Call Preservation Feature Description and Administration Guide

Release 6.2
Issue 2
August 2012

© 2012 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases

For full support information, please see the complete documents, ***Avaya Support Notices for Software Documentation***, **document number 03-600758 and *Avaya Support Notices for Hardware Documentation*, document number 03-600759.**

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not 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. Customer and/or 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. 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 through the following Web site:
http://www.avaya.com/support.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

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

1 Overview 5

1.1 Document scope 5

1.2 Component descriptions 6

1.3 Related resources 7

1.4 Terminology 7

2 Basic Call Center configuration 9

2.1 Call flow examples 10

2.1.1 New call after SM failure 10

2.1.2 SM fails while a call is in CM queue 10

2.1.3 SM fails while the call is in the “established” phase 12

3 Experience Portal Call Center configuration 13

3.1 Experience Portal Call Center Configuration with Intelligent Customer Routing (ICR) Service 14

3.2 Call flow examples 15

3.2.1 New call after SM failure 15

3.2.2 SM fails while the calls is in CM’s queue 16

4 Configuring Basic Call Center for Call Preservation 17

4.1 Configuration assumptions 17

4.2 Defining a Failover Group 17

4.3 Administering System Manager for Call Preservation 18

4.3.1 SIP Entity Administration 18

4.3.2 Adding a new Failover Group 19

4.3.3 Adding the peer SIP entities to the Failover Group 20

4.4 Administering Communication Manager for Call Preservation 21

4.4.1 Verifying Signaling Group and Trunk Group administration 22

4.4.2 Administering FGDN Route Patterns 24

4.4.3 Administering the Failover Group Domain Map 26

4.5 Administering Mediant™ 3000 for Call Preservation 27

4.5.1 Adding the FGDN to Internal DNS Tables 28

4.5.2 Creating a Proxy Set 31

4.5.3 Creating an IP Group Table 32

4.5.4 Configuring General Parameters 34
4.5.5 Configuring Proxy Settings 35
4.5.6 Configuring Routing Settings 36
4.5.7 Creating Routing Rules 37
4.6 Administering G860 for call preservation using an EMS Client 39
4.6.1 Adding the FGDN to Internal DNS Tables 39
4.6.2 Creating a Proxy Set 44
4.6.3 Creating an IP Group Table 46
4.6.4 Configuring General Parameters 49
4.6.5 Configuring Proxy Settings 50
4.6.6 Configuring Routing Settings 51
4.6.7 Creating Routing Rules 52
4.6.8 Administer Alternate Tel to IP settings: 53
5 Configuring Experience Portal Call Center for Call Preservation 54
5.1 Configuration assumptions 54
5.2 Configuring the system for Call Preservation 54
5.3 Administering Experience Portal for Call Preservation 54
5.3.1 Verify DNS server administration on Experience Portal 55
5.3.2 Adding and configuring a SIP connection for Call Preservation 55
Appendix 1 – Adding a FGDN to a corporate DNS server 58
Windows 2003 DNS Manager 59
Adding a forward lookup zone 59
Adding Host A-Records to the zone 60
Adding Service Location Records (SRV) 61
A DNS zone file example 63
Appendix 2 – FGDN Planning Worksheet 64

1 Overview

Leading the industry in SIP redundancy, Avaya announces a groundbreaking Call Preservation feature with Session Manager that is applicable for contact centers. The Avaya Aura® Call Preservation feature enables queued calls to be preserved across core Session Manager failures. Not only is the voice path of a connection preserved, but agents and users can also manipulate calls with in-call signaling after a Session Manager (SM) failure. For example, calls after a failure can be held, un-held, transferred, or conferenced, as users or work flows require.

Typically in a contact center, a large number of calls stay in-queue waiting for agents while the caller listens to announcements, wait treatment or music on hold. If a core SM is lost due to hardware or other failure, the Avaya Aura® Call Preservation feature prevents these calls from failing. By preserving the signaling path over a SM failure, these queued calls will still be properly connected to agents in the order they were received.

This feature organizes a pair of SM servers into a SM Failover Group and associates peer entities with the failover group. These peer entities support SM Call Preservation by utilizing enhanced SIP timing and recovery techniques to provide signaling path continuity in the event of a SM failure. Only such approved entities may be associated with a SM Failover Group.

Avaya Aura® Call Preservation leverages several IETF RFCs including RFCs 2782 and 3263 for locating SIP servers, RFC 3261 for core SIP and RFC 3262 for provisional response reliability. This feature preserves calls queued to H.323 agent endpoints only.

Note

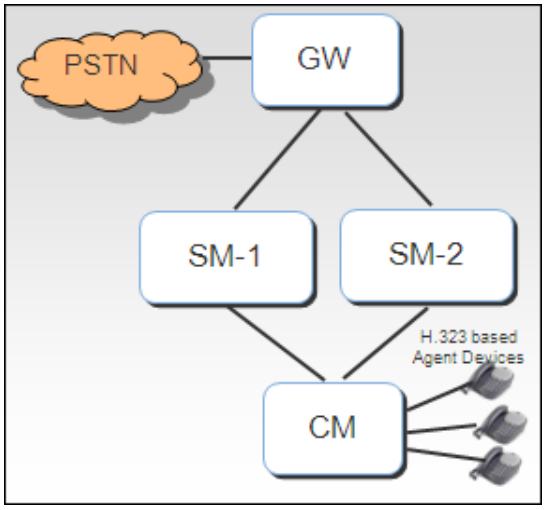
SIP endpoints follow a different redundancy and preservation scheme using dual registration; therefore SIP endpoints do not receive this Call Preservation treatment.

1.1 Document scope

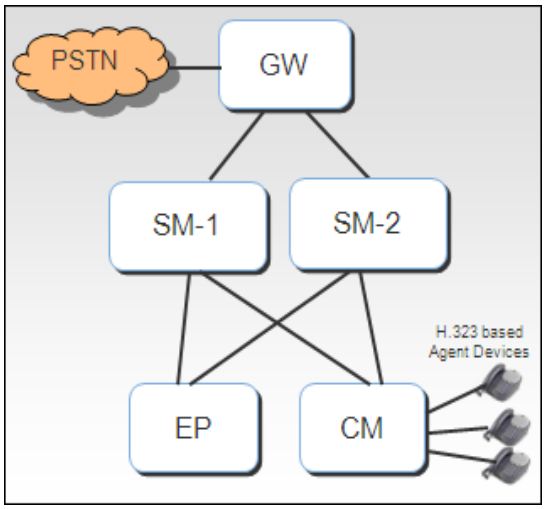
This document describes the Call Preservation feature administration for two Call Center configurations that include the following components only:

- PSTN-GW – G860 R3.0 Media Gateway available at http://support.avaya.com/products/P0481/g860-media-gateway/ for download.
- PSTN-GW – AudioCodes Mediant™ 3000 R2.0 Gateway (M3K) available at http://support.avaya.com/products/P0982/audiocodes-mediant-3000-gateway/ for download.
- EP - Avaya Aura® Experience Portal 6.0 available at http://support.avaya.com/products/P0407/avaya-aura-experience-portal/ for download.
- SM1/SM2 - Avaya Aura® Session Manager Release 6.2 available at http://support.avaya.com/products/P0533/avaya-aura-session-manager/ for download.
- CM – Avaya Aura® Communication Manager Release 6.2 available at http://support.avaya.com/products/P0001/avaya-aura-communication-manager/ for download.

Basic Call Center configuration:



Experience Portal Call Center configuration:



1.2 Component descriptions

- **Avaya Aura® Session Manager** is the core of Avaya's revolutionary Session Initiated Protocol (SIP) based architecture. The Session Manager platform makes it possible to unify media, modes, networks, devices, applications and real-time, actionable presence across a common infrastructure. Session Manager enables multi-vendor integration, centralized dial plans and user profiles, easier centralized SIP trunking, much easier "on-net" call routing, and greatly enhanced SIP scalability and security.
- **Avaya Aura® System Manager** centralizes provisioning, maintenance and troubleshooting to simplify and reduce management complexity and solution servicing. System Manager is used by administrators who centrally manage multiple Avaya applications and/or systems (for example, Communication Manager, Session Manager, etc.).
- **Avaya Aura® Communication Manager** software is the open, highly-reliable and extensible IP Telephony foundation on which Avaya delivers Unified Communications solutions to enterprises

large and small. It delivers rich voice and video capabilities and provides for a resilient, distributed network of gateways and analog, digital and IP-based communication devices. In addition, Avaya Aura® Communication Manager provides robust PBX features, high reliability and scalability, and multi-protocol support. It includes advanced mobility features, built-in conference calling and contact center applications, and E911 capabilities.

- **Avaya Aura® Experience Portal** is the latest major release of Avaya Voice Portal. Avaya Aura® Experience Portal provides organizations with a single point of orchestration of all automated voice and multimedia applications across inbound phone or video, as well as outbound, phone, email, or SMS applications. Intelligent Customer Routing (ICR) is a managed application, which runs on Avaya Aura® Experience Portal. ICR effectively handles customer calls for an organization by providing a self service facility. ICR provides the most optimal route for live assistance to the end consumer, which leverages resources of the enterprise.
- **AudioCodes Mediant™ 3000** is a feature rich high density SIP trunk gateway. The Mediant™ 3000 supports high-density PSTN interfaces, such as DS3. Large enterprises deploy business critical contact centers where the high availability of the Mediant™ 3000 is a key factor. The gateway is capable of directly interfacing with Session Manager using the SIP protocol for call establishment while still routing RTP traffic directly to the PBX or endpoints.
- **The G860 Media Gateway** is a high-density trunking gateway that supports up to 9 active DS3 interfaces in a single, 5U chassis. It uses SIP-based call control and integrates into Avaya Aura® Session Manager networks by leveraging SIP trunking. It has carrier grade, NEBS III-compliant reliability with redundant system elements and hot-swappable modules.

1.3 Related resources

For additional administrative support, go to http://support.avaya.com to access the following material referenced in this document:

- Administering Avaya Aura® Session Manager
- Mediant™ 3000 Setup Guide
- Avaya G860 Media Gateway Setup
- Administering Avaya Aura® Experience Portal
- Administering Avaya Aura® Communication Manager

1.4 Terminology

- **SM Failover Group** – An ordered collection of two SM instances that work collectively with SM failover group peer entities to provide end-to-end signalling path recovery and continuity in the event of a failure of one of the SMs.
- **SM Failover Group Peer Entity** – A SIP user agent (UA) entity that directly peers with SMs in a given SM failover group. The peer entity is administratively associated with the failover group on the Call Preservation Failover Group form in System Manager. Peer entities support SM Call Preservation by utilizing enhanced SIP timing and recovery techniques to provide signaling path recovery and continuity in the event of a SM failure. Only such approved entities may be associated with a SM Failover Group. A given peer entity may only be associated with a single failover group.

- **Primary SM** – The SM that will carry all new call preserved traffic in a sunny day scenario. It is the primary SM for new dialogs whenever it is running. The primary SM will also accept call preserved traffic that is rerouted from the secondary SM when it fails. It is administered on the Call Preservation Failover Group page in System Manager. In the administrative examples that follow, SM1 is the primary SM.
- **Secondary SM** – The SM that will carry new call preserved traffic in a rainy day scenario (i.e. when the primary SM is down). The secondary SM is the primary SM for new dialogs whenever the primary SM has failed. The secondary SM will also accept call preserved traffic that is rerouted from the primary SM when it fails. It is administered on the Call Preservation Failover Group page in SMGR. In the administrative examples that follow, SM2 is the secondary SM.
- **FQDN** – Fully Qualified Domain Name. A FQDN is a network based identification of a system and consists of the host name (including all sub-names) and the domain name, including the top level domain. The FQDN can be resolved into one or more IPV4 addresses by contacting a DNS server with an 'A' record query.

Note

Some peer entities, such as Avaya Aura® Communication Manager resolve FQDNs using administrative mechanisms in place of DNS. In the administrative examples that follow, sm1.avaya.com is the primary SM's FQDN and sm2.avaya.com is the secondary SM's FQDN.

- **FGDN** – Failover Group Domain Name. A fully qualified domain name (FQDN) that is resolvable into an ordered set of SM contacts within a SM failover Group. There are two FGDNs in use in a SM Failover Group. The primary SM uses a FGDN that prefers the primary SM over the secondary SM. The secondary SM uses a FGDN that prefers the secondary SM over the primary. The FGDN becomes part of the route set of SIP dialogs. Which FGDN is used depends upon which SM the dialog began on.

  The FGDN is resolved using RFC 3263 DNS procedures (i.e. by using SRV and A queries). Note: Some peer entities, such as Avaya Aura® Communication Manager resolve FGDNs using administrative mechanisms.
- **Primary FGDN** – A FGDN that resolves to an ordered set of SM contacts that prefers the primary SM over the secondary SM. In the administrative examples that follow, sm1-sm2.avaya.com is the primary FQDN.
- **Secondary FGDN** – A FGDN that resolves to an ordered set of SM contacts that prefers the secondary SM over the primary SM. In the administrative examples that follow, sm1-sm2-i.avaya.com is the secondary FQDN.
- **Failover Port** – A contact port on the SM assigned to carry call preserved traffic. There is one failover port assigned for TCP traffic and one port for TLS traffic.
- **Dialog Affinity** – From the perspective of the SM failover group peer entity, dialog affinity represents the SM in the failover group that the peer will send dialog related SIP messages to. It is also the SM that the peer entity expects to receive dialog messages from. It is possible for dialog affinity to change over the dialog's lifetime due to a SM failure.

  A peer entity maintains multiple simultaneous dialogs representing multiple simultaneous calls. It is possible that some dialogs will have different affinities based on their experience with SM failures over the lifetime of the dialog.
- **Preferred SM** – For SM failover group peers, the SM that currently has the dialog affinity. For

FGDNs, the SM with the top priority. The primary SM is initially the primary SM in for new calls in sunny day flows. If the primary fails or is failed when the dialog begins, then the secondary SM becomes the primary SM.

- **Alternate SM** – For SM failover group peers, the SM that doesn't have the dialog affinity. For FGDNs, the SM with the lower priority.
- **DNS** – The Domain Name System (DNS) enables name resolution of FQDNs to IP addresses for systems in a network. DNS also supports resolution of other queries notably the SRV query described in RFC 3263 and RFC 2782.

2 Basic Call Center configuration

This section describes the Call Preservation feature with a configuration involving an AudioCodes PSTN-GW, a pair of Session Manager instances (SM1 and SM2), and a Communication Manager (CM). In this configuration, PSTN-GW directs a call over a SIP trunk to Session Manager (SM1). The call is routed by SM1 to CM. Here is the flow of a typical incoming call in the sunny day scenario.

1. PSTN-GW receives the customer call routed through the PSTN trunk.
2. PSTN-GW directs the call to SM1 via SIP.
3. Session Manager routes the call to CM via SIP.
4. CM routes the call to the agent stations.

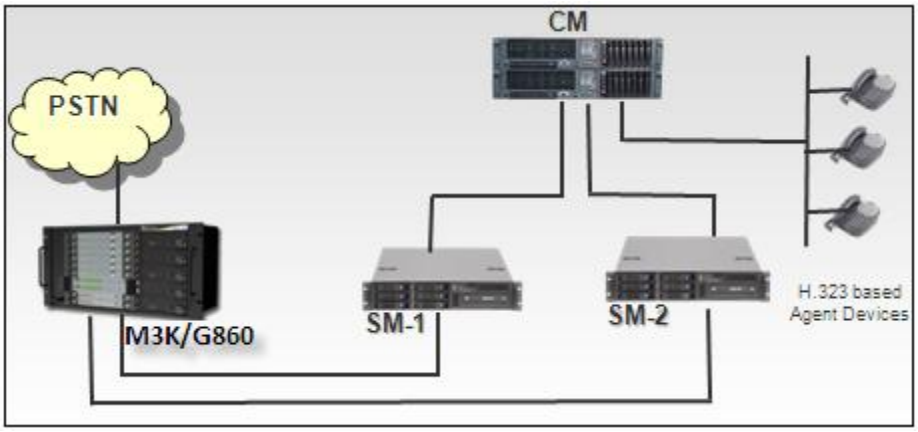


Figure 1: Basic Call Center configuration

Without Call Preservation administered, calls in-progress or in-queue drop during a SM failover. With Call Preservation administered, if the primary Session Manager (SM1) fails, peer entities (PSTN-GW and CM) detect the outage of the primary Session Manager (SM1) and will reroute traffic to the secondary Session Manager (SM2) without dropping calls belonging to the failover group.

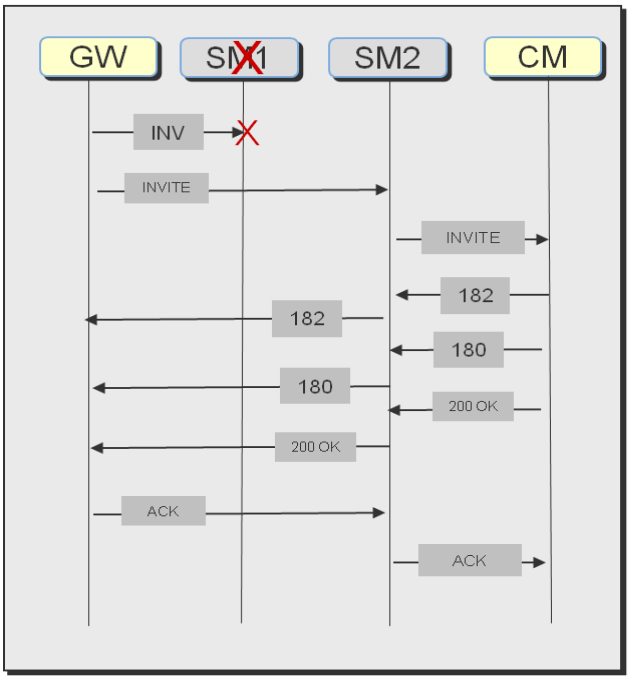
As different calls may be in different phases when the primary SM goes down, the following subsection describes the operation of Call Preservation in different phases. For example, new calls, calls in queue, and calls in active/established phase.

2.1 Call flow examples

2.1.1 New call after SM failure

Figure 2 is an example of a Session Manager failure just before a new call begins.

1. SM1 fails.
2. As the PSTN-GW has not yet detected the SM1 failure, the PSTN-GW routes the inbound call from the PSTN to the primary Session Manager (SM1).
3. Upon detecting the outage, the PSTN-GW reroutes the traffic to the secondary Session Manager (SM2).
4. SM2 routes the request to the destination (CM).
    - For this call, SM2 becomes the preferred Session Manager for both the source and destination peer entities (PSTN-GW and CM). Both peers establish initial affinity for the existing call to SM2.
    - If SM1 is later restored, new dialogs start via SM1. However, dialog affinity for the existing dialogs managed by the peer entities ensure that the existing mid-dialog traffic stays with SM2.
    - Only if SM2 fails, will the existing mid-dialog dialog traffic converge on SM1.
5. Subsequent requests and responses for the existing call are routed via SM2.



SM1 goes down before the call is routed. The call is routed and established via the alternate SM (SM2)

***Note**: For brevity, only prominent SIP messages are shown.*

Figure 2: Session Manager failure before the initial request

2.1.2 SM fails while a call is in CM queue

Figure 3 is an example of how Call Preservation works when a Session Manager fails while a call is in the CM queue.

1. The PSTN-GW is processing an inbound call from the PSTN for routing to the primary Session Manager (SM1).
2. The Primary Session Manager routes the call to CM.
3. The caller is waiting in queue for the agent's availability when the primary SM fails. The call is not yet established (not in the conversation phase).
4. SM1 fails.
5. CM detects the failure of the primary Session Manager (SM1) when a subsequent response (180 in this case) times out.
6. Upon detecting the outage of SM1, CM reroutes the response via the secondary Session Manager (SM2).
7. With the Call Preservation feature, SM2 successfully forwards the response to the source (PSTN-GW).
    - For this call, SM2 becomes the preferred Session Manager for both the source and destination peer entities (PSTN-GW and CM). Both peers establish initial affinity for the existing call to SM2.
    - If SM1 is later restored, new dialogs start via SM1. However, dialog affinity for the existing dialogs managed by the peer entities ensure that the existing mid-dialog traffic stays with SM2.
    - Only if SM2 fails, will the existing mid-dialog dialog traffic converge on SM1.
8. Subsequent requests and responses for this call are routed via SM2.

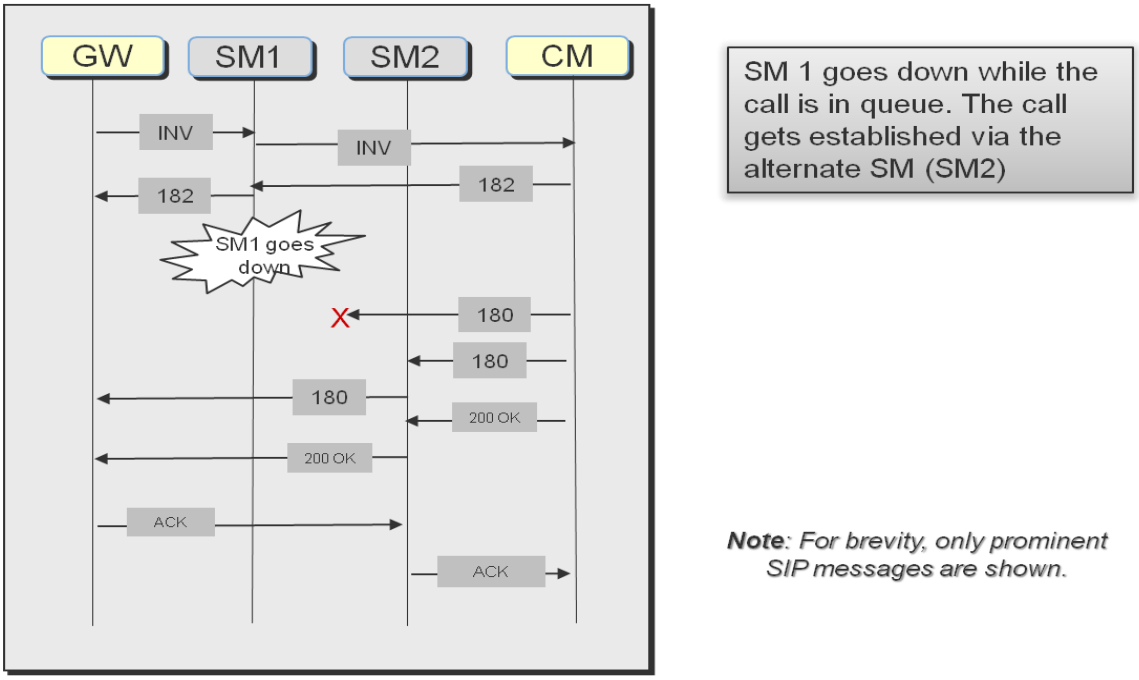


Figure 3: Session Manager failure when the call is in queue

2.1.3 SM fails while the call is in the "established" phase

Figure 4 shows a typical incoming call scenario where the caller is talking to the agent when the primary SM (SM1) fails. The call is established via SM1 before SM1 goes down. The INVITE transaction (that is, INVITE, 200 OK, ACK) has taken place via SM1.

1. SM1 fails while the caller is talking with the agent.
2. CM detects the failure of the primary Session Manager (SM1) when a subsequent mid-dialog request (like a session refresh request) times out.
3. CM reroutes the request via the secondary Session Manager (SM2).
4. With the Call Preservation feature, SM2 successfully forwards the response to the source (PSTN-GW).
    - For this call, SM2 becomes the preferred Session Manager for both the source and destination peer entities (PSTN-GW and CM). Both peers establish initial affinity for the existing call to SM2.
    - If SM1 is later restored, new dialogs start via SM1. However, dialog affinity for the existing dialogs managed by the peer entities ensure that the existing mid-dialog traffic stays with SM2.
    - Only if SM2 fails, will the existing mid-dialog dialog traffic converge on SM1.

