# Table of Contents

## 1 Overview ............................................................................................................. 11
  1.1 Features ............................................................................................................. 12
  1.2 Benefits ............................................................................................................. 13
  1.3 Simplicity .......................................................................................................... 13
  1.4 ARM-Routed Devices ....................................................................................... 13
  1.5 Third-Party Open-Source Software ................................................................. 14

## 2 Getting Started with the ARM ............................................................................ 15
  2.1 Logging in .......................................................................................................... 15
  2.2 Getting Acquainted with the ARM GUI ............................................................ 15
    2.2.1 Getting Acquainted with the Network Map Topology Layer ..................... 16
    2.2.2 Getting Acquainted with the Network Map Quality Layer ....................... 18
    2.2.3 Getting Acquainted with Network Map Page Actions ............................... 21
    2.2.3.1 Node Information and Actions ............................................................... 21
    2.2.3.2 VoIP Peer Information and Actions ....................................................... 24
    2.2.3.3 Connection Information and Actions ..................................................... 25
    2.2.3.4 Peer Connection Information and Actions ............................................. 26
    2.2.4 Peer Connections Page Actions ................................................................. 28
    2.2.5 Connections Page Actions ......................................................................... 29

## 3 Defining a Network .............................................................................................. 31
  3.1 Adding Connections .......................................................................................... 31
  3.2 Synchronizing Topology ................................................................................... 32
  3.3 Building Star Topology ..................................................................................... 33
  3.4 Testing a Routing Rule ..................................................................................... 34
  3.5 Network Statistics ............................................................................................ 37
    3.5.1 Overall Network Statistics .......................................................................... 37
    3.5.1.1 Network Summary ................................................................................ 37
    3.5.1.2 General Statistics .................................................................................. 37
    3.5.1.3 Top 5 Routes Pane ................................................................................ 39
    3.5.1.4 Test Route ............................................................................................. 40
    3.5.2 Statistics on a Selected Element ................................................................. 40

## 4 Administering Users ........................................................................................... 41
  4.1 Administering Users ......................................................................................... 41
  4.2 Administering User Groups ............................................................................... 43
  4.3 Administering the Property Dictionary ............................................................ 45
  4.4 Administering LDAP Servers ........................................................................... 45
    4.4.1 Adding / Editing a Property ....................................................................... 50

## 5 Configuring Settings .......................................................................................... 53
  5.1 Network Services Settings ................................................................................ 53
    5.1.1 Editing a Syslog Server .............................................................................. 53
    5.1.2 Adding/Editing an NTP Server .................................................................... 55
  5.2 Call Flow Settings ............................................................................................ 56
    5.2.1 Adding a Normalization Group .................................................................... 56
    5.2.2 Adding/Editing a Prefix Group ................................................................... 57
    5.2.3 Normalization Before Routing ................................................................... 59
    5.2.4 Policy Studio .............................................................................................. 60
      5.2.4.1 Example of a Policy Studio Rule ............................................................ 62
5.3 Routing Settings ..................................................................................................... 63
   5.3.1 Configuring Criteria for a Quality Profile ....................................................... 63
   5.3.2 Configuring a Time Based Routing Condition ............................................... 64
   5.3.3 Configuring SIP Alternative Route Reason ..................................................... 66
   5.3.4 Configuring Global Routing Settings ............................................................... 68
5.4 Administration Settings ......................................................................................... 70
   5.4.1 Configuring a Software License ....................................................................... 70
   5.4.2 Securing the ARM .......................................................................................... 71
   5.4.3 Adding/Editing an Operator ............................................................................. 72
5.5 Adding a Routing Server ....................................................................................... 73
   5.5.1 Editing a Routing Server .................................................................................. 74
   5.5.2 Locking/Unlocking a Routing Server ............................................................. 75
6 Defining Calls Routing ............................................................................................ 77
   6.1 Adding a Routing Group ..................................................................................... 78
       6.1.1 Editing a Routing Group .............................................................................. 79
       6.1.2 Moving a Routing Group ............................................................................ 80
       6.1.3 Deleting a Routing Group .......................................................................... 81
   6.2 Adding a New Routing Rule .............................................................................. 82
       6.2.1 Editing a Routing Rule .............................................................................. 89
       6.2.2 Moving a Routing Rule .............................................................................. 89
       6.2.3 Deleting a Rule ........................................................................................... 90
   6.3 Testing a Route ................................................................................................... 92
   6.4 Viewing Routing Performance Statistics ........................................................... 92
       6.4.1 Group Statistics | ARM Statistics ............................................................... 92
   6.5 Using the Routing Rules Table View Page ......................................................... 94
7 Viewing Alarms ....................................................................................................... 95
   7.1 Collecting Information via SNMP to Enhance Network Telephony Performance 96
   7.2 Locating a Specific Alarm .................................................................................. 98
8 Migrating Device Routing to the ARM ................................................................. 99
   8.1 AudioCodes Device Application Types .............................................................. 99
   8.2 ARM Network Routing Logic ........................................................................... 99
       8.2.1 SBC Routing Logic ................................................................................... 99
       8.2.2 Gateway Routing Logic ............................................................................ 99
       8.2.3 Hybrid Device Routing Logic ................................................................... 100
   8.3 Connecting the Device to the ARM Topology Server ....................................... 100
   8.4 Migrating SBC/Gateway/Hybrid Routing to the ARM ..................................... 103
   8.5 Migrating SBC Routing to the ARM ................................................................. 104
   8.6 Migrating Media Gateway Routing to the ARM .............................................. 107
   8.7 Migrating Hybrid Routing to the ARM ............................................................. 109
A Checklist for Migrating SBC Routing to the ARM .............................................. 113
B Prefixes .................................................................................................................. 117
C Examples of Normalization Rules ......................................................................... 119
D Call Routing .......................................................................................................... 121
E Configuring the SBC to Send SIP Requests other than INVITE to the ARM ....... 123
List of Figures

Figure 2-1: ARM GUI - Network Page - Map View ................................................................. 15
Figure 2-2: Network Map Layers .......................................................................................... 18
Figure 2-3: Quality Layer ....................................................................................................... 19
Figure 2-4: Example: Quality Layer – Connection ................................................................. 20
Figure 2-5: Example: Quality Layer - Peer Connection ......................................................... 21
Figure 2-6: Node Information ................................................................................................. 21
Figure 2-7: Node Actions ....................................................................................................... 22
Figure 2-8: Node Update ....................................................................................................... 23
Figure 2-9: SIP Trunk Information ......................................................................................... 24
Figure 2-10: PBX Information ............................................................................................... 24
Figure 2-11: PSTN Information ............................................................................................. 24
Figure 2-12: IP Phone Information ....................................................................................... 24
Figure 2-13: VoIP Peer Actions ............................................................................................. 24
Figure 2-14: VoIP Peer Update ............................................................................................. 25
Figure 2-15: Connection Information .................................................................................... 25
Figure 2-16: Connection Actions .......................................................................................... 25
Figure 2-17: Connection Definition ...................................................................................... 26
Figure 2-18: Peer Connection Information ............................................................................ 26
Figure 2-19: Peer Connection Actions .................................................................................. 27
Figure 2-20: ARM GUI - Network Page - Peer Connections ................................................. 27
Figure 2-21: ARM GUI - Network Page - Peer Connections ................................................. 28
Figure 2-22: ARM GUI - Network Page - Connections ......................................................... 29
Figure 3-1: Add Connection .................................................................................................. 31
Figure 3-2: Defining a Connection ........................................................................................ 31
Figure 3-3: Build Star ............................................................................................................ 33
Figure 3-4: Test Route Menu Item ....................................................................................... 34
Figure 3-5: Test Route .......................................................................................................... 34
Figure 3-6: Route Path ......................................................................................................... 35
Figure 3-7: Test Route Details .............................................................................................. 35
Figure 3-8: Strip + from the Number .................................................................................... 35
Figure 3-9: Example of a Test Call with a 'Quality' Advanced Routing Condition .............. 36
Figure 3-10: Network Summary .......................................................................................... 37
Figure 3-11: General Statistics Pane .................................................................................... 38
Figure 3-12: Click + to Project a Zoom-in of the Graph to the Front .................................... 39
Figure 3-13: Top 5 Routes .................................................................................................... 39
Figure 3-14: Top 5 Routes – Route Details .......................................................................... 39
Figure 3-15: Popular Path Visualized in the Network Map .................................................... 40
Figure 3-16: Network Summary Pane Displaying Statistics Related to a Selected Element ... 40
Figure 4-1: Users Page – Users tab ..................................................................................... 41
Figure 4-2: User Details ....................................................................................................... 42
Figure 4-3: User Details ....................................................................................................... 42
Figure 4-4: Users Groups ..................................................................................................... 43
Figure 4-5: User Group Details ............................................................................................ 43
Figure 4-6: Users Page – Property Dictionary tab ................................................................. 43
Figure 4-7: Users Page – LDAP Servers tab ....................................................................... 45
Figure 4-8: LDAP Server Settings ....................................................................................... 46
Figure 4-9: LDAP Properties ............................................................................................... 47
Figure 4-10: Users Page – LDAP Servers tab – AD Summary ............................................. 48
Figure 4-11: LDAP Server Settings ..................................................................................... 48
Figure 4-12: Property Dictionary .......................................................................................... 50
Figure 4-13: Property .......................................................................................................... 51
Figure 5-1: Network Services ............................................................................................... 53
Figure 5-2: Syslog Details ...................................................................................................... 54
Figure 5-3: NTP Servers ....................................................................................................... 55
Figure 5-4: NTP Server Details ............................................................................................ 55
Figure 5-5: Normalization Groups ....................................................................................... 56
Figure 5-6: Normalization Groups ....................................................................................... 56
Figure 7-5: Searching for a Specific Alarm ................................................................. 98
Figure 8-1: Web Interface - Remote Web Services ....................................................... 100
Figure 8-2: Web Interface - HTTP Remote Services – Add Row ............................... 101
Figure 8-3: Web Interface - Remote Web Services – HTTP Remote Hosts .................. 101
Figure 8-4: Web Interface - Remote Web Services - HTTP Remote Hosts - Add ............ 102
Figure 8-5: Web Interface – Device Connected to ARM Topology Server ...................... 102
Figure 8-6: Web Interface – Remote Web Services - Routers ...................................... 102
Figure 8-7: Web Interface – SIP Interfaces .................................................................... 103
Figure 8-8: Web Interface – SIP Interfaces Table - Configuring a SIP Interface .................. 103
Figure 8-9: Web Interface – IP Groups ........................................................................ 104
Figure 8-10: Web Interface – IP Groups - Configuring an IP Group ............................... 104
Figure 8-11: Web Interface – IP-to-IP Routing ............................................................ 105
Figure 8-12: Web Interface – IP-to-IP Routing Table – Add Row – Rule tab .................... 105
Figure 8-13: Configuring a Routing Rule in the ARM .................................................. 105
Figure 8-14: Web Interface - Routing Settings Page .................................................... 107
Figure 8-15: Web Interface - IP Groups Page ............................................................... 107
Figure 8-16: Web Interface - Trunk Group Settings ...................................................... 108
Figure 8-17: Add Proxy Set – for SBC ........................................................................... 109
Figure 8-18: Proxy Sets .................................................................................................. 109
Figure 8-19: Add New Proxy Address .......................................................................... 110
Figure 8-20: IP Group for the SBC Application ............................................................ 110
Figure 8-21: New Proxy Set for Media Gateway Application ......................................... 110
Figure 8-22: Proxy Sets ............................................................................................... 111
Figure 8-23: Add New Proxy Address .......................................................................... 111
Figure 8-24: IP Group for the SBC Application ............................................................ 111
Figure E-1: Web Interface – Message Conditions ....................................................... 123
Figure E-2: Web Interface – IP-to-IP Routing ............................................................. 123
## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2-1:</td>
<td>ARM GUI – Map View</td>
<td>16</td>
</tr>
<tr>
<td>Table 2-2:</td>
<td>Network Page’s Map View – Network Entities</td>
<td>17</td>
</tr>
<tr>
<td>Table 2-3:</td>
<td>Quality Color Codes</td>
<td>19</td>
</tr>
<tr>
<td>Table 2-4:</td>
<td>Network Page’s Map View – Viewing Node Information</td>
<td>22</td>
</tr>
<tr>
<td>Table 4-1:</td>
<td>User Group Details</td>
<td>44</td>
</tr>
<tr>
<td>Table 4-2:</td>
<td>LDAP Server Settings</td>
<td>46</td>
</tr>
<tr>
<td>Table 4-3:</td>
<td>Active Directories Summary</td>
<td>48</td>
</tr>
<tr>
<td>Table 4-4:</td>
<td>Add Property</td>
<td>51</td>
</tr>
<tr>
<td>Table 5-1:</td>
<td>Syslog Details</td>
<td>54</td>
</tr>
<tr>
<td>Table 5-2:</td>
<td>NTP Server Details</td>
<td>55</td>
</tr>
<tr>
<td>Table 5-3:</td>
<td>Normalization Groups</td>
<td>57</td>
</tr>
<tr>
<td>Table 5-4:</td>
<td>Prefix Group Details</td>
<td>58</td>
</tr>
<tr>
<td>Table 5-5:</td>
<td>Normalization Before Routing</td>
<td>59</td>
</tr>
<tr>
<td>Table 5-6:</td>
<td>Policy Studio Settings</td>
<td>61</td>
</tr>
<tr>
<td>Table 5-7:</td>
<td>Configuring Criteria for a Quality Profile</td>
<td>64</td>
</tr>
<tr>
<td>Table 5-8:</td>
<td>Time Condition</td>
<td>66</td>
</tr>
<tr>
<td>Table 5-9:</td>
<td>Routing Settings</td>
<td>69</td>
</tr>
<tr>
<td>Table 5-10:</td>
<td>Security Settings</td>
<td>71</td>
</tr>
<tr>
<td>Table 5-11:</td>
<td>Operator Details</td>
<td>72</td>
</tr>
<tr>
<td>Table 5-12:</td>
<td>Routing Server Details</td>
<td>73</td>
</tr>
<tr>
<td>Table 5-13:</td>
<td>Server Details</td>
<td>74</td>
</tr>
<tr>
<td>Table 6-1:</td>
<td>Call Routing / Test Mode Combinations</td>
<td>84</td>
</tr>
<tr>
<td>Table 6-2:</td>
<td>Source Settings</td>
<td>84</td>
</tr>
<tr>
<td>Table 6-3:</td>
<td>Destination Settings</td>
<td>85</td>
</tr>
<tr>
<td>Table 6-4:</td>
<td>Routing Actions</td>
<td>87</td>
</tr>
<tr>
<td>Table 6-5:</td>
<td>Routing Actions – Call Discard</td>
<td>88</td>
</tr>
<tr>
<td>Table 7-1:</td>
<td>SNMP Destination Details</td>
<td>97</td>
</tr>
<tr>
<td>Table A-1:</td>
<td>SBC Migration Checklist</td>
<td>113</td>
</tr>
<tr>
<td>Table B-1:</td>
<td>Prefixes</td>
<td>117</td>
</tr>
</tbody>
</table>
Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: July-24-2017

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.
## Related Documentation

<table>
<thead>
<tr>
<th>Manual Name</th>
<th>Related Documentation</th>
</tr>
</thead>
</table>

## Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at [http://www.audiocodes.com/downloads](http://www.audiocodes.com/downloads).

