



Avaya Aura™ Session Manager Case Studies

Issue 3
03-603478
Release 6.0
June 2010

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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(s) 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 this product. 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://www.avaya.com/support>. Please note that if you acquired the product 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/](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, AND 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(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. 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://www.avaya.com/support/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 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://www.avaya.com/support/>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, Avaya Aura™ System Manager, and Avaya Aura™ Session Manager are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: <http://www.avaya.com/support>

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://www.avaya.com/support>

Contents

Chapter 1: Overview.....	7
Chapter 2: A Network Case Study.....	9
Overview.....	9
The network.....	9
Core provisioning.....	11
Domains.....	11
SIP entities for Session Managers.....	12
SIP entity for Westminster Session Manager.....	12
SIP entity for NJ Session Manager.....	13
Locations.....	15
Locations with managed bandwidth.....	15
Locations without managed bandwidth.....	16
Time ranges.....	17
Non-Session Manager SIP entities.....	17
Harmonizing disparate PBXs.....	18
Adaptations for PBXs.....	19
SIP entities for PBXs.....	24
SIP service providers.....	30
SIP service provider adaptations.....	30
AT&T adaptation.....	30
Verizon adaptation.....	31
Hypothetical adaptation.....	32
SIP entities for SIP service providers.....	33
Single SIP entity behind SBC.....	34
Multiple SIP entities behind SBC.....	35
Routing policies for SIP service providers.....	36
Simple routing policy for routing policies for SIP service providers.....	37
Alternative routing policy for routing policies for SIP service providers.....	38
Dial patterns for SIP service providers.....	39
Simple routing policy for dial patterns for SIP service providers example.....	40
Alternative routing policy for dial patterns for SIP service providers.....	41
Tail-end hop-off.....	42
SIP foundation servers.....	45
Modular Messaging.....	45
Voice Portal-like SIP application service.....	48
Chapter 3: A New User Setup Case Study.....	53
Overview.....	53
Synchronize Communication Manager station data to the System Manager.....	53
Adding a SIP entity for the Session Manager.....	56
Adding the Session Manager Instance.....	57
Adding Domains.....	58
Adding Application Sequences.....	58
Adding a Home Location.....	58
Adding the Survivability Server.....	59
Adding a User (SIP end-point).....	60
General section.....	61

Identity section.....	61
Address section.....	62
Communication Profile section.....	62
Session Manager section.....	64
Endpoint Profile section (CM Station association).....	65
For a new station.....	66
Default Contact List.....	66
Chapter 4: A Call Handling Case Study.....	67
Overview.....	67
Scenario Definition.....	67
Using Application Sequence.....	69
Adding an Application (e.g. CM Feature Server).....	69
Creating an Application Sequence from Existing Applications.....	71
Administering Implicit Users.....	72
Index.....	75

Chapter 1: Overview

This document explains different scenarios about the functionality of Avaya Aura™ Session Manager which provide a practical understanding on administering and configuring Session Manager. This should be read in conjunction with the book *Administering Avaya Aura™ Session Manager, 03-603324*. The book covers the following case studies:

1. A Network Case Study
2. A New User Setup Case Study
3. A Call Handling Case Study

Refer to the book *Administering Avaya Aura™ Communication Manager Server Options, 03-603479* for understanding different Communication Manager Server roles in the Session Manager environment.

Intended Audience

This book is meant for all those who are involved in either understanding, administering and troubleshooting Session Manager.

Chapter 2: A Network Case Study

Overview

The following case study describes a network which uses Session Manager to provide the following solutions:

- Harmonizing disparate PBXs, both extension lengths and brands
- VoIP connections to SIP service providers (access to the public switched telephone network [PSTN] via SIP signaling)
- Tail-end hop-off - maintaining calls on the internal core network as long as possible, hopping off to the PSTN at a point where calls are local and/or where they possibly cost less.
- Access to SIP foundation servers including Avaya Aura™ Modular Messaging.

These solutions make use of the following Session Manager features:

- Geographically redundant network session control structure
- Least cost routing
- Alternate routing around network faults based on active SIP monitoring
- Network bandwidth use limitation based on session admission control
- Load balancing
- Session (or call) detail recording.

The network

This Case Study network consists of:

- Two Session Managers in the core network for redundancy
- Communication Managers in Westminster, Highlands Ranch, New Jersey HQ, and Avaya Labs New Jersey with differing length (3, 4, and 5-digit) dial plans
- Cisco CallManager in San Jose with a 5-digit dial plan
- A separate SIP trunk to the AT&T SIP service provider

- A session border controller through which trunks to Verizon and hypothetical SIP service providers can be accessed
- Modular Messaging system that serves all users in the enterprise
- A Voice Portal Service for 1-866-GO-Avaya provided in separate locations in the network.

Before beginning to administer Session Manager, we must decide:

- Domains that are used for routing. We make Session Manager authoritative for both avaya.com and avayalabs.com. The avayalabs.com domain is used for calls originated from the Avaya Labs NJ Communication Manager.
- The enterprise-wide dial plan and any domain-specific dial plans. Each user on one of the PBXs can dial another user, local or remote, through a unique 7-digit enterprise-canonical number.
- The locations that are defined for call admission control and any location-specific dial plans.

We adopt a basic philosophy to guide us in administering adaptation and the dial plan:

- The Session Manager dial plan routes internal enterprise-wide numbers and E.164 numbers (including E.164 representations of internal numbers).
- Calling party numbers are sent from the local PBXs in their local dial plan format. These numbers are all converted to enterprise-canonical on ingress to the Session Manager.
- Called party numbers are sent from the local PBXs in their local dial plan format. These numbers are all converted to either enterprise-canonical numbers or E.164 on ingress to the Session Manager.
- Calling party numbers that are in enterprise-canonical format are converted to whatever the service provider requires when a request is forwarded by the Session Manager.

After some initial, core provisioning, for each solution, we follow the administration of this configuration in the order recommended in Routing. This suggests defining in order, domains, locations, adaptations, SIP entities, SIP entity links, time ranges, routing policies, and dialing patterns.

Core provisioning

Core provisioning includes:

- The domains for which Session Manager is authoritative. However, these can be added as more are created.
- The SIP entities for the Session Manager servers. You can add these as more entities are created, linking other SIP entities as appropriate.
- Locations used to group entities for differing dial plans and/or bandwidth management. Again, you can add these as necessary.

Related topics:

[Domains](#) on page 11

[SIP entities for Session Managers](#) on page 12

[SIP entity for Westminster Session Manager](#) on page 12

[SIP entity for NJ Session Manager](#) on page 13

Domains

First, we add the two domains that appear in the request-URI of INVITE messages sent by the Communication Managers:

Domain Management

2 Items | [Refresh](#)

<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	avaya.com	sip	<input type="checkbox"/>	
<input type="checkbox"/>	avayalabs.com	sip	<input type="checkbox"/>	

Select : [All](#), [None](#)

The Cisco PBX and the service providers send the IP address of the Session Manager in the request-URI. Later, we administer the Session Manager to convert this IP address into the avaya.com domain so that calls from these entities can be routed.

SIP entities for Session Managers

Though routing suggests finishing the locations and adaptations before beginning SIP entities, Session Manager typed SIP entities are special in that they are not associated with a location nor an adaptation. The other SIP entities normally have both associations. Another, possibly more natural, course is to provision the location, adaptation and SIP entity detail for each SIP entity in turn rather than doing all locations and adaptations before proceeding to the SIP entities.

SIP entity for Westminster Session Manager

Adaptation and location are not necessary for Session Manager instances which essentially define the core network. These are necessary only for other SIP entities.

Generally, Session Manager listens for connections on ports specified in the entity link table, which is detailed later in this case study. If a port is specified in the Session Manager's sip entity port table (as shown below), SIP messages which contain this Session Manager's IP address in their Request-URI have it replaced by the domain specified in the port table. The Cisco PBX and some service providers can send a request with the Session Manager's IP address in the Request-URI. This port table entry is also currently necessary if SIP monitoring is to be used to monitor connectivity between Session Manager instances within the core network.

SIP Entity Details

CommitCancel

General

* Name: NA:US:CO

* FQDN or IP Address: 135.9.95.8

Type: Session Manager

Notes: Core Westminster

Location:

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

AddRemove

0 Items RefreshFilter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted

Port

AddRemove

1 Item RefreshFilter: Enable

	Port	Protocol	Default Domain	Notes
	5060	TCP	avaya.com	

Select : All, None (0 of 1 Selected)

* Input Required

CommitCancel

SIP entity for NJ Session Manager

This differs only in minor ways from the Westminster Core Session Manager. A network with two Session Manager instances would normally have each SIP entity connecting to both instances so that one instance can act as backup for the other in case of network or Session Manager failure.

Commit Cancel

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

Add Remove

0 Items Refresh Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>						

Port

Add Remove

1 Item Refresh Filter: Enable

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	

Select: All, None (0 of 1 Selected)

* Input Required

Commit Cancel

So that sessions can be alternately routed through another Session Manager in the case of network failure of connectivity between a non-Session Manager SIP entity and a particular Session Manager, the Session Manager instances need to be connected. This connection, like all inter-SIP entity connections, is specified with an entity link entry.

Currently, all entity links should be marked as **Trusted** or else they will not function. Unless there are restrictions against its use, the inter Session Manager entity link should use the **Protocol** TLS. If TLS is used by other SIP entities then it must be used, the reason being that SIP security standards do not allow passing secure information (like media encryption keys) over a connection where one of the inter-proxy connections is not TLS. Using TLS works, however, even if a SIP entity does not support TLS on its connection to Session Manager.

If there were three Session Manager instances in this case study, there would need to be an entity link between each pair, for a total of three.

Locations

Putting SIP entities into different locations currently serves two purposes:

- Provides a way to use different dialing plans. Calls originating from SIP entities in different locations can match different dialing pattern entries and route differently even though the dialed address are precisely the same.
- Can be used to limit the bandwidth used between the core network and that location.

In this case study each edge SIP entity is given its own location. Locations can be created and the location with which a given SIP entity is associated can be changed at any time.

Related topics:

[Locations with managed bandwidth](#) on page 15

[Locations without managed bandwidth](#) on page 16

Locations with managed bandwidth

In this case study the Westminster location exemplifies one where bandwidth is managed by setting the **Managed Bandwidth** value to only allow 100 simultaneous calls in or out of Westminster. The current release of Session Manager assumes that each call to and from the location use the **Average Bandwidth per Call** amount of network bandwidth. Note that the calls that stay within the location, even if they route through Session Manager, are not counted. Thus, the number of simultaneous calls allowed to and from that location are calculated by dividing the **Managed Bandwidth** value by the **Average Bandwidth per Call** value. The two values may be scaled differently, so this might not be a simple division. In the example below, the **Managed Bandwidth** is 8000 Kbits/s and the **Average Bandwidth per Call** is 80 Kbits/s, so the calculation is simple ($8000/80 \Rightarrow 100$). But if the **Managed Bandwidth** was instead 8 Mbits/s, then the 8 would need to be scaled to 8000 Kbits/s before the calculation is performed.

Incoming calls are associated with SIP entities in varying ways. If the call is associated with a particular SIP entity, it is deemed to have come from the location associated with that SIP entity. If a location contains location pattern IP address patterns, it can override the location association with the SIP entity. If a SIP entity's IP address is listed explicitly in the IP address patterns, as in this example, then there is no doubt about with which location it is associated.

Location Details [Commit] [Cancel]

General

* **Name:** NA:US:CO:Westminster

Notes:

Managed Bandwidth: 8000 Kbit/sec

* **Average Bandwidth per Call:** 80 Kbit/sec

Location Pattern

[Add] [Remove]

1 Item Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* [135.9.43.56]	

Select: All, None

Locations without managed bandwidth

The Research location exemplifies one without managed bandwidth. This does not mean there is unlimited bandwidth between this location and the core, just that Session Manager does not manage the bandwidth and does not limit the number of calls it sends to this location. There may be other limiting factors (like the number of calls the SIP entity will accept) to which Session Manager reacts. Simply leaving the **Managed Bandwidth:** field blank keeps Session Manager from managing the bandwidth.

