



VoIP Application Note:

AltiGen IP-PBX SIP Trunk Configuration Using
Bandwidth.com



Prepared by: Sean Rivers
Date: 5/1/09



Table of Contents:

GOAL..... 3

INTRODUCTION 3

PREREQUISITES 3

 SIP TRUNKING INFORMATION PROVIDED BY BANDWIDTH.COM: 3

 EDGEMARC 4500 SERIES: 3

 INGATE SIPARATOR SERIES:..... 3

 ALTIEN MAX 1000:..... 3

 REFERENCES:..... 3

INSTALLATION WORKSHEET..... 4

 WAN SIDE: 4

 LAN SIDE:..... 4

 PBX INFO:..... 4

 NAT TRAVERSAL: 4

 NOTES: 4

CALL QUALITY MANAGEMENT..... 5

 INTERNET ACCESS QUALITY:..... 5

Traffic Shaping: 5

Voice Optimized Internet Access: 5

Packet Prioritization:..... 5

 LAN QUALITY:..... 5

SIP Aware Firewall / ALG:..... 5

VLANs:..... 5

PoE: 5

APPROVED NETWORK TOPOLOGIES..... 6

 INGATE SYSTEMS – SIPARATOR/FIREWALL: 6

 EDGEWATER NETWORKS - EDGEMARC APPLIANCE: 6

INGATE SIPARATOR CONFIGURATION..... 7

EDGEMARC CONFIGURATION 9

ALTIEN SETUP 12

 TURN ON SIP TRUNKING 12

 CONFIGURING IN ALTIENTERPRISE MANAGER 12

CONFIGURING IN ALTIWARE ADMINISTRATOR 13

NUMBERING INFO 17

INITIAL TESTING AND TROUBLESHOOTING 17

 INITIAL TEST PLANS: 17

 TROUBLESHOOTING GUIDE:..... 17

NOTES: 18

Configure an AltiGen IP-PBX

Goal

Provide a reference to AltiGen-certified dealers for configuring an AltiGen IP PBX (AltiServ) with Bandwidth.com's SIP Trunking service.

Introduction

From an AltiGen administrator's point of view, a SIP trunk is very similar to a Triton analog trunk. Once it is up and running, administrators can assign a trunk access code to it. They also can mix SIP trunks with analog trunks, T1, or PRI trunks in the Out Call Routing table. Like analog trunks, each SIP trunk has a PSTN number. They can also receive caller name as well as caller ID.

Prerequisites

SIP trunking information provided by Bandwidth.com:

- Primary, SIP proxy server IP address **216.82.224.202** or DNS **sp-udp01.iad.bandwidth.com**
- Secondary, SIP proxy server IP address **216.82.225.202** or DNS **sp-udp01.sna.bandwidth.com**
- Or, you can use DNS SRV **ot.bandwidth.com** (the EdgeMarc router supports this)
- Trunking DID(s):
 - The DID(s) are forwarded to the Public WAN IP address(s), DNS or DNS SRV records of the EdgeMarc or InGate SIParator.

EdgeMarc 4500 series:

The EdgeMarc is used to provide NAT traversal for SIP messaging. It is also a SIP-aware firewall and VoIP traffic shaping device.

- Production release VOS software 7.9.9 or better
- Private LAN IP Address
- Public IP address for WAN SIP Trunking
- Private IP address of the Altigen

InGate SIParator series:

The InGate SIParator is used to provide NAT traversal for SIP messaging. It is optionally capable of providing a SIP-aware firewall and tagging packets for SIP QoS.

- Production release 4.5.2 (or better)
- Private LAN IP Address
- InGate Startup Tool 1.1.7 (or better)
- Private IP address of the AltiGen IP-PBX
- Public IP address for WAN SIP trunking

AltiGen Max 1000:

- AltiWare Version 6.0 Update 1 ACC or ACM (or better)
- Any phones that work with Altigen Max 1000

References:

- Ingate SIParator [Getting Started Guide](#)
- AltiGen Administrator's Guide
- EdgeMarc 4500 [Administrator's Guide](#)
- Bandwidth.com Connecting with SIP



Installation Worksheet

Use this form to aid in setting up your SIP Trunking service.

WAN Side:

Internet Access Type & Speed:	
WAN IP Address:	
WAN Subnet Mask:	
WAN Gateway IP Address:	

LAN Side:

LAN IP of SIPParator/EdgeMarc:	
LAN Subnet Mask:	
LAN IP Address of AltiGen IP-PBX:	
VLAN ID:	

PBX Info:

Model:	
Firmware Version:	
Number of SIP Trunk Licenses:	
Add-on Software Applications:	
Number of Users:	
Number of Concurrent Calls:	

NAT Traversal:

Devise:	
Serial #:	
MAC:	
Firmware Version:	

Notes:



Call Quality Management

Internet Access Quality:

Traffic Shaping: The EdgeMarc appliance from EdgeWater Networks is the device we use to deploy traffic shaping. It shapes both inbound and outbound data/voice using standard TCP collision management. The benefit of this method is very competent voice quality on any Tier 1-provided Internet connection. For more information on this, check out the knowledgebase at www.edgewaternetworks.com.

Voice Optimized Internet Access: Voice Optimized Internet access is a specially delivered circuit with two separate subnets: one prioritized for voice, and one for data. The benefit of this method is that it is offered on DSL and T-1, and the voice quality is excellent. There is also a proprietary router provided with this solution. The InGate or EdgeMarc can still be used behind the router for NAT traversal.