Subsequent requests and responses for this call are routed via SM2.

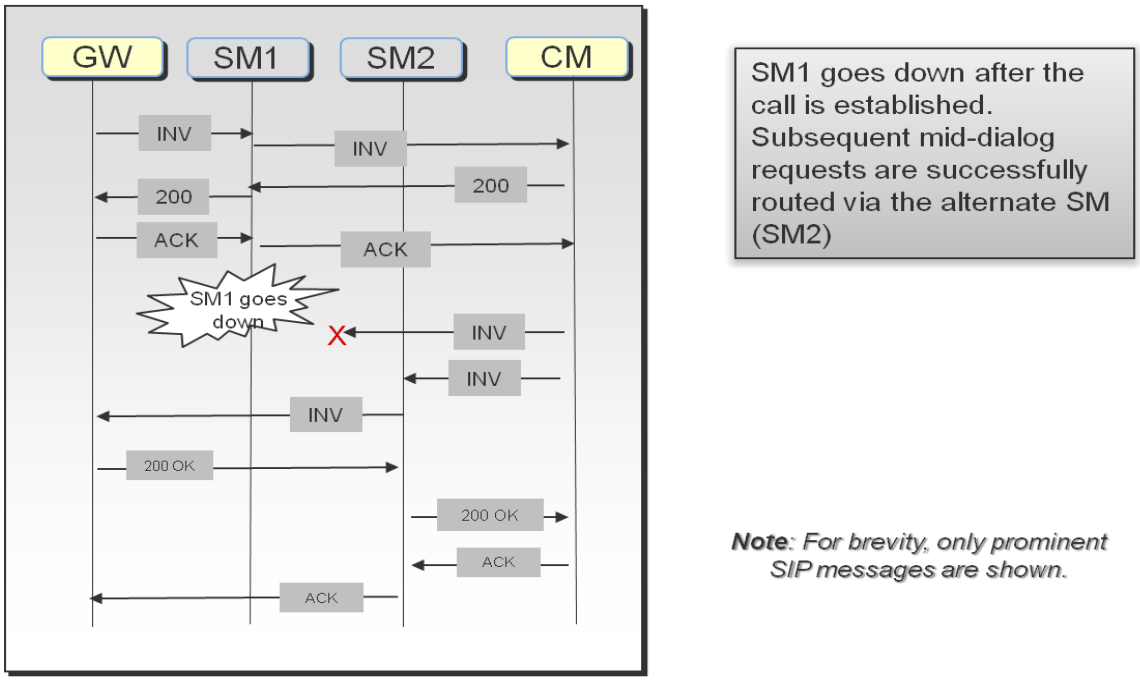


Figure 4: Session Manager failure after the call is established

While the peer entities in the above examples have used the timeout of the call related messages (request and response) to detect the outage of the primary Session Manager, the peer entity may detect the outage using other means, like SIP OPTIONS pinging.

3 Experience Portal Call Center configuration

This section describes the Call Preservation feature with a configuration involving an AudioCodes PSTN-GW, a pair of Session Manager instances (SM1 and SM2), an Experience Portal (EP), and a Communication Manager (CM). In this configuration, the PSTN Gateway (PSTN-GW) directs a call over a SIP trunk to SM1. SM1 routes the call to EP for customer self service (interactive voice response - IVR). After completing self service, the customer may opt to speak to a contact center agent, at which point the call is routed by SM1 to CM. Refer to the following sunny day scenario:

1. PSTN Gateway (PSTN-GW) receives the customer call routed through the PSTN trunk.
2. PSTN-GW directs the call to SM1.
3. SM1 routes the call to EP which begins the Self Service workflow.
4. Customer desires to talk to an agent and selects the appropriate option from the workflow.
5. EP redirects the call to CM via SM1.
6. CM places the call in a queue.
7. When the agent becomes available, CM routes the call to the agent stations.
8. Upon detecting agent's availability, EP redirects PSTN-GW to place a call to the agent (CM) replacing the call between EP and CM.
9. PSTN-GW establishes the call with CM (agent) via SM1.

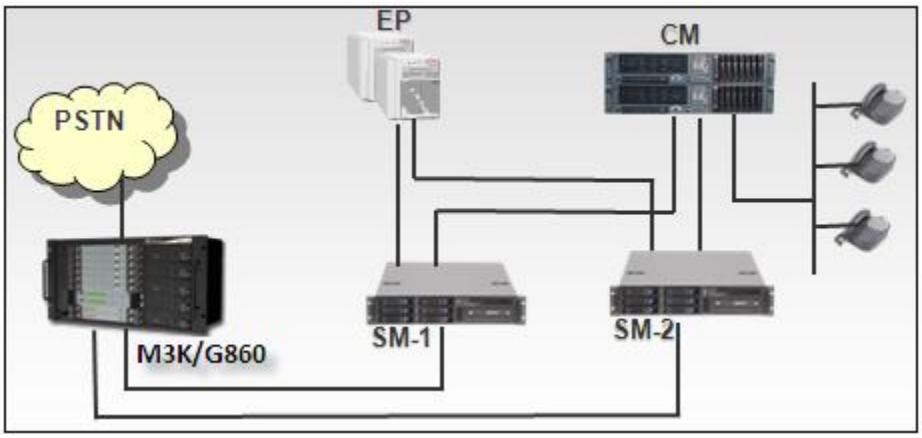


Figure 5: Experience Portal Call Center configuration

Without Call Preservation administered, calls in-progress or in-queue drop during a SM failover. With Call Preservation administered, if the primary Session Manager (SM1) fails, peer entities (PSTN-GW, EP and CM) detect the outage of the primary Session Manager (SM1) and will reroute traffic to the secondary Session Manager (SM2) without dropping calls belonging to the failover group.

As different calls may be in different phases when the primary SM goes down, the following subsection describe the operation of Call Preservation in different phases. For example, new calls and calls in active/established phase.

3.1 Experience Portal Call Center Configuration with Intelligent Customer Routing (ICR) Service

ICR is an optional application available with EP. In an ICR based configuration, a typical customer call enters through the PSTN Gateway (PSTN-GW). The PSTN-GW delivers the call to one of the Session Managers (say, SM1 in the sunny day). SM then routes the call to EP for customer self service using interactive voice response interaction. During the self service, the customer may opt to speak to a contact center agent, at which point self service application contacts the ICR Core for the optimal routing. The ICR Core determines which CM can provide the best service for the customer. The ICR Core sends a polling INVITE request to the preconfigured VDNs to get the Estimated Wait Time (EWT) from CMs. Once the analysis is done, the ICR places a no media call in queue on CM. The customer media streams remains on EP until an agent becomes available. Once an agent is available, EP connects the caller with the agent by referring the PSTN-GW to CM.

Without the Call Preservation feature, the calls in-progress or in-queue drop during a SM failover. With Call Preservation, if the primary Session Manager (SM1) fails, peer entities (PSTN-GW, EP, ICR and CM) detect the outage of the primary Session Manager (SM1) and will reroute traffic to the secondary Session Manager (SM2) without dropping calls belonging to the failover group.

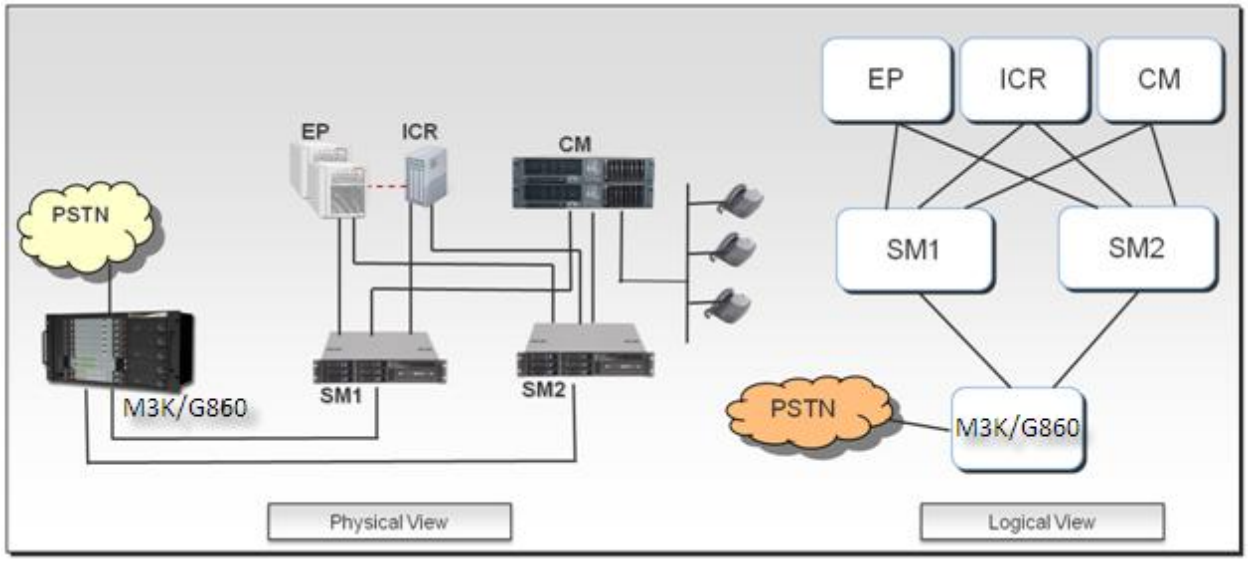


Figure 6: Experience Portal Call Center with ICR configuration

The main difference between the ICR flow and EP flow is the polling INVITE dialog between ICR and CM. In the ICR solution, the ICR Core fetches the EWT from CM by sending a polling INVITE request. If primary SM fails during this transaction and the request times out, the ICR Core launches another request via the alternate SM. The retry to get the EWT does not impact the user experience. The ICR calls at EP (with media) and queued calls at CM (without media) continue to be preserved.

3.2 Call flow examples

3.2.1 New call after SM failure

Figure 7 is an example of a Session Manager failure just before a new call begins.

1. SM1 fails.
2. As the PSTN-GW has not yet detected the SM1 failure, the PSTN-GW routes the inbound call from the PSTN to the primary Session Manager (SM1).
3. Upon detecting the outage, the PSTN-GW reroute the traffic to the secondary Session Manager (SM2).
4. SM2 routes the request to the destination (EP).
    - For this call, SM2 becomes the preferred Session Manager for both the source and destination peer entities (PSTN-GW and EP). Both peers establish initial affinity for the existing call to SM2.
    - If SM1 is later restored, new dialogs start via SM1. However, dialog affinity for the existing dialogs managed by the peer entities ensure that the existing mid-dialog traffic stays with SM2.
    - Only if SM2 fails, will the existing mid-dialog dialog traffic converge on SM1.

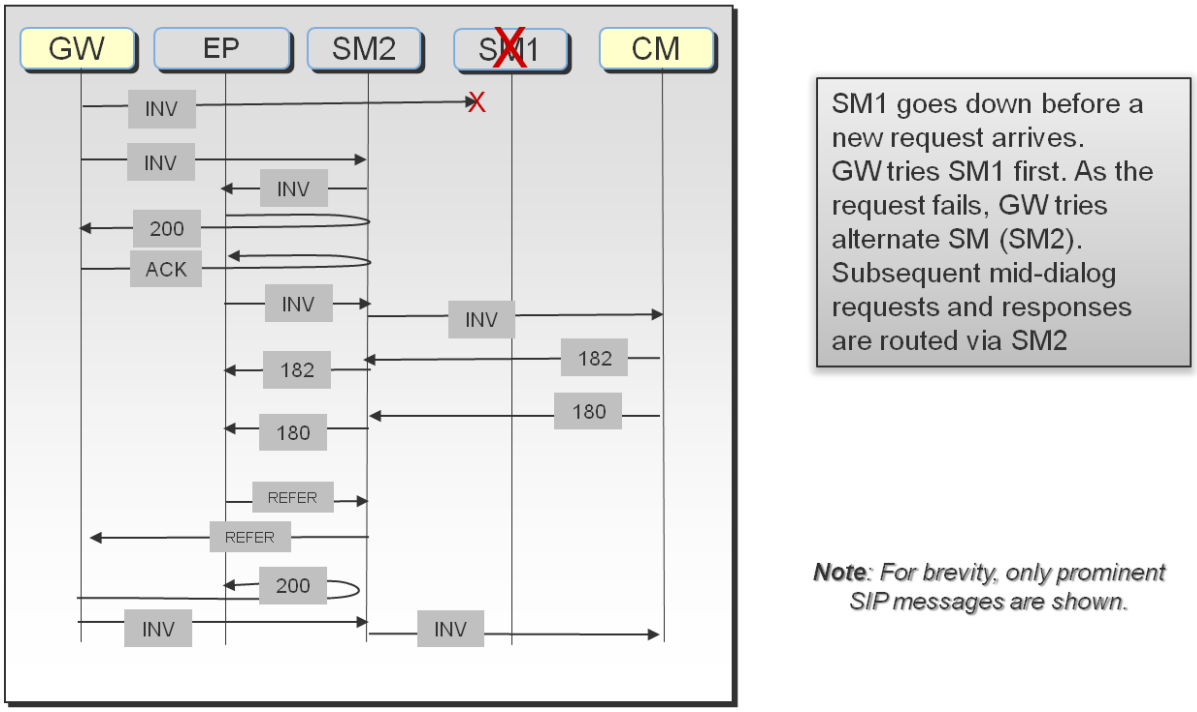


Figure 7: Session Manager failure before the initial request

3.2.2 SM fails while the calls is in CM's queue

Figure 8 is an example of an established call that begins before the primary Session Manager (SM1) fails.

1. The caller is waiting in the queue for the agent's availability when the primary Session Manager (SM1) fails. The call is not yet established.
2. The initial request is routed from the PSTN-GW to EP via SM1.
3. Upon receiving caller's intent to speak with an agent, EP launches a call towards CM via SM1.
4. SM1 goes down.
5. CM detects the outage of the primary Session Manager (SM1) when the response acknowledgement times out. CM reroutes the response via the secondary Session Manager (SM2).
6. With the Call Preservation feature, SM2 successfully forwards the response to the source (EP)
    - For this call, SM2 becomes the preferred Session Manager for PSTN-GW, EP, and CM. These peers establish initial affinity for the existing call to SM2.
    - If SM1 is later restored, new dialogs start via SM1. However, dialog affinity for the existing dialogs managed by the peer entities ensure that the existing mid-dialog traffic stays with SM2.
    - Only if SM2 fails, will the existing mid-dialog dialog traffic converge on SM1.
7. EP then redirects PSTN-GW to CM via SM2.
8. PSTN-GW establishes the call with the agent (CM) via SM2.

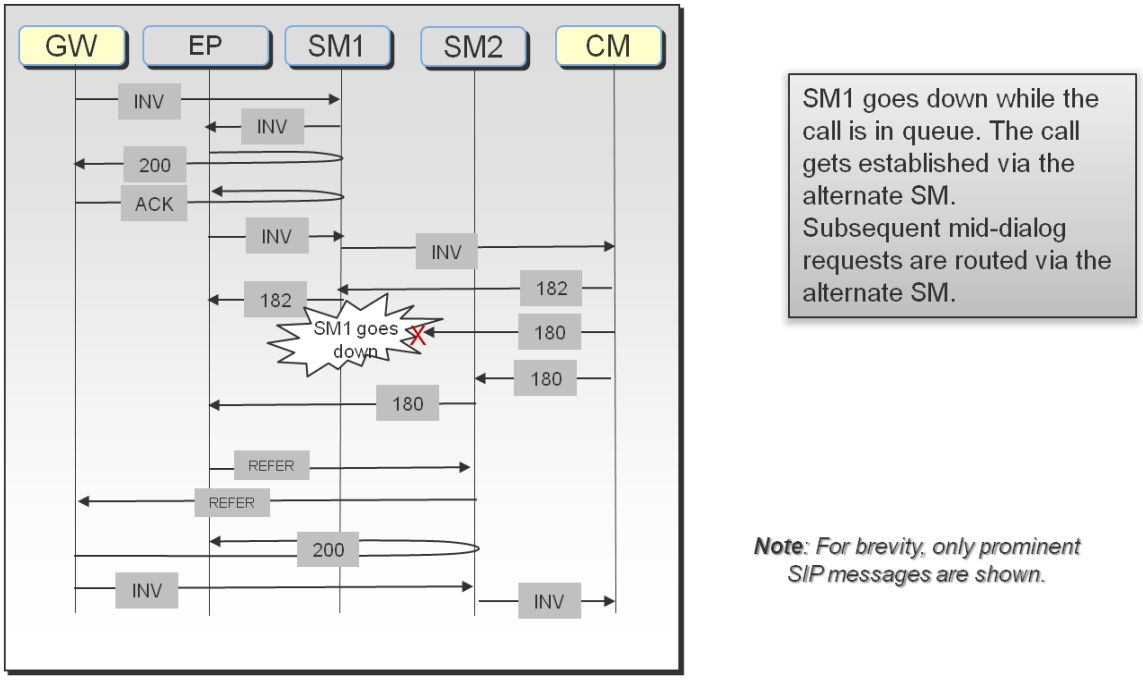


Figure 8: Session Manager failure while the call is in CM's queue

4 Configuring Basic Call Center for Call Preservation

4.1 Configuration assumptions

- Minimum software requirements are met by all components. Refer to section 1.1 Document Scope for release requirements.
- The PSTN Gateway is installed and configured. Connectivity to the PSTN is established and operational.
- Session Manager 1 (SM1)/ Session Manager 2 (SM2) are installed, configured and operational.
- Communication Manager is installed, configured and operational.

Note

Call routing administration, for the above components, is not covered in this document. Refer to section 1.3 Related Resources for basic system and SIP administration support.

4.2 Defining a Failover Group

- Refer to the Terminology section 1.4 for a definition of Failover Group Domain Name (FGDN) which is required for Call Preservation administration.
- Define your primary FGDN and secondary FGDN and record these names on the FGDN Planning Worksheet in Appendix 2. These names must be consistently administered for each product belonging to the failover group.
- The FGDN naming convention identifies the primary Session Manager's SIP Entity hostname, then the secondary Session Manager's SIP Entity hostname, followed by the SIP domain name. Use the planning worksheet to determine how to locate **SM1/SM2 SIP Entity** and the **SIP domain** information.
- Throughout this document, examples are given to assist with administrative decisions. The planning worksheet lists the reference information you will need during administration, a description for what each reference item is, how to locate it, and the example value used during administration. The FGDN example used throughout this document is:

  The primary FGDN: sm1-sm2.avaya.com.

  The secondary FGDN: sm1-sm2-i.avaya.com.

Note

It is not advised to use a secondary FGDN naming convention such as sm2-sm1.avaya.com because that implies SM2 is the primary SM in the failover group, which can be misleading. The secondary identifier (-i in this example) can be anything.

Other examples are: -inverse, -secondary or -alternate.

- It is recommended that you review the FGDN Planning Worksheet in advance to determine other design decisions, such as consistent port IDs for TCP and TLS transport used by all components, use of external DNS or internal DNS administration, and deciding the peer entities that will be allowed in the failover group. Regardless, each administration section will guide you through the process of populating required information.

4.3 Administering System Manager for Call Preservation

Worksheet references

1. The following references will be needed from the FGDN Planning Worksheet in Appendix 2.
    - Failover Group Name
    - SM1 SIP entity
    - primary FGDN
    - SM2 SIP entity
    - secondary FGDN
    - CM SIP entity name
    - PSTN-GW SIP entity name
    - EP SIP entity name
    - SM1 preferred transport
    - SM2 preferred transport
    - SM1 TLS failover port
    - SM2 TLS failover port
    - SM1 TCP failover port
    - SM2 TCP failover port

4.3.1 SIP Entity Administration

Pre-existing SIP entity and entity link administration is assumed.

Procedure

1. On the System Manager console, navigate to **Elements>Routing>SIP Entities** in the left navigation pane to open **SIP Entities**. For each Session Manager entity involved in the failover group (SM1/SM2), add TCP and TLS failover port IDs and **commit** the changes. **(SM1 TCP failover port, SM1 TLS failover port, SM2 TCP failover port, SM2 TLS failover port** from the worksheet). Example: TCP 5060, TLS 5061. The failover port identification is specific to Call Preservation.
2. If SM1 and SM2 do not already have both TCP and TLS entity links administered between them, add the missing link under **Routing>Entity Links**. The transport type port IDs must match the failover port IDs administered in each SM SIP Entity in the previous step. Call Preservation requires both TCP and TLS transport links between SMs.
3. Verify under **Routing>Entity Links** that the peer entities being used in the failover group have links to each SM using the same TCP or TLS port ID as administered in SM SIP Entity failover ports. One transport type is sufficient for entity links between SM's and the peer devices.

4.3.2 Adding a new Failover Group

Procedure

1. On the System Manager console, navigate to **Elements> Session Manager**>**Network Configuration >Failover Groups** in the left navigation pane to open the **Failover Groups** administration page (Figure 9).
2. To add a new Failover Group entry, click **Add**.
3. Enter the appropriate information from the FGDN Planning Worksheet on the **Edit Failover Group** page (Figure 10) as instructed below.
   - Enter a descriptive name representing the Failover Group in the **Group Name** field, such as sm1-sm2 in this example. (**Failover Group Name**)
   - In the Session Manager 1 section:
     i. Enter the primary FGDN name, as identified in the FGDN Planning Worksheet, in the **Preferred Domain Name** field. (**primary FGDN**)
     ii. Select the primary Session Manager of the primary FGDN in the **Session Manager** drop down box. (**SM1 SIP entity**)
   - In the Session Manager 2 section:
     i. Enter the secondary FGDN name, as identified in FGDN Planning Worksheet, in the **Preferred Domain Name** field. (**secondary FGDN**)
     ii. Select the secondary Session Manager of the secondary FGDN in the **Session Manager** drop down box. (**SM2 SIP entity**)

   Note

   Review your administration carefully before committing. Make sure you have administered the correct FGDN names (primary and secondary) and selected the appropriate Session Managers for this Failover Group.

4. Click **Commit**. If the required failover ports have not been administered, the commit operation will fail and the audit result will provide a link to the appropriate administration page to enter the required information. If the required entity links are not present the **Session Manager Entity Link Audit** page indicates which required links are missing and must be added to ensure failover service. This audit result also provides the ability to automatically add the appropriate administration by selecting **Commit** on this audit page.