The advantage to having Session Manager manage bandwidth is that it recognizes bandwidth exhaustion to a particular location before attempting to route a call there and it can then perform alternate routing earlier than if it had to wait for the SIP entity at that end to tell it that bandwidth was not available. Additionally Session Manager can associate multiple SIP entities with a given location and manage the bandwidth to the entire location where each SIP entity would not know the full bandwidth status of the location.

Location Details

CommitCancel

General

Name: NA:US:NJ:BaskingRidge:Research

Notes:

Managed Bandwidth: Kbit/sec

Average Bandwidth per Call: 80 Kbit/sec

Location Pattern

AddRemove

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 135.9.43.58	

Select : All, None

Time ranges

These are used for alternate routing. They are not associated with any particular SIP entity, but are needed for the specification of the ranking of routing preferences (even if routing does not depend upon the time of day). It is useful to have defined at least the All Day time range.

Time Ranges

EditNewDuplicateDeleteMore ActionsCommit

4 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	All Day	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	
<input type="checkbox"/>	Business	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	09:00	17:00	
<input type="checkbox"/>	Week Day	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	00:00	23:59	
<input type="checkbox"/>	Weekend	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Non-Session Manager SIP entities

The provisioning details of the non-Session Manager SIP entities is outlined as the solutions with which they are associated are explained below. The resulting SIP entities in this case study are listed here in the SIP Entities table. Note that currently the **Type** of the entity matters only if it is Session Manager. All other types are effectively the same, though this could change in future releases, so it is best to choose an appropriate type.

In this case study non-Session Manager SIP entities fall into one of three categories:

- PBXs that front telephones and PSTN trunks
- SIP service providers that essentially front PSTN trunks. Even though they might route some calls entirely within their SIP network it is assumed all or a known subset of PSTN numbers can be reached through them.
- SIP foundation servers such as Avaya Modular Messaging or Voice Portal or any other server that creates communication sessions with SIP.

SIP Entities

EditNewDuplicateDeleteMore ActionsCommit

14 ItemsRefreshFilter: Enable

<input type="checkbox"/>	Name	Entity Links	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	NA:US:CO	▶	135.9.95.8	Session Manager	Core Westminster
<input type="checkbox"/>	NA:US:NI	▶	135.9.43.191	Session Manager	Core BaskingRidge
<input type="checkbox"/>	NA:US:CO:HighlandsRanch	▶	hr.avaya.com	CM	444
<input type="checkbox"/>	NA:US:CO:Westminster	▶	135.9.43.66	CM	538
<input type="checkbox"/>	NA:US:NI:BaskingRidge:HQ	▶	135.9.43.67	CM	953
<input type="checkbox"/>	NA:US:NI:BaskingRidge:Research	▶	135.9.43.68	CM	695-5
<input type="checkbox"/>	NA:US:CA:SanJose	▶	135.9.106.161	Other	661
<input type="checkbox"/>	NA:US:CO:AppServer001	▶	135.9.95.7	Other	SIPAppServer-cmarch7
<input type="checkbox"/>	NA:US:CO:Westminster:MM	▶	mm.dr.avaya.com	Other	ModularMessaging
<input type="checkbox"/>	ATT	▶	135.9.43.69	SIP Trunk	AT&T Flex Reach Global
<input type="checkbox"/>	HypotheticalISP	▶	sbcl.dr.avaya.com	SIP Trunk	
<input type="checkbox"/>	Verizon	▶	sbcl.dr.avaya.com	SIP Trunk	Verizon Business
<input type="checkbox"/>	APAC:App800	▶	go.jp.avaya.com	Voice Portal	APAC GO-AVAYA
<input type="checkbox"/>	NA:US:App800	▶	go.avaya.com	Voice Portal	Main GO-AVAYA

Harmonizing disparate PBXs

This case study has two brands of PBXs: Communication Manager and Cisco Call Manager. Additionally the PBXs have different length extensions (or dial plans). These two aspects require the Session Manager to adapt (that is, alter) SIP messages to the standard SIP messaging performed by Session Manager as well as the E.164 and Enterprise Canonical (that is, common) dial plan used in this example.

Related topics:

[Adaptations for PBXs](#) on page 19

[SIP entities for PBXs](#) on page 24

Adaptations for PBXs

Adaptation is normally needed for all of the PBX devices that connect to the Session Manager. They, like locations, can be created before a given PBXs SIP entity. This is particularly useful if two PBXs might use the same adaptation. Alternatively, one can create SIP entities with blank adaptations first and then modify the SIP entity to use a particular adaptation created later.

Adaptation digit conversion is likely the most complex aspect of and requires the most planning for the deployment of this example.

Related topics:

[Westminster PBX adaptation](#) on page 19

[NJ HQ Communication Manager adaptation](#) on page 20

[Avaya Labs research PBX adaptation](#) on page 21

[San Jose PBX adaptation](#) on page 22

Westminster PBX adaptation

The Westminster Communication Manager has a local 5-digit dial plan (8xxxx). Each extension can also be dialed from other systems using the 7-digit enterprise canonical number 538-xxxx. The PBX also has DID numbers assigned; a PSTN caller can dial +1303538xxxx to reach an extension.

This adaptation uses the DigitConversionAdapter. The Westminster PBX is set up to be authoritative for dr.avaya.com on its network region form. This means that INVITEs sent from Session Manager to the PBX must have dr.avaya.com in the host part of the request-URI. The odstd parameter to the adaptation module specifies this. The PBX also uses dr.avaya.com as the far-end domain on the signaling group to the Session Manager, which means that the P-Asserted-Identity header of incoming INVITEs must be changed to dr.avaya.com. We use the osrcd parameter to the adaptation module to accomplish this.

The digit conversion tables are set up accordingly. The text that is placed in the Adaptation Module box is DigitConversionAdapter odstd=dr.avaya.com osrcd=dr.avaya.com (the parameter osrcd means override source domain).

Adaptation Details

General

Adaptation name:

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls

+ 4 Items Refresh
Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 011	* 4	* 36	* 3	+	both	to E.164
<input type="checkbox"/>	* 1	* 11	* 11	* 0	+	both	to E.164
<input type="checkbox"/>	* 8	* 5	* 5	* 0	53	both	to 7-digit Enterprise Canonical
<input type="checkbox"/>	* 8	* 10	* 10	* 0	+1	both	to E.164

Selected: All, None (0 of 4 Selected)

Digit Conversion for Outgoing Calls

2 Items Refresh
Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* +1303538	* 12	* 12	* 7		both	E.165 to 5-digit extension
<input type="checkbox"/>	* 538	* 7	* 7	* 2		both	EC to 5-digit extension

NJ HQ Communication Manager adaptation

The NJ HQ Communication Manager has a local 4-digit dial plan (xxxx). Each extension can also be dialed from other systems using the 7 digit enterprise canonical number 953-xxxx. The PBX also has DID numbers assigned; a PSTN caller can dial +1908953xxxx to reach an extension.

This adaptation uses the DigitConversionAdapter. The NJ HQ PBX is set up to be authoritative for nj.avaya.com on its network region form. It also uses nj.avaya.com as the far-end domain on the signaling group to the Session Manager. These domain conversions are specified as parameters to the adaptation module. The text that is placed in the Adaptation Module box is DigitConversionAdapter odstd=dr.avaya.com osrcd=dr.avaya.com

Adaptation Details Commit Cancel

General

Adaptation name:

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls

4 Items Filter:

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 011	* 4	* 35	* 3	+	both	to E.164
<input type="checkbox"/>	* 1	* 11	* 11	* 0	+	both	to E.164
<input type="checkbox"/>	* x	* 4	* 4	* 0	953	both	to 7-digit Enterprise Canonical
<input type="checkbox"/>	* x	* 10	* 10	* 0	+1	both	to E.164

Select: All, None (0 of 4 Selected)

Digit Conversion for Outgoing Calls

2 Items Filter:

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* +1908953	* 12	* 12	* 8		both	E.164 to 4-digit extension
<input type="checkbox"/>	* 953	* 7	* 7	* 3		both	EC to 4-digit extension

Avaya Labs research PBX adaptation

The Avaya Labs Communication Manager has a local 3-digit dial plan (xxx). Each extension can also be dialed from other systems using the 7-digit enterprise canonical number 696-5xxx. The PBX also has DID numbers assigned; a PSTN caller can dial +19086965xxx to reach an extension.

This adaptation uses the DigitConversionAdapter. The Communication Manager is set up to be authoritative for avayalabs.com on its network region form. It also uses avayalabs.com as the far-end domain on the signaling group to the Session Manager, which means that the P-Asserted-Identity header of incoming INVITEs must be changed to avayalabs.com.

The text that is placed in the Adaptation Module box is DigitConversionAdapter
odstd=avayalabs.com osrcd=avayalabs.com

Adaptation Details

Commit Cancel

General

Adaptation name: NA:US:ND:BaikingRidge

Module name: DigitConversionAdapter

Module parameter: cmarch.dr.avaya.com

Egress URI Parameters:

Notes: TEHO + 1908

Digit Conversion for Incoming Calls

Add Remove

4 Items Refresh

Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 011	* 4	* 36	* 3	+	both	to E.164
<input type="checkbox"/>	* 1	* 11	* 11	* 0	+	both	to E.164
<input type="checkbox"/>	* x	* 3	* 3	* 0	6965	both	to 7-digit Enterprise Canonical
<input type="checkbox"/>	* x	* 10	* 10	* 0	+1	both	to E.164

Select: All, None (0 of 4 Selected)

Digit Conversion for Outgoing Calls

Add Remove

2 Items Refresh

Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* +19086965	* 12	* 12	* 9		both	E.164 to 3-digit extension
<input type="checkbox"/>	* 6965	* 7	* 7	* 4		both	EC to 3-digit extension

San Jose PBX adaptation

The San Jose PBX has a local 5-digit dial plan (1xxxx). This means that extensions connected to this PBX normally dial each other by entering only five digits. Each extension can also be dialed from other systems using the 7-digit enterprise-canonical number 661-xxxx. The PBX also has DID (direct inward dialing) numbers assigned; a PSTN caller can dial +1408661xxxx to reach an extension. For calls made by local users, adaptation converts

- Numbers dialed by local users into enterprise canonical numbers (for example, a San Jose user calls another San Jose user via the Session Manager)
- Local Calling party numbers into enterprise-canonical numbers (for example, San Jose user calls a Westminster user. The calling party number displayed in Westminster is the enterprise-canonical number)
- Calls to international numbers to E.164 format (for example, someone dials 011+digits)
- Calls to North American numbers to E.164 format

For calls made to the San Jose PBX, adaptation must convert:

- The called party enterprise-canonical number into a local extension number (for example, a 661-xxxx number into a 1xxxx number)
- The E.164 number into a local extension number, for calls coming from a service provider (for example, +1408661xxxx into 1xxxx)

This adaptation uses the CiscoAdapter to convert between the proprietary headers Cisco uses to convey display and diversion information with the standard headers used by Avaya products. CiscoAdapter, like all currently available adapters, can also perform digit conversion. The Cisco PBX also needs its IP address (135.9.106.161) as the host part of the request-URI, so this conversion is specified as a parameter (odstd, which means override destination domain).

The digit conversion tables convert between the local 1xxxx dial plan and the enterprise canonical 661-xxxx dial plan. On ingress to the Session Manager, digit strings in the local 1xxxx dial plan need to be converted into the enterprise canonical form. On egress from the Session Manager, the 661-xxxx enterprise canonical numbers need to be converted into the local extensions.

The digit conversion tables also convert dialed numbers for international calls (011+digits) or calls within North America (10 digit, 1+10 digit) to E.164 form when requests enter the Session Manager. Similarly, E.164 and enterprise canonical calls to local users must be converted into local form on egress from the Session Manager.

