Wave SIP Trunk Configuration Guide

FOR BROADVOX

Last updated 1/7/2014

Contents

Overview

This guide describes how to configure SIP trunks on the Wave Server when you are using SIP trunking from Broadvox LLC.

Throughout this guide, “your ITSP” refers specifically and only to Broadvox.

SIP trunk configuration consists of the following tasks:

- Enable SIP trunking on the Wave Server.
- Create a new signaling control point (SCP) for your ITSP.
- Configure bandwidth management zones.
- Configure outbound routing for SIP calls.
- Allocate VoIP resources.

Optional configuration tasks include:

- Set up emergency 911 service.
- Configure a backup proxy server to maintain SIP trunk service if the primary SIP proxy server fails, your ITSP has provided you with backup proxy server configuration information.

Special Notes

Wave Software Version 4.0

- Does not support RTCP.
- Codec support: The system is configured for G.729 and G.711 codecs, with G.729 being the top Priority codec. However reINVITEs from Wave contain G711 as the top priority codec. Issue resolve when hotfixes No 18, 22 & 23 are applied.
- Diversion header is not supported (in Call forwarding scenarios).
- Off net blind transfer - No Ringback tone to external caller (Ref JIRA TM-10/12)
- Fax (G711 and T.38): This configuration does NOT support fax, for workarounds use Analog/T1/ISDN trunks or see Wave Manuals for more information.
- Backup proxy server configuration not supported (page 12/20) (Ref JIRA TM-125), for workaround setup backup SCP & backup secondary outbound routing table.

Before you begin

Required SIP trunk provisioning and configuration information

Before you begin, make sure that you have obtained the following information from your ITSP:

- **Proxy server information:**

  Registrar Server: nd01-03.fs.broadvox.net
  Proxy Server: nd01-03.fs.broadvox.net

  Outbound proxy1 ____

Outbound proxy2 ____

- **Pilot Identity Bulk Registration Credentials:**

  Username ____

  Password ____

- **SIP Domain Name:**

  ____

- **SIP codec to use:**

  ____

- **DID phone numbers:**

  ____

  ____

- **Technical support contact information**

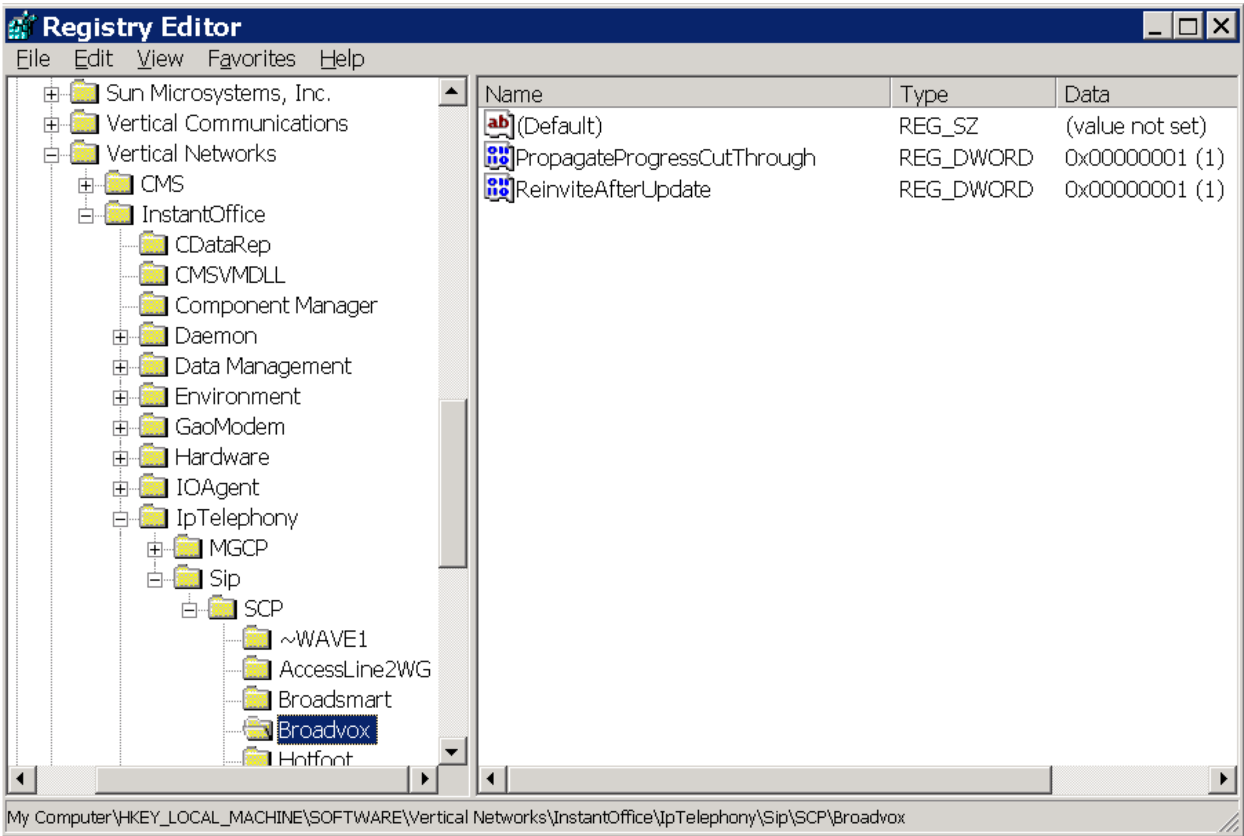
  ____

Wave Server requirements

- **Wave ISM version:** Verify that the Wave Server is running one of following versions :
  - Wave 4.0 base version
  - Wave 3.0 + Feature Pack 1 or higher
  - Wave ISM 2.5 + HotFix 16 or higher
  - Wave ISM 2.0 Service Pack 1 + HotFix 24 or higher
- **Wave licensing:** Add the following Wave licenses, in addition to any other Wave licenses required to support your configuration:
  - **Wave IP User license**. Depending on the IP phones that you use, you will need one or more of the following types of licenses:
    - **Wave IP User – Edge IP and ViewPoint Phone license:** For Edge 5000-series IP phones or the ViewPoint Softphone.
    - **Wave IP User – Certified Third Party IP Phone license:** For supported Aastra or Edge 1500-series IP phones
    - **Wave IP User – Generic Third Party IP Phone:** For third-party IP phones.
  - **Wave SIP Trunk license**

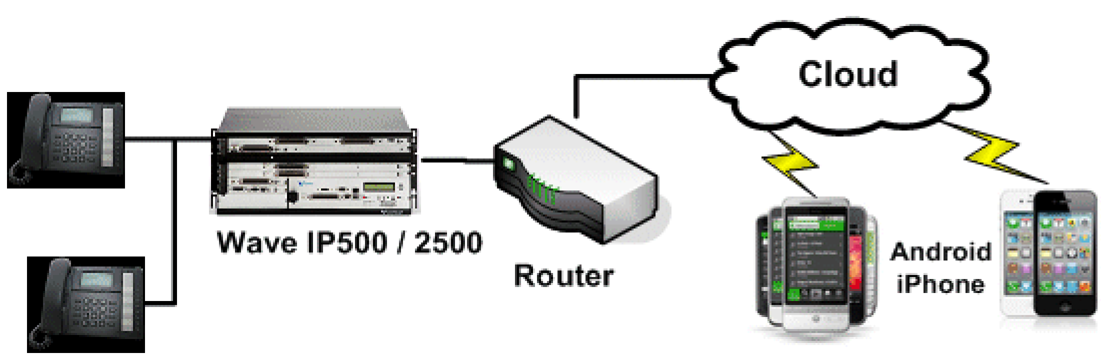
- **Wave IP Gateway license**

- **Registry:** Add setting the ReinviteAfterUpdate Registry setting to 1 HKEY_LOCAL_MACHINE\SOFTWARE\Vertical Networks\InstantOffice\IpTelephony\Sip\SCP\scpname



Router requirements

You can use any NAT router with a DMZ option as a default gateway for Wave and all IP phones. Wave registers with your ITSP and handles all inbound and outbound calls over the SIP trunks.