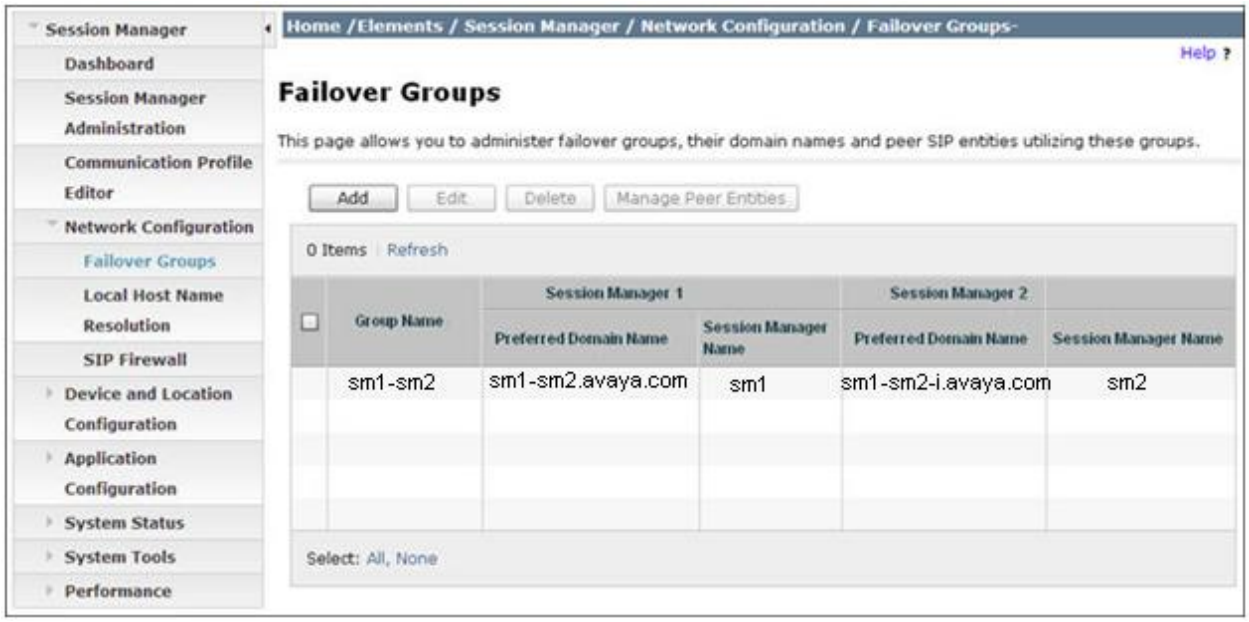


Figure 9: Failover Group Web page

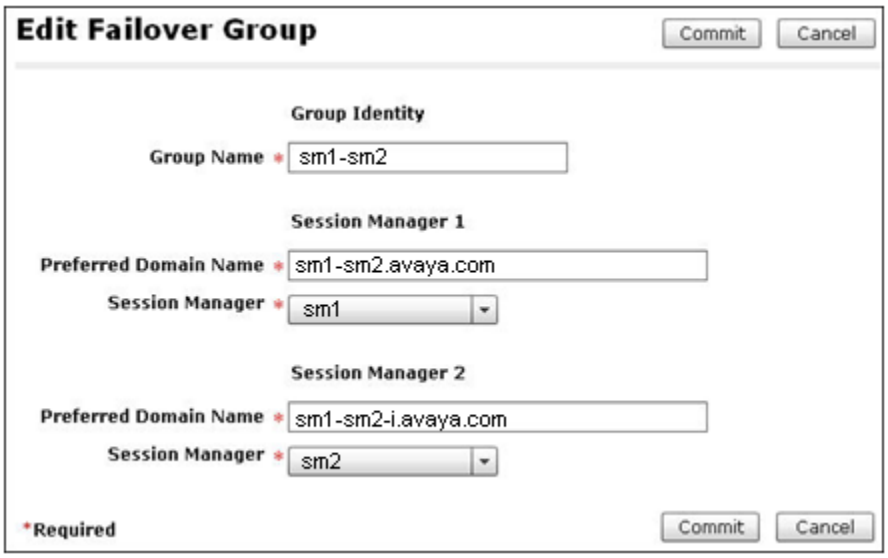


Figure 10: Edit Failover Groups page

4.3.3 Adding the peer SIP entities to the Failover Group

This section provides the basic steps for adding peer SIP entities associated with the respective Failover Group. You can add or remove one or more peer SIP entities within the Failover Group. The peer SIP entities displayed during the add operation adhere to the following criteria:

- A peer SIP entity can be associated with only one Failover Group. Thus, when you want to add peer SIP entities, only those not associated with any other Failover Group are displayed.

- “Session Manager” type entities are not displayed.

Note

Only the supported components listed in section 1.1 qualify as managed peer entities. Select only qualified entities.

Procedure

1. From the main **Failover Group** page, select the respective check box for the Failover Group and click **Manage Peer Entities** to open the **Manage SIP Entities** page.
2. Click **Add** to select from the list of all previously administered SIP entities.
3. On the **Add Peer SIP Entities** page, select the respective qualified SIP entities to be added to the Failover Group. (**CM SIP entity; PSTN-GW SIP entity; EP SIP entity***).

   *optional depending on configuration; required for EP Call Center configuration”
4. Click **Add Selected** for associating the selected peer SIP entities with the Failover Group.
5. Click **Return** to go back to the **Failover Groups** page.

Note

If for any reason it is desired to temporarily disable Call Preservation, simply removing the peer entities from the failover group will disable the feature without having to remove each product’s individual administration.

4.4 Administering Communication Manager for Call Preservation

Worksheet references

1. The following references will be needed from the FGDN Planning Worksheet in Appendix 2.
   - Failover Group Name
   - SM1 node name
   - primary FGDN
   - SM2 node name
   - secondary FGDN
   - CM node name
   - CM near-end port
   - SM1 TLS failover port
   - SM2 TLS failover port
   - SM1 TCP failover port
   - SM2 TCP failover port
   - SM1 trunk group identifier
   - SM2 trunk group identifier
   - CM primary FGDN Route
   - CM secondary FGDN Route

4.4.1 Verifying Signaling Group and Trunk Group administration

Previous SIP trunk administration between CM and SM (primary and secondary) is assumed. If the existing trunk and signaling group administration meets Call Preservation requirements, they can be reused. Here are a few guidelines for Call Preservation administration decisions in CM:

1. To add a failover group in CM you must have a SIP trunk and route pattern to reference for each SM. It is recommended to have dedicated route patterns for this specific administration since the first two trunks in the route must be the two trunks associated to the primary SM and secondary SM. This will be described further in the Route Pattern administration section.
2. It is important to note that some modification to any existing SIP trunks to Session Manager may be required if the ports in use on the signaling resource do not match the failover ports defined on the System Manager. Port IDs must match.
3. If your CM has trunk groups administered to any SM other than the Session Managers defined in the Failover Group, remove those additional signaling and trunk groups in CM and those entity links in System Manager. Otherwise in some outage scenarios, calls could be routed to the non-FGDN Session Manager resulting in dropped calls if a Session Manager fails.
4. You can also optionally add two dedicated trunks (one to each SM) rather than reuse the existing trunks. These trunks must be referenced in the route pattern form for the FGDN, but need not be used for calls.

Whether new or existing, verify your signaling group and trunk group administration meets the following criteria (Figures 11 and 12):

- You have at least two signaling groups defined, one for connectivity to the primary SM in the FGDN and one for the secondary SM in the FGDN.
- The Signaling and Trunk group types must be **SIP**.
- IMS must be disabled on the SIP signaling group. The Call Preservation feature is intended for non-SIP based endpoint support over SIP trunks in Communication Manager and Session Manager.
- Peer detection on the signaling group should be set to **Y**. If Peer detection is set to **N**, the peer server should be statically set to **SM**.
- Near-end Node Name must map to the System Manager FGDN Managed Peer entity. (for example, Procr or a CLAN interface) (**CM node name**).
- Near-end Node Port must match with the System Manager SIP entity link for Port. (**CM near-end Port**).
- Far-end Node Name must map to the Session Manager instances defined in the System Manager Failover Group. (**SM1 node name; SM2 node name**).
- Far-end Node Port must match with the Failover TCP or TLS port defined on the Session Manager SIP Entity form for which you have the entity link defined. (**SM1 TCP or TLS failover port; SM2 TCP or TLS failover port**).

```
display signaling-group 1
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y   Peer Server: SM



   Near-end Node Name: procr                  Far-end Node Name:  sm1
 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
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? 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                   Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? y            Alternate Route Timer(sec): 6

Command:
```

Figure 11: Administering Signaling Group

```
display trunk-group 1                                          Page   1 of  22
                                TRUNK GROUP

Group Number: 1                     Group Type: sip           CDR Reports: y
  Group Name: to sm1                       COR: 1        TN: 1        TAC: #001
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                          Member Assignment Method: auto
                                                    Signaling Group: 1
                                                  Number of Members: 1
```

Figure 12: Administering Trunk Group

4.4.2 Administering FGDN Route Patterns

Communication Manager needs the administration of two dedicated route patterns per Failover Group - one for the primary FGDN and another for the secondary FGDN.

Communication Manager does not use this route pattern to route the calls unless you choose to place this route in an outgoing dial pattern (not recommended). These two route patterns provide Communication Manager a method to resolve the FGDN to a particular node name and to validate link status to the FGDN Session Managers through the specified signaling/trunk group(s).

In summary, the trunks identified in these route patterns are used to:

- Determine a socket level connectivity with the Session Manager instances to determine a link status.
- Determine which FGDN resolves to which node-name and subsequently an ip-address.

Procedure:

1. To modify the route pattern, use **change route-pattern <x>** where <x> is the pattern number you wish to associate to the primary FGDN ordered pair. (**CM primary FGDN route**)
2. Enter the first and second preferences as the ordered SIP trunks associated to the SMs in the primary FGDN. (**SM1 trunk group identifier; SM2 trunk group identifier**)

   Figure 13 shows an example for route pattern 1, where route pattern 1 is mapped to the primary FGDN defined in System Manager. The first preference has the Session Manager associated to the primary SM in the primary FGDN, in the example this is SM1. The second preference has the Session Manager associated to the secondary SM in the primary FGDN, in the example this is SM2.

3. To modify the route pattern for the secondary FGDN, use **change route-pattern <y>** where <y> is the pattern number you wish to associate to the secondary FGDN ordered pair. (**CM secondary FGDN route**).
4. Enter the first and second preferences as the ordered SIP trunks associated to the SMs in the secondary FGDN. (**SM2 trunk group identifier; SM1 trunk group identifier**).

   Figure 14 shows an example for route pattern 2, where route pattern 2 is mapped to the secondary FGDN defined in System Manager. The first preference has the Session Manager associated to the primary SM in the secondary FGDN, in the example this is SM2. The second preference has the Session Manager associated to the secondary SM in the secondary FGDN, in the example this is SM1.

```
display route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: FGDN primary
                              SCCAN? n     Secure SIP? n
   Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
   No          Mrk Lmt List Del  Digits                                QSIG
                              Dgts                                     Intw
1: 1     0                                                               n    user
2: 2     0                                                               n    user
3:                                                                       n    user
4:                                                                       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  n           rest                                        next
2: y y y y y n  n           rest                                        none
3: y y y y y n  n           rest                                        none
4: y y y y y n  n           rest                                        none
5: y y y y y n  n           rest                                        none
6: y y y y y n  n           rest                                        none
```

The first preference is associated to primary Session Manager

The second preference is associated to secondary Session Manager

Figure 13: Route Pattern 1

```
display route-pattern 2                                          Page   1 of   3
                    Pattern Number: 2   Pattern Name: FGDN inverse
                              SCCAN? n     Secure SIP? n
   Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
   No          Mrk Lmt List Del  Digits                                QSIG
                              Dgts                                     Intw
1: 2     0                                                               n    user
2: 1     0                                                               n    user
3:                                                                       n    user
4:                                                                       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  n           rest                                        next
2: y y y y y n  n           rest                                        none
3: y y y y y n  n           rest                                        none
4: y y y y y n  n           rest                                        none
5: y y y y y n  n           rest                                        none
6: y y y y y n  n           rest                                        none
```

The first preference is associated to secondary Session Manager

The second preference is associated to primary Session Manager

Figure 14: Route Pattern 2

Note

All subsequent preference entries will be ignored for FGDN mapping. Do not enter additional preferences here.

4.4.3 Administering the Failover Group Domain Map

Communication Manager uses the Failover Group Domain Map to resolve the Failover Group to a set of node-names (using the route pattern association). The Communication Manager administrator adds two failover group domain maps - one for the primary FGDN and another for the secondary FGDN. The Communication Manager administrator specifies the route patterns for each domain.

Note

The CM interface should be associated with only one failover group. Multiple group association is prohibited in System Manager FGDN administration.

Procedure:

1. To modify a Failover Group Domain Map table, use the **change failover-grp-domain-map** command.
2. Populate the form with the following information:
   - **Domain 1**: **primary FGDN.** For example, sm1-sm2.avaya.com.

     This is the primary FGDN defined on the SMGR failover group administration form.
   - **Route Pattern**: **CM primary FGDN route.** Route pattern 1 in this example.

     This is the route pattern for the primary FGDN created in the route pattern administration above.
   - **Domain 2**: **secondary FGDN.** For example, sm1-sm2-i.avaya.com.

     This is the secondary FGDN defined on the SMGR failover group administration form.
   - **Route Pattern**: **CM secondary FGDN route.** Route pattern 2 in this example.

     This is the route pattern for the secondary FGDN created in the route pattern administration above.

```
display failover-grp-domain-map

                    FAILOVER GROUP DOMAIN MAPPING

 Domain 1: sm1-sm2.avaya.com
 Route Pattern: 1
 Domain 2: sm1-sm2-i.avaya.com
 Route Pattern: 2
 Domain 3:
 Route Pattern:
 Domain 4:
 Route Pattern:
 Domain 5:
 Route Pattern:
 Domain 6:
 Route Pattern:
 Domain 7:
 Route Pattern:
 Domain 8:
 Route Pattern:
 Domain 9:
 Route Pattern:

Command:
```

Figure 15: Failover Group Domain Map

4.5 Administering Mediant™ 3000 for Call Preservation

Worksheet references

The following information will be used from the FGDN Planning Worksheet in Appendix 2:

- External DNS Server IP Address (optional)
- SM1 DNS A-Record Name
- SM1 SM100 IP Address
- SM2 DNS A-Record Name
- SM2 SM100 IP Address
- primary FGDN
- secondary FGDN
- M3K SIP destination port
- SM1 and SM2 primary/secondary FGDN DNS SRV priority
- SM 1 and SM2 primary/secondary FGDN DNS SRV weight
- M3K SIP local listen port
- M3K SIP transport
- M3K IP group identifier
- M3K proxy set identifier
- M3K IP profile identifier

If you have an existing M3K, the FGDN changes connectivity administration to Session Manager. You may need to modify and possibly remove in some cases, previous administration. Use the instructions in this section to determine where changes impact existing administration.

4.5.1 Adding the FGDN to Internal DNS Tables

Note

Internal DNS administration is recommended. However, if using external DNS SRV in support of the Call Preservation feature, administer the external DNS SRV under **Configuration>VOIP>Network>DNS>DNS Settings**. Refer to the **External DNS Server IP Address** (es) on the FGDN Planning Worksheet. This operation requires a reset of the M3K. Also, refer to Appendix 1 for adding the FGDN to your corporate DNS server.

Within the below instructions, the following example will be used from the FGDN Planning Worksheet in Appendix 2:

- Session Manager 1 (sm1) SM100 Security Module has a FQDN of sm1.avaya.com and IPv4 address as 192.168.1.1. (See **SM1 DNS A-Record Name** and **SM1 SM100 IP Address** on the Planning Worksheet)
- Session Manager 2 (sm2) SM100 Security Module has a FQDN of sm2.avaya.com and IPv4 address as 192.168.2.1. (See **SM2 DNS A-Record Name** and **SM2 SM100 IP Address** on the Planning Worksheet)

Procedure:

1. Navigate to **Configuration>VOIP>Network>DNS>Internal DNS Table** (Figure 16)
2. Define an A-record entry for the Session Manager 1 in the failover group in the Internal DNS table with the following fields:

   Domain Name= **SM1 DNS A-Record Name.** For example, sm1.avaya.com.

   First IP Address= **SM1 SM100 IP Address.** For example, 192.168.1.1.

   Note

   Leave the fields Second IP Address, Third IP Address and others, with the default value of 0.0.0.0 or blank.

3. Then, define another DNS A-record entry for the Session Manager 2 in the failover group in the Internal DNS table with the following fields:

   Domain Name= **SM2 DNS A-Record Name.** For example, sm2.avaya.com.

   First IP Address= **SM2 SM100 IP Address.** For example, 192.168.2.1.

   Note

   Leave the fields Second IP Address, Third IP Address, and others, with the default value of 0.0.0.0 or blank.

4. Click **Submit** to save changes.
5. Navigate to **Configuration>VOIP>Network>DNS>Internal SRV Table**. (Figure 17)

   Note

   Each Session Manager has a SIP traffic interface known as the SM100 interface which needs to be represented as a fully qualified domain name (FQDN) in this internal DNS table. This name

must map to a valid IPV4 address that matches the Session Manager SM100 address. Please ensure you have defined these DNS A-record entries in the DNS Internal table (previous step) prior to executing the DNS SRV specification of the Failover Group Domain Name (FGDN) in this step.

6. Using the same values for **primary FGDN** and the **secondary FGDN** from the FGDN Planning worksheet that were previously administered on the System Manager, add 2 SRV records; one for the primary FGDN and another for the secondary FGDN in this internal SRV table.

   The FGDN is made up of 2 Session Manager entities. The example SRV records are, one is defined as the primary Session Manger (sm1.avaya.com) and the other is defined as the secondary Session Manager (sm2.avaya.com). In the example:

   - The **primary FGDN** is sm1-sm2.avaya.com comprised of the ordered pair (sm1.avaya.com, sm2.avaya.com)
   - The **secondary FGDN** is sm1-sm2-i.avaya.com comprised of the ordered pair (sm2.avaya.com, sm1.avaya.com)

   This will result in two SRV records defined in the internal SRV table of the M3K.

For the first record, additional details need to be specified:

1. **Domain Name**= **primary FGDN**. For example, sm1-sm2.avaya.com.
2. **Transport Type** = **M3K SIP transport.** For example, TCP.

   Choose the transport type, TCP or TLS, which matches the entity link definition on System Manager for the M3K SIP entity.
3. **DNS Name 1**= **SM 1 DNS A-Record Name.** For example, sm1.avaya.com.

   This is the fully qualified domain name specified in the earlier A-record definition for Session Manager 1.
4. **Priority** = **SM 1 primary FGDN DNS SRV priority.** For example, the priority 1 for sm1.avaya.com in the ordered pair.

   The lower the value the more preferred (the recommendation is to make this value more preferred or lower than the value for “DNS Name 2” below).
5. **Weight** = **SM1 primary FGDN DNS SRV weight.** For example, a relative weight for records with the same priority.

   The sum of the weight for “DNS Name 1” plus the weight for “DNS name 2” cannot exceed 100 (the recommendation is to make the priority of “DNS name1” more preferred than the priority of “DNS name 2” so the value of weight should not come into play, so using the value of 50 here would be acceptable).
6. **Port** = **M3K SIP destination port.** For example, 5060.

   Specify the Session Manager 1 TCP or TLS port used in the SIP Entity Link defined on System Manager for this M3K.
7. **DNS Name 2**= **SM2 DNS A-Record Name.** For example, sm2.avaya.com.

   This is the fully qualified domain name specified in the earlier A-record definition for Session Manager 2.
8. **Priority** = **SM2 primary FGDN DNS SRV priority.** For example, the priority 2 for sm2.avaya.com in the ordered pair.

The lower the value the more preferred (the recommendation is to make this value “less preferred” or higher than the value for “DNS Name 1”).

9. **Weight** = **SM2 primary FGDN DNS SRV weight.** For example, a relative weight for records with the same priority.

   The sum of the weight for “DNS name 1” plus the weight for “DNS name 2” cannot exceed 100 (the recommendation is to make the priority of “DNS name1” more preferred than the priority of “DNS name 2” so the value of weight should not come into play, so using the value of 50 here would be acceptable).

10. **Port** = **M3K SIP destination port.** For example, 5060.

    Specify the Session Manager 2 TCP or TLS port used in the SIP Entity Link defined on System Manager for this Mediant™ 3000.

For the second SRV record additional details need to be specified:

1. **Domain Name**= **secondary FGDN.** For example, sm1-sm2-i.avaya.com.
2. **Transport Type** = **M3K SIP transport.** For example, TCP.

   Choose the transport type that matches the entity link definition on System Manager for the M3KSIP entity. Recall UDP is not supported at this time for Call Preservation.

3. **DNS Name 1**= **SM2 DNS A-Record Name.** For example, sm2.avaya.com.

   This is the fully qualified domain name specified in the earlier A-record definition for Session Manager 2.

4. **Priority** = **SM2 secondary FGDN DNS SRV priority.** For example, the priority 1 for sm2.avaya.com in the ordered pair.

   The lower the value the more preferred (the recommendation is to make this value more preferred or lower than the value for “DNS Name 2” below).

5. **Weight** = **SM2 secondary FGDN DNS SRV weight.** For example, a relative weight for records with the same priority.

   The sum of the weight for “DNS Name 1” plus the weight for “DNS name 2” cannot exceed 100 (; the recommendation is to make the priority of “DNS name1” more preferred than the priority of “DNS name 2” so the value of weight should not come into play, so using the value of 50 here would be acceptable).

6. **Port** = **M3K SIP destination port.** For example, 5060.

   Specify the Session Manager 2 TCP or TLS port used in the SIP Entity Link defined on SMGR for this Mediant™ 3000.

7. **DNS Name 2**= **SM1 DNS A-Record Name.** For example, sm1.avaya.com.

   This is the fully qualified domain name specified in the earlier A-record definition for Session Manager 1.

8. **Priority** = **SM1 secondary FGDN DNS SRV priority.** For example, the priority 2 for sm1.avaya.com in the ordered pair.

   The lower the value the more preferred (the recommendation is to make this value “less preferred” or higher than the value for “DNS Name 1”).

9. **Weight** = **SM1 secondary FGDN DNS SRV weight.** For example, a relative weight for records with the same priority.

The sum of the weight for “DNS name 1” plus the weight for “DNS name 2” cannot exceed 100 (the recommendation is to make the priority of “DNS name1” more preferred than the priority of “DNS name 2” so the value of weight should not come into play, so using the value of 50 here would be acceptable).

10. **Port** = **M3K SIP destination port.** For example, 5060.

    Specify the SM 1 TCP or TLS port used in the SIP Entity Link defined on SMGR for this M3K.

11. Click **Submit** to save changes.

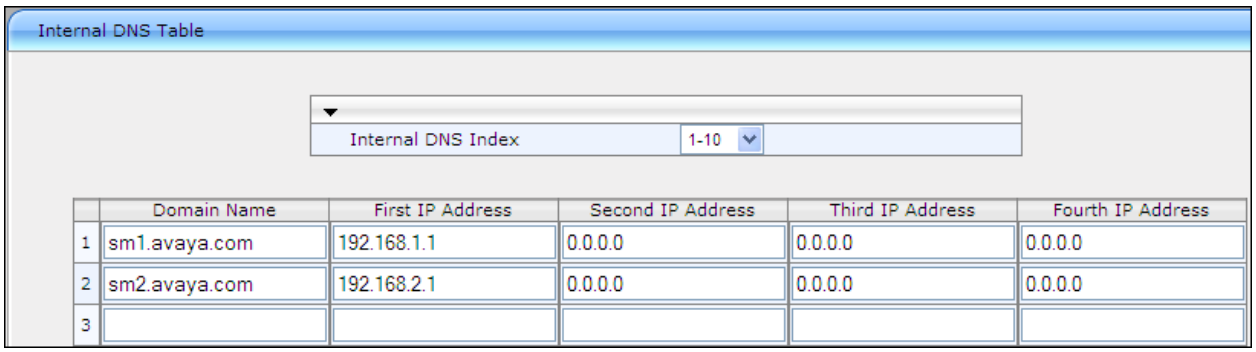


Figure 16: Adding the FQDNs to the Internal DNS Tables

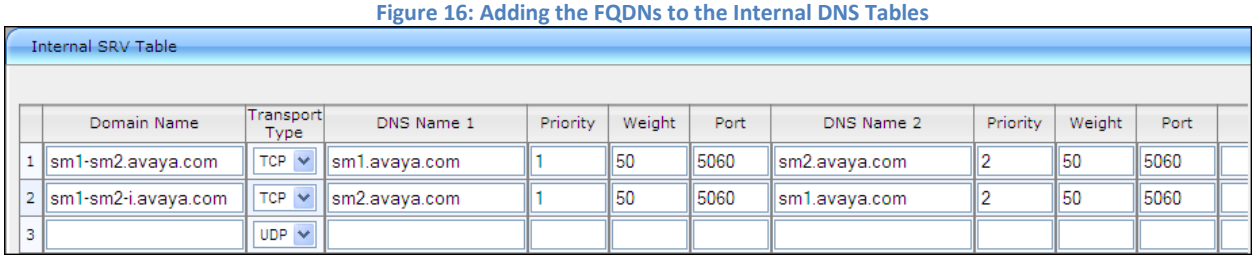


Figure 17: Internal SRV Table

4.5.2 Creating a Proxy Set

1. Navigate to **Configuration>VOIP>Control Network>Proxy Sets Table** (Figure 18) and create a new entry "1" for example. Do not use 0 this is reserved for the default outbound proxy set specification.
2. Under the Proxy Address fields
   - Enter the **primary FGDN** (position 1), for example, **sm1-sm2.avaya.com**.
   - Enter the **secondary FGDN** (position 2), for example **sm1-sm2-i.avaya.com.**
3. Enter the **Transport Type** as TCP or TLS (**M3K SIP transport**).

