NetVanta Unified Communications Technical Note

Configuring the NetVanta Unified Communications ITSP

1 Introduction

This technical note provides guidelines for configuring the NetVanta Unified Communications Server in combination with the Ingate SIParator and ITSPs that provide SIP trunking capabilities. For details on UC server configuration please refer to the NetVanta technical documentation. Likewise, for details on the Ingate configuration refer to the Ingate reference documentation.

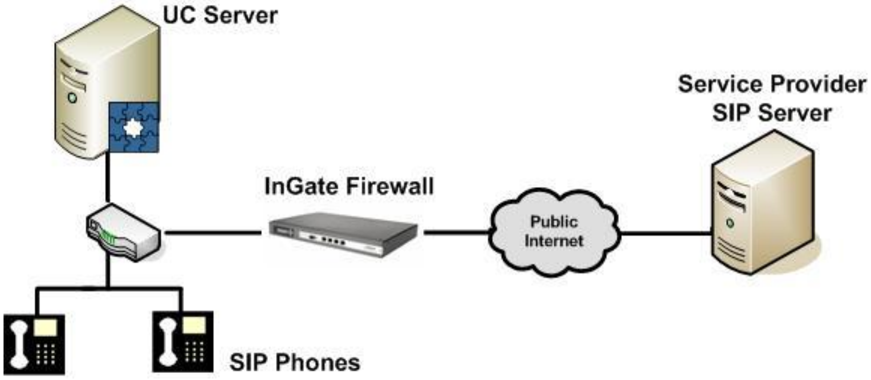
Ingate has a number of SIP-aware firewall (SIP ALG) products. Although all the Ingate Firewalls are NAT firewalls and SIP protocol Application Layer Gateways (ALGs) ADTRAN recommends using the **SIParator** product in **Standalone** mode. The SIParator is used in UC server installations to provide SIP connectivity between the UC server and ITSPs. The number of SIP traversals supported by the Ingate gateway is dependent on the number of traversals purchased but may be upgraded in the field.

1.1 Minimum Requirements

Participants	**Version**
Validated ITSPs	See 0
Ingate SIParator	4.8.1 SIP Trunking Module
Ingate Startup Tool	2.4.2
NetVanta UC Server	4.2.0 or higher (note that because this guide covers a number of the UC server releases the configuration diagrams may not look identical to a live system)

2 Typical SIP Trunking Network Diagram

The main application for UC server SIP Trunking is to provide VoIP telephony services for PSTN access for enterprise networks over IP. Below is a typical diagram showing a SIP Trunking application to a carrier or service provider.



3 NetVanta Unified Communications Server

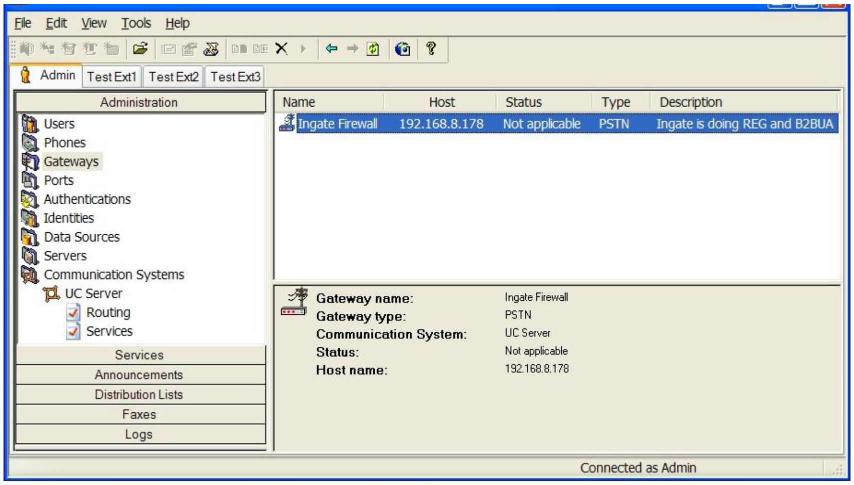
This section provides configuration guidelines for the UC server as it applies to the SIP Trunking application. It highlights the recommended settings to allow for a SIP Trunking call to traverse the Ingate from the SIP Trunking perspective.

3.1 Configuring SIP Trunking

An ITSP gateway may be added in the initial configuration of the UC server or in the Gateway view of the Administration section of UC Client. The following sections explain how to set up an ITSP gateway on the UC server.

To start the Add Gateway Wizard

1. From the Gateway view on the UC Client select **New Gateway** to begin configuring the Ingate SIParator.



Name	Host	Status	Type	Description
Ingate Firewall	192.168.8.178	Not applicable	PSTN	Ingate is doing REG and B2BUA

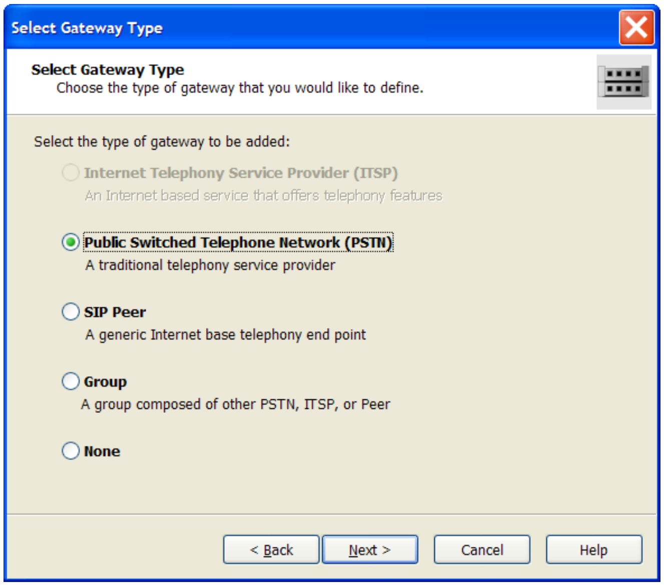
Gateway name: Ingate Firewall
Gateway type: PSTN
Communication System: UC Server
Status: Not applicable
Host name: 192.168.8.178

The Add Gateway Wizard starts.

2. Click **Next** to add the Ingate SIParator.

3.1.1 Select Gateway Type

- In the Add Gateway Wizard there are several options to choose from; for SIP Trunking, select **Public Switched Telephone Network (PSTN)**.



Select Gateway Type
Choose the type of gateway that you would like to define.

Select the type of gateway to be added:

○ **Internet Telephony Service Provider (ITSP)**
An Internet based service that offers telephony features

● **Public Switched Telephone Network (PSTN)**
A traditional telephony service provider

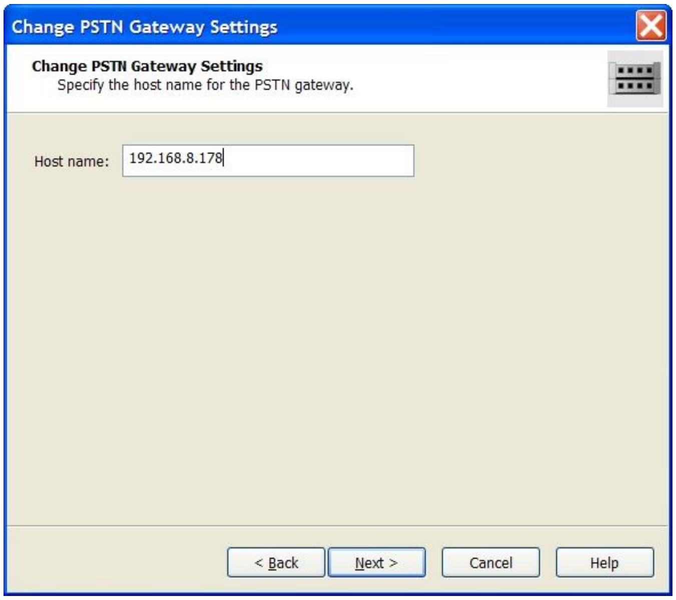
○ **SIP Peer**
A generic Internet base telephony end point

○ **Group**
A group composed of other PSTN, ITSP, or Peer

○ **None**

3.1.2 Ingate Firewall Location

In the Host name field, enter the IP address or domain name (if it has been defined in DNS) of the Ingate Firewall/SIParator.



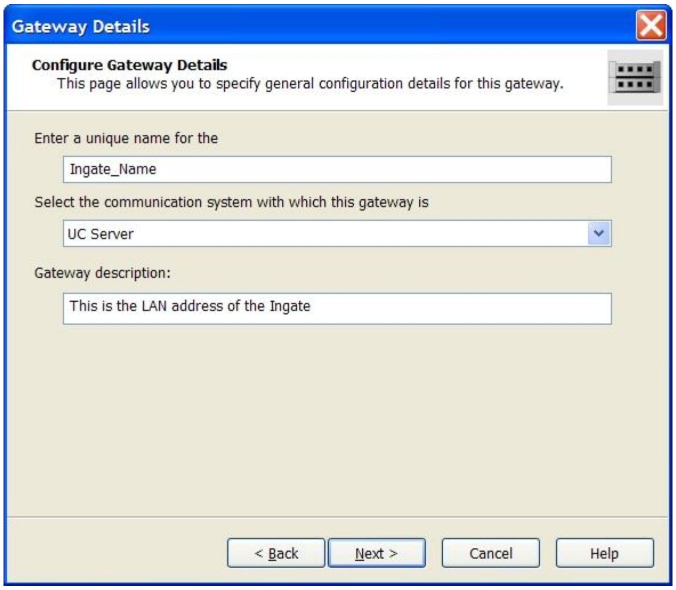
Change PSTN Gateway Settings

Change PSTN Gateway Settings
Specify the host name for the PSTN gateway.

Host name: 192.168.8.178

3.1.3 Ingate Details

Enter a unique name and any description required.



Gateway Details

Configure Gateway Details
This page allows you to specify general configuration details for this gateway.

Enter a unique name for the
Ingate_Name

Select the communication system with which this gateway is
UC Server

Gateway description:
This is the LAN address of the Ingate

3.2 Other UC Server Documentation References

To complete the configuration for the ITSP two more items are required: an **Identity** (typically an extension number) to answer incoming calls and a **Routing–Dial Plan entry** to direct outgoing calls to the ITSP. Please refer to the *NetVanta Unified Communications Server Administrator Guide*, available online at *http://kb.adtran.com*, for details regarding these features.

The outgoing routing dial plan entry is the same type as that used for routing PSTN calls to a SIP to PSTN gateway. In many cases all that must be done is to change the gateway that is referenced in the 7+ and 11+ dial plan entries. Special attention must be paid, however, to the identity to which incoming ITSP calls are directed. Please see 0for details on specific ITSPs.

3.2.1 Administrator Guide - Section 3.7 - Managing identities

Using the Identities view, you can create a new user, attendant, or group identity. An identity, which is defined as a dial-able entity, corresponds to any of the following: user extension, auto-attendant, or e-mail address. An ITSP can dial the attendant identity to connect a caller directly to an auto-attendant. When callers dial in to the system they can access, for example, a user extension, the auto-attendant, or a hunt group.

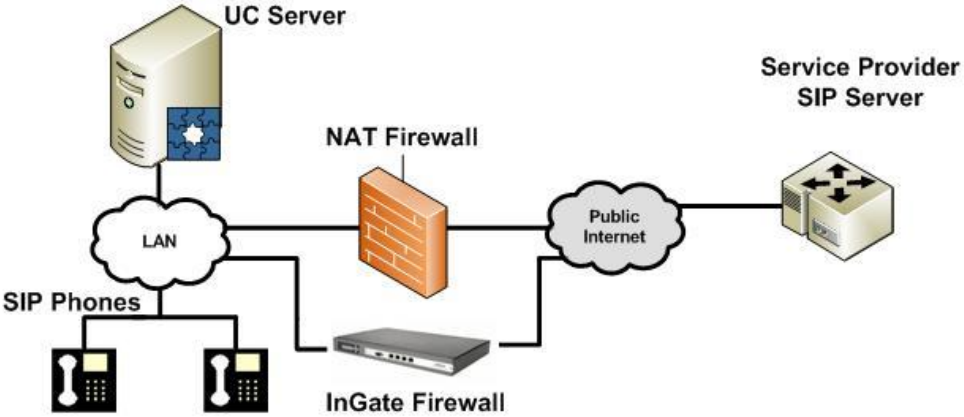
3.2.2 Administrator Guide - Section 3.10 - Managing communication systems

The dial plan is used to route calls. Dial plans may be assigned to an ISTP gateway or a host. Adding digits to the dial plan allows for the specification of a range of numbers, attendant line, or other set of digits. Dialing plan digits are managed using regular expressions. Regular expressions are a flexible way of delivering patterns that are a match. For example, if you specify the regular expression [0-9]{7,}, the UC server recognizes any digits from zero to nine, repeated a maximum of seven times, in other words, a regular local telephone number.

4 Ingate SIParator

This section provides general guidelines for the Ingate SIParator products as they apply to UC server connectivity to ITSP SIP Trunking. For more details about the Ingate SIParator configuration, please refer to the Ingate reference documentation. ADTRAN recommends installing the SIParator in **Standalone** mode and configuration information for this mode is given below. In this configuration, the SIParator must have a public IP address on one Ethernet interface, while the rest of the Ethernet interfaces are connected to the internal network. In this configuration, no changes are needed to the traditional firewall.

For background information on other modes refer to *Appendix B Ingate Manual Configuration*.



The recommended configuration procedure is to start with the Ingate Startup Tool which, with the proper choice of ITSP, will fully configure the gateway for ITSP operation. Details are provided, however, in Appendix B on how to manually configure the Ingate gateway through its webpage.

4.1 Ingate Startup Tool

The Ingate Startup Tool is an installation tool for Ingate products using the Ingate SIP Trunking software module or the Remote SIP Connectivity module, which facilitates the setup of complete SIP trunking solutions or remote user solutions.

The tool automatically configures a user's Ingate to work with the UC server and a SIP Trunking service. The configuration tool automatically creates a SIP trunk connection designed to the user's individual setup.

Note: There are site-specific requirements that may require manual programming. See *Appendix B Ingate Manual Configuration* for manual programming instructions.

The Startup Tool can also be used for the Remote SIP Connectivity module because it sets up all the routing needed to enable remote users to access and use the enterprise IP-PBX.

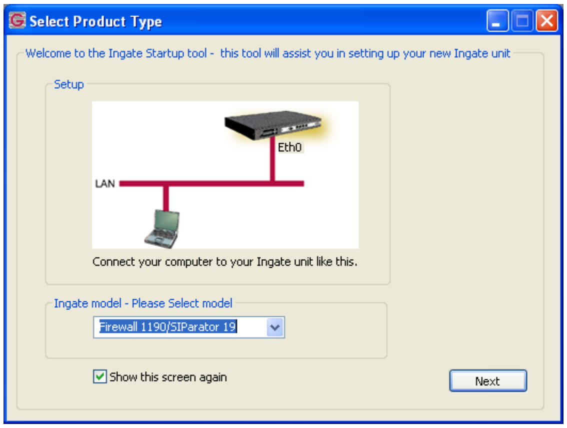
The startup tool can be downloaded from *http://www.ingate.com/startuptool.php*.

4.1.1 Establish Contact (Step 1 of 4)

The first step of this Quick Start Tool is to establish a connection with the Ingate unit.

To launch the Quick Start Tool

1. Select the product type Firewall 1190/SIParator 19 and select Next.



Select Product Type

Welcome to the Ingate Startup tool - this tool will assist you in setting up your new Ingate unit

Setup

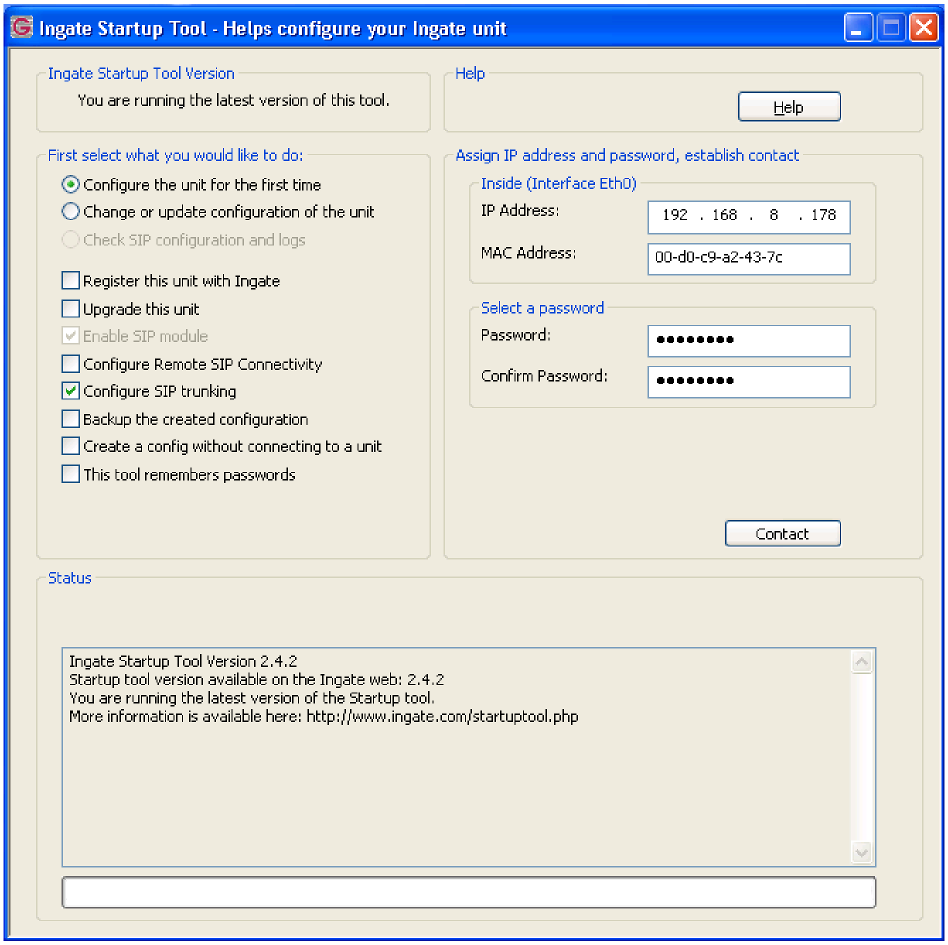
Connect your computer to your Ingate unit like this.