Adaptation Details

Commit Cancel

General

Adaptation name: NA:US:CA:SanJose

New module name: CiscoAdapter

Module parameter: odstd=135.9.106.161

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls

Add Remove

4 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 011	* 4	* 36	* 3	+	both	Int'l call to E.164
<input type="checkbox"/>	* 1	* 5	* 5	* 0	66	both	to 7-digit Enterprise Canonical
<input type="checkbox"/>	* 1	* 11	* 11	* 0	+	both	to E.164
<input type="checkbox"/>	* x	* 10	* 10	* 0	+1	both	to E.164

Select: All, None (0 of 4 Selected)

Digit Conversion for Outgoing Calls

Add Remove

2 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* +1408661	* 12	* 12	* 7		both	E.164 to 5-digit extension
<input type="checkbox"/>	* 661	* 7	* 7	* 2		both	EC to 5-digit extension

SIP entities for PBXs

The PBXs in this case study are shown in the SIP entity table above as type Communication Manager or Other (though not all Other-typed SIP entities are edge PBXs). They are each administered similarly. The FQDN/IP Address is the primary distinguishing attribute. It is used to identify sessions as originating from that SIP entity and to where it should send messages to establish sessions to the entity. The location associated with the SIP entity (unless overridden) factors into the routing and the adaptation affects how the messages may be modified.

Related topics:

- [Single interface](#) on page 24
- [Multiple interfaces](#) on page 25
- [Routing policies for PBXs](#) on page 27
- [Dial patterns for PBXs enterprise canonical numbering](#) on page 29

Single interface

The Westminster Communication Manager exemplifies one with a single interface, where its IP address is specified. The other PBXs: Basking Ridge HQ, Basking Ridge Research, and San Jose (even being a Cisco Call Manager) are all similar.

SIP Entity Details

Commit

Cancel

General

Name

NA.US.CO.Westminster

FQDN or IP Address

135.9.43.66

Type

CM

Notes

Location

NA.US.CO.Westminster

Outbound Proxy

Time Zone

America/Denver

Credential name

SIP Link Monitoring

SIP Link Monitoring

Use Session Manager Configuration

Entity Links

Add

Remove

0 items

Refresh

Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
	NA.US.CO	TCP	5060	NA.US.CO:Westm	5060	<input checked="" type="checkbox"/>
	NA.US.NJ	TCP	5060	NA.US.CO:Westm	5060	<input checked="" type="checkbox"/>

Generally, PBXs do not need call detail records created for each call, so the **Call Detail Recording** field is set to none. SIP monitoring should be used for all SIP entities that support it (and most all PBXs do), and so the value of **Monitoring on/off** should be left as Use Session Manager configuration, which allows specification of global (to this Session Manager instance) SIP monitoring parameters.

To define the ports and transport types supported by this SIP entity, **Entity Links** entries are made. The entity link table for this SIP entity shows that this SIP entity connects to both Session Manager instances in the network.

In both cases TCP port 5060 is used, not only for connections out to the SIP entity, but connections in from it. **SIP Entity 1** is always a Session Manager SIP entity. Conventionally, the **Name**, which must be unique for all links in the system, contains some representation of the name of the Session Manager SIP entity and that of the non-Session Manager SIP entity, though this is not necessary. Currently, the entity link must always be marked as **Trusted** or else it fails to function.

Multiple interfaces

The Highlands Ranch Communication Manager shows a SIP entity with multiple interfaces. This might be typical of a large Communication Manager with more than one C-LAN. It allows for redundant routing and a higher level of fault tolerance. Routing to it is handled by specifying an FQDN for it, which resolves to multiple IP addresses.

SIP Entity Details [Commit] [Cancel]

General

* Name: NA-US-CO-HighlandsRanch

* FQDN or IP Address: hr.araya.com

Type: CM

Notes: 444

Location: NA-US-CO-HighlandsRanch

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

[Add] [Remove]

0 Items | Refresh Filter: Enable

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
NA-US-CO	TLS	5061	NA-US-CO-High	5061	<input checked="" type="checkbox"/>
NA-US-NJ	TLS	5061	NA-US-CO-High	5061	<input checked="" type="checkbox"/>

This particular SIP entity supports TLS, so the entity link protocol and port are adjusted accordingly.

The FQDN in this case can either be resolved by DNS or through a locally provisioned FQDN to IP address mapping. The latter mapping is specified in the Session Manager Element manager's Local Host Name Resolution table

Local Host Name Resolution
This page allows you to add, edit, or remove local host name entries. Host name entries on this page will override information provided by DNS.

Local Host Name Entries

9 Items | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Host Name	IP Address	Port	Priority	Weight	Transport
<input type="checkbox"/>	hr.avaya.com	135.9.43.69	1	100	100	TLS
<input type="checkbox"/>	hr.avaya.com	135.9.43.159	1	200	100	TLS

This table is used both for simple FQDN to IP address mapping (like this example) plus full port and transport specification (shown later). For the simple case, the **Port** and **Transport** values are ignored because they are specified in the entity link table (5061 and TLS). The convention of giving the **Port** a value of 1 is used to indicate this. The **Priority** is used, and given that the first line has a higher priority (lower numbered value), it is always used first. The only time the second entry is used is if a failure is encountered while using the first IP address.

To realize this connectivity, the HighlandsRanch Communication Manager requires four signaling and trunk groups: one from each C-LAN to each of the Session Managers. The first signaling group:

```
display signaling-group 1
SIGNALING GROUP
Group Number: 1          Group Type: sip
                        Transport Method: tls
IMS Enabled? n

Near-end Node Name: cwc-clan    Far-end Node Name: NA:US:CO
Near-end Listen Port: 5061      Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Domain: avaya.com

Bypass If IP Threshold Exceeded? n

DTMF over IP: rtp-payload      Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3  IP Audio Hairpinning? n
Enable Layer 3 Test? y          Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n  Alternate Route Timer(sec): 4

Command:
```

The transport method and port match those specified in the entity link from each Session Manager to the Communication Manager. The IMS Enabled field should not be set for standard SIP scenarios. Level 3 tests enabled has the Communication Manager perform OPTIONS monitoring of the Session Manager instances. The Bypass request should probably not be enabled. Communication Manager tests if the network characteristics between its media processors and the Session Manager are suitable for media and Communication Manager should not be sending media to the Session Manager. The four signaling groups:

List signaling-group										
SIGNALLING GROUPS										
Grp No.	Group Type	FAS?	Trunk Erds	Pri D-Ch/ Near-node	Sec D-Ch/ Far-node	Max NCA	Max TSC	Max CA	Max TSC	No. Adm'd NCA TSCs
1	sip	y	1	cmc-clan	NA:US:CO	0	0	0	0	0
2	sip	y	1	g600-clan	NA:US:CO	0	0	0	0	0
11	sip	y	1	cmc-clan	NA:US:NJ	0	0	0	0	0
12	sip	y	1	g600-clan	NA:US:NJ	0	0	0	0	0

Assuming all the SIP trunk groups associated with the signaling groups used the same group number, an outgoing routing pattern would look like:

change route-pattern 2										
Pattern Number: 2 Pattern Name: External										
SCCAN? n Secure SIP? n										
Grp No	FRL	NPA	Pfx	Hop	Toll	No. Inserted	DCS/ QSIG	IXC		
Msk Lmt List Del Digits							Intw			
1:	1	0					n	user		
2:	2	0					n	user		
3:	11	0					n	user		
4:	12	0					n	user		
5:							n	user		
6:							n	user		
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR										
0 1 2 M 4 W Request							Dgts Format Subaddress			
1:	y	y	y	y	y	n		rest		next
2:	y	y	y	y	y	n		rest		next
3:	y	y	y	y	y	n		rest		next
4:	y	y	y	y	y	n		rest		none
5:	y	y	y	y	y	n		rest		none
6:	y	y	y	y	y	n		rest		none

The Communication Manager would try each of its connections to its local Session Manager (PBX and Session Manager NA:US:CO are both in CO) before trying the remote Session Manager (NA:US:NJ in NJ). The LAR (look-ahead routing) field must be next on every preference that needs to skip to the next route on an error.

Routing policies for PBXs

Routing policies indicate the rank order of a particular SIP entity. Multiple routing policies can be associated with a dial pattern (as shown later) to specify alternate routing. Additionally, the rank of a routing policy can be changed by the time of day. For simple PBX routing (like in this example) specific dial patterns are associated with only one PBX and these do not vary by the time of day. For these types of routing policies the convention is to use the SIP entity's name as the routing policy name too.

Routing Policies					
<input type="button" value="Edit"/> <input type="button" value="New"/> <input type="button" value="Duplicate"/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/> <input type="button" value="Commit"/>					
14 Items Refresh					Filter: Enable
<input type="checkbox"/>	Name	Disabled	Destination	Notes	
<input type="checkbox"/>	NA:US:NJ:BaskingRidge:Research	<input type="checkbox"/>	NA:US:NJ:BaskingRidge:Research		
<input type="checkbox"/>	NA:US:NJ:BaskingRidge:HQ	<input type="checkbox"/>	NA:US:NJ:BaskingRidge:HQ		
<input type="checkbox"/>	NA:US:CO:Westminster	<input type="checkbox"/>	NA:US:CO:Westminster		
<input type="checkbox"/>	NA:US:CO:HighlandsRanch	<input type="checkbox"/>	NA:US:CO:HighlandsRanch		
<input type="checkbox"/>	NA:US:CA:SanJose	<input type="checkbox"/>	NA:US:CA:SanJose		

The routing policy detail allows the association of the routing policy with the SIP entity. There is no time-of-day routing associated with this policy so only the All Day time range is added to the Time of Day section. Also this is not to be part of an alternate route so Ranking of 0 is used. The dial patterns are shown here, but they are defined on another form.

Routing Policy Details													Commit	Cancel
General														
* Name: <input type="text" value="NA:US:CO:Westminster"/>														
Disabled: <input type="checkbox"/>														
Notes: <input type="text"/>														
SIP Entity as Destination														
<input type="button" value="Select"/>														
Name	FQDN or IP Address	Type	Notes											
NA:US:CO:Westminster	135.9.43.66	CM	538											
Time of Day														
<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="View Gaps/Overlaps"/>														
1 Item Refresh													Filter: Enable	
<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes		
<input type="checkbox"/>	0	All Day	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59			
Select: All, None (0 of 1 Selected)														
Dial Patterns														
<input type="button" value="Add"/> <input type="button" value="Remove"/>														
3 Items Refresh													Filter: Enable	
<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes							
<input type="checkbox"/>	+1303	12	12	<input type="checkbox"/>	-ALL-	-ALL-	TEHO to Westminster							
<input type="checkbox"/>	+1303538	12	12	<input type="checkbox"/>	-ALL-	-ALL-	E.164 to Westminster							
<input type="checkbox"/>	538	7	7	<input type="checkbox"/>	-ALL-	-ALL-	OnNet to Westminster							

Dial patterns for PBXs enterprise canonical numbering

The dial patterns defined in this solution allow the on-net 7-digit dialing between the disparate PBXs.

Dial Patterns						
<input type="button" value="Edit"/> <input type="button" value="New"/> <input type="button" value="Duplicate"/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/> <input type="button" value="Commit"/>						
13 Items Refresh Filter: Enable						
<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
<input type="checkbox"/>	953	7	7	<input type="checkbox"/>	-ALL-	OnNet to BaskingRidge:HQ
<input type="checkbox"/>	6965	7	7	<input type="checkbox"/>	-ALL-	OnNet to BaskingRidge:Research
<input type="checkbox"/>	661	7	7	<input type="checkbox"/>	-ALL-	OnNet to SanJose
<input type="checkbox"/>	538	7	7	<input type="checkbox"/>	-ALL-	OnNet to Westminster
<input type="checkbox"/>	444	7	7	<input type="checkbox"/>	-ALL-	OnNet to HighlandsRanch

In the details for the dial pattern, a blank **Domain** indicates the pattern matches any domain. The originating location and routing policy associated with this dial pattern are -ALL- and the Westminster PBX SIP entity respectively. This means a session created from anywhere with a user part of 538xxxx routes to this particular PBX. Specific originating locations could be denied access to this dial pattern (that is, the call would be denied).