The following information assumes that you are using a Linksys RV042 router. If you are using a different router, equivalent configuration settings should be available.

- **Network settings:**

LAN IP:	IP address ON of router (LAN)
WAN IP:	IP address ON of router WAN I/f
DMZ IP:	0.0.0.0
Mode:	Gateway
DNS:	Provided by your ISP or ITSP
DDNS:	OFF
DMZ Host:	Wave IP address

- **Firewall settings:**

SPI (Stateful Packet Inspection):	ON
DoS (Denial of Service):	ON
Block WAN Request:	ON

- **VPN settings:**

Tunnel(s) Used:	0
Tunnel(s) Available:	50

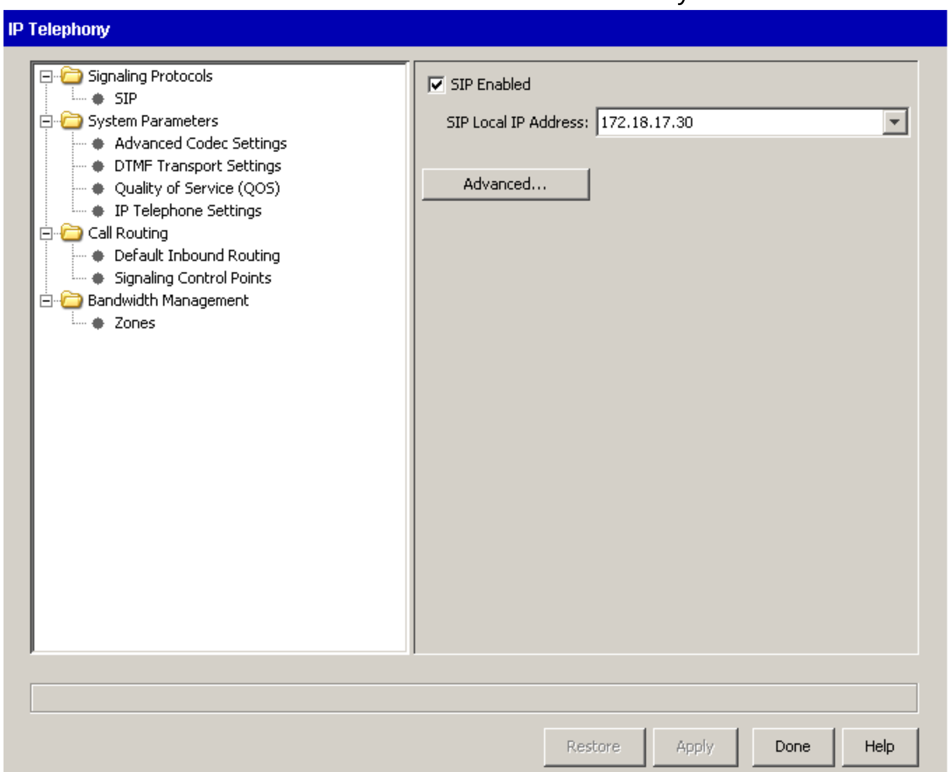
No VPN Group is defined.

Configuring SIP trunks for Broadvox

The steps and screenshots in this guide reflect the configuration process on a Wave 4.0 Server. Since the Wave user interface has been modified over time, if you are configuring SIP trunking on an earlier version of Wave, if necessary see Chapter 6 in the *Wave Global Administrator Guide* for that version for specific details.

Enabling SIP trunking on the Wave Server

1. Start the Wave Global Administrator Management Console. Click **IP Telephony**, located in the PBX Administration section.
2. Expand **Signaling Protocols** in the left pane and then click **SIP**. Select the **SIP Enabled** checkbox. **SIP Local IP Address** is selected automatically.



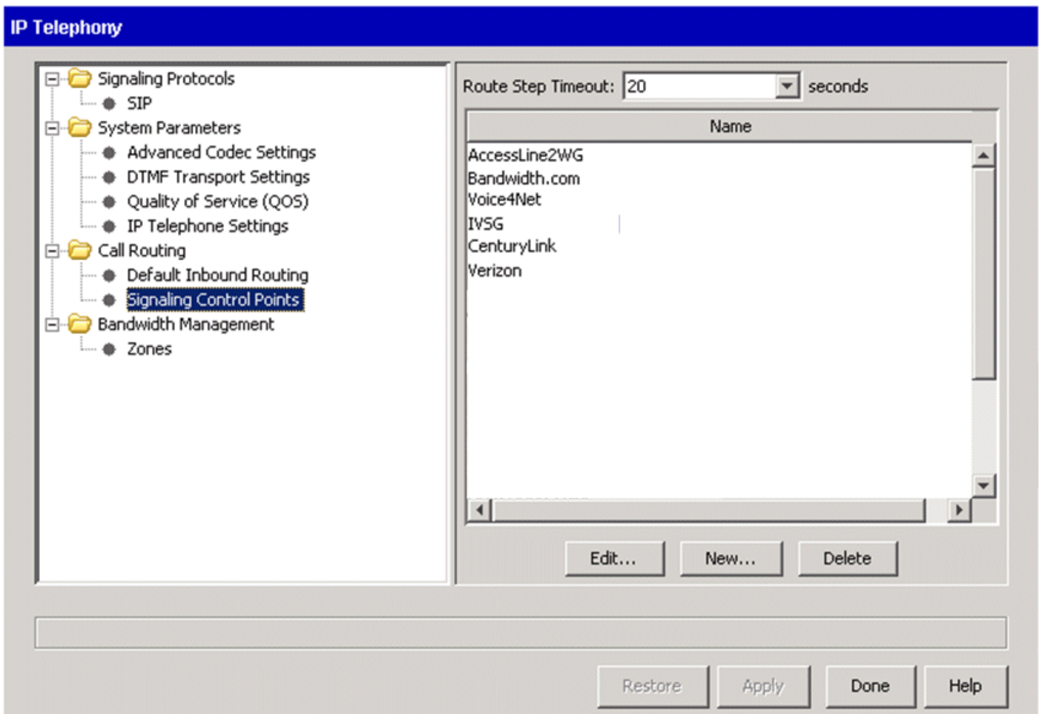
Creating a new signaling control point (SCP)

This section describes how to create a new SCP and then:

- Set up inbound routing.
- Add a rule to the inbound routing table.
- Set up Caller ID.
- Configure SIP settings.

