Call Type	ANI Reqd
10xxx0	6	6	deny	op	n
10xxx0	16	16	deny	op	n
10xxx01	14	22	deny	iop	n
10xxx011	15	23	deny	intl	n
10xxx1	16	16	deny	fnpa	n
1200	11	11	deny	fnpa	n
1209	11	11	10	natl	n
1300	11	11	deny	fnpa	n
1400	11	11	deny	fnpa	n

3. Submit the form.

   The system saves the changes for ARS analysis.

Administering the Proxy Route

About this task

Use the **change locations** command to add the appropriate Route Pattern as your proxy route.

Procedure

1. On SAT, enter the **change locations** command.
2. In the **Name** field, enter a Name (for example, Main).
3. In the **Proxy Sel Rte Pat** field, enter the appropriate Route Pattern number.
4. Submit the form.
   The system adds the selected Route Pattern for proxy route.

Administering Incoming Call Handling Treatment

About this task

Use Incoming Call Handling Treatment, using **change inc-call-handling-trmt trunk-group *x*** command, to strip down any SIP station calls that are sent to the Communication Manager feature server or evolution server as a 12-digit number. Delete the number of digits as necessary to match the SIP extension length in the Communication Manager feature server or evolution server.

In the following example, any 12-digit calls starting with +1209833 that arrive on Trunk Group 10 has the first 7 digits deleted to match the 3xxxx SIP extensions.

Ensure to follow this process for any trunk group going to Session Manager from the Communication Manager feature server or evolution server.

Procedure

1. On SAT, enter **change inc-call-handling-trmt trunk-group *10***.
2. In the **Number Len** field, enter **12**.
3. In the **Number Digits** field, enter **+1209833**.
4. In the **Del** field, enter **7**.
5. Submit the form.
   The system saves the changes for incoming call handling treatment.

Adding a Survivable Remote Server

Procedure

1. On SAT, enter **add survivable-processor *node-name*** where *node-name* is the name of the remote server. For example, lsp6 was added on the **change node-name ip** form.
2. If you have an LSP or Survivable Remote server, ensure that the **Type** field is **lsp** for each Survivable Remote server.
3. Ensure that the **Cluster ID/MID** matches the MID number used in the Web interface of the Survivable Remote server in **Server Maintenance** > **Server Configuration** > **Server Role**.
4. Submit the form.
   The system adds the survivable remote server.

Administering Public Unknown Numbering

About this task

Perform this task to add appropriate information so that the system displays the caller ID in the E.164 format.

Procedure

1. On SAT, type **change public-unknown-numbering 0**.

2. In the **Ext Len** field, type the number of digits of the extension.
3. In the **Ext Code** field, type one or more starting digits of the extension.
4. In the **CPN Prefix** field, type the digits to be attached as a prefix to the digit string.

Connection type	Server	Numbering format	Country code required?	Plus sign (+) required?	Action
SIP	Session Manager	Full international E.164 number	Yes	Yes	Communication Manager automatically inserts the plus sign (+)
SIP	other	Full international E.164 number	Yes	Yes	On the Protocol Variation screen of the SIP trunk group, set the **Prepend '+' to Calling Number** field 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	Full international E.164 number	Yes	No	Set the **Format** field on an ISDN trunk group to intl-pub

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

Note:

The value in the **CPN Prefix** field is combined with the extension that matches the entry on the Numbering –Public/Unknown Format screen. If the length of the number that is generated is longer than the length defined in **Total CPN Len**, then the system deletes the leading digits from the extension until the length of the number is equal to the length defined in **Total CPN Len**.

6. Submit the form.

Validating Minimum time of network stability

About this task

Validate that the **Minimum time of network stability** is set to 3 minutes. With the 3-minute timer, the gateway can failback to the main Communication Manager feature server or evolution server when it becomes available. The 3-minute timer also prevents unnecessary failback and failover when the network is unreliable.

Procedure

1. On SAT, enter **change system-parameters mg-recovery-rule 1**.
2. In the **Minimum time of network stability** field, verify that the value is **3**.
3. If the value of the **Minimum time of network stability** field is not **3**, change the value to **3**.
4. Submit the form.

Validating Gateway recovery rule

About this task

1. On SAT, enter **display media-gateway *x*** where *x* is the number of the Gateway.
2. Validate that the correct recovery rule number is specified for each Gateway in the **Recovery Rule** field.
3. Enter **Recovery Rule** numbers from 1 to 50 or **(none)** to disable the recovery rule.
4. You can enter values up to 250 on the Gateway form, where 250 is the maximum number of supported Gateways on any platform. **(none)** indicates that the system does not accept any automatic fallback registrations. The value of 1 to 250 applies the specific recovery rule to that gateway. You can apply a single rule to all Gateways, or each Gateway can have its own rule and any permutation in between.

The recovery rules are administered on the **system-parameters mg-recovery-rule** form. Also **system-parameters mg-recovery-rule** gives you the assigned **Recovery Rule** numbers from 1 to 50.

Procedure

1. On SAT, enter **change media-gateway *x*** where *x* is the number of the Gateway.
2. In the **Recovery Rule** field, verify the number of the recovery rule associated with this Gateway.

3. Submit the form.

Adding a privileged administrator

About this task

Add a privileged administrator to be used only by System Manager. Use the Administrator Accounts page to add a login that is a member of the **suser** group.

Procedure

1. Log in to the Communication Manager server System Management Interface (SMI).
2. Select **Security** > **Administrator Accounts** from the menu on the left.
3. Select **Action** > **Add Login** > **Privileged Administrator**.
4. Click **Submit**.
5. In the **Login Name** field, enter your login name.
6. In the **Password** field, enter your password.
7. Re-enter the password in the **Re-enter password** field.
8. Click **No** for **Force password/key change on next login**.
9. Click **Submit**.

System Manager Administration

Creating a Communication Manager managed element

About this task

System Manager uses the Communication Manager managed element to synchronize with the Communication Manager feature server or evolution server and enable the ability to add SIP stations to the Communication Manager feature server or evolution server from System Manager.