Packet Prioritization: This method utilizes priority marked queues or packets to ensure quality across the carrier Internet backbones.

Qwest Priority T-1 – This method provided by Qwest allows voice to reside on a priority queue for outbound traffic. The issues with this method are price and non-prioritization of inbound traffic. This is also only available on Internet T-1s.

LAN Quality:

SIP Aware Firewall / ALG: Most people think of a firewall as purely a security device, but most one-way and no-way audio issues can be traced to an improperly configured or non-SIP ALG firewall devices. Bandwidth.com supports the InGate SIParator and the EdgeMarc from Edgewater networks and has tested and certified it to handle both the security needs of the customer network and the ALG needs of the SIP trunking service.

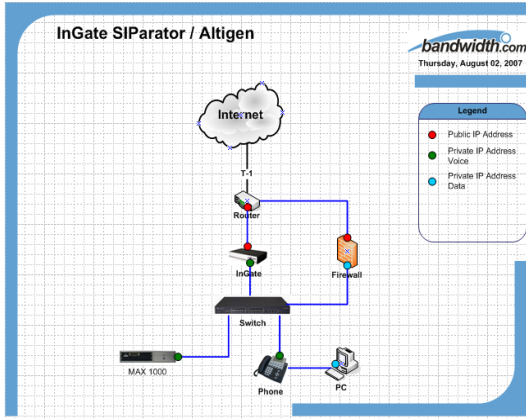
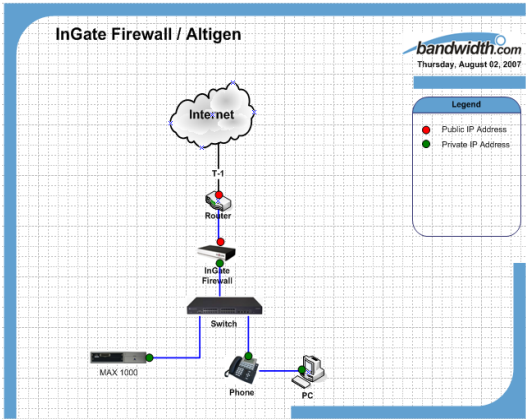
VLANs: VLANs are a standard way to separate virtually the voice and data traffic on the customer LAN. This allows for easy prioritization and limits the effect of viruses and other broadcast events on the customer's network from affecting voice quality.

PoE: While PoE provides power to the phones, it also cleans power and can reduce or eliminate power-related issues, such as hum and static, on IP phones.

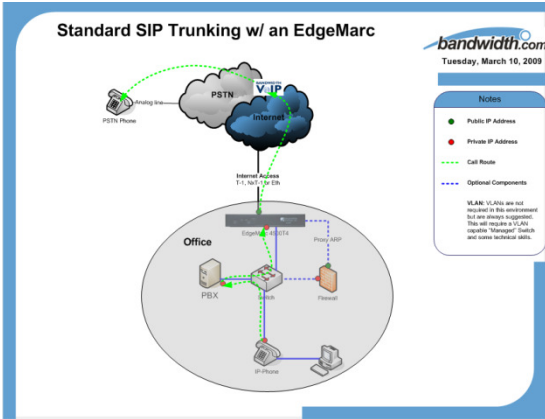


Approved Network Topologies

Ingate Systems – SIParator/Firewall: The Ingate SIParator is an appliance that provides SIP ALG for NAT traversal. The SIParator is utilized when there is a complex network in place and the implementation requires a standalone VoIP appliance. InGate also has a firewall product with QoS options. For more information, visit www.ingate.com.

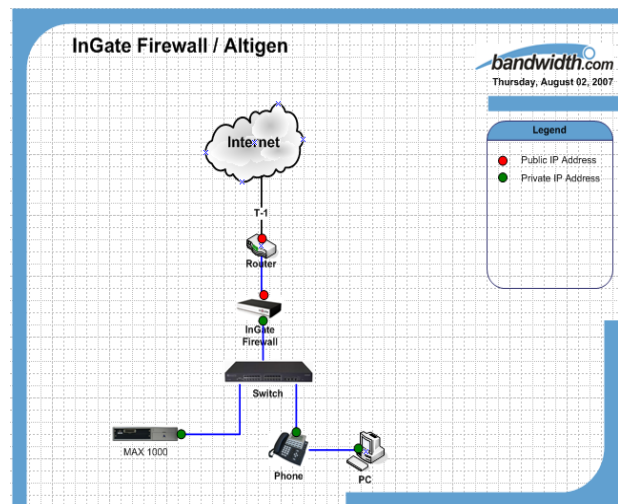
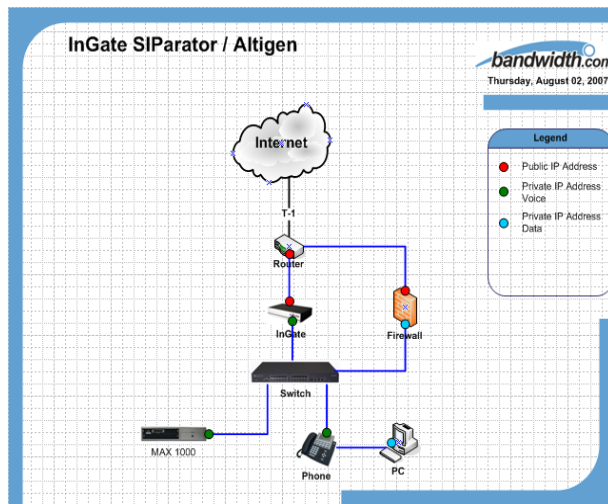



