



## **Application Note**

### **Configuration Guide for ShoreTel and Ingate with PAETEC**

29 August 2008

# Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>2</b>	<b>PAETEC CONFIGURATION.....</b>	<b>2</b>
2.1	CPE REQUIREMENTS .....	2
2.2	PAETEC'S DYNAMIC IP SERVICE DEPLOYMENTS .....	2
2.2.1	MPLS – SIP Trunking Only .....	2
2.2.2	Both MLPS – SIP Trunking and Internet.....	3
<b>3</b>	<b>SHORETEL CONFIGURATION.....</b>	<b>4</b>
3.1	OVERVIEW .....	4
3.1.1	Version Support .....	4
3.1.2	ShoreTel Unsupported Features.....	4
3.2	SHORETEL CONFIGURATION.....	4
3.2.1	Call Control Settings .....	5
3.2.2	Sites Settings.....	7
3.2.3	Switch Settings - Allocating Ports .....	8
3.2.4	System Settings – Trunk Groups .....	9
3.2.5	System Settings – Individual Trunks .....	13
<b>4</b>	<b>INGATE CONFIGURATION.....</b>	<b>15</b>
4.1	ABOUT.....	15
4.1.1	Startup Tool.....	15
4.1.2	Web Admin.....	15
4.2	CONNECTING THE INGATE FIREWALL/SIPARATOR.....	16
4.3	USING THE STARTUP TOOL .....	18
4.3.1	Configure the Unit for the First Time .....	18
4.3.2	Change or Update Configuration.....	21
4.3.3	Network Topology.....	24
4.3.4	IP-PBX.....	29
4.3.5	ITSP.....	30
4.3.6	Upload Configuration.....	32
4.4	ADDITIONAL MANUAL PROGRAMMING .....	34
4.4.1	Ingate SIParator - LAN SIParator Deployment .....	34
4.4.2	Ingate Firewall Deployment .....	35
<b>5</b>	<b>TROUBLESHOOTING .....</b>	<b>36</b>
5.1	STARTUP TOOL TROUBLESHOOTING .....	36
5.1.1	Status Bar .....	36
5.1.2	Configure Unit for the First Time.....	36
5.1.3	Change or Update Configuration.....	37
5.1.4	Network Topology.....	38
5.1.5	IP-PBX.....	38
5.1.6	ITSP .....	39
5.1.7	Apply Configuration .....	39
5.2	INGATE WEB GUI CONFIG.....	40
5.2.1	Network – Network and Computers.....	40
5.2.2	Basic Configuration – SIParator Type (SIParator Only).....	40
5.2.3	SIP Service – Basic.....	41
5.2.4	SIP Service – Interoperability.....	41
5.2.5	SIP Traffic – Filtering .....	42
5.2.6	SIP Traffic – User Database.....	42
5.2.7	SIP Traffic – Routing .....	42
5.2.8	SIP Traffic – Dial Plan.....	43
5.3	USING THE INGATE FOR TROUBLESHOOTING .....	44
5.3.1	Troubleshooting Outbound Calls.....	44
5.3.2	Troubleshooting Inbound Calls .....	46

Tested versions:     Ingate Firewall/SIParator - Version 4.6.2  
                          Ingate Startup Tool – Version 2.4.0

Revision History:

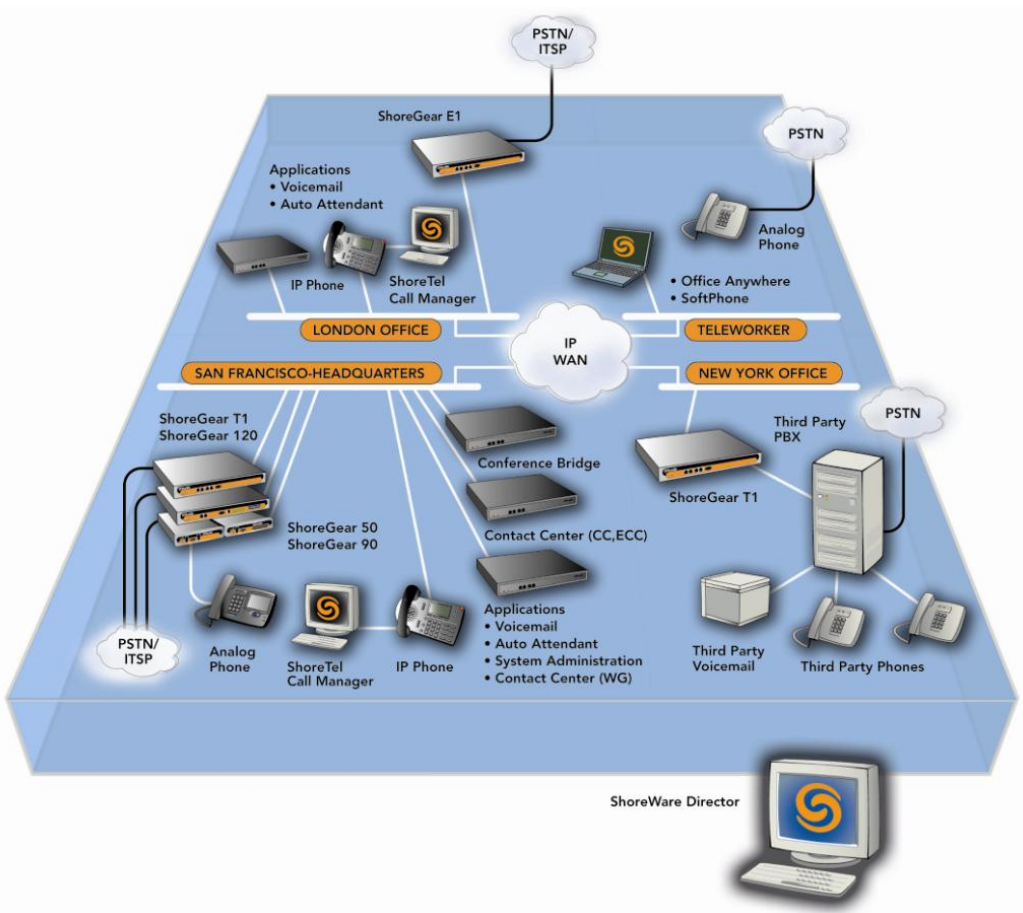
Revision	Date	Author	Comments
1	2008-08-29	Scott Beer	1 <sup>st</sup> Release

# 1 Introduction

This document provides details for connecting the ShoreTel® system through the Ingate SIParator® / Firewall to PAETEC (ITSP) for SIP Trunking to enable audio communications. The document focuses on the network architecture needed to set up these systems to interoperate.

ShoreTel and Ingate have teamed up to build a solid security focused solution, ShoreTel being the IP PBX which sits on the LAN and connects to the Ingate SIParator® or as an Ingate Firewall to provide Data and Voice security. Together providing a solution to allow customers the ability to connect to SIP Trunks offered by Paetec. As Paetec provide their MPLS service for SIP trunking, the Ingate then is connected to the LAN, providing the typical firewall security abilities but also intelligent SIP routing and such SIP features as:

- Registration
- Digest Authentication
- Dial Plan Modification
- Back to Back User Agent (Terminates SIP messaging on both LAN and WAN side)
- Transfer conversion of SIP REFER to SIP reINVITE messaging (critical)
- Quick configuration templates for each of the certified ITSPs



## 2 PAETEC Configuration

PAETEC's Dynamic IP Service, customer locations must reside in the on-net markets served by PAETEC. PAETEC's Dynamic IP Service is an ideal option for customers who want to leverage converged, dynamic IP voice and data services while continuing to utilize an IP telephony systems

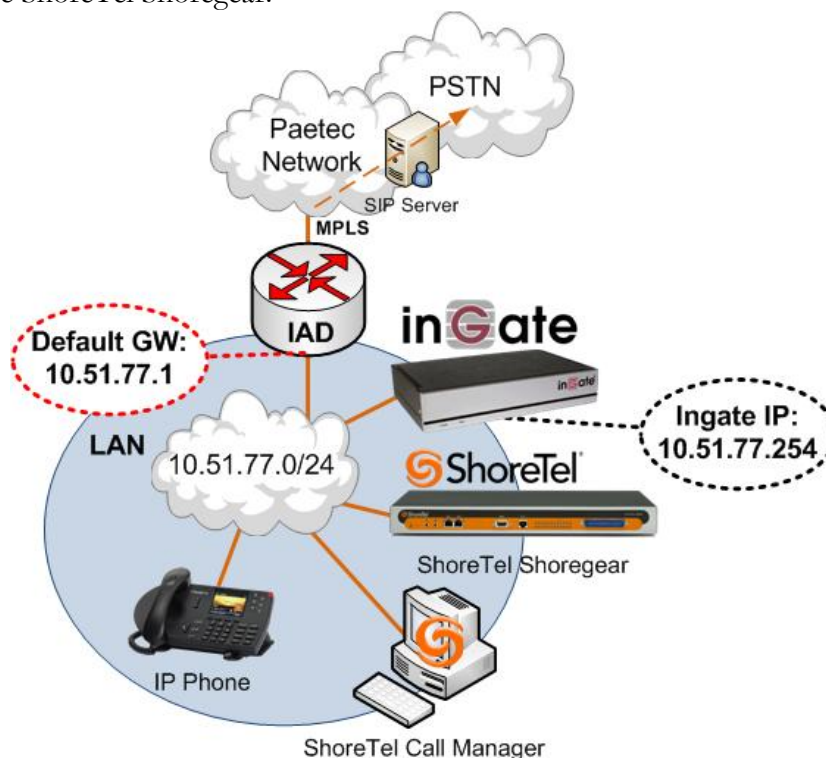
### 2.1 CPE Requirements

- PAETEC-certified Integrated Access Device (IAD) is required to integrate with traditional telephony systems.
- SIP-compliant CPE is required for IP telephony systems (the Ingate and ShoreTel).
- Location of Paetec SIP Server.

### 2.2 PAETEC's Dynamic IP Service Deployments

#### 2.2.1 MPLS – SIP Trunking Only

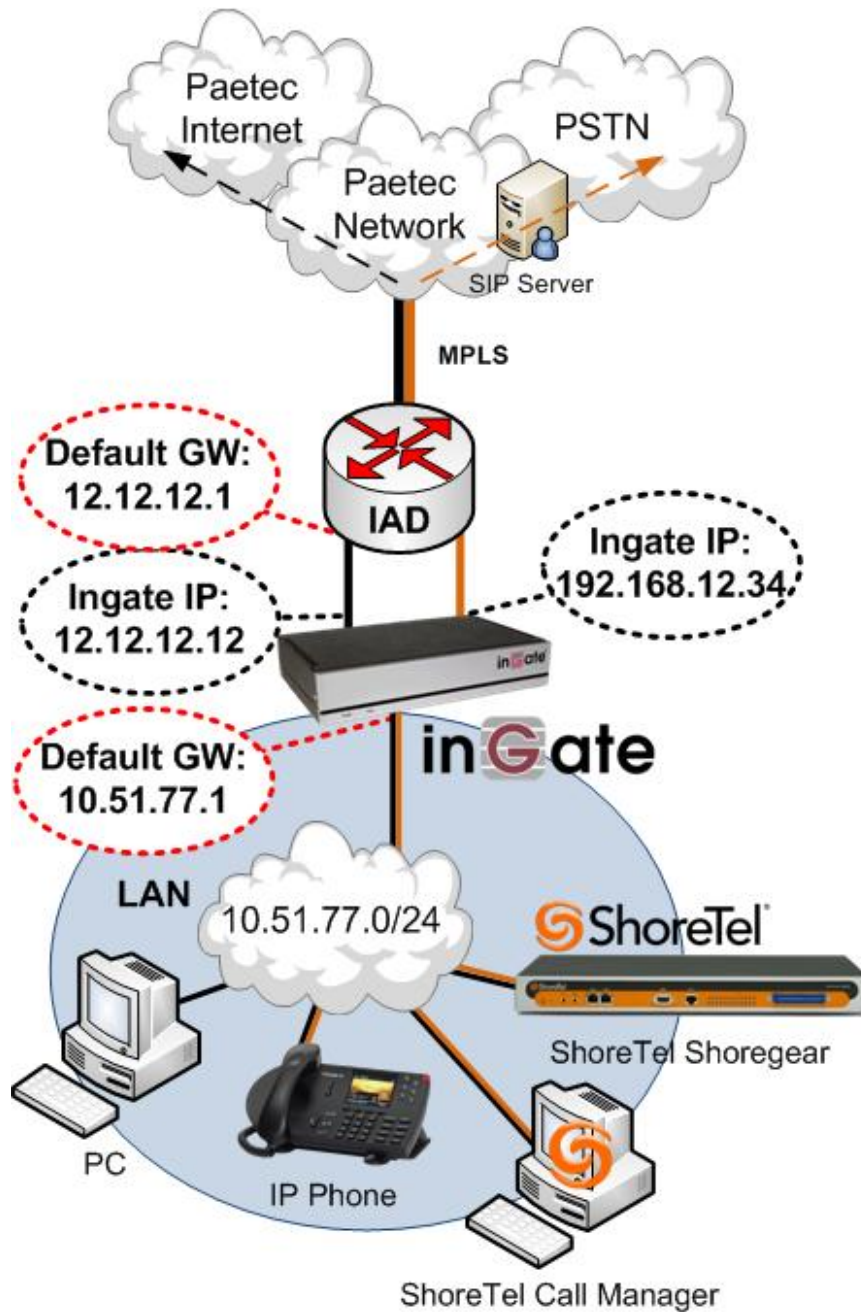
Here, Paetec is providing only the SIP Trunking services over MPLS. Internet is handled elsewhere. The Ingate is in a LAN SIParator type of deployment and is on the same LAN as the ShoreTel Shoregear.



**Note:** There is no Firewall in this scenario; Paetec is providing a private extension of their network directly to the CPE. Internet connectivity is handled elsewhere.

## 2.2.2 Both MLPS – SIP Trunking and Internet

Here, PEATEC is providing both Internet and SIP Trunking over the same MPLS link. The services are separated into two physical connections on the PEATEC IAD. One Ethernet connection for Internet services and the other connection can be used for the SIP Trunking services. The Ingate Firewall (product type: Firewall) can be used to provide security for the Data traffic security and Voice traffic security.