Procedure

1. On the System Manager web interface, under **Elements**, select **Inventory** > **Manage Elements**.
2. Click **New**.
3. In the **Type** field, select **CM** from the drop-down menu.
4. In the **Application** section, perform the following steps:
   a. Enter the **Name** of the Communication Manager server.
   b. In the **Node** field, enter the management IP address of the Communication Manager (address for SAT access).
5. In the **Attributes** section, perform the following steps:
   a. In the **Login** field, enter the SSH SAT login. The SAT login is the login you created earlier for privileged administrator.
   b. In the **Password** field, enter the password (the password you created earlier for privileged administrator).
   c. In the **Confirm Password** field, retype the password that you typed in **Password** field to confirm the password.

      Note:

      Services logins MUST NOT be used (for example, craft, dadmin, inads) Create a NEW login for System Manager only. You will add this SAME login and password on Communication Manager to allow System Manager access to Communication Manager. Synchronization will not occur unless the Communication Manager login administration is done.
   d. Select the **Is SSH Connection** check box.
   e. In the **Port** field, enter `5022`.
6. Click **Commit**.
   System Manager creates the Communication Manager system managed element.

Synchronizing Communication Manager data

About this task

After adding the Communication Manager server as an Inventory item, System Manager automatically attempts to synchronize with the Communication Manager server.

Procedure

1. Using the System Manager web interface, under **Elements** , select **Inventory** > **Synchronization** > **Communication System**

2. If synchronization has not started for the Communication Manager server:
   a. Select the check box in front of the appropriate Communication Manager server name.
   b. Scroll to the bottom of the Element List table.
   c. Select **Initialize data for selected devices**.
   d. Click **Now**.
      The system displays the status alert icon.

      The synchronization process might take several minutes. At the top of the table, click **Refresh** to show the current synchronization status. The **Sync Status** displays **Completed** when synchronization is completed.

Adding a Communication Manager server as a SIP Entity

About this task

Add a Communication Manager feature or evolution server as a SIP entity. No adaptation should be used on the Communication Manager server so that SIP headers created by the Communication Manager server are maintained for proper application sequencing and routing.

Procedure

1. Using the System Manager web interface, under **Elements**, select **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, enter the name of the Communication Manager server.
4. In the **FQDN or IP Address** field, enter the IP address of the Communication Manager server.
5. In the **Type** field, select **CM** from the drop-down list.
6. In the **Notes** field, enter a short description of the Communication Manager.
7. In the **Location** field, select the location of the Communication Manager Server.
8. In the **Time Zone** field, select a value from the drop-down menu.
9. Click **Commit**.
   The system adds the Communication Manager server name to the SIP entities list.

Adding a survivable remote server as a SIP entity

Procedure

1. Using the System Manager Web interface, in **Elements**, select **Routing** > **SIP Entities**.
2. Select **New**.
3. In the **FQDN or IP Address** field, enter the IP address of the security module of the Survivable Remote Session Manager server.
4. In the **Type** field, select **Session Manager** from the drop-down menu.
5. Click **Commit**.
   The system adds the survivable remote server as a SIP entity.

Creating entity links

About this task

Create the entity links between the following, when applicable:

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

If you configure separate entities and entity links in the core for the feature server (feature server or IMS) link and the trunk gateway (trunk gateway or non-IMS) link, then an entity link must be configured from the survivable remote server to each of those entities for a total of two entity links on the survivable remote server. If you use only one entity or entity link, as in an evolution server configuration, then only one link is administered on the Survivable Remote server.

The transport and port does not have to be TLS and 5061. The Branch Session Manager to Communication Manager entity links must match the transport and port values used in the links between the core Session Manager and Communication Manager.

Procedure

1. On the System Manager Web console, click **Elements** > **Routing** > **Entity Links**.
2. Click **New**.
3. In the **Name** field, enter a descriptive Entity Link name, that is, from one Session Manager server to a Communication Manager feature server.

4. In the **SIP Entity 1** field, select the name of the survivable remote Session Manager server from the drop-down menu that the Communication Manager Server must be linked to.
5. In the **Protocol** field, enter `tls`.
6. In the **Port** field, enter `5061`.
7. In the **SIP Entity 2** field, select the name of the Communication Manager server from the drop-down menu that the survivable remote Session Manager server must be linked to.
8. In the **Port** field, enter `5061`.
9. In the **Connection policy** list box, select `Trusted`.
10. (Optional) In the **Notes** field, enter a note about the entity link you are creating.
11. Click **Commit**.
    The system creates the entity link and displays the entity link in the **Entity lists** list.

Checking the connections

Procedure

1. On Communication Manager, perform the following steps:
   a. Enter the command **list history**.
   b. Verify that you are logged into Session Manager.
   c. Verify that initial data synchronization has begun.
2. Check the Communication Manager SIP Entity Link status by performing the following steps:
   a. On System Manager, under **Elements**, select **Session Manager** > **System Status** > **SIP Entity Monitoring**.
   b. Select the Communication Manager server name from the list of **All Monitored SIP Entities**.
   c. Verify that in the **Link Status** field, Up is selected for the Communication Manager server.
3. Check the Session Manager Dashboard by performing the following steps:
   a. On System Manager, under **Elements** , select **Session Manager** .
   b. Verify that Session Manager is active.

Administering the Communication Manager server as an application

About this task

Administer the Communication Manager server as an application for an application sequence.

Procedure

1. On the System Manager console, under **Elements** , select **Session Manager** > **Application Configuration** > **Applications**.
2. Click **New**.
3. Enter the application **Name**.
4. In the **SIP Entity** field, select the associated Communication Manager server from the drop-down list.
5. Select the Communication Manager managed element that you created earlier from the **CM System for SIP Entity** drop-down list.
6. (Optional) Enter a description for the CM managed element.
7. Leave the **Application Handle** and **URI Parameters** fields blank.
8. Click **Commit**.

Administering Communication Manager in an application sequence

About this task

Create an application sequence for the Communication Manager server application.

Important:

If Communication Manager has been configured as an evolution server, Communication Manager must be last in the origination vector and *first* in the termination vector. Since Communication Manager as an evolution server operates in the full-call model, there is no flexibility in positioning applications with respect to Communication Manager.

Procedure

1. On the System Manager console, under **Elements**, select **Session Manager** > **Application Configuration** > **Application Sequences**.
2. Click **New**.
3. Enter a **Name** and a **Description** for the application sequence.