Edgewater Networks - EdgeMarc Appliance: The EdgeMarc Network Appliance is a Router with either T-1 or a 10/100 WAN interface. It also has four switched 10/100 LAN interfaces. The EdgeMarc will provide SIP ALG for NAT Traversal, Traffic Shaping and a fully functional firewall. The EdgeMarc will also resolve Bandwidth.com’s DNS SRV record to allow for SIP survivability. Typically, the EdgeMarc is used when a T-1 router is needed with Traffic Shaping, but it can reside behind an existing router. For more information, visit www.edgewaternetworks.com.



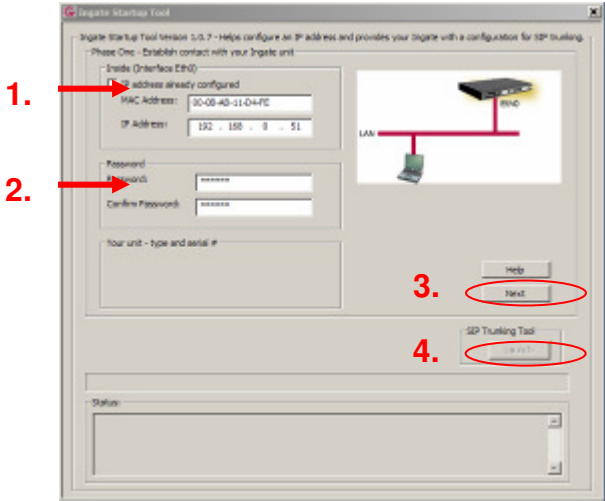
InGate SIParator Configuration

This configuration assumes that the SIParator is set at the factory default. If the SIParator is coming from Bandwidth.com, it will most likely be pre-configured for your network.

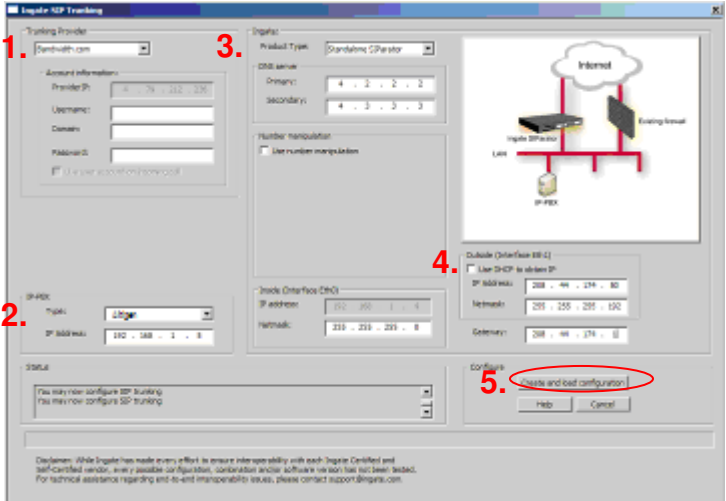


1. If the SIParator was preconfigured by Bandwidth.com, skip to step 10.
2. Go to "www.ingate.com" -> "**Support**" -> "**Register Account**" and register your company.
3. Choose Login to the site and choose "**Register a new unit.**" Make sure you have your serial number in front of you.
4. Activate the necessary licenses using "**Activate License**" link. This will download a .lic file for each license file required. If you are downloading more than one license, you will need to rename the files so that they do not overwrite each other. Typical license examples are: SIP trunking (typically comes with SIParator when delivered by Bandwidth.com), additional call traversal licenses, QoS, and SIP-Aware Firewall.
5. Next you will need to download the latest "**InGate Startup Tool**", a link is provided in the InGate portal.
6. Once the InGate Startup Tool is downloaded, please install it on the computer that will be configuring the InGate.
7. Connect the laptop or computer with the InGate Startup Tool to the Eth0 port on the SIParator using a standard CAT5 Ethernet cable.
8. After connecting the SIParator, double-click on the  on your desktop. Insure the laptop or computer being used is on the same LAN subnet as the SIParator.
9. Plug the SIParator into a power source.