Creating a new SCP and setting up inbound routing

1. Expand **Call Routing** in the left pane and choose **Signaling Control Points**.

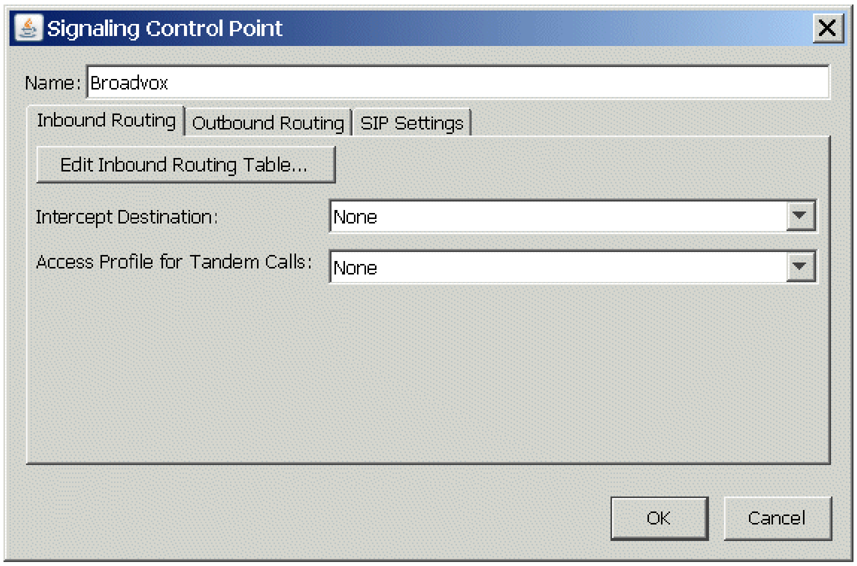


2. Click **New**.

3. In the Signaling Control Point dialog, enter a **Name** for the new SCP, for example “Broadvox”. (When you configure outbound call routing, this name will appear in the Routing Table as “IP”, a vertical bar (|), and the name you enter here, for example “IP|Broadvox”.)

   You can enter alphanumeric characters as well as the following special characters:

   ‘ ~ ! # $ % & * ( ) - = + | { } ; : “ , . / < > ?

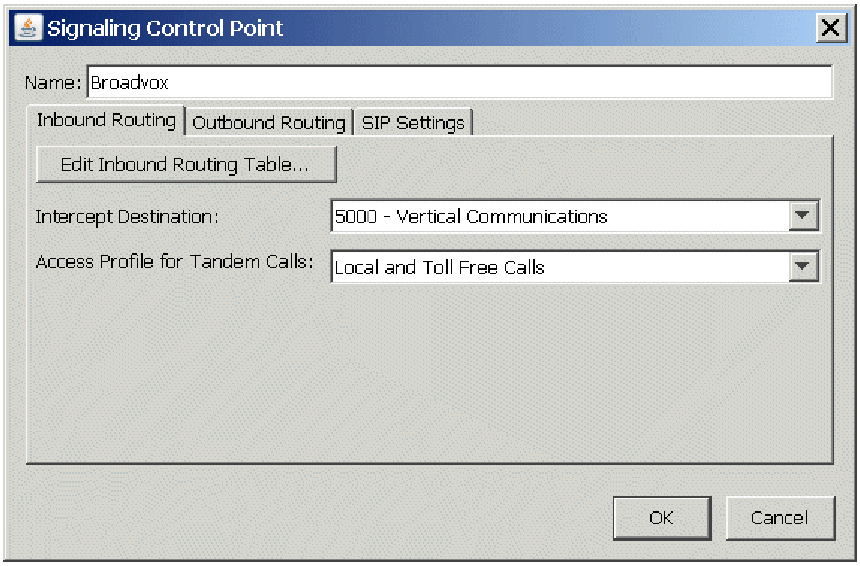


Setting up inbound routing for the new SCP

1. On the Inbound Routing tab, for **Intercept Destination**, select the extension from the drop-down list to which any incoming call from this SCP that is not matched in the Inbound Routing Table will be directed.
2. For **Access Profile for Tandem Calls**, select the access profile to apply to calls received from this SCP that will be connecting to another trunk. (Access profiles identify the different calling privileges that can be associated with SCPs, and can also be associated with extensions, trunk groups, and digital connections. For more information, see “Configuring specific access profiles” in Chapter 9 in the *Wave Global Administrator Guide*.)

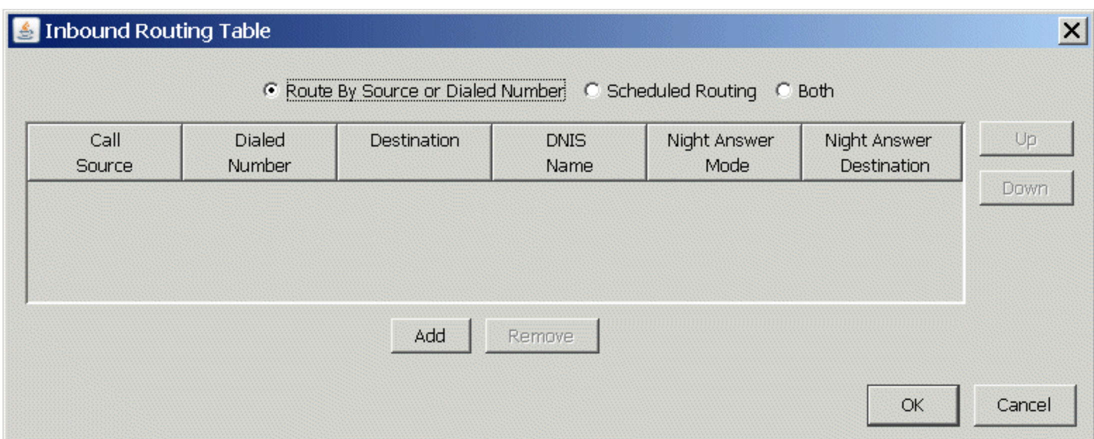
   If you are not sure which access profile to choose, you can select the “Unrestricted” profile.

   Warning! If you have not modified the default “Unrestricted” access profile, selecting “Unrestricted” here could leave your system vulnerable to hackers who are able to identify your Tandem Access Profile number.



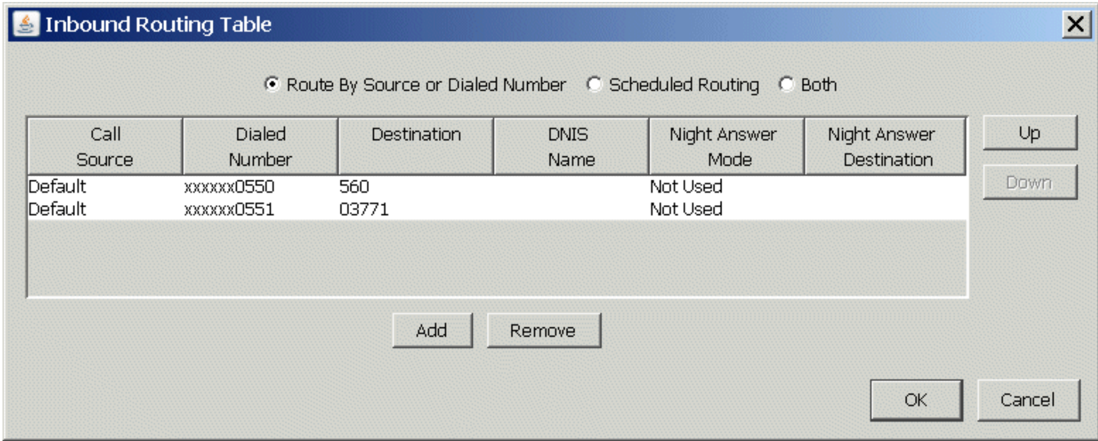
Adding a rule to the inbound routing table for the new SCP

1. Still on the Inbound Routing tab, click **Edit Inbound Routing Table**.
2. In the Inbound Routing Table dialog, verify that **Route By Source or Dialed Number** is selected. (This setting lets you decide how calls from this SCP get routed based on the DID digits the caller dialed.)



