Administering Avaya Aura® Communication Manager Server Options

03-603479
Release 6.0.1
Issue 2.2
April 2011

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.

For full hardware support, please see the document, *Avaya Support Notices for Hardware Documentation*, document number 03–600759 on the Avaya support web site, http://www.avaya.com/support.

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 Web sites 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 Web site: 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.

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 End User a license within the scope of the license types described below. 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 End User. “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. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

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

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Downloading Documentation

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

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: Overview

Purpose of this document

The purpose of this document is to provide administration information, procedures, and references for the Avaya Partners and customer administrators who will configure an Avaya Aura® Communication Manager as a feature server or evolution server.

Overview

Avaya Aura® Communication Manager 6.0.1 may be configured as a:

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

feature server or as an evolution server.

Avaya 96XX IP telephones which are configured as SIP stations utilize the Avaya Aura® Session Manager User Registration feature and require a Communication Manager configured as either a feature server or evolution server.

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

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

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

Avaya Aura® System Manager Release 6.1 and Avaya Aura® Session Manager Release 6.1 support Communication Manager Release 6.0.1.

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 that allows 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. Routing of such calls directly to ISDN trunks is not supported.
- Traditional phones such as DCP, H.323, ISDN, and analog are not supported.
- 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 may 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. It provides Communication Manager features to both SIP and non-SIP endpoints. It 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 a evolution server by disabling IMS on the signaling group to Session Manager. Session Manager handles call routing for SIP endpoints

and allows them 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

G430 and G450 gateways provide connection preserving failover and failback to Survivable Core and Survivable Remote processors. Communication Manager as an evolution server can support G650 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. Traditional Communication Manager adheres to the full call model.

Application sequencing has significant limitations when at least one of the servers in a sequence adheres to the full call model. When Communication Manager is administered as an evolution server, Communication Manager is the only supported application.

For the full call model, the IMS-enabled field on the SIP signaling group form must be 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 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. Only IMS to IMS and non-IMS to non-IMS traffic is allowed.

Two SIP signaling groups need to be created from Communication Manager to Session Manager. One is a 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 2: 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.

Assumptions

It is assumed that:

- Communication Manager is already installed on System Platform and has basic administration.
- The appropriate patches have been installed, if applicable.
- The Communication Manager license has been loaded using the System Platform web console's **Server Management** > **License Management** > **WebLM** using the MAC address of the Communication Manager feature/evolution server.
- The Communication Manager Authentication file has been loaded using the System Platform web console's **User Administration** > **Authentication File** upload tool.
- System Manager and Session Manager are already active in an existing SIP routing deployment.

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/from Avaya Aura®. 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/ARS to reach extensions assigned to another Communication Manager.

Feature Server/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 SAT screens, then administered using System Manager.

Prerequisites:

- Session Manager has been installed and administered.
- The appropriate service packs have been installed, if applicable.
- Communication Manager has been installed with a license and has basic administration.

#	Action	Link	✔
1	Log in to the main Communication Manager server.		
2	Change the dial plan analysis.	Changing dialplan analysis on page 15	

#	Action	Link	✔
3	Add the feature access codes for AAR and ARS.	Changing feature access codes on page 15	
4	Add the appropriate SIP domain in the Network Region that will be used.	Changing an IP network region on page 16	
5	Administer a node name for the IP address of the Session Manager Security Module.	Adding a node name on page 16	
6	Administer a SIP signaling group.	Adding a SIP signaling group on page 16	
7	Add trunk groups for each Session Manager.	Adding a SIP trunk group on page 17	
8	Configure the appropriate Route Patterns.	Administering a Route Pattern on page 18	
9	Administer the Uniform Dial Plan for non-SIP calls.	Changing the Uniform Dial Plan on page 19	
10	Administer AAR analysis.	Administering AAR on page 20	
11	Administer ARS Analysis for non-SIP calls.	Administering ARS Analysis on page 20	
12	Add the appropriate Route Pattern as the Proxy Route.	Administering the Proxy Route on page 21	
13	Administer incoming call handling treatment.	Administering Incoming Call Handling Treatment on page 21	
14	Add a Survivable Remote server, if applicable.	Adding a Survivable Remote Server on page 22	
15	Change public unknown numbering so that the caller-id will appear as E.164.	Administering Public Unknown Numbering on page 22	
16	If applicable, validate the minimum time of network stability for media gateways to failback to the main Communication Manager when it becomes available.	Validating Minimum time of network stability on page 23	
17	If applicable, validate the media gateway recovery rule.	Validating media gateway recovery rule on page 23	
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 23	