## Document Revision Record

<table>
<thead>
<tr>
<th>LTRT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>41880</td>
<td>Initial release</td>
</tr>
<tr>
<td>41881</td>
<td>New features: Adding ADs, Users and Users Groups, Adding an LDAP Property, Adding a User, Adding a User Property, Adding a User Group, Configuring Settings, Adding Operators, Adding Routing Servers, Configuring a Syslog Server, Adding a Number Manipulation Group, Adding a Prefix Group, Adding an NTP Server, Adding a Software License, Routing</td>
</tr>
<tr>
<td>41882</td>
<td>New: Section 8, Migrating Media Gateway Routing</td>
</tr>
<tr>
<td>41883</td>
<td>Modified performance capability, added new GUI screens, deleted Network Table view, added Time-Base Routing, added Policy Studio, other minor additions.</td>
</tr>
<tr>
<td>41885</td>
<td>Time-based routing condition; Pcon Weight; Detach (Pcons); Routing Rules Hits Counting; Load Balancing; Single Sign On; New ARM login; Router Lock/Unlock; Test Routing Rule.</td>
</tr>
</tbody>
</table>
1 Overview

This document shows how to use the AudioCodes Routing Manager (ARM). The ARM is a LINUX-based, software-only, telephony management product which expedites and streamlines IP telephony routing for enterprises with multiple globally distributed branches. The ARM determines the quickest, least expensive, and best call quality routes in packet networks.

Routing data, previously located on the SBC, Unified Communications (UC) application (e.g., Microsoft's Skype for Business), or Media Gateway, is now located on the ARM server. If an enterprise has an SBC in every branch, a single ARM, deployed in HQ, can route all calls in the globally distributed corporate network to PSTN, the local provider, enterprise headquarters, or to the IP network.

Routing rules, configured by the IT manager in the ARM's Routing Table, perform the routing.

If an enterprise has only one or two branches, its IT manager can easily independently implement maintenance changes. In globally distributed enterprises, IT managers until now had to laboriously implement changes, multiple times, per branch. With the ARM, IT managers implement changes only once, saving significant labor and time resources and costs.

The figure below shows a typical, globally-distributed, multi-branch enterprise VoIP network.
VoIP networks like this typically require:

- Distributed routing & policy enforcement
- Distributed PSTN
- Multiple VoIP network elements configurations (i.e., SBC, Media Gateway)
- Multiple Dial Plans
- SIP Interworking between IP PBXs
- Large number of end users policies
- Efficient ARM routing management

1.1 Features

ARM features are as follows:

- Centralized, enterprise-wide session routing management
- Centralized & optimized PSTN routing
- Automatic discovery of VoIP network elements
- Smart Dial Plan management
  - Centralized Dial Plan logic; simple, clear, intuitive and easy to maintain
  - Dialing plan dry test by 'Test Route' simulation
  - Incoming number manipulation
  - Outgoing number manipulation
  - User properties manipulation
- Reduces SIP trunk costs
  - Implements Tail-End-Hop-Off Routing
  - Assigns a number of actions to routing rules with different sequence
  - Source and destination number manipulation
- Advanced routing based on user properties
- Quality-based routing
- Time-based routing
- Flexible load balancing
- Automatic topology network generation
- Manual network generation (simply drawing lines between dots)
- On-the-fly routing calculation:
  - Centralized management of Network Routing Rules
  - Routing decision is based on source / destination call parameters, and user properties
  - Predefined weights on connections
  - User information from external Data Bases (e.g., LDAP)
  - Flexible API
- Intuitive graphical representation of the enterprise VoIP network
- Personalized Call Routing Applications
  - Communication-Enabled Business Process
  - Full on-line management and routing via REST API
  - Fallback to SBC routing table if call does not match ARM configuration
1.2 Benefits

The ARM benefits users as follows:

- Reduces operational time spent on designing and provisioning network topology
- Reduces OPEX, avoiding routing configuration of VoIP network elements
- Reduces time spent implementing network evolutions such as:
  - Adding new connections to PSTN (e.g., SIP trunks)
  - Adding new branches to the enterprise VoIP network
  - Modifying user voice services privileges

1.3 Simplicity

- VoIP network elements registering in the ARM
- Auto-discovery of VoIP peers
- One-click topology network creation, star formation
- Customized topology network.
  - Configuring a connection is as simple as drawing a line.
  - Modify by adding, deleting and changing connections
- ARM connects to users data base

1.4 ARM-Routed Devices

The following devices can be routed by the ARM:

- Mediant 9000 SBC
- Mediant 4000 SBC
- Mediant 2600 E-SBC
- Mediant SE/VE SBC
- Mediant 1000B Gateway and E-SBC and Mediant 1000B MSBR
- Mediant 800B Gateway and E-SBC and Mediant 800B MSBR
- Mediant 500 E-SBC
- Mediant 500L MSBR and Mediant 500 MSBR
1.5 Third-Party Open-Source Software

The following third-party open-source software is supported by the ARM:

- CentOS Linux 6.6
- Spring Framework (released under version 2.0)
- MariaDB relational database management system
- ActiveMQ (using the Apache 2.0 license)
- HiberNate (projects licensed under Lesser General Public License (LGPL) v2.1)
- Log4J (Apache License 2.0)
- Guava (Google core libraries - Apache License 2.0)
- jackson-core
- Apache Commons Logging™
- HttpClient - Apache
- XStream (Group: com.thoughtworks.xstream)
- Jersey client
- Joda-Time
- SLF4J (Simple Logging Facade for Java)
- HikariCP Java 6
- AspectJ™ extension to Java
- SNMP4J (Open Source SNMP API for Java)
- Mockito
2 Getting Started with the ARM

After installing the ARM and performing initial configuration (see the ARM Installation Manual), you can get started with the ARM.

2.1 Logging in

This section shows how to log in.

➢ To log in:

1. Point your web browser to the ARM's IP address and press Enter.

2. In the Login to ARM screen, log in using the default Operator and Operator username and password. It's advisable to change these as soon as possible (see Section 5.4.3 for instructions on how to change them).

The ARM opens in the Network page, Map view (default) in your browser. By default, all VoIP entities managed in the network are displayed.

2.2 Getting Acquainted with the ARM GUI

This section familiarizes you with the ARM GUI. The Internet browser based graphic user interface visualizes VoIP network topology and its components, providing centralized, dynamic network management and router rules and logic management. After logging in, the Network page, Map view opens by default, as shown in the figure below.

Figure 2-1: ARM GUI - Network Page - Map View

Use Table 2-1 below as a reference to Figure 2-1 shown above.
### Table 2-1: ARM GUI – Map View

<table>
<thead>
<tr>
<th>#</th>
<th>GUI Area</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1  | Actions Bar       | - Sync Topology  
- Add Connection  
- Edit  
- Delete  
- Lock/Unlock  
- Center Map  
- Save Items Location (saves network elements positions in the map)  
- Refresh  
- Layers  
  ✓ topology  
  ✓ quality |
| 2  | Toolbar           | Toolbar icons let you navigate to the following ARM pages: NETWORK, ROUTING, USERS, ALARMS and SETTINGS. |
|    |                   | Located on the right side of the toolbar. Click to:  
- Save logs  
- Lock  
- Log out  
- Display the ARM version (About)  
- Display how much time remains before the session terminates |
| 3  | Search            | Lets you locate specific information in the Network page's Map view, Routing page, Users page, Alarms page and Settings page. |
| 4  | Main Screen       | The Network page displays a Map view of network entities. |
| 5  | Summary Panes     | The Network page, Map view, displays these summary panes:  
- **Network Summary**  
  ✓ Nodes (Available, Unavailable, Locked)  
  ✓ Peer Connections (Available, Unavailable, Locked)  
  ✓ Connections (Available, Unavailable)  
- **General Statistics**  
  ✓ Routing Attempts per 5 Minutes  
  ✓ Unsuccessful Routes per 5 Minutes  
  ✓ Unsuccessful Routes (Alternative Attempts / Destinations Not Routable)  
  ✓ Calls per 5 Minutes (Destination Calls / Transient Calls)  
- **Top 5 Routes**  
- **Test Route** |

### 2.2.1 Getting Acquainted with the Network Map Topology Layer

In the Network page, Map view, you can view node information and perform network map actions. Network Map view shows the four main entities that comprise the network topology:

- Nodes
- VoIP Peers
- Peer Connections
- Connections
The table below explains each.

**Table 2-2: Network Page’s Map View – Network Entities**

<table>
<thead>
<tr>
<th>Network Entity</th>
<th>Icon</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| Node           | ![Node Icon] | Indicates an AudioCodes SBC communicating with the ARM. It's part of the ARM network topology.  
Blue = operative state available/logging in  
Red = operative state unavailable/unrouteable  
Orange = operative state logged out  
Strikethrough = locked  
No strikethrough = unlocked |
|                | ![Node Icon] | Indicates an AudioCodes gateway communicating with the ARM. It's part of the ARM network topology.  
Blue = operative state available  
Red = operative state unavailable  
INVALID CONFIGURATION  
Orange = operative state logged out  
Strikethrough = locked  
No strikethrough = unlocked |
|                | ![Node Icon] | Indicates a hybrid AudioCodes device (AudioCodes’ Gateway and SBC in one).  
Blue = operative state available  
Red = operative state unavailable  
INVALID CONFIGURATION  
Orange = operative state logged out  
Strikethrough = locked  
No strikethrough = unlocked |
| VoIP Peer      | ![VOIP Icon] | Indicates a non-AudioCodes device or entity that is also part of the ARM network topology: PBXs, SIP trunks, other vendors' SBCs / gateways. These devices participate in processing ARM network calls and are connected to Nodes by 'Peer Connections'. The ARM operator can configure one of six VoIP Peer types.  
SIP trunk  
PSTN  
IP PBX and IP phone  
Legacy PBX  
N/A (Not applicable) |
| Connection     | ![Connection Icon] | Indicated by a blue line (available) or a red line (unavailable). Joins two Nodes. Calls can be routed between two Nodes only if there is a Connection between them. Defined by adding an IP Group (at Node level). From AudioCodes' gateway/SBC perspective, a 'Connection' is an 'IP Group'. Connections between Nodes are added by the ARM operator. |
| Peer Connection| ![Peer Connection Icon] | Indicated by a black line between a Node and a VoIP Peer. Represents a group of routing destinations/sources (connections to a VoIP Peer), 'last mile' connectivity. From AudioCodes' gateway/SBC perspective, a Peer Connection is a 'PSTN Trunk Group' or 'IP Group'.  
Red line = administrative state is unlocked / operative state is unavailable (no connection between the AudioCodes device and the
### Network Entity | Icon | Explanation
--- | --- | ---
remote device) / predeleted (IP Group was deleted from the device) |  | Black line through a red sphere = unavailable and locked
Black line through a black sphere = available but locked

#### 2.2.2 Getting Acquainted with the Network Map Quality Layer

The Network page’s Map view displays a **Layers** tab that allows the operator to choose **topology** and / or **quality**.

![Figure 2-2: Network Map Layers](image)

The **topology** layer displays the *availability status* of network elements.

The **quality** layer displays the *quality status* of network Connections and Peer Connections. When both are selected, the network map displays the *aggregated availability status and quality status*. 
Figure 2-3: Quality Layer

The figure above shows the Quality Layer. Table 2-3 describes the colors indicating the different quality options.

Table 2-3: Quality Color Codes

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>GOOD quality Connection</td>
</tr>
<tr>
<td>Grey</td>
<td>GOOD quality Peer Connection</td>
</tr>
<tr>
<td>Orange</td>
<td>FAIR quality Connection / Peer Connection</td>
</tr>
<tr>
<td>Red</td>
<td>BAD quality Connection / Peer Connection</td>
</tr>
<tr>
<td>Dotted grey</td>
<td>UNKNOWN quality, i.e., there is insufficient data to determine quality statistics. After a sufficient number of calls are routed by the Connection / Peer Connection, the color changes from grey to the color of the determined quality static.</td>
</tr>
</tbody>
</table>
The figure above shows a Connection whose quality was determined to be GOOD.
The figure above shows a Peer Connection whose quality cannot be determined (UNKNOWN) because there is currently insufficient data to determine quality statistics.

### 2.2.3 Getting Acquainted with Network Map Page Actions

#### 2.2.3.1 Node Information and Actions

In the Network page, Map view, you can view node information and perform node actions.

- **To view node information:**
  1. Point your cursor over the node whose information you want to view; the node information pops up:

![Figure 2-6: Node Information](image)
2. Use the table below as reference.

**Table 2-4: Network Page’s Map View – Viewing Node Information**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the Node</td>
</tr>
<tr>
<td>Type</td>
<td>The type of Node</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the Node</td>
</tr>
<tr>
<td>SW Version</td>
<td>The Node’s software version</td>
</tr>
<tr>
<td>Administrative State</td>
<td><strong>Locked</strong> (default) or <strong>Unlocked</strong>. Can be changed in the Actions popup</td>
</tr>
<tr>
<td>Operative State</td>
<td>Available / Unavailable / Unrouteable / Logged out / Logging in.</td>
</tr>
</tbody>
</table>

➢ To perform an action on a node:

1. Click the node on which to perform an action and then click the **icon displayed; the actions menu pops up.**

   ![Figure 2-7: Node Actions](image)

2. From the menu you can select:
   a. Lock/Unlock Node
   b. Sync Node
   c. Build Star (Topology)
   d. Add Connection
      ♦ Make sure that the relevant SIP interface in the SBC is provisioned and configured as ‘Used by routing server’
      ♦ Click **Add Connection** and then click the Node to which to make the Connection; a line is defined to indicate that the connection was made.
      ♦ In the Connection Definition dialog that opens, select the routing interface for Node-1 and then for Node-2, and then click **Apply**. See Section 3.1 for more information.
   e. Edit
      ♦ In the NODE UPDATE dialog that opens, shown in the figure below, update the credentials of the device if necessary (Name, User name and Password).
From the ‘Protocol’ dropdown, select the protocol that the ARM Configurator (server) uses when communicating with this node. Default: **HTTPS**. If you don’t want to encrypt the traffic – e.g., when debugging - select **HTTP**.

From the ‘Routing policy’ dropdown, select either:

- **Round Robin** (default). For each request, the node selects a different router.

- **Sticky Last Available**. The node picks the first available router from the routers that are listed in order of priority under ‘Selected Routing Server’, and stays with it until it fails. If it fails, the node continues down the list. The node therefore only functions with one router at a time.

- **Sticky Primary**. The node picks the first available router from the routers that are listed in order of priority under ‘Selected Routing Server’, and stays with it until it fails. If it fails, the node goes to the highest available router in the list. The node therefore functions at any time with the highest available router in the list.

**Specifying Routing Server**

- The Routing Servers section allows the network administrator to select routers to operate with a selected node. This is useful, for example, if an enterprise has servers located in different regions and the network administrator wants a node in one region to be served by routers located only in that region.

  The ‘Selected Routing Server’ pane lets the network administrator define the order of the routers in the node, which is relevant for the Sticky routing policies.

f. **Delete Node.** Only applies to a Node that is **Locked** and with which no routing rules and Policy Studio rules are associated. If routing rules are associated with the Node or its Peer Connections and you want to delete it, update or delete the rule so it does not refer to the Topology element which is going to be deleted.

g. **Configure.** Lets you directly configure a node (or SIP module) from the ARM's GUI without needing to provide the node’s credentials (Single Sign-on) to the node's Web interface. See the AudioCodes device's *User's Manual* for detailed information. Nodes version 7.2.150 and later are supported. Earlier node versions do not support single sign-on; you must provide credentials before you can access their Web interface. Selecting the **Configure** option from the node’s popup menu automatically opens a new tab displaying the node's Web interface, without prompting the operator for credentials.
2.2.3.2 VoIP Peer Information and Actions

In the Network page, Map view, you can view VoIP Peer information and perform VoIP Peer actions. There are six types of VoIP Peers:

- SIP Trunk
- PBX
- IP PBX
- PSTN
- IP Phone
- N/A (default)

➢ To view VoIP Peer information:

1. Point your cursor over the VoIP Peer whose information you want to view; a VoIP Peer popup pops up displaying the Name and Device Type.