   This value needs to match the earlier provisioned SRV record specification and similarly the entity link specification on the System Manager.
4. Modify the following Call Preservation related settings (accept defaults otherwise):
   - **Enable Proxy Keep Alive** should be set to "Using Options"; (this is a method in SIP used to determine service readiness of the FGDN defined in the proxy list).
   - **Proxy Keep Alive Time** = 60; (this is the interval at which the OPTION message is sent to the FGDNs defined in the proxy list above).

- **Proxy Load Balancing Method** = Disable (this means that no round robin route between the proxy addresses, round robin works on a rotation basis where the first entry on the proxy list would be used for the first call, then the second entry on the proxy list would be used for the second call; alternating between the entries on this list; load balancing of any kind should be avoided with the Call Preservation feature).
- **Is Proxy Hot Swap** =Yes (this implies the active-active configuration that Core SM redundancy provides).

5. **Proxy Redundancy Mode**=Homing (Parking=if primary fails/becomes unavailable stay on secondary until secondary fails/becomes unavailable; Homing=if primary proxy fails/becomes unavailable; go to secondary proxy, when primary proxy recovers, go back to primary proxy).
6. Click **Submit** to save changes.

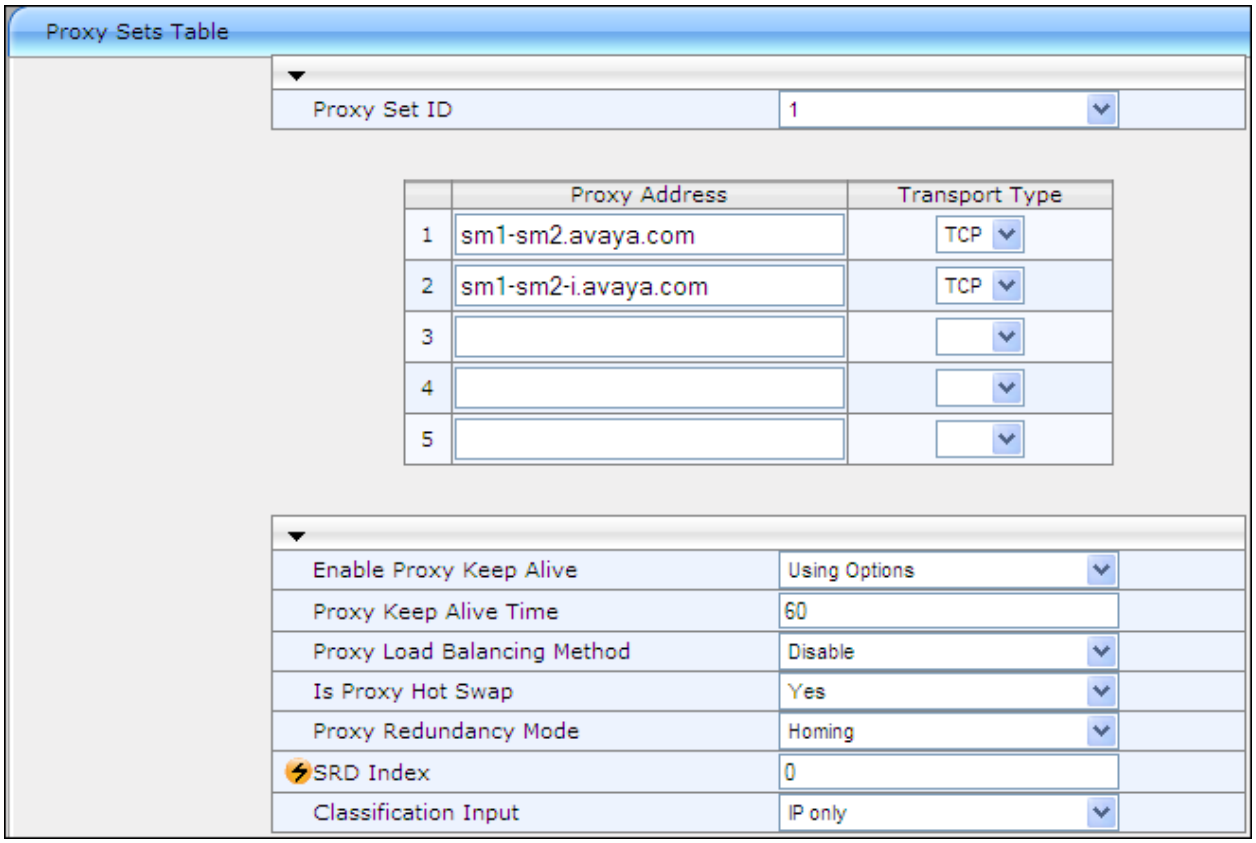


Figure 18: Create an IP Group and Proxy Set

4.5.3 Creating an IP Group Table

1. Navigate to **Configuration>VOIP>Control Network>IP Group Table** (Figure 19) and create a new index "1" for example. Do not use 0 this is reserved for the default outbound IP Group/Proxy set specification. Generation of the IP Group is done to establish the M3Kcall routing rules for the FGDNs.
2. Under the **Common Parameters** section complete the following administration:
   - Create a **Description** to identify the IP Group.

- **Proxy Set ID** = **M3K proxy set identifier.** For example, 1.

  Use the same index number you created in the Proxy Sets Table above (this is 1 in this example)

- **SIP Group Name** = **SIP domain.** For example, avaya.com.

  Set the **SIP Group Name** to the root level domain (that is, avaya.com) or whatever you would like to see in the Request-URI for outbound SIP requests to Session Manager.

- **Contact User** = <blank> Leave this optional field blank unless you want to modify what is shown in the contact header of the SIP INVITE message.

- **IP Profile ID** = **M3K IP profile identifier**. For example, 1.

  Index to the IP Profile that you wish to assign to this group (in this example it is 1)* no specific modifications for Call Preservation were made to the defaults on the IP Profile Settings.

3. Under the **Gateway Parameters** section complete the following administration:
   a. Under **Always Use Route Table** = No. This allows for use of the proxy set defined earlier in route decisions.
   b. **Routing Mode** = Request-URI; the SIP request is routed according to the IP/hostname. specified in the request-uri.
   c. **SIP Re-Routing Mode** = Standard which means that call redirection handling (that is, REFER) uses Refer-To header in the 3xx response in the routing decision; this is the preferred method of administration for Call Preservation.
4. Click **Submit** to save changes.

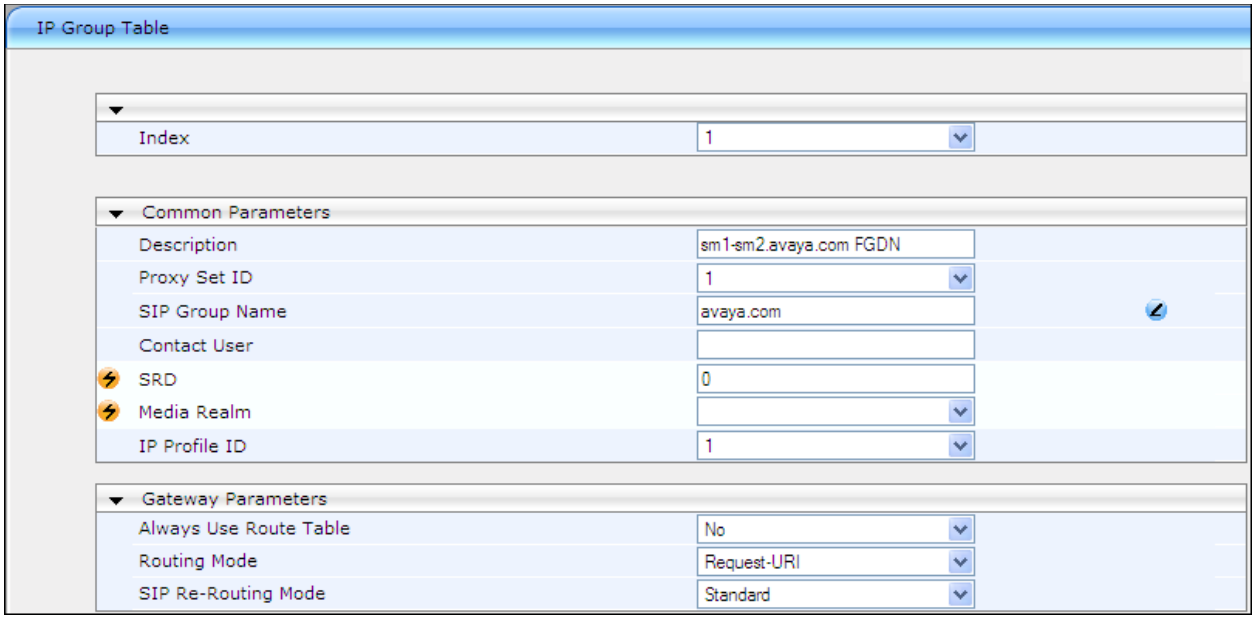


Figure 19: Creating an IP Group Table

4.5.4 Configuring General Parameters

1. Navigate to **Configuration> VOIP>SIP Definitions>General Parameters** (Figure 20).
2. Under SIP General modify the following fields (accept defaults otherwise).
   - **Minimum Session-Expires** should ideally match what is administered on page 2 of the trunk form on Communication Manager for Preferred Minimum Session Refresh Interval. Both on the M3K and the Communication Manager this is specified in seconds. This is the elapsed interval before a re-invite is sent to refresh the SIP session. Example: 600 seconds.
   - **SIP Transport Type** = TCP/TLS - UDP is <u>not</u> supported with this Call Preservation feature release. This field must match what is administered on the System Manager for the trusted entity link connection to the M3KSIP entity. (**M3K SIP transport)**
   - **SIP TCP/TLS Local Port**s needs to match administered System Manager for the trusted entity link connection for the M3KSIP entity. (**M3K SIP local listen port)**
   - **Enable TCP Connection Reuse** should be set to "Enable".
   - **SIP Destination Port** should match the listener port defined for Session Manager for this connection on the SIP entity form. (**M3K SIP destination port**)
   - **TCP Timeout** is the Timer B (INVITE transaction timeout) and Timer F(non-INVITE transaction timeout) to allow for faster failover this parameter can be adjusted down to a minimum value of 6 seconds (so as to not overlap with Session Manager Timer B/F policies for alternate routing). The default is 32 seconds. The example shows 8 seconds.
   - **Forking Handling Mode** should be set as Sequential. Parallel forking is not supported in Session Manager Release 6.2. Scroll down the page to see more. (Not shown in Figure 19)

2. Click **Submit** to save changes.

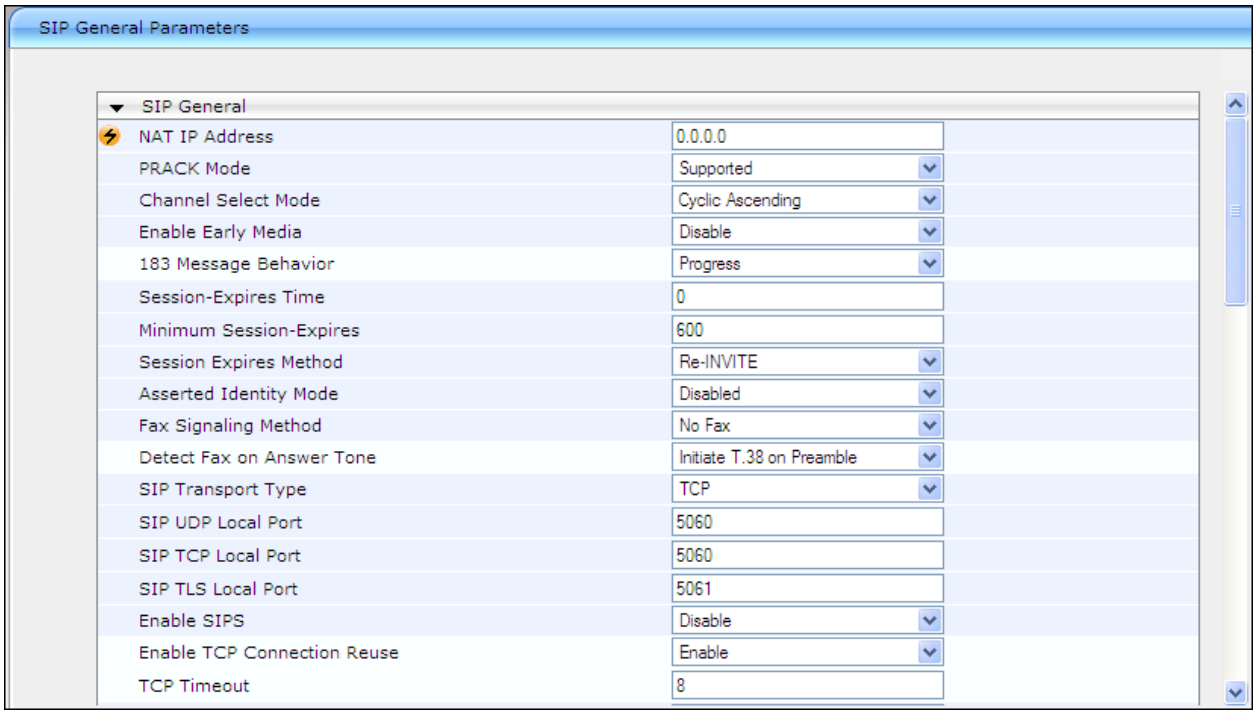


Figure 20: Configuring General Parameters

4.5.5 Configuring Proxy Settings

1. Navigate to **Configuration>VOIP>SIP Definitions>Proxy & Registration** (Figure 21)
2. Modify the following fields (accept defaults otherwise).
   - **Use Default Proxy** = No (this is to avoid only using a default outbound proxy in routing decisions)
   - **Proxy Name**= sm1-sm2.avaya.com for example (this is the name that is used in the Request-URI and the host part of the To header)
   - **Redundancy Mode**= Homing (Parking=if primary fails/becomes unavailable stay on secondary until secondary fails/becomes unavailable; Homing=if primary proxy fails/becomes unavailable; go to secondary proxy, when primary proxy recovers, go back to primary proxy).
   - **Redundant Routing Mode**= Proxy
   - **SIP Re-Routing Mode**= Use Routing Table
   - **DNS Query Type** = SRV
   - **Proxy DNS Query Type**=SRV
   - **Use Gateway Name for OPTIONS** = Server
3. Click **Submit** to save changes. You do not need to select the Register or Unregister options.

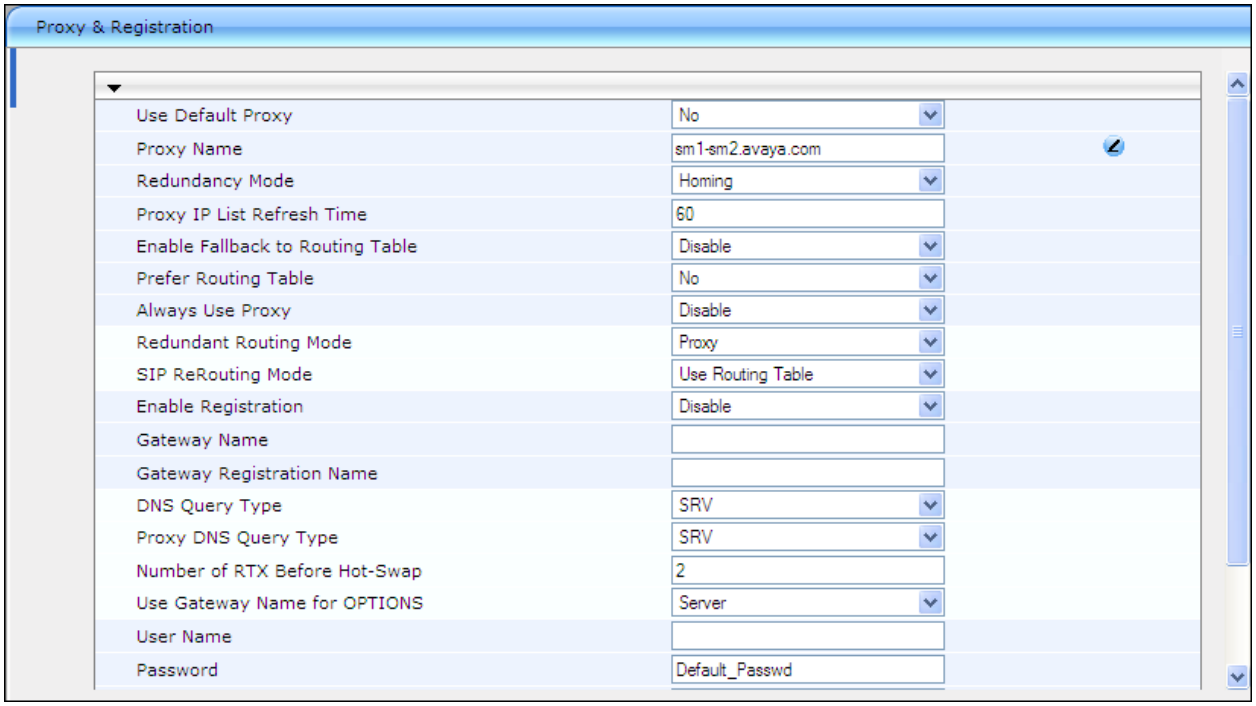


Figure 21: Configuring Proxy Settings

4.5.6 Configuring Routing Settings

1. Navigate to **Configuration >VOIP>GW and IP to IP>Routing>General Parameters** (Figure 22).
2. Modify the following fields (accept defaults otherwise):
   - **Enable Alt Routing Tel to IP** = Enable (this must be set to allow the M3Kto route calls to an alternate Session Manager)
   - **Alt Routing Tel to IP Mode** = Both (enable alternate routing to destination if OPTION fails, poor QoS is detected or is the DNS hostname does not resolve)
   - **Alt Routing Tel to IP Connectivity Method** = SIP OPTIONS (The destination is considered "down" if the latest OPTION transaction has timed out; any response(including error responses) will bring the state of the destination to "up")
3. Click **Submit** to save changes.
4. Navigate to **Configuration>VOIP>GW and IP to IP>Routing>Alternative Routing Reasons** (Figure 23). The information entered in the Tel to IP Reasons table instructs the M3Kas to when it should alternate route after receiving an error response.
5. Enter 408 (No Response), 503 (Service Unavailable) and 480 (Temporarily Unavailable). Optionally add additional reason codes as your implementation requires.
6. Click **Submit** to save changes.

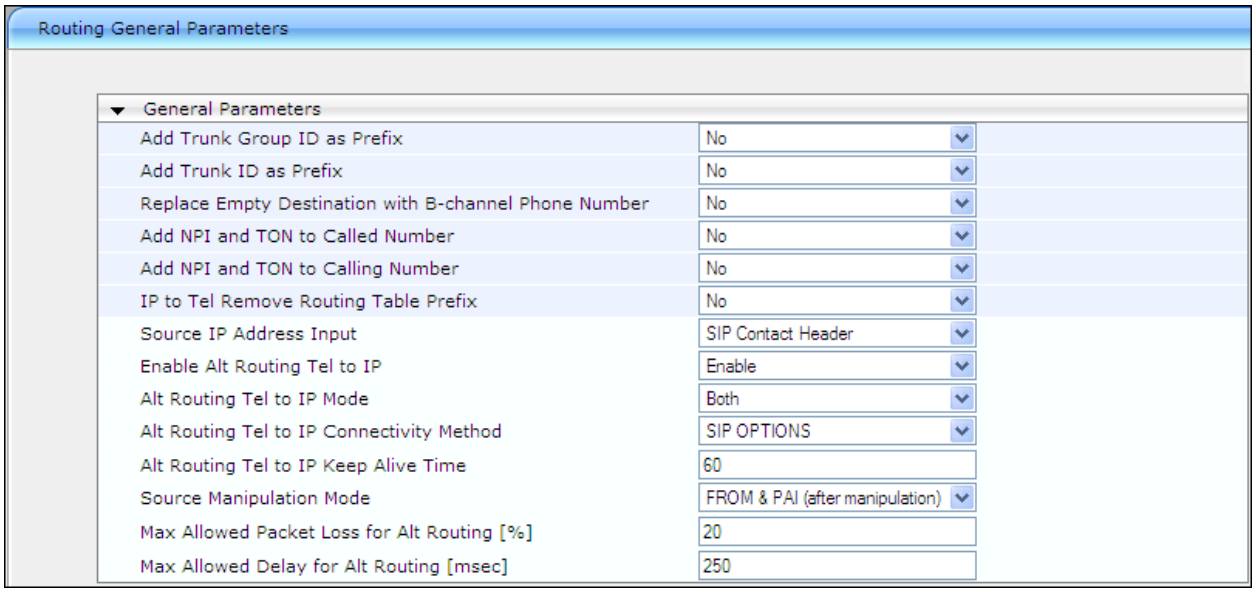


Figure 22: Configuring Routing General Parameters

Figure 23: Reasons for alternate routing

4.5.7 Creating Routing Rules

1. Navigate to **Configuration>VOIP>GW and IP to IP>Routing>Tel to IP Routing** (Figure 24). This table is used to configure OUTBOUND call handling from the M3K to the Session Manager. Refer to the M3K setup guide referenced in section 1.3 for additional call routing administration guidelines.

   Note

   If you are using this table to map phone prefixes from a particular trunk resource to a specific destination, you need to tie any information in this table to the previously administered IP Group from above. Also, you should not specify an IP-address or a port for any entry in the table. Use of the IP Group allows the M3K to look at the proxy set assigned to the IP Group to determine the destination entity, which is required for the Call Preservation feature.

2. After specifying any required pattern match/trunk select information, verify the following:
   a. **Dest. IP Address** = <blank>
   b. **Port**= <blank>
   c. **Transport Type** = **M3K SIP transport.** For example, TCP.
   d. **Dest. IP Group ID** = **M3K IP group identifier.** For example, 1.
3. Navigate to **Configuration>VOIP>GW and IP to IP>Routing>IP to Tel Routing** (Figure 25). This table is used to configure INBOUND call handling to the M3K from the Session Manager.

   Note

   If you are using this table to map phone prefixes from a particular trunk resource to a specific destination, you need to tie any information in this table to the previously administered IP Group from above. Also, you should not specify an IP-address or a port for any entry in the table. Use of the IP Group allows the M3K to look at the proxy set assigned to the IP Group to determine the destination entity, which is required for the Call Preservation feature.