**Note:** The Ingate Firewall will only support one Default Gateway, in this scenario the Default Gateway is the way to the Internet. So the Default Gateway will be on Internet side of the IAD. A Static Route will have to be created for the SIP Server and Media Server should be defined on the second external interface.

### 3 ShoreTel Configuration

The configuration information below shows examples for configuring the ShoreTel, Ingate using Paetec. Even though configuration requirements can vary from setup to setup, the information provided in these steps, along with the Planning and Installation Guide and documentation provided by Ingate and Paetec, should prove to be sufficient. However every design can vary and some may require more planning than others.

#### 3.1 Overview

##### 3.1.1 Version Support

Products are certified via the Technology Partner Certification Process for the ShoreTel system. Table below contains the matrix of Ingate Firewall and Ingate SIParator versions firmware releases certified on the identified ShoreTel software releases.

**Ingate Firewall and Ingate SIParator version**

	4.5.1 with the patch ig-patch-4-5-1-shoretel-2 applied	4.5.2	4.6.0	4.6.1	4.6.2
ShoreTel 7.0	✓	✓	✓	✓	✓
ShoreTel 7.5	✓	✓	✓	✓	✓

##### 3.1.2 ShoreTel Unsupported Features

At the time of this writing, the following features are not supported, though support will be added in an upcoming future release:

- Fax redirect not supported today via SIP Trunks (though direct Direct Inward Dialing (DID) to fax endpoint is supported)
- Office Anywhere

#### 3.2 ShoreTel Configuration

This section describes the ShoreTel system configuration to support SIP Trunking. The section is divided into general system settings and trunk configurations (both group and individual) needed to support SIP Trunking.

**Note:** ShoreTel basically just points its Individual SIP Trunks to the Ingate SIParator.

The first settings to address within the ShoreTel system are the general system settings. These configurations include the Call Control, the Site and the Switch settings. If these items have already been configured on the system, skip this section and go on to the “ShoreTel System Settings – Trunk Groups” section below.

### 3.2.1 Call Control Settings

The first settings to configure within ShoreWare Director are the Call Control Options. To configure these settings for the ShoreTel system, log into ShoreWare Director and select “Administration” then “Call Control” followed by “Options”.

#### Administration Call Control Options



The “Call Control Options” screen will then appear.

#### Call Control Options

A screenshot of the 'Call Control Options' configuration page in ShoreWare Director. The page title is 'Call Control Options' with an 'Edit' link below it. On the right side, there are 'Save' and 'Reset' buttons and a 'Help' link. Below the title bar, there is a blue bar with 'Edit this record' and a 'Refresh this page' link. The main content area contains several settings: 'Enable SIP Session Timer' (checked), 'Session Interval (0 - 9999):' (1800 sec), 'Refresher:' (Caller (UAC)), 'Voice Encoding and Quality of Service:' section with 'Intra-Site Calls:', 'Inter-Site Calls:', and 'FAX and Modem Calls:' all set to '64 Kbps (G.711)', 'Maximum Inter-Site Jitter Buffer:' (50 msec), and 'DiffServ / ToS Byte (0-255):' (0). At the bottom, there are three unchecked checkboxes: 'Admission control algorithm assumes RTP header compression is being used.', 'Enable Media Encryption.', and 'Always Use Port 5004 for RTP.'



Enable SIP Session Timer.

Session Interval (0 - 9999):  sec

Refresher:

**Voice Encoding and Quality of Service:**

Intra-Site Calls:

Inter-Site Calls:


FAX and Modem Calls:

Maximum Inter-Site Jitter Buffer:  msec

DiffServ / ToS Byte (0-255):

Admission control algorithm assumes RTP header compression is being used.

Enable Media Encryption.

Always Use Port 5004 for RTP. 

Within the “Call Control Options” screen, confirm that the appropriate settings are made for the “Enable SIP Session Timer”, “Intra-Site Calls”, “Inter-Site Calls” and “Always Use Port 5004 for RTP” fields.

The first step is to make sure that the “Enable SIP Session Timer” box is checked. Next the Session Interval Timer needs to be set. The recommended setting for “Session Interval” is 1800 seconds. The last item to select is the appropriate refresher (from the pull down menu) for the SIP Session Timer. The “Refresher” field will be set either to “Caller (UAC)” [User Agent Client] or to “Callee (UAS)” [User Agent Server]. If the “Refresher” field is set to “Caller (UAC)”, the Caller’s device will be in control of the session timer refresh. If “Refresher” is set to “Callee (UAS)”, the device of the person called will control the session timer refresh.

The next settings to verify are the “Intra-Site Calls” and the “Inter-Site Calls” settings under the “Voice Encoding and Quality of Service” prompt. For the Intra-Site Calls, verify that the desired audio bandwidth is selected for the CODEC for calls within the system. The settings should then be confirmed for the desired audio bandwidth CODEC for Inter-Site calls (calls between sites).

**Note:** SIP uses both G.711 and G.729 CODECs. The CODEC setting will be negotiated to the highest CODEC supported (fax requires G.711 at minimum).

**Note:** Unchecking the box for “Always Use Port 5004 for RTP” is required for implementing SIP on the ShoreTel system. For SIP configurations, Dynamic User Datagram Protocol (UDP) must be used for RTP Traffic. If the box is unchecked, MGCP will no longer use UDP port 5004; MGCP and SIP traffic will use dynamic UDP ports. Once this parameter is unchecked, make sure that “everything” (IP Phones, ShoreGear Switches, ShoreWare Director, Distributed Voice Services / Remote Servers, Conference Bridges and Contact Centers) is “fully” rebooted – this is a “one time only” item. By not performing a full system reboot, one way audio will probably occur during initial testing.

### 3.2.2 Sites Settings

The next settings to address are the administration of sites. These settings are modified under the ShoreWare Director by selecting “Administration”, then “Sites”.

#### Administration Site



This selection brings up the “Sites” screen. Within the “Sites” screen, select the name of the site to configure. The “Edit Site” screen will then appear. The only change required to the “Edit Site” screen is to the “Admission Control Bandwidth” field.



**Note:** Bandwidth of 1024 is just an example. Please see the Planning and Installation Guide for additional information on setting Admission Control Bandwidth.

#### Sites Edit screen – Admission Control Bandwidth

The Admission Control Bandwidth defines the bandwidth available to and from the site. This is important as SIP devices will be counted against the site bandwidth. Bandwidth needs to be set appropriately based on site setup and configuration with the ITSP SIP Trunking. See the ShoreTel Planning and Installation Guide for more information.

### 3.2.3 Switch Settings - Allocating Ports

The final general settings to input are the ShoreGear switch settings. These changes are modified by selecting “Administration”, then “Switches” in ShoreWare Director.

#### Administration Switches



This action brings up the “Switches” screen. From the “Switches” screen simply select the name of the switch to configure. The “Edit ShoreGear ...Switch” screen will be displayed. Within the “Edit ShoreGear ...Switch” screen, select the desired number of SIP Trunks from the ports available.

#### ShoreGear Switch Settings



Each port designated as a SIP Trunk enables the support for 5 individual trunks.

### 3.2.4 System Settings – Trunk Groups

ShoreTel Trunk Groups support both Dynamic and Static SIP endpoint Individual Trunks.

**Note:** A ShoreGear switch can only support one Trunk Group with Dynamic IP addressing.

In trunk planning, the following need to be considered.

1. Are the SIP devices using DHCP or Static IP?
2. Are the SIP devices endpoints (like Attached Technology Attachments (ATAs), Conference Phone or WiFi handset) or non-endpoint devices like an ITSP?

If the SIP Trunk Groups have already been configured on the system, skip down to the “ShoreTel System Settings - Individual Trunks” section. The settings for Trunk Groups are changed by selecting “Administration”, then “Trunks” followed by “Trunk Groups” within ShoreWare Director.

#### Administration Trunk Groups



This selection brings up the “Trunk Groups” screen.

#### Trunk Groups Settings



From the pull down menus on the “Trunk Groups” screen, select the site desired and select the “SIP” trunk type to configure and click on the “Go” link from “Add new trunk group at site:”. The “Edit SIP Trunk Group” screen will appear.

## SIP Trunk Group Settings



**Trunk Groups**  
Edit SIP Trunk Group

New Copy Save Delete Reset Help

Refresh this page \* modified

**Edit this record**

Name: SIP Masergy

Site: Headquarters

Language: English

Teleworker

Enable Digest Authentication

User ID:

Password:

Enable SIP Info for G.711 DTMF Signaling

For the Ingate SIP Trunking, the trunks need to be configured as inter-site trunks (trunks between sites). The trunks will also be configured as static.

The next step within the “Edit SIP Trunks Group” screen is to input the name for the trunk group. In the example in Figure 9, the name “SIP” has been created. The next step is to verify the setting of the “Teleworker” check box. The “Teleworker” check box needs to be checked since the trunk groups have been configured as inter-site. Once this box is checked, it will count against the site bandwidth.

The “Enable Digest Authentication” field is not required when connecting to an Ingate box.

The “Enable SIP Info for G.711 DTMF Signaling” box should not be checked. Enabling SIP info is currently only used with tie trunks between ShoreTel systems.

The next item to change in the “Edit SIP Trunks Group” screen is to make the appropriate settings for the “Inbound:” fields.

## Inbound

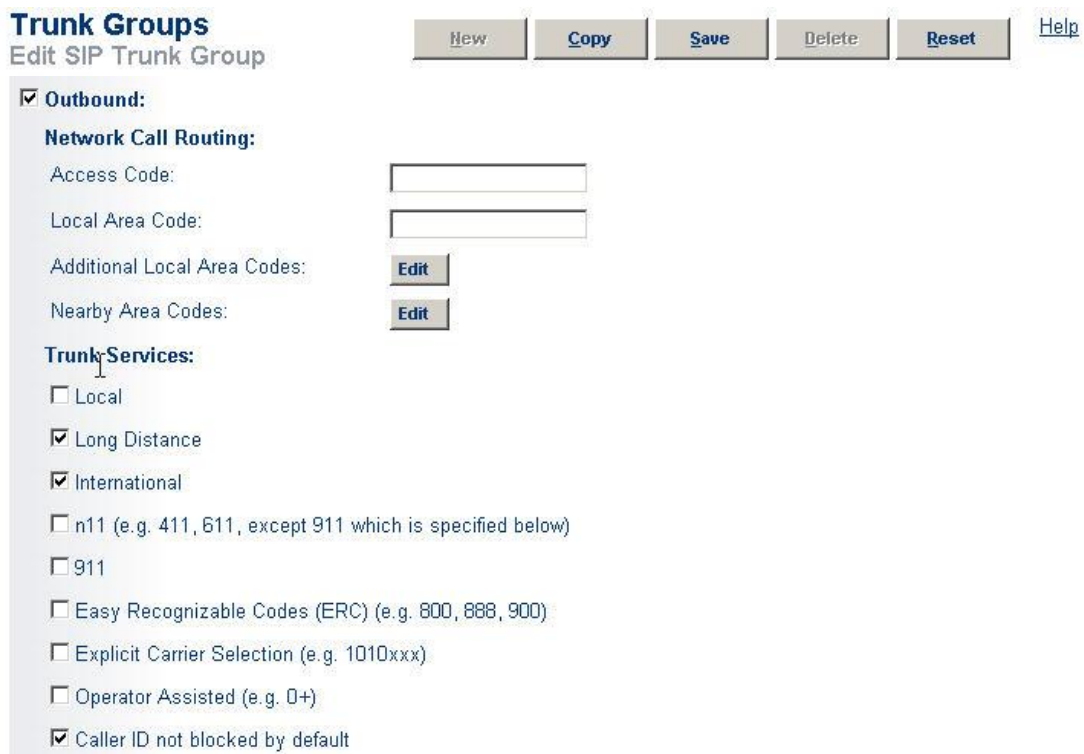
<b>Edit this record</b>		<a href="#">Refresh this page</a>
Name:	<input type="text" value="SIP - ITSP Example"/>	
Site:	HQ Sunnyvale Demo	
Language:	<input type="text" value="English(US)"/>	
<input checked="" type="checkbox"/> Teleworkers		
<input type="checkbox"/> Enable SIP Info for G.711 DTMF Signaling		
<input type="checkbox"/> Enable Digest Authentication		
User ID:	<input type="text"/>	
Password:	<input type="text"/>	
<b>Inbound:</b>		
Number of Digits from CO:	<input type="text" value="10"/>	
<input checked="" type="checkbox"/> DNIS	<input type="button" value="Edit DNIS Map"/>	
<input checked="" type="checkbox"/> DID	<input type="button" value="Edit DID Range"/>	
<input checked="" type="checkbox"/> Extension		
<input checked="" type="radio"/> Translation Table:	<input type="text" value="&lt;None&gt;"/>	
<input type="radio"/> Prepend Dial In Prefix:	<input type="text"/>	
<input type="radio"/> Use Site Extension Prefix		
<input checked="" type="checkbox"/> Tandem Trunking		
User Group:	<input type="text" value="Executives"/>	
Prepend Dial In Prefix:	<input type="text"/>	
Destination:	<input type="text" value="5200 : Main Menu"/> <input type="button" value="Search"/>	

Within the “Inbound:” settings ensure the “Number of Digits from CO” is set to <XX ITSP provided> and ensure the “DNIS” or “DID” box is checked , along with the Extension parameter(see Planning and Installation Guide for further information on configuration).

Tandem Trunking is not required unless you plan on routing incoming SIP trunk calls out other ShoreTel trunks.

**Note:** This section is configured no different then any normal Trunk Group

## Trunk Services



**Trunk Groups**  
Edit SIP Trunk Group

New Copy Save Delete Reset Help

**Outbound:**

**Network Call Routing:**

Access Code:

Local Area Code:

Additional Local Area Codes:  Edit

Nearby Area Codes:  Edit

**Trunk Services:**

Local

Long Distance

International

n11 (e.g. 411, 611, except 911 which is specified below)

911

Easy Recognizable Codes (ERC) (e.g. 800, 888, 900)

Explicit Carrier Selection (e.g. 1010xxx)

Operator Assisted (e.g. 0+)

Caller ID not blocked by default

On the “Trunk Services:” screen, make sure the appropriate services are checked or unchecked based on what the ITSP supports and what features are needed from this Trunk Group.