3. Click **Add** to add a new rule to the table for the DID numbers provided to you by your ITSP.
4. For each DID number, double-click in the following columns in the new rule:

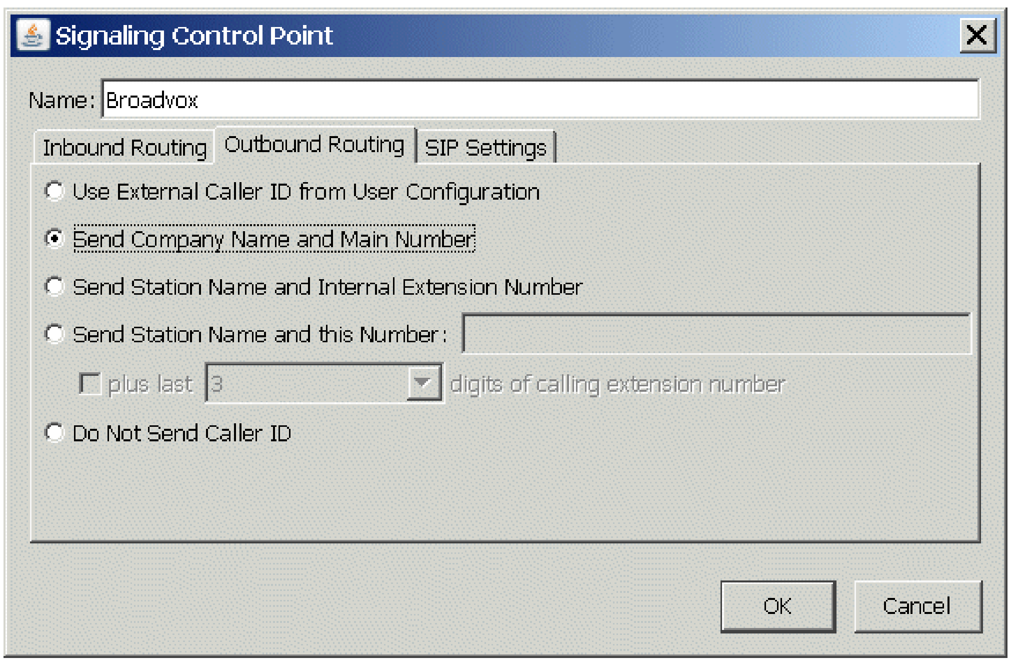
- For **Dialed Number**, enter one of the DID numbers provided by your ITSP. You can enter the entire 10-digit number, or use “x” characters as wildcards.
- For **Destination**, enter the extension or external phone number to which calls with this DID number will be routed. This number is interpreted as if dialed from an internal station, so for an external number, be sure to enter the external access digit as defined in the First Digit Table.



5. Click **OK** to save your changes to the Inbound Routing table.

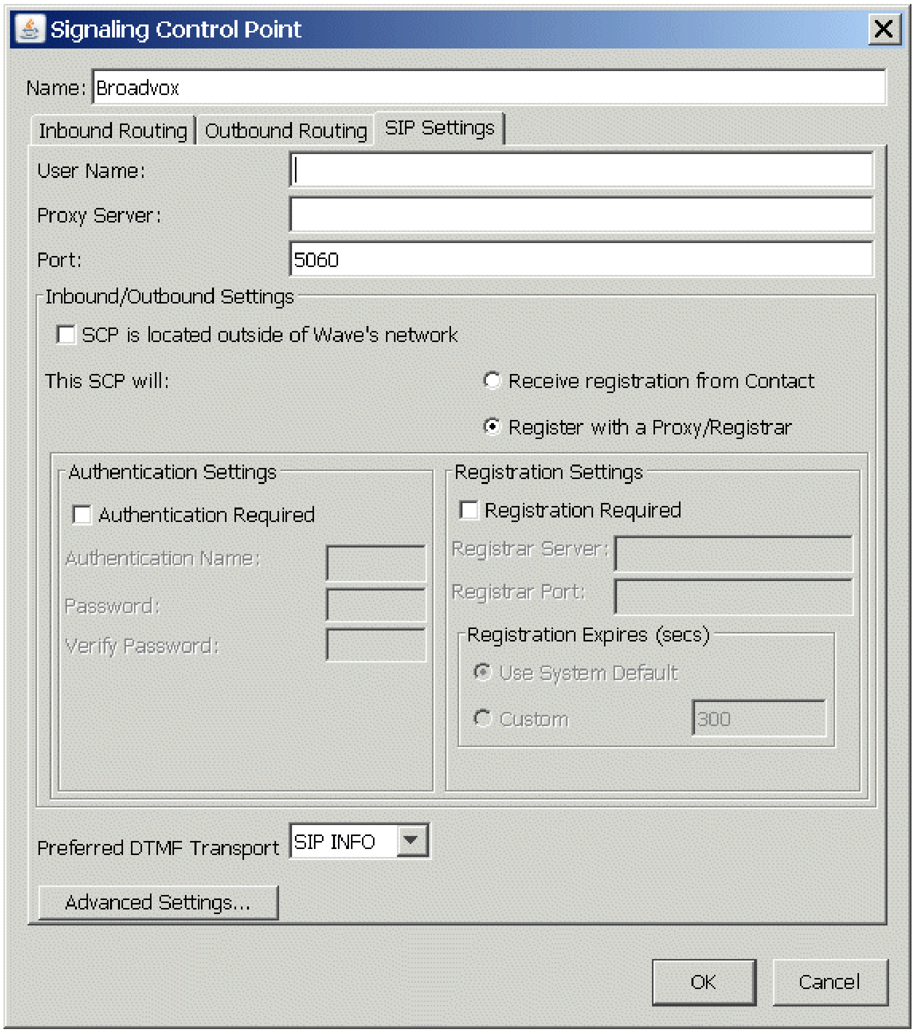
Setting up Caller ID for the new SCP

1. Still in the Signaling Control Point dialog, select the Outbound Routing tab.
2. Choose one of the Caller ID formats to send on outbound calls to this SCP. (Note that your ITSP may not support all of the listed formats.)



Configuring SIP settings for the new SCP

1. Still in the Signaling Control Point dialog, select the SIP Settings tab.



2. Enter the following information:

- For **User Name**, enter the main telephone number (also known as “Pilot Identity”) provided by your ITSP, for example “4084180145”.
- For **Proxy Server**, enter the DNS name or IP address of the proxy server provided by your ITSP.
- For **Port**, leave the default port number, “5060”.