#	Action	Link	✔
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 24	
22	Synchronize Communication Manager data.	Synchronizing Communication Manager data on page 25	
23	Add the Communication Manager feature/evolution server as a SIP Entity.	Adding a Communication Manager server as a SIP Entity on page 25	
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 26	
25	Create Entity Links between Session Manager and Communication Manager.	Creating Entity Links on page 26	
26	Verify the connections between Communication Manager and Session Manager.	Checking the connections on page 27	
27	Administer the Communication Manager server as an application.	Administering the Communication Manager server as an application on page 28	
28	Administer the Communication Manager server in an Application Sequence.	Administering Communication Manager in an application sequence on page 28	
29	Add users.	Adding users on page 29	
30	Verify users.	Verifying a new SIP user on page 32	
31	Test Session Manager and Main Communication Manager feature/ evolution server calls.	Testing Session Manager and Communication Manager calls on page 32	

SAT Administration Commands

Changing dialplan analysis

1. On Communication Manager, enter the SAT command **change dialplan analysis**
2. Enter the appropriate dial plan digits as required. The following is an example:

Dialed String	Total Length	Call Type	Reason
9	1	Feature Access Code (fac)	ARS/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

Changing feature access codes

Add the feature access codes for Automatic Alternate Routing (AAR) and Automatic Route Selection (ARS).

1. Enter **change feature-access-codes**
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.

Changing an IP network region

Administer the IP network region that will be referred to in the SIP signaling group to Session Manager (defined later).

1. Enter **change ip-network-region *x*** where *x* is an IP network region number.
2. In the **Authoritative Domain** field, enter the appropriate SIP domain name that will be used (i.e., MyCompany.com).
3. In the **Name** field, enter a descriptive name (for example, Main_SM_NR).
4. Submit the form.

Adding a node name

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.

1. Enter **change node-names ip**
2. In the **Name** field, enter the name associated with the IP address of the Session Manager Security Module (i.e., SM1HostName).
3. In the **IP Address** field, enter the IP address of the Session Manager Security Module.
4. Submit the form.

Adding a SIP signaling group

Add a SIP signaling group for each Session Manager Security Module in the system configuration. The **IMS Enabled?** field on this form determines whether the Communication Manager server operates as a feature server or evolution server.

1. Enter **add signaling-group *next***
2. Note the value of the **Group Number**.

3. The **Group Type** should be `sip`. If it is not, in the **Group Type** field, select `sip` from the drop-down menu and right-click to display the associated fields on the screen.
4. For the **IMS Enabled?** field:
   a. If you are configuring Communication Manager as a feature server, set the **IMS Enabled?** field to `y`. Setting this field to `y` only applies when Communication Manager is being configured as a feature server.
   b. If you are configuring Communication Manager as an evolution server, leave the **IMS Enabled?** field set to `n`.
5. Set the **Transport Method** to `tls` if it is not already set to `tls`.
6. Set **Peer Detection Enabled?** to `y` if it is not already set to `y`.

   Selecting **Peer Detection Enabled = y** causes a message interchange between Communication Manager and the connected SIP server. The value for **Peer Server** will be changed to `SM` when the SIP signaling group is put into service.
7. Set the **Near-end Node Name** to `procr`
8. Set the **Far-end Node Name** to the name of the Session Manager Security Module.
9. Set the **Far-end Network Region** to the same Network Region number that you used on the **change ip-network-region**
10. Set the **Far-end Domain** to the SIP domain being used in Session Manager.
11. Set **Enable Layer 3 Test?** to `y`. This field appears when the Far-end Node Name has been entered.

    Important:

    If this field is set to `n`, the links will not be monitored by Communication Manager. This test is required for trunks connected to Session Manager. Maintenance software will take the trunks out of service if this test is not enabled.
12. Set **Initial IP-IP Direct Media** to `y`.
13. If you are configuring the Communication Manager as a Evolution Server, set **H.323 Station Outgoing Direct Media** to `y`.
14. Submit the form.

Adding a SIP trunk group

Add a SIP trunk group to the SIP signaling group 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 will get ARS calls.
- Use **private** numbering for a trunk that will get SIP calls.