Dial Pattern Details						<input type="button" value="Commit"/>	<input type="button" value="Cancel"/>
General							
* Pattern: <input type="text" value="538"/> * Min: <input type="text" value="7"/> * Max: <input type="text" value="7"/> Emergency Call: <input type="checkbox"/> SIP Domain: <input type="text" value="-ALL-"/> Notes: <input type="text" value="OnNet to Westminster"/>							
Originating Locations and Routing Policies							
<input type="button" value="Add"/> <input type="button" value="Remove"/>							
1 Item Refresh Filter: Enable							
<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes	
<input type="checkbox"/>	-ALL-	Any Locations	NA:US:CO:Westminster	<input type="checkbox"/>	NA:US:CO:Westminster		
Select: All, None (0 of 1 Selected)							
Denied Originating Locations							
<input type="button" value="Add"/> <input type="button" value="Remove"/>							
0 Items Refresh Filter: Enable							
<input type="checkbox"/>	Originating Location	Notes					

SIP service providers

This case study depicts three SIP service providers: AT&T, Verizon, and Hypothetical. AT&T is connected through one session boarder controller (though it could be connected directly) while Verizon and Hypothetical are connected through a different, though shared SBC.

For connections to SIP service providers to be useful for outgoing as well as incoming traffic, each PBX must, in addition to routing their on-net 7-digit calls, route their PSTN calls to the Session Manager core. As seen before the 7-digit calls are routed to other PBXs while the PSTN numbers are converted to E.164 and routed to SIP service providers (as seen in this section).

Related topics:

[SIP service provider adaptations](#) on page 30

[AT&T adaptation](#) on page 30

[Verizon adaptation](#) on page 31

[Hypothetical adaptation](#) on page 32

SIP service provider adaptations

SIP service providers typically send in digit strings formatted for the calling area in which the service is provided. In North America they may be 10- or 7-digit called and calling party numbers. For outgoing calls (relative to the Session Manager network) they may allow only calling party numbers from a block of purchased ones (that is, those they route into the Session Manager network over the SIP facility). Adaptation can be used for the necessary conversions.

AT&T adaptation

When a request comes in from AT&T, the calling and called party numbers is 10 digits for calls originated from North America and E.164 for international calls. Session Manager converts the called party number to E.164 form.

When sending requests to AT&T, Session Manager has to convert calling and called party numbers. AT&T requires that the host part of the request-URI be their IP address (in this example, 135.9.43.69). The called party number must be sent in the request-URI as either 011+ digits for international calls or as a 10-digit North American number. The calling party number must be sent as a 10-digit number.

This adaptation uses the AttAdapter, which does digit conversion and strips the History-Info header from requests, as the AT&T network is not compatible with this header that is used by Communication Manager. The IP address supplied by AT&T must be specified as a parameter

to convert the host-part of the request-URI. Thus, the text to enter in the Adaptation Module box is AttAdapter odstd=135.9.43.69.

Adaptation Details

Commit Cancel

General

Adaptation name: NA:AT&T

New module name: AttAdapter

Module parameter: odstd=1.2.3.4

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls

Add Remove

3 Items Refresh

Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*x	4	9	0	+	both	to E.164
<input type="checkbox"/>	*x	10	10	0	+1	both	NA to E.164
<input type="checkbox"/>	*x	11	36	0	+	both	to E.164

Select: All, None (0 of 3 Selected)

Digit Conversion for Outgoing Calls

Add Remove

6 Items Refresh

Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*+	4	36	1	011	both	E.164 to intl
<input type="checkbox"/>	*+1	12	12	1		both	E.164 to NA
<input type="checkbox"/>	*538	7	7	0	303	origination	EC to NA
<input type="checkbox"/>	*561	7	7	0	408	origination	EC to NA
<input type="checkbox"/>	*595	7	7	0	908	origination	EC to NA
<input type="checkbox"/>	*953	7	7	0	908	origination	EC to NA

Verizon adaptation

Verizon adaptation is similar to AT&T adaptation, with these differences:

- Verizon uses the VerizonAdaptation adaptation module. This module does digit conversion and converts the History-Info header to a Diversion header and vice-versa.
- In this case study the Verizon connection and the following Hypothetical service provider connection is done through a common session border controller (SBC). The conversion of the domain in the SIP message request URI to the IP address of the Verizon gateway is handled by the SBC.

Adaptation Details

Commit Cancel

General

Adaptation name: NA:Verizon

New module name: VerizonAdapter

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls

Add Remove

2 Items Refresh

Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*x	10	10	0	+	both	N. America to E.164
<input type="checkbox"/>	*x	11	35	0	+	both	to E.164

Select: All, None (0 of 2 Selected)

Digit Conversion for Outgoing Calls

Add Remove

6 Items Refresh

Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*+	4	35	1	011	destination	E.164 to intl
<input type="checkbox"/>	*+1	12	12	1		destination	E.164 to NA
<input type="checkbox"/>	*538	7	7	0	303	origination	Calling party EC to N. Am.
<input type="checkbox"/>	*651	7	7	0	408	origination	Calling party EC to N. Am.
<input type="checkbox"/>	*696	7	7	0	908	origination	Calling party EC to N. Am.
<input type="checkbox"/>	*953	7	7	0	908	origination	Calling party EC to N. Am.

Hypothetical adaptation

The basic DigitConversionAdapter may suffice for adapting connectivity to other SIP service providers. Alternatively, some adaptation functions could be provided by an external SBC which is used in this particular case study, leaving the DigitConversionAdapter to simply convert digit fields in the SIP message.

When a request comes in from Hypothetical, the calling and called party numbers are 10 digits for calls originated from North America and E.164 for international calls. Session Manager converts the called party number to the E.164 form.

When sending requests to Hypothetical, Session Manager has to convert calling and called party numbers. Hypothetical requires that the host part of the request-URI be “hyposp.com” and that DNS be used to locate the correct server. The called party number must be sent in the request-URI as either 011+ digits for international calls or as a 1+10 digit North American number. The calling party number must be sent as a 10-digit number.

When calls originate from one of the PBXs, the calling party numbers are in the enterprise-canonical format. On egress to Hypothetical, these numbers must be converted to 10-digit North American numbers. The Digit Conversion for Outgoing Calls table below has been set

up to do this. The choice of the origination address in the Address to modify column indicates that only calling party numbers (in the P-Asserted-Identity header) of the request is modified. The choice of the destination in the rule that converts E.164 to North American format indicates that only the Request-URI is modified.

This adaptation uses the DigitConversionAdapter. The hyposp.com domain must be specified as a parameter to convert the host-part of the request-URI. Also, Hypothetical requires the 'user=phone' parameter in the request-URI. This is entered in the **Egress URI Parameters** box on the form.

Adaptation Details

CommitCancel

General

Adaptation name: NA:HypotheticalSP

Module name: DigitConversionAdapter

Module parameter: odstd=hyposp.com

Egress URI Parameters: user=phone

Notes:

Digit Conversion for Incoming Calls

AddRemove

2 Items | Refresh

Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*X	10	10	0	+	both	N. America to E.164
<input type="checkbox"/>	*X	11	36	0	+	both	to E.164

Select: All, None (0 of 2 Selected)

Digit Conversion for Outgoing Calls

AddRemove

6 Items | Refresh

Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*+	4	36	1	011	destination	E.164 to intd
<input type="checkbox"/>	*+1	12	12	1		destination	E.164 to NA
<input type="checkbox"/>	*538	7	7	0	303	origination	Calling party EC to N. Am.
<input type="checkbox"/>	*661	7	7	0	408	origination	Calling party EC to N. Am.
<input type="checkbox"/>	*696	7	7	0	908	origination	Calling party EC to N. Am.
<input type="checkbox"/>	*953	7	7	0	908	origination	Calling party EC to N. Am.

Note that the **Adaptation Module** and **Egress URI Parameters** fields allow free format text. These fields scroll horizontally so their complete values may not show on the form without active selection and scrolling (as seen in this particular example). Additionally, the system does not validate the values in these fields, so enter these values carefully.

SIP entities for SIP service providers

SIP service provider connections differ from edge PBXs in various ways. Normally they are connected through session border controllers, and they require call detail recording. In this

case study there are three SIP service provider connections: one, AT&T, is connected through a dedicated SBC while the other two, Hypothetical and Verizon, share an SBC. Other minor differences are highlighted.

Related topics:

[Single SIP entity behind SBC](#) on page 34

[Multiple SIP entities behind SBC](#) on page 35

Single SIP entity behind SBC

A single connection behind an SBC has the characteristic that the IP address of the SBC can be considered to represent the one and only SIP entity behind it. There is no reason to distinguish messages coming from the SBC from those intended for the SIP entity. The SIP entity configuration looks similar to that of any other SIP entity.

SIP Entity Details [Commit] [Cancel]

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

0 items | Refresh Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
	NA:US:CO	UDP	5060	ATT	5060	<input checked="" type="checkbox"/>
	NA:US:IJ	UDP	5060	ATT	5060	<input checked="" type="checkbox"/>

In this example the IP address of the SBC is used. The **Type** is marked SIP Trunk for categorization.

The **Call Detail Recording:** field is set at egress, meaning that all sessions established out to this SIP entity are recorded. Incoming sessions are not recorded, unless they route out to a SIP entity that is marked for **egress** or **both** CDR recording.

Again, an entity link must be created for each Session Manager to this SIP entity, in this case UDP is the Protocol used, though the SBC could be used to translate the UDP supported by AT&T to TCP. The SBC must also be willing to accept messages from each Session Manager and route messages to either Session Manager (in case of network or Session Manager failure).

Multiple SIP entities behind SBC

In this example, both the Verizon and Hypothetical service providers are behind an SBC at an IP address specified by an FQDN. We do not have an entry in the Local Host Name Resolution table for this. The Session Manager goes to the network's DNS server to resolve the IP address.

SIP Entity Details [Commit] [Cancel]

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

0 items | Refresh Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
	NA-US-DO	TCP	5060	Verizon	5060	<input type="checkbox"/>
	NA-US-NJ	TCP	5060	Verizon	5060	<input checked="" type="checkbox"/>

The entity links specified for this SIP entity use the standard ports for TCP.

The Hypothetical service provider's gateway, behind the SBC, is located in the same location as that of Verizon, so any bandwidth management for that location applies to both SIP entities. The time zone, used for time-of-day routing differs. Although this may sound strange (same location, but different time zone), it is an artifact of grouping them together for bandwidth management. Both, in this case study, are reached over the same physical communication link to the SBC, but behind that, their respective gateways are located in different time zones and the tariffs they specify have different rates depending upon the time zone in which the gateways are located. Additionally, Hypothetical does not support any form of SIP monitoring, so this is

disabled on the SIP entity form.

The screenshot shows the 'SIP Entity Details' form with the following fields and values:

- Name:** HypotheticalSP
- FQDN or IP Address:** abc1.dravys.com
- Type:** SIP Trunk
- Notes:** (empty)
- Location:** NA-US-NJ-Verizon-POP
- Outbound Proxy:** (empty)
- Time Zone:** America/Chicago
- Credential name:** (empty)
- SIP Link Monitoring:** Disable monitoring

Below the form is the 'Entity Links' section with a table showing two links:

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
NA-US-CO	TLS	5062	HypotheticalSP	5062	<input checked="" type="checkbox"/>
NA-US-NJ	TLS	5062	HypotheticalSP	5062	<input checked="" type="checkbox"/>

The special entity link administration is what makes this configuration possible. Notice that the ports are different and nonstandard on both sides of the entity link. The SBC must be programmed to send messages from Hypothetical's gateway to port 5062 using the TLS protocol and must be willing to accept connections to port 5062 and forward those messages to Hypothetical (the ports could have been different). Using the different ports is what allows the Session Manager to distinguish the traffic from the same SBC IP address to be from different SIP entities.

Routing policies for SIP service providers

The routing policies Alternate-AT&T, Alternate-Verizon, and HypotheticalSP are the primary policies that route to the SIP service providers. The Alternate-BaskingRidge policies are for tail-end hop-off (discussed later), and the Ap800 policies are for some SIP foundation servers (also discussed later).