Ingate model - Please Select model

Firewall 1190/SIParator 19

☑ Show this screen again

2. On the next screen enter the IP address and MAC address of the LAN (inside) Interface.
3. Enter the username and password for the Ingate that you would like to use.
4. Click Contact, and check the status of the connection.



Ingate Startup Tool - Helps configure your Ingate unit

Ingate Startup Tool Version

You are running the latest version of this tool.

Help

First select what you would like to do:

● Configure the unit for the first time
○ Change or update configuration of the unit
○ Check SIP configuration and logs

□ Register this unit with Ingate
□ Upgrade this unit
☑ Enable SIP module
□ Configure Remote SIP Connectivity
☑ Configure SIP trunking
□ Backup the created configuration
□ Create a config without connecting to a unit
□ This tool remembers passwords

Assign IP address and password, establish contact

Inside (Interface Eth0)

IP Address: 192 . 168 . 8 . 178

MAC Address: 00-d0-c9-a2-43-7c

Select a password

Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

Status

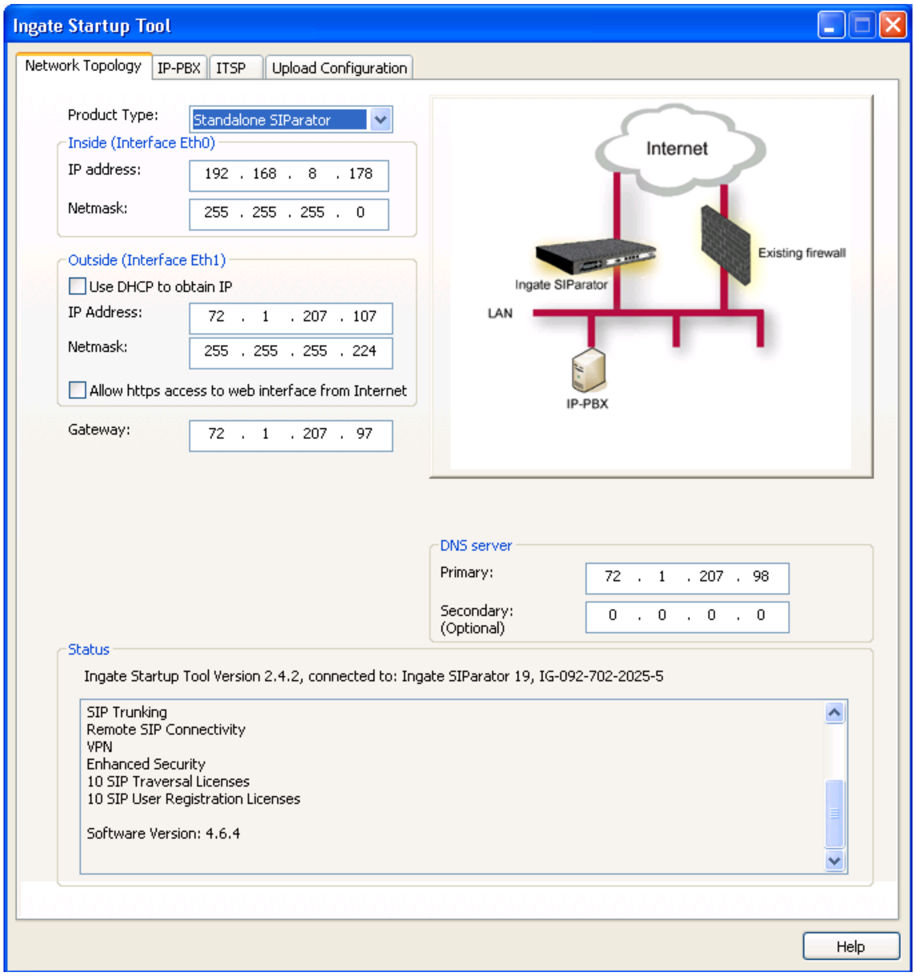
```
Ingate Startup Tool Version 2.4.2
Startup tool version available on the Ingate web: 2.4.2
You are running the latest version of the Startup tool.
More information is available here: http://www.ingate.com/startuptool.php
```

4.1.2 Configure Network Topology (Step 1 of 4)

- Select the Network Topology tab.

Configuration Steps

1. Select the Standalone SIParator Product Type.
2. Enter the IP Address of the LAN (inside) interface and the Netmask for the SIParator.
3. Enter the IP Address of the WAN (outside) interface and the Netmask.
4. Enter the Default Gateway (WAN) IP Address.
5. Enter the IP address of the Primary DNS Server (WAN). If available enter the IP address of the Secondary DNS Server.



Product Type: Standalone SIParator

Inside (Interface Eth0)

IP address: 192 . 168 . 8 . 178

Netmask: 255 . 255 . 255 . 0

Outside (Interface Eth1)

□ Use DHCP to obtain IP

IP Address: 72 . 1 . 207 . 107

Netmask: 255 . 255 . 255 . 224

□ Allow https access to web interface from Internet

Gateway: 72 . 1 . 207 . 97

DNS server

Primary: 72 . 1 . 207 . 98

Secondary: (Optional) 0 . 0 . 0 . 0

Status

Ingate Startup Tool Version 2.4.2, connected to: Ingate SIParator 19, IG-092-702-2025-5

SIP Trunking
Remote SIP Connectivity
VPN
Enhanced Security
10 SIP Traversal Licenses
10 SIP User Registration Licenses

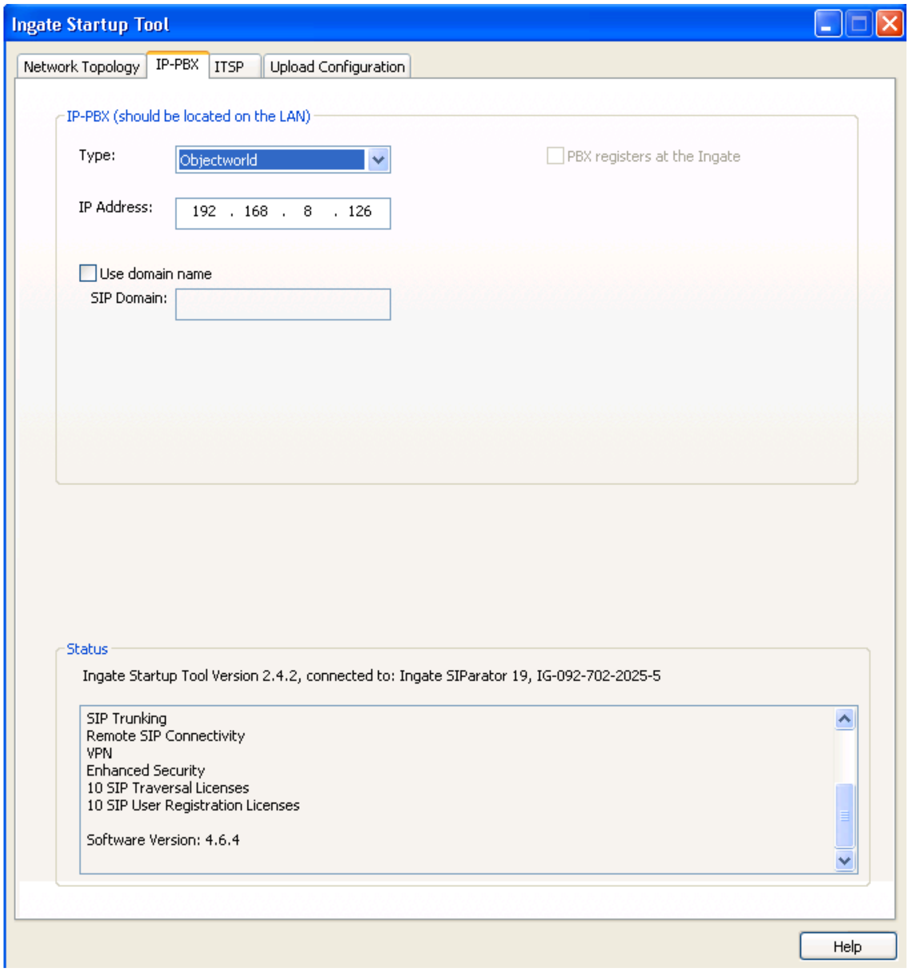
Software Version: 4.6.4

4.1.3 Configure UC Server Information (Step 2 of 4)

- Select the IP-PBX tab to define the connection to the UC server.

Configuration Steps

1. Select NetVanta as the PBX Type.
2. Enter the LAN IP Address of the UC server.



Type: Objectworld

IP Address: 192 . 168 . 8 . 126

□ PBX registers at the Ingate

□ Use domain name

SIP Domain:

Ingate Startup Tool Version 2.4.2, connected to: Ingate SIParator 19, IG-092-702-2025-5

```
SIP Trunking
Remote SIP Connectivity
VPN
Enhanced Security
10 SIP Traversal Licenses
10 SIP User Registration Licenses

Software Version: 4.6.4
```

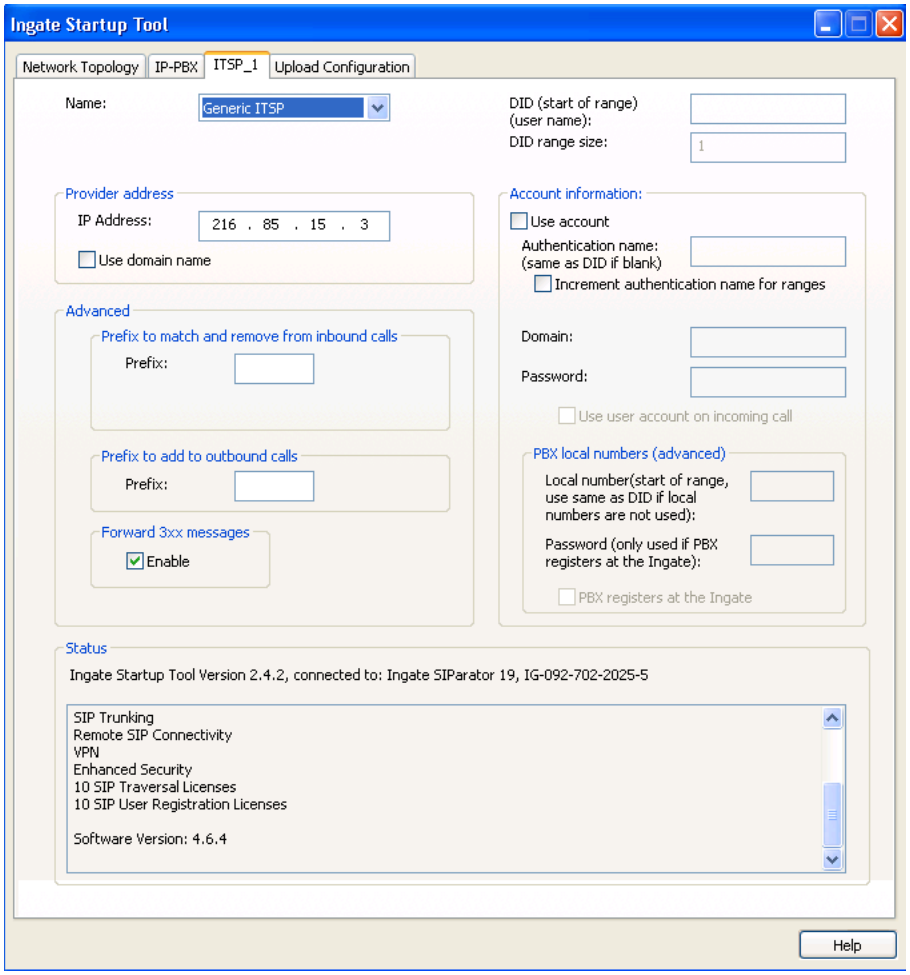
4.1.4 Configure ISTP Information (Step 3 of 4)

- Select the ITSP tab.

Note: If the ITSP provider cannot be selected refer to 0 for a list of ADTRAN supported ITSPs and how to configure them manually.

Configure the UC Server IP-PBX

1. From the Name drop-down list select the ITSP service provider.
2. The ITSP service provider information required varies. Fill in the fields with the information provided by the service provider.



Name: Generic ITSP

DID (start of range) (user name):

DID range size: 1

Provider address

IP Address: 216 . 85 . 15 . 3

□ Use domain name

Account information:

□ Use account

Authentication name: (same as DID if blank)

□ Increment authentication name for ranges

Domain:

Password:

□ Use user account on incoming call

Advanced

Prefix to match and remove from inbound calls

Prefix:

Prefix to add to outbound calls

Prefix:

Forward 3xx messages

☑ Enable

PBX local numbers (advanced)

Local number(start of range, use same as DID if local numbers are not used):

Password (only used if PBX registers at the Ingate):

□ PBX registers at the Ingate

Status

Ingate Startup Tool Version 2.4.2, connected to: Ingate SIParator 19, IG-092-702-2025-5

```
SIP Trunking
Remote SIP Connectivity
VPN
Enhanced Security
10 SIP Traversal Licenses
10 SIP User Registration Licenses

Software Version: 4.6.4
```

4.1.5 Load Configuration (Step 4 of4)

- Select the Upload Configuration tab.

Configure the UC Server IP-PBX

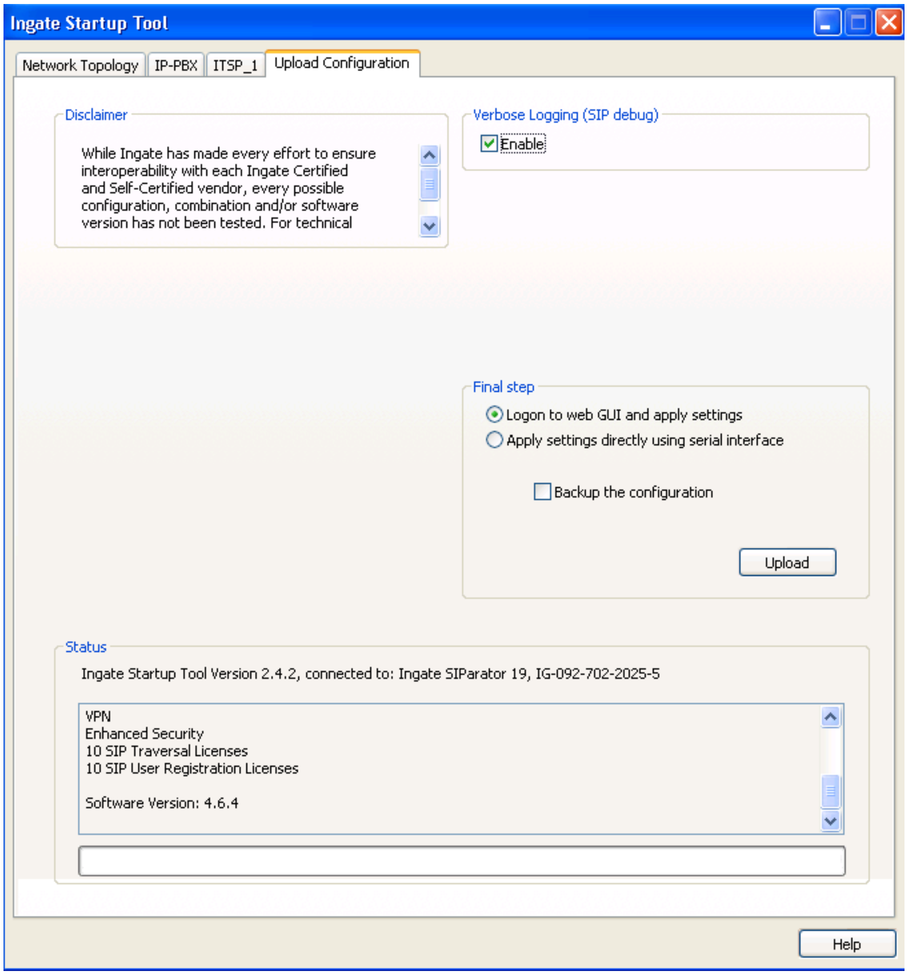
1. Click the Upload button to send the configuration information to the Ingate.
2. Log into the management configuration webpage using the LAN IP address specified above and ensure that the configuration changes have been applied.

Licenses

Make sure the Ingate has the following modules and licenses.

Installed modules:

- Standard SIP features
- SIP Trunking Module (this is a requirement in this configuration)



While Ingate has made every effort to ensure interoperability with each Ingate Certified and Self-Certified vendor, every possible configuration, combination and/or software version has not been tested. For technical

☑ Enable

● Logon to web GUI and apply settings
○ Apply settings directly using serial interface

□ Backup the configuration

Ingate Startup Tool Version 2.4.2, connected to: Ingate SIParator 19, IG-092-702-2025-5

```
VPN
Enhanced Security
10 SIP Traversal Licenses
10 SIP User Registration Licenses

Software Version: 4.6.4
```

Optional installed licenses:

- # SIP Traversal Licenses - Determines a value for the maximum number of simultaneous SIP Trunking calls

4.2 SIP Trunking Module License

If the licenses are not already installed, please follow the instructions below to activate licenses for the Ingate unit. Located along with the UC server Purchase Key is the Ingate SIP Trunking Module License Code. This License Code is used to download an activation key from the Ingate website. This code unlocks the SIP Trunking Module on the Ingate product.