4. After specifying any required pattern match/trunk select information, verify the following:

a. **Source IP Address** = <blank>

b. **Source IP Group ID** = **M3K IP group identifier.** For example, 1.

Tel to IP Routing

Basic Parameter List

Routing Index: 1-10

Tel To IP Routing Mode: Route calls before manipulation

	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address	Port	Transport Type	Dest. IPGroup ID	Dest. SRD	IP Profile ID
1	1	*	*				TCP	1	-1	1
2	2	*	*				TCP	1	-1	1
3	3	*	*				TCP	1	-1	1
4	4	*	*				TCP	1	-1	1
5	5	*	*				TCP	1	-1	1
6	6	*	*				TCP	1	-1	1
7							Not Configured	-1		
8							Not Configured	-1		
9							Not Configured	-1		
10	10	*	*				TCP	1	-1	1

Figure 24: Tel to IP Routing table

IP To Trunk Group Routing Table

Basic Parameter List

Routing Index: 1-10

IP To Tel Routing Mode: Route calls before manipulation

	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	->	Trunk Group ID	IP Profile ID	IP
1	*	*	*	*			1	1	1
2	*	*	*	*			2	1	1
3	*	*	*	*			3	1	1
4	*	*	*	*			4	1	1
5	*	*	*	*			5	1	1
6	*	*	*	*			6	1	1
7									
8									
9									
10	*	*	*	*			10	1	1

Figure 25: IP to Tel Routing table

Note

Some edits require a reset for the failover group to work properly. Hence, after administration you should BURN the configuration changes and perform a system reset.

4.6 Administering G860 for call preservation using an EMS Client

This section describes administration of the G860 for Call Preservation using the AudioCodes EMS Client.

The user is expected to have working knowledge of the G860 system.

1. Log on to your EMS client and Double-click the G860 device being administered.
2. Select the appropriate 6310 board to access the settings. This is the root location for most of the administration and the navigation path is **G860 > board# > service name**.

If you have an existing G860, the FGDN changes connectivity administration to Session Manager. You may need to modify and possibly remove in some cases, previous administration. Use the instructions in this section to determine where changes impact existing administration.

4.6.1 Adding the FGDN to Internal DNS Tables

Note

For external DNS, click **Networking->Network Settings->Network Services**. Refer to the **External DNS Server IP Address** (es) on the FGDN Planning Worksheet. This operation requires a reset of the G860. Also, refer to Appendix 1 for adding the FGDN to your corporate DNS server.

Within the below instructions, the following example will be used from the FGDN Planning Worksheet in Appendix 2:

- Session Manager 1 (sm1) SM100 Security Module has a FQDN of sm1.avaya.com and IPv4 address as 192.168.1.1. (See **SM1 DNS A-Record Name** and **SM1 SM100 IP Address** on the Planning Worksheet)
- Session Manager 2 (sm2) SM100 Security Module has a FQDN of sm2.avaya.com and IPv4 address as 192.168.2.1. (See **SM2 DNS A-Record Name** and **SM2 SM100 IP Address** on the Planning Worksheet)

For A-Record

1. For internal DNS, navigate to **Board# > SIP > SIP General > DNS**. (Figure 26)
2. Under **Navigation**, add two rows, one for A-Record of each SM.
3. Edit by selecting the row and then under **Configuration** select **SIP Routing DNS Settings**. (Figure 27)
4. Enter the A Record settings for the Primary SM in the FGDN and Click Apply on the SIP Routing DNS Settings page. See FGDN Planning Worksheet for details.
   a. **Name =** For example, primary FGDN.
   b. **Domain Name**= **SM1 DNS A-Record Name.** For example, sm1.avaya.com.
   c. **First IP Address**= **SM1 SM100 IP Address.** For example, 192.168.1.1.
5. On the second row, enter the A Record settings for the Secondary SM in the FGDN and Click Apply on the SIP Routing DNS Settings page. See FGDN Planning Worksheet for details.
   a. **Name =** Secondary. For example, secondary FGDN.
   b. **Domain Name**= **SM2 DNS A-Record Name.** For example, sm2.avaya.com.
   c. **First IP Address**= **SM2 SM100 IP Address.** For example, 192.168.2.1.
6. Return to Navigation and unlock each row.

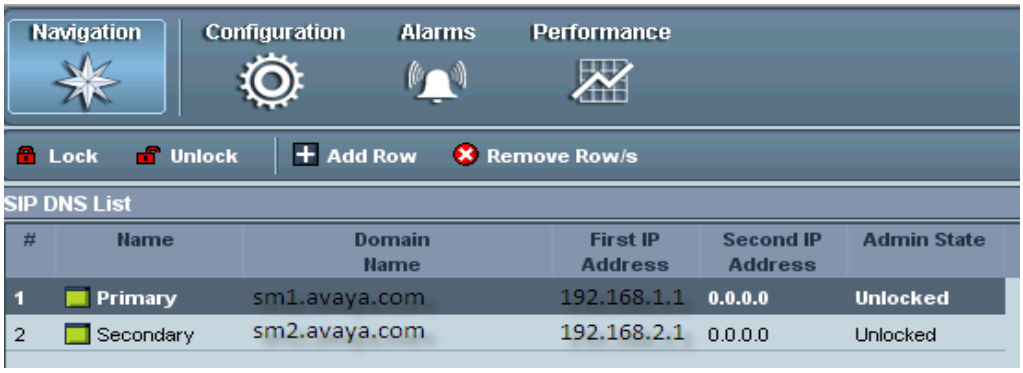


Figure 26: Adding the FQDNs to the Internal DNS Tables

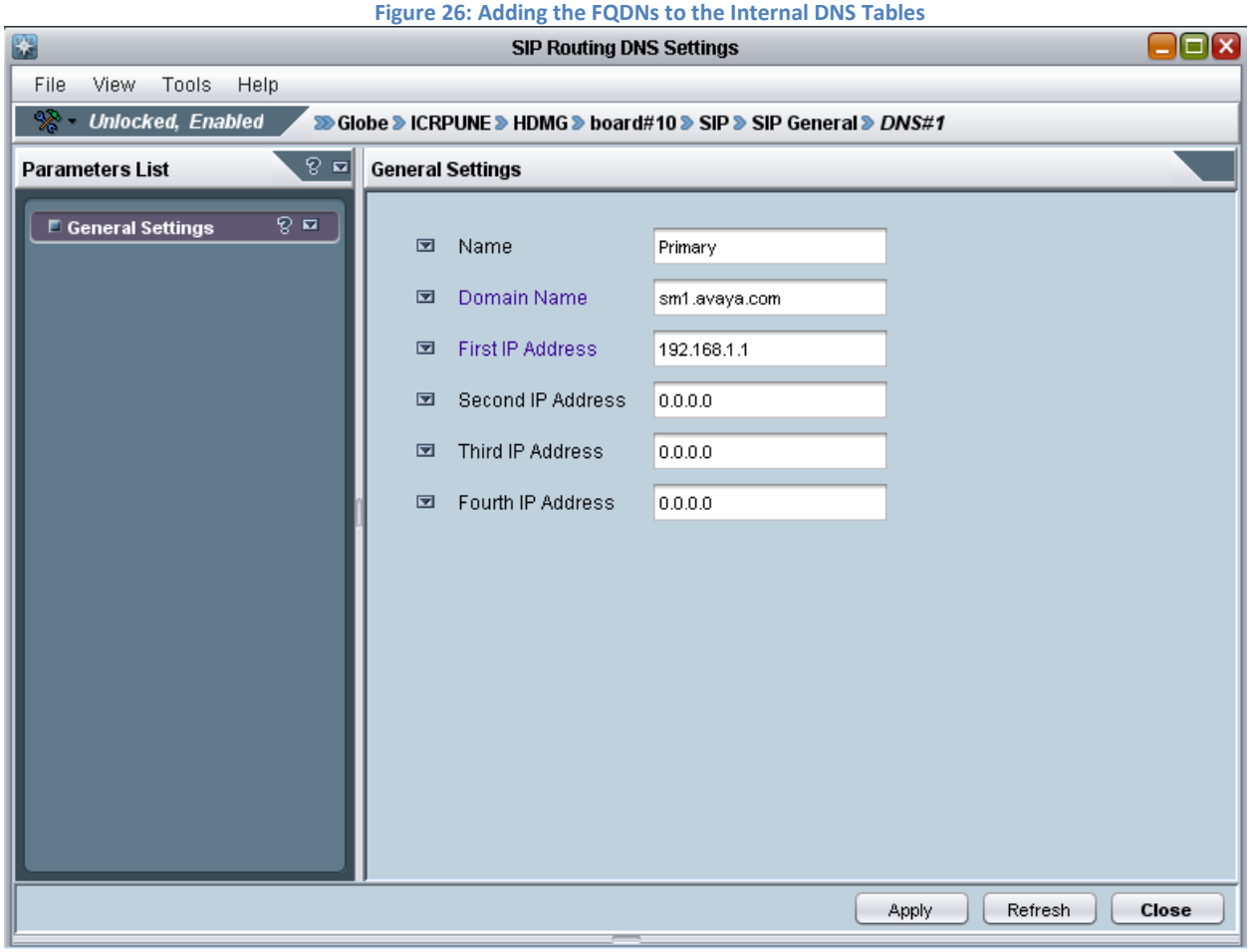


Figure 27: SIP Routing DNS Settings

For SRV Record

1. Navigate to **Board# > SIP> SIP General > SRV**. (Figure 28)
2. Under **Navigation**, add a row for the SRV Record.
3. Edit the row by selecting the row and then under **Configuration** select **SIP SRV to IP Settings**. (Figure 29)
4. Using the same values for primary FGDN and the secondary FGDN from the FGDN Planning worksheet that were previously administered on the System Manager, add 2 SRV records; one for

the primary FGDN and another for the secondary FGDN in this internal SRV table.

The FGDN is made up of 2 Session Manager entities. The example SRV records are, one is defined as the primary Session Manger (sm1.avaya.com) and the other is defined as the secondary Session Manager (sm2.avaya.com). In the example:

- The **primary FGDN** is sm1-sm2.avaya.com comprised of the ordered pair (sm1.avaya.com, sm2.avaya.com)
- The **secondary FGDN** is sm1-sm2-i.avaya.com comprised of the ordered pair (sm2.avaya.com, sm1.avaya.com)

This will result in two SRV records defined in the internal SRV table of the G860.

For the first SRV record,

a. **Name** = For example, primary FGDN**.**

b. **Internal Domain Name**= **primary FGDN**. For example, sm1-sm2.avaya.com.

c. **Transport Type** = **G860 SIP transport.** For example, TCP.

Choose the transport type, TCP or TLS, which matches the entity link definition on System Manager for the G860 SIP entity. Recall UDP is not supported at this time for Call Preservation.

d. **DNS Name 1**= **SM1 DNS A-Record Name.** For example, sm1.avaya.com.

e. **Priority 1** = **SM1 secondary FGDN DNS SRV priority.** For example, the priority 1 for sm1.avaya.com in the ordered pair.

f. **Weight** 1= **SM1 secondary FGDN DNS SRV weight.** For example, a relative weight for records with the same priority.

The sum of the weight for “DNS name 1” plus the weight for “DNS name 2” cannot exceed 100 (the recommendation is to make the priority of “DNS name1” more preferred than the priority of “DNS name 2” so the value of weight should not come into play, so using the value of 50 here would be acceptable).

g. **Port 1** = **G860 SIP destination port.** For example, 5060.

h. DNS Name 2= SM2 DNS A-Record Name. For example, sm2.avaya.com.

i. Priority 2 = SM2 secondary FGDN DNS SRV priority. For example, the priority 2 for sm2.avaya.com in the ordered pair.

j. Weight 2 = SM2 secondary FGDN DNS SRV weight. For example, a relative weight for records with the same priority.

The sum of the weight for “DNS name 1” plus the weight for “DNS name 2” cannot exceed 100 (the recommendation is to make the priority of “DNS name1” more preferred than the priority of “DNS name 2” so the value of weight should not come into play, so using the value of 50 here would be acceptable).

k. **Port2** = **G860 SIP destination port.** For example, 5060.

5. Click **Apply** to save the changes.
6. Return to Navigation and select the row and unlock.
7. Similarly for the second SRV record, enter the following details. (Figure 29)

a. **Name** For example, secondary FGDN**.**

b. **Internal Domain Name**= **secondary FGDN**. For example, sm1-sm2-i.avaya.com.

c. **Transport Type** = **G860 SIP transport.** For example, TCP.

Choose the transport type, TCP or TLS, which matches the entity link definition on System Manager for the G860 SIP entity. Recall UDP is not supported at this time for Call Preservation.

d. **DNS Name 1**= **SM2 DNS A-Record Name.** For example, sm2.avaya.com.

e. **Priority 1** = **SM2 secondary FGDN DNS SRV priority.** For example, the priority 1 for sm2.avaya.com in the ordered pair.

f. **Weight** 1= **SM2 secondary FGDN DNS SRV weight.** For example, a relative weight for records with the same priority.

The sum of the weight for "DNS name 1" plus the weight for "DNS name 2" cannot exceed 100 (the recommendation is to make the priority of "DNS name1" more preferred than the priority of "DNS name 2" so the value of weight should not come into play, so using the value of 50 here would be acceptable).

g. **Port 1** = **G860 SIP destination port.** For example, 5060.

h. DNS Name 2= SM1 DNS A-Record Name. For example, sm1.avaya.com.

i. Priority 2 = SM1 secondary FGDN DNS SRV priority. For example, the priority 2 for sm2.avaya.com in the ordered pair.

The lower the value the more preferred (the recommendation is to make this value "less preferred" or higher than the value for "DNS Name 1").

j. Weight 2 = SM1 secondary FGDN DNS SRV weight. For example, a relative weight for records with the same priority.

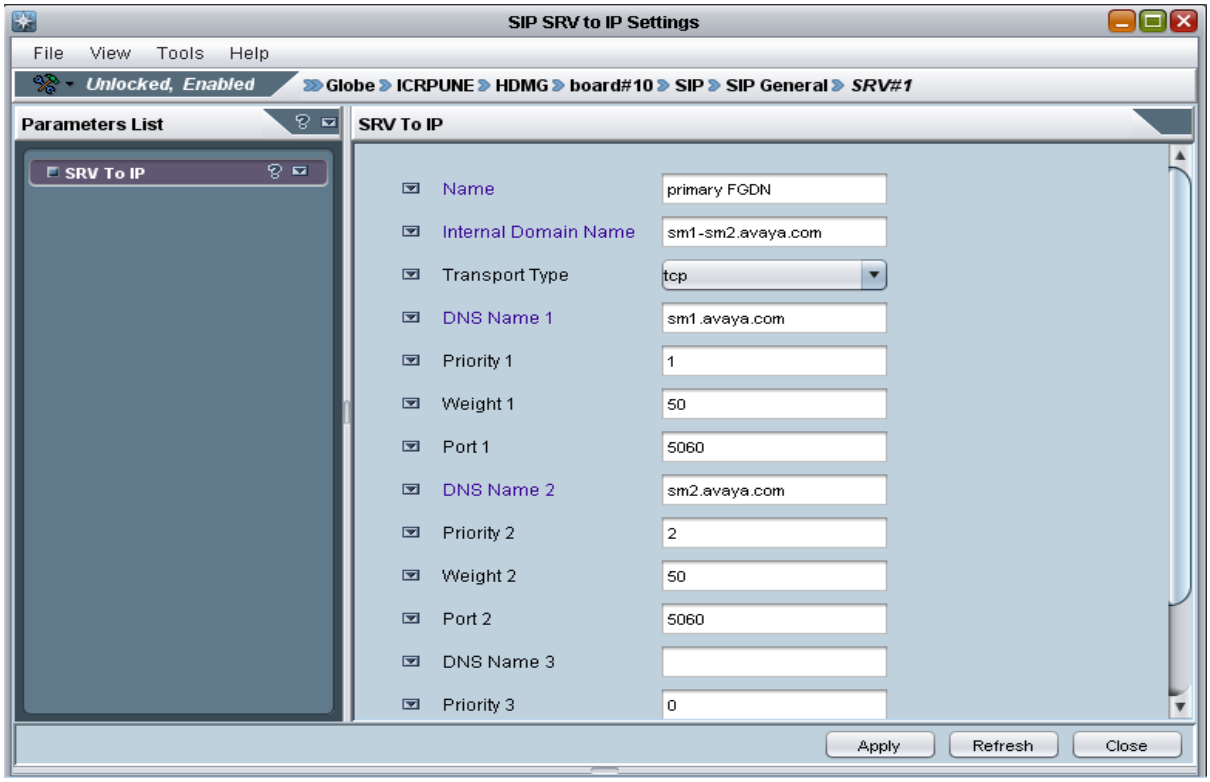
The sum of the weight for "DNS name 1" plus the weight for "DNS name 2" cannot exceed 100 (the recommendation is to make the priority of "DNS name1" more preferred than the priority of "DNS name 2" so the value of weight should not come into play, so using the value of 50 here would be acceptable).

k. **Port2** = **G860 SIP destination port.** For example, 5060.

8. Click **Apply** to save the changes.

9. Return to Navigation and select the row and unlock.

Figure 28: Internal SRV Table



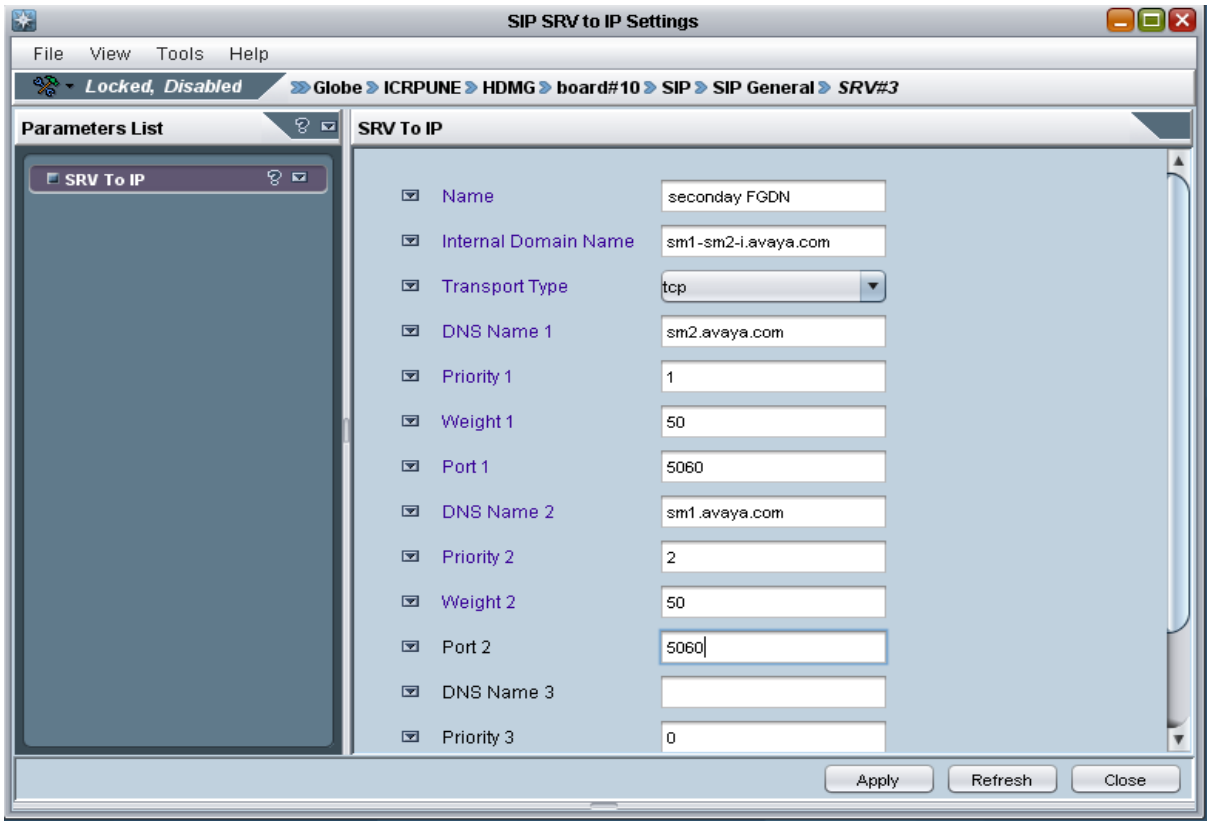


Figure 29: Add SRV records

4.6.2 Creating a Proxy Set

Note

The first SIP Proxy Set (SIP Proxy Set List No. 1 or first row) is reserved for internal use. If it does not already exist in your system, add the first row and name it as “internal use” (or anything) and leave it locked.

1. Navigate to **Board > SIP > SIP General > ProxySet**. (Figure 30)
2. Ensure that the first row exists with **Admin State** as Locked.
3. Add a row to create proxy set 2 and select it to access **SIP Proxy Set Settings** under **Configuration**. (Figure 31)
   a. **Name** = for example, FGDN Use.
   b. **Proxy Load Balancing Method** = disable; (this means that no round robin route between the proxy addresses, round robin works on a rotation basis where the first entry on the proxy list would be used for the first call, then the second entry on the proxy list would be used for the second call; alternating between the entries on this list; load balancing of any kind should be avoided with the Call Preservation feature).
   c. **Enable Proxy Keep Alive**= "Using Options"; (this is a method in SIP used to determine service readiness of the FGDN defined in the proxy list).
   d. **Proxy keep Alive Time** = 60; (this is the interval at which the OPTION message is sent to the FGDNs defined in the proxy list above).
   e. **Is Proxy Hot Swap**=Yes; (this implies the active-active configuration that Core SM redundancy provides).
   f. **Proxy Redundancy Mode**=Homing. (Parking=if primary fails/becomes unavailable stay on secondary until secondary fails/becomes unavailable; Homing=if primary proxy fails/becomes unavailable; go to secondary proxy, when primary proxy recovers, go back to primary proxy).

   Note

   For other fields, use default values.
4. Click **Apply** to save the changes.
5. Under Proxy Servers, add two rows to enter the proxy server information. See FGDN Planning worksheet for details (figure 32).
   a. For **IP Address** (row 1), enter the primary FGDN, for example **sm1-sm2.avaya.com**. Enter your **Transport Type** (for example, TCP).
   b. For **IP Address** (row 2), enter the secondary FGDN, for example **sm1-sm2-i.avaya.com**. Enter your **Transport Type** (for example, TCP).
6. Click **Apply** to save the changes. Right click each row’s Admin State to change from locked to unlocked state.
7. Return to navigation and select the proxy set row and unlock it.