Routing Policies					
<input type="button" value="Edit"/> <input type="button" value="New"/> <input type="button" value="Duplicate"/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/> <input type="button" value="Commit"/>					
15 Items			Filter: Enable		
<input type="checkbox"/>	Name	Disabled	Destination	Notes	
<input type="checkbox"/>	Alternate-AT&T	<input type="checkbox"/>	ATT	1 - primary	
<input type="checkbox"/>	Alternate-BaskingRidge:HQ	<input type="checkbox"/>	NA:US:NJ:BaskingRidge:HQ	prefer on Weekends	
<input type="checkbox"/>	Alternate-BaskingRidge:Research	<input type="checkbox"/>	NA:US:NJ:BaskingRidge:Research	prefer on Week Days	
<input type="checkbox"/>	Alternate-Verizon	<input type="checkbox"/>	Verizon	2 - secondary	
<input type="checkbox"/>	Ap800 APAC 1	<input type="checkbox"/>	APAC:App800	1 APAC	
<input type="checkbox"/>	Ap800 APAC 2	<input type="checkbox"/>	NA:US:App800	2 NA	
<input type="checkbox"/>	Ap800 NA 1	<input type="checkbox"/>	NA:US:App800	1 NA	
<input type="checkbox"/>	Ap800 NA 2	<input type="checkbox"/>	APAC:App800	2 APAC	
<input type="checkbox"/>	HypotheticalSP	<input type="checkbox"/>	HypotheticalSP		

Related topics:

[Simple routing policy for routing policies for SIP service providers](#) on page 37

[Alternative routing policy for routing policies for SIP service providers](#) on page 38

Simple routing policy for routing policies for SIP service providers

The HypotheticalSP is a simple routing policy. No alternate routing to it is anticipated, so it has a single Rank 0 time of day entry. A unique dial pattern references this policy and no other.

Routing Policy Details												Commit	Cancel
General													
* Name: <input type="text" value="HypotheticalSP"/>													
Disabled: <input type="checkbox"/>													
Notes: <input type="text"/>													
SIP Entity as Destination													
<input type="button" value="Select"/>													
Name	FQDN or IP Address	Type	Notes										
HypotheticalSP	sbc1.dr.avaya.com	SIP Trunk											
Time of Day													
<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="View Gaps/Overlaps"/>													
1 Item Refresh Filter: Enable													
<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes	
<input type="checkbox"/>	0	All Day	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59		

Alternative routing policy for routing policies for SIP service providers

The Alternate-AT&T and Alternate-Verizon routing policies are meant to work in concert. The convention used here is to name such routing policies with the Alternate prefix and put their relative ranking in the **Notes** field. Here the Alternate-AT&T policy has a 10 ranking while the Alternate-Verizon has 20, so any dial pattern that references both of these routing policies prefers Alternate-AT&T.

Another convention is to rank policies in increments of 10 at the start. This allows insertion of intermediately ranked policies without having to renumber all that would come later.

Note that when routing sessions, the Session Manager chooses the lower ranked routing policy for one of three reasons:

- SIP monitoring has declared all endpoints identified by the all higher ranked policies as down.
- This call fails to route (due to a bad return code or TimerB failure).
- This call fails to route due to managed bandwidth being exhausted to the destination location.

Routing Policy Details
Commit Cancel

General

Name: Alternate-AT&T

Disabled: ☐

Notes: 1-primary

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ATT	135.9.43.69	SIP Trunk	AT&T Flex Reach Global

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh

Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	10	All Day	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Select: All, None (0 of 1 Selected)

Routing Policy Details

CommitCancel

General

Name: Alternate-Verizon

Disabled: ☐

Notes: 2-secondary

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Verizon	sbc1.dr.avaya.com	SIP Trunk	Verizon Business

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item Refresh

Filter: Enable

	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	20	All Day	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Select: All, None (0 of 1 Selected)

Dial patterns for SIP service providers

The E.164 dial pattern entries exist mainly because our case study network is connected to the PSTN through SIP service providers. They fall into four categories, marked in the **Notes** field:

- APP route directly to a SIP foundation server (see below). These are marked.
- TEHO for Tail-End Hop-Off (see below)
- E.164 route DID numbers from the SIP service provider to the proper PBX. The relatively low number of entries of this type result from the PBXs in question *owning* the full bank of DID numbers (for example, the Westminster PBX owns all numbers +13035380000 to +13035389999). If this were not the case, the discrepancy could be solved with more entries, either with a larger set of more explicit ones to route fewer numbers to the given PBX, or with more explicit ones that route exceptions elsewhere (like the +13035389077 entry).
- PSTN (the + entries) are very general patterns which essentially match any E.164 number not matched by a more explicit entry.

As shown in all the adaptations, all the PBXs and incoming service provider calls have their destination addresses converted to E.164 (that is, a + is prepended), so that matching dial patterns can be more uniform and predictable.

Note that the first + entry in the table below is distinct from the second, because it only applies if the destination has a domain of avayalabs.com, while the second pattern matches any other domain.

The four entries:

Dial Patterns						
<input type="button" value="Edit"/> <input type="button" value="New"/> <input type="button" value="Duplicate"/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/> <input type="button" value="Commit"/>						
16 Items Refresh Filter: Enable						
<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
<input type="checkbox"/>	+18554528292	12	12	<input type="checkbox"/>	-ALL-	APP: GO AVAYA
<input type="checkbox"/>	+13035385077	12	12	<input type="checkbox"/>	-ALL-	APP: Modular Messaging
<input type="checkbox"/>	+1908953	12	12	<input type="checkbox"/>	-ALL-	E.164 to BaskingRidge:HQ
<input type="checkbox"/>	+19085965	12	12	<input type="checkbox"/>	-ALL-	E.164 to BaskingRidge:Research
<input type="checkbox"/>	+1720444	12	12	<input type="checkbox"/>	-ALL-	E.164 to HighlandsRanch
<input type="checkbox"/>	+1408561	12	12	<input type="checkbox"/>	-ALL-	E.164 to SanJose
<input type="checkbox"/>	+1303538	12	12	<input type="checkbox"/>	-ALL-	E.164 to Westminster
<input type="checkbox"/>	±	1	36	<input type="checkbox"/>	avayalabs.com	PSTN via SIP Service Providers
<input type="checkbox"/>	±	1	36	<input type="checkbox"/>	-ALL-	PSTN via SIP Service Providers
<input type="checkbox"/>	+1908	12	12	<input type="checkbox"/>	-ALL-	TEHO to BaskingRidge
<input type="checkbox"/>	+1303	12	12	<input type="checkbox"/>	-ALL-	TEHO to Westminster

Related topics:

[Simple routing policy for dial patterns for SIP service providers example](#) on page 40

[Alternative routing policy for dial patterns for SIP service providers](#) on page 41

Simple routing policy for dial patterns for SIP service providers example

The simple case dictates that any session destined for any E.164 address with the domain avayalabs.com routes only using the HypotheticalSP routing policy. In this case study the avayalabs.com domain is used by the BaskingRidge:Research SIP entity. Therefore all E.164 numbers that do not match any of the other patterns are routed using the HypotheticalSP SIP service provider.

Dial Pattern Details
Commit Cancel

General

Pattern:
 Min:
 Max:
 Emergency Call: ☐
 SIP Domain:
 Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	HypotheticalSP	<input type="checkbox"/>	HypotheticalSP	

Alternative routing policy for dial patterns for SIP service providers

This dial pattern entry performs two distinct route selections for all E.164 numbers (except those to the avayalabs.com domain). If the originating location is SanJose, then the HypotheticalSP service provider is used. Any other originating location selects (using alternate routing) the Alternate-AT&T and Alternate-Verizon routing policies.

Dial Pattern Details
Commit Cancel

General

* Pattern:
* Min:
* Max:
Emergency Call: ☐
SIP Domain:
Notes:

Originating Locations and Routing Policies

Add Remove

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	NA:US:CA:SanJose		HypotheticalSP	<input type="checkbox"/>	HypotheticalSP	
<input type="checkbox"/>	-ALL-	Any Locations	Alternate-AT&T	<input type="checkbox"/>	ATT	1 - primary
<input type="checkbox"/>	-ALL-	Any Locations	Alternate-Verizon	<input type="checkbox"/>	Verizon	2 - secondary

Select: All, None (0 of 3 Selected)

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

Tail-end hop-off

TEHO builds on the E.164 routing to the SIP service providers and relies on the same fundamental assumption that PBXs route their PSTN calls into the Session Manager core. Select E.164 patterns route first or exclusively to a PBX which has PSTN trunks of its own to handle the call. In this case study both BaskingRidge PBXs can handle calls to the 908 area code. The dial pattern entry identifies one of four route policies.

Dial Pattern Details

General

Pattern: +1908
 Min: 12
 Max: 12
 Emergency Call: ☐
 SIP Domain: -ALL-
 Notes: TENO to BaskingRidge

Originating Locations and Routing Policies

Add Remove

4 Items | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	Alternate-BaskingRidge:Research	<input type="checkbox"/>	NA:US:NJ:BaskingRidge:Research	prefer on Week Days
<input type="checkbox"/>	-ALL-	Any Locations	Alternate-BaskingRidge:HQ	<input type="checkbox"/>	NA:US:NJ:BaskingRidge:HQ	prefer on Weekends
<input type="checkbox"/>	-ALL-	Any Locations	Alternate-AT&T	<input type="checkbox"/>	ATT	1 - primary
<input type="checkbox"/>	-ALL-	Any Locations	Alternate-Verizon	<input type="checkbox"/>	Verizon	2 - secondary

Select: All, None (0 of 4 Selected)

The Alternate-AT&T and Alternate-Verizon entries were shown before. They have ranks for 10 and 20, respectively. The other entries Alternate-BaskingRidge:Research and Alternate-BaskingRidge:HQ are shown below to have time-of-day varying ranks.

Routing Policy Details

General

Name: Alternate-BaskingRidge:Research
 Disabled: ☐
 Notes: prefer on weekdays

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
NA:US:NJ:BaskingRidge:Research	135.9.43.68	CM	696-5

Time of Day

Add Remove View Gaps/Overlaps

2 Items | Refresh Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	1	Week Day	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	00:00	23:59	
<input type="checkbox"/>	2	Weekend	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Select: All, None (0 of 2 Selected)

BaskingRidge:Research has a rank of 1 on weekdays and a rank of 2 on weekends and BaskingRidge:HQ has a rank of 2 on weekdays and a rank of 1 on weekends.

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
NA:US:MD:BaskingRidge:HQ	135.9.43.57	CM	953

Time of Day

Add Remove View Gaps/Overlaps

2 Items | Refresh Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	1	Weekend	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	
<input type="checkbox"/>	2	Week Day	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	00:00	23:59	

Select: All, None (0 of 2 Selected)

Thus the routing policy (and so SIP entity) ordering is as such:

- Weekdays:
 - BaskingRidge:Research
 - BaskingRidge:HQ
 - AT&T
 - Verizon
- Weekends:
 - BaskingRidge:HQ
 - BaskingRidge:Research
 - AT&T
 - Verizon

It is desirable for the two BaskingRidge PBXs to be able to make use of the SIP service provider trunks even for 908 area code calls if their PSTN trunks are in use or out of service. To do this, and to make configuration of the PBXs routing simpler they route all their PSTN calls into the Session Manager core. A potential problem is when the 908 area code calls get routed back to them. If no consideration is made for this, the calls are simply routed back to the Session Manager core only to potentially loop back into the very same PBX. To avoid this, adaptation for the PBXs changes the destination address so that the PBX can recognize it as needing routing out of its PSTN trunk rather than back into the Session Manager core.

Adaptation for BaskingRidge:Research:

Digit Conversion for Outgoing Calls

3 Items | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*+1908	* 12	* 12	* 1	*9000	both	TEHO 000 => CM will use local
<input type="checkbox"/>	*+19086965	* 12	* 12	* 9		both	E.164 to 3-digit extension
<input type="checkbox"/>	*6965	* 7	* 7	* 4		both	EC to 3-digit extension

Select: [All](#), [None](#) (0 of 3 Selected)

The +1908 entry modifies all 908 area code numbers to be destined for *9-000-1-908-xxx-xxxx. The PBX must recognize this to be a specially routed number. In the case of this Communication Manager, the *9 is the ARS access code and the 000 is an otherwise nondialable digit string that can be used for this unique identification.

SIP foundation servers

The two SIP application types shown in this case study are Modular Messaging and Voice Portal. Both of these applications handle incoming and outgoing calls, although Modular Messaging primarily handles incoming calls. Like any SIP entity, adaptation for digit conversion can be used, but that is needed primarily for existing Modular Messaging or Voice Portal applications with existing dial plans. New applications can be provisioned to use the full length E.164 numbers (save possibly to delete and add the +) internally.