To activate a license code

1. To register with Ingate and activate a license code, log on to *www.ingate.com* and choose “Support.”

2. If you have not already, register the unit by selecting "Register Account."
3. Complete the Registration process.
4. To apply the License code, choose "Login for Upgrades, activation of licenses, user manuals and training."
5. In your account home page, choose the option "Activate Licenses."
6. Enter the Ingate license code provided upon purchasing your UC server.
7. Enter the serial number of the machine that you want associated with the license code.

The license code is now activated.

8. If you purchased a license, a key file is downloaded that you need to upload to your firewall/SIParator.
9. In such case, login into your Firewall/SIParator and upload the key file on the "Upgrade" page. Press upgrade.

4.3 Other Considerations

Once the configuration is complete using the Startup Tool the system should be able to handle incoming and outgoing calls. There are however two issues that must be considered beyond the Startup Tool configuration. If changes are required they must be done manually through the Ingate web page by pointing a web browser to the LAN IP address of the Ingate and entering the defined user name and password.

4.3.1 Toll Fraud

Some of the important features of the UC server require incoming PSTN calls to be redirected back out to the PSTN. For this reason outgoing calls to the PSTN cannot be toll restricted based on source since there is no advance knowledge of who will be forwarded back out to the PSTN. This creates an opening for toll fraud if security is not carefully considered.

With the default configuration of the Ingate only incoming calls from the ITSP are accepted and routed to a UC server application. Unless teleworkers are to be supported no changes are required.

4.3.2 Teleworkers

If support for teleworkers is required, then consult *Configuring NetVanta Unified Communications for Telecommuters* technical note, available online at *http://kb.adtran.com*.

4.3.3 Outgoing Calling Names & Numbers

Many PSTN users have a service that allows them to see the name and number of who is calling. If the call is originated from an analog trunk then the carrier takes care of the generation of that information. If the originator is digital system then it is the responsibility of the customer premises equipment to generate that information.

4.3.3.1 Outgoing Calling Name

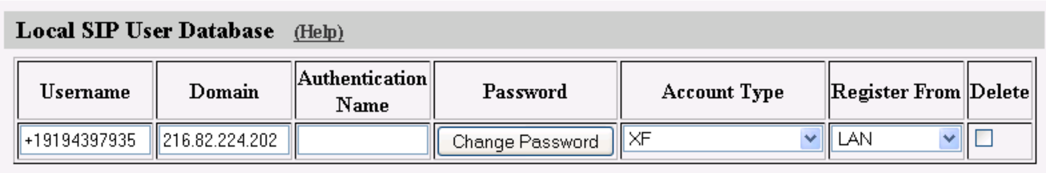
The name that is sent is the Display Name defined for the SIP user. For an ITSP account it is the Ingate that is communicating directly with the ITSP. There is no ability to define the Display Name, consequently Call Name cannot be provided for ITSP calls.

4.3.3.2 Outgoing Calling Number

The calling number for an ITSP call is taken from the "From" field on the SIP call. Since the Ingate is communicating directly with the ITSP the information must be programmed in the Ingate if this feature is required.

Some ITSPs require registration and some do not. In general if the ITSP requires registration then the calling number will already be configured. The following steps will ensure that the correct information is provided:

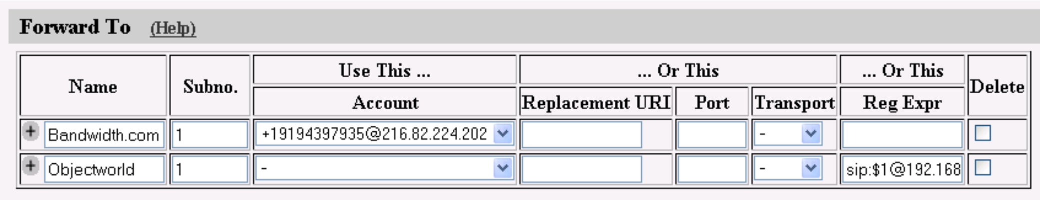
1. In **SIP Traffic** > **User Database** determine if there is an entry in the **Local SIP User Database** for the ITSP account. If there is not and the account the account should not require registration so create an account with the appropriate **Username** and **Domain** as provided by the ITSP. Choose XF as the **Account Type** and **Register From** the LAN.



Local SIP User Database (Help)

Username	Domain	Authentication Name	Password	Account Type	Register From	Delete
+19194397935	216.82.224.202		Change Password	XF	LAN	☐

2. In the **SIP Traffic** > **Dial Plan** Dial Plan table there is an entry which takes NetVanta calls and Forwards them to the ITSP. For the matching entry in the **Forward To** section delete the value in **Reg Expr** and instead choose the user account that has just been created in the drop down list for **Account.** The final result should appear like:



Forward To (Help)

Name	Subno.	Use This ...	... Or This			... Or This	Delete
		Account	Replacement URI	Port	Transport	Reg Expr	
+ Bandwidth.com	1	+19194397935@216.82.224.202			-		☐
+ Objectworld	1	-			-	sip:$1@192.168	☐

Note: if the regular expression that is deleted has a + sign at the beginning i.e., sip:\+ then modify the UC server dial plan so that calls being sent to the Ingate have a + inserted at the beginning of the dial string.

3. Click **Save, Apply**, and **Save**.

4.3.3.3 Multiple Outgoing Calling Numbers

If there is a requirement to have different outgoing calling numbers for different users than multiple accounts must have been arranged with the ITSP. For each user there must be an entry created in the **Matching From Header** section that matches their identity in the **Username** field. An equivalent entry in the **Forward To** section must be created that chooses the correct account number in the **Account** drop down field. Finally a route must be setup in the **Dial Plan** section to route the call.

This must be repeated for each user who requires their own outgoing phone number.

5 Fax Calls

T.38 is a standard for sending fax messages over IP networks in real time by encapsulating a standard T.30 fax data stream. UC server fax Services supports T.38 fax calls. The UC server can support simultaneous voice and fax calls, making and receiving both voice and fax calls from the UC server to the ITSP.

Not all ITSPs support T.38 fax. If it is a requirement the ITSP should be contacted to determine if faxing is supported.

Appendix A ITSPs

The following ITSPs have been successfully interoperability tested to work in conjunction with the UC server.

A.1. Bandwidth.com

With Ingate Startup Tool

To configure the SIP Trunking Provider

1. From the Trunking Provider from the list, select **"Bandwidth.com."**
2. Enter the Username, Password and Domain.
3. Enter a Primary and Secondary DNS Server.

Manual Configuration

User Database

Define the Bandwidth.com ITSP SIP Accounts, for Registration (type: XF/Register) and FROM Header replacement (type: XF) for Call Line Identification (CLI).

A.2. Bandtel

BandTel provides a document listing their connection information and your account details. Make sure you have the following information:

Required:

- SIP Trunking Server: proxy1.bandtel and proxy2.bandtel
- SIP Registrar: registrar.bandtel
- SIP Port: 5060
- The SIP Trunk Account Number (phone number) assigned by BandTel (usually starts with a 2)
- The Registration Authentication Username and Password
- SIP Domain: registrar.bandtel.com
- DNS Server: Primary - 65.175.129.140 Secondary - 66.237.65.68

With Ingate Startup Tool

To configure the SIP Trunking Provider

1. From the Trunking Provider from the list, select **"BandTel."**
2. Enter the Username, Password and Domain.
3. Enter a Primary and Secondary DNS Server.

Manual Configuration

User Database

Define the BandTel ITSP SIP Accounts, for Registration (type: XF/Register) and FROM Header replacement (type: XF).

A.3. Broadvox

Broadvox provides a document listing their connection information and the customer account details. The following information is required:

- The FQDN of Broadvox's SIP Trunking Server is psrv.labsip.broadvox.net or psrv.sip.broadvox.net
- The port number (default 5060) for the service provider's SIP Trunking Server
- The SIP Trunk Account Number (phone number) assigned by the service provider

With Ingate Startup Tool

To configure the SIP Trunking Provider

1. From the Trunking Provider from the list, select **"Broadvox"**.
2. Enter a Primary and Secondary DNS Server.

Manual Configuration

User Database

Define the Broadvox SIP Accounts, for Registration (type: XF/Register) and FROM Header replacement (type: XF) for Call Line Identification (CLI).

A.4. Vocal-Net

With Ingate Startup Tool

To configure the SIP Trunking Provider

1. Select **"Generic"** in the Trunking Provider from the drop down list.
2. Enter the Vocal-Net SIP Server IP Address (208.34.86.40) in the IP Address field.

Manual Configuration

User Database

Define the Vocal-Net ITSP SIP Accounts, Registration is not required for Vocal-Net and FROM Header replacement (type: XF) is used for Call Line Identification (CLI).

A.5. AGN Networks

With Ingate Startup Tool

To configure the SIP Trunking Provider

1. From the Trunking Provider from the list, select **“Generic.”**
2. Define the IP Address of the AGN Networks SIP Trunking Server, 64.95.245.15.
3. If required, enter the Username, Password and Domain.
4. If required, select “Use user account on incoming call” if the Ingate is required to REGISTER with the ITSP SIP trunking Provider.
5. Enter a Primary and Secondary DNS Server.

Manual Configuration

User Database

Define the AGN Networks SIP Accounts, for Registration (type: XF/Register) and FROM Header replacement (type: XF) for Call Line Identification (CLI).

A.6. Clarity Communications

With Ingate Startup Tool

To configure the SIP Trunking Provider

1. From the Trunking Provider from the list, select **“Generic.”**
2. Define the IP Address of the Clarity SIP Trunking Server (DNS sip.det01.clarityvoice.com).
3. Enter the Username, Password and Domain.
4. Select “Use user account on incoming call” if the Ingate is required to REGISTER with the ITSP SIP trunking Provider.
5. Enter a Primary and Secondary DNS Server.

Manual Configuration

User Database

Define the Clarity SIP Accounts, for Registration (type: XF/Register) and FROM Header replacement (type: XF) for Call Line Identification (CLI).

Appendix B Ingate Manual Configuration

B.1. Manual Configuration

The Ingate Startup Tool provides general configuration of the Ingate products. Because of site-specific requirements, additional programming is sometimes required. This section provides detailed programming instructions for all aspects of the Ingate product.

Note: This is a sample configuration and actual implementation may vary, depending on individual site requirements. Instructions are for both the Firewall and SIParator products, unless otherwise indicated.

B.2. Ingate SIParator versus Firewall

Ingate SIParators, are a Deny All firewall, and have no traditional firewall capabilities. They operate as an adjunct to an existing firewall and used as an outbound SIP proxy. In addition, the SIParator ensure that voice media streams traverse the SIParator rather than the default gateway router. The SIParator does an additional ALG traversal of the IP addresses contained in the SDP of the SIP signaling.

The Ingate Firewall and SIParator can be connected to your network in different ways, depending on the network requirements.

B.3. Preparation

Network Connectivity

Prior to any operation the Ingate Firewall/SIParator requires some basic information. Make sure you have the following information:

Required:

- The IP address or FQDN of the LAN and WAN Interfaces
- Default Gateway from Internet Service Provider (ISP)
- DNS Server address, if required

SIP Trunking

ITSPs provide documents listing their connection information and your account details. Make sure you have the following information:

Required:

- SIP Trunking Servers
- SIP Port
- The SIP Trunk Account Number (phone number) assigned by the ITSP

Note: T.38 Fax may or may not be supported by the ITSP.

B.4. Networks and Computers Definition

The network must be defined within the Ingate. It is important to note that you must clearly identify the WAN addressing and LAN addressing.

In the Network section, you can associate network addresses to specific Ethernet interfaces. This section will define the Lower Limit of the accessible network addresses, and then the Upper Limit of the accessible network addresses.

B.4.1. Defining WAN Networks

The Internet has every Class A, B and C type network addresses so setup WAN access to have a Lower Limit of 0.0.0.0 and an Upper Limit of 255.255.255.255. This ensures that all public IP addresses are accessible.

To define WAN access

1. Enter a Name for the Internet.
2. Enter the Lower limit of IP addresses for the Internet.
3. Enter the Upper limit of IP addresses for the Internet.
4. From the Interface/VLAN list, select the Ethernet Interface that is connected to the Internet.

B.4.2. Defining LAN Networks

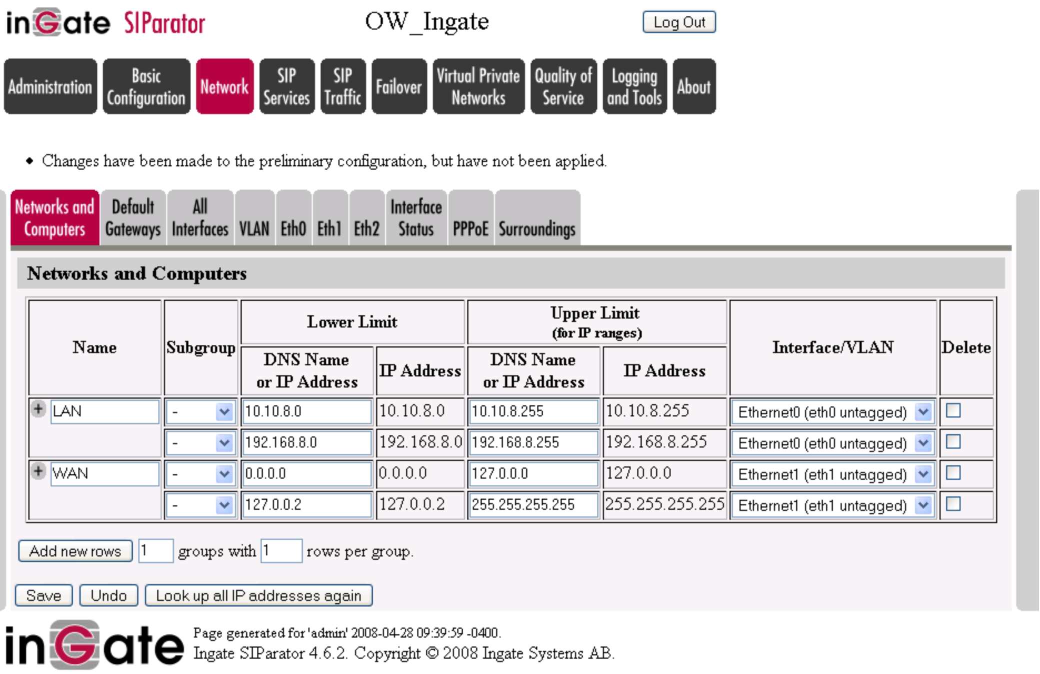
There are three classes for private addresses:

- Class A network IP address range = 10.0.0.0 - 10.255.255.255
- Class B networks IP address range = 172.16.0.0 - 172.31.255.255
- Class C network IP address range = 192.168.255.0 - 192.168.255.255

To direct traffic to the LAN segment, set up LAN access to have a Lower and Upper Limit of either the Class A, B, or C addresses. This ensures that all private IP addresses are accessible.

To define a LAN network

1. Enter a Name for the LAN.
2. Enter the Lower limit of IP addresses for the LAN.
3. Enter the Upper limit of IP addresses for the LAN.
4. From the Interface/VLAN list, select the Ethernet Interface that is connected to the LAN.



- Changes have been made to the preliminary configuration, but have not been applied.

Networks and Computers

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		
+ LAN	-	10.10.8.0	10.10.8.0	10.10.8.255	10.10.8.255	Ethernet0 (eth0 untagged)	□
	-	192.168.8.0	192.168.8.0	192.168.8.255	192.168.8.255	Ethernet0 (eth0 untagged)	□
+ WAN	-	0.0.0.0	0.0.0.0	127.0.0.0	127.0.0.0	Ethernet1 (eth1 untagged)	□
	-	127.0.0.2	127.0.0.2	255.255.255.255	255.255.255.255	Ethernet1 (eth1 untagged)	□

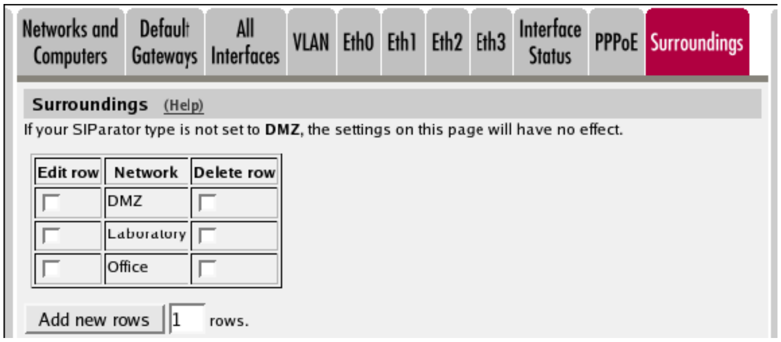
Add new rows 1 groups with 1 rows per group.

Save Undo Look up all IP addresses again

Page generated for 'admin' 2008-04-28 09:39:59 -0400.
Ingate SIParator 4.6.2. Copyright © 2008 Ingate Systems AB.

B.5. Surroundings (SIParator Only – DMZ Type Only)

To make the SIParator aware of the network structure the networks you define must be listed on the Surroundings page. One effect of this is that for traffic between two users on different networks, or between one of the listed networks and a network not listed in the Surroundings section, NAT will be applied. Another effect is that for connections between two users on the same network, or on networks where neither is listed in Surroundings, no ports for RTP sessions are opened, because the SIParator assumes that they are both on the same side of the firewall. Normally, at least one network must be listed here. If no networks are listed, the SIParator does not perform NAT for any traffic.