The last checkbox determines if the call is sent out as <unknown> or with caller information (Caller ID). User DID etc. will impact how information is passed out to the SIP Trunk group.

After these settings are made to the “Edit SIP Trunk Group” screen, press the “Save” button to input the changes.

This completes the settings needed to set up the trunk groups on the ShoreTel system.

### 3.2.5 System Settings – Individual Trunks

This section covers the configuration of the individual trunks. Select “Administration”, then “Trunks” followed by “Individual Trunks” to configure the individual trunks.

#### Individual Trunks



The “Trunks by Group” screen that is used to change the individual trunks settings then appears.

#### Trunks by Group



Select the site for the new individual trunk(s) to be added and select the appropriate trunk group from the pull down menu in the “Add new trunk at site” area. In this example, the site is “Headquarters” and the trunk group is “SIP”. Click on the ”Go” button to bring up the “Edit Trunk” screen.

#### Edit Trunks Screen for Individual Trunks





From the individual trunks “Edit Trunk” screen, input a name for the individual trunks, select the appropriate switch, select the SIP Trunk type and input the number of trunks. When selecting a name, the recommendation is to name the individual trunks the same as the name of the trunk group so that the trunk type can easily be tracked. Select the switch upon which the individual trunk will be created. For the ITSP Trunk, select “Use IP Address” button and input an IP address of the Ingate SIParator product. The last step is to select the number of individual trunks desired (each one supports “one” audio path – example if 5 is input, then 5 audio paths can be up at one time). Once these changes are complete, press the “Save” button to input the changes.

**Note:** Individual SIP Trunks cannot span networks. SIP Trunks can only terminate on the switch selected. There is no failover to another switch. For redundancy, two trunk groups will be needed with each pointing to another Ingate SIParator – just the same as if PRI were being used.

After setting up the trunk groups and individual trunks, refer to the ShoreTel Product Installation Guide to make the appropriate changes for the User Group settings. This completes the settings for the ShoreTel system side.

## 4 Ingate Configuration

### 4.1 About

Ingate products are compatible with communications equipment from other vendors and service providers who support the SIP Protocol. The Ingate products are a security device designed to sit on the Enterprise network edge, an ICSA Labs Certified security product, focused on SIP communications security and network security for the Enterprise.



Ingate products are designed to solve the issues related to SIP traversing the NAT (Network Address Translation) which is a part of all enterprise class firewalls. The NAT translates between the public IP address(es) of the enterprise, and the private IP addresses which are only known inside the LAN. These private IP addresses are created to enable all devices to have an IP address, and also provide one of the security layers of the enterprise network. In addition, the Ingate products provide routing rules to assign to SIP traffic flow to ensure only allowed SIP traffic will pass.

#### 4.1.1 Startup Tool

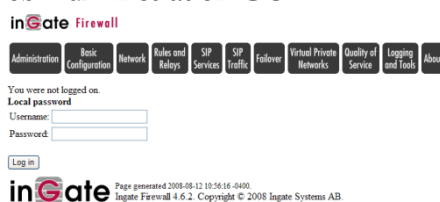
The Ingate Startup Tool is an installation tool for Ingate Firewall® and Ingate SIParator® products, facilitates the “out of the box” set up of SIP Trunking solutions with ShoreTel and various Internet Telephony Service Providers. Designed to simplify SIP trunk deployments, the tool will automatically configure a user’s Ingate Firewall or SIParator® to work with ShoreTel and the SIP Trunking service provider of your choice. With the push of a button, the configuration tool will automatically create a SIP trunk deployment designed to the user’s individual setup.

Users can select ShoreTel from a drop-down menu and the Internet Telephony Service Provider (ITSP) they use; the configuration tool will automatically apply the correct settings to the Ingate Firewall or SIParator to work seamlessly with that vendor or service provider. A list of SIP Trunking service providers that have demonstrated interoperability with the Ingate products is incorporated into the interface. Please note that not all SIP Trunking service providers listed in this interface have been certified by ShoreTel. Consult the ShoreTel Certified Technology Partner list of vendors for a current list. ([http://www.shoretel.com/partners/technology/certified\\_partners.html](http://www.shoretel.com/partners/technology/certified_partners.html))

The configuration tool is available now as a free download for all Ingate Firewalls and SIParators. It can be found at <http://www.ingate.com/startuptool.php>. Also available here is a Startup Tool Getting Started Guide to assist in using the Startup Tool.

#### 4.1.2 Web Admin

By default the Ingate units does not come pre-assigned with an IP Address or Password, once these are assigned by the Startup Tool or Console Port, the Ingate units can be administered via the web. Using a Browser, simply enter the IP Address assigned to the unit, this will launch the Web Administration GUI.



## 4.2 Connecting the Ingate Firewall/SIParator

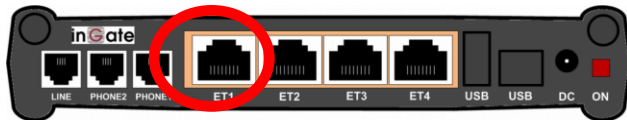
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

The following will describe a process to connect the Ingate unit to the network then have the Ingate Startup Tool assign an IP Address and Password to the Unit.

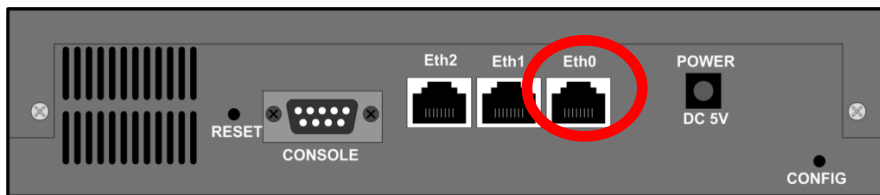
### Configuration Steps:

1. Connect Power to the Unit.
2. Connect an Ethernet cable to “Eth0”. This Ethernet cable should connect to a LAN network. Below are some illustrations of where “Eth0” are located on each of the Ingate Model types. On SIParator SBE connect to “ET1”.

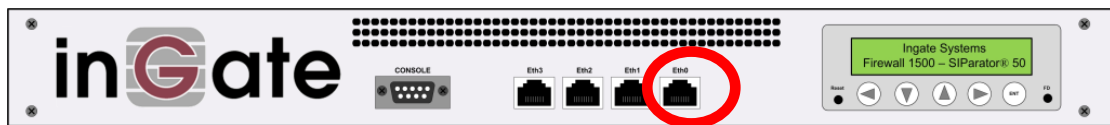
#### Ingate SIParator SBE (Back)



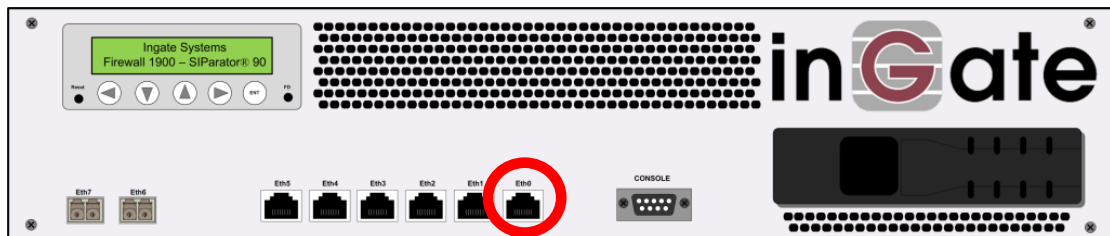
#### Ingate 1190 Firewall and SIParator 19 (Back)



#### Ingate 1500/1550/1650 Firewall and SIParator 50/55/65

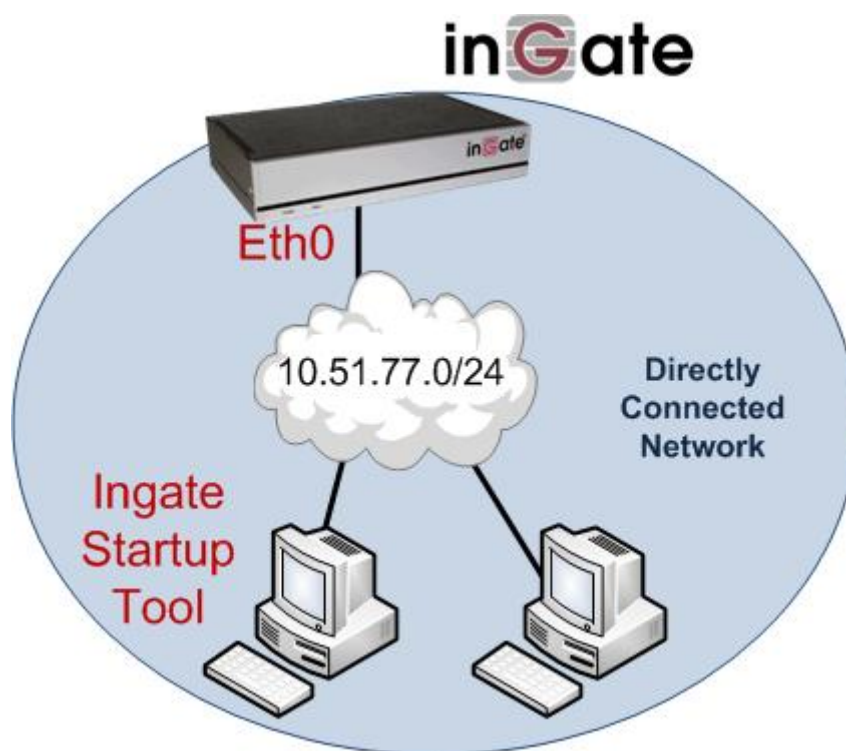


#### Ingate 1900 Firewall and SIParator 90



3. The PC/Server with the Startup Tool should be located on the same LAN segment/subnet. It is required that the Ingate unit and the Startup Tool are on the same LAN Subnet to which you are going to assign an IP Address to the Ingate Unit.

**Note:** When configuring the unit for the first time, avoid having the Startup Tool on a PC/Server on a different Subnet, or across a Router, or NAT device, Tagged VLAN, or VPN Tunnel. Keep the network Simple.



4. Proceed to Section 4.3: Using the Startup Tool for instructions on using the Startup Tool.

## 4.3 Using the Startup Tool

There are three main reasons for using the Ingate Startup Tool. First, the “Out of the Box” configuring the Ingate Unit for the first time. Second, is to change or update an existing configuration. Third, is to register the unit, install a License Key, and upgrade the unit to the latest software.

**Note:** The Startup Tool does not have the ability to program the third (Eth2) Ethernet port. This programming will have to be done manually.

### 4.3.1 Configure the Unit for the First Time

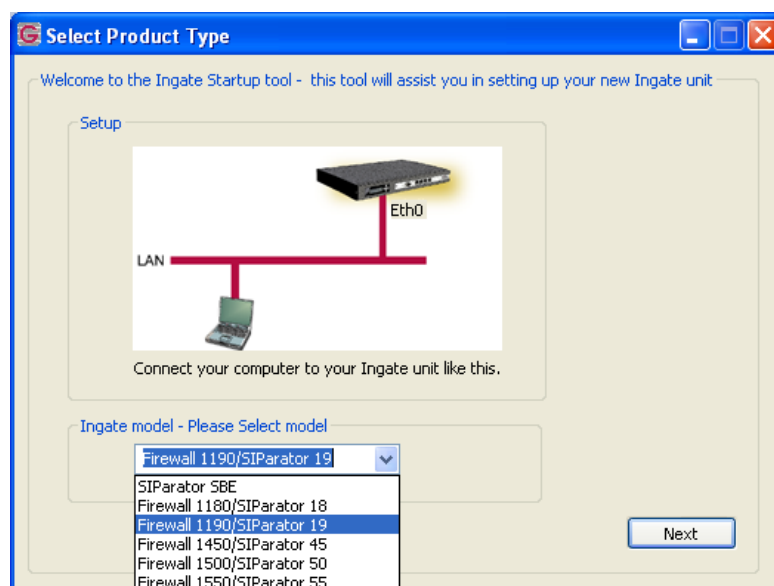
From the factory the Ingate Firewall and SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

In the Startup Tool, when selecting “Configure the unit for the first time”, the Startup Tool will find the Ingate Unit on the network and assign an IP Address and Password to the Ingate unit. This procedure only needs to be done ONCE. When completed, the Ingate unit will have an IP Address and Password assigned.

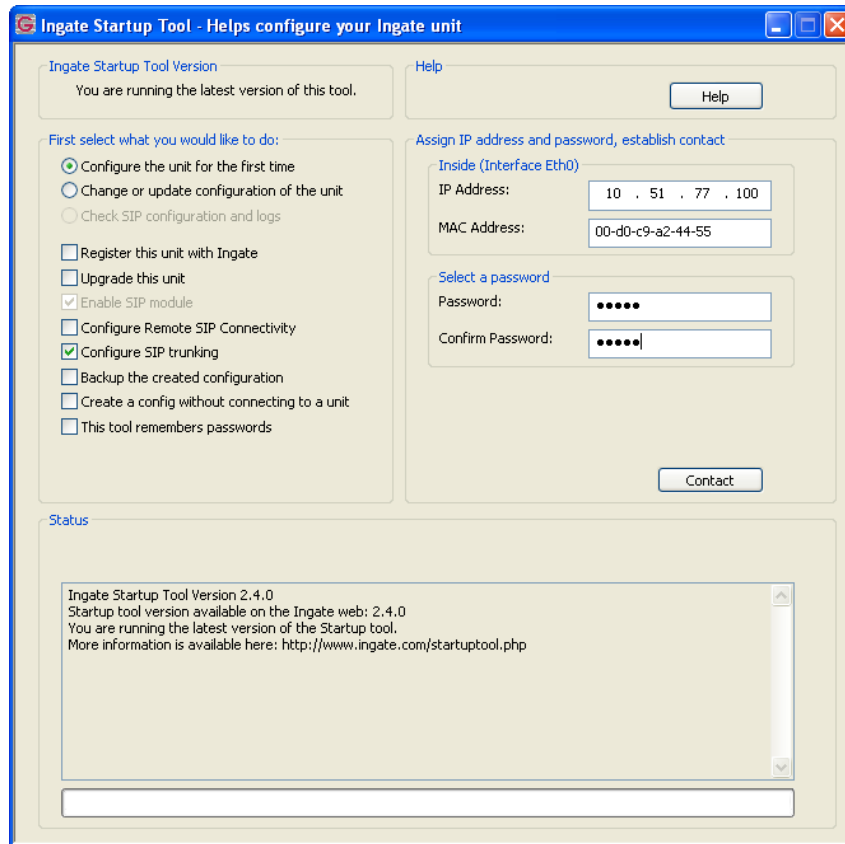
**Note:** If the Ingate Unit already has an IP Addressed and Password assigned to it (by the Startup Tool or Console) proceed directly to Section 3.3.2: “Change or Update Configuration”.