   Figure 2-9: SIP Trunk Information

   ![SIP Trunk Information]

   Figure 2-10: PBX Information

   ![PBX Information]

   Figure 2-11: PSTN Information

   ![PSTN Information]

   Figure 2-12: IP Phone Information

   ![IP Phone Information]

➢ To perform an action on a VoIP Peer:

- In the Network page, Map view, click the VoIP Peer on which to perform an action and then click the icon displayed; the actions menu pops up.

   Figure 2-13: VoIP Peer Actions

   ![VoIP Peer Actions]

   - From the actions popup, you can select Edit; the VoIP Peer Update dialog is displayed, as shown in Figure 2-14.
2.2.3.3 Connection Information and Actions

In the Network page, Map view, you can view connection information and perform connection actions.

➢ To view connection information:

1. Point your cursor over the connection whose information you want to view; a connection popup pops up.

2. You can view the:
   - name of the connection
   - Weight (Range: 0-100. Default: 50)
   - Operative State

➢ To perform an action on a connection:

1. Click the connection on which to perform an action and then click the icon displayed; an actions menu pops up.
2. From the menu you can select:
   - Edit
   - Delete

3. Select **Edit**; the Connection Definition screen opens.

   **Figure 2-17: Connection Definition**

   ![Connection Definition Screen]

4. You can edit the:
   - name of the connection
   - Weight (Range: 0-100. Default: 50)
   - Transport Type (Default: UDP)

   Note that **Add**, **Edit** and **Delete** are also available as Actions buttons in the Network Map page.

5. Leave the option **use global** at its default for quality-based routing to be applied using global (ARM level) settings. Select **use specific** in order to overwrite the global settings of quality-based routing condition for a specific connection, and then select the enabled 'MOS' and/or 'ASR' option (see Section 5.3 for related information).

2.2.3.4 Peer Connection Information and Actions

In the Network page, Map view, you can view Peer Connection information and perform peer connection actions.

- **To view peer connection information:**

1. Point your mouse over the peer connection whose information you want to view; a peer connection information popup pops up.

   **Figure 2-18: Peer Connection Information**

   ![Peer Connection Information Popup]

2. View the Peer Connection's:
   - Name
   - IPGroup Name
   - Node name
   - Administrative state
   - Operative State
   - Peer connection type
   - Quality
   - Weight
To perform an action on a peer connection:

1. Click the peer connection on which to perform an action and then click the icon displayed; a Peer Connection Actions menu pops up. Note that Add connection, Edit and Delete are also available as Actions buttons in the Network Map page.

![Figure 2-19: Peer Connection Actions](image)

Figure 2-19 shows available actions for a Peer Connection joining a Node to a VoIP Peer.

2. You can:
   - Lock / Unlock the Peer Connection
   - Edit the Peer Connection:
     a. Click the Edit option.
     b. Modify the weight (Range: 0-100; Default: 50) for the ARM to calculate the optimal call path. Use if you have a VoIP Peer as a Routing Rule action and you want to prioritize a specific Peer Connection (e.g., SIP trunk) to be chosen for calls routing. Also use to reflect Peer Connection cost or bandwidth.
     c. From dropdown list, select the VoIP Peer that this Peer Connection is connected to.
     d. From the dropdowns, select the Normalization Rule for Source and Destination URI User if pre-routing manipulation is required for a specific Peer Connection (defined as shown in Section 5.2.1).
     e. Leave use global quality definitions selected (default) for this Peer Connection to use the global quality profile configured as shown in Section 5.3.1.
     Select use specific quality definitions for this Peer Connection to use only the 'MOS' or the 'ASR' criteria of the quality profile configured as shown in Section 5.3.1.
   - Test the Route (see Section 3.4)
   - Delete the Peer Connection. Only Peer Connections in locked and pre-deleted state, unassociated with routing rules or with a Policy Studio rule, can be deleted.
If this Peer Connection is connected to a VoIP Peer that is connected to more than one Peer Connection, you can detach it. You'll be prompted to define a name for a new VoIP Peer.

In the example above, four Peer Connections lead to the VoIP Peer 'USA_Lync', so a Peer Connection can be detached.

### 2.2.4 Peer Connections Page Actions

In the Peer Connections page, accessed by clicking the Peer Connections tab in the Network page, you can view the Peer Connections.

**Figure 2-21: ARM GUI - Network Page - Peer Connections**

You can view the following information on each Peer Connection:

- Status
- Node
- Name
VoIP Peer
IP Group
Operative State
Administrative State
Quality

The information displayed in the Network page's Peer Connection view is identical to that displayed in the Network page's Map view described under Section 2.2.3.4. You can search for the name of a Node associated with the Peer Connection, its name, or a VoIP Peer name. It's useful to find, for example, all Peer Connections of a specific Node.

You can perform the following actions:

- Sync Topology
- Edit (after selecting the row of the Peer Connection to edit)
- Delete (after selecting the row of the Peer Connection to delete)
- Lock/Unlock (after selecting the row of the Peer Connection to lock/unlock)

Multiple rows can be selected; multiple actions (delete, lock/unlock, etc.) are supported. For more information about Sync Topology, see Section 3.2. For more information about the Edit, Delete and Lock/Unlock actions, see under Section 2.2.3.4.

2.2.5 Connections Page Actions

In the Connections page, accessed by clicking the Connections menu under the NETWORK menu, you can view the connections you defined.

Figure 2-22: ARM GUI - Network Page - Connections

You can view the following information on each connection:

- Status
- Node 1
- Routing Interface 1
- Name
- Node 2
- Routing Interface 2
- Weight
- Quality

The Search functionality is allowed for all the relevant information fields: Node Name, Connection Name, Weight or Routing Interface.
The information displayed in the Network page’s Connections view is identical to that displayed in the Network page’s Map view described under Section 2.2.3.3.

You can perform the following actions:

- Sync Topology
- Add Connection (after selecting the row of the connection to edit)
- Edit Connection (after selecting the row of the connection to edit)
- Delete Connection (after selecting the row of the connection to edit)

Multiple rows can be selected and multiple delete is supported. For more information about Sync Topology, see Section 3.2. For more information about the Add, Edit and Delete Connection, see under Section 2.2.3.3.
3 Defining a Network

The ARM features auto-detection capability. It automatically detects and discovers network entities, allowing you to begin defining actions immediately after auto-detection.

Note: Do not modify the SBC-level / gateway-level configuration of the connections created by the ARM. It will disrupt routing decisions/performance.

3.1 Adding Connections

You can define a connection between two nodes.

➢ To add a connection:

1. In the Network page’s Map view, click the node from which to define the connection, click the icon displayed, and from the actions popup select Add Connection.

   ![Figure 3-1: Add Connection](image)

   Alternatively, point the mouse over node A and when a circle appears, drag and drop on node B; a line is drawn between the nodes and this screen is displayed:

   ![Figure 3-2: Defining a Connection](image)

2. Provide an intuitive name for the connection to facilitate user-friendly management in the ARM GUI.

4. From the ‘Transport Type’ dropdown, select **UDP** (default), **TCP** or **TLS**.
5. From the ‘Node-1’ dropdown, select Node-1 and from the ‘Routing Interface-1’ dropdown, select its routing interface.
7. For defining Advanced Conditions (quality-based routing), see Section 5.3.
8. Click **OK**; the connection is made.
9. Click **Apply** and **Close**.

### 3.2 Synchronizing Topology

The Sync Topology feature allows you to perform manual synchronization *per Node* or *per global topology synchronization*, depending on where the synchronization action was run. It's important that node status is fully synchronized with the ARM server *at all times* for the ARM GUI to display the node successfully and for routing to be performed correctly.

For an SBC / Media Gateway to be displayed in the ARM GUI, you need to point it to the ARM server IP address using the Web interface.

The ARM auto-discovers all network elements such as Nodes, Peer Connection and VoIP Peers, associates a VoIP peer with each Peer Connection, and displays them in the Network page's Map view.

The ARM detects activity originating from a node and puts the node on the map (peer collection). The ARM recognizes a newly added node and extracts all IP groups (i.e., Peer Connections). Users must add connections between nodes and change the VoIP peer types (see the previous section).

If a node's status is changed, the ARM detects the change when synchronization is performed and automatically maps it. When synchronizing, the ARM obtains the names and statuses of connections and Peer Connections from each node and compares them to what it already knows. The Sync Topology feature therefore makes sure that the ARM is fully identified with the node's identifiers: IP address, credentials, node type, software version.

**To sync:**

- In the Network page, click **Sync Topology** on the actions bar shown below; global synchronization of the entire network is performed.

![Sync Topology actions bar](image-url)
3.3 Building Star Topology

You can build a star topology, as illustrated in the figure below. In a star topology, every node is connected to a central node, as illustrated here:

All VoIP traffic transitions through the central node. Advantage: It's easy to add more nodes. Disadvantage: Single point of failure, namely, the central node.

➢ To build a star topology:

1. In the Network page’s Map view, click the node; the icon \( \text{ } \) pops up. [Note that the Map page's Actions panel can alternatively be used, as well as the Connections table view].

2. Click the icon; the actions menu shown below is displayed.

3. Select Build Star; the topology is built.
3.4 Testing a Routing Rule

You can configure and test a routing rule to make sure it performs according to expectations, with or alternatively without impacting live calls traffic.

➢ To test a route:

1. In the Network page, click the Peer Connection to test and then click Figure 3-4: Test Route Menu Item

2. From the actions menu that pops up, select TEST ROUTE.

3. [Optional] Enter the Source and Destination Route. From the dropdown, select the Peer Connection.

4. From the Test route mode dropdown under 'Advanced Options', select either Use only routing rules in Test Mode or Use routing rules in Call Routing:
   - Use only routing rules in Test Mode. Lets you test the Routing Rule or Dial Plan offline without impacting or disrupting live calls traffic.
   - Use routing rules in Call Routing. When a new call destination is calculated, the Routing Rule is taken into consideration and live traffic may be impacted.

   Each routing rule can be enabled or disabled separately for 'Call Routing' mode and for 'Test' mode (see also under Section 6.2).

5. Click Find Routes. Test routing is performed as if a real call is occurring, taking Operative State and Admin State of topology elements (Connections, nodes, Peer Connections), and the Admin State of routing rules, into account. In addition, the Topology element's Quality or Time/Date criteria are taken into consideration if required by the Routing Rule (Advanced Condition). The Route Path is highlighted violet (shown in Figure 3-6); the TEST ROUTE pane on the right displays detailed information.
Figure 3-6: Route Path

6. In the Test Route pane shown in Figure 3-6, click Details.

Figure 3-7: Test Route Details

7. In the example above:
   - Compare the column ORIGINAL to the column NEW; the number changed as a result of a normalization rule that was applied. The normalization rule was configured in the Normalization Group rules attached to the Peer Connection. For related information, see also under Section 2.2.4 and Appendix C.

Figure 3-8: Strip + from the Number

- Column WHEN indicates when manipulation was performed, i.e., before or after routing. In the example above, manipulation was performed before routing.
- Column ENTITY indicates which part of the SIP Request was manipulated.
  - Possible values: Source URI User, Source URI Host, Destination URI User, Destination URI Host, Destination IP Address, Destination Port, Destination Protocol, User Credential User Name, User Credential Password
- Column CHANGED BY – the first row indicates by global Normalization Group – see under Section 5.2.1 and Section 5.2.3 for detailed information; the second row indicates that the normalization was attached to a Peer Connection - see under Section 2.2.3.4 for detailed information.
- Column NORMALIZATION/MANIPULATION GROUP indicates which "Manipulation Group" the entity passed through, according to which regular expression the entity was changed.
The figure below shows an example of a test call with a quality advanced condition. The condition avoids passing through 'bad' or 'fair' Connections/Peer Connections.

**Figure 3-9: Example of a Test Call with a 'Quality' Advanced Routing Condition**
3.5 Network Statistics

The panes in the right margin of the Network Map page display network statistics. You can choose to display:

- Overall Network Statistics - statistics related to the entire network are displayed by default; no element in the Network Map is selected. See Section 3.5.1.
- Statistics on a network element – select the network element in the Network Map for which to display statistics. See Section 3.5.2.

3.5.1 Overall Network Statistics

Statistics related to the entire network are by default displayed. No element in the Network Map is selected. This pane displays four sections:

- Network Summary (see below)
- General Statistics (see Section 3.5.1.2)
- Top 5 Routes (see Section 3.5.1.3)
- Test Route (see Section 3.5.1.4)

3.5.1.1 Network Summary

The Network Summary pane displays routing statistics and availability network statuses which help operators optimize routing in their telephony networks, reducing unnecessary consumption of resources and decreasing expenses.

The pane displays:

- Network Elements Statuses (left to right):
  - The total number of nodes/Peer Connections/Connections in the network
  - The number of nodes/Peer Connections/Connections in the network that are unlocked and available, i.e., 'normal'
  - The number of nodes/Peer Connections/Connections in the network that are 'fault', i.e., unavailable
  - The number of nodes/Peer Connections in the network that are 'locked' (Connections cannot be locked/unlocked)

When Quality Layer is selected, the 'Faulty' counters for Peer Connections and Connections can change. All red (bad), orange (fair) or unknown Connections / Peer Connections are considered 'Faulty' because they less than perfect.

3.5.1.2 General Statistics

You can display statistics related to the entire network.
To display statistics related to the entire network:

- Open the ARM's network map and in the General Summary window, click the **General Statistics** tab.

![Figure 3-11: General Statistics Pane](image)

Three graphs are displayed (top to bottom):

- The number of routing attempts made in the entire network every five minutes
- The number of unsuccessful routes made every five minutes, including the number of alternative attempts and the number of unrouteable destinations
- The number of calls made every five minutes, including the number of destination calls and the number of transient calls.

You can click the `+` next to each of the three graphs to project a zoomed-in graph to the front, facilitating your analysis.
### 3.5.1.3 Top 5 Routes Pane

The Top 5 Routes pane under the **Top 5 Routes** tab gives operators visibility into the routes most frequently used over the last three hours.

**Figure 3-13: Top 5 Routes**

Select a route to display its details: Source Node/Peer Connection and destination Node/Peer Connection.

**Figure 3-14: Top 5 Routes – Route Details**
Selecting a specific route also displays the popular path visually in the Network map, as you can see in the figure below.

**Figure 3-15: Popular Path Visualized in the Network Map**

### 3.5.1.4 Test Route

See Section 3.4 for detailed information.

### 3.5.2 Statistics on a Selected Element

When you select one of elements in the map, the Network Summary window displays statistics related to that selected element.

**Figure 3-16: Network Summary Pane Displaying Statistics Related to a Selected Element**
4 Administering Users

The USERS page in the ARM allows the ARM operator to administer:

- Users (see the next section)
- Users Groups (see Section 4.2)
- LDAP Servers (see Section 4.4)
- Property Dictionary (see Section 4.3)

4.1 Administering Users

Enterprises have databases in which employee information is stored. Enterprises generally store information related to employees on Microsoft's Active Directory (AD) server. The ARM supports multiple ADs. The ARM's user administration feature can connect to an AD and import user calls routing related information into the ARM database. Operators can alternatively add users who are not listed in an AD database, to the ARM database.

Enterprises that store their users in another format (Excel, for example) can also import these users into the ARM as local ARM users using the ARM northbound REST API. For more information and assistance, contact AudioCodes Professional Services.