4. Under the **Available Applications** section, click the + sign in front of the appropriate Communication Manager server.
   When the screen refreshes, the **Mandatory** check box gets selected.
5. Click **Commit**.

Adding users

About this task

You can ignore any input fields that has not been mentioned in the following steps. There are some fields which are not used for Session Manager user administration.

A user can have more than one communication profile. For more information regarding the fields, refer to the online help.

If there is a secondary Session Manager defined for a user, the route pattern in Communication Manager needs to have two trunks listed:

- First trunk is associated with the primary Session Manager.
- Second trunk is associated with the secondary Session Manager.

  There also needs to be a second signaling group to the secondary Session Manager.

Procedure

1. On the System Manager console, under **Users**, select **User Management** > **Manage Users**.
2. Click **New**.
3. In the **Identity** section, perform the following steps:
   a. In the **Last Name** field, enter the last name of the user.
   b. In the **First Name** field, enter the first name of the user.
   c. In the **Middle Name** field, enter the middle name of the user.
   d. (Optional) In the **Description** field, enter the description about the user you are going to add.
   e. Using the appropriate SIP domain in Session Manager, in the **Login** field, enter the login in the format: `name@domain.com`
   f. In the **Authentication Type** field, enter the value as `Basic`.
   g. In the **Login Password** field, enter your password. Note that the password must start with a lower or upper case alphabet.
   h. In the **Confirm Password** text box, re-enter the password that you entered in the **Login Password** field.
   i. In the **Localized Display Name** field, enter the name of the user that is displayed to the calling party.
   j. In the **Endpoint Display Name** field, enter the full text name of the user.

k. From the **Language Preference** drop-down menu, select a language.
l. From the **Time Zone** drop-down menu, select a time zone.

4. Select the **Communication Profile** tab at the top of the screen.
5. In the **Communication Profile Password** field, enter your communication profile password.

Note:

This field *must* be administered. The password must all be numeric characters. This is the password that is used when logging in to the telephone. Remember this password as it will be used later for the Endpoint Profile Security code.

6. In the **Confirm Communication Profile Password** text box, re-enter your communication profile password to confirm it.
7. In the **Communication Address** section:
   a. Click **New**.
   b. From the **Type** drop-down menu, select **Avaya SIP**.
   c. In the **Fully Qualified Address** field, enter the full extension number of the SIP telephone.
   d. Select the correct domain from the drop-down menu following the @ sign.
   e. Click on the **Add** button.
   f. Check the box in front of the entry you just added.
   g. Click on the **New** button.
   h. From the **Type** drop-down field, select **Avaya E.164**.
   i. If you are using private numbering, administer **Fully Qualified Address**, which is the private handle. The private handle depends on the numbering format.
   j. Select the appropriate domain from the drop-down menu following the @ sign.
   k. Click **Add**.
8. Click the **Session Manager Profile** show / hide button.
9. Check the box to the left of the **Session Manager Profile** show/hide button.
10. In the **Session Manager Profile** section:
    a. In the **Primary Session Manager** field, select the appropriate Session Manager instance that should be used as the home server from the drop-down menu.
    b. If applicable, in the **Secondary Session Manager** field, select the appropriate Session Manager instance that should be used as the backup server from the drop-down menu.

       As soon as you select the primary Session Manager and secondary Session Manager, the system displays the count in the table, which is towards the right side of these sections.

c. In the **Origination Application Sequence** field, select the appropriate application sequence name that will be used when calls are routed from this user from the drop-down menu. This field is optional.
d. In the **Termination Application Sequence** field, select the appropriate application sequence name that will be used when calls are routed to this user from the drop-down menu. This field is optional.
e. In the **Survivability Server** field, select the entity that will be used for survivability. This field is optional. For a Survivable Remote Session Manager, select the Survivable Remote Session Manager SIP Entity from the drop-down menu.
f. In the **Home Location** field, select the Communication Manager server SIP Entity that should be used as the home location for call routing for this user.

11. Verify that data synchronization has completed:
    a. On the System Manager console, under **Elements** , select **Inventory** > **Synchronization** > **Communication System** .
    b. The synchronization status is displayed in the **Sync Status** column.
12. Assign the user to a Communication Manager station:

    Note:

    This step cannot be done until synchronization of the data has completed.

    a. Click the show/hide button next to **Endpoint Profile**.
    b. Check the box to the left of the **Endpoint Profile** show/hide button.
    c. In the **System** field, select the Communication Manager server from the drop-down menu.
    d. From the **Profile Type** drop-down box, select the profile type.
    e. Leave the box for **Use Existing Stations** unchecked.
    f. Enter the extension that is administered on Communication Manager for the existing or new station in the **Extension** field.
    g. Select the appropriate **Template** from the drop-down menu. For a Session Manager server, use the SIP version of the template (i.e., DEFAULT_9640SIP_CM_6_0).
    h. In the **Set Type** field, enter the set type.
    i. The **Security Code** field can be left blank. The Security Code is not used to log in to the telephone.
    j. Enter `IP` in the **Port** field.
    k. In the **Voice Mail Number** field, enter the voice mail number.
    l. Select the **Delete Endpoint on Unassign of Endpoint from User** check box.
    m. Select the **Override Endpoint Name** check box.
13. Click **Commit**.
    System Manager adds the new station in Communication Manager.

Verifying a new SIP user

Procedure

1. Login to the SIP telephone using the Endpoint Profile `extension` and `password`.
2. Check the Registration Summary:
   a. On System Manager, under **Elements**, select **Session Manager** > **System Status** > **User Registration**
   b. In the table, click **Show** in the row containing the Address and Login Name of the user.
   c. Verify that the information in the **Registration Detail** record is correct.
3. Check the station information:
   a. On Communication Manager, enter **display station xxx** where *xxx* is the telephone extension of the user.
   b. Verify that the telephone type is **SIP**.
   c. Go to Page 6 of the station form.
   d. Verify that **SIP Trunk** is **aar**.
4. Check the off-pbx-teletelephone station mapping:
   a. On Communication Manager, enter **display off-pbx-telephone station-mapping xxx** where *xxx* is the phone extension of the user.
   b. Verify that **Trunk Selection** for the phone extension is **aar**.