Surroundings (Help)

If your SIParator type is not set to **DMZ**, the settings on this page will have no effect.

Edit row	Network	Delete row
□	DMZ	□
□	Laboratory	□
□	Office	□

Add new rows 1 rows.

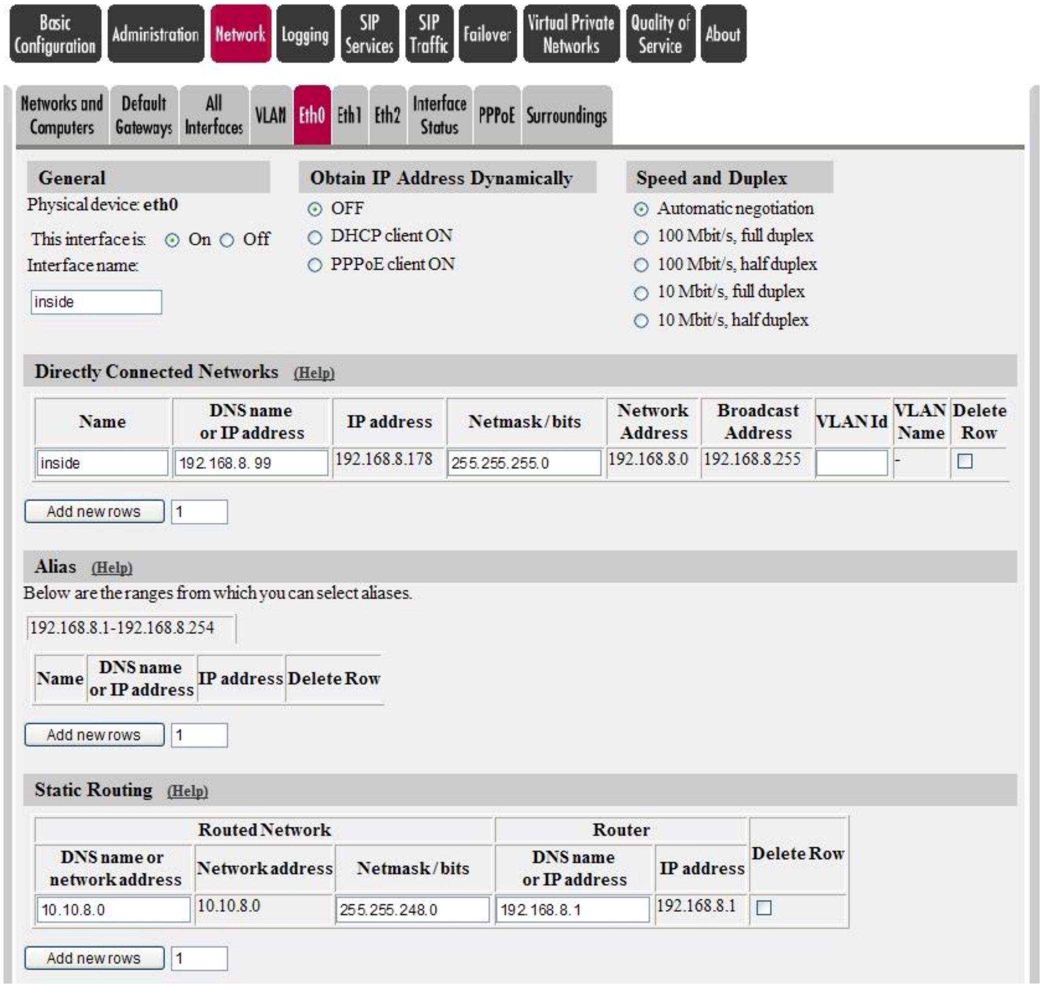
B.6. LAN Ethernet Interface

There is a tab for each network interface (Eth0, Eth1, ...) on the Ingate. Select a tab to configure the interface that you want to be connected to the LAN. Go to Directly Connected Networks and enter the IP address of the firewall and the size of the network connected to this interface. Enter the interface name, whether the interface is on or off, the IP address, alias, and static routing.

The Default Gateway, configured on the Default Gateways page, is automatically entered in this table on the corresponding interface page, when added to the Default Gateways table.

To configure the LAN Ethernet interface

1. Turn On the Interface.
2. In Directly Connected Networks do the following:
    a. Enter a Name
    b. Enter an IP address on the LAN network
    c. Enter a Netmask
3. In Static Routing, if there is a router between the firewall and a computer network that the firewall is serving, name the router and the network.



General

Physical device: **eth0**

This interface is: ● On ○ Off

Interface name: inside

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 Row
inside	192.168.8. 99	192.168.8.178	255.255.255.0	192.168.8.0	192.168.8.255		-	□

Add new rows 1

Alias (Help)

Below are the ranges from which you can select aliases.

192.168.8.1-192.168.8.254

Name	DNS name or IP address	IP address	Delete Row

Add new rows 1

Static Routing (Help)

Routed Network			Router		Delete Row
DNS name or network address	Network address	Netmask/bits	DNS name or IP address	IP address	
10.10.8.0	10.10.8.0	255.255.248.0	192.168.8.1	192.168.8.1	□

Add new rows 1

B.7. WAN Ethernet Interface

There is a tab for each network interface (Eth0, Eth1, ...) on the Ingate. Select a tab to configure the interface that you want to be connected to the WAN. Go to Directly Connected Networks and enter the IP address of the firewall and the size of the network connected to this interface. Enter the interface name, whether the interface is on or off, the IP address, alias, and static routing.

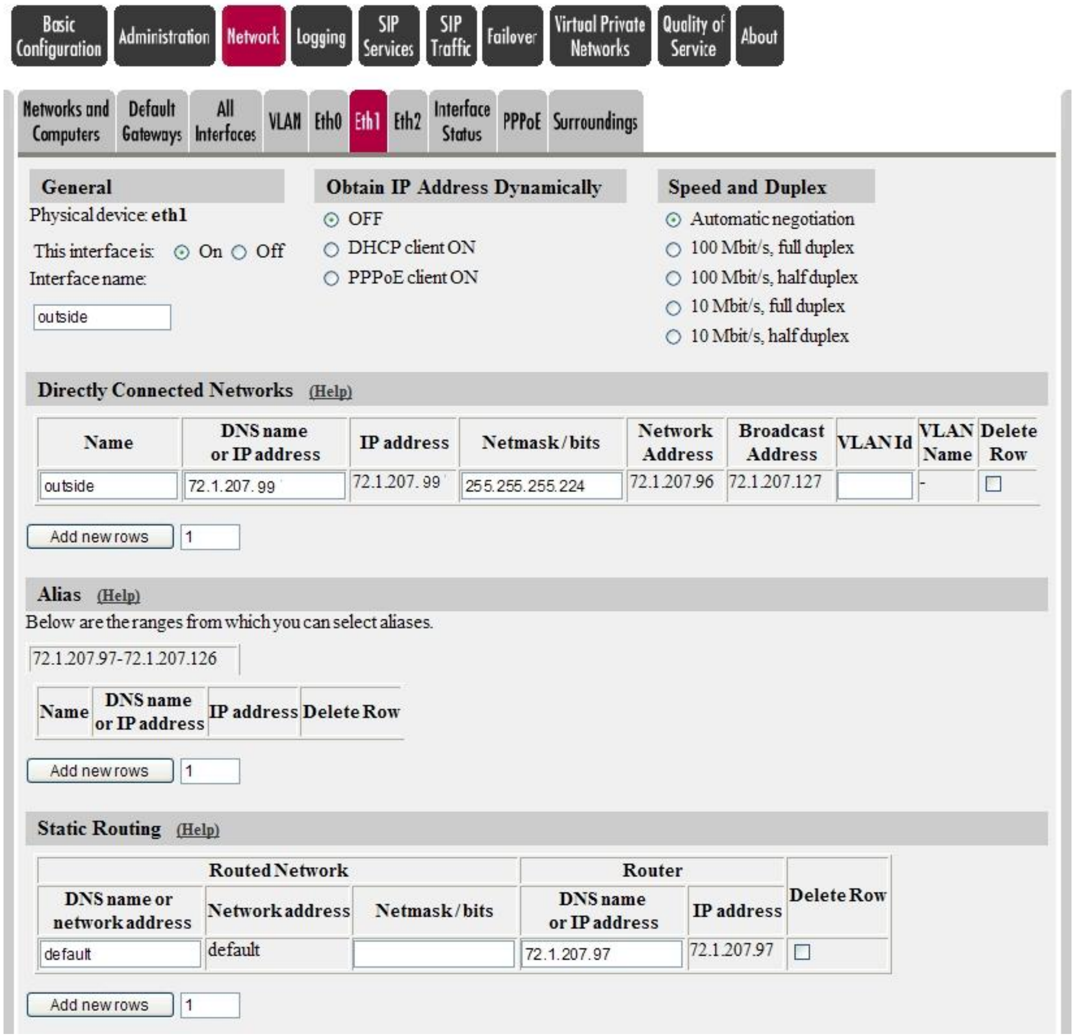
The Default Gateway, configured on the Default Gateways page, is automatically entered in this table on the corresponding interface page, when added to the Default Gateways table.

To configure the WAN Ethernet interface

1. Turn On the Interface.
2. In Directly Connected Networks do the following:
    a. Enter a Name.

    b. Enter an IP address on the WAN network.

    c. Enter a Netmask.
3. In Static Routing, if there is a router between the firewall and a computer network that the firewall is serving, you must name the router and the network here.



General

Physical device: **eth1**

This interface is: ● On ○ Off

Interface name:

outside

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 Row
outside	72.1.207.99	72.1.207.99	255.255.255.224	72.1.207.96	72.1.207.127		-	□

Add new rows 1

Alias (Help)

Below are the ranges from which you can select aliases.

72.1.207.97-72.1.207.126

Name	DNS name or IP address	IP address	Delete Row

Add new rows 1

Static Routing (Help)

Routed Network			Router		Delete Row
DNS name or network address	Network address	Netmask/bits	DNS name or IP address	IP address	
default	default		72.1.207.97	72.1.207.97	□

Add new rows 1

B.8. Default Gateway

A service provider provides a network extension of its own network to an enterprise. There is a physical network demarcation point from the service provider to the enterprise, usually identified as a router. Ensure that the proper Gateway address, Subnet Masks, and if required DNS Servers, are identified. A default gateway is the IP address of a router that is used to contact the outside world. The network provider typically assigns this an IP address.

B.8.1. Firewall

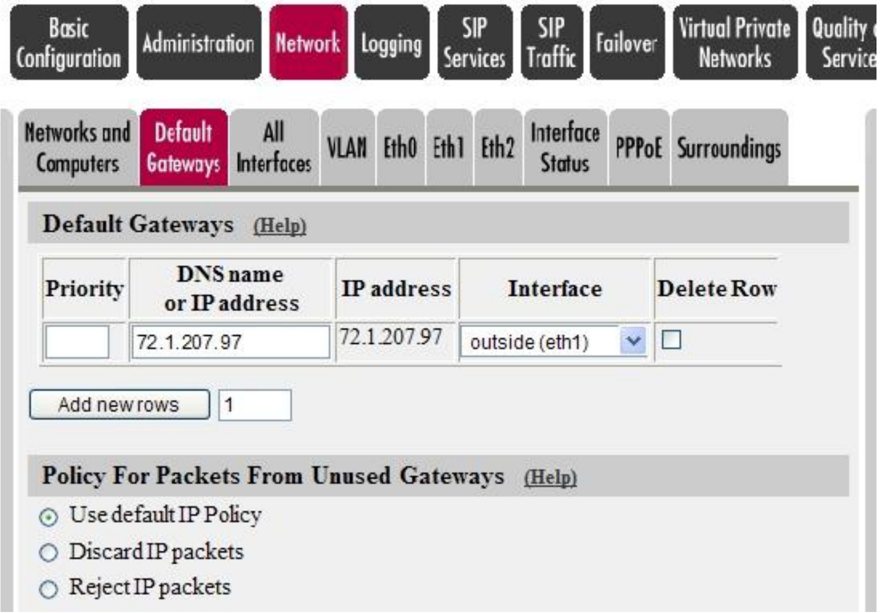
A default gateway must be an IP address from one of the directly connected networks of the firewall’s interfaces used to contact the WAN. If the SIP module is active, you must enter a default gateway. You can enter more than one default gateway. The firewall uses one of them until it stops responding, and then switches to the next one.

B.8.2. SIParator

The default gateway must be an IP address from one of the directly connected networks of the SIParator’s interfaces. The SIParator must have at least one default gateway to work. You can enter more than one default gateway. The SIParator uses one of them until it stops responding, and then switches to the next one.

To configure the default gateway

1. Enter the Default Gateway IP address used to contact the WAN.
2. Associate the Ethernet Interface used to contact the WAN.



Default Gateways (Help)

Priority	DNS name or IP address	IP address	Interface	Delete Row
	72.1.207.97	72.1.207.97	outside (eth1)	□

Add new rows 1

Policy For Packets From Unused Gateways (Help)

● Use default IP Policy
○ Discard IP packets
○ Reject IP packets

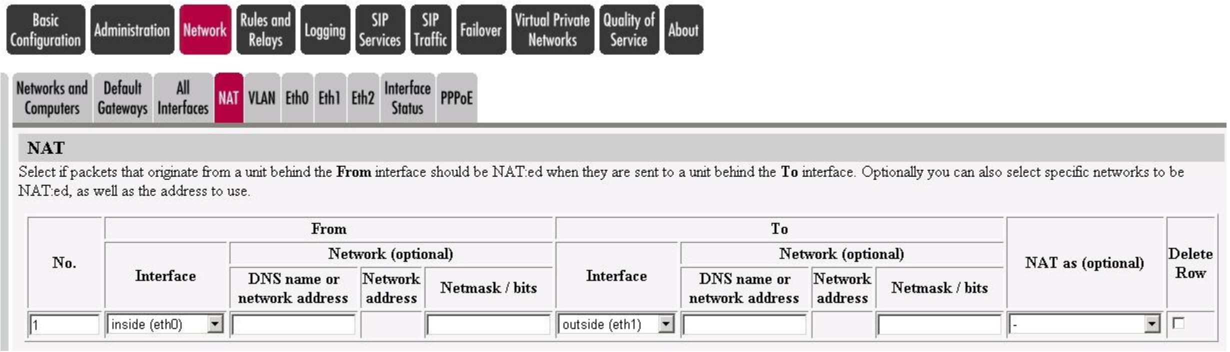
B.9. NAT Definition (Firewall Only)

NAT requirements are specific to the Ingate Firewalls and are not required in the SIParators. SIP Trunking requires that the Ingate Firewall be programmed to ensure that the NAT traversal of the SIP signaling and media is defined.

To hide IP addresses located behind one interface for a network, behind another interface, turn on NAT for that interface or only for that network. NAT makes it more difficult to access the computers on a network directly from another network. For example, internal networks can be hidden from external networks, such as the Internet. To access computers (for example, a Web server) you need a relay. If a network with private IP addresses is connected to eth0 traffic from these addresses must have NAT applied when sent out to the Internet. You can also select to have NAT traffic bound to a specific network behind the destination interface.

To define NAT

1. In the From field, select the Ethernet Interface of the LAN.
2. In the To field, select the Ethernet Interface of the WAN.



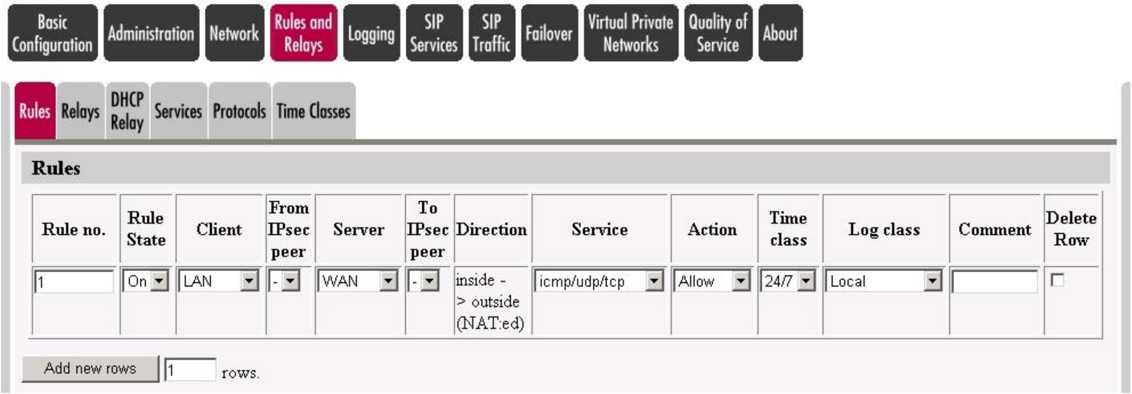
NAT

Select if packets that originate from a unit behind the **From** interface should be NAT:ed when they are sent to a unit behind the **To** interface. Optionally you can also select specific networks to be NAT:ed, as well as the address to use.

No.	From				To				NAT as (optional)	Delete Row
	Interface	Network (optional)			Interface	Network (optional)				
		DNS name or network address	Network address	Netmask / bits		DNS name or network address	Network address	Netmask / bits		
1	inside (eth0)				outside (eth1)				-	☐

B.10. Rules and Relays (Firewall Only)

You do not need to do anything for SIP on the Rules or Relays tabs.