To view the users listed in the AD database and their AD attributes, you need to provision the LDAP server as shown under Section 4.4.

➢ To add a user who is not listed in an AD database, to the ARM database:

1. In the ARM's Users page, click the Users tab; the Users page opens.

2. Click Add; the User Details screen opens.
User Details are taken from the Property Dictionary screen. If a property is added in the Property Dictionary screen, it appears here. To add a property, see Section 4.3. Note that if an LDAP server is provisioned, the ARM automatically brings users from it to the ARM database, and displays them in the GUI under the User tab.

3. Click OK; the user is added and displayed in the Users page. To view and/or edit, select the user's row and click Edit; the screen shown below is displayed.

Note that in the figure above the grayed fields indicate that the origin of this user isn't ARM and as such, cannot be edited. Non-grayed fields indicate that the origin of the user is ARM and as such, can be edited.
4.2 Administering User Groups

You can define User Groups by defining a set of criteria in the users properties. The ARM automatically associates users with the defined User Group, based on the conditions you define. You can then use the User Groups in your Routing Rules as match conditions. Each User Group has one 'Dialable Number' attribute. When a route request is received with a source or destination URI matching the group’s 'Dialable Number' property for one of the users in the group, the Routing Rules with this source or destination User Group are matched.

A User Group can have a single attribute condition or a combination of attributes conditions. For a user to be a part of the User Group, all the conditions must be matched. A single condition can have a set of values to compare to. If any of the values of the condition are matched, the condition is considered a match.

Example: You can create a User Group where the 'Dialable Number' attribute is 'Mobile phone number' and the conditions are Country equals Germany and Department equals Marketing or Sales.

➢ To add a user group:

1. In the Users page, click the Users Groups tab.

![Figure 4-4: Users Groups](image)

2. Click Add.

![Figure 4-5: User Group Details](image)

3. Configure the details using Table 4-1 as reference.
Table 4-1: User Group Details

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the group for intuitive future reference.</td>
</tr>
<tr>
<td>Dialable</td>
<td>From the dropdown, select one of the Dialable Number properties. This is the user’s property that is compared to the received source or destination URI to determine if the route request is from/to one of the users in this User Group. Example: ‘Office phone number’.</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Click the field and from the dropdown, select a user attribute according to which the user will be associated with the group. Example: Country. Click the plus button + to add more attributes. All attributes must match for the user to be a member of the group.</td>
</tr>
<tr>
<td>equals / not equals</td>
<td>From the dropdown, select the operation to be used to define the criterion.</td>
</tr>
<tr>
<td>contains / not contains</td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>Enter a value for the attribute, according to which the user will be associated with the group. Example: Sweden. Press enter to add more values. At least one of the values must match for the attribute to be considered a match.</td>
</tr>
</tbody>
</table>

➢ To edit a user group:

1. In the Users page, select the user group to edit and then click Edit; the User Group Details screen opens – under the Properties tab. You can see the users who are associated with the group under the Users tab of the User Group Details screen.

2. Edit using the table above as reference, and then click the USERS tab; the screen shown above right opens allowing you to view the users that were associated to the group in the Users tab of the User Group Details dialog.
4.3 Administering the Property Dictionary

The Users page’s Property Dictionary tab lets the operator administer the Property Dictionary, a set of all the properties that a user can have.

![Figure 4-6: Users Page – Property Dictionary tab](image)

After adding a property to the dictionary, you can add it to some or all of your LDAP servers. Properties added to an LDAP server will automatically be read from the LDAP server. Properties not added can be set locally in the ARM for each user. The Properties from the dictionary can then be used as User Group conditions as well as in ‘Policy Studio’.

4.4 Administering LDAP Servers

Network administrators can add multiple Active Directories (ADs) to the ARM database using LDAP protocol.

➢ To add an LDAP server:

1. In the Users page, click the **LDAP Servers** tab.

   ![Figure 4-7: Users Page – LDAP Servers tab](image)

2. Click **Add**; the LDAP Server Settings open.
3. Configure the settings using the table below as reference.

**Table 4-2: LDAP Server Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>Enter an intuitive name for the LDAP server.</td>
</tr>
<tr>
<td>Host</td>
<td>IP address or DNS name of the LDAP server on which the AD is located.</td>
</tr>
<tr>
<td>Port</td>
<td>The LDAP port. Default: 389</td>
</tr>
<tr>
<td>Base Object</td>
<td>Consult your IT manager responsible for the Active Directory in your enterprise. The setting defines the full path (DN) to the object in the AD tree where the user's information is located. The valid value is a string of up to 256 characters. Example (read from right to left): <code>ou=Users;ou=APC;ou=Israel;ou=AudioCodes;dc=corp;dc=audiocodes;dc=com</code> The DN path is defined by the LDAP names OU (organizational unit) and DC (domain component).</td>
</tr>
<tr>
<td>Search Filter</td>
<td>An LDAP search filter used when fetching the users from the LDAP server under the base DN. The default is 'objectClass=user'.</td>
</tr>
<tr>
<td><strong>Security Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Bind DN</td>
<td>The DN (distinguished name) or username of the user used to bind to the LDAP server. For example: <code>ldap_bind@corp.audiocodes.com</code></td>
</tr>
<tr>
<td>Password</td>
<td>Defines the LDAP password used in order to connect.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Enables or disables the connection over SSL. Default: Disable. When disabled, communications with the AD server will be open, i.e., unencoded/unencrypted. When left unchanged at the default; the <strong>Browse</strong> button adjacent to 'Certificate File to Upload' will be unavailable; when enabled, the <strong>Browse</strong> button becomes available.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Certificate file</td>
<td>Enables verification that it is the AD server and no other entity that is communicating with the ARM server. Allows you to browse for a root certificate. When the AD server then sends a certificate, the ARM server uses the root certificate to verify that it is the AD server and no other entity on the other side. Following verification, communications are SSL-encoded.</td>
</tr>
</tbody>
</table>

**Updates**

<table>
<thead>
<tr>
<th>Updates</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check for updates every ( n ) minutes</td>
<td>Defines how frequently the ARM server checks the AD server for updates. Note that during the update, the ARM only obtains new AD users or relevant user information updates (only the delta).</td>
</tr>
<tr>
<td>Perform full update every ( n ) days at</td>
<td>Defines how frequently the ARM server performs a full update from the AD server. Note that a full update is mainly required to remove users deleted from the organization's AD (this information cannot be obtained by an AD update).</td>
</tr>
<tr>
<td>Updates timeout</td>
<td>If the AD server doesn't answer within the period set, the ARM server determines that the AD server is disconnected and a refresh is sent.</td>
</tr>
<tr>
<td>Test Connectivity</td>
<td>Click the button to test the connectivity between the ARM server and the AD server.</td>
</tr>
</tbody>
</table>

4. **Click OK** now or click it after the **Next** button. You can also click **Test connectivity**; the LDAP Properties page opens:

![Figure 4-9: LDAP Properties](image)

Properties that have LDAP mappings will be synced from the LDAP server. Properties that do not have LDAP mappings can be configured locally.

- **To attach a Normalization Group (Rule) to an LDAP property:**
  1. Select the row of the LDAP property to which to attach a Normalization Group (Rule).
  2. From the property's Attribute Normalization dropdown, select a Normalization Group. See Section 5.2.1 for information on how to configure a Normalization Group.
  3. Click **Finish**.
To view the AD summary:

- In the Users page, click the LDAP Servers tab and select the AD whose summary you want to view.

![Figure 4-10: Users Page – LDAP Servers tab – AD Summary](image)

Table 4-3: Active Directories Summary

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync</td>
<td>ARM and AD databases synchronization schedule. Displays the synchronization frequency: 1-48, i.e., between once every hour (most frequent) to once every two days (most infrequent).</td>
</tr>
<tr>
<td>Last Sync</td>
<td>Displays the last time the ARM and the Active Directory databases were synchronized.</td>
</tr>
<tr>
<td>Full Sync</td>
<td>Displays the time (hour and minute) at which to start a full synchronization. Also displays the frequency: 1-7, i.e., between once a day (most frequent) to once a week (most infrequent).</td>
</tr>
<tr>
<td>Last Full Sync</td>
<td>Displays the last time the ARM and the Active Directory databases were fully synchronized.</td>
</tr>
</tbody>
</table>

To edit an LDAP server:

1. In the Users page under the LDAP Servers tab, select the server to edit and then click Edit; the LDAP Server Settings open.

![Figure 4-11: LDAP Server Settings](image)
2. Edit the LDAP Server Settings screen, click **Test Connectivity** to test the connection settings and then click **Next**; the LDAP Properties screen shown in Figure 4-9 opens.

3. For each LDAP property's LDAP Mapping dropdown, select a mapping. Properties that have LDAP mappings will be synced from the LDAP server. Properties that do not have LDAP mappings can be configured locally.

4. Select the row of the LDAP property to which to attach a Normalization Group (Rule) and then from the property's Attribute Normalization dropdown, select a Normalization Group. See Section 5.2.1 for information about how to configure a Normalization Group.

5. Click **Finish**.

After updating an LDAP server, a full sync is started. After a short while (depending on the size and responsiveness of the LDAP server), you can view the updated users in the Users page.
4.4.1 Adding / Editing a Property

You can add / edit a property.

➢ To add / edit a property:


Figure 4-12: Property Dictionary

2. Click Add or Edit; the Property dialog opens.
3. Use the table below as reference.

### Table 4-4: Add Property

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Define an intuitive name for the property, for intuitive future reference.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a brief description of the property, for intuitive future reference.</td>
</tr>
<tr>
<td>Dialable</td>
<td>Defines whether or not this property is a dialable number. Only dialable</td>
</tr>
<tr>
<td></td>
<td>numbers are used for matching with a received source or destination URI in a</td>
</tr>
<tr>
<td></td>
<td>route request. Examples of dialable number properties: Office phone number,</td>
</tr>
<tr>
<td></td>
<td>mobile phone number, Skype number, etc.</td>
</tr>
<tr>
<td>Display in Users Table</td>
<td>Select the option in order to display the user property in the Users page.</td>
</tr>
<tr>
<td></td>
<td>The option can be used to reduce clutter on the Users page.</td>
</tr>
</tbody>
</table>
This page is intentionally left blank.
5 Configuring Settings

The Settings page (under the Settings menu) lets you

- **Network Services Settings**
  - Syslog server (see Section 5.1.1)
  - NTP server (see Section 5.1.2)

- **Call Flow Settings**
  - Normalization Groups (see Section 5.2.1)
  - Prefix Groups (see Section 5.2.2)
  - Normalization Before Routing (see Section 5.2.3)
  - Policy Studio (see Section 5.2.4)

- **Routing Settings**
  - Configuring a Quality Based Routing Condition (see Section 5.3.1)
  - Configuring a Time Based Routing Condition (see Section 5.3.2)
  - Configuring SIP Alternative Route Reason (see Section 5.3.3)
  - Configuring Global Routing Settings (see Section 5.3.4)

- **Administration Settings**
  - Software License (see Section 5.4.1)
  - Security (see Section 5.4.2)
  - Operators (see Section 5.4.3)

- **Routing Servers Settings**
  - Adding a Routing Server (see Section 5.5)
  - Editing a Routing Server (see Section 5.5.1)
  - Locking/Unlocking a Routing Server (see Section 5.5.2)

5.1 Network Services Settings

This section shows how to edit a syslog server and add/edit an NTP server.

5.1.1 Editing a Syslog Server

This section shows how to edit a Syslog Server.

➢ **To edit a Syslog Server:**

1. In the Settings page, click theSyslog tab.

![Figure 5-1: Network Services](image)

2. Select the Router or Topology row and then click the then-enabled Edit button.
3. Configure the syslog details using Table 5-1 as reference.

### Table 5-1: Syslog Details

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP address or host name of the remote syslog server to which messages are sent.</td>
</tr>
<tr>
<td>Port</td>
<td>Port of the remote syslog server to which messages are sent.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Leave at default (UDP).</td>
</tr>
<tr>
<td>Debug Level</td>
<td>From the 'Debug Level' dropdown select either:</td>
</tr>
<tr>
<td></td>
<td>• WARN (default level for the Router; only messages whose debug level is WARNING are sent to the syslog server)</td>
</tr>
<tr>
<td></td>
<td>• TRACE</td>
</tr>
<tr>
<td></td>
<td>• DEBUG (default level for Topology; only messages whose debug level is DEBUG and higher are sent to the syslog server)</td>
</tr>
<tr>
<td></td>
<td>• INFO</td>
</tr>
<tr>
<td></td>
<td>• ERROR</td>
</tr>
</tbody>
</table>

**Note:** When enabling syslog for a Router, there's a single syslog server for all Routing servers in the ARM. All ARM Routers will send their syslog to this syslog server (at the same 'Debug Level'). This is necessary for proper calls debugging, as a single call can be processed by several different ARM Routers (they are state-less). For the ARM Configurator, however, you can assign a different syslog server.
5.1.2 Adding/Editing an NTP Server

This section shows how to add an NTP server.

➢ To add an NTP server:

1. Open the NTP Servers page (Settings menu > Network Services tab > NTP Servers item).

![Figure 5-3: NTP Servers](image)

2. Click Add.

![Figure 5-4: NTP Server Details](image)

3. Configure the NTP server details using the table below as reference.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the NTP server.</td>
</tr>
<tr>
<td>Address</td>
<td>Enter the IP address or host name of the NTP server.</td>
</tr>
</tbody>
</table>

4. Click OK.
5.2 Call Flow Settings

5.2.1 Adding a Normalization Group

You can add a Normalization Group. A Normalization Group can comprise one rule or multiple rules. If there are multiple rules in a group, manipulation is performed in the order the rules are listed. The output of the first rule will be the input of the next.

➢ To add a Normalization Group:
1. Open the Normalization Groups page (Settings menu > Call Flow Configurations tab > Normalization Groups).

![Figure 5-5: Normalization Groups](image)

2. Click Add.

![Figure 5-6: Normalization Groups](image)

3. Use the table below as reference.
### 5. Configuring Settings

#### Table 5-3: Normalization Groups

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Enter a Group Name for intuitive future reference.</td>
</tr>
<tr>
<td>Normalization Rules</td>
<td>1. Click the + button adjacent to the pane as shown in the figure above.</td>
</tr>
<tr>
<td></td>
<td>2. In the left textbox, enter a regular expression. For more information about</td>
</tr>
<tr>
<td></td>
<td>regular expressions, refer to online tutorials or see Appendix C.</td>
</tr>
<tr>
<td></td>
<td>3. In the replace by field, enter the text that will replace the found regex.</td>
</tr>
<tr>
<td></td>
<td>You can use groups collected by brackets (...) in the regex in the replacement</td>
</tr>
<tr>
<td></td>
<td>string using $1, $2,…. See a regex tutorial for more information.</td>
</tr>
<tr>
<td>Rules Simulation: Test</td>
<td>Use the rules simulation to test different possible inputs and verify that the</td>
</tr>
<tr>
<td></td>
<td>regex sequence you entered produces the result you intended.</td>
</tr>
<tr>
<td></td>
<td>• Enter any value you want to test and click Test; the result of each</td>
</tr>
<tr>
<td></td>
<td>individual rule is displayed to the right; the final result of all the rules</td>
</tr>
<tr>
<td></td>
<td>together is displayed lowermost right.</td>
</tr>
</tbody>
</table>

**Note:** After a Normalization Group is defined, you can attach it to a:
- Peer connection (see Section 2.2.3.4).
- Globally (see Section 5.2.3)
- Routing Rule action (see Section 6.2)
- LDAP attribute (see Section 4.4)

**Note:** The same Normalization Group can be reused/attached several times in any of the above cases.

### 5.2.2 Adding/Editing a Prefix Group

This section shows how to make routing management and Dial Plan management easier, more efficient and more convenient for operators, using Prefix Groups. The Prefix Groups feature also makes it possible to import an existing customer’s Dial Plan into the ARM using the northbound REST API.