Related topics:

[Modular Messaging](#) on page 45

[Voice Portal-like SIP application service](#) on page 48

Modular Messaging

On each Communication Manager system, Modular Messaging is associated with a hunt group and assigned a routing digit string to route covered and direct sessions with media and a Voice Mail handle for message waiting indication subscriptions and notifications. Both types of sessions must be routed by Session Manager from each supported Communication Manager to the appropriate Modular Messaging system.

On the Communication Managers in this case study the following hunt group data is entered:

add hunt-group 1 Page 2 of 60

HUNT GROUP

Message Center: sip-adjunct

Voice Mail Number: 3035389077 Voice Mail Handle: xxx Routing Digits: *9
(e.g., AAR/ARS Access Code)

The number 3035389077 is routed through a dial pattern entry:

Dial Pattern Details Commit Cancel

General

* Pattern: +13035389077

* Min: 12

* Max: 12

Emergency Call: ☐

SIP Domain: -ALL-

Notes: APP:ModularMessaging

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	NA:ModularMessaging	<input type="checkbox"/>	NA:US:CO:Westminster:MM	

Select: All, None (0 of 1 Selected)

that identifies a SIP entity. CDR can be on, and it might be interesting to track calls into the Modular Messaging system, though the Modular Messaging system itself has an internal CDR capability. It may also be useful to implement bandwidth management on the Modular Messaging system in its own location, but it has also has a way of limiting calls. What is interesting is the load balancing between the multiple message access servers (MASs) within a Modular Messaging system. And in this particular case the local host name resolution table is used to provide the multiple IP addresses as well as the port and transport information needed to contact the MASs.

SIP Entity Details Commit Cancel

General

* Name: NA.US.CO.Westminster.MM

* FQDN or IP Address: mm.dr.avaya.com

Type: Other

Notes: MediatraMessaging

Location: NA.US.CO.Westminster

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

0 Items Refresh Filter: Enable

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
NA.US.CO	TCP	5060	NA.US.CO.West	5060	<input checked="" type="checkbox"/>
NA.US.NJ	TCP	5060	NA.US.CO.West	5060	<input checked="" type="checkbox"/>

With entity links from both the Session Managers, checking **Override Port & Transport with DNS SRV** on the SIP entity form indicates that both the Port and Protocol (aka Transport) on the SIP entity form are ignored. The convention used here is that a Port value of 1 indicates that both are ignored.

SRV records within the DNS server accessed by the Session Managers could be used to provide the necessary overridden information, but it is much easier to include this information in the Local Host Name Resolution table:

Local Host Name Resolution

This page allows you to add, edit, or remove local host name entries. Host name entries on this page will override information provided by DNS.

Local Host Name Entries

New Edit Delete

9 Items Refresh Filter: Enable

Host Name	IP Address	Port	Priority	Weight	Transport
<input type="checkbox"/> mm.dr.avaya.com	135.9.43.34	5061	1	10	TLS
<input type="checkbox"/> mm.dr.avaya.com	135.9.43.33	5061	1	20	TLS

In this particular case TLS connections are made to port 5061 of both of the MASs at the indicated IP addresses. Load balancing is done on a statistically weighted basis, because each MAS is at the same priority. About 10/30 (or one third) of the calls are given to the MAS at 135.9.43.34 while two-thirds of the calls go to the other. This ratio is valid over many calls. There is a possibility that for any given small set of calls, more or less than 1/3 of the calls go to the first MAS.

The message waiting indication subscribe and notify sessions are routed with the handle specified in Communication Manager (mm@avaya.com in this case). Handles are currently routed using the regular expressions table:

Regular Expression Details Commit Cancel

General

Pattern	Rank Order	Deny	Notes
*mm@avaya.com	0	<input type="checkbox"/>	

Routing Policy

Add Remove

1 Item | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	NA:ModularMessaging	<input type="checkbox"/>	NA:US:CO:Westminster:MM	

The pattern here is very precise with no meta character pattern matching symbols only because a specific handle needs to be matched. The fewer the meta characters, the more efficient the match. The routing policy selected by this match is the same one selected by the dial pattern of the number associated with the Communication Manager hunt group (that is, +13035389077).

Voice Portal-like SIP application service

The other SIP application service shown in this case study is similar to how calls are routed to a Voice Portal. The Voice Portal administration itself is not shown nor is this application fully set up to make outgoing calls. Adaptation would most likely be necessary for this.

This Voice Portal-like application is reached when 1-866-GO-AVAYA is dialed. The dial pattern is quite complex:

Dial Pattern Details

Commit Cancel

General

* Pattern: +18664528292

* Min: 12

* Max: 12

Emergency Call: ☐

SIP Domain: -ALL-

Notes: APP:GO AVAYA

Originating Locations and Routing Policies

Add Remove

6 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	APAC:JP:Tokyo:Shinjuku		App800 APAC 1	<input type="checkbox"/>	APAC:App800	1 APAC
<input type="checkbox"/>	APAC:JP:Tokyo:Shinjuku		App800 APAC 2	<input type="checkbox"/>	NA:US:App800	2 NA
<input type="checkbox"/>	APAC:AU:Sydney		App800 APAC 1	<input type="checkbox"/>	APAC:App800	1 APAC
<input type="checkbox"/>	APAC:AU:Sydney		App800 APAC 2	<input type="checkbox"/>	NA:US:App800	2 NA
<input type="checkbox"/>	-ALL-	Any Locations	App800 NA 2	<input type="checkbox"/>	APAC:App800	2 APAC
<input type="checkbox"/>	-ALL-	Any Locations	App800 NA 1	<input type="checkbox"/>	NA:US:App800	1 NA

Select: All, None (0 of 6 Selected)

Denied Originating Locations

Add Remove

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
<input type="checkbox"/>	NA:US:CA:SanJose	
<input type="checkbox"/>	NA:US:CO:Westminster	
<input type="checkbox"/>	NA:US:ND:BaskingRidge:Research	

To paraphrase the routing policy selection, without actually listing the routing policies themselves:

- SIP entities in the locations Tokyo and Sydney prefer the APAC:App800 foundation server (a SIP entity) and falls back to the NA:US:App800 server. There are, however, no SIP entities associated with these locations yet.
- All other SIP entities (including the ones defined in this case study PBX and SIP service provider alike) prefer the NA:US:App800 server.
- SIP entities in the SanJose, Westminster, and BaskingRidge:Research locations cannot route calls to this dial pattern. The calls are denied.

The SIP entities for the foundation servers are similar.

SIP Entity Details

Commit

Cancel

General

Name

APAC:App800

FQDN or IP Address

go.jp.avaya.com

Type

Voice Portal

Notes

APAC GO-AVAYA

Location

APAC:JP-Tokyo Shinjuku

Outbound Proxy

Time Zone

Asia/Tokyo

Credential name

SIP Link Monitoring

SIP Link Monitoring

Use Session Manager Configuration

Entity Links

Add

Remove

0 Items

Refresh

Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
	NA:US:NJ	TLS	5061	APAC:App800	1	<input checked="" type="checkbox"/>
	NA:US:CO	TLS	5061	APAC:App800	1	<input checked="" type="checkbox"/>

They have different FQDNs, are in different locations and time zones, but they both choose to override the port and transport specified in the entity link.

SIP Entity Details

Commit

Cancel

General

Name

NA:US:App800

FQDN or IP Address

go.avaya.com

Type

Voice Portal

Notes

MAIN GO-AVAYA

Location

NA:US:NJ

Outbound Proxy

Time Zone

America/New_York

Credential name

SIP Link Monitoring

SIP Link Monitoring

Use Session Manager Configuration

Entity Links

Add

Remove

0 Items

Refresh

Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
	NA:US:CO	TLS	5061	NA:US:App800	1	<input checked="" type="checkbox"/>
	NA:US:NJ	TLS	5061	NA:US:App800	1	<input checked="" type="checkbox"/>

The Local Host Name Resolution table shows why this override is necessary at least in the case of the NA:US:App800 SIP entity. The APAC:App800 SIP entity just has one associated IP address that uses the standard TLS port.

Local Host Name Entries						
<input type="button" value="New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/>						
9 Items Refresh Filter: Enable						
<input type="checkbox"/>	Host Name	IP Address	Port	Priority	Weight	Transport
<input type="checkbox"/>	go.avaya.com	135.9.95.101	55800	100	10	TCP
<input type="checkbox"/>	go.avaya.com	135.9.95.100	55800	100	30	TLS
<input type="checkbox"/>	go.avaya.com	135.9.43.29	55800	100	50	TLS
<input type="checkbox"/>	go.avaya.com	135.9.95.102	55800	100	10	UDP
<input type="checkbox"/>	go.jp.avaya.com	135.98.98.98	5061	100	100	TLS

The NA:US:App800 SIPentity chooses one of four different server IP addresses based on a total weight of 100. Ten percent of the time it goes to 135.9.95.101 with TCP, 30% to 135.9.95.100 with TLS, 50% to 135.9.43.29 with TLS, and the remaining 10% to 135.9.95.102 with UDP.

Chapter 3: A New User Setup Case Study

Overview

Fred Flintstone just joined our Highlands Ranch office. He is the new Network Engineer and will be working in the Network Management group. The following case study describes the necessary steps for adding Fred as a user and registering his user profile with a Session Manager for accessing enhanced enterprise call handling facilities through

- an application sequence (with CM feature server and other applications)
- modular messaging mailbox
- telephone set

thereby providing the option of choosing his preferred communication devices.

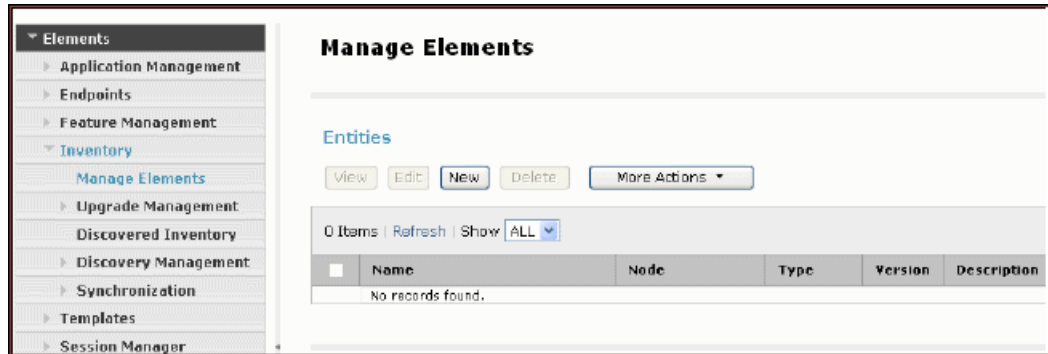
Before user setup is done, it is important to synchronize the CM Station Data to System Manager as shown in the section *Synchronize CM station data to the System Manager*. The various stages for the user setup are listed as follows:

1. Adding a SIP entity for the Session Manager (with listen ports)
2. Adding the Session Manager instances (for both primary and secondary Session Manager)
3. Adding SIP Domains
4. Adding Application Sequences
5. Adding Survivability Server
6. Adding Home Location
7. Adding a User (SIP end-point)

Synchronize Communication Manager station data to the System Manager

The Communication System Manager interface is used to synchronize Communication Manager station data to the System Manager database.

1. Each Communication Manager must be administered as an Entity using the Manage Elements web page located at **Elements > Inventory > Manage Elements** in the navigation menu. The main page shows all of the administered entities and for those corresponding to Communication Manager, the **Type** column indicates **CM**.



2. Click the **New** button and select **CM** to add a new Communication Manager entity. In the New CM Instance page, under the *Application* section, enter the name of the Communication Manager instance and specify the management IP address for the Communication Manager (the address that is used for SAT login) in the **Node** field.

New CM Instance

[Application](#) | [Port](#) | [Access Point](#) | [SNMP Attributes](#) | [Attributes](#) | [Expand All](#) | [Collapse All](#)

Application

*

Name

135.9.147.75

*

Type

CM

Reset

Description

*

Node

135.9.147.75

CM IP Address for SSH SAT Access

Port

Access Point

3. The default (none) is OK for the *SNMP Attributes* section.

4. Finally, the Communication Manager SAT login information must be configured in the *Attributes* section. For most users (for SSH SAT login), enter the SAT login in the **Login** field and the associated password in the **Password** field. Click the **Commit** button on the bottom of the page.