1. Enter **add trunk-group *next***
2. For the **Group Type**, enter `sip`.
3. For the **Group Name**, enter the name of the Session Manager Security Module.
4. Add a **TAC** per the dac added in the dial plan analysis table (i.e., *110).
5. The **Direction** should be `two-way`
6. The **Service Type** should be `tie`
7. For **Signaling Group**, enter the SIP signaling group number that you added earlier.
8. In the **Number of Members** field, enter the number of trunk group members that will be needed 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.

Administering a Route Pattern

Non-enterprise number route patterns are used for calls going to non-SIP phones. 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 strictly for SIP phones. 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 will allow calls to fail over to multiple trunk groups in the event of a trunk failure.

1. For non-enterprise number routing:
   a. Enter **change route-pattern *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 (+) will be prepended to the digits.

f. Submit the form.

2. For enterprise number routing:

a. Enter **change route-pattern *x*** where *x* is the number of the 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.

Changing the Uniform Dial Plan

Add entries in the Uniform Dial Plan to prepare digits to be routed via the AAR table.

In the following example, 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 via AAR. In this example, the inserted digit string is **120983.** This example is for non-enterprise station calls.

1. Enter **change uniform-dialplan *x*** where *x* is the number of the dial plan.
2. Enter the date in the table. The information below is an example.
3. When finished, submit the form.

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

Administering AAR

Automatic Alternate Routing (AAR) routes calls within a company over the company's private network.

Add appropriate entries for SIP station and non-SIP station calls.

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 the SAT, enter **change aar analysis *x*** where *x* is an AAR table number. In this example, use 0.
2. Enter information in the AAR table (use the information below as an example), then submit the form.

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

Administering ARS Analysis

Administer ARS Analysis for non-enterprise calls to send the appropriate 9+11-digit calls.

1. Enter **change ars analysis *x*** where *x* is the number of the ARS Anaylsis table.
2. Enter data in the table. The following is an example.
3. When finished, submit the form.

Dialed String	Total Min	Total Max	Route Pattern	Call Type	ANI Reqd
1	11	11	10	natl	n
101xxxx0	8	8	deny	op	n
101xxxx0	18	18	deny	op	n
101xxxx01	16	24	deny	iop	n
101xxxx011	17	25	deny	intl	n
101xxxx1	18	18	deny	fnpa	n
10xxx0	6	6	deny	op	n

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

Administering the Proxy Route

Add the appropriate Route Pattern as the Proxy Route.

1. On the SAT, enter **change locations**
2. In the **Name** field, enter a Name (i.e., Main).
3. In the **Proxy Sel Rte Pat** field, enter the appropriate Route Pattern number.
4. Submit the form.

Administering Incoming Call Handling Treatment

Use Incoming Call Handling Treatment to strip down any SIP station calls that are sent to the Communication Manager feature/evolution server as a 12-digit number. Delete the number of digits necessary to match the SIP extension length in the Communication Manager feature/evolution server.

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

Be sure to do this for any trunk group going to Session Manager from the Communication Manager feature/evolution server.

1. On the 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.

Adding a Survivable Remote Server

1. On the SAT, enter **add survivable-processor *node-name*** where *node-name* is the name of the remote server (for example, lsp6) that was added on the **change node-name ip** form.
2. The **Type** field should be **lsp**. If you have an LSP/Survivable Remote server, do this for each survivable remote server.
3. The **Cluster ID/MID** matches the MID number used in the web interface of the Survivable Remote server under **Server Maintenance** > **Server Configuration** > **Server Role**
4. Submit the form.

Administering Public Unknown Numbering

Add the appropriate information so that the caller-id (P-Asserted-Identity SIP Header) will appear as E.164.

The **CPN Prefix** field contains the digits that will be inserted at the beginning of the digit string to form an 11-digit number. Because the public unknown table is being used, Communication Manager will automatically insert a plus (+).

1. On the SAT, enter **change public-unknown-numbering 0**
2. In the **Ext Len** field, enter the number of digits in the SIP extensions.
3. In the **Ext Code** field, enter the starting digit of the SIP extensions.
4. In the **CPN Prefix** field, enter the digits that will be inserted at the beginning of the digit string to form an 11–digit number.
5. In the **Total CPN Len** field, enter the total number of digits to be sent.
6. Submit the form.

Validating Minimum time of network stability

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

1. On the 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 media gateway recovery rule

Validate that the correct recovery rule number is specified for each Media Gateway in the **Recovery Rule** field.