Every routing rule can have scores of prefixes. Grouping prefixes and then associating groups with routing rules reduces visual complexity and allows for more effective management. Prefix Groups save operators from repeatedly having to add prefixes to rules.

Once defined, the Prefix Group comprising multiple prefixes is associated with a routing rule (see Section 6.2 for information on how define a routing rule). If, for example, an enterprise has distributed offices, the following can be defined: If a caller calls from source prefix x, the call is sent from SBC 1; if a caller calls from source prefix 2, the call is sent from SBC 2.

**Note:** To develop a customer-specific Dial Plan into an ARM Prefix Group, the REST API is available. This can significantly facilitate ARM provisioning.

➢ **To add a Prefix Group:**
1. Open the Prefix Groups page (Settings menu > Call Flow Configurations tab > Prefix Groups item).
2. Click the Add icon.

Figure 5-8: Prefix Group Details

3. Configure the Prefix Group using Table 5-4 as reference.

Table 5-4: Prefix Group Details

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the prefix group.</td>
</tr>
<tr>
<td>Values</td>
<td>Enter a Prefix or a number of prefixes and then click Enter. The syntax for prefixes in ‘Prefix group’ is the same as for a single prefix in a Routing rule. See also Appendix B.</td>
</tr>
</tbody>
</table>

4. Click OK, after creating a group, open the Routing page and associate the group with a rule’s condition – it can be associated with Source, Destination or both.
5.2.3 Normalization Before Routing

This section shows how to apply a normalization rules group to a routing request's source user part and to a routing request's destination user part. See Section 5.2.1 for information on how to add a normalization rules group.

When the ARM receives a routing request, it normalizes the routing request's source user part with the chosen Normalization Group, and the routing request's destination user part with the chosen Normalization Group.

'Global Normalization Before Routing' parameters configured in this page are used globally for the entire network as pre-routing normalization. This global normalization can be overwritten at a Peer Connection level with other Normalization Rules if required (see under Section 2.2.3.4).

To attach a normalization rules group globally before routing:

1. Open the Normalization Before Routing page (Settings menu > Call Flow Configurations tab > Normalization Before Routing item).

Figure 5-9: Normalization Before Routing

2. Use the table below as reference.

Table 5-5: Normalization Before Routing

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source URI User</td>
<td>From the dropdown, select the normalization rules group. This will be the normalization on the Source URI User field.</td>
</tr>
<tr>
<td>Destination URI User</td>
<td>From the dropdown, select the normalization rules group. This will be the normalization on the Destination URI User field.</td>
</tr>
</tbody>
</table>

3. Click Submit.
5.2.4 **Policy Studio**

This feature allows adding information to route requests that is not contained in the route requests but is taken from the user table. To accomplish this with legacy products without ARM, the LDAP server must be queried for every call using complex query rules, creating delays and straining the server. In the ARM, the user table is loaded to memory and information gathering is handled internally in real time. Policy Studio Use Examples:

- Each user has an internal 4-digit extension and an unrelated external phone number. When a user makes a call outside the enterprise, the source number, i.e., the user's extension, must be replaced with their external number. When a call comes in from outside, the external number must be replaced with the user's extension.

- Same as the previous example but, in addition, there can be more than one user with the same extension, and what differentiates them is their hostname. The ARM can locate the user based on a combination of the extension and hostname attributes.

Policy Studio is a set of rules. Each rule contains a match condition and an action. The match condition is a set of route request fields to be compared, and a set of user properties to be compared to. The match condition also has a source node or Peer Connection or set of source nodes or Peer Connections. The action is a set of route request or response fields to be replaced, and a set of user fields to replace them with. For every route request received, the ARM processes all the rules from top to bottom. For each, the ARM searches in the users table for a user that matches all of the fields. If a user is not found, the ARM proceeds to the next rule. If a user is found, the ARM stops parsing the rules and performs the action in this rule. The action is to replace all of the listed fields with the properties of the user, as configured.

➢ **To add a Policy Studio rule:**

1. Open the Policy Studio page (Settings menu > Call Flow Configurations tab > Policy Studio item).

2. Click Add.
3. Configure the settings using Table 5-9 as reference.

Table 5-6: Policy Studio Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Defines the name of the Policy Studio rule to add, to facilitate management of the feature.</td>
</tr>
<tr>
<td>MATCH</td>
<td>The set of match conditions for finding a user from the Users table. Click + to add more conditions.</td>
</tr>
<tr>
<td>Source Nodes / Peer Connections</td>
<td>Select a Node or Peer Connection - or set of Nodes or Peer Connections - for which this rule will be used. If left empty, the rule is used regardless of the origin of the call.</td>
</tr>
<tr>
<td>Request field</td>
<td>Select a route REQUEST field from the following available fields (this is a field from the route REQUEST that is compared with the user properties):</td>
</tr>
<tr>
<td>Action</td>
<td>The set of replacement actions that will be performed on the route request and route response fields for a found user.</td>
</tr>
<tr>
<td>Action field</td>
<td>Select a route request or route response field from the following available fields (when a user is found, this field will be replaced with the value of the configured user properties):</td>
</tr>
</tbody>
</table>

- SOURCE_URI_USER
- SOURCE_URI_HOST
- DEST_URI_USER
- DEST_URI_HOST
- CONTACT_URI_USER
- CONTACT_URI_HOST
- CONTACT_URI_HOST

If a call matches the selected criterion, the manipulative action you select below will be performed.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_CREDENTIALS_PASSWORD</td>
<td>Multiple actions can be defined. Click + to define another action. <strong>Note</strong>: If either USER_CREDENTIALS_USER_NAME or USER_CREDENTIALS_PASSWORD is used in an action, you must add both.</td>
</tr>
</tbody>
</table>

**Request User Property**
Select a set of user properties. The request field is compared to these properties of the users. If any of the properties of a user is equal to the value of the field, then this condition is considered a match.

**Replacement User Property**
Select a set of user properties. The action is to replace the value in the request or response field with the value of this user property. If the found user has no value for this property, then no action is done on this field. If there more than one property is listed here, then ARM replaces the field with the first property if the user has it. If the user does not have it, ARM proceeds to the next property in the list, in the configured order.

### 5.2.4.1 Example of a Policy Studio Rule

Refer to the defined Policy Studio rule shown in Figure 5-12 below:

- For every route request, ARM will search for a user whose *extension* property is equal to the value of the SOURCE_URI_USER field and whose *domain* property is equal to the SOURCE_URI_HOST field.
- ARM will then replace the SOURCE_URI_USER field with the value of the found user's *external phone number* property.

**Figure 5-12: Policy Studio Rule Example**
5.3 Routing Settings

5.3.1 Configuring Criteria for a Quality Profile

You can configure criteria for a quality profile for bad, fair or good call paths based on the calculation of MOS and ASR.

You can configure a specific Peer Connection to exclude either the MOS or the ASR criterion (see Section 2.2.3.4).

After enabling 'Use Quality Based Routing' (see the figure below), the quality status of Peer Connections and Connections will be displayed in the network map's Quality Layer.

The configured quality profile can be associated with a Routing Rule (see Section 6.2) which will be applied only if all Peer Connections and Connections in the route meet the criteria.

Note: The quality of voice on a line is calculated based on the quality of voice measured in multiple calls over a period of time. The ARM issues alarm indications for quality change.

➢ To configure a quality based routing condition:

1. Open the Advanced Conditions screen (Settings > Routing > Quality Based Routing). The Use Quality Based Routing option is by default selected. If it isn't, select it.

Figure 5-13: Configuring Criteria for a Quality Profile

2. Activate either MOS, ASR or both and then configure criteria by dragging the range indicators to the lower and upper limit you require. Use the table below as reference.
Table 5-7: Configuring Criteria for a Quality Profile

<table>
<thead>
<tr>
<th>Quality Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOS (Mean Opinion Score)</td>
<td>Specified by ITU-T recommendation P.800, MOS is the average grade on a quality scale of Good to Failed, given to voice calls made over a VoIP network, after testing. MOS-LQ = listening quality, i.e., the quality of audio for listening purposes; it doesn't take bi-directional effects, such as delay and echo into account. MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects.</td>
</tr>
<tr>
<td>ASR (Answer-Seizure Ratio)</td>
<td>Measurement of network quality and rate of successful calls. % of answered calls relative to the total call volume.</td>
</tr>
</tbody>
</table>

3. Click Submit; a quality profile is generated which you can associate with a Routing Rule (see Section 6.2).

5.3.2 Configuring a Time Based Routing Condition

The time based routing feature allows you to configure a routing rule activated only at the time specified in a time condition. You can configure a condition and then associate it with a routing group or a routing rule, or both (see Section 6.2 under 'Advanced Conditions').

➢ To configure a time-based routing condition:

1. Open the Time Based Routing screen (Settings > Routing > Time Based Routing).

2. Add a time-based routing condition: Click Add; the Time Condition screen is displayed (see Figure 5-15 on the next page).
3. Configure a time-based routing condition. Use the table below as reference. See the figure above for an example.
Table 5-8: Time Condition

<table>
<thead>
<tr>
<th>Time Condition</th>
<th>Description</th>
</tr>
</thead>
</table>
| Daily/Weekly   | Select either Daily or Weekly.  
Daily - This is a daily recurring time period.  
Weekly - This is a time period recurring on given days of the week.  
The figure above shows a configured weekly condition. Green 'day' button: activated on that day. Blue 'day' button: selected in order to configure. |
| Name           | Enter an intuitive name to later be able to easily identify the condition when applying it. |
| Start time     | From the dropdowns, select the hour and the minutes past the hour. The times are configured in UTC (Coordinated Universal Time). |
| End time       | From the dropdowns, select the hour and the minutes past the hour |
| All day        | Select this option in order to base the routing condition on the entire day. |
| Enable period  | Select this option in order to base the routing condition on a period. |
| Start of period| From the calendar icon, select the date on which the period will start. From the dropdowns, select the hour and the minutes past the hour. |
| End of period  | From the calendar icon, select the date on which the period will end. From the dropdowns, select the hour and the minutes past the hour. |

4. Click OK; a profile is generated which you can associate with a Routing Rule (see Section 6.2 under 'Advanced Conditions'. In addition, you can associate the configured time condition with a Routing Group. In this case, it will apply to all Routing Rules in the Group. Note that the same time condition profile can be reused multiple times.

5.3.3 Configuring SIP Alternative Route Reason

The ARM operator can configure SIP responses in the SIP Alternative Route Reason page, which will cause the ARM to apply alternative routing paths if available.

**Note**: If a call fails and the SIP response received from the remote side is not configured in the SIP Alternative Route Reason page, the ARM will not apply an alternative route for the call.

The page allows operators to change the default ARM behavior for an Alternative Routing decision.

- **To configure a SIP Alternative Route Reason:**
2. Click the Add tab.

Figure 5-18: Adding an Alternative Routing SIP Reason

3. Enter the SIP Response number (200-600).
4. Provide a description of the reason.
5. Select the Active option to activate the configuration.
6. Click the now-enabled OK button.

➢ To edit a SIP Alternative Route Reason:
1. In the Alternative Routing SIP Reasons screen, select the SIP response to edit.

Note:
- SIP responses are listed in numerical order.
- You can browse to the next page or to the last page of responses.
- You can browse to the page before the page you are on, if you’re not on the first page, or you can browse to the first page.

2. Click Edit.
3. Edit according to your requirements and click **OK**.

**Note:** By clearing the 'Active' option, the operator can 'deactivate' a SIP reason without deleting its row in the table. If a SIP reason is 'deactivated', the ARM will not apply an alternative route. The ARM will function as if there is no row at all. The 'deactivated' row, however, remains in the table, and if the operator redecides, it can be 'reactivated' by selecting the 'Active' option.

➢ To delete a SIP Alternative Route Reason:
1. In the Alternative Routing SIP Reasons screen, select the SIP response to delete.

2. Click **Delete**.

### 5.3.4 Configuring Global Routing Settings

This section shows how to configure global routing settings.

➢ To configure global routing settings:
1. Open the Routing Settings page (**Settings** menu > **Routing** tab > **Routing Settings** item).

2. Configure the parameters using **Table 5-9** as reference.
### Table 5-9: Routing Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of Routing Attempts</td>
<td>Defines the maximum number of routing attempts per call. If the maximum number of routing attempts has not yet been reached, the ARM searches for an alternative routing possibility for the specific call.</td>
</tr>
<tr>
<td>Maximum number of Routing Attempts per Routing Rule Action</td>
<td>Defines the maximum number of routing attempts per destination. If the maximum number of routing attempts has not yet been reached, the ARM tries to re-route the call to a preferable destination.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.
5.4 Administration Settings

This section shows how to perform administrative tasks:
- Configure a software license (see the section below)
- Manage security (see Section 5.4.2)
- Add an operator (see Section 5.4.3)

5.4.1 Configuring a Software License

The ARM must be licensed with a valid license for the product to become fully operational. This section shows how to configure one.

➢ To activate a license:
1. Open the SW License page (Settings menu > Administration tab SW License item).

Figure 5-22: Software License Page

2. Select and copy the 'Machine ID' shown in red in the figure above.
3. Activate the product through the AudioCodes License Activation tool at www.audiocodes.com/swactivation. You'll need your Product Key and the Server Machine ID for the activation process. An email will subsequently be sent to you with your Product License.
4. Copy and paste the Product License string that AudioCodes sends you into the 'License Key' field, and then click Submit; the number of sessions purchased and the license expiry date are displayed.
5. Make sure the license details (the number of sessions purchased and the license's expiry date) are those that you purchased.
5.4.2 Securing the ARM

This section shows how to secure the ARM.

➢ To secure the ARM:

1. Open the Security page (Settings menu > Administration tab Security item).

   Figure 5-23: Security Page

2. Use the table below as reference.

   Table 5-10: Security Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session timeout</td>
<td>Closes the session timeout and forces the user to reenter their password (in order to reopen the session) if the timeout you define (in hours) expires.</td>
</tr>
<tr>
<td>(hours)</td>
<td></td>
</tr>
<tr>
<td>Inactivity period</td>
<td>Suspends the user's account if the user does not log in to the ARM over the period you define. 0 disables the feature; users accounts will then never be suspended due to inactivity.</td>
</tr>
<tr>
<td>(minutes)</td>
<td></td>
</tr>
<tr>
<td>http/https enabled</td>
<td>Enables an HTTP/HTTPS connection between the ARM server and the SBC / Gateway.</td>
</tr>
<tr>
<td>Username</td>
<td>Username and Password are the default credentials that ARM uses when communicating with the node. Default: Admin/Admin. The ARM uses this Username and Password if you select the Use general credentials option in the NODE UPDATE screen (see above). Change the Username only if the credentials of the node isn't Admin/Admin.</td>
</tr>
<tr>
<td>Password</td>
<td>Username and Password are the default credentials that ARM uses when communicating with the node. Default: Admin/Admin. The ARM uses this Username and Password if you select the Use general credentials option in the NODE UPDATE screen (see above). Change the Password only if the credentials of the node isn't Admin/Admin.</td>
</tr>
</tbody>
</table>

3. Click Submit; the security configuration is saved.
5.4.3 Adding/Editing an Operator

This section shows how to add an operator (i.e., network administrator or IT manager).