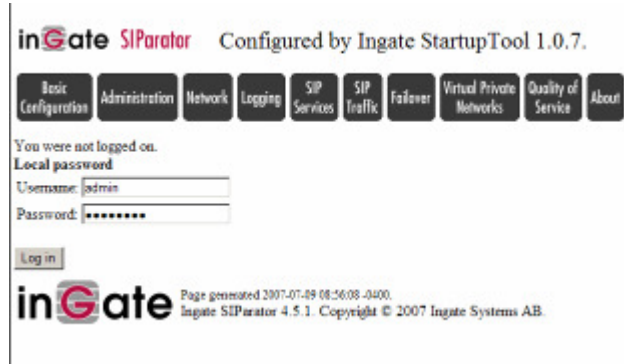
1st Screen



2nd Screen

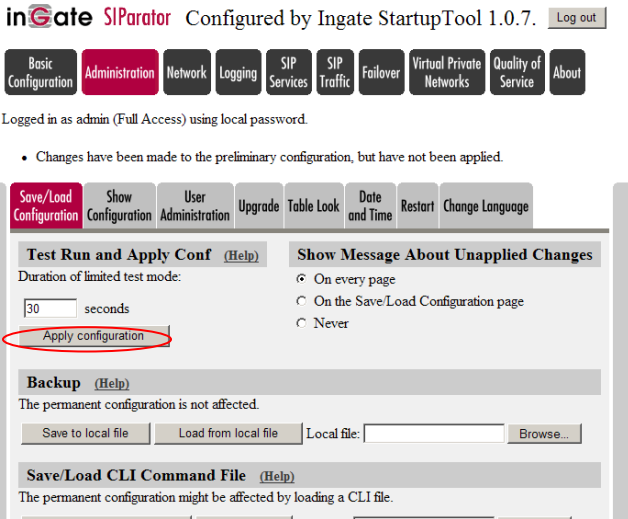


Web GUI Login



Apply Configuration

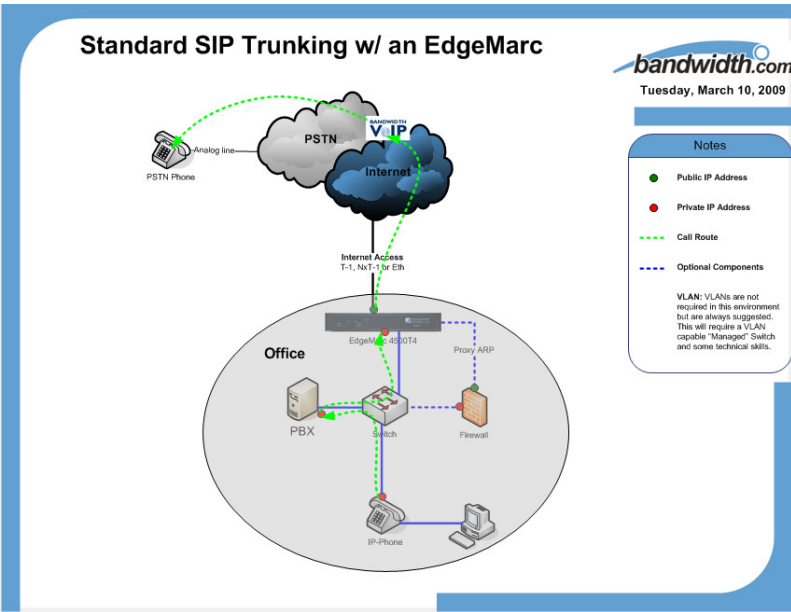
(this is a 2 step process; be sure to confirm!)



10. Once the setup is complete, connect the WAN network to the **Eth1** port and the LAN network (same as PBX) to the Eth0 port of the SIParator.

EdgeMarc Configuration

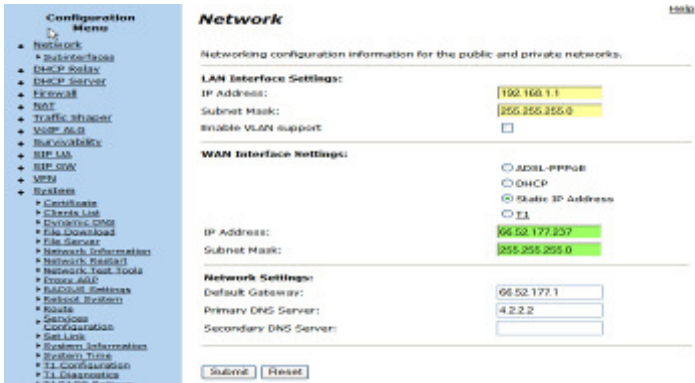
This configuration assumes that the EdgeMarc is set at the factory default. If the EdgeMarc is coming from Bandwidth.com, it will most likely be pre-configured for your network.



1. Connect and configure PC to the LAN subnet to which the Edgemarc is connected.
2. Log into the EdgeMarc (Factory Default) by opening a web browser and entering <http://192.168.1.1> Once you have clicked on the link, you will be prompted for a login:

Login: root
Password: default

3. Click on the “Network” link.
4. Configure the “WAN and LAN Interface Settings”



5. Select “Submit”
6. Click on the “DHCP Server” link and disable the DHCP server;



Configuration Menu

- Network
- DHCP Relay
- DHCP Server
- DHCP Leases
- Firewall
- NAT
- Traffic Shaper
- VoIP ALG
- Survivability
- SIP UA
- SIP GW
- VPN
- System
- Certificate
- Clients List
- Dynamic DNS
- File Download
- File Server
- Network Information
- Network Restart
- Network Test Tools
- Proxy ARP
- RADIUS Settings
- Reboot System
- Route

Help

DHCP Server

DHCP IP Address Ranges		
Start Address	End Address	Action
192.168.1.150	192.168.1.199	[X]
192.168.1.2	192.168.1.2	Add

Enable DHCP Server:

Subnet Mask: 255.255.255.0

Lease Duration (Days): 7

Time Offset, +/- hours (option 2):

NTP Server Address (option 42):

WINS Address (option 44):

TFTP/FTP Server Name (option 66): 192.168.1.1

VLAN ID Discovery (option 129):

From Network page:

Primary DNS: 205.171.3.65

Secondary DNS: 205.171.2.65

Default Gateway: 192.168.1.1

7. Select **“Submit”**
8. Click on the **“VoIP ALG”** link
9. Select **“SIP”**
10. Configure **“SIP Server Address”** and port (typically port 5060 for SIP). Add the DNS SRV Record: **ot.bandwidth.com** under **“SIP Server Domain Name”** or click **“Add Row”** and enter the following two SIP Server Addresses: **216.82.224.202** and **216.82.225.202** using port 5060 for both. The EdgeMarc will direct all Outbound calls to the primary SIP server address and failover to the secondary should a service outage go into effect. Make sure to check the box marked, **“Enable Multi-homed Outbound Proxy Mode”**.