#### Configuration Steps:

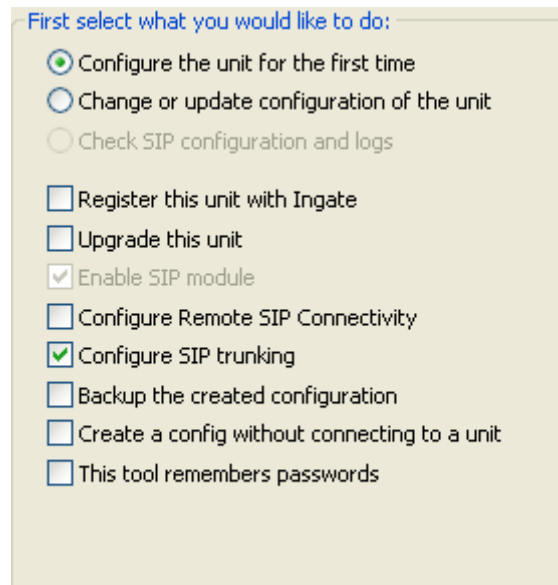
1. Launch the Startup Tool
2. Select the Model type of the Ingate Unit, and then click Next.



3. In the “Select first what you would like to do”, select “Configure the unit for the first time”.



4. Other Options in the “Select first what you would like to do”,



- a. Select “Configure SIP Trunking” if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.
- b. Select “Configure Remote SIP Connectivity” if you want the tool to configure Remote Phone access to an IP-PBX

- c. Select “Register this unit with Ingate” if you want the tool to connect with [www.ingate.com](http://www.ingate.com) to register the unit.
  - d. Select “Upgrade this unit” if you want the tool to connect with [www.ingate.com](http://www.ingate.com) to download the latest software release and upgrade the unit. If selected, see Section 4.3: Licenses and Upgrades.
  - e. Select “Backup the created configuration” if you want the tool to apply the settings to an Ingate unit and save the config file.
  - f. Select “Creating a config without connecting to a unit” if you want the tool to just create a config file.
  - g. Select “The tool remembers passwords” if you want the tool to remember the passwords for the Ingate unit.
5. In the “Inside (Interface Eth0)”,
    - a. Enter the IP Address to be assigned to the Ingate Unit.
    - b. Enter the MAC Address of the Ingate Unit, this MAC Address will be used to find the unit on the network. The MAC Address can be found on a sticker attached to the unit.

Inside (Interface Eth0)

IP Address:

MAC Address:

6. In the “Select a Password”, enter the Password to be assigned to the Ingate unit.

Select a password

Password:

Confirm Password:

7. Once all required values are entered, the “Contact” button will become active. Press the “Contact” button to have the Startup Tool find the Ingate unit on the network, assign the IP Address and Password.

Assign IP address and password, establish contact

Inside (Interface Eth0)

IP Address:

MAC Address:

Select a password

Password:

Confirm Password:

8. Proceed to Section 3.3.3: Network Topology.

### 4.3.2 Change or Update Configuration

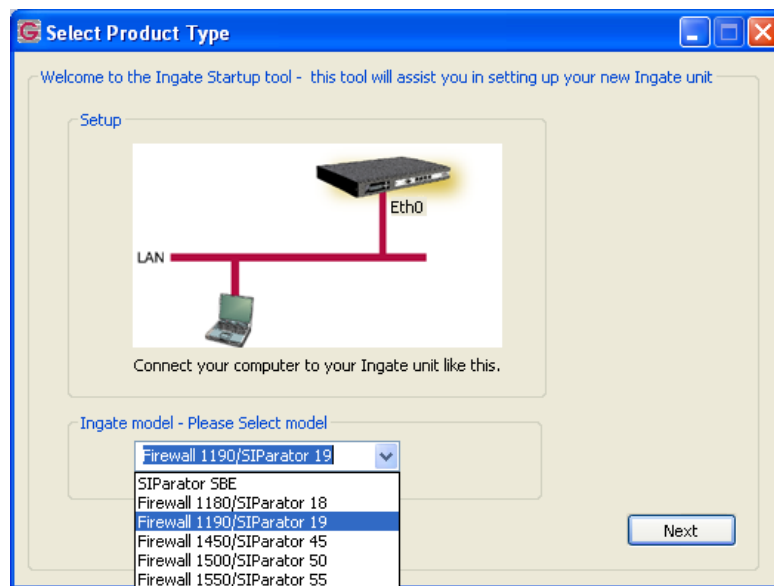
When selecting the “Change or update configuration of the unit” setting in the Startup Tool the Ingate Unit must have already been assigned an IP Address and Password, either by the Startup Tool – “Configure the unit for the first time” or via the Console port.

In the Startup Tool, when selecting “Change or update configuration of the unit”, the Startup Tool will connect directly with the Ingate Unit on the network with the provided IP Address and Password. When completed, the Startup Tool will completely overwrite the existing configuration in the Ingate unit with the new settings.

**Note:** If the Ingate Unit does not have an IP Addressed and Password assigned to it, proceed directly to Section 3.3.1: “Configure the Unit for the First Time”.

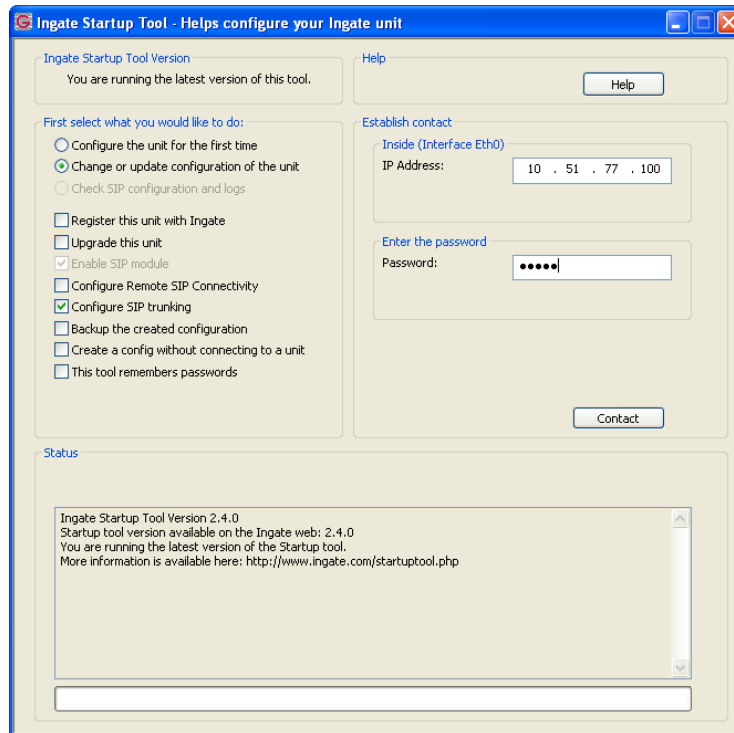
#### Configuration Steps:

1. Launch the Startup Tool
2. Select the Model type of the Ingate Unit, and then click Next.

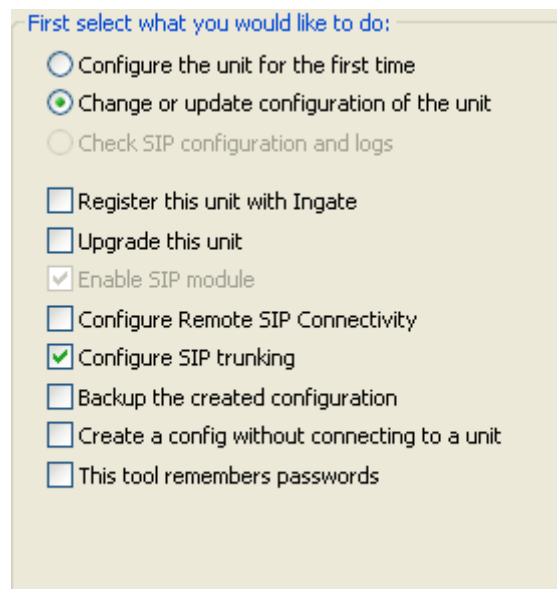




3. In the “Select first what you would like to do”, select “Change or update configuration of the unit”.

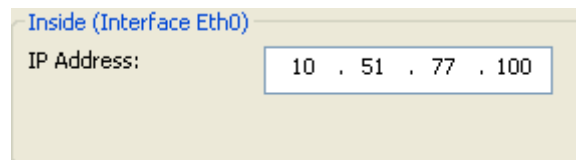


4. Other Options in the “Select first what you would like to do”,



- a. Select “Configure SIP Trunking” if you want the tool to configure SIP Trunking between a IP-PBX and ITSP.
- b. Select “Configure Remote SIP Connectivity” if you want the tool to configure Remote Phone access to an IP-PBX
- c. Select “Register this unit with Ingate” if you want the tool to connect with [www.ingate.com](http://www.ingate.com) to register the unit.

- d. Select “Upgrade this unit” if you want the tool to connect with [www.ingate.com](http://www.ingate.com) to download the latest software release and upgrade the unit. If selected, see Section 4.3: Licenses and Upgrades.
  - e. Select “Backup the created configuration” if you want the tool to apply the settings to an Ingate unit and save the config file.
  - f. Select “Creating a config without connecting to a unit” if you want the tool to just create a config file.
  - g. Select “The tool remembers passwords” if you want the tool to remember the passwords for the Ingate unit.
5. In the “Inside (Interface Eth0)”,
    - a. Enter the IP Address of the Ingate Unit.



Inside (Interface Eth0)

IP Address:

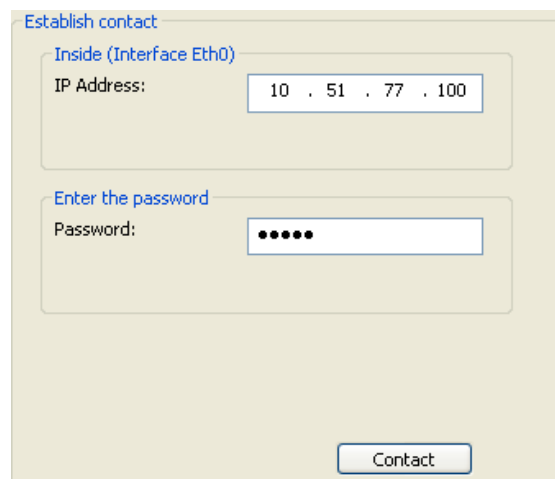
6. In the “Enter a Password”, enter the Password of the Ingate unit.



Enter the password

Password:

7. Once all required values are entered, the “Contact” button will become active. Press the “Contact” button to have the Startup Tool contact the Ingate unit on the network.



Establish contact

Inside (Interface Eth0)

IP Address:

Enter the password

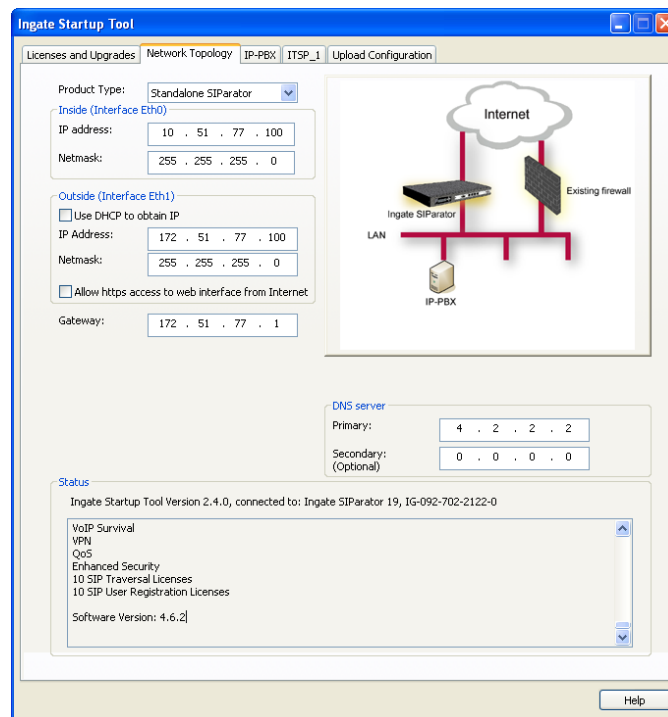
Password:

8. Proceed to Section 3.3.3: Network Topology.

### 4.3.3 Network Topology

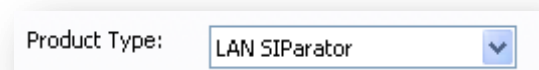
The Network Topology is where the IP Addresses, Netmask, Default Gateways, Public IP Address of NAT'ed Firewall, and DNS Servers are assigned to the Ingate unit. The configuration of the Network Topology is dependent on the deployment (Product) type. When selected, each type has a unique set of programming and deployment requirements, be sure to pick the Product Type that matches the network setup requirements.

**Note:** The Startup Tool does not program the PAETEC-ShoreTel-Ingate deployment perfectly in both scenarios. Some manual modification will be needed in both cases; this programming will have to be done over the Web GUI.