➢ To add an operator:

1. Open the Operators page (Settings menu > Administration tab Operators item).

   Figure 5-24: Operators

2. Click Add.

   Figure 5-25: Operator Details

3. Configure the operator details using the table below as reference.

   Table 5-11: Operator Details

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the operator to log in with.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password for the operator to log in with.</td>
</tr>
<tr>
<td>Password confirm</td>
<td>Confirm the password.</td>
</tr>
<tr>
<td>Security Level</td>
<td>Select a Security Level for the operator: ADMIN or SECURITY_ADMIN. ADMIN cannot (for example) change passwords, add or change operators, or perform licensing.</td>
</tr>
</tbody>
</table>

4. Click OK; the operator is added.
5.5 Adding a Routing Server

This section shows how to add a Routing Server.

➢ To add a Routing Server:

1. Open the Routing Servers page (Settings menu > Routing Servers tab).

![Figure 5-26: Routing Servers](image)

2. Click Add.

![Figure 5-27: Server Details](image)

The ARM operator can edit the Nodes list when adding the new router. After it's added, the operator can connect or disconnect the Node to/from a specific router via the node's Properties (see Figure 2-8 and the description under Section 2.2.3.1).

3. Configure the routing server using Table 5-12 below as reference.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the ARM Router (routing server).</td>
</tr>
<tr>
<td>Address</td>
<td>Enter the IP address or host name for the ARM Router (routing server).</td>
</tr>
<tr>
<td>Port</td>
<td>[Read only] ARM Router (routing server) port number. Default: 443</td>
</tr>
<tr>
<td>Protocol</td>
<td>[Read only] HTTPS</td>
</tr>
<tr>
<td>Nodes</td>
<td>Allows you to specify to which Nodes (SBCs/Gateways) the routing server will be added. Only possible when adding a routing server, not when editing.</td>
</tr>
</tbody>
</table>

4. Click OK; the routing server is added.
5.5.1 Editing a Routing Server

This section shows how to edit a routing server.

➢ To edit a Routing Server:

1. Open the Routing Servers page (Settings menu > Routing Servers tab).

![Figure 5-28: Routing Servers](image1)

2. Select the row of the routing server to edit, and then click Edit.

![Figure 5-29: Server Details](image2)

3. Configure the server details using the table below as reference.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>[Read-only] The name of the ARM Router (routing server).</td>
</tr>
<tr>
<td>Address</td>
<td>Enter the IP address or host name for the ARM Router (routing server).</td>
</tr>
<tr>
<td>Port</td>
<td>[Read only] ARM Router (routing server) port number. Default: 443.</td>
</tr>
<tr>
<td>Protocol</td>
<td>[Read only] HTTPS</td>
</tr>
<tr>
<td>Nodes</td>
<td>[Read only] The Nodes (SBCs or Gateways) to which the router was added.</td>
</tr>
<tr>
<td>Advanced Configuration</td>
<td>To display this parameter, click adjacent to Advanced Configuration. From the dropdown, select the protocol between the Configurator and the Router (HTTP or HTTPS). Default: HTTPS. HTTP can temporarily be used for debugging purposes.</td>
</tr>
</tbody>
</table>

![Table 5-13: Server Details](image3)
5.5.2 Locking/Unlocking a Routing Server

The ARM allows users to lock routing servers, for troubleshooting or maintenance purposes. Locking a routing server causes the devices to disconnect from the locked routing server, causing all traffic to divert to the other unlocked and available servers. Unlocking a routing server causes the devices to reconnect, and makes the routing server fully functional.

A locked routing server can also be associated with ARM Nodes without participation in calls routing. This can be useful during the preparation phase for network setup.

➢ To lock or unlock a Routing Server:
1. Open the Routing Servers page (Settings > Routing Servers).

   ![Figure 5-30: Routing Servers - Administrative State]

2. Determine from the icon under the 'Administrative State' column whether a routing server is locked or unlocked, and then click the Lock / Unlock button.

   An unlock performs a restart of the Routing Manager software. The action takes a few seconds, during which time the Routing Manager is unavailable due to the restart. A lock action is immediate.

   These actions can be applied to any particular ARM router. The functionality lets you gracefully take a particular router temporarily out of service. A locked router responds to all keep-alive and login requests, from all nodes, with a standard 'Service Unavailable' HTML error. This behavior causes all nodes to be disconnected from the router, effectively taking the router out of service. The router still responds to any other request from the nodes or the configurator, which makes the lock action graceful since calls, statistical calculations and software upgrades are unaffected.
This page is intentionally left blank.
6 Defining Calls Routing

The ARM lets IT managers, responsible for enterprise VoIP, define call routing. ARM routing provides a comprehensive call routing solution for a telephony network.

➢ To define calls routing:

- Open the Routing page ('Routing' menu); the page opens under the Routing Groups tab by default.

Figure 6-1: Routing

➢ Follow this procedure when defining calls routing policy (ARM Dial Plan):

1. Add a new Routing Group (see Section 6.1)
2. Add a new Routing Rule (see Section 6.2)
3. Test the route (see Section 3.4)
6.1 Adding a Routing Group

Before adding a rule, you must add a Routing Group. Routing Groups help you present rules in the GUI in an organized fashion, enhancing user experience. Routing Groups also allow you to move a group of Routing Rules, collectively changing their routing priority.

➢ To add a Routing Group:

1. In the Routing page under the Routing Groups tab, click Add Group.

   ![Add Group]

   The Routing Group Settings dialog opens, shown in the figure below.

   ![Routing Group Settings]

2. Define a name for the Routing Group to be added. Define a user-friendly name to facilitate intuitive management by administrators. Some example of groups you can add are 'Restricted Calls', 'Calls to Europe', 'Calls to Far East', 'Calls to ROW', etc.

   **Note:** The routing group's name must be distinct from names of other routing group names, and must be between 1-999 characters.

3. Select the use time conditions option to attach a time condition to the Routing Group. See Section 5.3.2 for related information on how to attach a time condition to a Routing Rule. You can attach multiple time conditions. These conditions will apply to all rules in the group. Note that if you attach a time condition to a group, it's indicated visually in the Routing Groups page as follows:

   ![Routing Conditions]

4. Click OK; the new Routing Group is added to the list.

   **Note:**
   - Routing Groups listed higher take precedence over those lower.
   - Routing Groups in the list can be reordered (see Section 6.1.2).
   - Priority is calculated internally, based on Previous and Next groups.
6.1.1 Editing a Routing Group

You can edit a Routing Group if necessary.

➢ To edit a Routing Group:

1. In the Routing page under the **Routing Groups** tab, select the Routing Group to edit, and then either:
   a. Click **Edit Group** shown in the figure below -or-

   **Figure 6-4: Edit Group**

   ![](Figure_6-4.png)

   b. Click the **Edit** icon in its row which is then enabled, shown in the figure below.

   **Figure 6-5: Routing Group**

   ![](Figure_6-5.png)

   The Routing Group Settings dialog opens.

   **Figure 6-6: Routing Group Settings**

   ![](Figure_6-6.png)

2. Edit the 'Name' field. Enter a user-friendly name in order to facilitate intuitive management by network administrators.

3. Edit the time condition. You can clear the **use time conditions** option to remove the condition. See Section 5.3.2 for related information. You can alternatively remove a single condition if multiple time conditions are attached.

4. Click **OK**.
6.1.2 Moving a Routing Group

You can promote or demote a Routing Group listed in the Routing Groups page. When moving a Routing Group, all its Routing Rules are moved and the routing priority of all the Routing Rules in the group are collectively changed at once. Routing Groups listed higher in the page take precedence over those listed lower.

➢ To move a routing group:

1. In the Routing page, under the Routing Groups tab, either drag and drop the Routing Group to where you want to locate it, or select it and then click the then-enabled Move icon next to it.

![Figure 6-7: Move Icon](image)

The Move Routing Group dialog opens:

![Figure 6-8: Move Routing Group](image)

2. Select Before or After, click the Routing Group before which / after which to move the Routing Group you want to promote/demote, and then click OK.

Alternatively, you can move a Routing Group by clicking the icon shown in the figure below, and then dragging it and dropping it in the Routing Groups page.

![Figure 6-9: Moving a Routing Group by Dragging and Dropping](image)
6.1.3 Deleting a Routing Group

You can delete a Routing Group if necessary, including rules associated with the group.

- **To delete a Routing Group:**
  - In the Routing page under the **Routing Group** icon, select the Routing Group to delete and then either:
    - **a.** Click **Delete Group:**
      - Figure 6-10: Delete Routing Group

      ![Figure 6-10: Delete Routing Group](image)

      - **-or-**
    - **b.** Click the **Delete** icon in its row which is then enabled:
      - Figure 6-11: Delete Routing Group

      ![Figure 6-11: Delete Routing Group](image)

      You're prompted to confirm:

      ![Confirmation Dialog](image)

      - **c.** Click **Delete.**
6.2 Adding a New Routing Rule

After adding a Routing Group, add a new Routing Rule to associate with the Group. Each Routing Rule is given a unique priority within the Routing Group. A rule listed higher than another, even if in the same Routing Group, takes precedence.

**Note:**
- Routing rules are defined within Routing Groups.
- To view a specific Routing Group’s Routing Rules, click that Group.
- To view all Routing Rules, click the **Routing Rules** tab.
- Any modification to the routing configuration (adding, deleting or modifying) takes effect within 60 seconds after the modification request is answered by the configurator and does not affect active calls.
- Any modification to routing logic as a result of an operational state change to a node or Peer Connection takes effect within 60 seconds after the status change is identified by the configurator.
- Any modification to routing logic as a result of a node or Peer Connection administrative state change takes effect within 60 seconds after the status change is identified by the configurator.
- Changes in users or user groups take effect within 60 seconds after the modification is identified by the configurator.

Routing Rules include:
- **Conditions:** [Optional] Define the characteristics of the route request, e.g., the User Group and phone prefix of the originator/destination.
- **Actions:** [Mandatory] Define actions performed if the call matches the rule conditions i.e., routes the call to the specified destination, or discards it specifying a SIP reason.

![Figure 6-12: Example of a Routing Rule](image)

The ARM parses from the top Routing Group listed, to the bottom Routing Group listed, and within each Routing Group from the top Routing Rule listed to the bottom Routing Rule listed. If it finds a matching rule and if devices and Connections/Peer Connections are available, it sends the call to the destination configured for that rule. If it doesn’t find a matching rule, it indicates that a route for the call has not been found.

**Alternative Routing**

The ARM performs alternative routing as follows:
- The ARM attempts to build an alternative path for the same Routing Rule action (Node, Peer Connection, VoIP Peer), if available.
- ARM attempts to build an alternative action (Node, Peer Connection, VoIP Peer), if available, for this call, in the order that actions are listed in the Routing Rule.
- All routing alternatives are sorted by weighted path, cost and then by number of hops.

**Load Balancing**

The ARM can balance call traffic between multiple destinations of the same Action. Call traffic can be distributed equally between destinations, or the distribution can be defined by the operator.

**Discard Call** - the ARM can be configured to discard calls matching specific conditions as a single action, or as the last action of a rule if previous destinations were unavailable.
To add a new Routing Rule to a Routing Group:

1. In the Routing Groups page under the Routing Groups tab, select the Routing Group with which to associate the rule, and then click Add Rule.

   Figure 6-13: Add Rule

   ![Add Rule Screen](Image)

   This screen opens:

   Figure 6-14: Routing Rule Settings

   ![Routing Rule Settings](Image)

2. Enter a name for the routing rule that is distinct from the names of the other routing rules in the same group. Define a user-friendly name to facilitate intuitive management by network administrators. The name can be between 1-999 characters.

3. Switch ON or OFF the parameters Call Routing and/or Test Mode. See Section 3.4.
   - **Call Routing.** When set to ON, the rule will be taken into consideration for live calls traffic.
- **Test Mode.** When set to **ON**, the route will be tested offline without impacting live calls traffic.

**Figure 6-15: Call Routing / Test Mode**

By default, new routing rules are added with 'Test Mode' set to **ON** and 'Call Routing' set to **OFF**. The table below shows the combinations that are supported for a Routing Rule:

**Table 6-1: Call Routing / Test Mode Combinations**

<table>
<thead>
<tr>
<th>Call Routing / Test Mode Combination</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Routing is <strong>ON</strong> and Test Mode is <strong>ON</strong></td>
<td>The rule will be taken into account for both options of 'Test route mode', and for real traffic.</td>
</tr>
<tr>
<td>Call Routing is <strong>ON</strong> and Test Mode is <strong>OFF</strong></td>
<td>The rule will be taken into account when 'Test route mode' is set to <strong>Use routing rules in Call Routing</strong>, and for real traffic. Used to simulate rule removal.</td>
</tr>
<tr>
<td>Call Routing is <strong>OFF</strong> and Test Mode is <strong>ON</strong></td>
<td>The rule will only be taken into account for <strong>Use only routing rules in Test Mode</strong>. Used to simulate and test a newly added Routing Rule.</td>
</tr>
<tr>
<td>Call Routing is <strong>OFF</strong> and Test Mode is <strong>OFF</strong></td>
<td>The rule will not be used for testing nor for live traffic. Used to prepare a Dial Plan.</td>
</tr>
</tbody>
</table>

4. Configure the 'Source' settings - use the table below as reference.

**Table 6-2: Source Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefixes/Prefix Groups</td>
<td>Enter a source number prefix, or list of prefixes. You can also enter the name of a prefix group, or from the dropdown select a prefix group or list of prefix groups. See Section 5.2.2.</td>
</tr>
<tr>
<td>Hosts</td>
<td>Enter a source hostname, or list of hostnames.</td>
</tr>
<tr>
<td>User Groups</td>
<td>Enter the name of a source user group or list of source user groups, or select user groups from the dropdown. See Section 4.2.</td>
</tr>
<tr>
<td>Nodes/Peer Connections</td>
<td>Enter names of source nodes or peer connections, or a list of nodes or peer connections, or select nodes or peer connections from the dropdown. Must be configured if you want to define a routing rule applicable to specific call sources rather than (globally) to the entire network.</td>
</tr>
</tbody>
</table>

5. In the Routing Rule Settings screen, click **Destination**.

**Figure 6-16: Destination**

6. Configure the 'Destination' settings using the table below as reference.
Table 6-3: Destination Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix/Prefix Groups</td>
<td>Enter a destination number prefix, or list of prefixes. You can also enter</td>
</tr>
<tr>
<td></td>
<td>the names of a prefix group or select prefix groups from the dropdown.</td>
</tr>
<tr>
<td>Hosts</td>
<td>Enter a destination hostname or list of hostnames.</td>
</tr>
<tr>
<td>User Groups</td>
<td>Enter the names of a user group, or list of destination user groups or</td>
</tr>
<tr>
<td></td>
<td>select user groups from the dropdown.</td>
</tr>
</tbody>
</table>

7. In the Routing Rule Settings screen, click **Advanced Conditions**.

![Figure 6-17: Advanced Conditions](image)

8. Under ‘Quality Based Routing’, select the option **include paths with the following quality**; the dropdown becomes available. From it, select the quality criteria that you defined as shown in Section 5.3. Criteria for bad, fair and good quality, based on the calculation of MOS and ASR, can be defined. This screen lets you associate the criteria you defined with the Routing Rule.

9. Under 'Time Based Routing', select the option **use time conditions**; the pane becomes available. From the dropdown, select the time on which routing will be based, configured under **Settings > Routing > Time Based Routing** (see Section 5.3 for information about configuring a time range).