SIP ALG using DNS SRV

Help

SIP Settings

SIP protocol settings.

The SIP Server settings specify the address and port that all client traffic shall be forwarded to.

SIP Server Address:

SIP Server Port:

List of SIP Servers:

Enable Multi-homed Outbound Proxy Mode:

Enable Transparent Proxy Mode:

Limit Allowed Proxies:

Stale Timer
The stale timer, if set, is used to automatically delete SIP clients that have not registered within the given time period.

Stale client time (m):

Registration Rate-Pacing parameters are available on the [Survivability page](#).

Check that DNS SRV works in the Survivability section

Current SIP Server reachability status:

Name	Address	Port	P	W	Lost	Rcvd	Status
sp-udp01.iad.bandwidth.com	216.82.224.202	5060	100	10	0	0	Active
sp-udp01.atl.bandwidth.com	4.79.212.236	5060	200	10	0	0	Idle
sp-udp01.snv.bandwidth.com	216.82.225.202	5060	300	10	0	0	Idle

SIP Server Redundancy Configuration

Redundancy allows the DNS server to give multiple SIP Server names in the answers to SRV lookups. Each server will be monitored using periodic messages and the highest priority answer which is currently reachable will be used for signaling.

SIP Server Redundancy Settings:

Enable SIP server redundancy:

Enable forward next REGISTER:

Enable sticky failover mode:

Enable keepalive messages for active server:

Time for declaring SIP messages lost (seconds):

SIP ALG using primary and secondary IP addresses

SIP Settings

SIP protocol settings.

The SIP Server settings specify the address and port that all client traffic shall be forwarded to.

SIP Server Domain name:

List of SIP Servers:

Priority	Sip Server Address	Port	x
0	216.82.224.202	5060	[X]
1	216.82.225.202	5060	[X]

Enable Multi-homed Outbound Proxy Mode:

Enable Transparent Proxy Mode:

Limit Allowed Proxies:

Stale Timer
The stale timer, if set, is used to automatically delete SIP clients that have not registered within the given time period.

Stale client time (m):

Registration Rate-Pacing parameters are available on the [Survivability page](#).

11. Select **“Submit”**

12. Select “SIP Trunking Page”
The SIP Trunking device needs to point to the IP-PBX’s IP address.

Configuration Menu

- Network
- DHCP Relay
- DHCP Server
- Firewall
- NAT
- Traffic Shaper
- VoIP ALG
 - H.323
 - MGCP
 - SIP
 - Trunking
- Survivability
- SIP UA
- SIP GW
- VPN
- System
 - Certificate
 - Clients List
 - Dynamic DNS
 - File Download
 - File Server
 - Network Information
 - Network Restart
 - Network Test Tools

SIP Trunking

Configuration of SIP trunking devices.

SIP Trunking devices

A SIP trunking device can be a PSTN gateway, or similar device, that does not issue REGISTER messages. Calls will be forwarded to the device based on the dial-plan rules below.

SIP Trunking Devices			
Select: All None			Action: Delete
Address	Port	Name	
<input type="checkbox"/> 192.168.1.2	5060	PBX	

Add a target

Action: Add new target

Name:

Address:

Port:

[Commit](#) [Reset](#)

13. Select “Commit”
14. Select “SIP Trunking Page – Rules”
Add a default call routing rule, which will route any inbound call to the PBX

- Proxy ARP
- RADIUS Settings
- Reboot System
- Route
- Services Configuration
- Set Link
- System Information
- System Time
- T1 Configuration
- T1 Diagnostics
- TACACS Settings
- Upgrade Firmware
- User Commands
- VoIP Subnet Routing
- VLAN Configuration

| Home | Help |

Rules

Rules are used to forward incoming calls to a specific SIP trunking device based on a pattern-matching string for the called number.

Dial Rules			
Select: All None			Action: Delete
Pattern-match	Strip	Add	Target
<input type="checkbox"/> Default Rule			PBX (192.168.1.2:5060)

Add a rule

Action: Add new rule

Default rule:

Pattern-match (if not default):

Strip digits:

Add string:

Target: Internal Gateway (192.168.1.253:1026)

[Commit](#) [Reset](#)

15. Select “Commit”
16. To allow for **Remote Phone Registration** and Calling make the following changes
 - a. Configuration Changes → NAT – enter the following NAT statements
 - i. tcp;WAN_IP / WAN_SUBNET - 10032>ALTIGEN_IP-10032
 - ii. tcp;WAN_IP / WAN_SUBNET - 10064>ALTIGEN_IP-10064
 - iii. udp;WAN_IP / WAN_SUBNET - 10060>ALTIGEN_IP-10060
 - b. Configuration Changes → System → User Commands – enter the IP Tables commands
 - i. iptables -I FORWARD 1 -i eth1 -d ALTIGEN_IP -p udp --dport 49152:49211 -j ACCEPT
 - ii. iptables -A PREROUTING -t nat -p udp --dport 49152:49211 -d WAN_IP -j DNAT --to ALTIGEN_IP:49152-49211
 - iii. iptables -A POSTROUTING -t nat -p udp -s ALTIGEN_IP --dport 49152:49211 -j SNAT --to WAN_IP
 - iv. iptables -t nat -A POSTROUTING -p udp -d ALTIGEN_IP --dport 49152:49211 -s LAN_BLOCK 192.168.1.0/24 -j SNAT --to LAN_IP

AltiGen Setup

Turn on SIP Trunking

1. Obtain a SIP trunk license from AltiGen.
2. Register the license using AltiGen's online license registration procedure.