Testing Session Manager and Communication Manager calls

Procedure

1. Place 5-digit calls from one SIP extension to another.
2. Place 9+11-digit calls from one SIP extension to another.
3. Place 5-digit calls to a non-SIP telephone on another PBX on Session Manager to validate routing.
4. Place 9+11-digit calls to a non-SIP telephone on another PBX on Session Manager to validate routing.

Chapter 4: Communication Manager as a trunk gateway

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

Trunk gateway administration checklist

#	Task	Link to description	✔
1	Log in to Communication Manager.		
2	Administer a node name for the IP address of the Session Manager Security Module.	Adding a node name on page 20	
3	Administer an IP network region that will be referred to in the SIP Signaling Group to Session Manager (defined later).	Changing an IP network region on page 20	
4	Administer a non-IMS SIP signaling group.	Adding a non-IMS SIP signaling group on page 42	
5	Administer a SIP trunk group to the SIP signaling group.	Adding a SIP trunk group on page 22	
6	Administer the dial plan.	Changing dialplan analysis (trunk gateway) on page 42	
7	Log in to System Manager.		
8	Add the Communication Manager server as a SIP entity.	Adding a Communication Manager server as a SIP Entity on page 32	
9	For routing, administer a Routing Policy with the trunk gateway as the destination.		

#	Task	Link to description	✔
10	Administer the Dial Pattern that uses the above Routing Policy.		

Adding a non-IMS SIP signaling group

About this task

Set up a SIP signaling group with IMS disabled from the Communication Manager trunk gateway to the Session Manager security module.

When the signaling group is released, peer detection will detect the peer server and change the value in the **Peer Server** field. The value should be `SM`.

Procedure

1. Enter `add signaling-group` *`next`*.
2. In the **Group Type** field, enter `sip`.
3. Set **IMS Enabled?** to `n`.
4. Set **Peer Detection Enabled** to **y**.
5. Set **Near-end Node Name** to `procr`.
6. Set **Far-end Node Name** to the name of the Session Manager Security Module.
7. Set **Far-end Domain** to the domain name.
8. Set **Enable Layer 3 Test?** to `y`.
   If this field is set to `n`, Communication Manager does not monitor the links.
9. Submit the form.
   The system adds the non-IMS SIP signaling group.

Changing dialplan analysis (trunk gateway)

About this task

Administer the dialplan to route the Communication Manager external numbers via AAR to the non-IMS signaling group and trunk to Session Manager.

Procedure

1. Enter **change dialplan analysis**
2. Enter a **Dialed String** to be used for the trunks.
3. In the **Call Type** field, enter **aar**.
4. Submit the form.
5. Enter **change aar analysis xx** where **xx** is the first two digits of the Dialed String.
6. In the **Dialed String** field, for each Dialed String you entered on the **change dialplan analysis** form:
   a. Enter the Dialed String
   b. Enter the total number of Minimum and Maximum digits.
   c. Enter the **Route Pattern** number that will be used.
   d. For **Call Type**, enter **pubu**.
7. Submit the form.

Chapter 5: Communication Manager as feature server and trunk gateway

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

Two SIP signaling groups are set up between Communication Manager and Session Manager. One is a non-IMS signaling group to access the trunk gateway part of Communication Manager, the other is an IMS-enabled signaling group for the connection to the feature server.

All routing for IMS users must be to Session Manager. For example, an incoming public trunk call to an IMS user must route directly to Session Manager on a non-IMS SIP signaling group which in turn routes the call back to the Communication Manager Trunk Gateway using the IMS-enabled signaling group to the Feature Server part of Communication Manager.

Feature server and trunk gateway administration checklist

Table 3: Feature server and trunk gateway administration checklist

#	Administration Action	Link to action	✔
1	Log in to Communication Manager.		
2	Add a node-name for the IP address of the Session Manager Security Module.	Adding a node name on page 20	
3	Define an IP network region that will be referred to in the Signaling Group to Session Manager (defined later).	Changing an IP network region on page 20	
4	Set up a SIP signaling group with IMS enabled.	Adding an IMS-enabled SIP signaling group on page 46	
5	Add a SIP trunk group to the SIP signaling group.	Adding a SIP trunk group on page 22	
6	Administer the dial plan to route the Communication Manager external numbers		

#	Administration Action	Link to action	✔
	via AAR to the non-IMS signaling group and trunk to Session Manager.		
7	Administer Communication Manager on System Manager.	Adding a Communication Manager server as a SIP Entity on page 32	
8	Add a non-IMS SIP signaling group and allow Incoming Dialog Loopbacks.	Adding a non-IMS SIP signaling group/allow Dialog Loopbacks on page 47	
9	Set up routing from trunk gateway to feature server.	Routing from trunk gateway to feature server on page 48	
10	Set up routing from feature server to trunk gateway.	Routing from feature server to trunk gateway on page 49	
11	Administer public numbering.	Administering public numbering on page 50	
12	Set up routing on System Manager	Administering routing for feature server and trunk gateway on System Manager on page 51	

Adding an IMS-enabled SIP signaling group

About this task

Set up a SIP signaling group with IMS enabled from the feature server Communication Manager PROCR to the Session Manager Security Module.

Procedure

1. Enter `add signaling-group` *`next`*.
2. Note the value of the signaling-group number.
3. Enter `sip` for the **Group Type**.
4. Set **IMS Enabled?** to `y`.
5. The **Transport Method** should be `tls`.
6. Set **Peer Detection Enabled?** to `y` if it is not already set to `y`.

   Selecting the value `y` for the field **Peer Detection Enabled** interchanges the message between Communication Manager and the connected SIP server. The value for **Peer server Type** will be changed to `SM` when the SIP signaling group is put into service.

7. Set **Near-end Node Name** to `procr`.
8. Set **Far-end Node Name** to the name of the Session Manager Security Module.
9. Set **Far-end Domain** to the same domain name that you entered as the **Authoritative Domain** on the **change ip-network-region** form (MyCompany.com)
10. Set **Enable Layer 3 Test?** to `y`.

    If this field is set to `n`, the links will not be monitored by Session Manager.
11. Submit the form.