#### Configuration Steps:

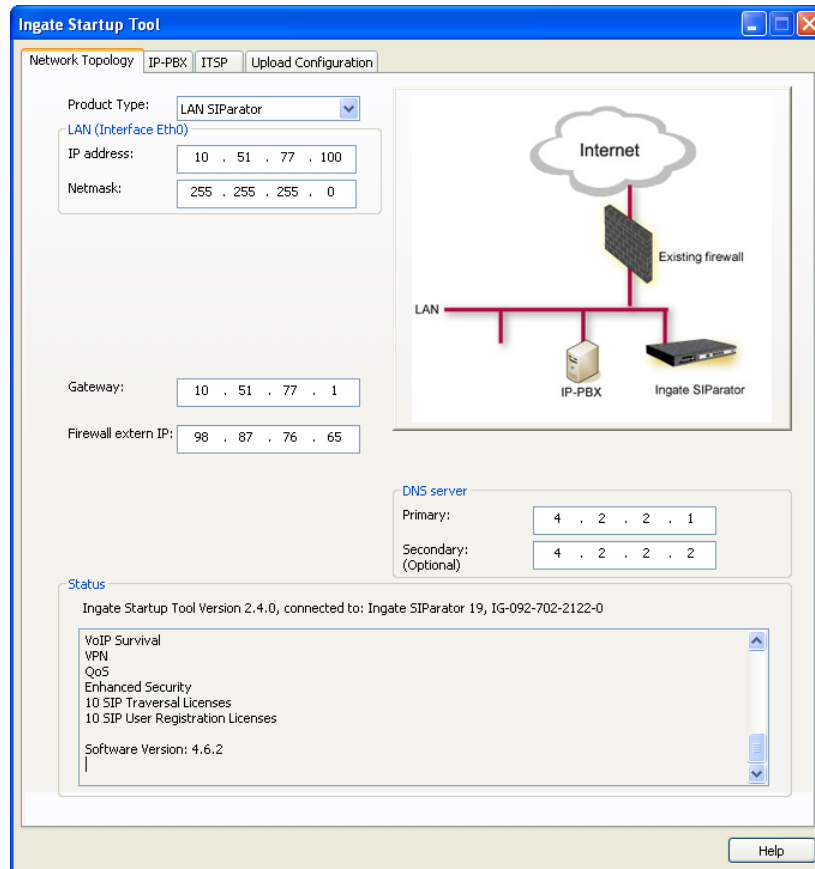
1. In the Product Type drop down list, select the deployment type of the Ingate Firewall or SIParator.



2. When selecting the Product Type, the rest of the page will change based on the type selected. LAN SIParator will be used with the MPLS – SIP Trunking Only scenario, and Firewall when using both Internet and SIP Trunking scenario.

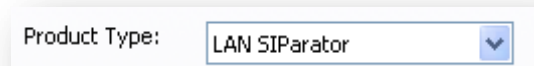
### 4.3.3.1 Product Type: LAN SIParator

When deploying an Ingate SIParator in a LAN configuration, the Ingate resides on a LAN network with all of the other network devices. As there is no existing Firewall, the Default Gateway for the LAN network is the Paetec IAD; the ISD is the primary edge device for all data and voice traffic out of the LAN to the WAN/Internet. SIP Signaling and Media must be forwarded to the Ingate SIParator, both from Paetec and the ShoreTel. The voice traffic from the LAN is directed to the SIParator then to the existing IAD and out to the Peatec SIP Server.

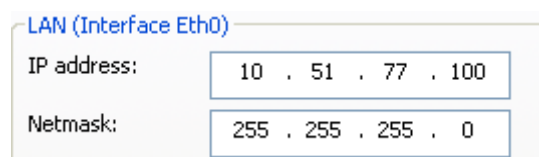


#### Configuration Steps:

1. In Product Type, select “LAN SIParator”.



2. Define the IP Address and Netmask of the inside LAN (Interface Eth0). This is the IP Address that will be used on the Ingate unit to connect to the LAN network.



3. Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.

Gateway:

4. Enter the existing Firewall's external WAN/Internet IP Address. This is used to ensure correct SIP Signaling and Media traversal functionality. This is required when the existing Firewall is providing NAT. This will be manually removed later.

Firewall extern IP:

5. Enter the DNS Servers for the Ingate Firewall. These DNS Servers will be used to resolve FQDNs of SIP Requests and other features within the Ingate. They can be internal LAN addresses or outside WAN addresses.

DNS server

Primary:

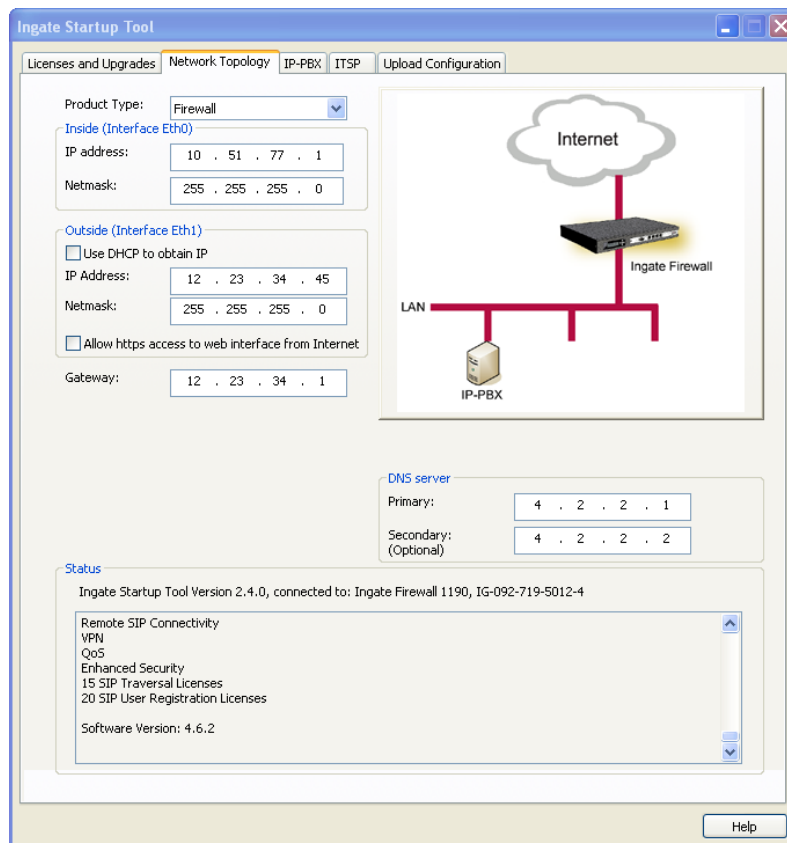
Secondary:  
(Optional)

6. On the Existing Firewall, the SIP Signaling Port and RTP Media Ports need to be forwarded to the Ingate SIParator. The Ingate SIParator is an ICSA Certified network edge security device, so there are no security concerns forwarding network traffic to the SIParator.

### 4.3.3.2 Product Type: Firewall

When deploying an Ingate Firewall, there is only one way the Firewall can be installed. The Firewall must be the Default Gateway for the LAN; it is the primary edge device for all data and voice traffic out of the LAN to the Internet.

**Note:** The Startup Tool does not have the ability to program the third (Eth2) Ethernet port. This programming will have to be done manually.

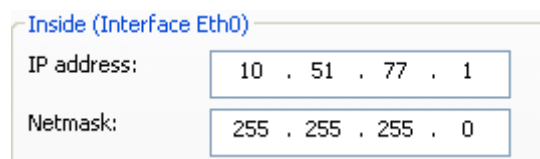


#### Configuration Steps:

1. In Product Type, select “Firewall”.



2. Define the Inside (Interface Eth0) IP Address and Netmask. This is the IP Address that will be used on the LAN side on the Ingate unit.



3. Define the Outside (Interface Eth1) IP Address and Netmask. This is the IP Address that will be used on the Internet (WAN) side on the Ingate unit.
  - a. A Static IP Address and Netmask can be entered
  - b. Or select “Use DHCP to obtain IP”, if you want the Ingate Unit to acquire an IP address dynamically using DHCP.

Outside (Interface Eth1)

Use DHCP to obtain IP

IP Address:

Netmask:

Allow https access to web interface from Internet

4. Enter the Default Gateway for the Ingate Firewall. The Default Gateway for the Ingate Firewall will always be an IP Address of the Gateway within the network of the outside interface (Eth1).

Gateway:

5. Enter the DNS Servers for the Ingate Firewall. These DNS Servers will be used to resolve FQDNs of SIP Requests and other features within the Ingate. They can be internal LAN addresses or outside WAN addresses.

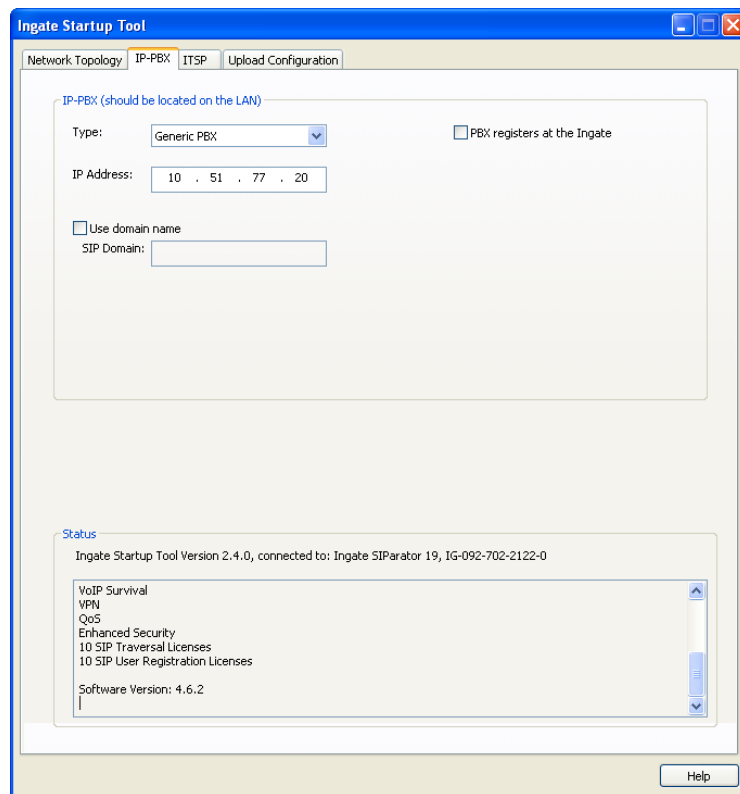
DNS server

Primary:

Secondary:  
(Optional)

## 4.3.4 IP-PBX

The IP-PBX section is where the IP Addresses and Domain location are provided to the Ingate unit. The configuration of the IP-PBX will allow for the Ingate unit to know the location of the IP-PBX as to direct SIP traffic for the use with SIP Trunking and Remote Phones. The IP Address of the IP-PBX must be on the same network subnet at the IP Address of the inside interface of the Ingate unit. Ingate has confirmed interoperability several of the leading IP-PBX vendors.

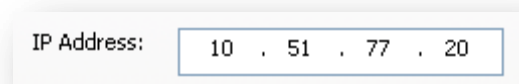


### Configuration Steps:

1. In the IP-PBX Type drop down list, select “ShoreTel”. Ingate has confirmed interoperability with ShoreTel, the unique requirements of the testing are contained in the Startup Tool.



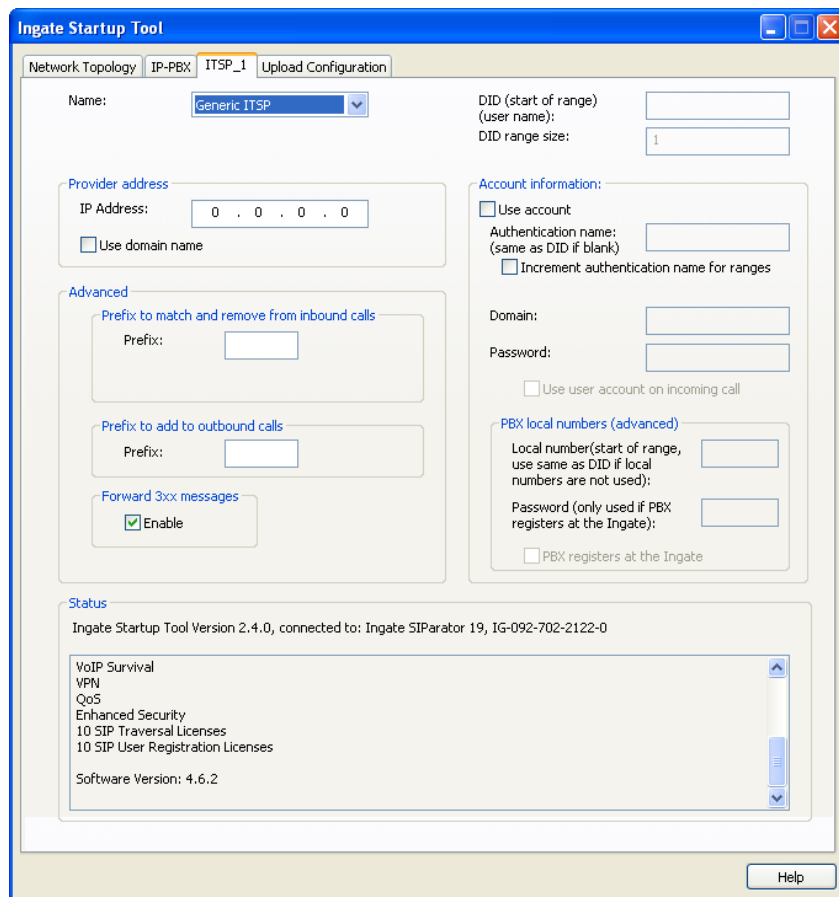
2. Enter the IP Address of the Shoregear switch. The IP Address should be on the same LAN subnet as the Ingate unit.





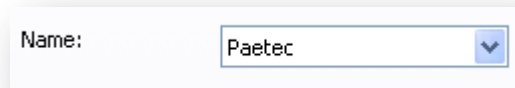
## 4.3.5 ITSP

The ITSP section is where all of the attributes of the SIP Trunking Service Provider are programmed. Details like the IP Addresses or Domain, DIDs, Authentication Account information, Prefixes, and PBX local number. The configuration of the ITSP will allow for the Ingate unit to know the location of the ITSP as to direct SIP traffic for the use with SIP Trunking. Ingate has confirmed interoperability many of the leading ITSP vendors.