6RP0000018-38D074C506	C8BE7623A7	UNKNOWN OR OBSO
R414000018-4ED055C7CE	E452465478	IP TALK SESSION
R505200018-BCF632CA31	F6C9AD7DE6	SIP TRUNK (5)

3. Reboot AltiServ.
4. After the system is rebooted, **SIP-Trunk** should show as "not ready" in Trunk View.

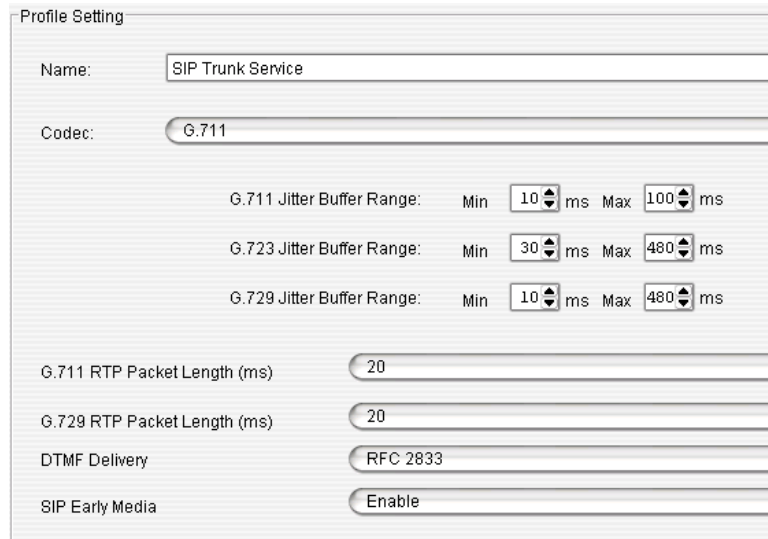
03:069	SIP-Tie	idle
03:070	SIP-Tie	idle
03:071	SIP-Tie	idle
03:072	SIP-Trunk	not ready
03:073	SIP-Trunk	not ready
03:074	SIP-Trunk	not ready
03:075	SIP-Trunk	not ready
03:076	SIP-Trunk	not ready

Configuring in AltiEnterprise Manager

1. Choose **AltiWare Administrator > VoIP > Enterprise Network Management**. This opens AltiEnterprise Manager.
2. In AltiEnterprise Manager, click the **Codec** button.
3. Add a codec profile. In this example, we name the new profile "SIP Trunk Service".

Name
Default
G711
SIP Trunk Service

4. Set the following:
 - **Codec** = G.711
 - **DTMF Delivery** = RFC 2833
 - **SIP Early Media** = Enable



Profile Setting

Name: SIP Trunk Service

Codec: G.711

G.711 Jitter Buffer Range: Min 10 ms Max 100 ms

G.723 Jitter Buffer Range: Min 30 ms Max 480 ms

G.729 Jitter Buffer Range: Min 10 ms Max 480 ms

G.711 RTP Packet Length (ms): 20

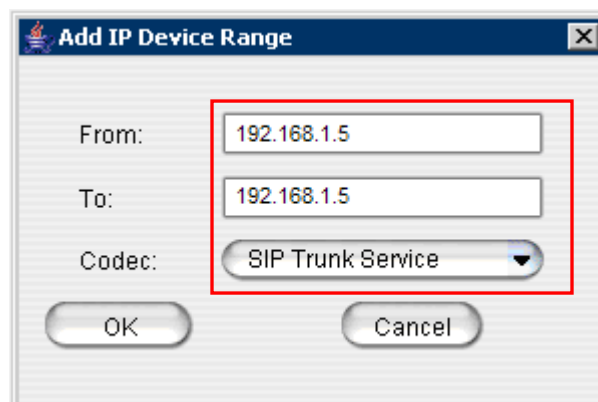
G.729 RTP Packet Length (ms): 20

DTMF Delivery: RFC 2833

SIP Early Media: Enable

5. In AltiEnterprise Manager, go to **Servers** button > **IP Codec** tab > **IP Device Range** panel. Add a range, using the SIP Proxy IP address that you got from your service provider. Use the LAN side address of the InGate or EdgeMarc. In this example, the IP address is 192.168.1.5. The range we add is:

- **From:** 192.168.1.5
- **To:** 192.168.1.5
- Set **Codec** as "SIP Trunk Service".