Adding a non-IMS SIP signaling group/allow Dialog Loopbacks

Procedure

1. Enter `add signaling-group` *`next`*
2. For **Group Type**, enter `sip`.
3. For **Transport Method**, enter `tcp`.
4. Set **IMS Enabled?** to `n`.
5. Set **Near-end Node Name** to `CLAN`
6. Set **Far-end Node Name** to the name of the Session Manager SM100 board.
7. Set **Near-end Listen Port** to a different port than the one defined in the IMS signaling group, such as 5070.
8. Set **Far-end Listen Port** to be the same as the Near-end Listen Port.
9. Set **Far-end Domain** to the same domain name that you entered as the **Authoritative Domain** on the **change ip-network-region** form.
10. Set **Incoming Dialog Loopbacks** to `allow`
11. Set **Enable Layer 3 Test?** to `y`

    If this field is set to `n`, the links will not be monitored by Communication Manager.
12. Submit the screen.

Routing from trunk gateway to feature server

This section describes how to set up routing for an incoming trunk call to an IMS user. It is necessary to prepend digits to the IMS user extension to route the call via the non-IMS trunk to Session Manager. The prepended digits are deleted in the route pattern entry.

Procedure

1. ARS digit conversion:
   a. Enter `change ars digit-conversion x`.
   b. Under **Matching Pattern**, add an entry for the incoming trunk call number.
   c. Enter the **Min** and **Max** number of digits allowed.
   d. In the **Del** field, enter the number of digits to delete from the trunk call number.
   e. In the **Replacement String** field, enter the digits to prepend to the trunk call number (i.e., 99).
   f. In the **Net** field, enter `aar` .
   g. For **Conv** and **ANI Req**, enter n.
   h. Submit the form.
2. AAR analysis:
   a. Enter `change aar analysis x`.
   b. Add an entry for dialed digits **xxyy**, where **xx** are the digits you entered for the **Replacement String** on the ars form, and **yy** are the first two digits of an IMS user's extension.
   c. Enter the **Min** and **Max** number of digits allowed.
   d. Enter a route pattern number to a non-IMS trunk group for the **xxyy** dialed digits.
   e. For **Call Type**, enter `pubu`.
   f. For **ANI Req**, enter n.
   g. Submit the form.
3. Route pattern:
   a. Enter `change route-pattern x`, where x is the Route Pattern number you entered on the aar screen.
   b. For **Grp No**, enter the group number of the non-IMS trunk group.
   c. For **No. Del Dgts**, enter the number of digits to delete in the route to the non-IMS trunk.
   d. Submit the form.

Routing from feature server to trunk gateway

For calls from the feature server to the public network, routing is administered to:

- route the outgoing call from the feature server via the IMS trunk to Session Manager
- route the incoming call via the non-IMS trunk to the trunk gateway.

Procedure

1. ARS analysis:
   a. Enter `change ars analysis x`
   b. Enter the digits for the **Dialed String**.
   c. Enter the **Min** and **Max** number of digits allowed.
   d. Enter the **Route Pattern** value.
   e. In the **Call Type** field, enter `pubu`
   f. Submit the screen.
2. Route Pattern 1:
   a. Enter `change route–pattern 1`
   b. Delete the international dialing prefix by entering the appropriate value for the number of digits to delete in the **No. Del Dgts** field.

      For example, in the U.S., the prefix is 011. The number of digits to delete is 3.
   c. In the **Inserted Digits** field, enter **p** . This adds a “+” to the beginning of the number.
   d. Submit the screen.
3. Route Pattern 2:
   a. Enter `change route–pattern 2`
   b. Delete the national dialing prefix by entering the appropriate value in the **No. Del Dgts** field.

      For example, in Germany, the national prefix is 0, so the number of digits to delete is 1.
   c. In the **Inserted Digits** field, enter **p**## , where ## is your own country code.
   d. Submit the screen.
4. Route Pattern 3: This Route Pattern is only needed for countries where dialing of subscriber numbers (public numbers without the Country Code and National Destination Code/City Code) is allowed (for example, Germany):
   a. Enter `change route–pattern 3`
   b. In the **Inserted Digits** field, enter **p**### , **p**### is the combination of your own Country Code and your own National Destination Code (City Code), etc.
   c. Submit the screen.

5. On the trunk gateway side, administer the incoming call handling treatment for each non-IMS trunk to insert digits for the routing to the public trunk.
   a. Enter `change inc-call-handingling-trmt trunk-group x`, where `x` is the non-IMS trunk group number.
   b. Enter several ICHT entries with different lengths.

      Public numbers can be of different lengths and need to be handled accordingly.
   c. Submit the screen.

Administering public numbering

About this task

The following describes the handling for public numbering.

Call to Public Network:

(Endpoint > Communication Manager Feature Server > Session Manager > Communication Manager Trunk Gateway > Public Network)

Even if the Communication Manager Feature Server is administered for Private Enterprise Canonical Numbers, the PAI for a call to the public network can be changed to a Public Long Number by choosing a public call type in the respective Route Pattern (i.e., **pubu** for the Call Type on the ARS form).

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

Call from Public Network:

(Public Network > Communication Manager Trunk Gateway > Session Manager > Communication Manager Feature Server > Session Manager > Endpoint)

In Session Manager, all public numbers should be international with the leading “+”. Because there is no adaptation of national numbers received from the public network to international numbers on the SIP trunk, the adaptation must be made with the number adaptation module in Session Manager.

Administering routing for feature server and trunk gateway on System Manager

About this task

Although the two functionality is within one Communication Manager, the feature server and trunk gateway need to be configured as separate SIP entities and entity links using System Manager routing.

Procedure

1. Define the entity and entity link for feature server and trunk gateway as a TCP connection with the ports defined in the Communication Manager signaling groups (TCP port 5060 for feature server, TCP port 5070 for trunk gateway).
2. For the routing from Feature Server to Trunk Gateway, define a dial pattern and routing policy to route an incoming “+” to the trunk gateway. See the Routing Policy Details screen on System Manager.
3. To add the Communication Manager server SIP domains for routing, perform the following steps:
   a. Under **Elements**, select **Routing** > **Domains**.
   b. Click **New**.
   c. Enter the domain name for Communication Manager.
   d. In the **Type** field, select **cm** from the drop-down menu.
   e. Click **Commit**.
   f. Click **New**.
   g. In the **Name** field, enter the domain name for Session Manager.
   h. In the **Type** field, select **sip** from the drop-down menu.
   i. Click **Commit**.
4. To administer Communication Manager as a SIP entity, perform the following steps:
   a. Under **Elements**, select **Routing** > **SIP Entities**.
   b. Click **New**.
   c. In the **Name** field, enter the name of the Communication Manager.
   d. In the **FQDN or IP Address** field, enter the IP address for the processor Ethernet of Communication Manager.