### Configuration Steps:

1. In the ITSP drop down list, select PAETEC as the ITSP vendor. Ingate has confirmed interoperability with PAETEC, the unique requirements are contained in the Startup Tool. If the vendor choice is not seen, select "Paetec".



When you select a specific ITSP vendor, the Startup Tool will have the individual connection requirements predefined for that ITSP, the only additional entries may be the specific site requirements.

2. PAETEC is trusted IP deployment.
  - a. In the case where the Service Provider uses a Trusted IP deployment, all that is required is to enter the IP Address or Domain of the PAETEC's SIP Server or SBC. Enter the IP Address here, or select "Use domain name" and enter the FQDN of the Service Provider.

Provider address

IP Address:

Use domain name

Provider address

Domain:

Use domain name

3. The Ingate has the ability to add/remove digits and characters from the Request URI Header. A typical scenario is the addition/removal of ENUM character "+". Many IP-PBX and ITSPs either need to add or remove this character prior to sending or receiving SIP requests. Here you can enter values to Match and remove from the Request URI.

Advanced

Prefix to match and remove from inbound calls

Prefix:

Prefix to add to outbound calls

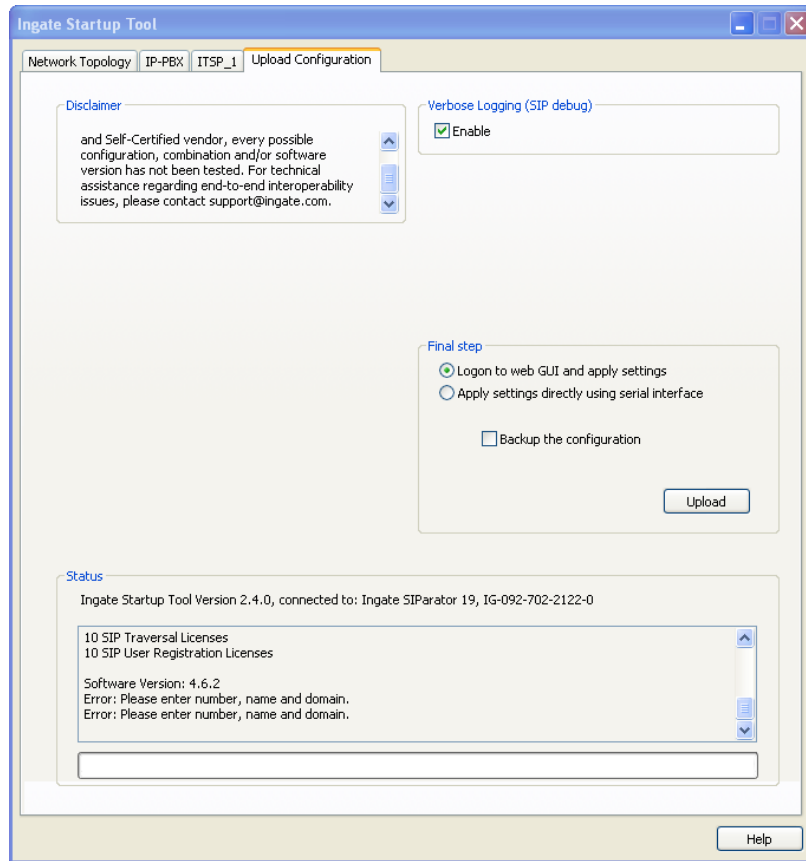
Prefix:

Forward 3xx messages

Enable

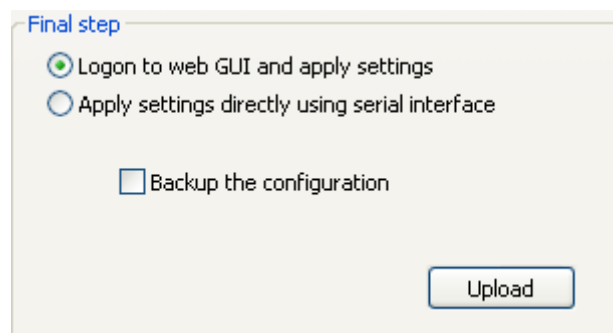
### 4.3.6 Upload Configuration

At this point the Startup Tool has all the information required to push a database into the Ingate unit. The Startup Tool can also create a backup file for later use.

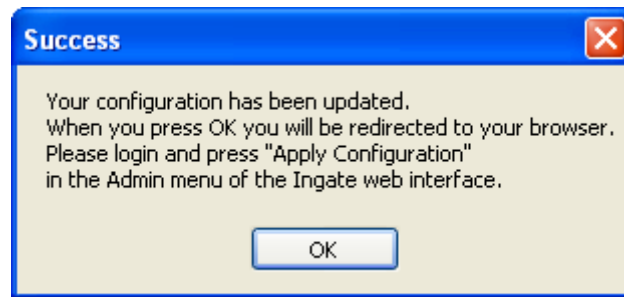


#### Configuration Steps:

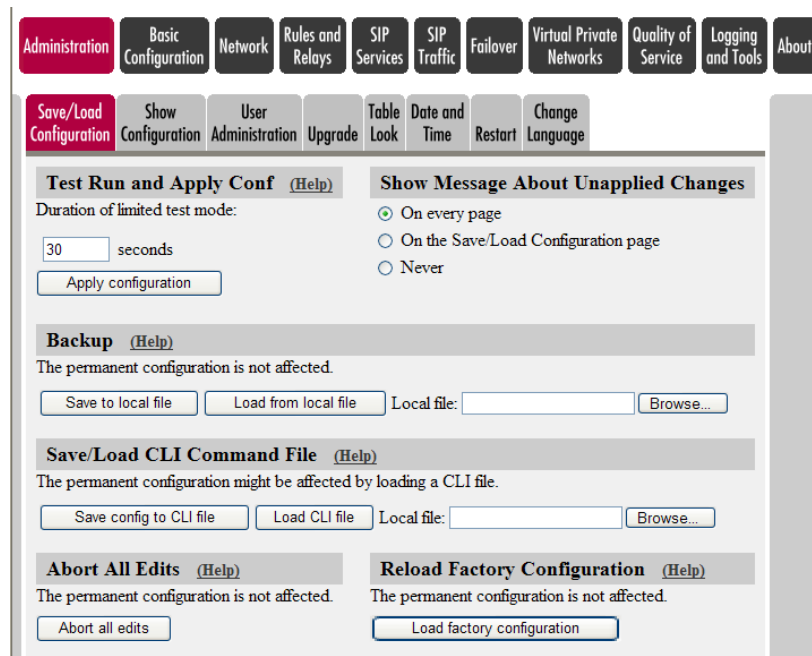
1. Press the “Upload” button. If you would like the Startup Tool to create a Backup file also select “Backup the configuration”. Upon pressing the “Upload” button the Startup Tool will push a database into the Ingate unit.



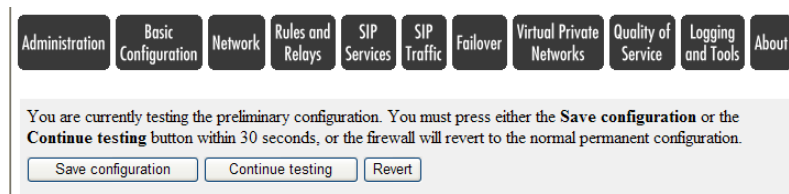
- When the Startup has finished uploading the database a window will appear and once pressing OK the Startup Tool will launch a default browser and direct you to the Ingate Web GUI.



- Although the Startup Tool has pushed a database into the Ingate unit, the changes have not been applied to the unit. Press “Apply Configuration” to apply the changes to the Ingate unit.



- A new page will appear after the previous step requesting to save the configuration. Press “Save Configuration” to complete the saving process.



- If using the Ingate SIParator in a LAN SIParator deployment proceed to Section 4.4.1.
- If using the Ingate Firewall to service both Data and Voice traffic proceed to Section 4.4.2.

## 4.4 Additional Manual Programming

### 4.4.1 Ingate SIParator - LAN SIParator Deployment

#### SIP Services – Interoperability

Remove any references in “Public IP address for NATed SIParator”. As there is no Firewall between the Ingate and Paetec’s IAD, this field is not needed.

**URI Encoding** (Help)  
Recommended setting: Always encrypt URIs

Always encrypt URIs  
 Use shorter, encrypted URIs  
 Escape URIs  
 Keep username in URIs

**Signaling Order of Re-INVITES** (Help)  
Recommended setting: Send re-INVITES all the way directly

Send re-INVITES all the way directly  
 Send response before re-INVITES are forwarded

**Public IP address for NATed SIParator** (Help)  
This setting is not supported for the Standalone configuration.

DNS Name or IP Address

#### SIP Traffic – Dial Plan

Inbound and Outbound traffic are being directed to the Ingate, the Startup Tool will assign the Existing Firewalls Public IP Address to the Inbound calls, but since there is no Firewall in this solution, the calls are directed to the Ingate private IP.

**Matching Request-URI** (Help)

Name	Use This ...				... Or This		Delete
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
Inbound	<input type="text"/>	<input type="text"/>	any character	<input type="text"/>	10.51.77.100	<input type="text"/>	<input type="checkbox"/>
Outbound	<input type="text"/>	<input type="text"/>	any character	<input type="text"/>	10.51.77.100	<input type="text"/>	<input type="checkbox"/>

Be sure to apply and save. These configuration changes will be fixed in the next version of Startup Tool.

## 4.4.2 Ingate Firewall Deployment

### Third Ethernet Interface

The Startup Tool does not define the third interface on the Ingate, thus it must be done manually. PAETEC's SIP server and Media server must be defined as a Static Route on this Interface. As the Ingate Firewall only supports one Default Gateway, which is being used for Data Traffic then Static Routes are defined to direct Voice traffic to PAETEC.

**General**

Physical device: eth2  
 This interface is:  On  Off  
 Interface name:

**Obtain IP Address Dynamically**

OFF  
 DHCP client ON  
 PPPoE client ON

**Speed and Duplex**

Automatic negotiation  
 100 Mbit/s, full duplex  
 100 Mbit/s, half duplex  
 10 Mbit/s, full duplex  
 10 Mbit/s, half duplex

**Directly Connected Networks** (Help)

Name	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete
SIP	172.51.77.1	172.51.77.1	255.255.255.0	172.51.77.0	172.51.77.255		-	<input type="checkbox"/>

Add new rows  rows.

**Alias** (Help)

Below are the ranges from which you can select aliases.

Name	DNS Name or IP Address	IP Address	Delete

Add new rows  rows.

**Static Routing** (Help)

Routed Network			Router		Delete
DNS Name or Network Address	Network Address	Netmask / Bits	DNS Name or IP Address	IP Address	
10.15.15.5	10.15.15.5	255.255.255.255	192.168.12.1	192.168.12.1	
10.15.15.30	10.15.15.30	255.255.255.255	192.168.12.1	192.168.12.1	

### Network and Computers

Any of PAETEC's networks, SIP Servers, Media Servers need to be defined here and associated with the third interface.

**Networks and Computers**

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	
LAN	-	10.51.77.0	10.51.77.0	10.51.77.255	10.51.77.255	inside (eth0 untagged)
Peatec_Servers	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	Ethernet2 (eth2 untagged)
ShoreTel	-	10.51.77.20	10.51.77.20			-
WAN	-	0.0.0.0	0.0.0.0	127.0.0.0	127.0.0.0	outside (eth1 untagged)
	-	127.0.0.2	127.0.0.2	255.255.255.255	255.255.255.255	outside (eth1 untagged)

## 5 Troubleshooting

### 5.1 Startup Tool Troubleshooting

#### 5.1.1 Status Bar

Located on every page of the Startup Tool is the Status Bar. This is a display and recording of all of the activity of the Startup Tool, displaying Ingate unit information, software versions, Startup Tool events, errors and connection information. Please refer to the Status Bar to acquire the current status and activity of the Startup Tool.



#### 5.1.2 Configure Unit for the First Time

Right “Out of the Box”, sometimes connecting and assigning an IP Address and Password to the Ingate Unit can be a challenge. Typically, the Startup Tool cannot program the Ingate Unit. The Status Bar will display “The program failed to assign an IP address to eth0”.



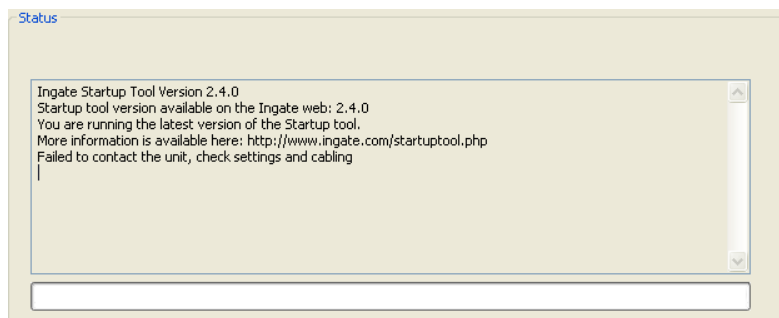
#### Possible Problems and Resolutions

Possible Problems	Possible Resolution
Ingate Unit is not Turned On.	Turn On or Connect Power (Trust me, I've been there)
Ethernet cable is not connected to Eth0.	Eth0 must always be used with the Startup Tool.
Incorrect MAC Address	Check the MAC address on the Unit itself. MAC Address of Eth0.
An IP Address and/or Password have already been assigned to the Ingate Unit	It is possible that an IP Address or Password have been already been assigned to the unit via the Startup Tool or Console
Ingate Unit on a different Subnet or Network	The Startup Tool uses an application called “Magic PING” to assign the IP Address to the Unit. It is heavily reliant on ARP, if the PC with the Startup

	Tool is located across Routers, Gateways and VPN Tunnels, it is possible that MAC addresses cannot be found. It is the intension of the Startup Tool when configuring the unit for the first time to keep the network simple. See Section 3.
Despite your best efforts...	<ol style="list-style-type: none"> <li>1. Use the Console Port, please refer to the Reference Guide, section “Installation with a serial cable”, and step through the “Basic Configuration”. Then you can use the Startup Tool, this time select “Change or Update the Configuration”</li> <li>2. Factory Default the Database, then try again.</li> </ol>

### 5.1.3 Change or Update Configuration

If the Ingate already has an IP Address and Password assigned to it, then you should be able use a Web Browser to reach the Ingate Web GUI. If you are able to use your Web Browser to access the Ingate Unit, then the Startup should be able to contact the Ingate unit as well. The Startup Tool will respond with “Failed to contact the unit, check settings and cabling” when it is unable to access the Ingate unit.