Add IP Device Range

From: 192.168.1.5

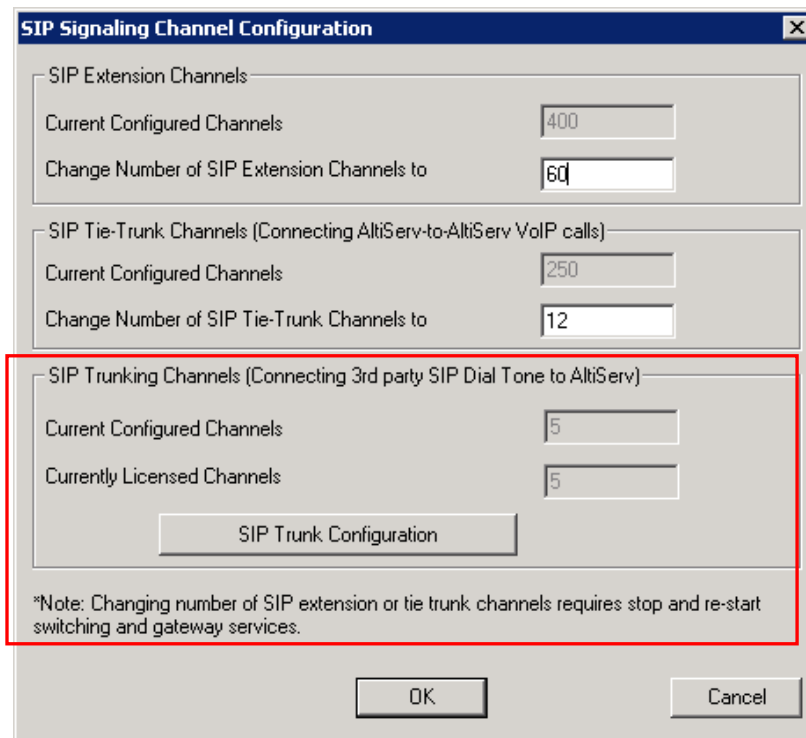
To: 192.168.1.5

Codec: SIP Trunk Service

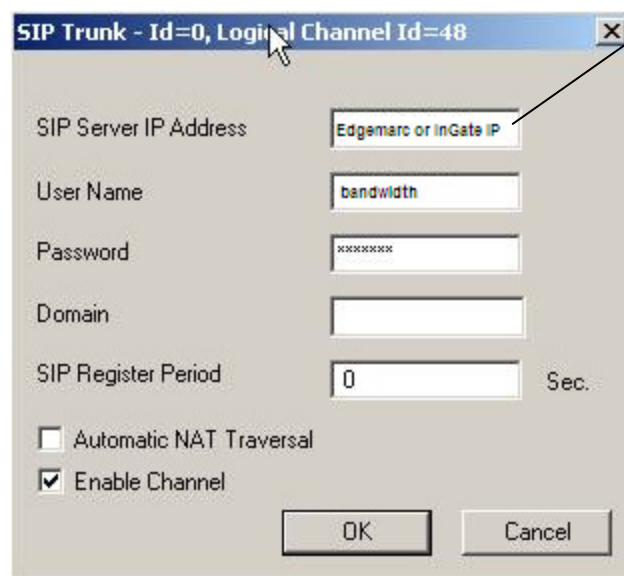
OK Cancel

Configuring in AltiWare Administrator

1. Under "SIPSP" board configuration, the number of configured channels and licensed channels are displayed. In this example, there are 5 SIP trunk channels.



2. Click the **SIP Trunk Configuration** button. The SIP Trunk Configuration dialog box opens.
3. Highlight an entry in the dialog box, and then click **Edit**. The following dialog box opens:

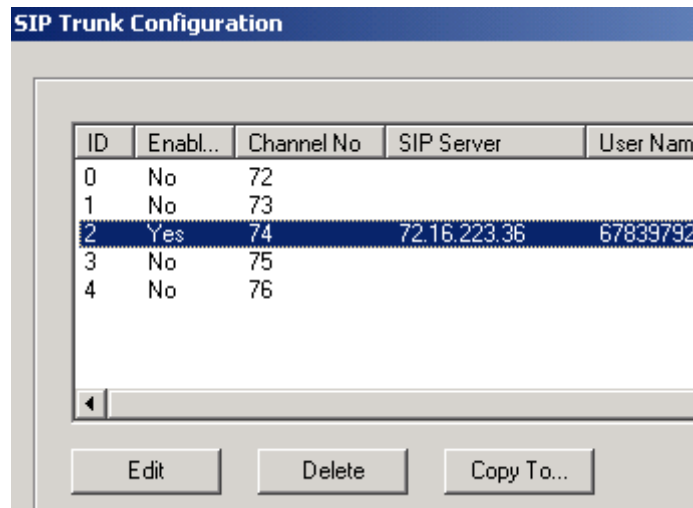


This is either LAN IP of the EdgeMarc or InGate ALG Firewall

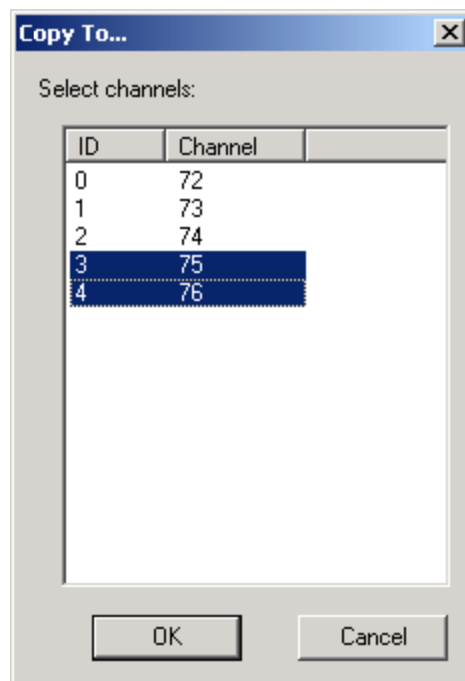
4. Enter the SIP Server IP Address, User Name <bandwidth>, Password <bandwidth>, and SIP Register Period <0>.
5. Uncheck **Automatic NAT Traversal** and check **Enable Channel**.