      The IP address is the near-end in the signaling group to Session Manager.
   e. In the **Type** field, select **CM** from the drop-down menu.
   f. Click **Commit**.
5. To create an entity link from the Session Manager entity to the Communication Manager entity, perform the following steps:

a. Under **Elements**, select **Routing** > **Entity Links**.
b. Click **New**.
c. Enter a name to be associated with the Entity Link.
d. For **SIP Entity 1**, select the Session Manager entity from the drop-down menu.
e. In the **Port** field, enter the port.
f. For **SIP Entity 2**, select the new Communication Manager entity from the drop-down menu.
g. In the **Port** field, enter the port.
h. Click **Commit**.

6. To administer Communication Manager as an application, perform the following steps:

a. Under **Elements**, select **Inventory** > **Manage Elements**
b. Click **New**.
c. In the **Type** field, select **CM** from the drop-down menu.
d. In the **Application** section, enter the Name of the Communication Manager. The selected type becomes deactivated.

   To change the **Type**, click the **Reset** link.
e. In the **Node** field, enter the management IP address of the Communication Manager (IP address for SAT access).
f. In the **Attributes** section, enter the SSH SAT login and password in **Login** and **Password** fields respectively.
g. Select the **Is SSH Connection** check box.
h. In the port field, enter the value as **5022**.
i. Under **Attributes**, enter a login and a password for Communication Manager (SAT SSH login and password).
j. Click **Commit**.

   The Communication Manager entity will be automatically scheduled for an initial incremental hourly data synchronization.

Chapter 6: Survivable Remote Session Manager Documentation Roadmap

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

The following must be completed on the main Communication Manager and Session Manager servers and are not part of the roadmap:

- The main Communication Manager is installed, licensed, configured either as a feature server or evolution server, and is operational.
- The main Communication Manager is administered as a SIP entity on Session Manager.

Table 4: Survivable Remote Session Manager documentation roadmap

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

Task	Book to use	Notes
If installing the embedded survivable remote template, install the Avaya S8300D Server in the gateway.	• *Quick Start for Hardware Installation: Avaya G250 Branch Gateway*, 03-300433 • *Quick Start for Hardware Installation: Avaya G350 Branch Gateway*, 03-300148 • *Quick Start for Hardware Installation: Avaya G430 Branch Gateway*, 03-603236 • *Quick Start for Hardware Installation: Avaya G450 Branch Gateway*, 03-602053 • *Quick Start for Hardware Installation: Avaya G700 Branch Gateway*, 555-233-150	Refer to the book for your particular Gxxx Gateway.
Install System Platform on the server.	*Implementing Avaya Aura® Communication Manager*, 03-603558	
Install license and authentication files	*Implementing Avaya Aura® Communication Manager*, 03-603558	
Install the appropriate Communication Manager template using the System Platform Web Console.	*Implementing Avaya Aura® Communication Manager*, 03-603558	
Administer the Survivable Remote Session Manager Security Module IP address for System Platform > Network Configuration.	*Implementing Avaya Aura® Communication Manager*, 03-603558	The SIP signaling groups will have the far-end node names with the core Session Manager instance replaced by this Survivable Remote Session Manager Security Module IP address.
Administer the Survivable Remote Session Manager using System Manager.	*Implementing Avaya Aura® Session Manager*, 03-603473	See the section *"Survivable Remote Session Manager administration checklist"*.
Verify registration.	*Implementing Avaya Aura® Session Manager*, 03-603473	
Test the installation.	*Implementing Avaya Aura® Session Manager*, 03-603473	

Chapter 7: SIP Phone administration

Administering 96xx SIP telephones

About this task

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

Procedure

1. Go to the configuration menu:
   a. On the hard telephone: Press the **Mute** button on the telephone and use the keypad to enter **CRAFT#**
   b. On the soft telephone: Enter `admin options`
2. In the **SIP Global Settings** menu:
   a. Set the **SIP Domain** to the domain of your Session Manager environment.
   b. Set the **Avaya Environment** to `auto`.
   c. Set **Reg. Policy** to `simulateous`
   d. Leave the **Avaya Config Server:** setting blank.
3. In **SIP Proxy Settings** of the telephone configuration menu:
   a. For the **SIP Proxy Server**, enter the IP address of the Primary Session Manager that the telephone should register to, and if applicable, enter the Secondary Session Manager as the second entry.
   b. Set **Transport** to `TCP` or `TLS`
   c. Set the **SIP Port** as defined in the Session Manager SIP Entity (usually 5060 for TCP).
4. To access the correct file server:
   a. Navigate to **Admin Procedures**
   b. Select **SSON**
   c. Enter the SSON.

Chapter 8: Feature Name Extension Administration

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

Administering feature name extensions on SAT

Procedure

1. Enter `change feature-access-codes`.
2. Enter the appropriate codes for the features you want to enable.
3. Submit the form.
4. Enter `change off-pbx-telephone feature-name-extensions set 1`
5. Enter the number you want to use for a particular feature (xxx-xxxx).
6. Submit the form.

Administering feature name extensions on System Manager

Procedure

1. On the System Manager console, under **Elements** , select **Session Manager** > **Application Configuration** > **Implicit Users**.
2. Select **New**.
3. Enter a telephone number in the **Pattern** field (xxx-xxxx).
4. Enter the Minimum number of digits to be matched by the system in the **Min** field.

5. Enter the Maximum number of digits to be matched by the system in the **Max** field.
6. Enter a description in the **Description** field. For example, Turn on EC500.
7. Select the appropriate **SIP Domain** from the drop-down menu.
8. Select the appropriate originating feature server name from the **Origination Application Sequence** drop-down menu.
9. Select the appropriate terminating feature server name from the **Termination Application Sequence** drop-down menu.
10. Click **Commit**.

Appendix A: Numbering configuration

Numbering

An **Enterprise Canonical Number** (ECN) is a number that is unique to Session Manager. This number can be a Public long number, Private long number, or short (internal number).