3. In the Inbound/Outbound Settings section:

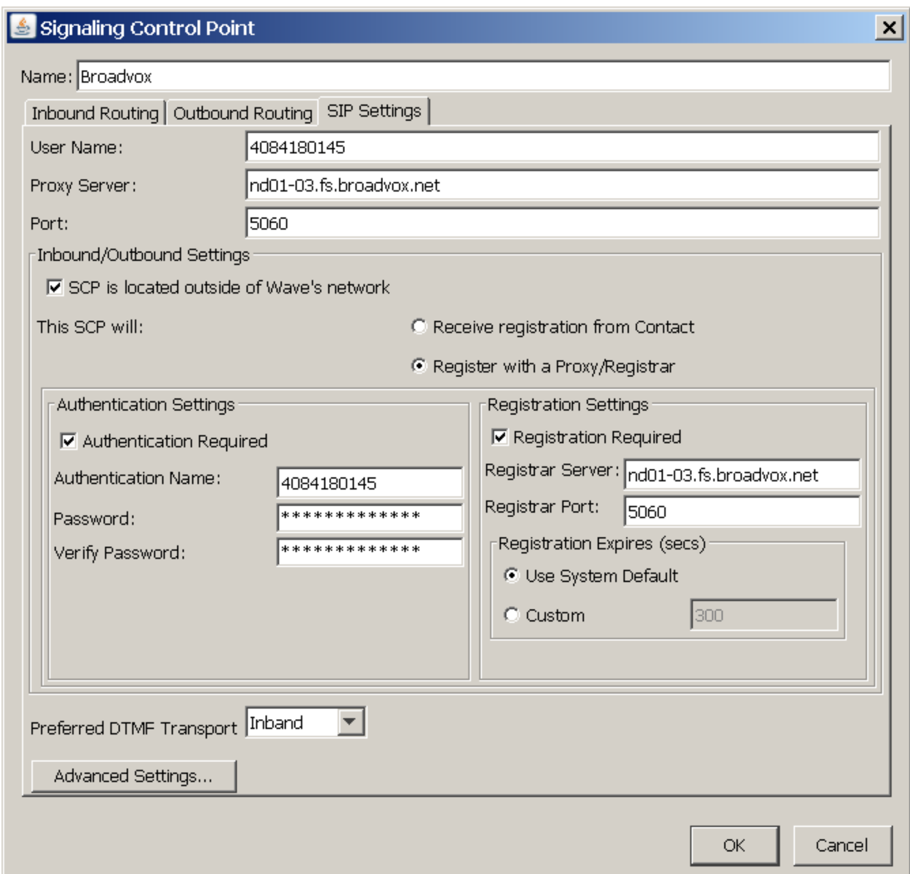
    - Select the **SCP is located outside of Wave's network** checkbox.
    - Select **Register with a Proxy/Registrar**.

4. In the Authentication Settings section:

    - Select the **Authentication Required** checkbox.
    - Enter the **Authentication Name** and **Password** provided by your ITSP.

5. In the Registration Settings section:

    - Select the **Registration Required** checkbox.
    - Enter the **Registrar Server** DNS name or IP address provided by your ITSP. (Typically, this is the same as the **Proxy Server** address that you entered above.)
    - For **Registrar Port** number, enter "5060".



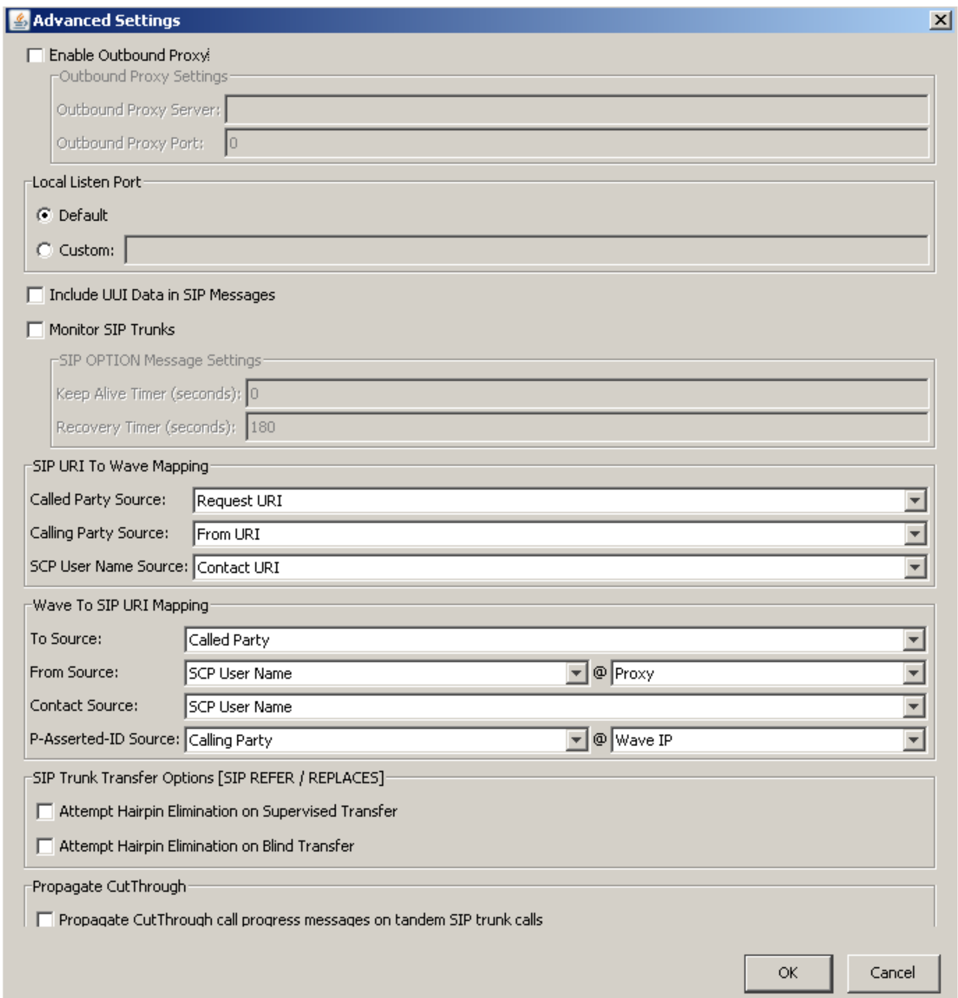
6. Click **Advanced Settings**.
7. If your ITSP has provided you with backup proxy server configuration information, do the following:

    - Select the **Enable Outbound Proxy** checkbox, and then enter the **Outbound Proxy Server** and **Outbound Proxy Server Port** (not supported Ref. JIRA TM-125).
    - Select the **Monitor SIP Trunks** checkbox, and then specify a **Keep Alive Timer** and **Recovery Timer** value in seconds.

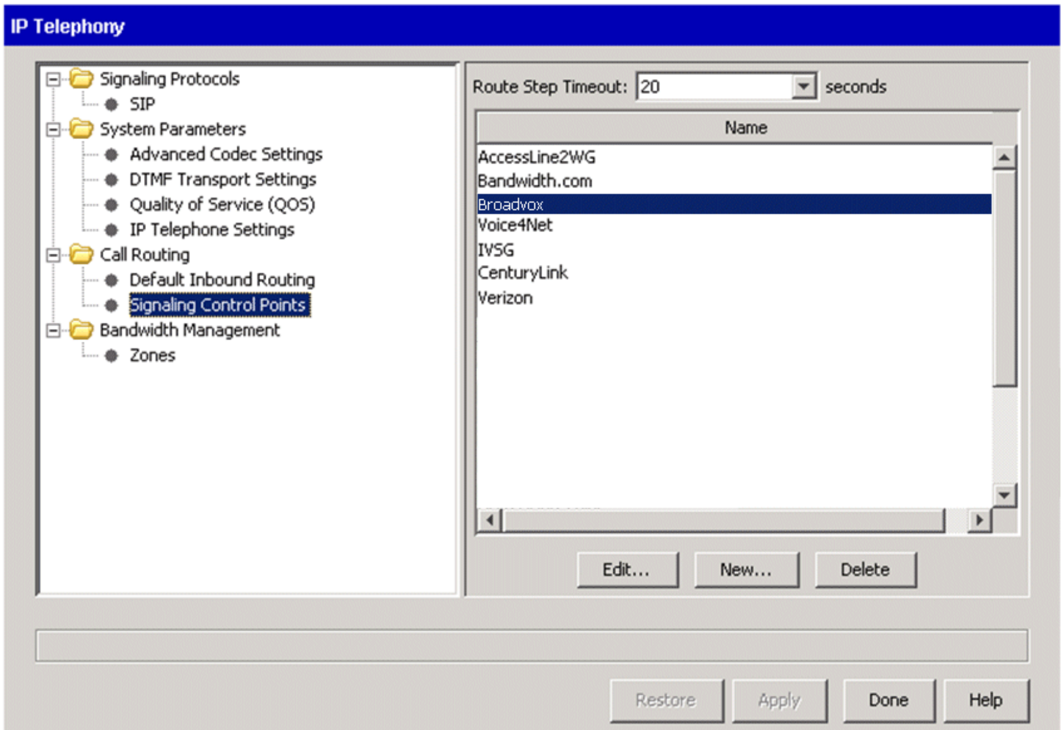
    For more about using a backup proxy server, including an additional required configuration step, see “Configuring a backup proxy server” on page 20.