Rules

Rule no.	Rule State	Client	From IPsec peer	Server	To IPsec peer	Direction	Service	Action	Time class	Log class	Comment	Delete Row
1	On	LAN	-	WAN	-	inside -> outside (NAT:ed)	icmp/udp/tcp	Allow	24/7	Local		☐

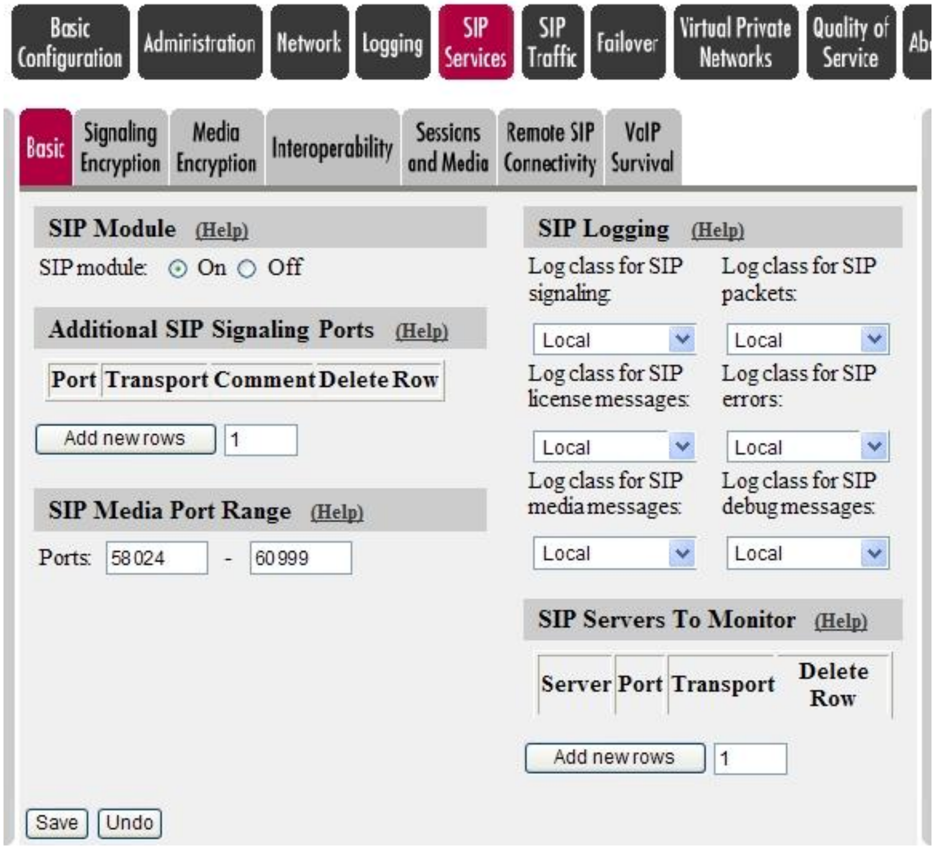
Add new rows 1 rows.

B.11. Enabling SIP Services

To enable SIP services

1. From the SIP Services – Basic page, enable the SIP module.
2. Optional, specify additional SIP Signaling Ports.
3. Optional, specify changes or restrictions to the Media Ports.

Note: This document does not address TLS and SRTP setup and application.



SIP Module (Help)

SIP module: ● On ○ Off

Additional SIP Signaling Ports (Help)

Port	Transport	Comment	Delete Row

Add new rows 1

SIP Media Port Range (Help)

Ports: 58 024 - 60 999

SIP Logging (Help)

Log class for SIP signaling: Local

Log class for SIP packets: Local

Log class for SIP license messages: Local

Log class for SIP errors: Local

Log class for SIP media messages: Local

Log class for SIP debug messages: Local

SIP Servers To Monitor (Help)

Server	Port	Transport	Delete Row

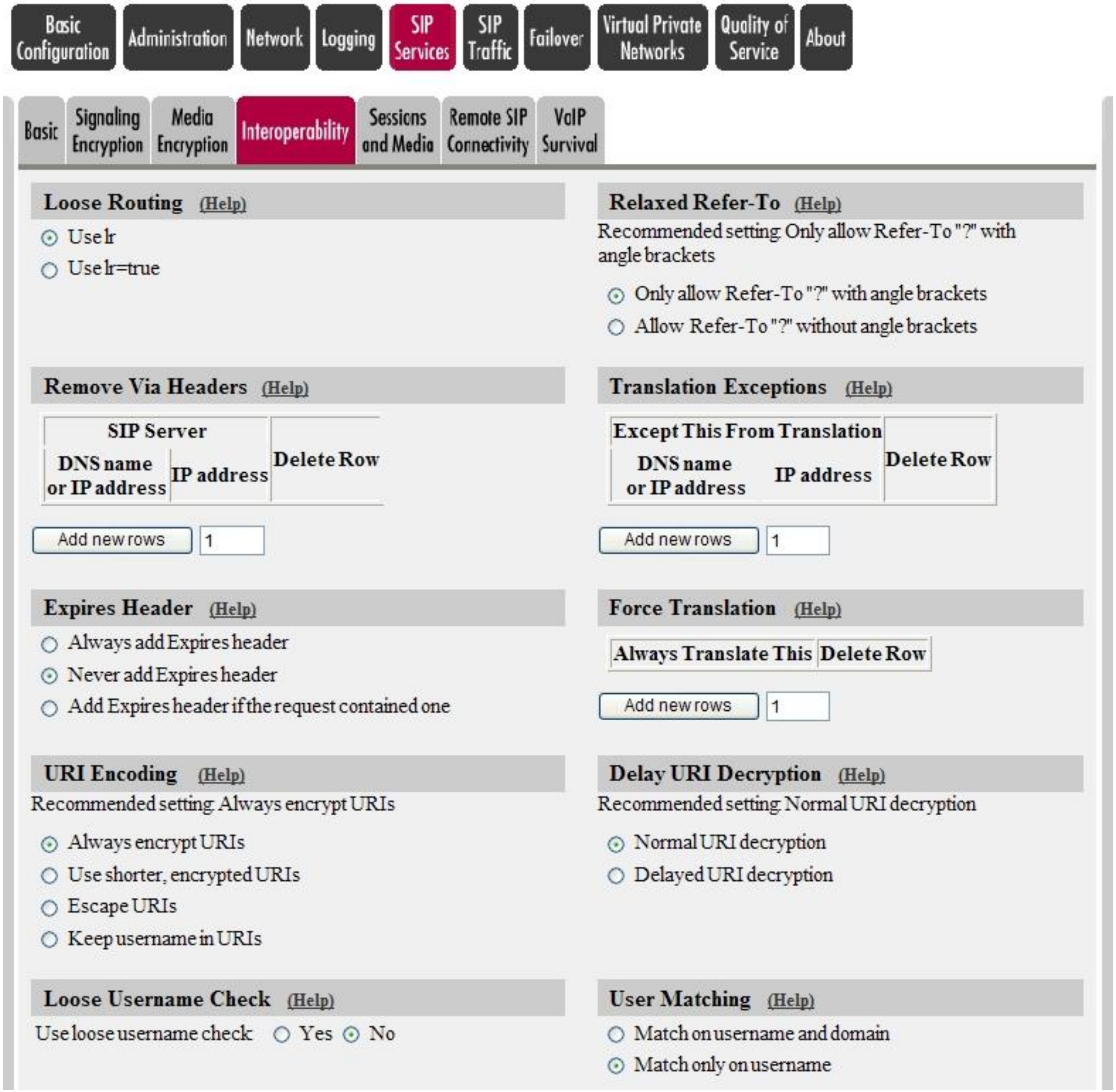
Add new rows 1

B.12. Interoperability

Configure interoperability using the tab in the SIP Services page.

To configure interoperability

1. For proper operation default settings are sufficient.
2. Optional, select **“Allow large UDP packets”** in some cases where the UDP packets are larger than standard.



Loose Routing (Help)

● Use lr

○ Use lr=true

Relaxed Refer-To (Help)

Recommended setting: Only allow Refer-To "?" with angle brackets

● Only allow Refer-To "?" with angle brackets

○ Allow Refer-To "?" without angle brackets

Remove Via Headers (Help)

SIP Server		Delete Row
DNS name or IP address	IP address	

Add new rows 1

Translation Exceptions (Help)

Except This From Translation		Delete Row
DNS name or IP address	IP address	

Add new rows 1

Expires Header (Help)

○ Always add Expires header

● Never add Expires header

○ Add Expires header if the request contained one

Force Translation (Help)

Always Translate This	Delete Row

Add new rows 1

URI Encoding (Help)

Recommended setting: Always encrypt URIs

● Always encrypt URIs

○ Use shorter, encrypted URIs

○ Escape URIs

○ Keep username in URIs

Delay URI Decryption (Help)

Recommended setting: Normal URI decryption

● Normal URI decryption

○ Delayed URI decryption

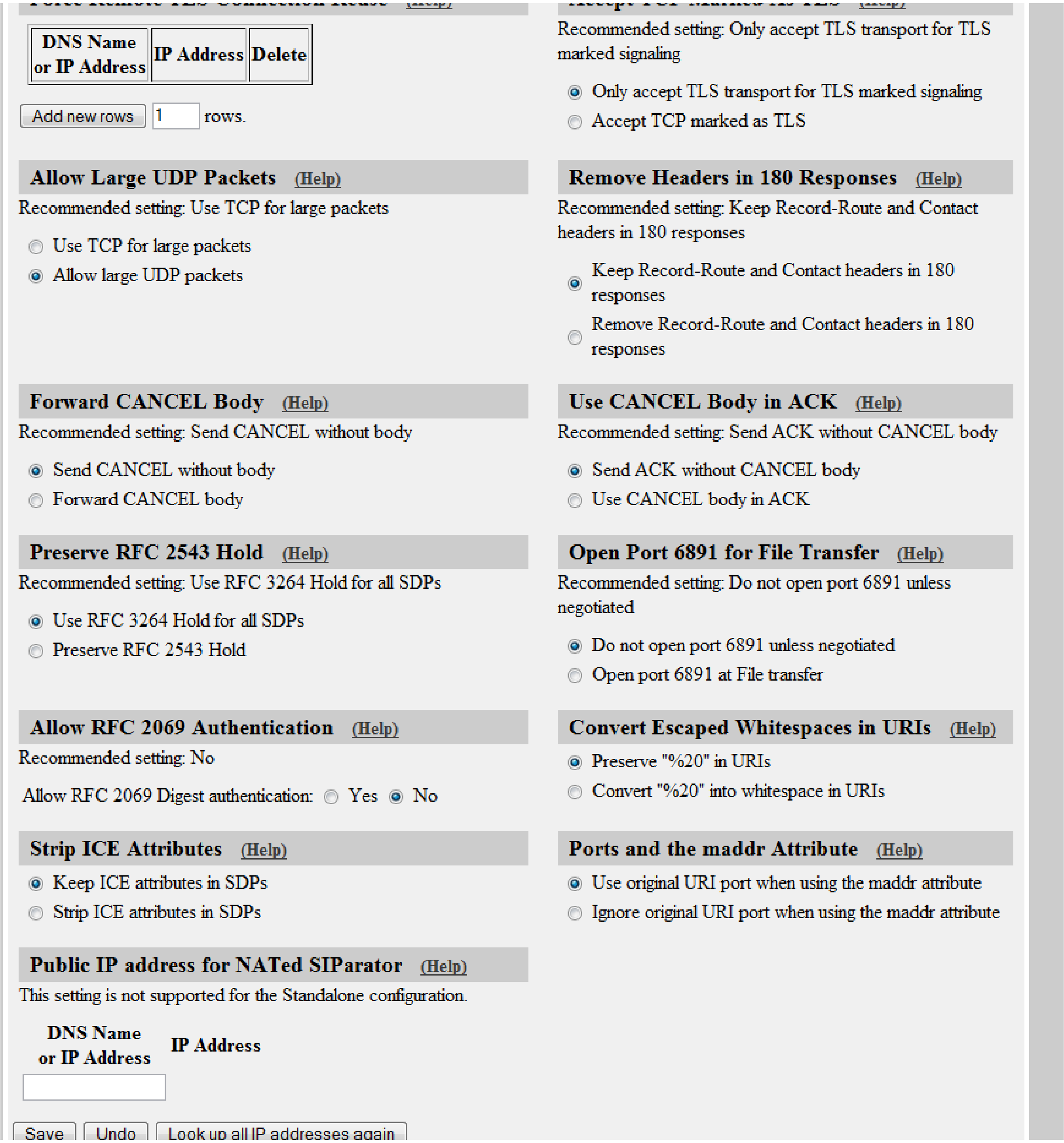
Loose Username Check (Help)

Use loose username check ○ Yes ● No

User Matching (Help)

○ Match on username and domain

● Match only on username



Force Remote TLS Connection Reuse (Help)

DNS Name or IP Address	IP Address	Delete

1 rows.

Allow Large UDP Packets (Help)

Recommended setting: Use TCP for large packets

○ Use TCP for large packets
● Allow large UDP packets

Forward CANCEL Body (Help)

Recommended setting: Send CANCEL without body

● Send CANCEL without body
○ Forward CANCEL body

Preserve RFC 2543 Hold (Help)

Recommended setting: Use RFC 3264 Hold for all SDPs

● Use RFC 3264 Hold for all SDPs
○ Preserve RFC 2543 Hold

Allow RFC 2069 Authentication (Help)

Recommended setting: No

Allow RFC 2069 Digest authentication: ○ Yes ● No

Strip ICE Attributes (Help)

● Keep ICE attributes in SDPs
○ Strip ICE attributes in SDPs

Public IP address for NATed SIParator (Help)

This setting is not supported for the Standalone configuration.

DNS Name or IP Address	IP Address

Accept TCP Marked As TLS (Help)

Recommended setting: Only accept TLS transport for TLS marked signaling

● Only accept TLS transport for TLS marked signaling
○ Accept TCP marked as TLS

Remove Headers in 180 Responses (Help)

Recommended setting: Keep Record-Route and Contact headers in 180 responses

● Keep Record-Route and Contact headers in 180 responses
○ Remove Record-Route and Contact headers in 180 responses

Use CANCEL Body in ACK (Help)

Recommended setting: Send ACK without CANCEL body

● Send ACK without CANCEL body
○ Use CANCEL body in ACK

Open Port 6891 for File Transfer (Help)

Recommended setting: Do not open port 6891 unless negotiated

● Do not open port 6891 unless negotiated
○ Open port 6891 at File transfer

Convert Escaped Whitespaces in URIs (Help)

● Preserve "%20" in URIs
○ Convert "%20" into whitespace in URIs

Ports and the maddr Attribute (Help)

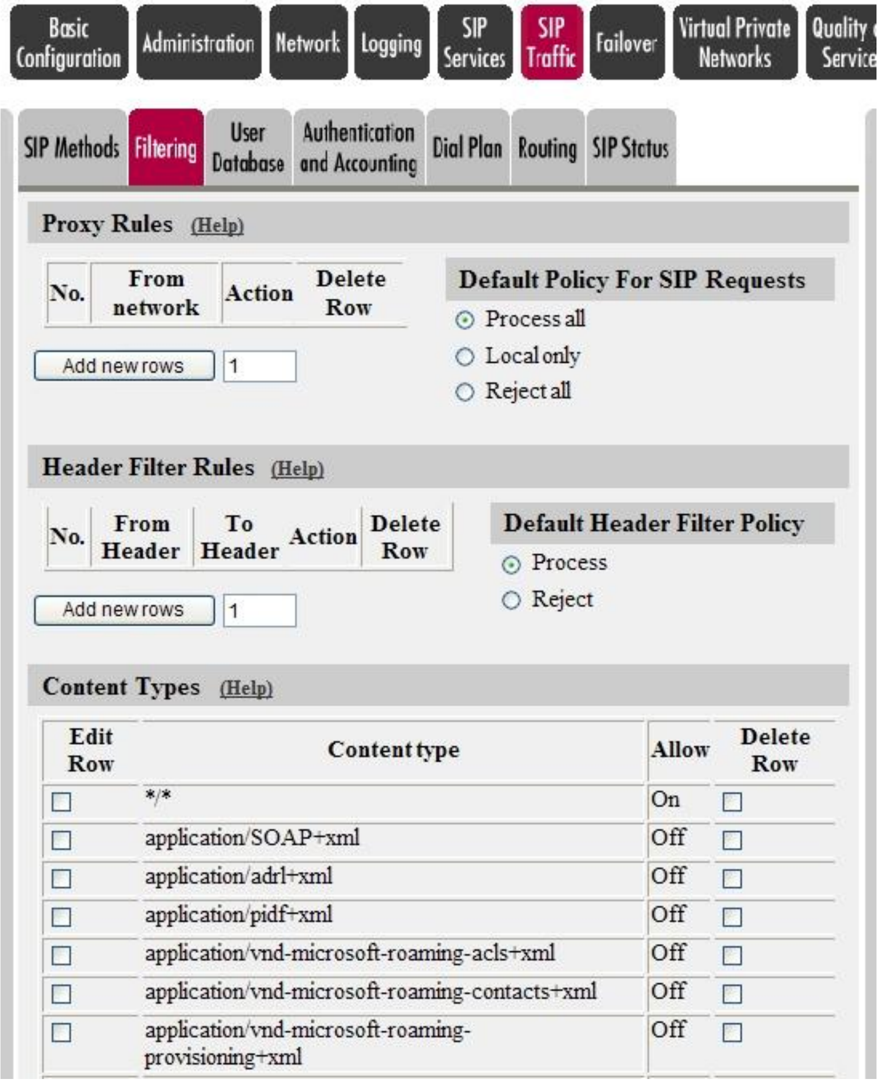
● Use original URI port when using the maddr attribute
○ Ignore original URI port when using the maddr attribute

B.13. Filtering

Configure filtering using the Filtering tab in the SIP Traffic page.

To configure filtering

1. In the **Proxy Rules**, make sure that the **Default Policy for SIP Requests** is set to Process all.
2. Add an additional **Content Type** of “message/sipfrag” and set **Allow** to ON, for SIP NOTIFY requests with sipfrag content access or simply enter “*/*” and set Allow=ON to indicate to the Ingate not to filter on any Content Type.