A **Public Number** must begin with a **+** sign.

A **Private Alias** for public numbering is needed when phones are not able to register with the **+** sign (such as Avaya hard phones).

The **OPTIM Table** converts a registration number (may be an ECN) to a short number.

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

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

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

Numbering administration

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

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

Following fields are evaluated for the numbering adaptation:

- Trunk Group: page 3 - Numbering Format

- **public**: calling number adaptation with entry in the **public-unknown-numbering** table
- **unk-pvt**: calling number adaptation with entry in the **private-numbering** table

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

- AAR analysis: Page 1 - **Call type** for the dialed string:
  - **aar**: the called number is determined to be a public number. The calling number will be adapted to public as well.
  - **pubu**: the called number is determined to be a public number. The calling number will be adapted to public as well.
  - **unku**: the called number is determined to be a private number.

  The call type setting in AAR has a higher priority than the numbering format in the trunk group form. When the calling party number is adapted to public, there needs to be a matching entry in the **public-unknown-numbering** table.
- Route Pattern: Page 1- **Numbering Format** for trunk entry
  - **pub-unk**: the called number is determined to be a public number. The calling number will be adapted to public as well.
  - **unk-unk**: the called number is determined to be a private number.
  - Empty field: the numbering setting from AAR and the trunk group are used.

  The numbering format setting in the Route Pattern has a higher priority than the AAR call type. When the calling party number is adapted to public, there needs to be a matching entry in the **public-unknown-numbering** table.

The following table shows the administration settings for the different numbering types. The numbering type used for registration needs to be differentiated from the numbering type that is signalled to the network.

Table 5: Administration settings for different numbering types

Registration numbering type	Signalled numbering type	Administration
private short	private short	Private short numbering on page 61.
private long	private long	Private long numbering on page 62.
private long	public	Long private numbering and public signalling on page 64.
public (+)	public	Public numbering on page 66.

private short or long (variation 1)	call to public number	Call to public extension (variation 1) on page 67.
private short or long (variation 2)	call to public number	Call to public extension (variation 2) on page 69.

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

Recommendations

The following are administration recommendations:

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

Private short numbering

Private short numbering format uses the private extension.

In Session Manager, only the private short number is administered.

In Communication Manager, the described administration does not change this internal extension.

This configuration is for the following numbering types:

- Registration numbering type: private short
- Signalled numbering type: private short

SAT Form	Page	Field	Value	Comment
off-pbx-telephone station-mapping	1	Phone Number	Extension number	
	1	Trunk Selection	aar	For station types 90xxSIP, the trunk selection is set on the last page of the station form.

SAT Form	Page	Field	Value	Comment
trunk-group	3	Numbering Format	private	
aar analysis	1	Dialed String	Extension number	
private-numbering	1	Ext Code	Extension number or patter for extension numbers.	
	1	Trk Grp	Leave blank.	Empty field means it applies to all trunks.
	1	Private Prefix	Leave blank.	
	1	Total Len	Extension length.	
public-unknown-numbering				No entries on public numbering form.
route-pattern	1	Grp Num	Trunk group.	List trunk group(s) with trunks to primary Session Manager listed first.
	1	FRL	0	
	1	Numbering format	Leave blank.	
ICHT				No entries on ICHT form.

Private long numbering

This numbering format uses the private extension extended by a prefix.

In Session Manager, only the private long number is administered.

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

This configuration is for the following:

- Registration numbering type: private long
- Signalled numbering type: private long

SAT Form	Page	Field	Value	Comment
off-pbx-telephone station-mapping	1	Phone Number	Long private extension number	
	1	Trunk Selection	aar	For station types 90xxSIP, the trunk selection is set on the last page of the station form.
trunk-group	3	Numbering Format	private	
aar analysis	1	Dialed String	Long private extension number	Dialed String is the extension or a pattern of extensions.
	1	Route Pattern	Pattern to route to Session Manager.	
	1	Call Type	unku	
private-numbering	1	Ext Len	Extension length.	
	1	Ext Code	Extension number or patter for extension numbers.	
	1	Trk Grp	Leave blank.	Empty field means it applies to all trunks.
	1	Private Prefix	Private prefix.	
	1	Total Len	Extension length plus prefix	
public-unknown-numbering				No entries on public numbering form.
route-pattern	1	Grp Num	Trunk group.	List trunk group(s) with trunks to primary Session Manager listed first.
	1	FRL	0	
	1	Numbering format	Leave blank.	
Incoming Call Handling Treatment	1	Len	Length of private long number.	

SAT Form	Page	Field	Value	Comment
	1	Number Digits	Private prefix	
	1	Del	Length of private prefix	
	1	Insert	Leave blank.	

Long private numbering and public signalling

This numbering format uses the private extension extended by a prefix.

In Session Manager, the private long number as well as the public number is administered.

In Communication Manager, the described administration changes the private long number to the extension and the outgoing direction to the public number.

This configuration is for the following:

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

SAT Form	Page	Field	Value	Comment
off-pbx-telephone station-mapping	1	Phone Number	Long private extension number	
	1	Trunk Selection	aar	For station types 90xxSIP, the trunk selection is set on the last page of the station form.
trunk-group	3	Numbering Format	public	
aar analysis	1	Dialed String	Long private extension number	Dialed String is the extension or a pattern of extensions.
	1	Route Pattern	Pattern to route to Session Manager.	
	1	Call Type	unku	
private-numbering	1			No entry in private numbering.

SAT Form	Page	Field	Value	Comment
public-unknown-numbering	1	Ext Len	Extension length.	
	1	Ext Code	Extension number or patter for extension numbers.	
	1	Trk Grp	Trunk number or leave blank.	Empty field means it applies to all trunks.
	1	CPN Prefix	Public prefix to the extension without the “+”. The “+” will be added automatically.	
	1	Total Len	Extension length plus CPN prefix	
route-pattern	1	Grp Num	Trunk group.	List trunk group(s) with trunks to primary Session Manager listed first.
	1	FRL	0	
	1	Numbering format	unk-unk	
Incoming Call Handling Treatment	1	Len	Length of public long number.	
	1	Number Digits	Public prefix	
	1	Del	Length of public prefix	
	1	Insert	Leave 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	Leave blank.	