8. In the SIP Trunk Transfer Options section, deselect both of the following:

    - **Attempt Hairpin Elimination on Supervised Transfer**
    - **Attempt Hairpin Elimination on Blind Transfer**



9. Leave all other advanced settings at their default values, unless instructed otherwise by your Wave provider. Click **OK** to save your changes, and exit the Signaling Control Point dialog.
10. Back on the main IP Telephony screen, select the new SCP and change the **Route Step Timeout** (at the top of the screen) to 20 seconds. This setting adjusts the amount of time that the system waits on this SCP before trying the next step in the outbound routing table, to allow for network or other delays.

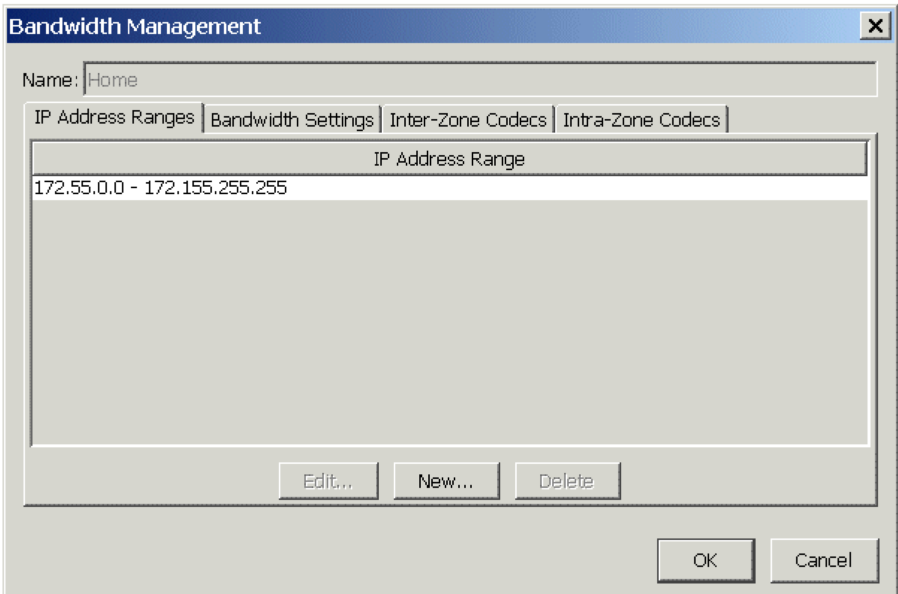


11. Click **Apply** to save your changes. Do not exit IP Telephony yet.

Configuring bandwidth management zones

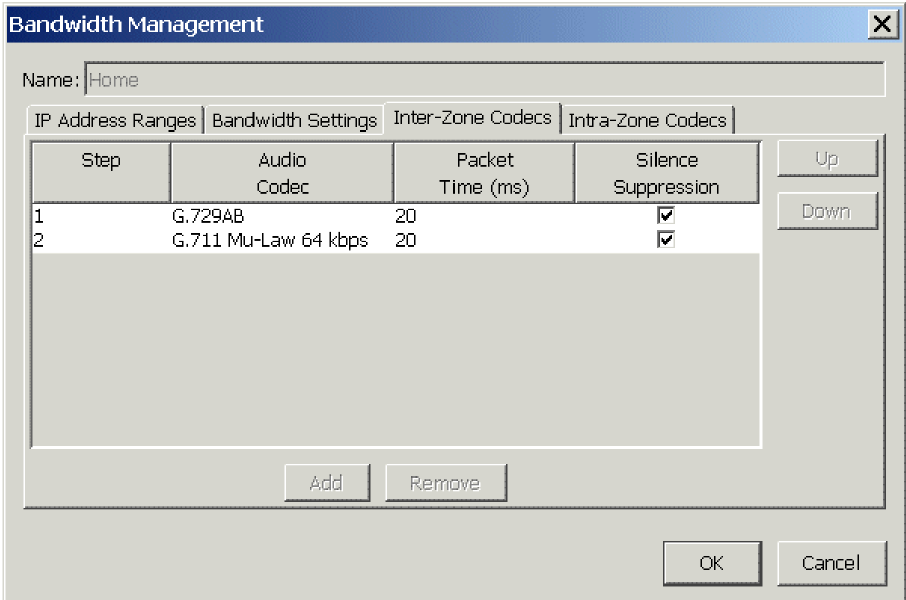
Configuring the Home zone

1. Expand **Bandwidth Management** in the left pane and click **Zones**.
2. In the **Zone Name** list, select "Home" and then click **Edit**.
3. In the Bandwidth Management dialog, select the IP Address Ranges tab.
4. Review the **IP Address Range** for the Home zone and make corrections if necessary. Leave all other values on this tab unchanged---these are expert settings that should not be modified unless you are instructed to do so by your Wave technical support representative.



5. On the Inter-Zone Codecs tab, do the following:

   - Make sure that the VoIP codec to use with your ITSP is in the Step 1 position. To change a codec's position in the list, select it and then click **Up** or **Down**.
   - Optionally, for each codec select the **Silence Suppression** checkbox.



6. On the Intra-Zone Codecs tab, make the same changes that you did in the previous step.
7. Click **OK** to save your changes, but don't exit IP Telephony yet.