Proxy Rules (Help)

No.	From network	Action	Delete Row

Add new rows 1

Default Policy For SIP Requests

● Process all
○ Local only
○ Reject all

Header Filter Rules (Help)

No.	From Header	To Header	Action	Delete Row

Add new rows 1

Default Header Filter Policy

● Process
○ Reject

Content Types (Help)

Edit Row	Content type	Allow	Delete Row
□	*/*	On	□
□	application/SOAP+xml	Off	□
□	application/adrl+xml	Off	□
□	application/pidf+xml	Off	□
□	application/vnd-microsoft-roaming-acls+xml	Off	□
□	application/vnd-microsoft-roaming-contacts+xml	Off	□
□	application/vnd-microsoft-roaming-provisioning+xml	Off	□

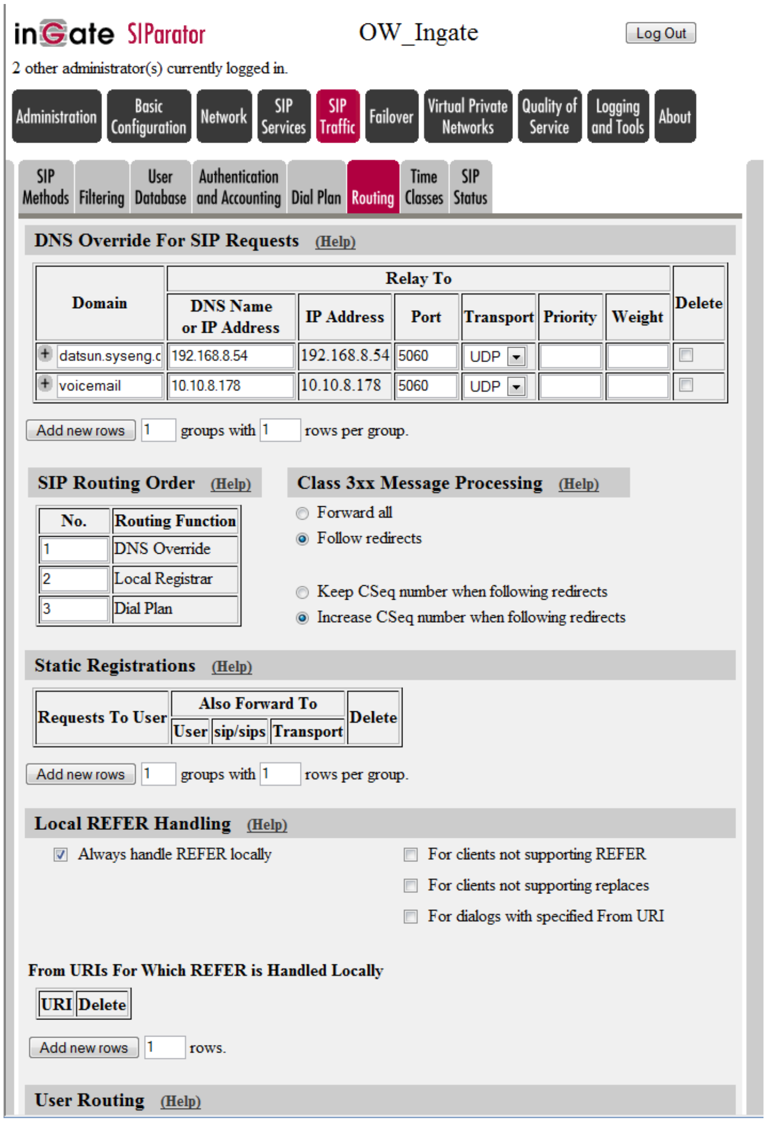
B.14. Routing

B.14.1. Class 3XX Message Processing

In the Routing section is a heading called "Class 3XX Message Processing." It is important that "Forward redirects" and "Increase CSeq number when following redirects: are enabled. It is important that 3XX message are not sent to the ITSP. Most ITSPs do not handle 3XX messages.

To configure routing

- In the **Routing tab**, under the **Class 3XX Message Processing**, ensure the "**Follow Redirects"** option is enabled.



2 other administrator(s) currently logged in.

DNS Override For SIP Requests (Help)

Domain	Relay To						Delete
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	
+ datsun.syseng.c	192.168.8.54	192.168.8.54	5060	UDP			□
+ voicemail	10.10.8.178	10.10.8.178	5060	UDP			□

Add new rows 1 groups with 1 rows per group.

SIP Routing Order (Help)

No.	Routing Function
1	DNS Override
2	Local Registrar
3	Dial Plan

Class 3xx Message Processing (Help)

○ Forward all
● Follow redirects

○ Keep CSeq number when following redirects
● Increase CSeq number when following redirects

Static Registrations (Help)

Requests To User	Also Forward To			Delete
	User	sip/sips	Transport	

Add new rows 1 groups with 1 rows per group.

Local REFER Handling (Help)

☑ Always handle REFER locally
□ For clients not supporting REFER
□ For clients not supporting replaces
□ For dialogs with specified From URI

From URIs For Which REFER is Handled Locally

URI	Delete

Add new rows 1 rows.

User Routing (Help)

B.14.2. Local REFER Handling

In the Routing section is a heading called “Local REFER handling.” It is important that this option be enabled. It is important that the Ingate handle all the REFERs locally and not allow any REFER message to be sent to the ITSP. Most ITSPs do not handle a REFER message.

To configure local REFER handling

- In the **Routing**, under the **Local REFER Handling**, ensure the “**Always handle REFER locally”** option is enabled.

B.15. Sessions and Media

B.15.1. Limitation of RTP Codecs

You can limit the use of some media codecs. There can be several reasons for this:

a. Some endpoints do not support the codecs,

b. Too many codec offers make the SIP request packet too large (which causes it to be fragmented),

c. They consume too much bandwidth,

d. You want to allow only codecs with good enough voice quality.

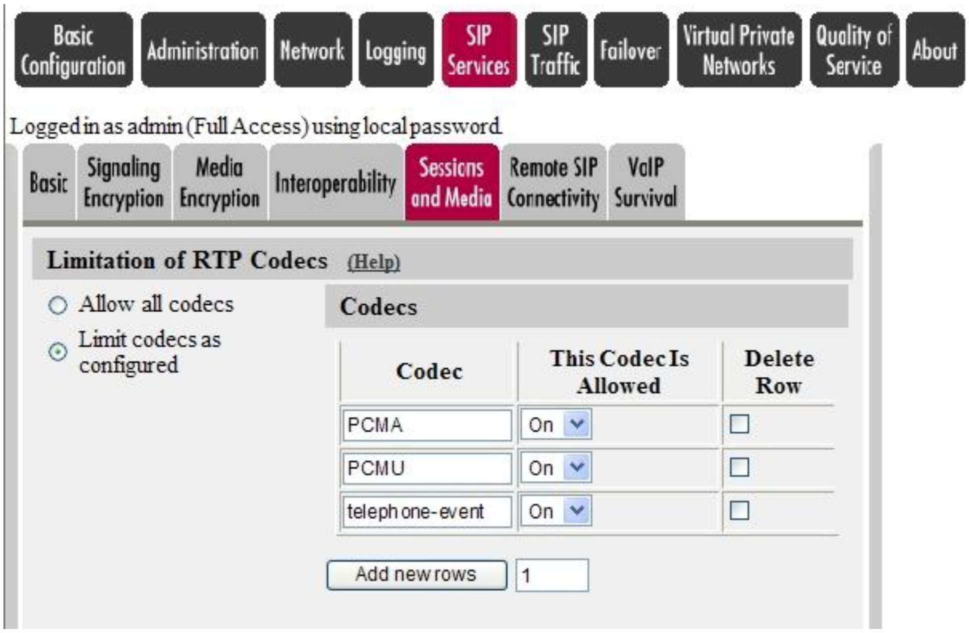
e. The Ingate does perform codec trans-coding, for example the Ingate does not change a G711/PCMU RTP stream and convert it to G729 RTP stream. Therefore, in some supervised transfer scenarios where one party is G711 and other is G729, these two calls cannot be transferred together. This option limits any incoming/outgoing SIP Trunk call to one common codec.

You can select to allow all codecs, or limit to only allow codecs listed as allowed in the Codecs table.

If no codec is left when all forbidden codecs have been removed from the SDP offer, an error message is displayed.

To limit RTP codecs

1. In the **Sessions and Media tab**, under the **Limitation of RTP Codecs**, enable “**Limit codecs as configured”** option.
2. Under Codecs, click “Add new rows”, and enter PCMU in the “Codec” column.
3. Select “On” in the “This Codec is Allowed” column.
4. Repeat the process for PCMU, and telephone event codec types.



Logged in as admin (Full Access) using local password.

Limitation of RTP Codecs (Help)

○ Allow all codecs
● Limit codecs as configured

Codecs

Codec	This Codec Is Allowed	Delete Row
PCMA	On	□
PCMU	On	□
telephone-event	On	□

Add new rows 1

B.16. SIP Trunking with Registrations

B.16.1. REGISTER

The Ingate Firewalls can manage ITSP SIP Account registrations, allowing the SIP Trunking Module to keep track of where to send incoming session requests. It also allows the ITSP to keep track of the SIP trunk destination. It is possible to change which SIP trunk accounts are used for outgoing calls to the ITSP. You can monitor which ITSP Accounts are currently registered. The Registrar keeps the required information to locate users inside the firewall.

For outgoing SIP requests, only a SIP proxy is needed, but the Ingate has the ability to replace the FROM Header using the SIP trunk Account provided. Incoming SIP requests need a mechanism to direct the call to the UC server, so that SIP requests can be relayed to the right machine and user. Using the Dial Plan or Static Registrations the incoming call can be directed to the UC server.

B.16.2. How a REGISTER Applies to SIP Trunking

It is important to note that the main Registrar within the Ingate is not used. The account UserID, Domain, Authentication Username and Password information within the Ingate main Registrar are not used. The "Local SIP Domains" (or FQDN) programmed in the User Database are different (or not used) from the Domain Name used by the UC server.

Instead, the Ingate is a client, initiating, monitoring and storing information from registrations done at an outside registrar. The Ingate performs a Domain Lookup when it sees a request for a domain that is not its own and forwards the SIP requests or responses to the UC server.

Of note, when the Ingate REGISTERs with a specific SIP URI, but the service provider sends SIP requests and responses to a different SIP URI, one that does not match the SIP URI in the UC server REGISTER, then a Dial Plan is required to ensure the service provider's SIP requests and responses traverse the firewall. In all cases a Dial Plan is created to handle incoming and outgoing callsUser Database

Listed below are the Account type selections commonly used in ITSP SIP Trunking. Different account types can change the behavior of the connectivity of the SIP Trunk call.

Register With this Account type, the SIParator registers the username with the SIP server associated with the domain. You may enter the address to send the request to in the User Routing table. This is useful when you have a SIP client that cannot register properly.

XF With this Account type, the SIParator replaces the From header with the username and domain of this XF user. The request is then forwarded to the address entered in the Dial Plan. If no address is entered there, the request is forwarded to the SIP server associated with the domain. Also Used for CLID purposes.

XF/Register With this Account type, the SIParator replaces the From header as described above, and then registers as described under Register above.

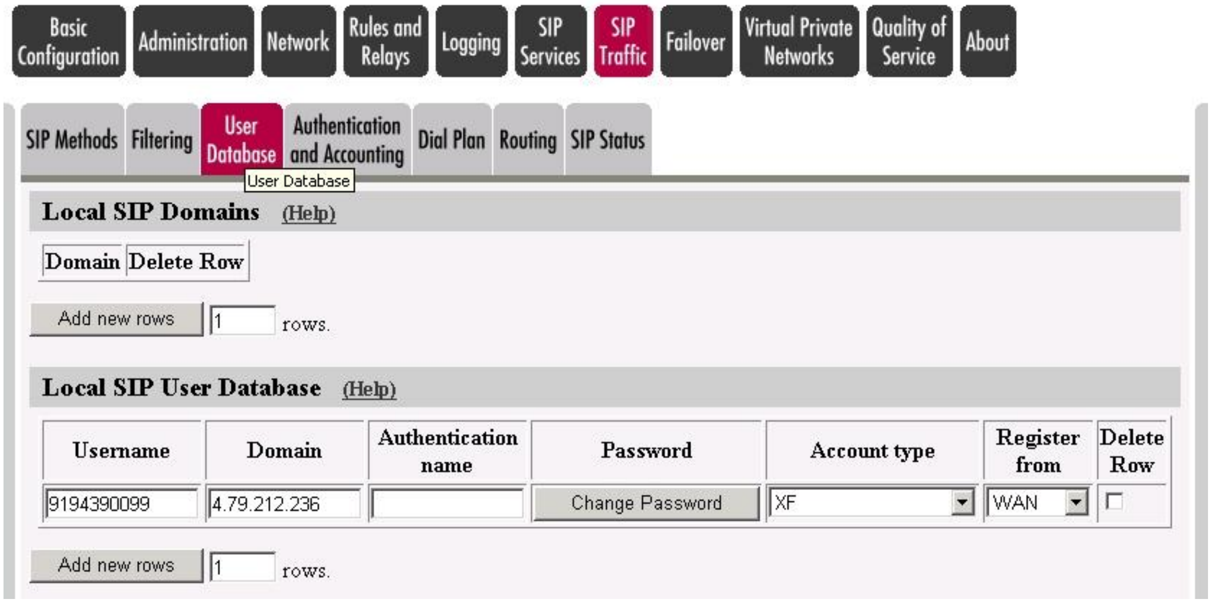
B2BUAWM With this Account type, the SIParator replaces the From header as described under XF. It also changes the SDPs to the effect that media is always sent using the SIParator.

B2BUAWM/Register With this Account type, the SIParator acts as described under B2BUAWM above. It also registers the user as described under Register above.

To configure the user database

1. In the **Local SIP User Database**, enter the Account Number in the Username field.
2. Enter the IP address or Domain of the ITSP in the Domain field.
3. If necessary, enter the Authentication Username and password.
4. Select the Account type based on the behavior desired, as mentioned above.

Note: In addition to the Startup Tool configuring the XF/Register account type, an XF account type is required to provide Caller Line Identification (FROM Header replacement) when using multiple accounts or other scenarios.



Local SIP Domains (Help)

Domain	Delete Row

Add new rows 1 rows.

Local SIP User Database (Help)

Username	Domain	Authentication name	Password	Account type	Register from	Delete Row
9194390099	4.79.212.236		Change Password	XF	WAN	☐

Add new rows 1 rows.

B.17. Dial Plan

A Dial Plan in the Ingate products allows the Ingate product to match the incoming Request-URI from the ITSP and forward the call to the domain or IP address of the UC server, and likewise match the incoming Request-URI from the UC server and forward it to the domain or IP address of the ITSP.

There are several advantages when using a Dial Plan.

- A dial plan works well for a range of numbers, for example, if there are a range of numbers, 6135559600-6135559699, a "Matching Request-URI" of 61355596 with a "Tail" of 0-9 can be programmed.
- Using a dial plan, there is the ability to route one number with different domains.
- A dial plan is more flexible in the ability to configure/change the ports and Transport based on the incoming Request-URI.