Attributes ▾

SSH SAT Login user and password

* **Login**

Password

Confirm Password

Is SSH Connection ☒

* **Port**

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Use defaults here for typical SSH SAT connection

Is ASG Enabled ☐

ASG Key

Confirm ASG Key

Location

5. Automatic CM Data Synchronization — After a Communication Manager has been added as an entity, it is automatically scheduled for an initial and subsequent incremental daily data synchronization. The synchronization status can be viewed for each Communication Manager using **Elements > Inventory > Synchronization > Communication System** in the navigation menu. Each Communication Manager is displayed in the table as shown below. The *Last Sync Time* column indicates the status of when the last data sync completed or the phase of synchronization for the current sync job in progress.

Synchronize CM Data/Launch Element Cut Through ⚙

2 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
<input type="checkbox"/>	135.9.147.75 cm14	135.9.147.75	Oct 22, 2009 02:00:28 AM -0600	Incremental	Completed		R015x.02.1.015.0
			Oct 22, 2009				

Adding a SIP entity for the Session Manager

1. You need to add a SIP entity as a Session Manager instance and hence you need to ensure that the SIP entity has been added in the Routing application as a SIP entity with type Session Manager.

SIP Entity Details [Commit] [Cancel]

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

[Add] [Remove]

0 Items | Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
--------------------------	--------------	----------	------	--------------	------	---------

Port

[Add] [Remove]

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	

Select : All, None (0 of 1 Selected)

* Input Required [Commit] [Cancel]

2. If not, you can create a SIP entity using **Routing > SIP Entities**.
3. You also need to specify Listen Port under Entity Links in Personal Settings screen.

Adding the Session Manager Instance

Add Session Manager
Commit Cancel

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

General

* SIP Entity Name NA:US:CO
Description
* Management Access Point Host Name/IP 135.9.95.8
* Direct Routing to Endpoints Enable

Security Module

SIP Entity IP Address
* Network Mask 255.255.255.0
* Default Gateway 135.9.95.8
* Call Control PHB 46
* QOS Priority 6
* Speed & Duplex Auto
VLAN ID

NIC Bonding

Enable Bonding
Driver Monitoring Mode ARP Monitoring
ARP Interval (msecs) 100 Link Monitoring Frequency (msecs) 100
ARP Target IP Down Delay (msecs) 200
ARP Target IP Up Delay (msecs) 200
ARP Target IP

Monitoring

Enable Monitoring

You need to administer the Session Manager (where Fred's phone will be registered) using **Elements > Session Manager > Session Manager Administration**.

Adding Domains

Domain Management

2 Items | [Refresh](#)

<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	avaya.com	sip	<input type="checkbox"/>	
<input type="checkbox"/>	avayalabs.com	sip	<input type="checkbox"/>	

Select : All, None

Fred's phone number is captured as a SIP handle as 538000@avaya.com where part of the SIP handle is a domain (avaya.com). Therefore, administer the domain using the Routing application (**Routing > Domains**). Enter the domain's name and select type *sip*

Adding Application Sequences

Fred can have an Origination Application Sequence and a Termination Application Sequence as his preferred way of handling calls. When a call is made from the user, a Session Manager will route the call through the origination sequence. Whereas when a call is made to the user, a Session Manager will route the call through the termination sequence. For details on configuring an Application Sequence, refer to the Call Handling Case Study.

Adding a Home Location

When this user calls numbers that are not associated with an administered user, dial-plan rules will be applied to complete the call based on this home location regardless of the physical location of the SIP device used to make the call.

**Note:**

Dial plan rules are applied using **Routing > Dial Patterns**.

Location Details [Commit] [Cancel]

General

* Name: NA:US:CO:Westminster

Notes:

Managed Bandwidth: 8000 Kbit/sec

* Average Bandwidth per Call: 80 Kbit/sec

Location Pattern

[Add] [Remove]

1 Item | Refresh Filter: Enable

	IP Address Pattern	Notes
<input type="checkbox"/>	* 135.9.43.66	

Select: All, None

Add a location using **Routing > Locations** as a Home Location element for Fred's Communication Profile. A Home Location can be specified to support mobility for the currently displayed user. A selection is mandatory.

Adding the Survivability Server

Prerequisites

To use a Branch Session Manager as a Survivability Server, you need to add a SIP entity of type "Session Manager".

For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura Core is lost. This is optional and is required only for survivability.

Add Branch Session Manager

General | Security Module | Monitoring | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All

General

* SIP Entity Name

bsm2-8300-sm

Description

*Management Access Point Host Name/IP

135.9.147.117

*Main CM for LSP

asm5-cm

Refresh

[View/Add CM Systems](#)

*Direct Routing to Endpoints

Enable

Adaptation for Trunk Gateway

None

Security Module

SIP Entity IP Address

*Network Mask

255.255.255.0

*Default Gateway

135.9.147.254

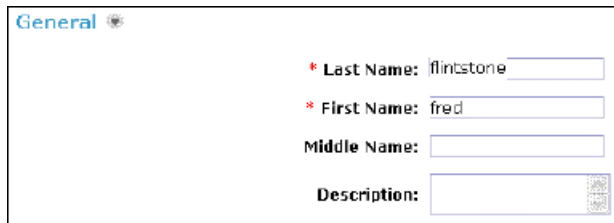
For administering Branch Session Manager as a Survivability Server, go to **Elements > Session Manager > Session Manager Administration** and click **New** on the *Branch Session Manager Instances* section of Session Manager Administration screen.

Adding a User (SIP end-point)

For basic setup of Fred's user profile, you need to complete the following sections in User Management application. Navigate to **Users > Manage Users** , click **New** and enter the following information:

1. General
2. Identity
3. Communication Profile
4. Default Contact List

General section



General

* Last Name: flintstone

* First Name: fred

Middle Name:

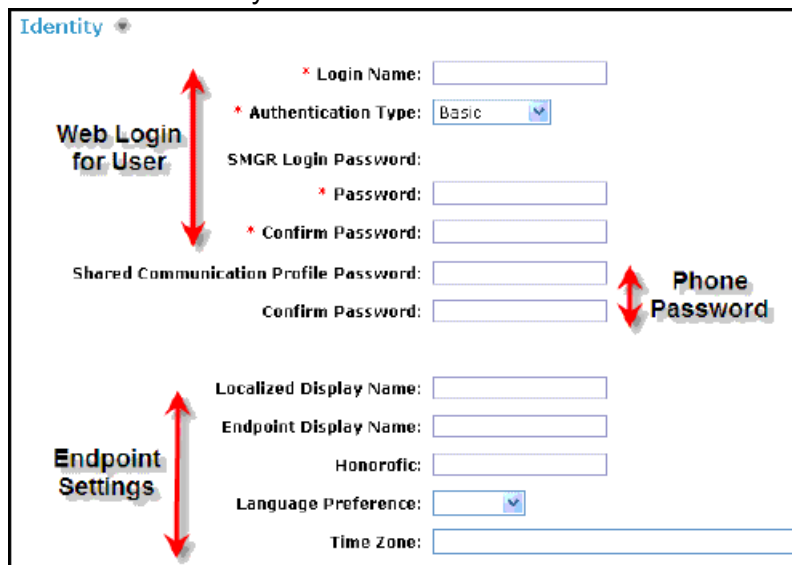
Description:

In User Management module, the general section allows you to specify the basic information about Fred's profile. In the General section,

1. Enter the Fred's last name and first name.
2. Enter a description in the Description field. This field is optional.

Identity section

1. Scroll to the Identity section.



Identity

* Login Name:

* Authentication Type: Basic

SMGR Login Password:

* Password:

* Confirm Password:

Shared Communication Profile Password:

Confirm Password:

Localized Display Name:

Endpoint Display Name:

Honorific:

Language Preference:

Time Zone:

Web Login for User

Phone Password

Endpoint Settings

2. Enter a **Login Name** for Fred. This is the unique system login name given to Fred and takes the form of *username@domain* (enterprise canonical number) which is used to create the Fred's primary handle.

3. Select the **Authentication Type** as *Basic*.
4. Enter an System Manager Login Password and confirm it. The password must start with an alpha (lower or upper case) character.
5. Enter the **Shared Communication Profile Password**. The password must be in numeric characters. This is the password that is used when logging in to the phone.
6. Enter the **Localized Display Name** of the Fred. This is the name that is displayed as the calling party.
7. Enter the full text name of the user for **Endpoint Display Name**.

Address section

In the Address section, add mailing address details of Fred in the Identity section.

The screenshot shows a web interface for managing addresses. At the top, there's a section titled "Address" with buttons for "New", "Edit", "Delete", and "Choose shared Address". Below this is a table with the heading "1 Item". The table has columns: Name, Address Type, Street, Locality Name, Postal Code, Province, and Country. One row is visible with the data: Fred Flintstone, office, and United States. At the bottom of the table, there's a selection bar that says "Select: All, None (0 of 1 Selected)".

Name	Address Type	Street	Locality Name	Postal Code	Province	Country
Fred Flintstone	office					United States

Communication Profile section

Fred may have one or more Communication Profiles for registering one or more SIP user handles (phone extensions) to the Session Manager. This will enable Fred to define (optional) an origination and termination application sequence as his preferred call routing method.

To register a SIP phone with Session Manager, at least one Communication Profile must be administered containing the Session Manager related details and must have defined at least one Communication Address of type SIP. The handles may also be associated with a Communication Manager station and/or messaging subscriber. You can specify the following information in Fred's Communication Profile:

A communication address can be used to communicate with the contact. This can be a phone number, e-mail address, SIP or IM of the contact. One or more communication addresses for Fred is defined in relation to handle plus domain in *userinfo@domainpart* format when routing a communication interaction to Fred. For Fred, the communication address is set as shown in

the figure below,

Communication Profile

New Delete Done Cancel

Name

Primary

Select : None

* Name: Primary

Default: ☒

Communication Address

New Edit Delete Users SIP handles (phone extensions)

Type	Handle	Domain
No Records found		

Type: Avaya SIP

* Fully Qualified Address: 5380000 Domain: avaya.com

Extension

Add Cancel

In Communication Address section,

1. Select **Type** which specifies the type of the handle which is set as *Avaya SIP*. Types are specified as followed:
 2. Enter the phone extension in the **Fully Qualified Address** field and finally select the correct domain from the drop-down menu.
- Handle is a unique communication address for Fred which is set as *5380000* and the name of the domain with which the handle is registered is set as *avaya.com*.

Session Manager section

☐ Session Manager Profile

* Primary Session Manager

Select

Secondary Session Manager

(None)

Origination Application Sequence

(None)

Termination Application Sequence

(None)

Survivability Server

(None)

* Home Location

Select

Primary	Secondary	Maximum

Primary	Secondary	Maximum

In the Session Manager Profile section, you can associate Fred with a Primary and Secondary Session Manager , specify Origination and Termination Application Sequences, a Survivability Server (e.g. Branch Session Manager), and also specify a Home Location for this user. Fred's phones will register with the selected Session Manager. Calls from or to Fred's phone will be routed through the selected origination or termination applications sequences respectively.

Home Location is a mandatory input field to support mobile users. Locations are administered using **Routing > Locations**.

Endpoint Profile section (CM Station association)

In Station Profile section, specify the Communication Manager station association for Fred as per the following cases:

☐ **Endpoint Profile**

* **System**

Use Existing Endpoints ☐

* **Extension**

* **Template**

Set Type

Security Code

* **Port**

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User ☐

☐ **Messaging Profile**

* **System**

Use Existing Subscriber on System ☐

* **Mailbox Number**

* **Template**

* **Password**

Delete Subscriber on Unassign of Subscriber from User ☐

1. Associate Fred with an existing station

1. Select the previously administered Communication Manager entity in the *System* drop-down menu.
2. Check the *Use Existing Endpoints* check box.
3. Enter (or select when prompted) the extension for the station.
4. Optionally, the template for the station, security code and/or port values for this station can be changed.