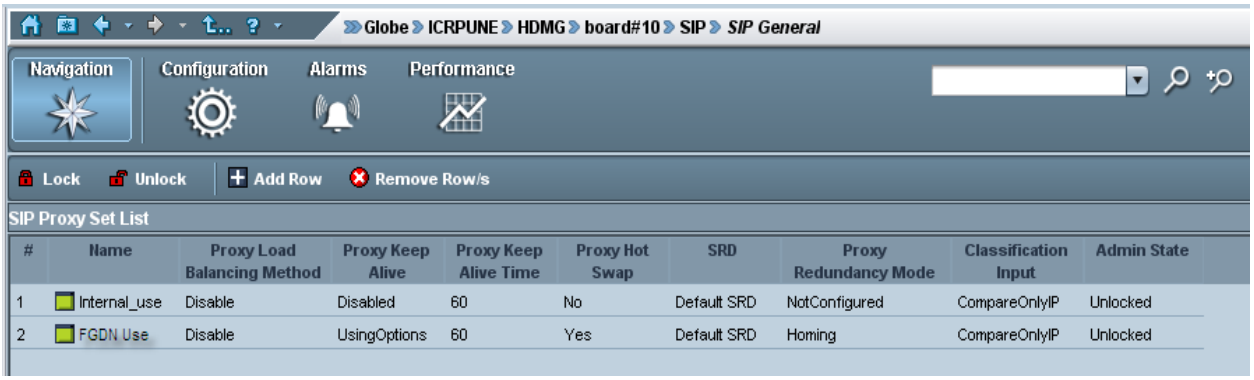


Figure 30: Create a SIP Proxy Set

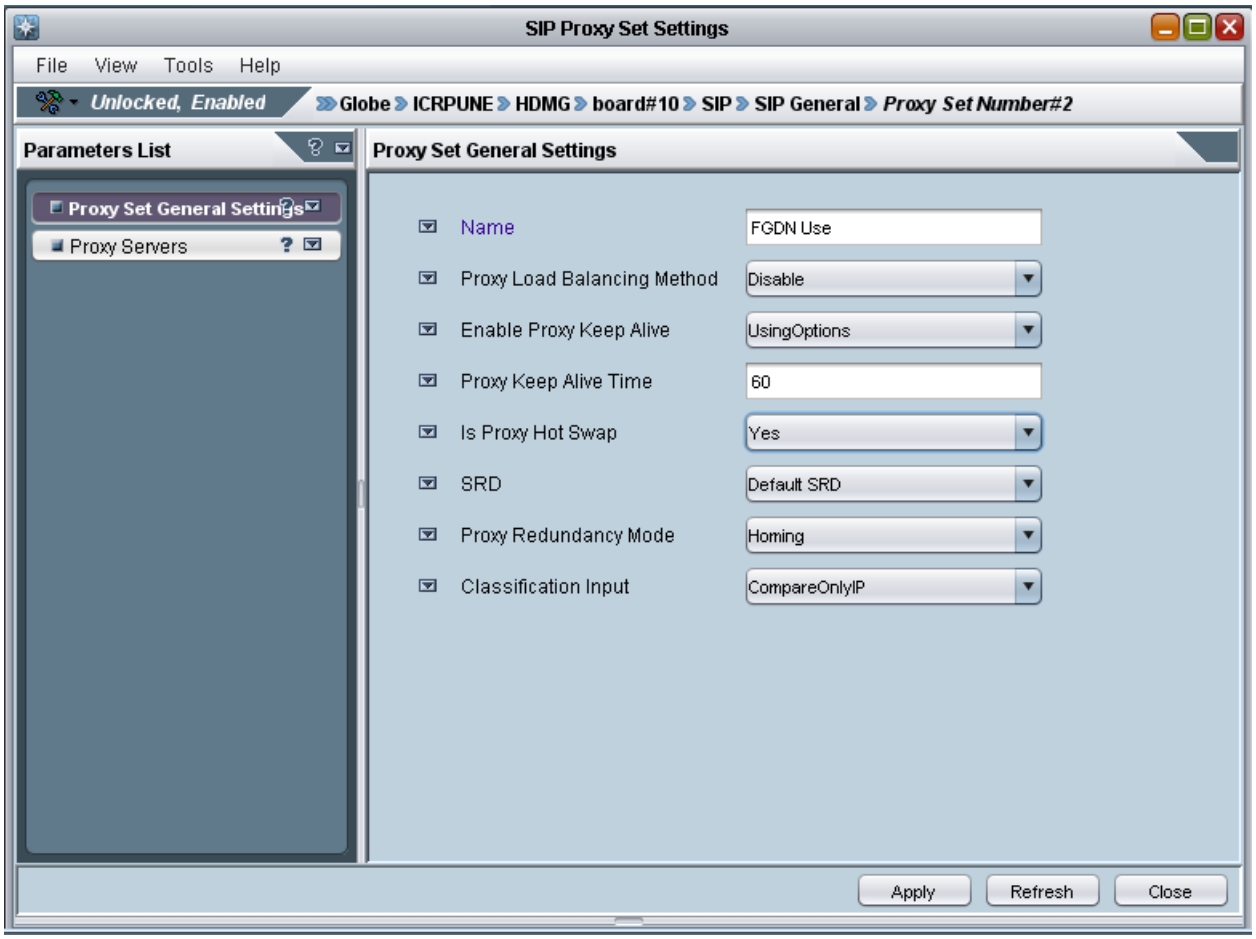


Figure 31: Configure SIP Proxy Set Settings

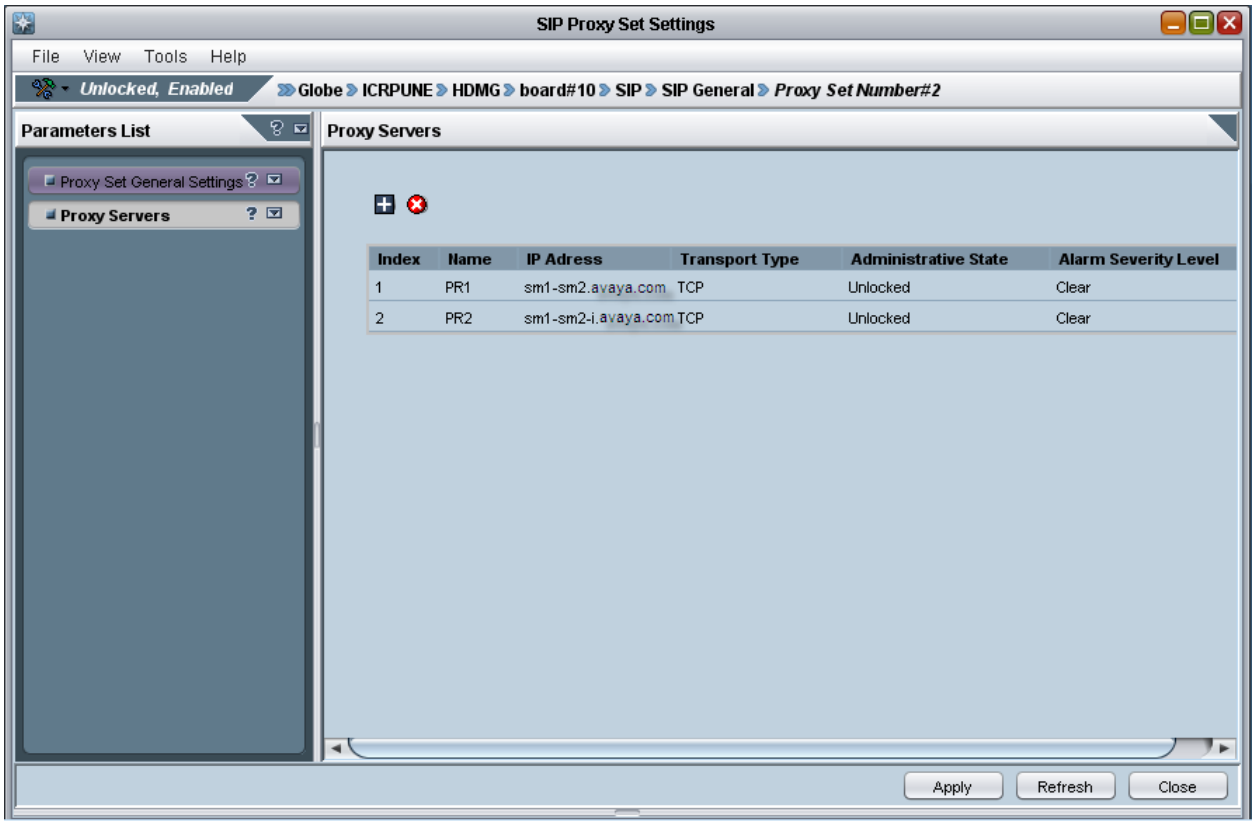


Figure 32: Add Proxy Server Settings

4.6.3 Creating an IP Group Table

Add an IP Profile

1. Navigate to **Board# > SIP > SIP General > IP Profile**. (Figure 33)
2. If there is no IP Profiles listed then add a row to create IP Profile 1.
3. Select the row and select SIP Profile IP settings under **Configuration**. (Figure 34)
4. Create a **Name** and a **Profile Name.** See FGDN Planning Worksheet for details.

   Index to the IP Profile that you wish to assign to this group (in this example it is 1)* no specific modifications for Call Preservation were made to the defaults on the IP Profile Settings.

   Note

   For other fields, use default values.

5. Click **Apply** to save the changes.
6. Go back to navigation and select the row and unlock.

For adding an IP Group

1. Navigate to **Board# > SIP > SIP General > IP Groups**. (Figure 35)
2. Add a row to create an IP group (for example, IP Group #1) and select it to access SIP IP Group Settings under **Configuration**.
3. Administer the following settings (Figure 36):

a. **Proxy Set** = Select the FGDN proxy set administered previously, for example FGDN Use.

b. **SIP Group Name** = Select your SIP domain, for example **avaya.com**.

c. **IP Profile ID** = Select the IP profile administered above, for example **Profile 1**.

d. **Always Use Route Table** = Disable; this allows for use of the proxy set defined earlier in route decisions.

e. **Routing Mode** = Request-URI; the SIP request is routed according to the IP/hostname as specified in the request-uri.

f. **SIP Re-Routing Mode**=Standard.

Note

For other fields, use default values.

7. Click **Apply** to save the changes.

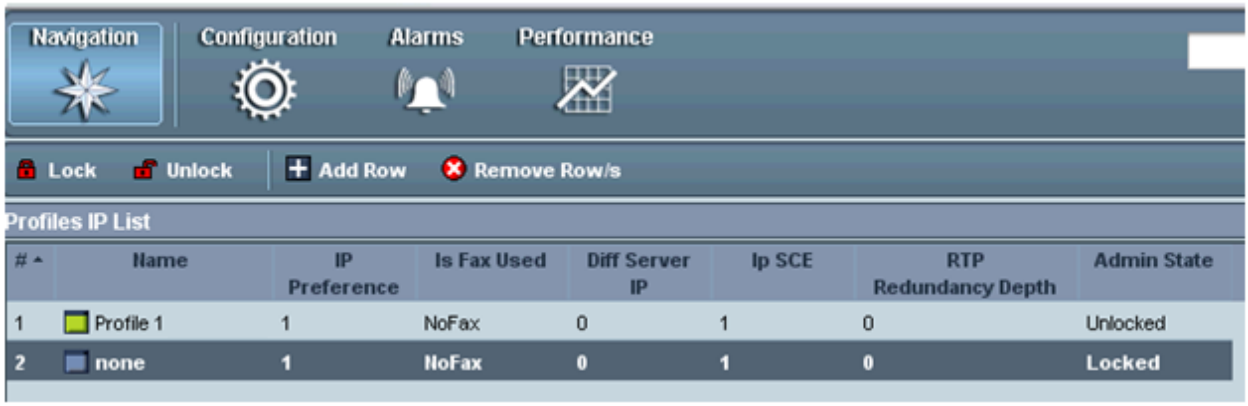


Figure 33: Profiles IP List

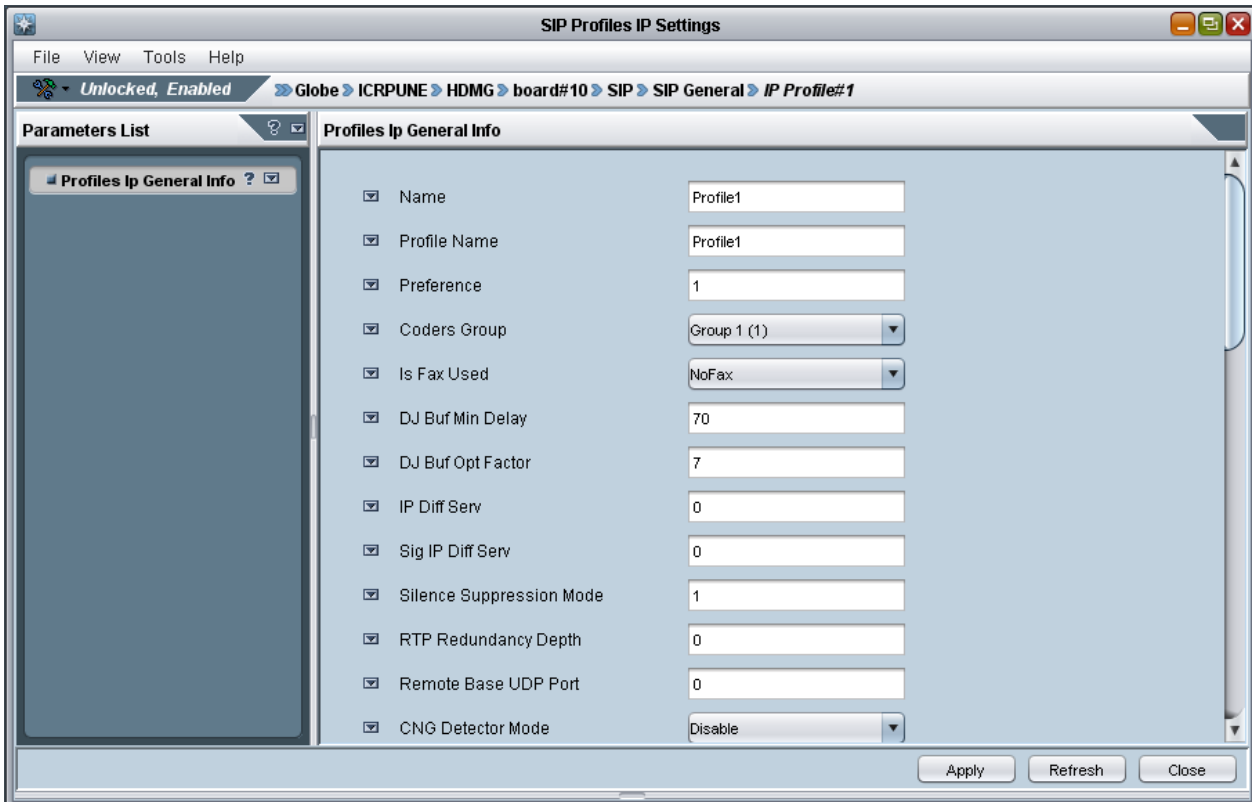


Figure 34: Configure SIP IP Profile Setting

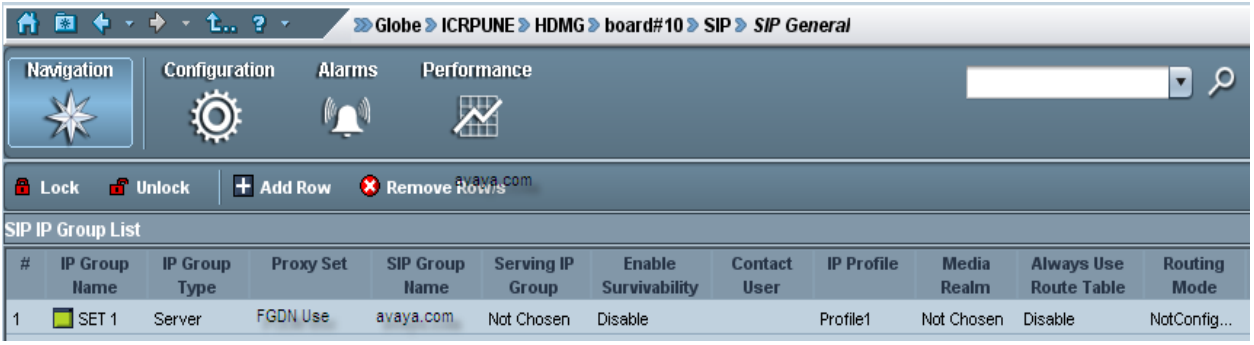


Figure 35: Add SIP IP Group

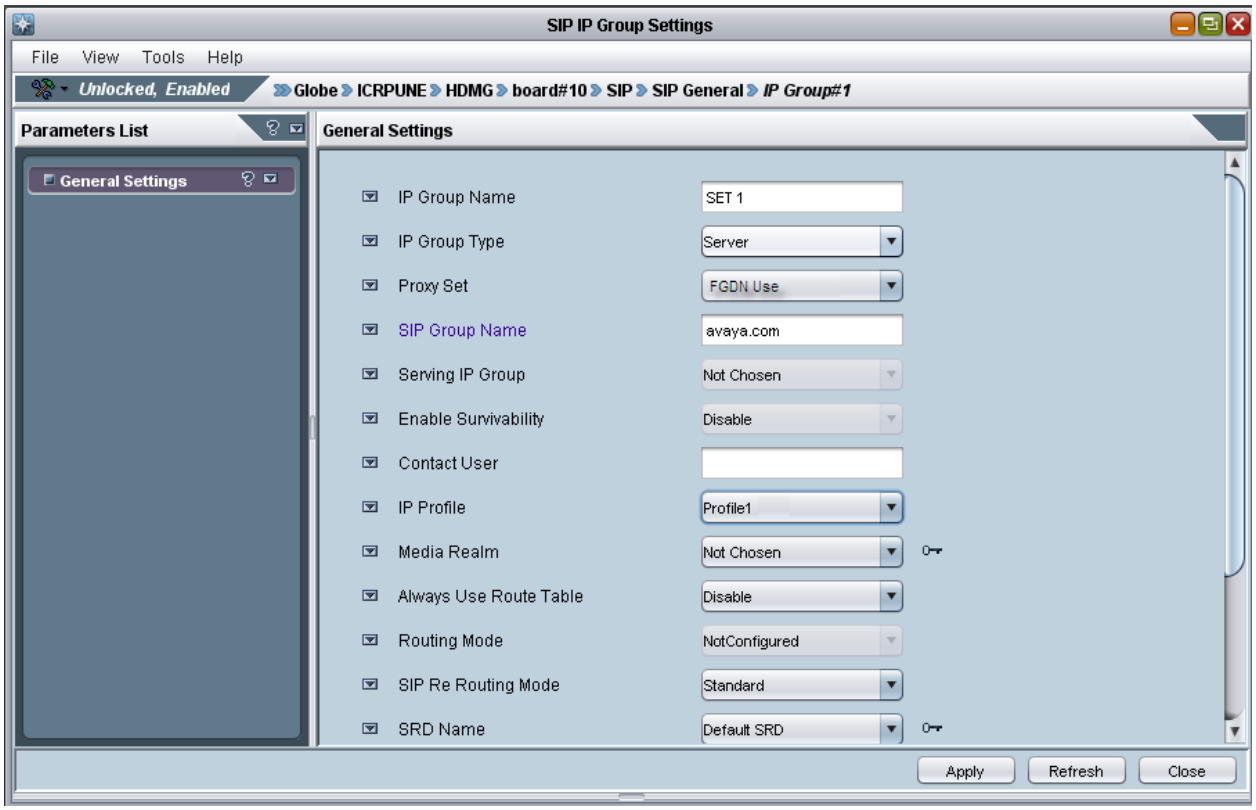


Figure 36: Configure SIP IP Group Settings

4.6.4 Configuring General Parameters

1. Navigate to **Board# > SIP > SIP General**. (Figure 37)
2. Under Configuration, select SIP Protocol Settings. Under **General Settings** modify the following fields (accept defaults otherwise).
   - **Transport Type** = TCP/TLS - UDP is not supported with this Call Preservation feature release. This field must match what is administered on the System Manager for the trusted entity link connection to the G860 SIP entity. (**G860 SIP transport)**
   - **SIP /TCP/TLS Local Port**s needs to match administered System Manager for the trusted entity link connection for the G860 SIP entity. (**G860 SIP local listen port)**
   - **SIP Destination Port** should match the listener port defined for Session Manager for this connection on the SIP entity form. (**G860 SIP destination port**)
   - **TCP Connection Reuse** should be set to "Enable".
   - **TCP Timeout** is the Timer B (INVITE transaction timeout) and Timer F (non-INVITE transaction timeout) to allow for faster failover this parameter can be adjusted down to a minimum value of 6 seconds (so as to not overlap with Session Manager Timer B/F policies for alternate routing). The default is 32 seconds. The example shows 8 seconds.
3. Click **Apply** to save the changes.

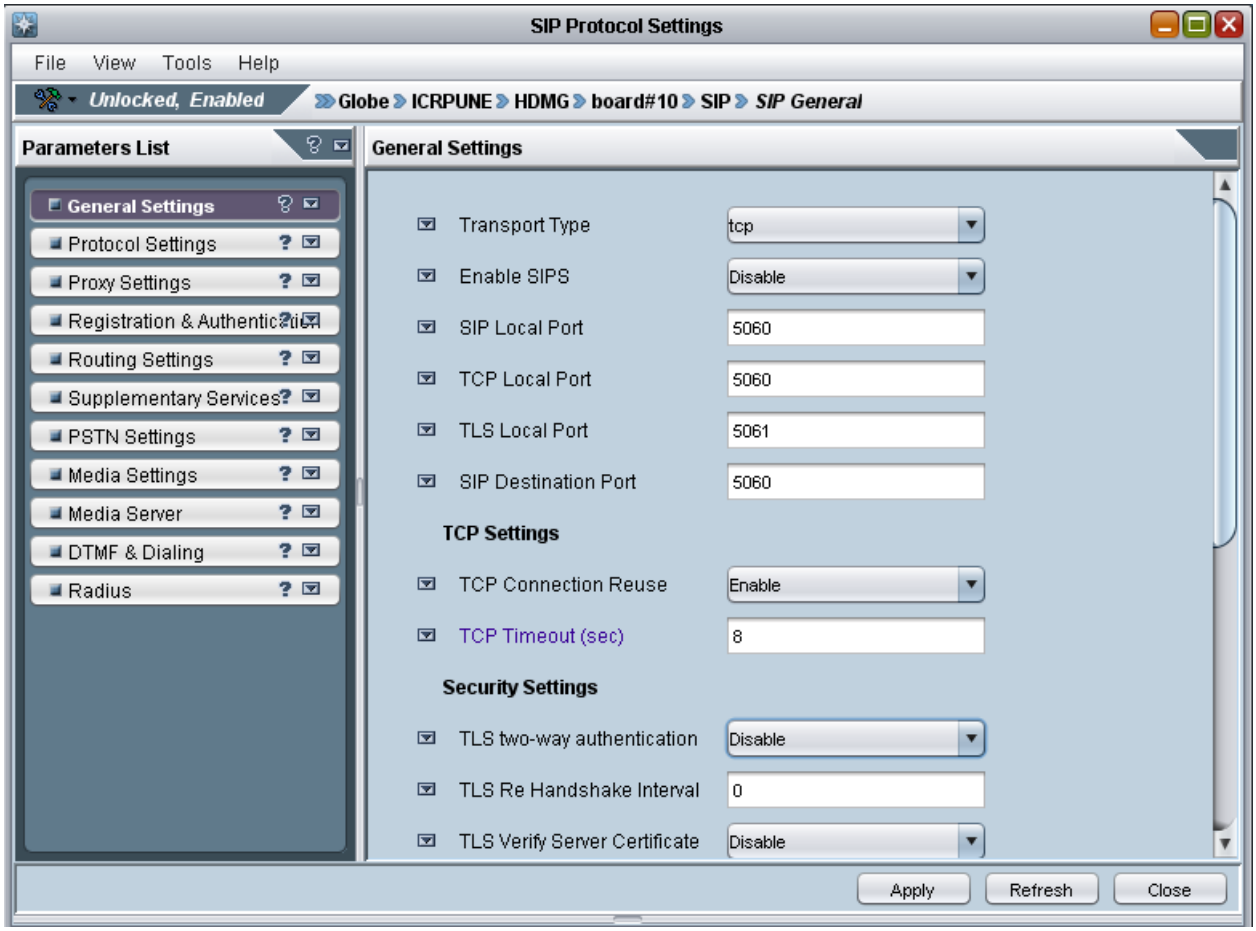


Figure 37: Configuring General Settings

4.6.5 Configuring Proxy Settings

1. Navigate to **Board# > SIP > SIP General**. (Figure 38)
2. Under Configuration, select SIP Protocol Settings. Under Proxy Settings, modify the following fields (accept defaults otherwise).
   - **Enable Proxy** = No (this is to avoid only using a default outbound proxy in routing decisions)
   - **Proxy Name**= sm1-sm2.avaya.com for example (this is the name that is used in the Request-URI and the host part of the To header)
   - **Proxy Redundancy Mode**= Parking (Parking=if primary fails/becomes unavailable stay on secondary until secondary fails/becomes unavailable; Homing=if primary proxy fails/becomes unavailable; go to secondary proxy, when primary proxy recovers, go back to primary proxy).
   - **Redundant Routing Mode**= RedundantProxy
   - **ReRouting Mode**= Routing Table
   - **Use Gateway Name for OPTIONS** = Enable
   - **Proxy DNS Query Type**=SRV
3. Click **Apply** to save the changes.