To configure a dial plan

1. Under **Use Dial Plan**, select ON.
2. In **Matching From Header**, "Add new rows," enter the following attributes:
    a. Name – Assign a name value "**LAN**"
    b. Username – Insert a " * " to allow any Username
    c. Domain – Insert a " * " to allow any Domain
    d. Transport – Select **UDP** to allow only UDP transport types
    e. Network – Select **LAN**, (generated for "Network and Computers")
    f. Repeat the process for "**WAN**", substituting Any for Transport and WAN for Network.
3. In **Matching Request-URI**, "Add new rows," enter the following attributes:

a. Name – Assign a name value

b. Prefix – Not required in most applications

c. Head – Leave blank

d. Tail – Select **Any Character**

e. Domain – Insert the Ingate WAN IP Address for incoming calls, **OR** Insert the Ingate LAN IP address for outgoing calls

4. In **Forward To**, “Add new rows,” enter the following attributes:

a. Name – Assign a name value for ITSP settings

b. Use this Account – if an **“XF”** Account was entered in the User Database for Registration or FROM Header replacement, select the account

c. Replacement URI – if No User was entered, assign the ITSP IP address – Primary and Secondary (if there is one)

Repeat for the UC server

a. Name – Assign a name value for the UC server

b. Use this Account – Leave unselected

c. Replacement URI – assign the IP Address of the the UC server

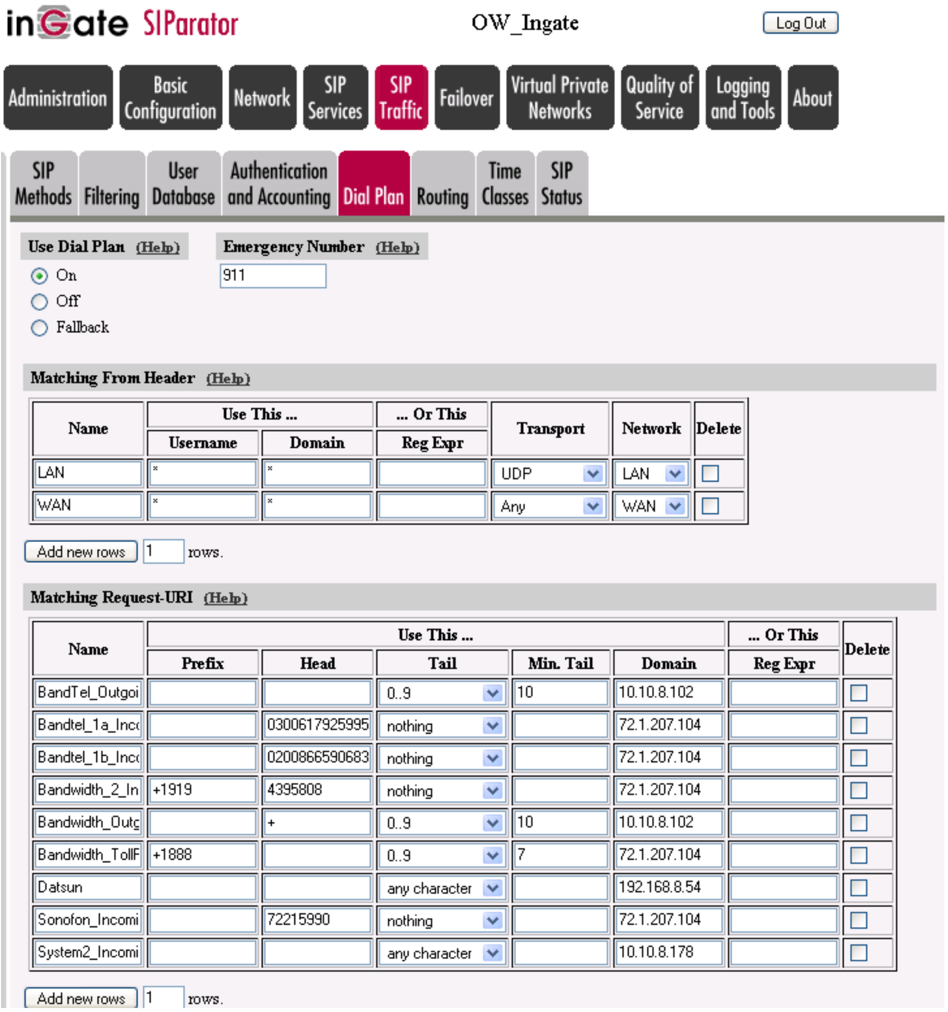
5. In **Dial Plan**, “Add new rows,” enter the following attributes:

a. From Header – Select the assigned Name given above from the “Matching From Header”

b. Request-URI – Select the assigned Name given above from the “Matching Request-URI”

c. Action – Select **Forward** from the drop down list

d. Forward To – Select the assigned Name given above from the “Forward To”



OW_Ingate

Use Dial Plan (Help)

● On
○ Off
○ Fallback

Emergency Number (Help)

911

Matching From Header (Help)

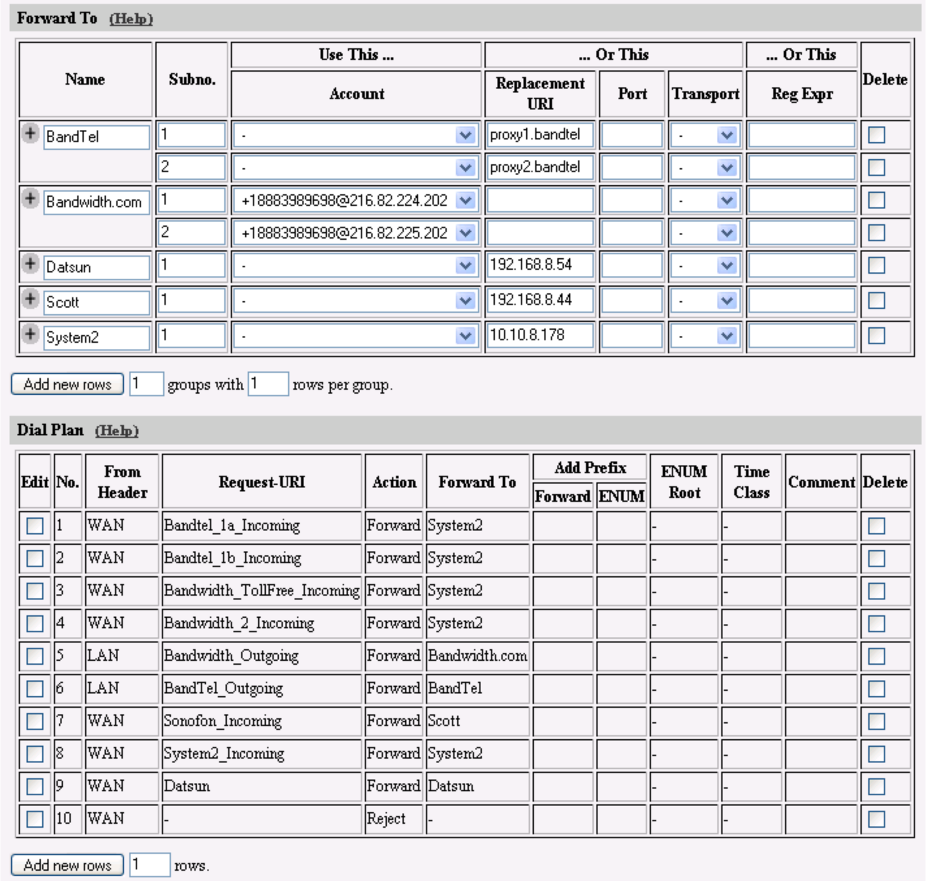
Name	Use This ...		... Or This	Transport	Network	Delete
	Username	Domain	Reg Expr			
LAN	*	*		UDP	LAN	□
WAN	*	*		Any	WAN	□

Add new rows 1 rows.

Matching Request-URI (Help)

Name	Use This ...					... Or This	Delete
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
BandTel_Outgoi			0..9	10	10.10.8.102		□
Bandtel_1a_Inc(		0300617925995	nothing		72.1.207.104		□
Bandtel_1b_Inc(		0200866590683	nothing		72.1.207.104		□
Bandwidth_2_In	+1919	4395808	nothing		72.1.207.104		□
Bandwidth_Outg		+	0..9	10	10.10.8.102		□
Bandwidth_TollF	+1888		0..9	7	72.1.207.104		□
Datsun			any character		192.168.8.54		□
Sonofon_Incomi		72215990	nothing		72.1.207.104		□
System2_Incomi			any character		10.10.8.178		□

Add new rows 1 rows.



Forward To (Help)

Name	Subno.	Use This ...	... Or This			... Or This	Delete
		Account	Replacement URI	Port	Transport	Reg Expr	
BandTel	1	-	proxy1.bandtel		-		□
	2	-	proxy2.bandtel		-		□
Bandwidth.com	1	+18883989698@216.82.224.202			-		□
	2	+18883989698@216.82.225.202			-		□
Datsun	1	-	192.168.8.54		-		□
Scott	1	-	192.168.8.44		-		□
System2	1	-	10.10.8.178		-		□

1 groups with 1 rows per group.

Dial Plan (Help)

Edit	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete
						Forward	ENUM				
□	1	WAN	Bandtel_1a_Incoming	Forward	System2			-	-		□
□	2	WAN	Bandtel_1b_Incoming	Forward	System2			-	-		□
□	3	WAN	Bandwidth_TollFree_Incoming	Forward	System2			-	-		□
□	4	WAN	Bandwidth_2_Incoming	Forward	System2			-	-		□
□	5	LAN	Bandwidth_Outgoing	Forward	Bandwidth.com			-	-		□
□	6	LAN	BandTel_Outgoing	Forward	BandTel			-	-		□
□	7	WAN	Sonofon_Incoming	Forward	Scott			-	-		□
□	8	WAN	System2_Incoming	Forward	System2			-	-		□
□	9	WAN	Datsun	Forward	Datsun			-	-		□
□	10	WAN	-	Reject	-			-	-		□

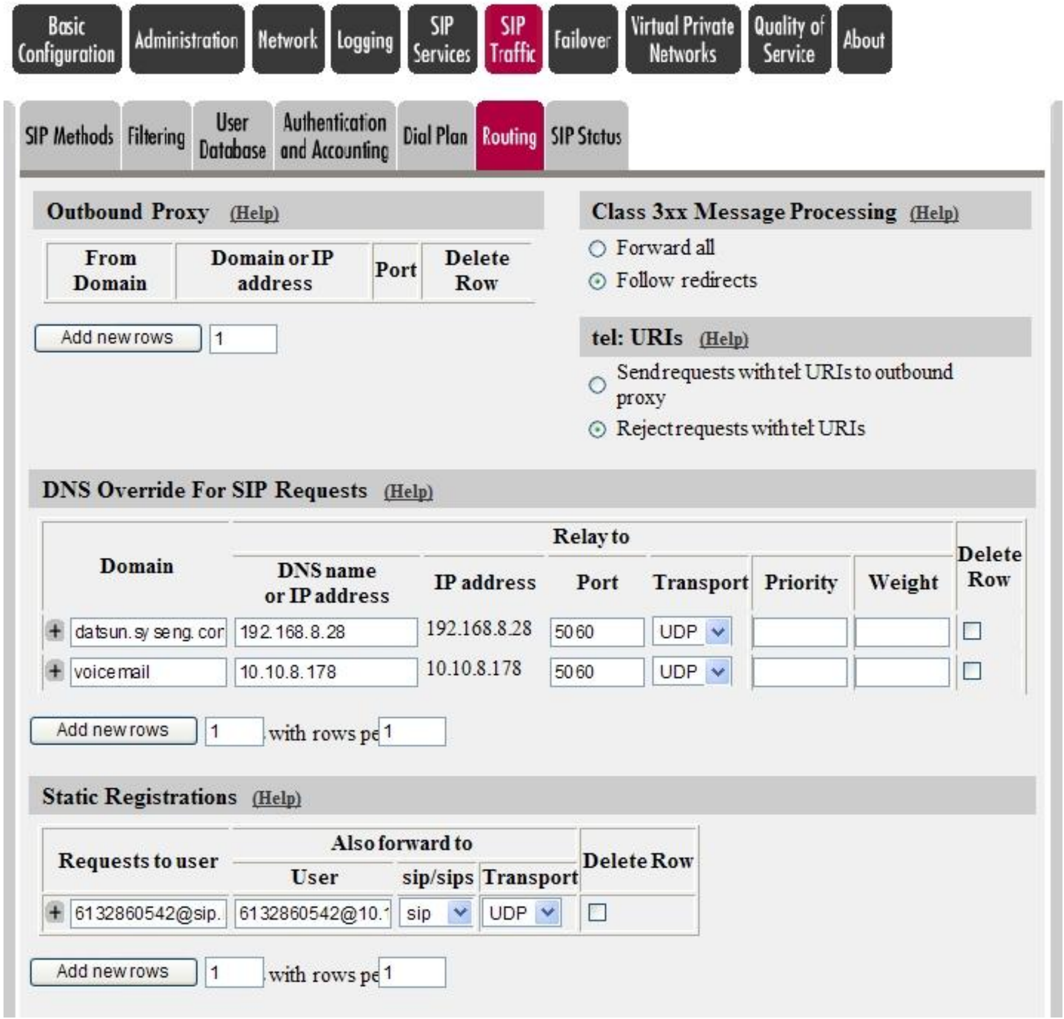
1 rows.

B.17.1.Static Registrations

Static registrations may not be required with an ITSP. The Dial Plan can perform this step in almost every application. But in the situation where there is a site-specific application the Static Registrations performs a Match a specific Request-URI (number@domain) and forwards it to a different SIP URI. In a few cases, for the purpose of SIP Trunking, if you have one number to forward to the UC server, it may be easier to set up a static registration. For example, an incoming call to the firewall with a Request-URI of 6135559698@72.1.207.99 gets forwarded to the internal UC server with a Request-URI of 6135559698@192.168.8.99.

To configure static registrations

1. Request to user – Program the Incoming SIP URI from the service provider
2. User – Program the SIP URI to call the UC server
3. Sip/sips – Select **sip**
4. Transport – Select **UDP**



Outbound Proxy (Help)

From Domain	Domain or IP address	Port	Delete Row

Add new rows 1

Class 3xx Message Processing (Help)

○ Forward all
● Follow redirects

tel: URIs (Help)

○ Send requests with tel: URIs to outbound proxy
● Reject requests with tel: URIs

DNS Override For SIP Requests (Help)

Domain	Relay to						Delete Row
	DNS name or IP address	IP address	Port	Transport	Priority	Weight	
+ datsun.sy seng.cor	192.168.8.28	192.168.8.28	5060	UDP			□
+ voicemail	10.10.8.178	10.10.8.178	5060	UDP			□

Add new rows 1 with rows pe 1

Static Registrations (Help)

Requests to user	Also forward to			Delete Row
	User	sip/sips	Transport	
+ 6132860542@sip.	6132860542@10.1	sip	UDP	□

Add new rows 1 with rows pe 1

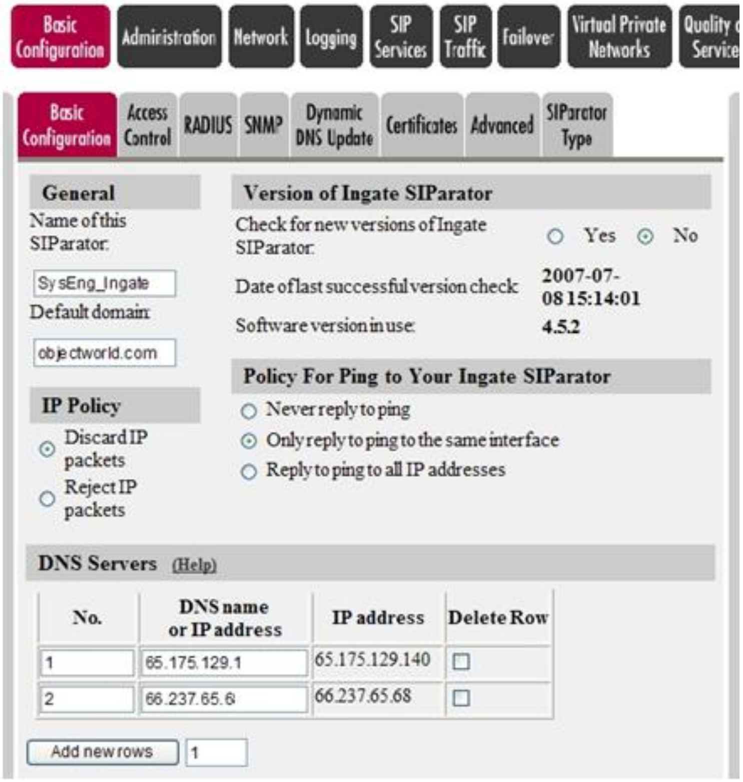
B.18. DNS Considerations

The Ingate gateways needs to do DNS queries for both incoming and outgoing traffic whenever it encounters a routing-participating header that contains an FQDN. Some ITSPs do require DNS Servers.

To configure DNS

In the Basic Configuration page:

1. Assign the IP address of the DNS Server, Primary and Secondary.



General

Name of this SIParator: SysEng_Ingate

Default domain: objectworld.com

IP Policy

- ● Discard IP packets
- ○ Reject IP packets

Version of Ingate SIParator

Check for new versions of Ingate SIParator: ○ Yes ● No

Date of last successful version check: **2007-07-08 15:14:01**

Software version in use: **4.5.2**

Policy For Ping to Your Ingate SIParator

- ○ Never reply to ping
- ● Only reply to ping to the same interface
- ○ Reply to ping to all IP addresses

DNS Servers (Help)

No.	DNS name or IP address	IP address	Delete Row
1	65.175.129.1	65.175.129.140	□
2	66.237.65.6	66.237.65.68	□

Add new rows 1

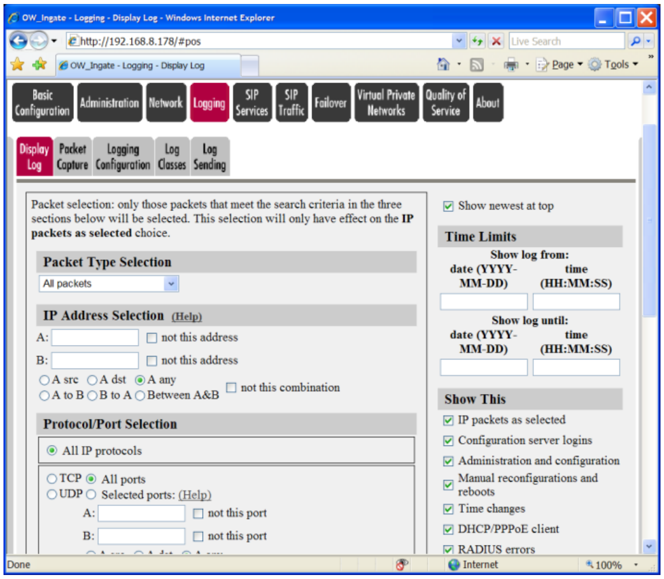
Appendix C Tools

C.1. Ingate Tools

The Ingate Firewalls provide troubleshooting tools. Included in the Ingate Firewall are Log Viewer, Packet Capture, and Syslog Server capabilities.

C.2. Display Log

The Ingate log viewer is a way to see SIP protocol-related messages. The logs show the SIP traffic on all interfaces/ports of the Ingate gateway. Also, when SIP Debug Messages is turned On, the Ingate gives more detailed information as to why there are errors in certain messages or what actions it took given the information it has.