For a new station

2. Add a new station on the Communication Manager for Fred

-
1. Select the previously administered Communication Manager entity in the *System* drop-down menu.
 2. Enter (or select when prompted) the extension for the station.
 3. Select a phone template for the Fred's phone.
 4. Enter (or select when prompted) a value for the *Port*.
 5. Optionally, enter a value for the *Security Code*.
-

Messaging Profile section

In the Messaging Profile section, specify the association of a subscriber mailbox for Fred. You can include the following details:

-
1. Add messaging system on which you need to add Fred.
 2. Add template (system defined and user defined) you want to associate with Fred. Templates are defined in the *Communication System Management* module.
 3. Add mailbox number for Fred.
-

Default Contact List

Fred can optionally be given a default Contact List by expanding the Contact List section toward the bottom of the page and pressing the **Add** button to select already administered users as contacts.



These contacts are transferred to Fred's phone if the phone supports contacts feature.

Chapter 4: A Call Handling Case Study

Overview

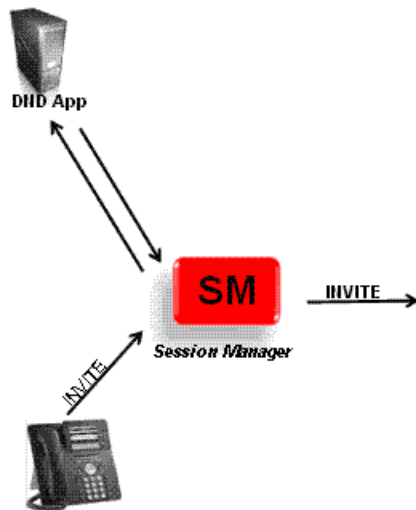
This case study shows call handling as per user's preferred set of applications using Application Sequence functionality or as per some enterprise dial pattern using Implicit User functionality. Some examples of such applications are as follows:

- Do-not call and selective call lists
- Caller-ID manipulation — Outsourcers or partners calling “on behalf of” their customer
- Conference bridge selector — Use built in 6-party conferencing first, then automatically switch to conference bridge (internal or hosted) if greater capacity needed
- Call Screener — Could be activated if user is in a meeting or depending on their presence status
- Selective call recording
- Call transcription/archiving

Scenario Definition

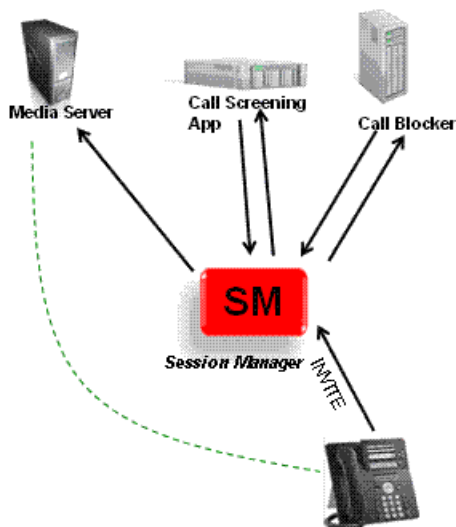
This scenario shows how a call from Barney for Fred is handled using Fred's Application Sequencing definition of his Communication Profile at Termination side.

Origination Side Sequencing



1. Barney makes an outbound call.
2. Session Manager signals the originating applications associated with Barney.
3. The DND Application (Do Not Call) verifies that the called party (Fred) is not listed in "Do Not Call" registry.
4. After verification, it forwards the call to Session Manager.
5. Session Manager sequences to the next application in the sequence

Termination Side Sequencing



1. Session Manager gets INVITE from Trunk.
2. Session Manager signals the Terminal Applications for the Called Party (Fred).
3. The Call Blocker application does not block call.

4. Session Manager signals the next application.
5. The call screening application checks Fred's status.
6. If Fred is Busy, call screening application forwards request to Media Server.
7. The Media Server plays custom message accordingly.

Using Application Sequence

Application Sequence functionality enables you to define and manage a set of applications for call sequencing as per user's Communication Profile. Some of the steps are outlined as follows:

-
1. You should setup application sequences before users are assigned.
 2. All applications should use Communication Manager as part of the sequence.
 3. Administer Communication Manager SIP entity beforehand using **Routing > SIP Entities**.
 4. Associate the user with a particular Session Manager instance and an application sequence as the originating and terminating sets as shown in the *New User Setup Case Study*.
-

Adding an Application (e.g. CM Feature Server)

-
1. Add the Feature Server SIP Entity — You need to add the Communication Manager feature server as a SIP Entity in the Routing application.
 2. Add the Application — The Communication Manager feature server can now be administered as an application using the Session Manager application.
 - For administering applications, use **Elements > Session Manager > Application Configuration > Applications**. The main page displays a list of currently administered applications. Click the **New** button to add a new

application.

Applications

This page allows you to add, edit, or remove applications for available SIP Entities.

Application Entries

[New](#)
[Edit](#)
[Delete](#)

9 Items [Refresh](#)

<input type="checkbox"/>	Application Name	SIP Entity	Description
<input type="checkbox"/>	DNDApp	DNDApp	
<input type="checkbox"/>	Media Server	Media Server	
<input type="checkbox"/>	Call Screening App	Call Screening App	
<input type="checkbox"/>	Call Blocker	Call Blocker	
<input type="checkbox"/>	ACM	ACM	

- Enter a name for the application as *ACM* and select the associated Communication Manager feature server for the SIP Entity input. Also select the CM System for this Communication Manager (you need to add an entity of type *CM* previously using **Elements > Inventory > Manage Applications**) for the data synchronization to System Manager.

Application Editor

Application Editor

*Name

*SIP Entity
"CM" from Routing > SIP Entities

*CM System for SIP Entity

view/Add CM Systems

Description

CM added on Elements > Inventory > Manage Applications (for data synchronisation to System Manager)

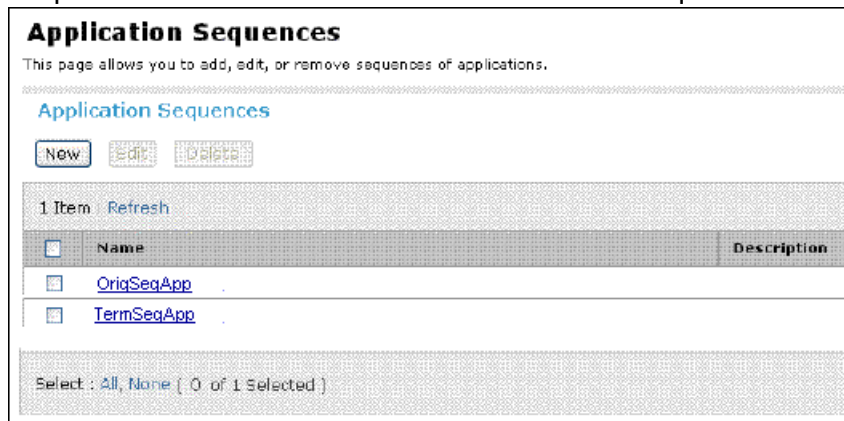
Add other applications to be added in the Fred's Application Sequence.

*** Note:**

By itself, an application cannot be associated with a user. Only application sequences consisting of one or more applications assigned in an order can be associated with a user for call routing.

Creating an Application Sequence from Existing Applications

1. The Application Sequences web page is located below the Applications page (**Elements > Session Manager > Application Configuration > Application Sequences**). The main page displays all currently administered Application Sequences. Press the **New** button to add a new sequence.



Application Sequences

This page allows you to add, edit, or remove sequences of applications.

[Application Sequences](#)

[New](#) [Edit](#) [Delete](#)

1 Item [Refresh](#)

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	OrigSeqApp	
<input type="checkbox"/>	TermSeqApp	

Select : [All](#), [None](#) (0 of 1 Selected)

2. Name the application sequence and click the (+) icon next to an available application (such as the Communication Manager Feature Server — ACM). Now, the selected application (ACM) will get added in the *Applications in this Sequence* table. This

suggests that ACM is now a part of the Application Sequence.

Application Sequence Editor [Commit] [Cancel]

Sequence Name

Name: TermSeqApp **Name the Sequence**

Description:

Applications in this Sequence

[Move First] [Move Last] [Remove]

1 Item **This table shows the current applications in the Sequence**

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		Media Server	Media Server	<input checked="" type="checkbox"/>	description

Select: All, None (0 of 1 selected)

Available Applications

9 Items Refresh **Click + to add an application in the application sequence** Filter: Enable

Name	SIP Entity	Description
+ DNDApp	DNDApp	
+ Media Server	Media Server	
+ Call Screening App	Call Screening App	
+ Call Blocker	Call Blocker	
+ ACM	ACM	

Checked means that calls will fail if they cannot be routed through this application

Administering Implicit Users

The Implicit User functionality allows routing calls to and/or from a specified dial pattern through application sequences. This is similar to specifying an origination and termination application sequence for a user, but it allows application sequencing to be applied to any dial pattern as opposed to a phone number for a user's registered phone. However at first, a match on an explicit users dial pattern is attempted. If no match is found, then an attempt is made to match on an implicit user. Some of the important points about Implicit Users are:

- Implicit users are not registered users
- Users can be on Third Party PBXs
- Also includes DCP, Analog or H.323 CM users
- Identified by phone numbers or extensions
- Can have Origination and Termination application sequences

To create an Implicit User rule:

1. From the navigation pane on the System Manager Common Console, click **Elements > Session Manager > Application Configuration > Implicit Users** to open the Implicit Users screen.

Implicit Users
This page allows you to define rules for implicit users.

Implicit User Rules

[New](#) [Edit](#) [Delete](#)

1 Item | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Pattern	Min	Max	SIP Domain	Origination Application Sequence	Termination Application Sequence	Description
<input type="checkbox"/>	3035384000	10	10	avaya.com		CM Feature Server	

Select: [All](#), [None](#) (0 of 1 Selected)

2. Click **New**. The Implicit User Rule Editor screen appears. The pattern, min and max input fields are similar to those on the Dial Pattern web page and are used to specify a dial pattern. The *SIP Domain* field allows restricting the origination and termination application sequencing to calls from or to a matching phone number on the specified domain only.

Implicit User Rule Editor [Commit](#) [Cancel](#)

Implicit User Rule Editor

* Pattern

* Min

* Max

Description

SIP Domain

Origination Application Sequence

Termination Application Sequence

*Required [Commit](#) [Cancel](#)

3. On the Implicit User Rule Editor screen, enter the appropriate information and click **Commit**.

Index

A

adaptations for PBXs	19
adding a Home Location	58
Adding a SIP entity for the Session Manager	56
adding an application	69
Adding Application Sequences	58
Adding Domains	58
Adding the Session Manager Instance	57
Adding the Survivability Server	59
administering Implicit users	72
alternative routing policy for dial patterns for SIP service providers	41
alternative routing policy for routing policies for SIP service providers	38
Application Sequencing Scenario	68
AT&T adaptation	30
Avaya Labs research PBX adaptation	21

C

core provisioning	11
creating an Application Sequence	71

D

dial patterns for PBXs enterprise canonical numbering	29
dial patterns for SIP service providers	39
domains	11

H

harmonizing disparate PBXs	18
hypothetical adaptation	32

L

legal notice	2
locations	15
locations with managed bandwidth	15
locations without managed bandwidth	16

M

Modular Messaging	45
-------------------------	--------------------

multiple interfaces	25
multiple SIP entities behind SBC	35

N

network, case study description	9
New User Setup	53
NJ HQ Communication Manager adaptation	20
non-Session Manager SIP entities	17

O

overview	7
----------------	-------------------

R

Routing	
case study	9
routing policies for PBXs	27
routing policies for SIP service providers	36

S

San Jose PBX adaptation	22
simple routing policy for dial patterns for SIP service providers example	40
simple routing policy for routing policies for SIP service providers	37
single interface	24
single SIP entity behind SBC	34
SIP entities for PBXs	24
SIP entities for Session Managers	12
SIP entities for SIP service providers	33
SIP entity for NJ Session Manager	13
SIP entity for Westminster Session Manager	12
SIP foundation servers	45
SIP service provider adaptations	30
SIP service providers	30
Synchronize CM station data to the System Manager	54

T

tail-end hop-off	42
time ranges	17

U	
Using Application Sequence	69
V	
Verizon adaptation	31
	Voice Portal-like SIP application service
	48
	W
	Westminster PBX adaptation
	19