**Note:**

- More than one Time Condition can be associated with the same Routing Rule. Activation of the Routing Rule is then performed in 'or' between Time Conditions.
- A Time Condition can be attached to a Routing Rule which belongs to a Routing Group with an already-associated time period; the ARM's calculation of this Routing Rule's activation will then be 'and'; the rule will be activated during the time period assigned to the Routing Group and the time period assigned to the Routing Rule.
10. In the Routing Rule Settings screen, click **Routing Actions**: The action or set of actions to be taken if this Routing Rule matches. Click + to add an action.

11. Use the table below as reference.
Table 6-4: Routing Actions

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Action] left dropdown field</td>
<td>Select from the dropdown the Peer Connection, VoIP Peer or Node to which the call will be routed. In the figure above, the Peer Connection IpGrp1 (Italy) is selected.</td>
</tr>
<tr>
<td>[Via] right dropdown field</td>
<td>[Optional] Select from the dropdown the Node that the call must pass through. In the figure above, the Node Paris_2 is selected. Only a single Node can be added in Via.</td>
</tr>
<tr>
<td>&gt; Normalization groups</td>
<td>Click &gt; to open post routing (after routing) normalization.</td>
</tr>
<tr>
<td>Source normalization group</td>
<td>Select a normalization group (see Section 5.2.1) to manipulate the source number in the outgoing call to the peer connection. The source normalization group can only be connected to an IP Group or VoIP Peer. It cannot be connected to a Node.</td>
</tr>
<tr>
<td>Destination normalization group</td>
<td>Select a normalization group (see Section 5.2.1) to manipulate the destination number in the outgoing call to the peer connection. The destination normalization group can only be connected to an IP Group or VoIP Peer. It cannot be connected to a Node.</td>
</tr>
</tbody>
</table>

12. Click **Add loading balancing**; the screen shown in Figure 6-20 on the next page is displayed.

**Figure 6-20: Routing Actions – Load Balancing - Equally Balanced (Default)**

Load balancing is added between more than one Peer Connection, Node or VoIP Peer. By default, these are *equally balanced*, i.e., the same percentage is assigned for each option, as shown in the figure above.

You can optionally define your own percentage by clearing the 'Equally Balance' option. Any distribution can be chosen, i.e., any percentage of calls can be handled by a specific routing option. Several routing destinations (more than two) are supported using the **Add load balancing** button, as shown in Figure 6-21 below.

13. Enter the percentage of routes that will take this action when load balancing is configured and **Equally Balance** is cleared. Make sure you have 100% in the Action's calls destinations summary else you won't be allowed to enable the action.
14. Click the Call Discard action icon

Figure 6-22: Routing Actions – Call Discard

15. Use the table below as reference

Table 6-5: Routing Actions – Call Discard

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard Action</td>
<td>In a routing rule, you can apply a policy to attempt a number of routing</td>
</tr>
<tr>
<td></td>
<td>options and to discard the call if none succeed. The <strong>Discard call</strong></td>
</tr>
<tr>
<td></td>
<td>routing action can be used - in addition to other routing actions of the</td>
</tr>
<tr>
<td></td>
<td>same rule - as a last routing rule action or as a sole action. You can</td>
</tr>
<tr>
<td></td>
<td>provide a specific SIP reason for 'Discard Call' as well as use the last</td>
</tr>
<tr>
<td></td>
<td>SIP reason received from the SBC or the Gateway.</td>
</tr>
<tr>
<td>SIP Reason</td>
<td>Enter the SIP reason to be returned to the source peer connection when</td>
</tr>
<tr>
<td></td>
<td>rejecting the call. Must be a valid SIP reason in range 400-699.</td>
</tr>
</tbody>
</table>

**Note:** If any field is left empty (Prefix Group/Host/User Group/Nodes/Peer Connections), the rule will not check it.
6.2.1 Editing a Routing Rule

You can edit a rule if necessary.

➢ To edit a Routing Rule:

■ Select the Routing Group under which the rule is defined, select the Routing Rule to edit, and then either:

a. Click the then-enabled **Edit Rule** button or click the then-enabled **Edit** icon, shown in the figure below; the screen shown in **Figure 6-14** is displayed.

![Figure 6-23: Edit Rule](image)

b. Edit the rule using the table above as reference.

c. To view a rule's conditions and actions, expand the rule by clicking the **▼** icon; the window shown in the figure below opens. In the left pane, you can see the route conditions. In the right pane, you can see the actions.

![Figure 6-24: Viewing a Routing Rule's Conditions-Actions](image)

6.2.2 Moving a Routing Rule

You can move a rule within the group under which it is defined, or you can move it to another group, above or below a rule defined within that group.

➢ To move a rule:

1. Select the Routing Group under which the rule is defined and then
   • Drag and drop the rule to the location you want to move it to as shown in the figure below -OR-
   • Select the rule to move and then click the now-enabled **Move** icon shown in the figure below.
The Move Routing Rule dialog is displayed.

2. From the 'Group' dropdown, select the group to which you want to move the rule.
3. Select either **Before** (default) or **After** and then select the rule before which or after which you want to move the rule.
4. Click **OK**; the rule is moved to the location you defined.

### 6.2.3 Deleting a Rule

You can delete a rule if necessary.

- **To delete a rule:**
  1. Open the group under which the rule is defined, and then adjacent to the defined rule that you want to delete, click the now-enabled **Delete** icon shown in the figure below – OR- click the now enabled **Delete Route** button also shown in the figure below.
2. In the Confirmation prompt ‘Are you sure you want to delete this rule?’ shown in the figure below, click **Delete**.

![Figure 6-28: Delete Icon](image)

The rule is deleted.
6.3 Testing a Route

You can test a route to make sure it performs according to expectations. See Section 3.4 for more information.

6.4 Viewing Routing Performance Statistics

The ARM's Routing page under the Routing Groups tab lets you determine network calls distribution and to debug, tune and optimize a Dial Plan. The pane on the right of the page allows you to view the distribution of statistics such as routing attempts, routing failures, routing first match, etc., between rules in the selected group and actions in the selected rule.

6.4.1 Group Statistics | ARM Statistics

You can view statistics for a selected group, on the top routing rules as well as on a selected routing rule.

- To view group statistics:
  1. In the Routing Groups page, select the group and then select a rule. The figure below shows an example of statistics displayed.

Figure 6-29: Group Statistics

- The uppermost graph displays statistics for the selected group.
6. Defining Calls Routing

2. From the ‘Statistic Type’ dropdown, choose either:
   • Routing Attempts
   • Routing Failures
   • Routing First/Second/Third Match
3. From the ‘Elements Type’ dropdown, choose Top Active or Least Active.
4. From the 'Number of Elements' dropdown, choose the number of bars to display in the group chart. Choose 5-50 in increments of 5.

➢ To view ARM statistics:
1. Click the ARM Statistics tab.

Figure 6-30: ARM Statistics

- The uppermost graph displays statistics related to groups.
- The lowermost graph displays statistics related to rules.
2. From the 'Statistic Type' dropdown, choose either:
   • Routing Attempts (shown in the figure above)
   • Routing Failures
   • Routing First/Second/Third Match
3. From the 'Elements Type' dropdown, choose Top Active or Least Active.
4. From the 'Number of Elements' dropdown, choose the number of bars to display in the group chart. Choose 5-50 in increments of 5.
6.5 Using the Routing Rules Table View Page

Some network administrators prefer to manage routing rules in the Routing Rules table view page. The page offers a significant advantage: Administrators can select multiple rules and perform a multi-action on the selection.

➢ To open the page:

1. In the Routing page, click the Routing Rules menu; the page shown in Figure 6-31 below opens.

![Figure 6-31: Routing Rules Table View Page](image)

2. Select a rule or select multiple rules; the actions buttons are activated. Administrators can:
   - Edit a rule
   - Delete rules
   - Lock / Unlock rules
   - Duplicate a rule (allows administrators to conveniently and easily add a rule based on an already defined rule)
   - Move rules

3. In the Search field, enter a search string. The functionality allows administrators to search in all the defined rules, not just in a Rules Group.
7 Viewing Alarms

The Alarms page shown in the figures below displays alarms generated in the enterprise's network topology, e.g., SBC disconnected. In the page, you can view alarms information displayed under two tabs:

- **Active Alarms** (default)
- **History Alarms**

Both pages display the following column headers:

- **SEVERITY**
- **DATE AND TIME**
- **NAME**
- **ALARM SOURCE**
- **DESCRIPTION**

Click any alarm listed on any page; that alarm's ALARM SUMMARY pane, shown in the figure below, displays the column information as well as:

- **ALARM TYPE**
- **PROBABLE CAUSE**
- **ADDITIONAL INFO1**
- **ADDITIONAL INFO2**
- **ACKNOWLEDGED**

![Figure 7-1: Alarms – Active Alarms + Alarm Summary](image-url)
In these pages you can
- Sort alarms, according to column header
- Use the 'Search' feature to locate specific alarms (see Section 7.2 below).
- Refresh the page / Stop Auto Refresh
- Acknowledge Alarm. Applies only to the Active Alarms page. Click the button to clear a selected alarm from the page. Note that after acknowledging it, the alarm can be still viewed in the History Alarms page.

7.1 Collecting Information via SNMP to Enhance Network Telephony Performance

This feature provides enterprise network administrators the option to collect information on devices via Operations Support Systems (OSS) traps sent over Simple Network Management Protocol (SNMP).

Network administrators can then modify that information to enhance telephony network performance.

➢ To collect information via SNMP:
1. In the Alarms page, click the SNMP Destinations tab and then click Add.

Figure 7-3: SNMP Destination Details

2. Use Table 7-1 on the next page as reference.
# Table 7-1: SNMP Destination Details

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the IP address of the OSS host.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the number of the port to which to send OSS traps.</td>
</tr>
<tr>
<td>Community</td>
<td>SNMP Community String. Sent with each Get-Request as a type of password to allow or deny access.</td>
</tr>
</tbody>
</table>
7.2 Locating a Specific Alarm

The search feature helps network administrators quickly and easily locate specific alarms. This facilitates effective management which in turn leads to improved network performance.

➢ To search for a specific alarm:

1. Enter a search string in the search field shown in the figure below, or for an advanced search, click the dropdown arrow; the dialog shown in the figure below it is displayed.

   ![Figure 7-4: Search Field](image)

   ![Figure 7-5: Searching for a Specific Alarm](image)

2. Enter any information about the alarm you know. You must enter information in at least one field.
   - The 'Name' field is identical to the simple search string field.
   - From the 'Severity' dropdown, select Clear, Indeterminate, Warning, Minor, Major or Critical. All alarms whose severity level match your selection will be displayed.
   - For the alarm 'Source', enter the node name or the Peer Connection name, if you know it. All alarms originating from that source will be displayed.
   - In the 'Description' field, enter a key word used to describe the alarm.
   - Select either Between Times, Last 24 hours, Last week or Last 30 days. All alarms whose timestamp matches your selection will be displayed.

3. Click Search.
8. Migrating Device Routing to the ARM

This section shows how to migrate device routing to the ARM.

Note:
- This section assumes familiarity with the AudioCodes device whose routing is to be migrated to the ARM. See Related Documentation for references to AudioCodes' device documentation.
- The screenshots shown in this section are of Web interface version 7.2. If you're using Web interface version 7.0 or earlier, refer to earlier versions of this document.

8.1 AudioCodes Device Application Types

Before migrating device routing to the ARM, it's best to first get acquainted with the routing logic of AudioCodes' device application types. This section describes the routing logic of the three AudioCodes device application types:

- SBC device application
- Gateway device application
- Hybrid device running both a Gateway application and an SBC application

8.2 ARM Network Routing Logic

AudioCodes device's routing logic is centralized in its local routing table independently of the ARM. The SBC's routing logic is centralized in the IP-to-IP Routing Table. The Gateway's routing logic is centralized in the Tel-to-IP and IP-to-Tel routing table.

To integrate a device into the ARM network, the routing logic must be migrated to the ARM so that:

- All calls will be routed by the ARM.
- If a device disconnects from the ARM, calls will be managed by the device's internal routing table.
- If the ARM cannot find any route that matches a specific call, the call will be managed by the device's internal routing table.
- If the device fails to establish a call according to the ARM's routing directive (for example, a SIP error is received), the call will be discontinued.

8.2.1 SBC Routing Logic

AudioCodes' SBC routes and handles IP-to-IP calls. The SBC routing logic is centralized in the IP-to-IP Routing Table. For the ARM to route calls, you must configure a related routing rule in the SBC's internal IP-to-IP Routing Table as described in Section 8.5.

8.2.2 Gateway Routing Logic

AudioCodes' Media Gateway routes and handles IP-to-Tel, Tel-to-IP and Tel-to-Tel calls using an internal loopback IP Group.

Gateway routing logic is configured in the device's internal IP-to-Tel and Tel-to-IP tables. To migrate the gateway application's routing logic to the ARM network, you must set the routing parameter 'Gateway Routing Server' to Enable. In this case, all internal routing tables of the device will be used as fallback as described in Section 8.2, and all calls will pass through the ARM. For more information, see Section 8.6.
8.2.3 Hybrid Device Routing Logic

The ARM routes calls from the hybrid device’s PSTN (gateway application) to IP (SBC application) or vice versa.

Calls cannot be routed from an IP Group (PCon in ARM) associated with a gateway application, to an IP Group associated with an SBC application on the same hybrid device.

To support a hybrid device, two internal IP Groups must be configured:
- From the SBC application to the Media Gateway application
- From the Media Gateway application to the SBC application

The ARM GUI does not display these two internal IP Groups. Routing is performed according to the logic described in the SBC and Media Gateway sections above, respectively.

See Section 8.7 for information about how to migrate hybrid device routing to the ARM.

8.3 Connecting the Device to the ARM Topology Server

You need to connect the device to the ARM Topology Server. Screenshots are for illustrative purposes.

➢ To connect the device to the ARM Topology Server:

1. In your internet browser, enter the device’s IP address in the Address bar, and then in the login page that opens, enter the User Name and Password (Admin, Admin are the defaults).

2. In the device’s Web interface that opens, check the Setup menu and then navigate to the HTTP Remote Services page (IP Network > Web Services > Remote Web Services).

![Figure 8-1: Web Interface - Remote Web Services](image)

3. Click +New or click here to add new row.
4. Configure the dialog using the figure above as reference, and click **Apply**.

5. Click the **HTTP Remote Hosts** link shown in the figure above.

6. In the HTTP Remote Hosts page that opens, click the **Add** tab.
7. Define the IP Address of the ARM Topology Server to which you want to point the device and define the ARM Topology Server settings, and then click Save; wait until connected.

8. Make sure in the Remote Web Services – HTTP Remote Hosts screen shown in the figure above that the status of the host, i.e., of the ARM Topology Server, is Connected.

9. Connect to the router/s.

10. Make sure that the device is connected to all HTTP ARM services i.e., ARM Topology Server and router/s, as shown in the figure above.
8.4 Migrating SBC/Gateway/Hybrid Routing to the ARM

This section shows how to migrate an AudioCodes device to the ARM network.

After making sure that the device is connected to all HTTP ARM services i.e., ARM Topology Server and router/s, you can begin to migrate the routing logic from that configured in the device, to the ARM. Screenshots in this section are for illustrative purposes. The section shows the general changes that must be made.

➢ To migrate an AudioCodes device to the ARM network:
• Configure IP Groups and SIP interfaces used by the ARM:
  1. In the device’s Web interface, navigate to the SIP Interface Table Page (Setup > Signaling & Media > Core Entities > SIP Interfaces).
  2. Navigate to the SIP Interface Table Page (Setup > Signaling & Media > Core Entities > SIP Interfaces).
  3. Locate the SIP Interface to expose the enterprise network to the ARM environment.