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

☑ Show newest at top

Time Limits

Show log from:
date (YYYY-MM-DD) time (HH:MM:SS)

Show log until:
date (YYYY-MM-DD) time (HH:MM:SS)

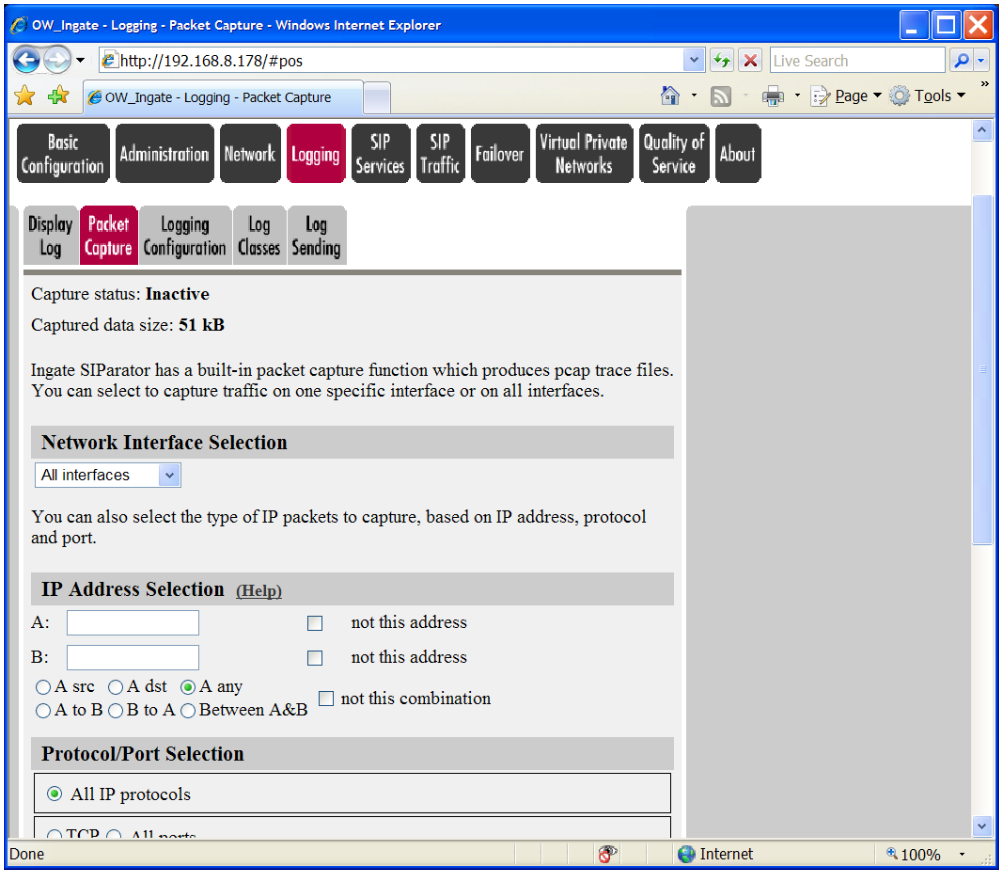
Show This

☑ IP packets as selected
☑ Configuration server logins
☑ Administration and configuration
☑ Manual reconfigurations and reboots
☑ Time changes
☑ DHCP/PPPoE client
☑ RADIUS errors

C.3. Packet Capture

The Ingate Firewall has the ability to capture packets in a Wireshark format (.pcap) from One or All interfaces/Ports. When selecting "All interfaces" in the Network Interface Selection, the Ingate captures Network activity from both the LAN port and the WAN port. Download the packet capture to the workstation and use Ethereal to view the packet capture to best determine the problem.

You must first select the interface to perform the packet capture, then Start the capture, duplicate the problem, then Stop the capture, and finally download the capture to your workstation to view with Ethereal (*www.ethereal.com*).



Capture status: **Inactive**

Captured data size: **51 kB**

Ingate SIParator has a built-in packet capture function which produces pcap trace files. You can select to capture traffic on one specific interface or on all interfaces.

Network Interface Selection

All interfaces

You can also select the type of IP packets to capture, based on IP address, protocol and port.

IP Address Selection (Help)

A: □ not this address

B: □ not this address

○ A src ○ A dst ● A any □ not this combination
○ A to B ○ B to A ○ Between A&B

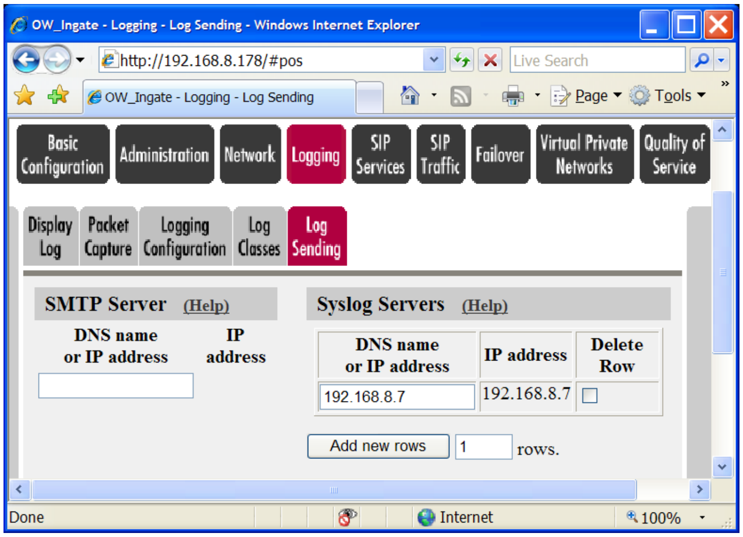
Protocol/Port Selection

● All IP protocols

○ TCP ○ All ports

C.4. Syslog Server

The Ingate has the ability to send the logs seen in the Display Log to a Syslog Server. Syslog Servers store logs over a long period of time. Provide the location of the Syslog Server, and then in Logging Configuration, indicate which of the Ingate Logs you want to go to the Syslog Server. Ensure that the SIP Events are configured as a minimum.



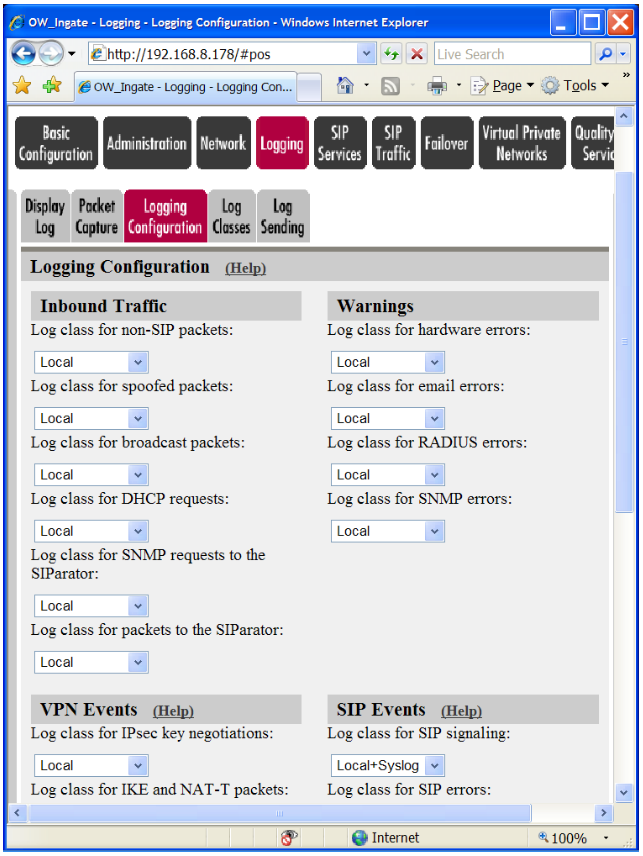
SMTP Server (Help)

DNS name or IP address	IP address

Syslog Servers (Help)

DNS name or IP address	IP address	Delete Row
192.168.8.7	192.168.8.7	□

Add new rows 1 rows.



Logging Configuration (Help)

Inbound Traffic

Log class for non-SIP packets: Local

Log class for spoofed packets: Local

Log class for broadcast packets: Local

Log class for DHCP requests: Local

Log class for SNMP requests to the SIParator: Local

Log class for packets to the SIParator: Local

Warnings

Log class for hardware errors: Local

Log class for email errors: Local

Log class for RADIUS errors: Local

Log class for SNMP errors: Local

VPN Events (Help)

Log class for IPsec key negotiations: Local

Log class for IKE and NAT-T packets:

SIP Events (Help)

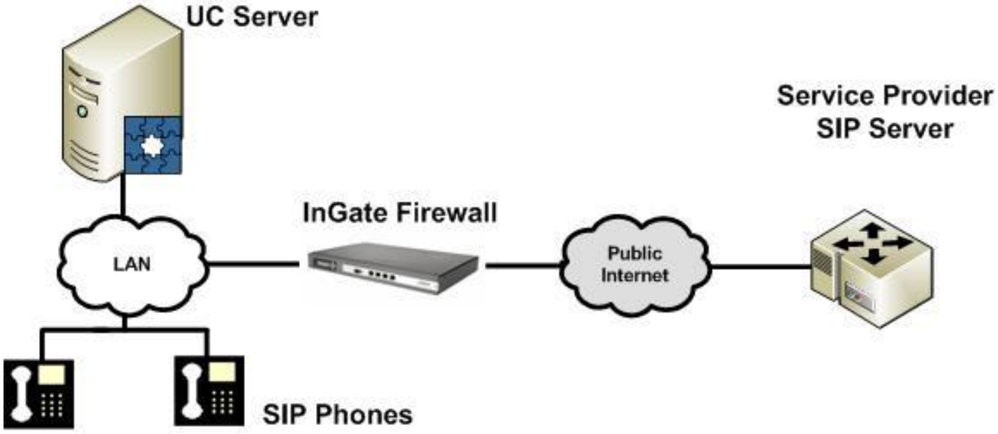
Log class for SIP signaling: Local+Syslog

Log class for SIP errors:

Appendix D Alternate Ingate Configurations

D.1. Ingate Firewall

In this configuration, the Ingate Firewall must have a public IP address on one Ethernet interface, while the rest of the Ethernet interfaces are connected to the internal network. Internal SIP users and devices must configure the firewall as the Default Gateway.



D.1.1. DMZ SIParator

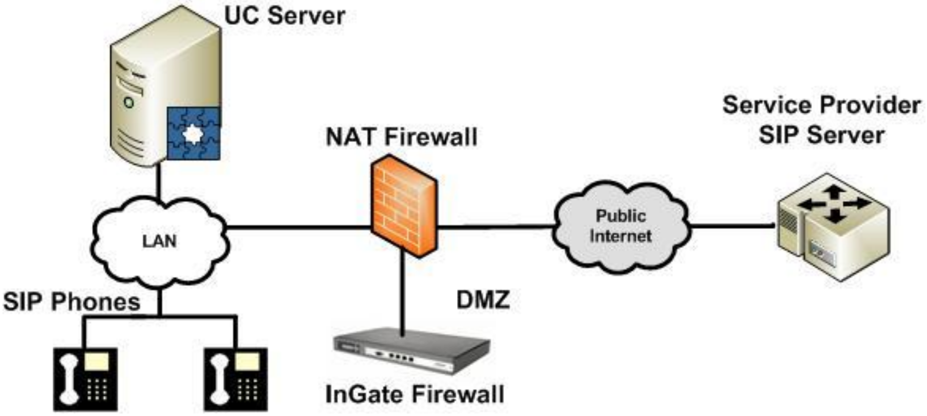
Using this configuration, the SIParator is located on the DMZ of the firewall and is connected to it with only one interface. Note that the SIParator must have a public (non-NAT) IP address for the SIP signaling to work correctly. The SIP traffic reaches the SIParator using DNS or by setting the SIParator as an outbound proxy on the clients. This is the most secure configuration, since all traffic goes through both the firewall and the SIParator. It is also the most flexible, since all networks connected to any of your firewall’s interfaces can be SIP-enabled.

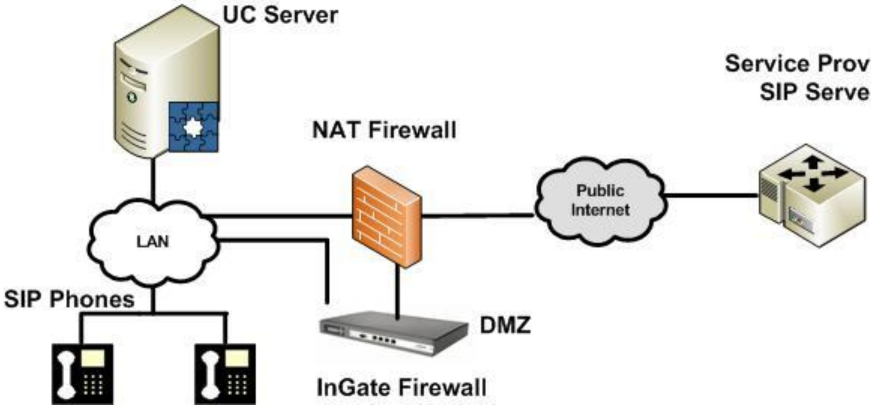
On the firewall, open the SIP port (normally UDP port 5060), and an open range of UDP ports for RTP traffic between the SIParator and the Internet, as well as between the SIParator and the internal networks. The firewall must not use NAT for the traffic between the SIParator and the internal networks or for the traffic between the SIParator and the Internet. However, the SIParator can itself use NAT for traffic to the Internet.

D.1.2. DMZ/LAN SIParator

Using this configuration, the SIParator is connected to the DMZ of the firewall with one of the Ethernet interfaces, while the rest of the interfaces are connected to the internal network. Note that the SIParator must have a public (non-NAT) IP address for the SIP signaling to work correctly. The SIParator can handle several networks on the internal interface even if they are hidden behind routers.

On the traditional firewall, open the SIP port (normally UDP port 5060), and a range of UDP ports for RTP traffic between the SIParator and the Internet. The other interface of the traditional firewall is connected to the internal network. Internal SIP users and devices have to configure the SIParator either as an outbound proxy, or an internal proxy has to use the SIParator as an outbound proxy.





Appendix E Glossary

ALG Application Layer Gateway (also known as Application-Level Gateway) consists of a security component that augments a firewall or NAT employed in a computer network. It allows legitimate application data to pass through the security checks of the firewall that would have otherwise restricted the traffic for not meeting its limited filter criteria.

Carrier A telephone company (or telco) provides telecommunications services such as telephony and data communications.

DNS The domain name system (DNS) stores and associates many types of information with domain names, but most importantly, it translates domain names (computer host names) to IP addresses.

Domain A group of networked computers that share a common communications address.

Enterprise A company organized for commercial purposes; a business firm.

ENUM T**E**lephone **NU**mber **M**apping is a suite of protocols to unify the telephone numbering system E.164 with the Internet addressing system DNS by using an indirect lookup method, to obtain NAPTR records. The records are stored in a DNS database.

FQDN A fully qualified domain name is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish a FQDN from a regular domain name, a trailing period is added, e.g., somehost.example.com. A FQDN differs from a regular domain name by its absoluteness; that is, a suffix cannot be added.

IP Address A unique address that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol (IP) standard— in simpler terms, a computer address.

ISP An Internet Service Provider (also called Internet Access Provider) is a business or organization that provides consumers with access to the Internet and related services.

ITSP An Internet Telephony Service Provider offers an Internet data service for making telephone calls using VoIP (Voice over IP) technology.

LAN A local area network is a computer network covering a small geographic area, such as a home, office, or a group of buildings.

NAT The process of Network Address Translation (also known as network masquerading, native address translation or IP-masquerading) involves re-writing the source and/or destination addresses of IP packets as they pass through a router or firewall.

Port A software port is a virtual data connection that can be used by programs to exchange data directly, instead of going through a file or other temporary storage location. The most common of these are TCP and UDP ports which are used to exchange data between computers on the Internet.

Proxy A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services.

PSTN The public switched telephone network is the network of the world's public circuit-switched telephone networks, in much the same way that the Internet is the network of the world's public IP-based packet-switched networks. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital, and now includes mobile as well as fixed telephones.

RTP Real-time Transport Protocol defines a standardized packet format for delivering audio and video over the Internet.

Service Provider See ISP, ITSP, or Carrier.

SDP Session Description Protocol is a format for describing streaming media initialization parameters. SDP is intended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation.

SIP Session Initiation Protocol is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.

SIP Trunk SIP Trunking is the mechanism used to interconnect SIP enabled PBX's and/or SIP User Agents to each other to establish voice sessions between each other over an IP network. Utilizing the now universal SIP Standard for signaling, SIP Trunking has emerged as a viable alternative to legacy (TDM) and fixed-line circuits for the establishment and transmission of voice communications.

SRTP The Secure Real-time Transport Protocol (or SRTP) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications.

Syslog A protocol for forwarding log messages in an IP network.

TCP The Transmission Control Protocol is a virtual circuit protocol that is one of the core protocols of the Internet protocol suite, often simply referred to as TCP/IP. Using TCP, applications on networked hosts can create connections to one another, over which they can exchange streams of data using Stream Sockets. The protocol guarantees reliable and in-order delivery of data from sender to receiver.

TDM Time-division multiplexing (TDM) is a type of digital or (rarely) analog multiplexing in which two or more signals or bit streams are transferred apparently simultaneously as sub-channels in one communication channel, but physically are taking turns on the channel. The time domain is divided into several recurrent timeslots of fixed length, one for each sub-channel. A sample, byte or data block of sub-channel 1 is transmitted during timeslot 1, sub-channel 2 during timeslot 2, etc. One TDM frame consists of one timeslot per sub-channel. After the last sub-channel the cycle starts all over again with a new frame, starting with the second sample, byte or data block from sub-channel 1, etc.

TLS Transport Layer Security and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, and other data transfers.

UDP The User Datagram Protocol is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages sometimes known as datagrams (using Datagram Sockets) to one another. UDP is sometimes called the Universal Datagram Protocol.

WAN Wide area network is a computer network that covers a broad geographical area (i.e., any network whose communications links across metropolitan, regional, or national boundaries). Or, less formally, a network that uses routers and public communications links.