The acceptable values for the **Recovery Rule** are (none) or a value between 1-250, where 250 is the maximum number of supported media gateways on any platform. **(none)** indicates that no automatic fallback registrations are accepted. The value of 1-250 applies the specific recovery rule to that gateway. A single rule may be applied to all Media Gateways , or each Media Gateway may have its own rule and any permutation in between.

The recovery rules are administered on the **system-parameters mg-recovery-rule** form.

1. On the SAT, enter **change media-gateway *x*** where *x* is the number of the media gateway.
2. In the **Recovery Rule** field, verify the number of the recovery rule associated with this media gateway.
3. Cancel or submit the form if a change was made.

Adding a privileged administrator

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

1. Log in to the the Communication Manager server System Management Interface (SMI).
2. Select **Security** > **Administrator Accounts** from the menu on the left.
3. Enter a **Login Name**.
4. Enter a **password** in the password field.
5. Re-enter the password in the **Re-enter password** field.
6. Click on the **No** button for **Force password/key change on next login.**
7. Click **Submit**

System Manager Administration

Creating a Communication Manager managed element

This information will be used by System Manager to synchronize with the Communication Manager feature or evolution server and enable the ability to add SIP stations to the Communication Manager server from System Manager.

1. Using 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:
   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:
   a. Enter the SSH SAT login and password (the login and password you created earlier for privileged administrator).

   Note:

   Services logins MUST NOT be used (e.g., craft, dadmin, inads, etc.) 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.

   b. Make sure the **Is SSH Connection** box is checked.

   c. Make sure the port is **5022**

6. Click **Commit**.

Synchronizing Communication Manager data

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

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. Check the 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 on **Now**
   e. The synchronization process may take several minutes. At the top of the table, click on **Refresh** to show the current synchronization status. The **Sync Status** will display **Completed** when synchronization is finished.

Adding a Communication Manager server as a SIP Entity

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.

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 menu.
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 on **Commit** when finished.

Adding a survivable remote server as a SIP Entity

The **Outbound Proxy** field provides a default SIP entity to route to if no routing policies are found for an incoming request. The outbound proxy is usually another routing element that may contain routing rules for the incoming request that Session Manager does not.

1. Using the System Manager web interface, under **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. In the **Outbound Proxy** field, select an outbound proxy from the drop-down menu.
6. Click **Commit**

Creating Entity Links

Entity links need to be created between the following when applicable:

- Each Session Manager server and the Communication Manager feature/evolution server
- The Survivable Remote Session Manager server and the Communication Manager feature/evolution server

If separate entities and entity links have been configured in the core for the feature server (feature server/IMS) link and the trunk gateway (trunk gateway/non-IMS) link, then an entity link should be configured from the survivable remote server to each of those entities for a total of 2 entity links on the survivable remote server. If only one entity/entity link is being used (as

in an evolution server configuration), then only one link will be administered on the survivable remote server.

The protocol(s) and transport(s) used should be exactly the same as those used between the primary Session Manager and the core Communication Manager entity (or entities).

1. On the System Manager console, under **Elements**, select **Routing** > **Entity Links**
2. Click on **New**
3. In the **Name** field, enter a descriptive Entity Link name (i.e., SM1 to CM-FS1).
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 should be linked to.
5. The **Protocol** should be `tls`.
6. The **Port** should be `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 should be linked to.
8. The **Port** should be `5061`.
9. The **Trusted** box *must* be checked.
10. The **Notes** field is optional.
11. Click on **Commit**.

Checking the connections

1. On Communication Manager:
   a. Enter the command **list history**
   b. Verify that Session Manager has logged in.
   c. Verify that initial data synchronization has begun.
2. Check the Communication Manager SIP Entity Link status:
   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 the **Link Status** is `Up` for the Communication Manager server.

3. Check the Session Manager Dashboard:
   a. On System Manager, under **Elements** , select **Session Manager**
   b. Verify that the Session Manager is active.

Administering the Communication Manager server as an application

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

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. Enter a description if desired.
7. Leave the **Application Handle** and **URI Parameters** fields blank.
8. Click **Commit**

Administering Communication Manager in an application sequence

Create an application sequence for the Communication Manager server application.

Important:

If the Communication Manager has been configured as an evolution server, the 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.

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.
5. When the screen refreshes, make sure the **Mandatory** box is checked.
6. Click **Commit**

Adding users

Any input fields not mentioned in the following steps can be ignored. There are a number of fields which are not used for Session Manager user administration.