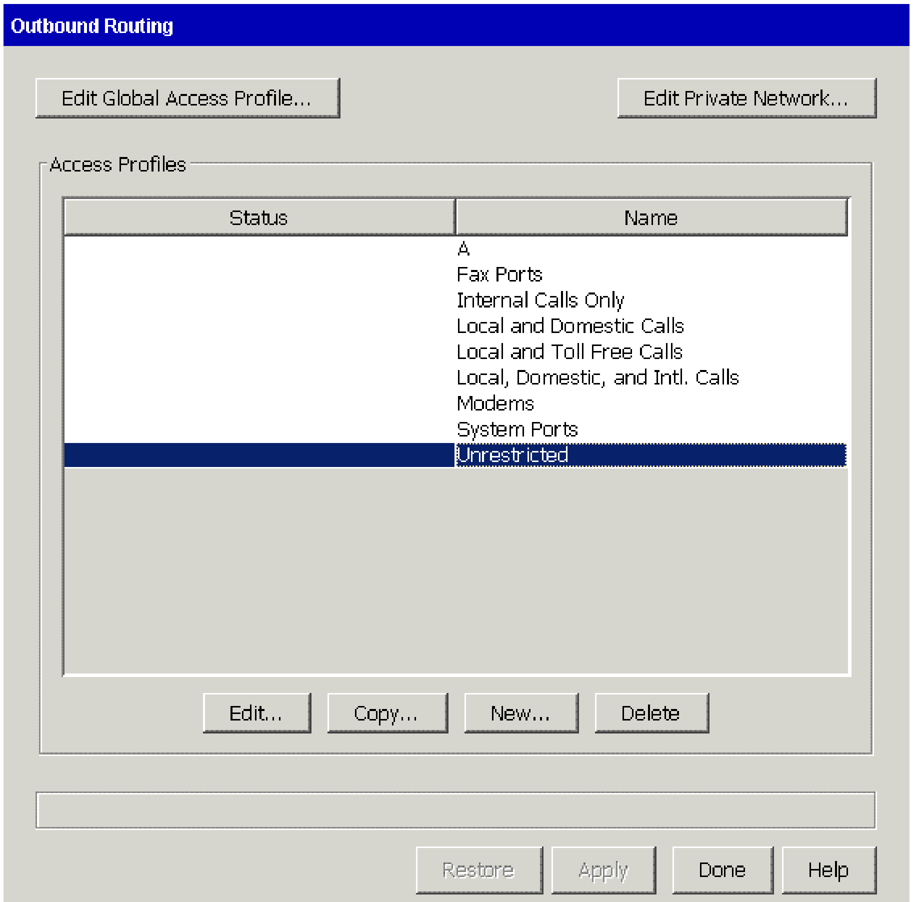
Configuring the Remote Default zone

All IP addresses outside of the Home zone are automatically in the Remote Default zone.

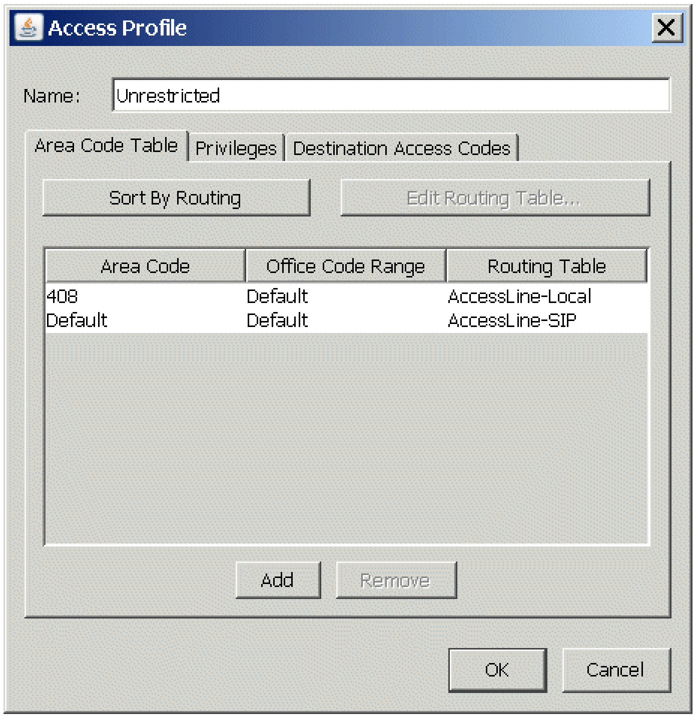
1. In the **Zone Name** list, select "Remote Default" and then click **Edit**.
2. On the Inter-Zone Codecs tab, do the following:
   - Make sure that the VoIP codec to use with your ITSP is in the Step 1 position. To change a codec's position in the list, select it and then click **Up** or **Down**.
   - Optionally, for each codec select the **Silence Suppression** checkbox.
3. On the Intra-Zone Codecs tab, make the same changes that you did in the previous step.
4. Click **OK** to exit the Bandwidth Management dialog.
5. Click **Apply** to apply all your changes, and then click **Done** to exit IP Telephony.

Configuring outbound routing for SIP calls

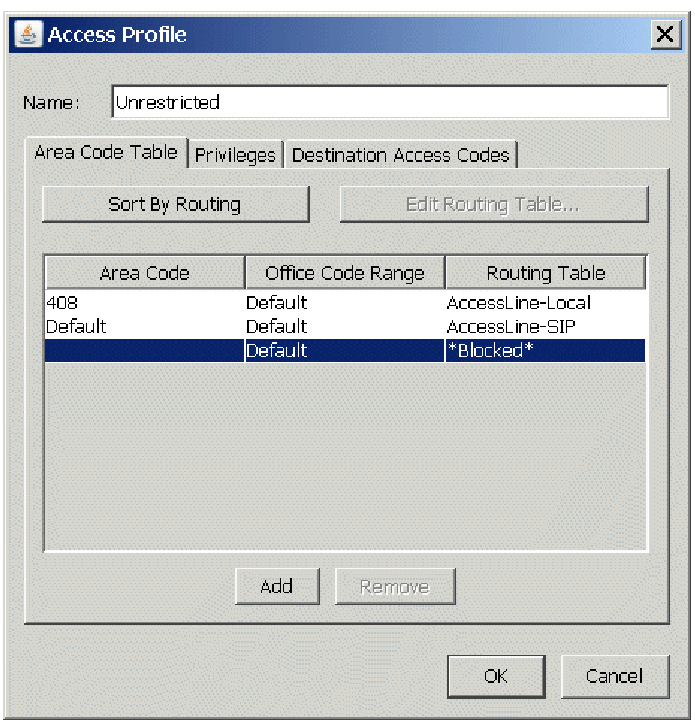
1. In the Global Administrator Management Console, click **Outbound Routing** in the Trunk Administration section.
2. In the Outbound Routing dialog, select the “Unrestricted” access profile and then click **Edit**.



3. The Access Profile dialog opens. On the Area Code Table tab, click **Add**.



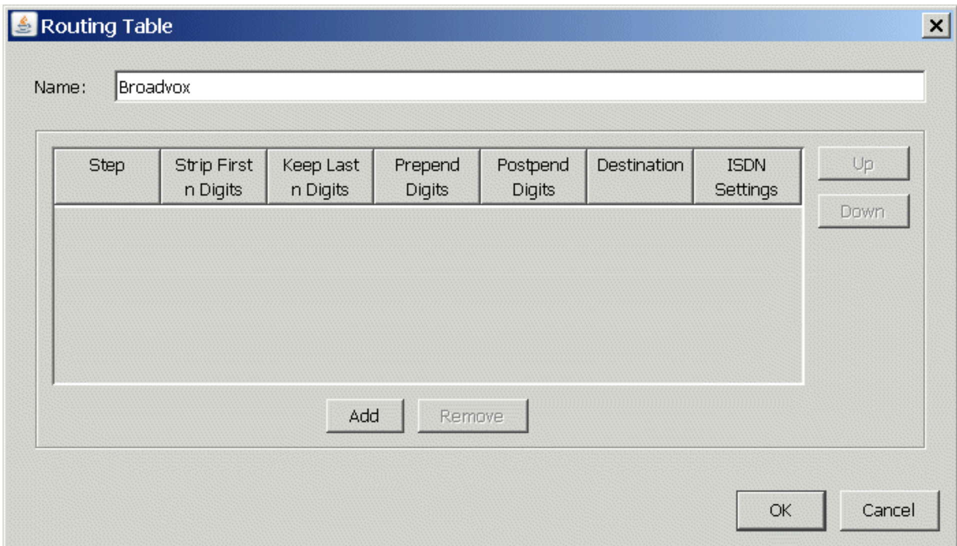
A new entry is added at the bottom of the Area Code list:



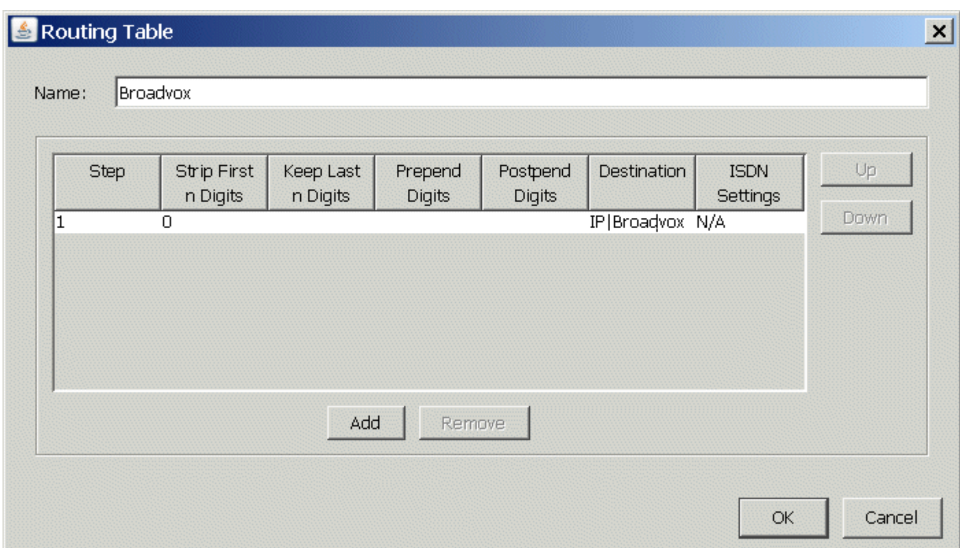
4. Double-click in the following columns:

- For **Area Code**, enter “Default”.
- Leave **Office Code Range** set to “Default”.
- For **Routing Table**, select “(New Routing Table)” from the drop-down list.

5. The Routing Table dialog opens. Enter a name for the new Routing Table entry, for example “Broadvox”.



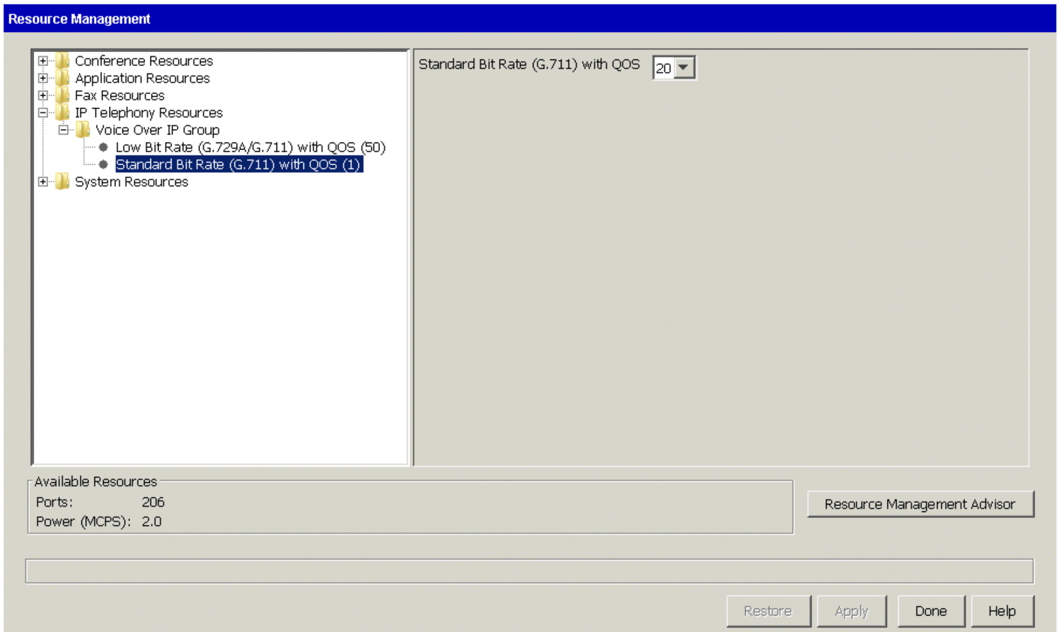
6. Click **Add** to add a new route.
7. Click in the **Destination** column and select “IP|Broadvox” from the drop-down list.



8. Leave all of the other default settings unchanged, and click **OK** to save the new route.
9. Click **Apply** to save your changes, and then click **Done** to exit Outbound Routing.

Allocating VoIP resources

1. In the Global Administrator Management Console, click **Resource Management**, located in the PBX Administration section.
2. Expand **IP Telephony Resources / Voice Over IP Group** in the left pane.
3. Select the appropriate **Low Bit Rate G.729A/G.711** or **Standard Bit Rate G.711** resource, and then allocate the number of VoIP resources to use by selecting a value from the drop-down list. (You only need to allocate VoIP resources to *one* codec.)



4. Click **Apply** to apply your changes, and then click **Done** to exit Resource Management.

This completes the SIP trunk configuration process. Contact your Wave provider if you have any further questions.

Making a test call

To verify that your SIP trunks are configured correctly:

- **Make an outbound call to an external number from a Wave phone,** answer the call and verify that there is a two-way voice path.
- **Make an inbound call to a DID number from outside the Wave network**, for example from a cell phone. Answer the call and verify that there is a two-way voice path.

Setting up emergency 911 service

Consult with your ITSP's technical support representative for detailed guidance on how to configure emergency 911 service. See "Setting up emergency dialing" in Chapter 9 in the *Wave Global Administrator Guide* for more information.

Important!

- Ensure that all employees, visitors, and any other people who may attempt to make an emergency call using a SIP trunk are aware of an alternate method to use to access emergency services in the event that VoIP service fails.
- If your specific configuration includes centralized trunking or multiple Wave Servers at different locations, it is imperative that emergency 911 calls are routed to the local public safety answering point (PSAP) that serves a specific caller's location.

Configuring a backup proxy server (not supported Ref. JIRA TM-125)

This section applies to you if your ITSP has provided you with backup proxy server configuration information.

When you configure and enable a backup proxy server, if the primary SIP proxy server fails, Wave will automatically switch to the backup proxy server to maintain SIP trunk service. When the primary SIP proxy server becomes available again, Wave will switch back automatically.

Backup proxy server configuration consists of the following tasks:

1. Configure and enable required settings when you create the SCP for your ITSP, as described in step 7 on page 12.
2. Edit the registry and add the following STRING registry value for the SCP you created for your ITSP:

   ```
   SOFTWARE\Vertical Networks\InstantOffice\IpTelephony\Sip\Scp\[SCP_NAME]
   \OutboundProxy2
   ```

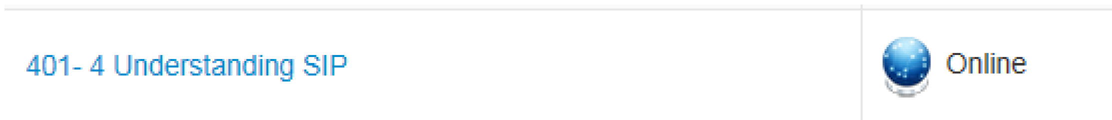
   For example:

   ```
   SOFTWARE\Vertical
   Networks\InstantOffice\IpTelephony\Sip\Scp\Broadvox\OutboundProxy2
   ```

   Set `OutboundProxy2` to the fully-qualified domain name of the backup proxy server as provided by your ITSP.

Troubleshooting

Please see Vertical University course:



This advanced course will be available after you pass Wave advanced instructor lead training.

This course has 3 modules;

- Introduction to SIP
- SIP Operation
- Troubleshooting SIP

For assistance please contact Vertical Technical Support at 1-877-Vertical. Prior to contacting Tech Support, please have available Wave Trace files, a Wireshark packet capture of the failure and a network diagram.