   Figure 8-7: Web Interface – SIP Interfaces

   Figure 8-8: Web Interface – SIP Interfaces Table - Configuring a SIP Interface

  4. Set the ‘Used By Routing Server’ parameter to Used.
  5. Click Save.
8.5 Migrating SBC Routing to the ARM

This section shows how to migrate SBC routing to the ARM network. After making sure the SBC is connected to all HTTP ARM services i.e., ARM Topology Server and router/s, you can begin to migrate the routing logic from that configured in the SBC, to the ARM. Screenshots in this section are for illustrative purposes only.

Note:
- See also Appendix A.
- 'IP Group' and 'Trunk Group' in the Web are called 'Peer Connection' in the ARM.

➢ To migrate routing logic to the ARM:
1. In the Web interface, navigate to the IP Groups page (Setup > Signaling & Media > Core Entities > IP Groups).
2. Locate the IP Group to expose the enterprise network to the ARM environment. Make sure the SIP interface associated with this IP Group is configured as ‘used by routing server’. See Section 8.4.

Figure 8-9: Web Interface – IP Groups

![Image of IP Groups page]

3. [Mandatory] Enter a unique name for the IP Group.
4. [Mandatory] Set the ‘Used By Routing Server’ parameter to Used.
5. Click Save.
6. In the ARM GUI, make sure the device is displayed in the Network page, Map view. Verify that the peer connection you configured is displayed. Unlock it (see Section 2.2.3.2); make sure its color is green (see Section 2.2.3.2).
Note: After configuring an IP group and then viewing it in the ARM, it is strongly recommended not to change its unique name. Changing its unique name will prevent routing by the ARM of calls to this Peer Connection (IP group) and receipt by the ARM of calls from this Peer Connection (IP group).

7. In the Web interface, open the IP-to-IP Routing page (Setup > Signaling & Media > SBC > IP-to-IP Routing). The screen below shows an example of two routing rules.

Figure 8-11: Web Interface – IP-to-IP Routing

Figure 8-12: Web Interface – IP-to-IP Routing Table – Add Row – Rule tab

8. Define a 'Name' and for 'Request Type', define INVITE (see Appendix E if you need to use the ARM to route other SIP Request Types such as MESSAGE or NOTIFY). Leave all other conditions fields undefined (i.e., No Conditions, or Any).

9. From the 'Destination Type' dropdown, select Routing Server. This rule will serve to perform routing via the ARM.

10. Leave all other fields undefined, and then click Add.

11. In the ARM GUI's Routing page, configure a rule parallel to one of the rules configured in the Web interface's IP-to-IP Routing page (see Section 6.1).

Figure 8-13: Configuring a Routing Rule in the ARM

12. In the ARM GUI, switch ON the routing rule; rule is now activated in the ARM.

13. In the Web interface, delete the routing rule. The transition is now complete.

14. Perform a Test Route (see Section 6.3 for detailed information).

15. Make a call and make sure it was established by the ARM.
Configure manually using the ini file, or in the Web interface’s ‘Admin’ page, configure ‘SendAcSessionIDHeader’ = 1 for the SBC/Gateway to preserve the Call ID when a call passes through multiple SBCs/Gateways.

Note: See also Appendix A.
8.6 Migrating Media Gateway Routing to the ARM

After making sure that the device (the gateway in this case) is connected to all HTTP ARM services i.e., ARM Topology Server and router/s, you can begin to migrate the routing rules from those defined in the Web interface to the ARM. Screenshots are for illustrative purposes.

**Note:** 'Trunk Group' and 'IP Group' in the Web are called 'Peer Connection' in the ARM.

- **To migrate gateway routing rules to the ARM:**
  1. In the Web interface, navigate to the Routing Settings page, and set the parameter 'Gateway Routing Server' to **Enable**.

     ![Figure 8-14: Web Interface - Routing Settings Page](image)

  2. Navigate in the Web interface to the IP Groups page.
  3. Locate the IP Group to expose the enterprise network to the ARM environment.
  4. [Mandatory] Enter a unique name for the IP Group as shown in the figure below.
  5. Set the 'Used By Routing Server' parameter to **Used** as shown in the figure below, and then click **Apply**.

     ![Figure 8-15: Web Interface - IP Groups Page](image)

  6. Navigate to the Trunk Group Settings page (**Setup > Signaling & Media > Gateway > Trunk Group Settings**) shown in Figure 8-16.
7. Locate the Trunk Group to expose the enterprise network to the ARM environment.
8. [Mandatory] Enter a unique name for the Trunk Group.
9. Set the 'Used By Routing Server' parameter to **Used**, and then click **Apply**.

![Figure 8-16: Web Interface - Trunk Group Settings](image)

10. In the ARM GUI, make sure the device is displayed in the Network page, Map view. Make sure the Peer Connection you configured is displayed. Unlock it and make sure its color is green.

**Note:** After viewing the trunk group or IP Group in the ARM, it is strongly recommended not to change its unique name. Changing its unique name will prevent routing by the ARM of calls to this Peer Connection (trunk / IP group) and receipt by the ARM of calls from this Peer Connection (trunk / IP group).

At this point, your routing service will still be operating according to that defined in the Tel-to-IP Routing and IP-to-Tel Routing pages in the gateway's Web interface.

11. In the ARM GUI's Routing page, configure a rule parallel to one of the rules configured in the Web interface's Tel-to-IP Routing or IP-to-Tel Routing pages.
12. Unlock the configured gateway Routing Rule in the ARM and check using the Test Route feature that the rules are functioning as required.
13. Delete the parallel rules configured in the Web interface's Tel-to-IP Routing or IP-to-Tel Routing pages.
8.7 **Migrating Hybrid Routing to the ARM**

After making sure that the hybrid device is connected to all HTTP ARM services i.e., ARM Topology Server and router/s, you can begin to migrate the routing rules from those defined in the Web interface to the ARM.

➢ **To migrate hybrid routing rules to the ARM:**

1. Perform migration of the SBC according to the instructions in Section 8.5.
2. Perform migration of the Media Gateway according to the instructions in Section 8.6.
3. Open the hybrid device's Web interface.
4. Create an IP Group (Peer Connection) for the SBC application:
   a. Open the Proxy Sets page (Setup > Signaling & Media > Core Entities > Proxy Sets) and then add a Proxy Set for the SBC application:

   ![Figure 8-17: Add Proxy Set – for SBC](image)

   b. From the 'SBC IPv4 SIP Interface' dropdown, select **SBC SIP Interface** and then click **Apply**; the Proxy Sets page opens showing the list of proxy sets, including the proxy set you added.

   ![Figure 8-18: Proxy Sets](image)

5. From the Proxy Sets list shown in the figure above, select the proxy set you added and then click the **Proxy Address** link.
Figure 8-19: Add New Proxy Address

![Image of Add New Proxy Address]

a. Enter the Proxy IP Address in the format `<IPAddress>:Port`. This address must point to the Gateway SIP interface address so a loop between the SBC SIP application and the Gateway SIP application is created.

b. Open the IP Groups page (Setup > Signaling & Media > IP Groups), add an IP Group (click New) and associate it with the Proxy Set you added in Step 4a:

Figure 8-20: IP Group for the SBC Application

6. Create an IP Group (Peer Connection) for the Media Gateway application:

a. Open the Proxy Sets page (Setup > Signaling & Media > Core Entities > Proxy Sets) and then add a Proxy Set (click New) for the Media Gateway application:

Figure 8-21: New Proxy Set for Media Gateway Application

b. Select **Gateway SIP Interface** from the ‘Gateway IPv4 SIP Interface’ dropdown and then click **Apply**; the Proxy Sets page opens showing the list of proxy sets, including the proxy set you added.
7. From the Proxy Sets list shown in the figure above, select the proxy set you added and then click the Proxy Address link.

8. Click Apply. Check in the ARM that calls can be routed to and from the hybrid device.
This page is intentionally left blank.
A Checklist for Migrating SBC Routing to the ARM

Administrators can use the checklist shown in the table below when migrating SBC routing to the ARM. Tick off the items in the list as you proceed.

Note: The screenshots shown in this section are of Web interface version 7.2. If you’re using Web interface version 7.0 or earlier, refer to earlier versions of this document.

Table A-1: SBC Migration Checklist

<table>
<thead>
<tr>
<th>Item</th>
<th>SBC-Level</th>
<th>What should be viewed in the ARM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure the SBC in the way you used to, including all the IP Groups for connectivity with external SIP trunks and PBXs.</td>
<td>Unrelated to ARM</td>
</tr>
<tr>
<td>2</td>
<td>Configure the IP address of the ARM’s ‘Configurator’&lt;br&gt;Note: Do not configure Routers independently. Only configure ‘Configurator’ IP address and credentials:&lt;br&gt;  - Configure in the SBC’s Web interface (Setup &gt; IP Network &gt; Web Services &gt; Remote Web Services):&lt;br&gt;    ✓ IP address of the Configurator&lt;br&gt;    ✓ User name and Password for connecting to the Configurator.&lt;br&gt;    Default: Admin/Admin</td>
<td>View the new Node. Make sure it becomes green-coded, indicating that it’s available.</td>
</tr>
</tbody>
</table>

- Make sure the status of each ARM service is ‘Connected’.
<table>
<thead>
<tr>
<th>Item</th>
<th>SBC-Level</th>
<th>What should be viewed in the ARM</th>
</tr>
</thead>
</table>
| 3    | Choose the SIP interfaces you want to use in the ARM (for ARM Peer Connections and ARM Connections) to be 'Used By Routing Server'.  
   • Open the SBC Web interface (Setup > Signaling & Media > Core Entities > SIP Interfaces)  
   ![General Interface](image) | You're able to select the chosen SIP Interfaces as ARM 'Routing Interfaces' for ARM Connections between the Nodes (SBCs) |
| 4    | Select each IP Group you want to use in the ARM as a Peer Connection for routing, to be **Used By Routing Server**. These should be, for example, SIP trunks and connections to IP PBXs.  
   • Open the IP Groups page (Setup > Signaling & Media > Core Entities > IP Groups).  
   ![General Interface](image) | View the selected IP Groups as ARM Peer Connections and attached VoIP Peers. View their availability status (green/red). In the ARM, unlock these Peer connections. |
### Item | SBC-Level | What should be viewed in the ARM
---|---|---
5 | At this stage, the ARM does not route calls, though you can apply a ‘test route’ at the ARM level. The Node (SBC) does not send a routing request to the ARM after a SIP invite. | In the ARM you can now:
- View and create ARM topology (connections between the Nodes)
- Add ARM routing groups and Routing rules, manipulation groups, etc.
- Test yourself using the ARM’s ‘test route’

6 | Command the SBC to route calls using the ARM:
- Open the SBC Web interface IP-to-IP Routing (Setup > Signaling & Media > SBC > IP-to-IP Routing).
- Make sure the rule that routes all INVITE requests to the ARM is configured. The following parameters are mandatory: ‘Request Type’ = INVITE; ‘Destination Type’ = Routing Server. | Calls are now routed by the ARM:
- SBC gets an INVITE
- Sends routing Request to ARM
- Get reply from ARM
- Sends INVITE further according to the ARM’s instructions

7 | Configure manually using the ini file (or in the ‘Admin’ Web interface page): `SendAcSessionIDHeader = 1` | Causes the SBC to preserve Call ID when a call passes through several SBCs.
This page is intentionally left blank.
## B Prefixes

The table below describes the prefixes rules.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>[n-m]</td>
<td>Represents a range of numbers. Note: numbers “n” and “m” should be of the same length.</td>
<td>[5551200-5551300]#: represents all numbers from 5551200 to 5551300. 123[100-200]: represents all numbers from 123100 to 123200.</td>
</tr>
<tr>
<td>[n,m,...] or n,m,l, ...</td>
<td>Represents multiple numbers or strings.</td>
<td>[2,3,4,5,6]#: represents a one-digit number starting with 2, 3, 4, 5, or 6. [11,22,33]XXX#: represents a five-digit number that starts with 11, 22, or 33. [111,222]XXX#: represents a six-digit number that starts with 111 or 222. [2X,3X,4X,50,54]XXXXXX#: represents an 8-digit number starting with 2, 3, 4, 50 or 54. aaa,bbb,ce,field: represents names that start with one of the strings: aaa, bbb, ce or field.</td>
</tr>
<tr>
<td>[n1-m1,n2-m2, a,b,c,n3-m3]</td>
<td>Represents a mixed notation of multiple ranges and single numbers.</td>
<td>[123-130,455,766,780-790]: represents numbers 123 to 130, 455, 766, and 780 to 790.</td>
</tr>
<tr>
<td>X (capital only)</td>
<td>Represents any single digit or character.</td>
<td>BobX: represents names starting with bob1 or <a href="mailto:bob2@audiocodes.com">bob2@audiocodes.com</a>. AliceX#: represents names of 6 characters length, starting with Alice such as Alice1.</td>
</tr>
<tr>
<td>Pound sign (#) at the end of a number</td>
<td>Represents the end of a number.</td>
<td>54324XX#: represents a 7-digit number that starts with 54324.</td>
</tr>
<tr>
<td>Empty</td>
<td>Represents any number or string</td>
<td></td>
</tr>
</tbody>
</table>
This page is intentionally left blank.
C Examples of Normalization Rules

This appendix shows examples of Normalization Rules and regular expressions.

- Remove any non-number text from the prefix of the number:

  Group Name: remove text from # prefix

  Manipulation Rules:
  
  `[^0-9]+`

  replace by: 

  Simulation Result: +9723456789

- Strip the + from the number:

  Group Name: Israel

  Manipulation Rules:
  
  \+972

  replace by: 972

  Simulation Result: +97239764263
Skype for Business: Remove "tel:" from the prefix and any text from the number’s suffix. In the Test field, the full number is tel:+97239762938 (ext:2938).

- If the fourth digit from the right is 4, change it to 8, and if the first digit is 0, change it to +972.

- Click OK and then click Submit.
D Call Routing

This appendix describes call routing.

- A routing request results in an HTTP error response if no routing is available.
- A routing request from a source node which has an alternate route option returns the next alternate route option. The call route is not recalculated. If the alternate route list is empty, a 404 result is returned.
- A routing request from a node which is not the source node returns the next hop in the routing chain according to the original route selection. The routing logic is not performed again.
This page is intentionally left blank.
E Configuring the SBC to Send SIP Requests other than INVITE to the ARM

This appendix shows how to configure the SBC to send MESSAGE and NOTIFY SIP requests to the ARM. To get not only INVITE but also NOTIFY and MESSAGE, create a new Condition in the Condition table with the value: "header.request-uri.methodtype == '5' or header.request-uri.methodtype == '13' or header.request-uri.methodtype == '14'".

To configure the SBC to send SIP Requests other than INVITE to the ARM:

1. Open the Message Conditions page (Setup > Signaling & Media > Message Manipulation > Message Conditions) and click Add.

2. Add the condition as shown in the figure above, and click Apply.

3. Open the IP-to-IP Routing page (Setup > Signaling & Media > SBC > Routing > IP-to-IP Routing), select the row of the Routing Rule that directs calls to the ARM, and click Edit.

4. Edit the Routing Rule (see the figure above):
   - Change 'Request Type' from Invite to All.
   - Select the 'Message Condition' you configured.

5. Click Apply.

6. Make a call and make sure the call was established by the ARM.

Configure manually using the ini file, or in the Web interface's 'Admin' page, configure 'SendAcSessionIDHeader' = 1. Note that this step is temporary and that a permanent solution is pending. It causes the SBC/Gateway to preserve Call ID when a call passes through several SBC/Gateways.