A user may have more than one Communication Profile. For more information regarding the fields, see the on-line help.

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

- The first trunk is associated with the primary Session Manager.
- The second trunk is associated with the secondary Session Manager.
- There also needs to be a second signaling group to the secondary Session Manager.

1. On the System Manager console, under **Users** , select **User Management** > **Manage Users**
2. Click on the **New** button.
3. In the **Identity** section:
   a. Enter the user's **Last Name**
   b. Enter the user's **First Name**
   c. The **Description** field is optional for user information.
   d. Enter a web **Login** name in the form of **name@domain.com** using the appropriate SIP domain in Session Manager.
   e. The **Authentication Type** should be `Basic`
   f. Enter a **Login Password**. The password must start with an alpha (lower or upper case) character.

g. Confirm the password.

h. Enter the **Localized Display Name** of the user. This is the name that is displayed to the calling party.

i. In the **Endpoint Display Name** field, enter the full text name of the user.

j. Select a **Language Preference** from the drop-down menu.

k. Select a **Time Zone** from the drop-down menu.

4. Select the **Communication Profile** tab at the top of the screen.
5. Enter a **Communication Profile Password**.

   This field *must* be administered. The password must be all numeric characters. This is the password that is used when logging in to the phone. Remember this password as it will be used later for the Endpoint Profile Security code.
6. Confirm the **Communication Profile Password**.
7. In the **Communication Address** section:

   a. Click on **New**

   b. Select **Avaya SIP** from the drop-down menu in the **Type** field if it is not set already.

   c. In the **Fully Qualified Address** field, enter the full extension number of the SIP phone.

   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. In the **Type** field, select **Avaya E.164** from the drop-down menu.

   i. The **Fully Qualified Address** (handle) depends on the numbering format. If you use private numbering, the private handle also needs to be administered.

   j. Select the appropriate domain from the drop-down menu following the **@** sign.

   k. Click on the **Add** button.
8. Click on 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.

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. Leave the box for **Use Existing Stations** unchecked.

    e. Enter the extension that is administered on Communication Manager for the existing or new station in the **Extension** field.

    f. 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).

    g. The **Security Code** field can be left blank. The Security Code is not used to log in to the phone.

    h. Enter `IP` in the **Port** field.

    i. Check the box for **Delete Endpoint on Unassign of Endpoint from User**.

13. Click **Commit**. System Manager will log into Communication Manager and add this station.

Verifying a new SIP user

1. Login to the SIP phone 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 on **Show** in the row containing the Address/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 phone extension of the user.
   b. Verify that the phone type is **SIP**.
   c. Go to Page 6 of the station form.
   d. Verify that **SIP Trunk** is **aar**.
4. Check the off-pbx-telephone 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

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 phone on another PBX on Session Manager to validate routing.
4. Place 9+11-digit calls to a non-SIP phone on another PBX on Session Manager to validate routing.

Chapter 3: 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 16	
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 16	
4	Administer a non-IMS SIP signaling group.	Adding a non-IMS SIP signaling group on page 34	
5	Administer a SIP trunk group to the SIP signaling group.	Adding a SIP trunk group on page 17	
6	Administer the dial plan.	Changing dialplan analysis (trunk gateway) on page 34	
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 25	
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

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`

1. Enter `add signaling-group` *next*
2. Enter `sip` for the **Group Type**.
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`, the links will not be monitored by Communication Manager.
9. Submit the screen.

Changing dialplan analysis (trunk gateway)

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

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 4: Communication Manager as feature server/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/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 16	
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 16	
4	Set up a SIP signaling group with IMS enabled.	Adding an IMS-enabled SIP signaling group on page 38	
5	Add a SIP trunk group to the SIP signaling group.	Adding a SIP trunk group on page 17	
6	Administer the dial plan to route the Communication Manager external numbers via AAR to the non-IMS		

#	Administration Action	Link to action	✔
	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 25	
8	Add a non-IMS SIP signaling group and allow Incoming Dialog Loopbacks.	Adding a non-IMS SIP signaling group on page 44	
9	Set up routing from trunk gateway to feature server.	Routing from trunk gateway to feature server on page 39	
10	Set up routing from feature server to trunk gateway.	Routing from feature server to trunk gateway on page 40	
11	Administer public numbering.	Administering public numbering on page 41	
12	Set up routing on System Manager	Administering routing for feature server/trunk gateway on System Manager on page 42	

Adding an IMS-enabled SIP signaling group

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

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 **Peer Detection Enabled = y** causes a message interchange 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 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 in order to route the call via the non-IMS trunk to Session Manager. The prepended digits are deleted in the route pattern entry.