Public numbering

This numbering format can only be used from softphones because the “+” is needed as a login character.

For all other phones, the public numbering is realized with a private alias using the private long and public signalling configuration.

In Session Manager, only the public number is administered.

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

This configuration is for the following:

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

SAT Form	Page	Field	Value	Comment
off-pbx-telephone station-mapping	1	Phone Number	Public number without the leading “+”	
	1	Trunk Selection	aar	For station types 90xxSIP, the trunk selection is set on the last page of the station form.
trunk-group	3	Numbering Format	public	
aar analysis	1	Dialed String	Public number without the leading “+”	Dialed String is the extension or a pattern of extensions.
	1	Route Pattern	Pattern to route to Session Manager.	
	1	Call Type	pubu	
private-numbering				No entry in private numbering.
public-unknown-numbering	1	Ext Len	Extension length.	
	1	Ext Code	Extension number or patter for	

SAT Form	Page	Field	Value	Comment
			extension numbers.	
	1	Trk Grp	Trunk number or leave blank.	Empty field means it applies to all trunks.
	1	CPN Prefix	Public prefix to the extension without the “+”. The “+” will be added automatically.	
	1	Total Len	Extension length plus CPN prefix	
route-pattern	1	Grp Num	Trunk group.	List trunk group(s) with trunks to primary Session Manager listed first.
	1	FRL	0	
	1	Numbering format	unk-unk	
Incoming Call Handling Treatment	1	Len	Length of public long number.	
	1	Number Digits	Public prefix	
	1	Del	Length of public prefix	
	1	Insert	Leave blank.	

Call to public extension (variation 1)

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

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

The administration for this version requires the public number of a user to be administered as a second handle in Session Manager (Secondary Session Manager).

This configuration is for the following:

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

SAT Form	Page	Field	Value	Comment
trunk-group	3	Numbering Format	private	
aar analysis	1	Dialed String	Private long or short number	Dialed String is the extension or a pattern of extensions.
	1	Route Pattern	Pattern to route to Session Manager.	
	1	Call Type	unku	
private-numbering	1	Ext Code	Extension number or pattern for extension numbers.	
	1	Trk Grp	Leave blank.	Empty field means it applies to all trunks.
	1	Private Prefix	Leave blank.	
	1	Total Len	Extension length.	
public-unknown-numbering	1	Ext Len	Extension length.	
	1	Ext Code	Extension number or patter for extension numbers.	
	1	Trk Grp	Trunk number or leave blank.	Empty field means it applies to all trunks.
	1	CPN Prefix	Public prefix to the extension without the “+”. The “+” will be added automatically.	
	1	Total Len	Extension length plus CPN prefix	

SAT Form	Page	Field	Value	Comment
route-pattern	1	Grp Num	Trunk group.	List trunk group(s) with trunks to primary Session Manager listed first.
	1	FRL	0	
	1	Numbering format	pub-unk	
Incoming Call Handling Treatment				No entries on ICHT form.

Call to public extension (variation 2)

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

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

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

This configuration is for the following:

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

SAT Form	Page	Field	Value	Comment
trunk-group	3	Numbering Format	private	
aar analysis	1	Dialed String	Private long or short number	Dialed String is the extension or a pattern of extensions.
	1	Route Pattern	Pattern to route to Session Manager.	
	1	Call Type	unku	
private-numbering	1	Ext Code	Extension number or pattern for extension numbers.	

SAT Form	Page	Field	Value	Comment
	1	Trk Grp	Leave blank.	Empty field means it applies to all trunks.
	1	Private Prefix	Leave blank.	
	1	Total Len	Extension length.	
public-unknown-numbering				No public numbering administration. The adaptation to public is done in Session Manager.
route-pattern	1	Grp Num	Trunk group.	List trunk group(s) with trunks to primary Session Manager listed first.
	1	FRL	0	
	1	Numbering Format	unk-unk	
Incoming Call Handling Treatment				No entries on ICHT form.

Index

Numerics

96xx SIP telephone administration 55

A

aar 42
AAR administration 25
add survivable-processor 27
add trunk-group 22
adding a node name 20
adding SIP signaling group 21
adding users 36
administration, ARS 25
administration, evolution server 16
administration, feature server 16
application sequence administration 35
application sequencing 15
ARS Analysis administration 25
Avaya Mentor videos 8

C

change dialplan analysis 19
checking connections 34
combination feature server and trunk gateway 13
Communication Manager evolution server 12
Communication Manager feature server 11
Communication Manager server application administration 35
configuring evolution server 15
configuring feature server 15

D

dialog loopbacks 47
document changes 8
document purpose 7

E

Enterprise Canonical Number 59
entity link administration 33
Evolution server 12
evolution server administration 16, 45
evolution server configuration 15

F

fac 19
feature access code 19
feature access codes 57
feature name extension administration 57
Feature Name Extension administration 57
feature server 11
feature server administration 16
feature server configuration 15
feature server/trunk gateway administration 45, 51
feature-name-extensions 57
FNE administration on System Manager 57
full-call model 13

G

Gateway recovery rule 29

H

half call model 12

I

ICHT administration 26
IMS-enabled SIP signaling group 46
incoming call handling treatment 26
IP network region 20
ip-network-region 20

L

legal notice 2

M

managed element administration 30
minimum time for network stability 29

N

network stability minimum time 29
New SIP user verification 39

node-name 20
non-IMS signaling group administration 42
non-IMS SIP signaling group 47
numbering 59
numbering administration 59

P

privileged administrator, adding 30
proxy route administration 26
public numbering administration 50
public unknown numbering administration 27
purpose of document 7

R

recovery rule validation 29
related documentation 8
related resources 8
Avaya Mentor videos 8
route pattern 23
route pattern administration 23
routing from feature server to trunk gateway 49
routing from trunk gateway to feature server 48

S

SIP Entity administration 32
SIP phone administration 55
SIP telephone administration, 96xx 55
support 9
contact 9
survivable remote documentation 53
survivable remote SIP Entity administration 33
synchronizing data 31
System Manager, feature server/trunk gateway administration 51

T

trunk gateway 13
trunk gateway administration 41
trunk gateway dial plan 42

U

uniform dial plan administration 24
users, adding 36

V

videos 8
Avaya Mentor 8

W

Warranty 9