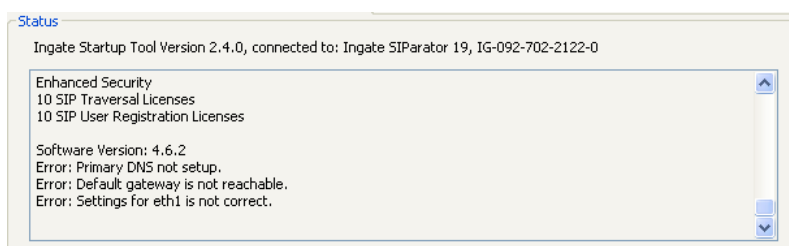
### Possible Problems and Resolutions

Possible Problems	Possible Resolution
Ingate Unit is not Turned On.	Turn On or Connect Power
Incorrect IP Address	Check the IP Address using a Web Browser.
Incorrect Password	Check the Password.
Despite your best efforts...	<ol style="list-style-type: none"> <li>1. Since this process uses the Web (http) to access the Ingate Unit, it should seem that any web browser should also have access to the Ingate Unit. If the Web Browser works, then the Startup Tool should work.</li> <li>2. If the Browser also does not have access, it might be possible the PC's IP Address does not have connection privileges in “Access Control” within the Ingate. Try from a PC that have access to the Ingate Unit, or add the PC's IP Address into “Access Control”.</li> </ol>



## 5.1.4 Network Topology

There are several possible error possibilities here, mainly with the definition of the network. Things like IP Addresses, Gateways, NetMasks and so on.

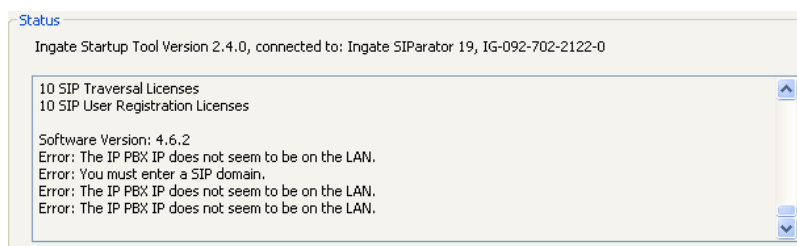


### Possible Problems and Resolutions

Possible Problems	Possible Resolution
Error: Default gateway is not reachable.	The Default Gateway is always the way to the Internet, in the Standalone or Firewall it will be the Public Default Gateway, on the others it will be a Gateway address on the local network.
Error: Settings for eth0/1 is not correct.	IP Address of Netmask is in an Invalid format.
Error: Please provide a correct netmask for eth0/1	Netmask is in an Invalid format.
Error: Primary DNS not setup.	Enter a DNS Server IP address

## 5.1.5 IP-PBX

The errors here are fairly simple to resolve. The IP address of the IP-PBX must be on the same LAN segment/subnet as the Eth0 IP Address/Mask.

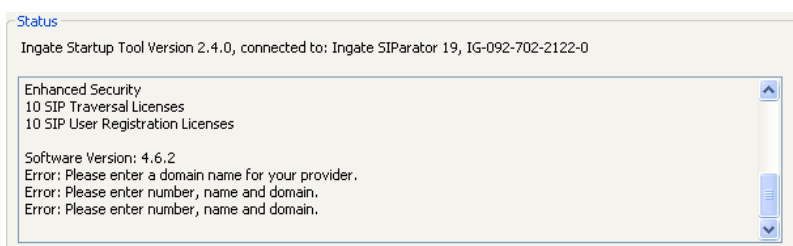


### Possible Problems and Resolutions

Possible Problems	Possible Resolution
Error: The IP PBX IP does not seem to be on the LAN.	The IP Address of the IP-PBX must be on the same subnet as the inside interface of the Ingate Eth0.
Error: You must enter a SIP domain.	Enter a Domain, or de-select "Use Domain"
Error: As you intend to use RSC you must enter a SIP domain. Alternatively you may configure a static IP address on eth1 under Network Topology	Enter a Domain or IP Address used for Remote SIP Connectivity. Note: must be a Domain when used with SIP Trunking module.

## 5.1.6 ITSP

The errors here are fairly simple to resolve. The IP address, Domain, and DID of the ITSP must be entered.



### Possible Problems and Resolutions

Possible Problems	Possible Resolution
Error: Please enter a domain name for your provider	Enter a Domain, or de-select “Use Domain”
Error: Please enter number, name and domain.	Enter a DID and Domain, or de-select “Use Account”

## 5.1.7 Apply Configuration

At this point the Startup Tool has pushed a database to the Ingate Unit, you have Pressed “Apply Configuration” in Step 3) of Section 4.7 Upload Configuration, but the “Save Configuration” is never presented. Instead after a period of time the following webpage is presented. This page is an indication that there was a change in the database significant enough that the PC could no longer web to the Ingate unit.



### Possible Problems and Resolutions

Possible Problems	Possible Resolution
Eth0 Interface IP Address has changed	Increase the duration of the test mode, press “Apply Configuration” and start a new browser to the new IP address, then press “Save Configuration”
Access Control does not allow administration from the IP address of the PC.	Verify the IP address of the PC with the Startup Tool. Go to “Basic Configuration”, then “Access Control”. Under “Configuration Computers”, ensure the IP Address or Network address of the PC is allowed to HTTP to the Ingate unit.

## 5.2 INGATE WEB GUI CONFIG

Configure your Ingate Firewall or Ingate SIParator to get basic network connectivity on all applicable interfaces. Please refer to the Reference Guide and other documentation as needed.

Remember to configure the following:

- Assign IP addresses on the inside and outside interface. For DMZ SIParators, use one interface only. (Network -> All Interfaces)
- Assign a default gateway. (Network -> Default Gateway)
- Assign a DNS server address. (Basic Configuration -> Basic Configuration)
- Define the IP subnet allowed to configure the Ingate and the interfaces to use for configuration. (Basic Configuration -> Access Control)

First make these basic settings and apply the configuration to have the unit working in your network environment. Then proceed with the following settings to get SIP Trunking to work with your service provider.

### 5.2.1 Network – Network and Computers

- Add a network for the Service Provider (ITSP IP). If you don't know the IP addresses used, you can put in 0.0.0.0 as lower limit and 255.255.255.255 as upper limit. In this way, requests from any IP address will be accepted.
- Add a network for the LAN (inside IP range).

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
ITSP_IP	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)	<input type="checkbox"/>
LAN	-	10.51.77.0	10.51.77.0	10.51.77.255	10.51.77.255	inside (eth0 untagged)	<input type="checkbox"/>
ShoreTel	-	10.51.77.20	10.51.77.20			-	<input type="checkbox"/>
WAN	-	0.0.0.0	0.0.0.0	127.0.0.0	127.0.0.0	outside (eth1 untagged)	<input type="checkbox"/>
	-	127.0.0.2	127.0.0.2	255.255.255.255	255.255.255.255	outside (eth1 untagged)	<input type="checkbox"/>

### 5.2.2 Basic Configuration – SIParator Type (SIParator Only)

Use the appropriate SIParator configuration for your deployment.

**Type of SIParator** [\(Help\)](#)

The SIParator can be connected to your network in three different ways, depending on your needs.

SIParator type:

DMZ

Save Undo

## 5.2.3 SIP Service – Basic

- SIP Module: On.

The screenshot shows the configuration page for SIP Service – Basic. The top navigation bar includes Administration, Basic Configuration, Network, SIP Services (highlighted), SIP Traffic, Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. The sub-navigation bar includes Basic (highlighted), Signaling Encryption, Media Encryption, Interoperability, Sessions and Media, Remote SIP Connectivity, VoIP Survival, and VoIP Survival Status. The main content area is titled 'SIP Module (Help)' and shows 'SIP module:  On  Off'. Below this are three sections: 'Additional SIP Signaling Ports (Help)' with a table for Port, Transport, Comment, and Delete, and an 'Add new rows' button; 'SIP Logging (Help)' with four dropdown menus for log classes; and 'SIP Media Port Range (Help)' with input fields for Ports (58024 - 60999).

## 5.2.4 SIP Service – Interoperability

1. URI Encoding – Use shorter, encrypted URI
2. Signaling Order of Re-INVITES – Send response before re-INVITE are forwarded
3. Public IP address for NATed SIParator – Only in DMZ, DMZ/LAN, and LAN configurations, assign the External Firewall Public IP address

The screenshot shows the configuration page for SIP Service – Interoperability. The top navigation bar is the same as in the previous screenshot. The sub-navigation bar includes Basic, Signaling Encryption, Media Encryption, Interoperability (highlighted), Sessions and Media, Remote SIP Connectivity, VoIP Survival, and VoIP Survival Status. The main content area is titled 'URI Encoding (Help)' and shows 'Recommended setting: Always encrypt URIs' with radio buttons for 'Always encrypt URIs', 'Use shorter, encrypted URIs' (selected), 'Escape URIs', and 'Keep username in URIs'. Below this is 'Signaling Order of Re-INVITES (Help)' with 'Recommended setting: Send re-INVITES all the way directly' and radio buttons for 'Send re-INVITES all the way directly' and 'Send response before re-INVITES are forwarded' (selected). At the bottom is 'Public IP address for NATed SIParator (Help)' with the note 'This setting is not supported for the Standalone configuration.' and a table with columns for 'DNS Name or IP Address' and 'IP Address'.

## 5.2.5 SIP Traffic – Filtering

1. Under Proxy Rules, change the Default Policy for SIP Requests to “Process All”.
2. Content Type: Add \*/\* and Allow - ON

The screenshot shows the configuration interface for SIP Traffic Filtering. The top navigation bar includes 'Administration', 'Basic Configuration', 'Network', 'SIP Services', 'SIP Traffic' (selected), 'Failover', 'Virtual Private Networks', 'Quality of Service', and 'Logging and Tracing'. Below this, sub-menus for 'SIP Methods', 'Filtering' (selected), 'User Database', 'Authentication and Accounting', 'Dial Plan', 'Routing', 'Time Classes', and 'SIP Status' are visible. The main content area is divided into three sections: 'Proxy Rules', 'Header Filter Rules', and 'Content Types'. In the 'Proxy Rules' section, a table shows 1 row with columns for 'No.', 'From Network', 'Action', and 'Delete'. The 'Default Policy For SIP Requests' is set to 'Process all' (selected), with 'Local only' and 'Reject all' as options. The 'Header Filter Rules' section also shows 1 row and has 'Process' selected as the 'Default Header Filter Policy'. The 'Content Types' section shows a table with 1 row for 'Content Type' \*/\* and 'Allow' set to 'On'.

## 5.2.6 SIP Traffic – User Database

Configure an account with details as provided from the ITSP.

## 5.2.7 SIP Traffic – Routing

- Local REFER handling: check Always handle REFER locally.

The configuration of the Ingate is now done and the changes must be applied on the Administration page to take effect. Note: This can also be done dynamically using the Dial Plan with a Regular Expression in the Forward To, with an expression that looks like “sip:\$1@10.51.77.20;b2bua”, the “;b2bua” indicates to the Ingate to use the Local REFER handling.

The screenshot shows the configuration interface for SIP Traffic Routing. The top navigation bar is the same as in the previous screenshot. The sub-menu 'Routing' is selected. The main content area is titled 'Local REFER Handling'. It contains a checked checkbox for 'Always handle REFER locally' and three unchecked checkboxes: 'For clients not supporting REFER', 'For clients not supporting replaces', and 'For dialogs with specified From URI'. Below this is a section titled 'From URIs For Which REFER is Handled Locally' with a table containing one row with columns for 'URI' and 'Delete'.

## 5.2.8 SIP Traffic – Dial Plan

Configure the Dial Plan according to the picture below.

Administration
Basic Configuration
Network
SIP Services
SIP Traffic
Failover
Virtual Private Networks
Quality of Service
Logging and Tools
About

SIP Methods
Filtering
User Database
Authentication and Accounting
Dial Plan
Routing
Time Classes
SIP Status

**Use Dial Plan** [\(Help\)](#)

On  
 Off  
 Fallback

**Emergency Number** [\(Help\)](#)

911

**Matching From Header** [\(Help\)](#)

Name	Use This ...		... Or This	Transport	Network	Delete
	Username	Domain	Reg Expr			
Generic ITSP	*	*		UDP	ITSP_IP	<input type="checkbox"/>
LAN	*	*		UDP	LAN	<input type="checkbox"/>
ShoreTel	*	*		UDP	ShoreTel	<input type="checkbox"/>
WAN	*	*		Any	WAN	<input type="checkbox"/>

Add new rows  rows.

**Matching Request-URI** [\(Help\)](#)

Name	Use This ...				... Or This	Delete
	Prefix	Head	Tail	Min. Tail	Domain	
Inbound			any character		123.123.123.123	<input type="checkbox"/>
Outbound			any character		10.51.77.100	<input type="checkbox"/>

Add new rows  rows.

**Forward To** [\(Help\)](#)

Name	Subno.	Use This ...	... Or This			... Or This	Delete
		Account	Replacement URI	Port	Transport	Reg Expr	
Generic ITSP	1	-			-	sip:\$1@12.12.12.	<input type="checkbox"/>
ShoreTel	1	-			-	sip:\$1@10.51.77.	<input type="checkbox"/>

Add new rows  groups with  rows per group.