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 screen.
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 screen.

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 screen.

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.

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

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/trunk gateway on System Manager

Prerequisites

It is assumed that Session Manager is already installed and functioning.

Although the two functionalities are 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.

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. Add the Communication Manager server SIP domains for Routing:
   a. Under **Elements**, select **Routing** > **Domains**
   b. Click **New**
   c. Enter the domain name for the Communication Manager.
   d. In the **Type** field, select **cm** from the drop-down menu.
   e. Click **Commit**
   f. Click **New**
   g. Enter the domain name for the Session Manager.
   h. In the **Type** field, select **sip** from the drop-down menu.

i. Click **Commit**

4. Administer the Communication Manager as a SIP entity:
   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 the 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. Create an entity link from the Session Manager entity to the Communication Manager entity:
   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. For **SIP Entity 2**, select the new Communication Manager entity from the drop-down menu.
   f. Click **Commit**
6. Administer Communication Manager as an application:
   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.
   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.
   g. Make sure the **Is SSH Connection** box is checked.
   h. Make sure the port is **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.

Adding a non-IMS SIP signaling group

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.

Chapter 5: 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 are assumed to have been 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 1: Survivable Remote Session Manager documentation roadmap

Task	Book to use	Notes
Administer survivability options on the main Communication Manager server.	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558	
Administer the Survivable Communication Manager using System Manager.	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558	
Administer the Survivable Remote Session Manager server on the main Communication Manager server.	*Installing and Configuring 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.

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 Media Gateway*, 03-300433 • *Quick Start for Hardware Installation: Avaya G350 Media Gateway*, 03-300148 • *Quick Start for Hardware Installation: Avaya G430 Media Gateway*, 03-603236 • *Quick Start for Hardware Installation: Avaya G450 Media Gateway*, 03-602053 • *Quick Start for Hardware Installation: Avaya G700 Media Gateway*, 555-233-150	Refer to the book for your particular Gxxx media gateway.
Install System Platform on the server.	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558	
Install license and authentication files	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558	
Install the appropriate Communication Manager template using the System Platform Web Console.	*Installing and Configuring Avaya Aura™ Communication Manager*, 03-603558	
Administer the Survivable Remote Session Manager Security Module IP address for System Platform > Network Configuration.	*Installing and Configuring 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.	*Installing and Configuring Avaya Aura® Session Manager*, 03-603473	See the section *"Survivable Remote Session Manager administration checklist"*.
Verify registration.	*Installing and Configuring Avaya Aura® Session Manager*, 03-603473	
Test the installation.	*Installing and Configuring Avaya Aura® Session Manager*, 03-603473	

Chapter 6: SIP Phone administration

Administering 96xx SIP phones

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

1. Go to the configuration menu:
   a. On the hard phone: Press the **Mute** button on the phone and use the keypad to enter **CRAFT#**
   b. On the soft phone: 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 phone configuration menu:
   a. For the **SIP Proxy Server**, enter the IP address of the Primary Session Manager that the phone 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 7: 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 the SAT

1. Enter `change feature-access-codes`
2. Enter the appropriate codes for the features you want to enable.
3. Submit the screen.
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 screen.

Administering Feature Name Extensions on System Manager

1. On the System Manager console, under **Elements** , select **Session Manager** > **Application Configuration** > **Implicit Users**
2. Select **New**
3. Enter a phone 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/Request-URI **and** calling party/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/Request-URI **and** calling party/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/private long number to a short number (called party/Request-URI **and** calling party/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, 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.

The fields that are evaluated for the numbering adaptation are:

- 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.

Registration numbering type	Signalled numbering type	Administration
private short	private short	Private short numbering on page 53
private long	private long	Private long numbering on page 54
private long	public	Long private numbering and public signalling on page 56
public (+)	public	Public numbering on page 58
private short or long (variation 1)	call to public number	Call to public extension (variation 1) on page 59

private short or long (variation 2)	call to public number	Call to public extension (variation 2) on page 61

The settings in the different routing/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/from Avaya Aura®. 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/ARS to reach extensions assigned to another Communication Manager.

Private short numbering

This 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:

- 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 (e.g., 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 (e.g., 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