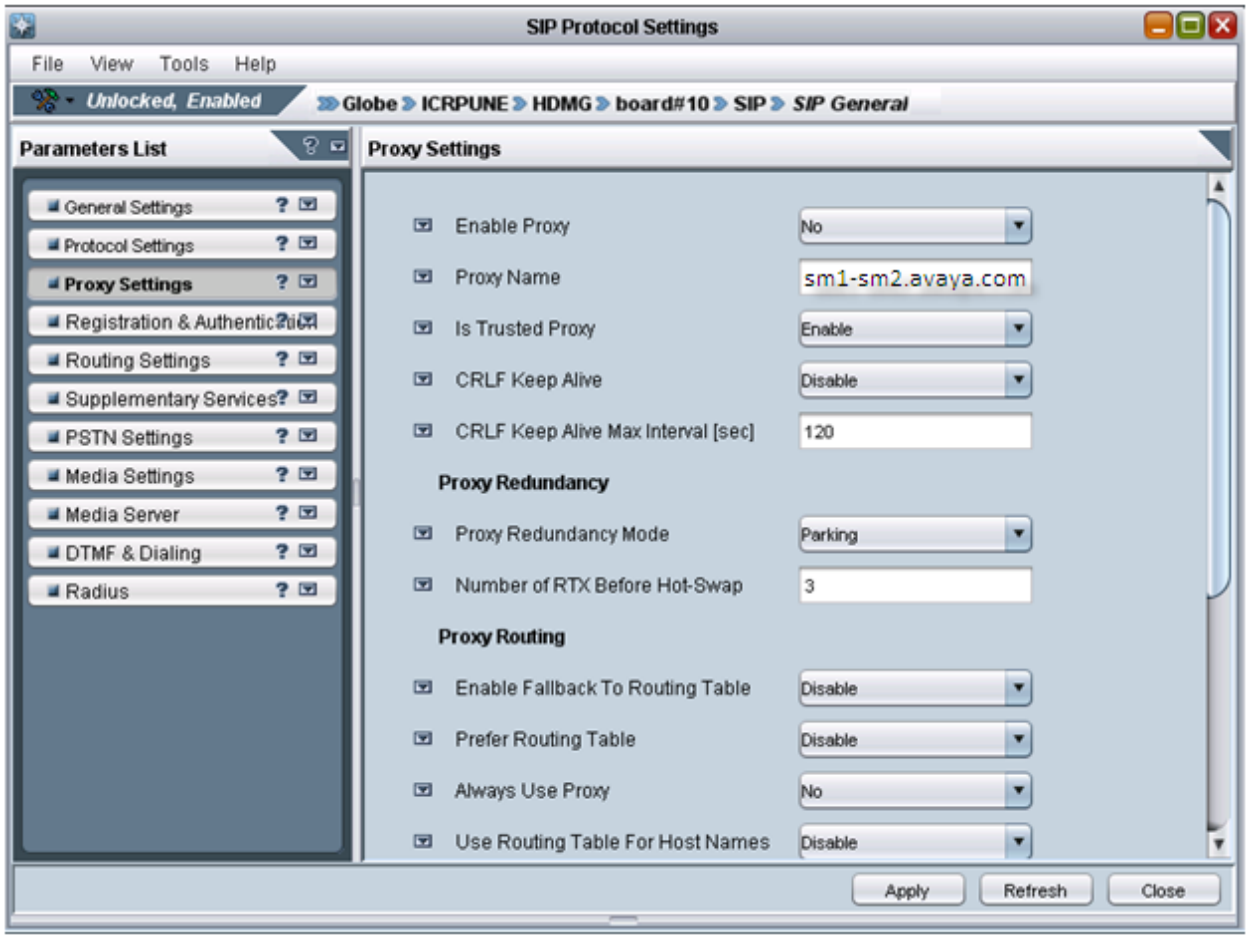


Figure 38: Configuring Proxy Settings

4.6.6 Configuring Routing Settings

1. Navigate to **Board# > SIP > SIP General**. (Figure 39)
2. Under Configuration, select SIP Protocol Settings. Under Routing Settings, modify the following fields (accept defaults otherwise):
   - **Enable Alternate Routing** = Yes (this must be set to allow the G860 to route calls to an alternate Session Manager)
   - **Alternate Routing Mode** = All (enable alternate routing to destination if OPTION fails, poor QoS is detected or is the DNS hostname does not resolve)
   - **Alternate Routing Tel to IP Connectivity Method** = SIP OPTIONS (The destination is considered "down" if the latest OPTION transaction has timed out; any response(including error responses) will bring the state of the destination to "up")
3. Click **Apply** to save the changes.

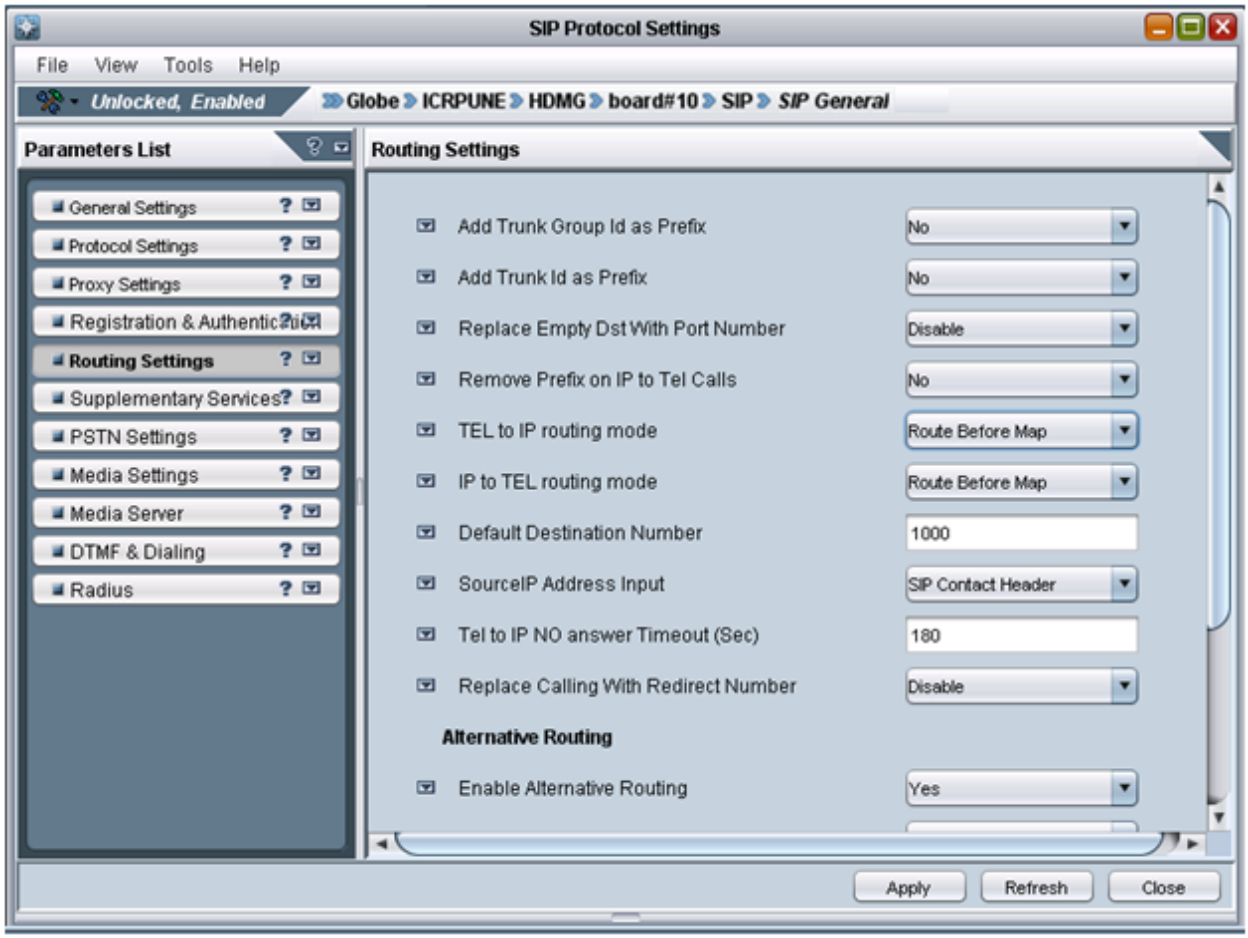


Figure 39: Configuring Routing Settings

4.6.7 Creating Routing Rules

Note

Make sure to add the trunks in the Trunk Group Table under **Board#>SIP>GW/IPtoIP>Trunk group**.

1. Navigate to **Board# > SIP > GW/IP to IP > Routing > Tel to IP/Outbound**. (Figure 40)
2. Add a row or edit existing Tel to IP rows.
3. Click the row and **select SIP Routing Tel to IP Settings** under **Configuration**.
4. Administer the following information. Example data is provided:
   a. **Name**
   b. **Source Trunk Group ID** = Match to an existing trunk group, for example 1.
   c. **Dest Phone Prefix = ***
   d. **Source Phone Prefix = ***

Note

Do not enter IP addresses for any field.

e. **Dest Port** = **G860 SIP Destination Port.** For example, 5060.

f. **Transport Type** = **G860 SIP transport.** For example, TCP.

g. **Dest IP Group** = **G860 IP group identifier.** For example, 1.

h. **IP Profile** = **G860 IP profile identifier.** For example, 1.

Note

For other fields, use default values.

5. Click **Apply** to save the changes.

Note

If you allow IP to Tel calls, administer that routing direction as well. This enables INBOUND call handling to the G860 from the Session Manager.

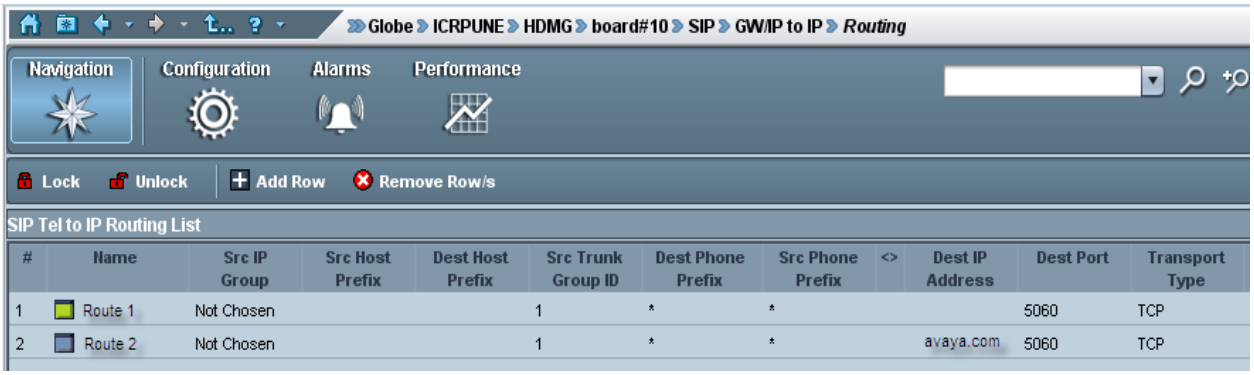


Figure 40: SIP routing Tel to IP settings

4.6.8 Administer Alternate Tel to IP settings:

1. Navigate to **Board# > SIP > GW/IP to IP > Routing > Alternate Tel to IP**. (Figure 41)

The information entered in the table instructs G860 regarding conditions to alternate route after receiving an error response.

2. Click the row and select **SIP Routing Redundant Tel to IP** under **Configuration**.
3. Enter 408 (No Response), 503 (Service Unavailable) and 480 (Temporarily Unavailable). Optionally add additional reason codes as your implementation requires.
4. Click **Apply** to save the changes.

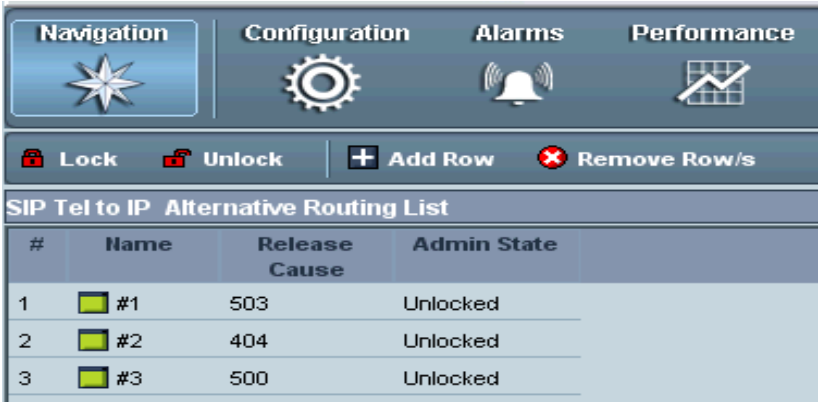


Figure 41: SIP Tel to IP Alternate Routing List

5 Configuring Experience Portal Call Center for Call Preservation

5.1 Configuration assumptions

- All configuration assumptions from Basic Configuration section 4.1 have been met.
- Experience Portal components are installed, configured and operational.

Note

Call routing administration is not covered in this document. Refer to section 1.3 Related Resources for basic system and SIP administration support.

5.2 Configuring the system for Call Preservation

See the **Basic call center configuration** sections for:

- 4.2 Defining a Failover Group
- 4.3 Administering System Manager for Call Preservation
- 4.4 Administering Communication Manager for Call Preservation
- 4.5 Administering Mediant™ 3000 for Call Preservation
- 4.6 Administering G860 for call preservation using an EMS Client

Also, see Appendix 1 – Adding a FGDN to a corporate DNS server.

5.3 Administering Experience Portal for Call Preservation

Avaya Aura® Experience Portal is the latest major release of Avaya Voice Portal and supports Call Preservation using external DNS SRV services. An internal DNS is not administrable.

Note

No administration is required within the Intelligent Customer Routing (ICR) application for Call Preservation support. The ICR_Core SIP Entity link (in System Manager) is not added as a Failover Group peer entity since BSR polling activity is not preserved.

Worksheet references

1. Use the following values from the FGDN Planning Worksheet in Appendix 2:

- External DNS Server IP Address
- primary FGDN
- SIP domain
- SM1 preferred transport
- SM1 TCP failover port
- SM1 TLS failover port

5.3.1 Verify DNS server administration on Experience Portal

1. See Appendix 1 – Adding a FGDN to a corporate DNS server for adding the FGDN to an external DNS server. Refer to Related Resource section 1.3 to locate Experience Portal Installation documentation if the DNS administration was not completed during the install process. DNS administrative experience is required.
2. Verify and modify if necessary the DNS server assigned to each component of the Experience Portal. The DNS server assignment needs to either be specified at install time or can be modified on the operating system post installation (for example, resolv.conf). This DNS server assigned needs to match the corporate external DNS server configured for the Failover Group resolution (see Appendix 1). (**External DNS Server IP Address**)

5.3.2 Adding and configuring a SIP connection for Call Preservation

1. Log on to the Experience Portal Web interface using an account with the Administration user role.
2. On the Experience Portal home page, click **System Configuration > VoIP Connections** in the left navigation pane. (Figure 42)
3. On the **SIP** tab, click **Add** to add a new SIP connection.
4. On the **Add SIP Connection** page (Figure 43), enter the following:
   - **Name**: **Failover Group Name**. For example, sm1-sm2.
   - **Enable**: Yes
   - **Proxy Transport: SM1 preferred transport**. For example, TCP/TLS.
   - **DNS SRV Domain: primary FGDN** For example, sm1 -sm2.avaya.com.

   Note

   The DNS SRV Domain entry must be a valid hostname and match the System Manager defined name for the primary FGDN. The secondary FGDN is resolved by the external DNS administration.

   - **Listener Port**: **SM1 TCP failover port or SM1 TLS failover port.** For example, 5060.
   - **SIP Domain**: **SIP domain**. For example, avaya.com.
5. Enter any remaining configuration detail specific to your environment or accept defaults. The Call Capacity Max Simultaneous Calls field is required and depends on licensed capacities.
6. Click **Save**.
7. If the MPP servers require a reset, you will be prompted with a reset message. Use the **MPP Manager** to reset each MPP.

Note

Verify that the Experience Portal MPP entity link has been added as a peer entity in the System Manager Failover Group administration, section 4.3.3. If the MPP entity was added in System Manager as an FQDN, verify that the transport type and port ID match under **Session Manager>Network Configuration>Local Host Name Resolution**.

Figure 42: VoIP Connection page

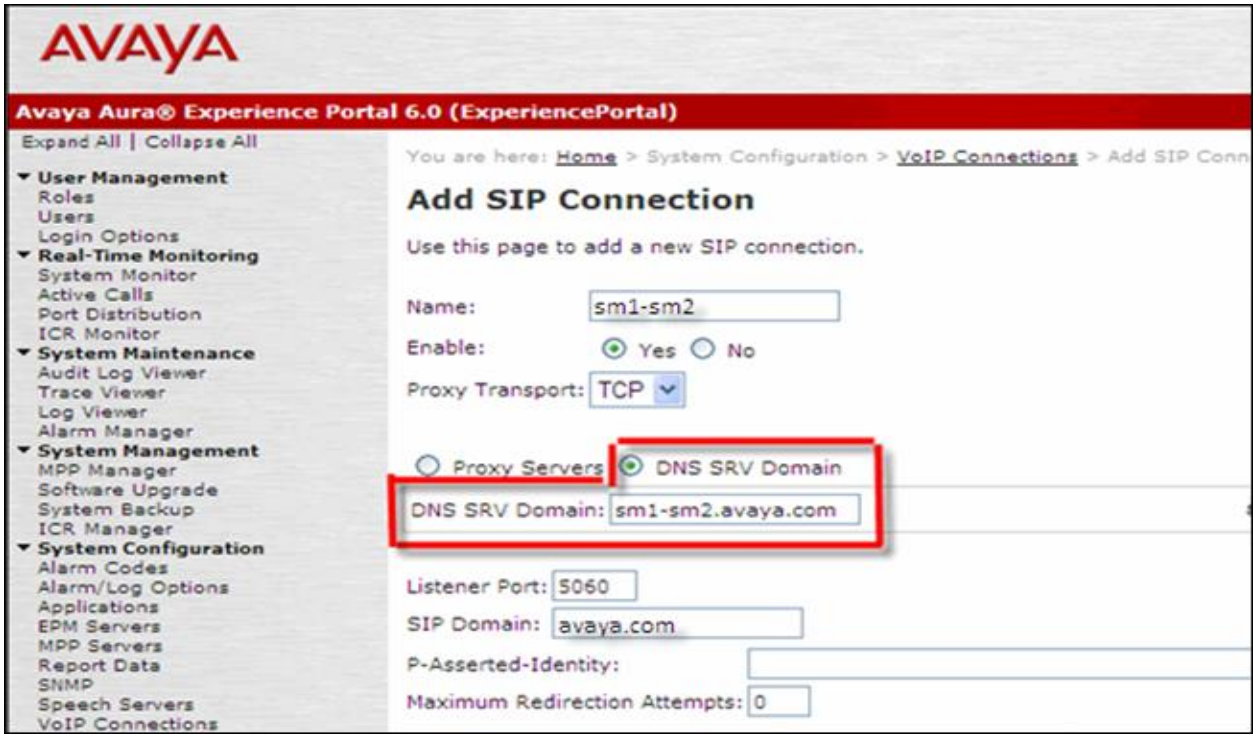


Figure 43: Add SIP Connection page (related to proxy server)

Appendix 1 – Adding a FGDN to a corporate DNS server

Assumptions and notes:

1. The external or corporate DNS server is already administered and operational.
2. Only those with DNS administrative experience and access privileges should attempt administration of the failover group records. Administration examples in this section are intended only as a guide and should not replace corporate procedure or the administrator's experience.
3. The external DNS server is optional for all products except the Experience Portal (EP). It is recommended to utilize the internal product based DNS/FGDN resolution tables where possible for SM, CM, and PSTN-GW described in earlier product-specific sections.

This section describes administering the FGDNs and SM SIP entities in a corporate (external) DNS Server. You will be defining a SIP domain name (zone), hostnames (A-Records) and the FGDNs within Service Records (SRV). The following information will be used from the FGDN Planning Worksheet in Appendix 2 and is information a corporate DNS administrator needs to create the records:

- External DNS Server IP Address
- Failover Group Name
- primary FGDN
- secondary FGDN
- SIP domain
- SM1 SM100 hostname
- SM1 DNS A-Record Name
- SM1 preferred transport
- SM1 TCP failover port
- SM1 TLS failover port
- SM 1 primary FGDN DNS SRV priority
- SM 1 primary FGDN DNS SRV weight
- SM 2 primary FGDN DNS SRV priority
- SM 2 primary FGDN DNS SRV weight
- SM2 SM100 hostname
- SM2 DNS A-Record Name
- SM2 preferred transport
- SM2 TCP failover port
- SM2 TLS failover port
- SM 1 secondary FGDN DNS SRV priority
- SM 1 secondary FGDN DNS SRV weight
- SM 2 secondary FGDN DNS SRV priority
- SM 2 secondary FGDN DNS SRV weight

Windows 2003 DNS Manager

Adding a forward lookup zone

Procedure:

1. From your Windows server, open the DNS Manager application.
2. In the console tree, expand the **Forward Lookup Zones** folder.
3. If the SIP domain name does not already exist, right-click on Forward Lookup Zone, and then click **New Zone** to open the New Zone Wizard. (Figure 44)
4. Follow the instructions in the wizard to create a new primary zone.
5. At the **Zone Name** prompt, enter the SIP domain name used by the FGDN being added, avaya.com in this example. (**SIP domain**)

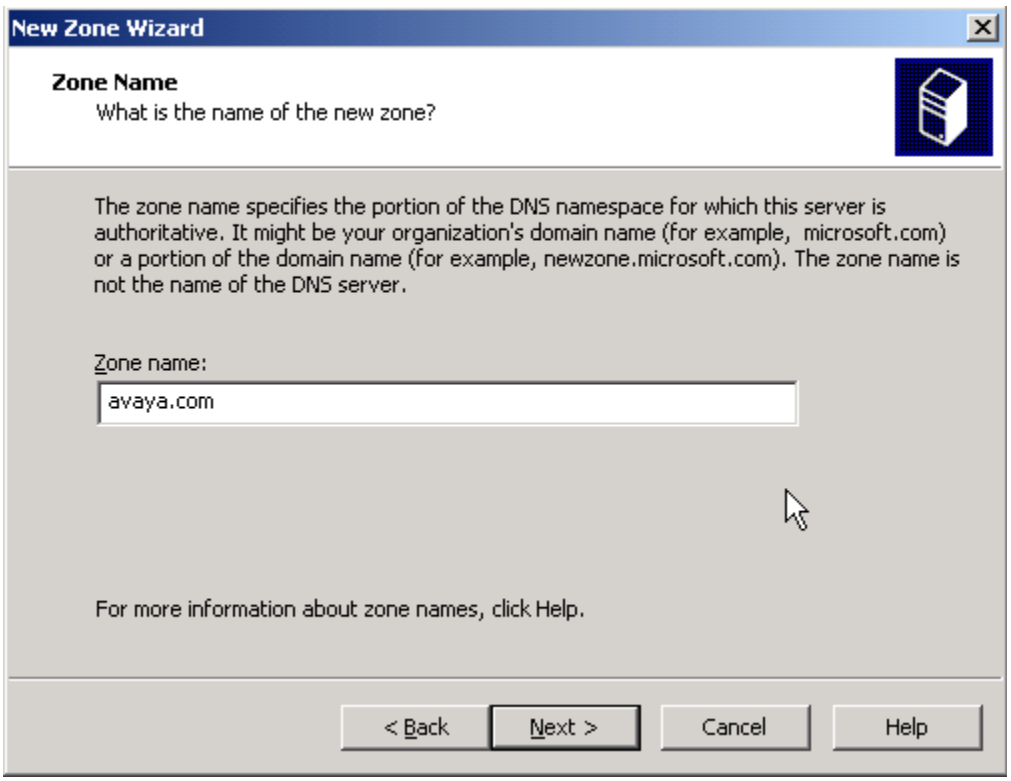


Figure 44: Adding Zone name

Note

This domain name must match the name administered in **Elements >Routing > Domains** on the System Manager web console and SIP domain entry on the FGDN Planning Worksheet.

Adding Host A-Records to the zone

Procedure:

1. In the console tree, right-click the SIP Domain zone and click New Host. (Figure 45) If the zone already existed, expand the folder and review the Host list.
2. In the **Name text** box, enter the primary SMs SIP Entity hostname. (for example, sm1) (SM1 SM100 hostname)

   Note

   The SM management host name and IP address is different from the SM Security Module (SM100) SIP Entity host name and IP address. On an existing system the SM-mgmt host may already exist. Make sure the SM SM100 SIP Entity is represented with a different host name.

3. In the **IP address** text box, enter the IP address for the SM SIP Entity. (**SM1 SM100 IP Address**)
4. Accept defaults. In this example, sm1.avaya.com is automatically populated and is the appropriate FQDN name. (**SM1 DNS A-Record Name**)
5. Click **Add Host** to add the new host record to the zone. The record appears in the zone directory. The Add Host window stays open for the next entry.
6. Add the secondary SMs SIP Entity hostname (sm2). (**SM2 SM100 hostname**)
7. In the **IP address** text box, enter the IP address for the SM SIP Entity. (**SM2 SM100 IP Address**)
8. Accept defaults. In this example, sm2.avaya.com is automatically populated and is the appropriate FQDN name. (**SM2 DNS A-Record Name**)
9. Close the **Add Host** window.

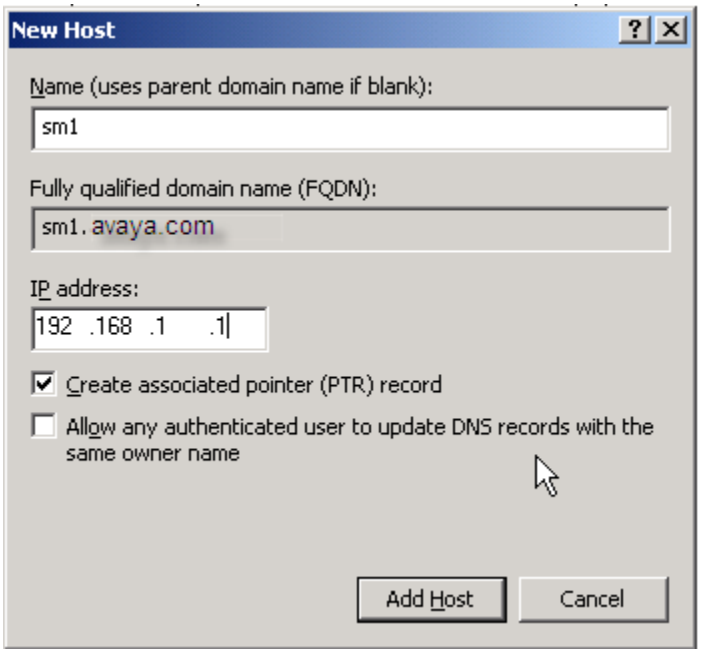


Figure 45: New Host

Adding Service Location Records (SRV)

Two new domains will be added under the SIP domain zone: one for the primary FGDN and one for the secondary FGDN. Within each domain, four SRV records are added (each SM host will have two records, one for each transport type-TCP/TLS). The following instructions demonstrate adding the primary FGDN domain and administering the first SRV record using TLS transport. Refer to the table, provided in step 8, for adding the remaining three SRV records. Then repeat in step 9 to add the secondary FGDN and its SRV records. Notice that the primary FGDN SRV records identify the primary FGDN and set the priority order between the two SMs. The secondary FGDN SRV records reverse the priority order.

Procedure:

1. In the console tree, right-click the zone and select **New Domain.** Enter the **Failover Group Name** as identified on the FGDN Planning Worksheet. (sm1-sm2 in the example) (**Failover Group Name**)
2. Click **OK** to add the new domain to the zone. A new folder is created under the zone name.
3. In the console tree, right-click the newly created domain folder and click **Other New Records**.
4. Select resource record type **Service Location (SRV)**.
5. Click **Create Record**.
6. In **New Resource Record**, enter the information as shown below. (Figure 46)
   a. The domain field automatically is populated with the full FGDN name. (sm1-sm2.avaya.com in the example) (**primary FGDN**)
   b. Change Service to **_sips**. (_sips = tls; _sip=tcp)
   c. Keep Protocol as **_tcp**. (this is describing the base protocol encompassing both TCP and TLS for the SIP transport)
   d. Priority is **0** in the example **(SM1 primary FGDN DNS SRV priority)**
   e. Change Weight to **1** in the example (**SM 1 primary FGDN DNS SRV weight)**
   f. Enter the Port Number being used by the primary FGDN. (5061 in the example) (**SM1 TLS failover port**)
   g. Under **Host offering this service**, enter the primary Session Manager FQDN (sm1.avaya.com in the example). (**SM1 DNS A-Record Name**)
7. Click **OK** to add the new record to the zone.
8. Follow this table to enter the remaining three SRV records for the primary FGDN (Note: the first record was completed in the previous step). Utilize the following references from the FGDN Planning Worksheet: **primary FGDN**;**SM1 TCP failover port; SM2 TLS failover port; SM2 TCP failover port; SM2 primary FGDN DNS SRV weight; SM2 primary FGDN DNS SRV priority; SM1 DNS A-Record Name; SM2 DNS A-record Name**

	Domain	Service	Protocol	Priority	Weight	Port number	Host
1	sm1-sm2.avaya.com	_sips	_tcp	0	1	5061	sm1.avaya.com
2	sm1-sm2.avaya.com	_sips	_tcp	1	1	5061	sm2.avaya.com
3	sm1-sm2.avaya.com	_sip	_tcp	0	1	5060	sm1.avaya.com
4	sm1-sm2.avaya.com	_sip	_tcp	1	1	5060	sm2.avaya.com

9. Repeat Steps 1-7 to create the secondary failover group domain (sm1-sm2-i) and to add the 4 SRV records listed below. Notice the reverse host priority. Utilize the following references from the FGDN Planning Worksheet: **secondary FGDN; SM1 TLS failover port; SM1 TCP failover port; SM2 TLS failover port; SM2 TCP failover port; SM2 secondary FGDN DNS SRV weight; SM2 secondary FGDN DNS SRV priority; SM1 DNS A-Record Name; SM2 DNS A-record Name.**

	Domain	Service	Protocol	Priority	Weight	Port number	Host
1	sm1-sm2-i.avaya.com	_sips	_tcp	0	1	5061	sm2.avaya.com
2	sm1-sm2-i.avaya.com	_sips	_tcp	1	1	5061	sm1.avaya.com
3	sm1-sm2-i.avaya.com	_sip	_tcp	0	1	5060	sm2.avaya.com
4	sm1-sm2-i.avaya.com	_sip	_tcp	1	1	5060	sm1.avaya.com

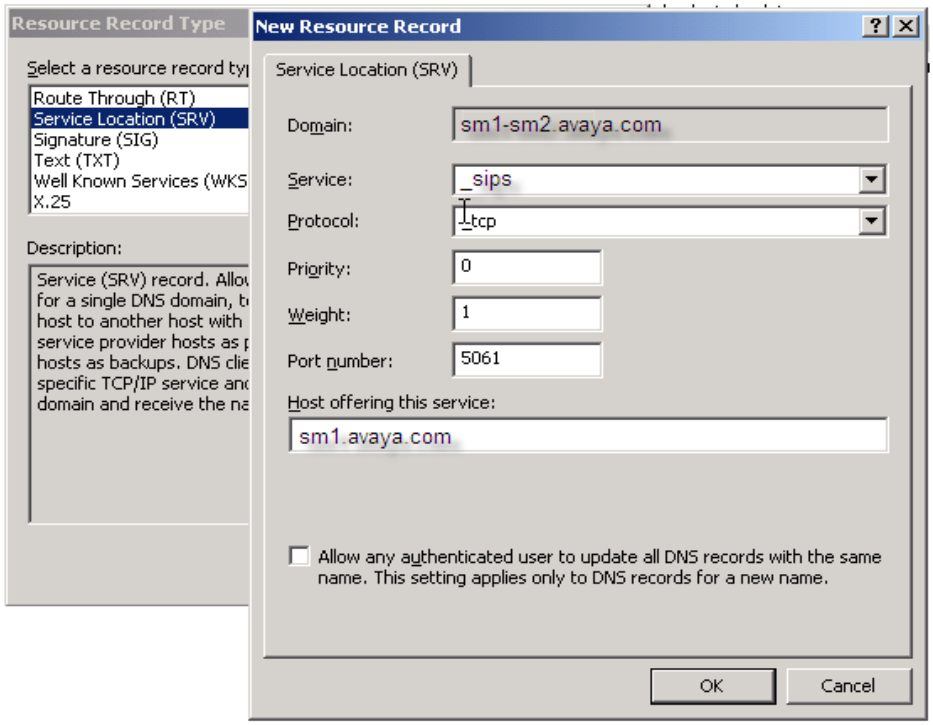


Figure 46: New SRV Resource record

A DNS zone file example

The following is an example of how DNS SRV and DNS A-records appear in a zone file after administering an FGDN. See figure 47.

```
$ORIGIN avaya.com.
$TTL 300
@ IN SOA dns.avaya.com. hostmaster.avaya.com. (
        2011021001      ; serial
        21600           ; refresh after 6 hours
        3600            ; retry after 1 hour
        604800          ; expire after 1 week
        86400           ; minimum TTL of 1 day
)
;
; Name server for this zone
      IN    NS    dns.avaya.com.
dns   IN    A     10.6.2.250

; A records for SM instances
sm1   60    IN    A     192.168.1.1
sm2   60    IN    A     192.168.2.1
;

; SRV records for primary FGDN sm1-sm2.avaya.com
_sips._tcp.sm1-sm2      60   IN    SRV   0     1     5061  sm1.avaya.com.
_sips._tcp.sm1-sm2      60   IN    SRV   1     1     5061  sm2.avaya.com.
_sip._tcp.sm1-sm2      60    IN    SRV   0     1     5060  sm1.avaya.com.
_sip._tcp.sm1-sm2      60    IN    SRV   1     1     5060  sm2.avaya.com.

; SRV records for secondary (inverse) FGDN sm1-sm2-i.avaya.com
_sips._tcp.sm1-sm2-i    60   IN    SRV   0     1     5061  sm2.avaya.com.
_sips._tcp.sm1-sm2-i    60   IN    SRV   1     1     5061  sm1.avaya.com.
_sip._tcp.sm1-sm2-i     60   IN    SRV   0     1     5060  sm2.avaya.com.
_sip._tcp.sm1-sm2-i     60   IN    SRV   1     1     5060  sm1.avaya.com.
```

Figure 47: Zone files

Figure 48 shows example PTR records that map the SM100 SIP IP address back to the SM SM100 hostname. Reverse lookup is optional but included here for completeness.

```
$ORIGIN 6.10.in-addr.arpa.
$TTL 300
@ IN SOA dns.avaya.com. hostmaster.avaya.com. (
        2011021402      ; serial
        21600           ; refresh after 6 hours
        3600            ; retry after 1 hour
        604800          ; expire after 1 week
        86400           ; minimum TTL of 1 day
)
;
;
@       60      IN      NS      dns.avaya.com.
250.2   60      IN      PTR     dns.avaya.com.

10.1    60      IN      PTR     sm1.avaya.com.
10.2    60      IN      PTR     sm2.avaya.com.
```

Figure 48: Reverse lookup zone files

Appendix 2 – FGDN Planning Worksheet

Reference	Description	Value	Example Value
External DNS Server IP Address (optional)	The corporate DNS server used to resolve A-record and SRV-record entries for the SMs and the FGDNs respectively		192.168.1.3
SIP domain	The domain for which the SM SIP proxy is authoritative		avaya.com
Failover Group Name	A descriptive name of the FGDN assigned on the SMGR **Elements>Session Manager>Network Configuration> Failover Groups** page		sm1-sm2
SM1 SIP entity	The name assigned to the SM1-SM100 under **Elements>Routing>SIP Entities**		sm1
SM1 SM100 hostname	The first element of the SM1 DNS A-Record Name without the domain.		sm1
SM1 DNS A-Record Name	The fully qualified domain name chosen to represent the **SM1-SM100**		sm1.avaya.com
SM1 SM100 IP Address	The IPV4 compliant address of the SM1-SM100 assigned on the SMGR **Elements>Routing>SIP Entities** page or optionally within an external DNS A-record.		192.168.1.1
SM1 node name	The descriptive name assigned within CM(**ch node-names ip**) to Session Manager1		sm1
SM1 TCP failover port	The TCP listen port assigned to SM1 within the SMGR under **Elements>Routing>SIP Entities** in the "Port" section for TCP Failover Port		5060
SM1 TLS failover port	The TLS listen port assigned to SM1 within the SMGR under **Elements>Routing>SIP Entities** in the "Port" section for TLS Failover Port.		5061
SM1 preferred transport	The transport (TLS/TCP) that will be used by SM1 in any product specific link(CM/PSTN-GW/EP) and SM entity link definition with the FGDN peer entities (optionally you could have both TCP and TLS in use to different peer entities –		TCP to CM TCP to M3K TCP to EP

	if that is the case, record specific transport for each here)		
primary FGDN	This is the Session Manager 1 Preferred Failover Group Domain Name as specified on the SMGR under **Elements>Session Manager>Network Configuration> Failover Groups.** This same value will be used in any external DNS SRV record and internal product SRV/FGDN definitions		sm1-sm2.avaya.com
SM1 primary FGDN DNS SRV weight	The sum of the weight for SM1 plus the weight for SM2 cannot exceed 100. The recommendation is to make the priority of SM1 more preferred than the priority of SM2 so the value of weight should not come into play, so using the value of 50 here would be acceptable. In the case of the external DNS – the important note to remember is that the value of both SMs in the FGDN for weight need to be the SAME to ensure load balancing is NOT invoked		50(or 1 for the external DNS example)
SM1 primary FGDN DNS SRV priority	The priority of SM1 in the primary FGDNordered pair. The lower the value the more preferred. The recommendation is to make this value more preferred or lower than the value for SM2.		1
SM2 primary FGDN DNS SRV weight	The sum of the weight for SM1 plus the weight for SM2 cannot exceed 100. The recommendation is to make the priority of SM1 more preferred than the priority of SM2 so the value of weight should not come into play, so using the value of 50 here would be acceptable. In the case of the external DNS – the important note to remember is that the value of both SMs in the FGDN for weight need to be the SAME to ensure load balancing is NOT invoked		50(or 1 for the external DNS example)
SM2 primary FGDN DNS SRV priority	The priority of SM2 in the primary FGDNordered pair. The lower the		2

	value the more preferred. The recommendation is to make this value less preferred or higher than the value for SM1.		
SM2 SIP entity	The name assigned to the SM2-SM100 under **Elements>Routing>SIP Entities**		sm2
SM2 SM100 hostname	The first element of the SM2 DNS A-Record Name without the domain.		sm2
SM2 DNS A-Record Name	The fully qualified domain name chosen to represent SM2-SM100		sm2.avaya.com
SM2 SM100 IP Address	The IPV4 compliant address of the SM2-SM100 assigned on the SMGR **Elements>Routing>SIP Entities** page or optionally within an external DNS A-record.		192.168.2.1
SM2 node name	The descriptive name assigned within CM(**ch node-names ip**) to Session Manager1		sm2
SM2 TCP failover port	The TCP listen port assigned to SM1 within the SMGR under **Elements>Routing>SIP Entities** in the "Port" section for TCP Failover Port		5060
SM2 TLS failover port	The TLS listen port assigned to SM1 within the SMGR under **Elements>Routing>SIP Entities** in the "Port" section for TLS Failover Port		5061
SM2 preferred transport	The transport (TLS/TCP) that will be used by SM2 in any product specific link(CM/PSTN-GW/EP) and SM entity link definition with the FGDN peer entities (optionally you could have both TCP and TLS in use to different peer entities – if that is the case, record specific transports for each here)		TCP to CM TCP to M3K TCP to EP
secondary FGDN	This is the Session Manager 2 Preferred Failover Group Domain Name as specified on the SMGR under **Elements>Session Manager>Network Configuration> Failover Groups.** This same value will be used in any external DNS SRV record and internal product SRV/FGDN definitions		sm1-sm2-i.avaya.com
SM 1 secondary FGDN DNS SRV weight	The sum of the weight for SM1 plus the weight for SM2 cannot		50(or 1 for the external DNS example)

	exceed 100. The recommendation is to make the priority of SM2 more preferred than the priority of SM1 so the value of weight should not come into play, so using the value of 50 here would be acceptable. In the case of the external DNS – the important note to remember is that the value of both SMs in the FGDN for weight need to be the SAME to ensure load balancing is NOT invoked		
SM 1 secondary FGDN DNS SRV priority	The priority of SM1 in the secondary FGDN ordered pair. The lower the value the more preferred. The recommendation is to make this value more preferred or lower than the value for SM1.		2
SM 2 secondary FGDN DNS SRV weight	The sum of the weight for SM1 plus the weight for SM2 cannot exceed 100. The recommendation is to make the priority of SM2 more preferred than the priority of SM1 so the value of weight should not come into play, so using the value of 50 here would be acceptable. In the case of the external DNS – the important note to remember is that the value of both SMs in the FGDN for weight need to be the SAME to ensure load balancing is NOT invoked		50 (or 1 for the external DNS example)
SM 2 secondary FGDN DNS SRV priority	The priority of SM1 in the primary FGDN ordered pair. The lower the value the more preferred. The recommendation is to make this value less preferred or higher than the value for SM2.		1
CM SIP entity name	The name assigned to the CM under **Elements>Routing>SIP Entities**		cm
CM node name	The descriptive name assigned within CM(**ch node-names ip**) to the CM IP interface that will be used for Call Preservation enabled SIP traffic (for example, Procr or a CLAN board identifier)		procr
CM near-end port	The TCP/TLS port used on the CM signaling group form (**ch sig <x>**)that will match the CM entity		5060

	link defined on SMGR under **Elements>Routing>Entity Links** to each of the SMs in the Failover Group		
CM SIP transport	Choose the transport type that matches the entity link definition on System Manager for the Communication Manager SIP entity under **Elements>Routing>Entity Links**.		TCP
SM1 signaling group identifier	The SIP Signaling Group assigned to the SM1 SM100 far-end node that uses the SM1 failover port chosen for the selected transport type. (use "**list sig**" to view all assigned signaling resources)		1
SM2 signaling group identifier	The SIP Signaling Group assigned to the SM2 SM100 far-end node that uses the SM2 failover port chosen for the selected transport type. (use "**list sig**" to view all assigned signaling resources)		2
SM1 trunk group identifier	The SIP Trunk Group assigned to the SM1 Signaling Group Identifier (use "**list trunk"** to view all assigned trunks)		1
SM2 trunk group identifier	The SIP trunk Group assigned to the SM2 Signaling Group Identifier (use "**list trunk"** to view all assigned trunks)		2
CM primary FGDN route	The route pattern (**ch route <x>**) that will be used with the primary FGDN for link status and node resolution. The route pattern should have **SM1 trunk group identifier** as preference 1 and **SM2 trunk group identifier** as preference 2.		1
CM secondary FGDN route	The route pattern (**ch route <x>**) that will be used with the primary FGDN for link status and node resolution. The route pattern should have **SM2 trunk group identifier** as preference 1 and **SM1 trunk group identifier** as preference 2.		2
M3K SIP entity name	The name assigned to the M3K under **Elements>Routing>SIP Entities**		m3k
M3K SIP local listen ports	The TCP and TLS port used on the M3K that will match the M3K entity link defined on SMGR under		5060 5061

	Elements>Routing>Entity Links to each of the SMs in the Failover Group. These ports define the SIP listener ports on the M3K. Recall UDP is not supported at this time for Call Preservation.		
M3K SIP Transport	Choose the transport type that matches the entity link definition on System Manager for the M3K SIP entity under **Elements>Routing>Entity Links**. Recall UDP is not supported at this time for Call Preservation		TCP
M3K SIP destination port	Specify the Session Manager TCP or TLS port used in the SIP Entity Link defined on SMGR for this M3K. It is recommended that both SM1 and SM2 use the same transport for connection to the Mediant™ 3000		5060
M3K IP group identifier	IP Group establishes the M3K call routing rules for the primary and secondary FGDNs. **Configuration>VOIP>Control Network>IP Group Table**		1
M3K proxy set identifier	**Configuration>VOIP>SIP Definitions>Proxy & Registration** This Proxy set defines the set of FGDNs that will be used in call routing		1
M3K IP profile identifier	The preferred IP profile to use when routing calls to/from the FGDNs. This allows you to group common parameters that may be associated or descriptive of the types of calls coming into/out of the specified trunk. **Configuration>VOIP>Coders and Profiles>IP Profile Settings**		1
EP SIP entity name	The name assigned to the EP-MPP under **Elements>Routing>SIP Entities**		EP
G860 SIP entity name	The name assigned to the G860 under **Elements>Routing>SIP Entities**		G860
G860 SIP local listen ports	The TCP and TLS port used on the G860 that will match the G860 entity link defined on SMGR under **Elements>Routing>Entity Links** to		5060 5061

	each of the SMs in the Failover Group. These ports define the SIP listener ports on the G860. Recall UDP is not supported at this time for Call Preservation.		
G860 SIP Transport	Choose the transport type that matches the entity link definition on System Manager for the G860 SIP entity under **Elements>Routing>Entity Links**. Recall UDP is not supported at this time for Call Preservation		TCP
G860 SIP destination port	Specify the Session Manager TCP or TLS port used in the SIP Entity Link defined on SMGR for this G860. It is recommended that both SM1 and SM2 use the same transport for connection to the Mediant™ 3000		5060
G860 IP group identifier	IP Group establishes the G860 call routing rules for the primary and secondary FGDNs.		1
G860 proxy set identifier	This Proxy set defines the set of FGDNs that will be used in call routing		1
G860 IP profile identifier	The preferred IP profile to use when routing calls to/from the FGDNs. This allows you to group common parameters that may be associated or descriptive of the types of calls coming into/out of the specified trunk.		1