**Dial Plan** [\(Help\)](#)

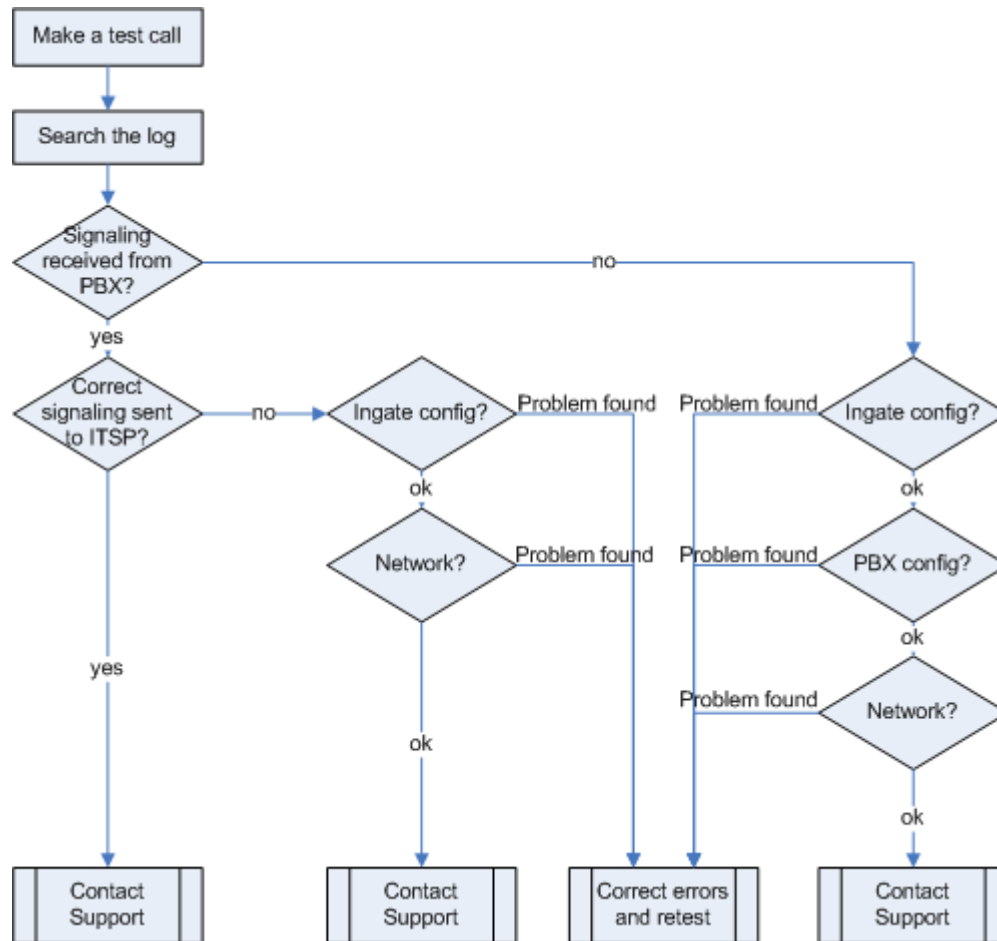
No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM
					Forward	ENUM	
1	ShoreTel	Outbound	Forward	Generic ITSP			-
2	Generic ITSP	Inbound	Forward	ShoreTel			-
3	WAN	-	Reject	-			-

## 5.3 USING THE INGATE FOR TROUBLESHOOTING

### 5.3.1 Troubleshooting Outbound Calls

**Symptom:** When trying to make a call from an internal ShoreTel extension to PSTN, there is no ringing signal on the PSTN phone.

**Note:** If you get a ringing signal on the PSTN phone, these troubleshooting steps will not help you to find the problem. Please contact your sales representative for support.

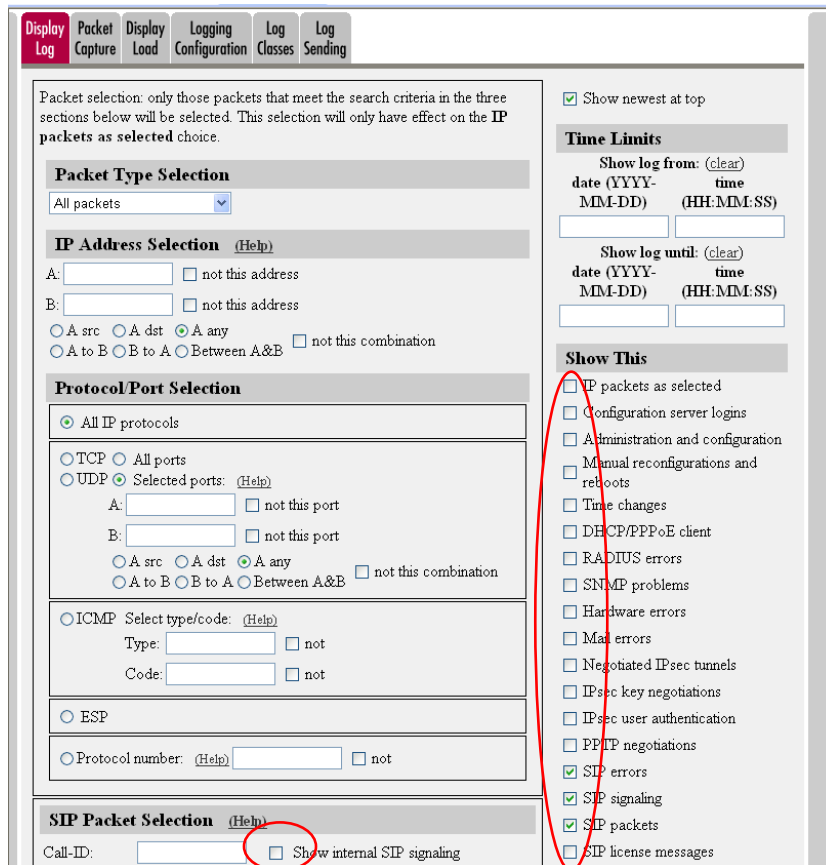


#### Outbound traffic troubleshooting overview

##### Get a log for the failing call:

First try to make a call to a PSTN number from a ShoreTel phone and notice the behavior on the ShoreTel phone as well as on the PSTN phone.

Next step is to search the log on the Ingate. Log in to the Ingate box and navigate to the Display Log page. Make necessary settings on this page according to the picture below. Especially make sure that you have the highlighted checkboxes in the correct state.



Then press “Display log” further down on the same page.

You will now see a log of all SIP packets received and sent by the Ingate, with the newest log entry on the top.

Ensure the signaling is received from the ShoreTel:

Localize the call initiation from the ShoreTel by searching for “invite sip” in your browser. You should look for the first packet coming from the ShoreTel system that starts with a “recv from <IP address of the ShoreGear switch>” as you can see in the example (only the first lines of the log messages are shown here).

```
>>> Info: sipfw: recv from 10.100.0.40:5060 via UDP connection 12746:
      INVITE sip:16037914522@10.100.0.13:5060 SIP/2.0
```

If you cannot find a packet like the one above, the problem is in the communication from Shoregear to the Ingate. Follow these steps:

1. Make sure the Ingate SIP module is turned on, SIP Services – SIP Module – On. Retest if you change any setting.
2. Make sure the ShoreTel configuration is correct. Check the IP address pointing at Ingate one extra time. Retest if you change any setting.
3. Make sure there is IP connectivity between the ShoreTel and Ingate. Contact your network administrator for assistance if needed.

If none of the steps above solves the problem, contact your sales representative for support.



Ensure the signaling to the ITSP works:

If you find the incoming packet, you should find a similar packet leaving the Ingate just above (just after in time) the incoming packet. The first rows of the outgoing packet will look something like this:

```
>>> Info: sipfw: send sf (0x8422820) to 208.49.124.49:5060 via UDP connection 12748:
```

```
INVITE sip:16037914522@208.49.124.49:5060;transport=udp SIP/2.0
```

If you don't see the outgoing packet, something is probably wrong with the Ingate configuration or you lack Internet connectivity:

1. Make sure that the Ingate is configured correctly.
2. Make sure the IP connectivity between the Ingate and the ITSP is working. Contact your network administrator for assistance if needed.

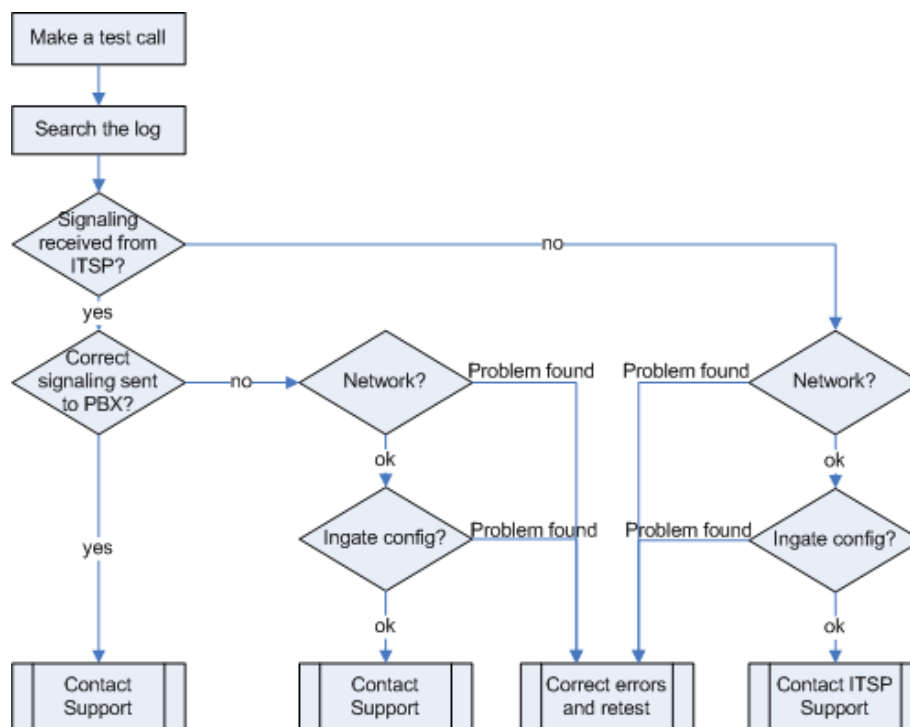
If you see a packet sent from the Ingate, verify that it is sent to the IP address provided by the ITSP. If not, correct your configuration and retest.

If none of the steps above solves the problem, contact your sales representative for support.

### 5.3.2 Troubleshooting Inbound Calls

**Symptom:** When trying to make an inbound call to a ShoreTel phone via the SIP Trunk there is no ringing signal on the ShoreTel phone.

**Note:** If you get a ringing signal on the ShoreTel phone, these troubleshooting steps will not help you to find the problem. Please contact your sales representative for support.



## Get a log for the failing call:

First try to make a call to a ShoreTel phone from a PSTN phone and notice the behavior on the ShoreTel phone as well as on the PSTN phone.

Next step is to search the log on the Ingate. Log in to the Ingate box and navigate to the Display Log page. Make necessary settings on the logging page according to the picture below. Especially make sure that you have the highlighted checkboxes in the correct state.

Packet selection: only those packets that meet the search criteria in the three sections below will be selected. This selection will only have effect on the IP packets as selected choice.

**Packet Type Selection**  
All packets

**IP Address Selection (Help)**  
A:   not this address  
B:   not this address  
 A src  A dst  A any  
 A to B  B to A  Between A&B  not this combination

**Protocol/Port Selection**  
 All IP protocols  
 TCP  All ports  
 UDP  Selected ports: (Help)  
A:   not this port  
B:   not this port  
 A src  A dst  A any  
 A to B  B to A  Between A&B  not this combination

ICMP Select type/code: (Help)  
Type:   not  
Code:   not

ESP

Protocol number: (Help)   not

**SIP Packet Selection (Help)**  
Call-ID:   Show internal SIP signaling

Show newest at top

**Time Limits**  
Show log from: (clear)  
date (YYYY-MM-DD) time (HH:MM:SS)  
   
Show log until: (clear)  
date (YYYY-MM-DD) time (HH:MM:SS)

**Show This**  
 IP packets as selected  
 Configuration server logins  
 Administration and configuration  
 Manual reconfigurations and reboots  
 Time changes  
 DHCP/PPPoE client  
 RADIUS errors  
 SNMP problems  
 Hardware errors  
 Mail errors  
 Negotiated IPsec tunnels  
 IPsec key negotiations  
 IPsec user authentication  
 PPP negotiations  
 SIP errors  
 SIP signaling  
 SIP packets  
 SIP license messages

Then press “Display log” further down on the same page.

You will now see a log of all SIP packets received and sent by the Ingate, with the newest log entry on the top.

### Ensure the signaling is received from the ITSP:

Localize the call initiation from the Trunking provider by searching for “invite sip” in your browser. (use Ctrl-F). You should look for the first packet coming from the ITSP system that starts with a “recv from <IP address of the ITSP>” as you can see in the example (only the first lines of the log are shown below).

```
>>> Info: sipfw: rcv from 208.49.124.49:5060 via UDP connection 12748:  
INVITE sip:6023574058;npdi=yes@193.12.253.37:5060 SIP/2.0
```

If you cannot find a packet like the one above, the problem is in the communication from the ITSP to the Ingate. Follow these steps:

1. Make sure you have IP connectivity between the Ingate and your ITSP. Contact your network administrator for assistance if needed

2. Make sure the Ingate SIP module is turned on, SIP Services – SIP Module – On.  
Retest if you change any setting.

If you still don't see any packets in the log, contact your ITSP for further troubleshooting.  
Ensure correct signaling to the ShoreTel PBX:

If you find the incoming packet, you should find a similar packet leaving the Ingate just above (just after in time) the incoming packet. The first lines of the outgoing packet will look something like this:

```
>>> Info: sipfw: send sf (0x8419848) to 10.100.0.40:5060 via UDP connection 12746:  
INVITE sip:6023574058;npdi=yes@10.100.0.40:5060;transport=udp SIP/2.0
```

If you don't see the outgoing packet, something is probably wrong with the Ingate configuration or you might lack a connection to your LAN where the ShoreTel is located:

1. Ensure you have IP connectivity between ShoreTel and the Ingate. Contact your network administrator for assistance if needed.
2. Make sure your Ingate is configured correctly.

If you see the outgoing packet, make sure the IP address it is sent to is the one used by the Shoregear switch.

If the call still fails after executing the steps described above, please contact your sales representative for support.