If multiple SIP trunks are subscribed, follow the steps below to copy the same settings to other SIP channels.

1. Highlight the source entry.



2. Click the **Copy To** button.



3. Highlight the destination channels and click **OK**.

SIP Trunk Configuration				
ID	Enabl...	Channel No	SIP Server	Us
0	No	72		
1	No	73		
2	Yes	74	72.16.223.36	67
3	Yes	75	72.16.223.36	67
4	Yes	76	72.16.223.36	67

In Trunk View, the SIP trunks will be displayed as **idle**. The SIP trunks are ready to use.

● 03:068	SIP-Tie	idle
● 03:069	SIP-Tie	idle
● 03:070	SIP-Tie	idle
● 03:071	SIP-Tie	idle
● 03:072	SIP-Trunk	not ready
● 03:073	SIP-Trunk	not ready
● 03:074	SIP-Trunk	idle
● 03:075	SIP-Trunk	idle
● 03:076	SIP-Trunk	idle

Configuring SIP trunks (trunk access code, in call routing, outcall routing, and so on) is similar to configuring analog trunks or T1/PRI trunks. See AltiWare Administrator online Help under "Trunk Configuration," or see the *AltiWare Administration Manual*, "Trunk Configuration" chapter.

To work behind the EdgeMarc you will also need to make the following change to your Windows Registry:

HKEY_LOCAL_MACHINE\SOFTWARE\AltiGen Communications, Inc.\AltiWare\Service Providers\SIPSP\EnableStdRouteSet

Needs to be changed from 0 to 1 when using the EdgeMarc. It will need to stay 0 when behind an Ingate.

Numbering Info

Remember that Bandwidth.com wants to see a “+” and a “1” on all outgoing calls, so this must be planned for. Also, we will be sending you a “+” and a “1” on every call, so make sure to plan for this when setting up your PBX. The InGate can add the + for E.164 numbering for you; see this will be done in Number Manipulation in the Setup Tool.

- Operator must be sent as a plain 0 (no 1)
- 911 must be sent as +1911
- 411 must be sent as +1411
- International calls are to be sent without 011. Example: +442151245
- Local and Long Distance Calls; Example: +19192971100

Initial Testing and Troubleshooting

Initial Test Plans:

If you run into an issue with any of these tests, consult the troubleshooting chart bellow:

1. Test an Outbound call to a Local Number. Check for Ringback, 2-way Audio, and Quality.
2. Test an Outbound call to a Long Distance Number. Check for Ringback, 2-way Audio, and Quality.
3. Test an Outbound call to an International Number. Check for Ringback, 2-way Audio, and Quality.
4. Test a Long Outbound call past 15 minutes.
5. Test multiple call concurrencies on Outbound calls. Setup multiple calls to PSTN
6. Test an Outbound Call to Operator “0”
7. Test an Outbound Call to Directory Assistance “411”
8. Test a 911 Call **(PLEASE IDENTIFY TO THE OPERATOR THAT THIS IS A TEST!!!!!!)**
9. Test an Inbound call to an internal DID. Check for Ringback, 2-way Audio, and Quality.
10. Test an Inbound call to Auto-Attendant. Check DTMF and Audio Quality.
11. Test Transferring calls off-site.
12. Test an Outbound call to an Auto-Attendant and verify DTMF.

Troubleshooting Guide:

Issue	Cause	Remedy
No Calls IN/Out	✔ InGate/EdgeMarc Configuration	✔ Check InGate/EdgeMarc Configuration
	✔ PBX Configuration	✔ Check PBX Configuration
	✔ Unqualified IP Address	✔ Note WAN IP Address and Contact Bandwidth.com
No Calls Out	✔ PBX Configuration	✔ Check PBX Configuration
	✔ Unqualified IP Address	✔ Note WAN IP Address and Contact Bandwidth.com
No Calls In	✔ PBX Configuration	✔ Check PBX Configuration
	✔ Unqualified IP Address	✔ Note WAN IP Address and Contact Bandwidth.com
One-Way Audio	✔ InGate/EdgeMarc Configuration	✔ Check InGate Configuration
Echo	✔ Excessive Delay	✔ Check LAN and WAN for high latency
	✔ Echo Cancellation Issue on PBX	✔ Check Echo settings and/or consult PBX
	✔ Echo Cancellation Issue on Bandwidth.com	✔ Call Bandwidth.com and report
Call Dropping	✔ Internet Access Issues	✔ Call Internet Access Provider
	✔ Extreme Latency on LAN	✔ Check Latency on LAN
	✔ SIP issue	✔ Call Bandwidth.com
Static or HUM on Phones	✔ Power issue	✔ Check power if using AC should not be issue in PoE
Missing Parts of Words	✔ Packet Loss or Latency on LAN	✔ Check LAN
	✔ Packet Loss or Latency on WAN	✔ Check with Internet Access Provider
	✔ Jitter Buffer Configuration	✔ Check with PBX



Notes:
